STRATEGIES FOR TEMPLATE-FREE DIRECT BIOMETRIC ENCRYPTION USING VOICE BASED FEATURES

A Thesis Submitted to the University of Kent
For the Degree of Doctor of Philosophy
In Electronic Engineering

By

ALEWO JOSHUA ATAH

SEPTEMBER 2010

Abstract

Current biometric systems references information stored on templates and it possess major drawbacks in their inability, if lost or stolen, to be revoked and re-issued as would be the case with passwords. Thus, once a biometric source has been compromised, the owner of the biometric, as well as the data protected by the biometric, is compromised for life. This research investigates the potential of the voice modality for employment in a template-free biometric system, which requires storage of neither biometric templates nor encryption keys. It works by directly encrypting the biometric data provided by the human voice and therefore eliminates the need for storing templates used for data validation, and thus increasing the security of the system. The research also introduces feature concatenation as a novel method of combining the binary information from the feature sets and also introduces five new revocation strategies based on the template-free method. The promising results allow us to conclude that voice may potentially form the basis for a practical template-free biometric system.

Publications and Manuscripts under Review

[1] J.A. Atah, Gareth Howells, Revocability of biometric keys generated from a voice based template-free biometric system, to appear in Engineering Letters Manuscript Number: EL_2009_12_17a. Manuscript submitted 17 December 2009, accepted 20 April 2010, final camera ready copy submitted 19 June 2010

[2] J.A. Atah, Gareth Howells, Key Generation in a Voice Based Template-free Biometric Security System, *Lecture Notes in Computer Science, Biometric ID Management and Multimodal Communication,* Volume 5707, September 2009, *pp* 170-177.

[3] J.A. Atah, Gareth Howells, Score Normalisation of Voice Features for Template-free Biometric Encryption, the 2008 multi-conference in Computer Science, Information Technology, Computer Engineering, Control and Automation Technology, Orlando, FL, USA (July 2008).

[4] J.A. Atah, Combining normalised voice features for use in efficient template-free biometric security system, World Congress in Computer Science, Computer Engineering, and Applied Computing, Las Vegas, Nevada USA (July 2008).

[5] J.A. Atah, Gareth Howells, Key Generation in a Voice Based Template-free Biometric Security System, Joint COST 2101 & 2102 International Conference on Biometric ID Management and Multimodal Communication 2009, Madrid, Spain, September 2009.

[6] J.A. Atah, Gareth Howells, Integrating Revocable Biometrics within a voice based Template-Free Biometric Security System, the 2009 International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV '09), World Congress in Computer Science, Computer Engineering, and Applied Computing, Las Vegas, Nevada USA (July 2009).

[7] J.A. Atah, Gareth Howells, Analysis of binary information in a voice based template-free biometric security system, International Association for Development of Information Society (IADIS) conference 2009, Algarve, Portugal (June 2009).

[8] J.A. Atah, Gareth Howells, Mapping of Information in Voice Features for use in an Efficient Template - Free Biometric Security System, the 2009 International Conference on Information Security and Privacy (ISP-09), Orlando, FL, USA (July 2009).

[9] Manuscript under Review: J.A. Atah, Gareth Howells, Calibration and Operation in a Voice Based Template-free Biometric Security System, to appear in EURASIP journal of signal processing. Manuscript Number: 504653.v1

Dedication

To the memory of my late father, who was passionate about my earning this degree but unfortunately passed on before the completion of the programme.

Acknowledgements

All glory goes to the almighty God for seeing me through this programme. I couldn't have made it without His help.

My supervisor, Gareth Howells deserves a lot of commendation for guiding me through. I appreciate his patience, thoroughness, and all the support. I also appreciate the contribution of Richard Guest and other members of staff in the School of Engineering and Digital Arts in the University of Kent.

I also thank my family (Monica, Divine, Daniel, and David) for their patience, understanding and support.

I acknowledge the encouragement received from Professor Julius Okojie and Professor Peter Okebukola, who actually urged me to start and kept encouraging me to press on with the programme. Incidentally, both of them will always ask me to explain what my research was all about and the progress made at each stage. Your prying questions actually kept me on my toes and were instrumental to some of my published works.

I appreciate the assistance of the Petroleum Technology Development Fund (PTDF) in Nigeria during this programme.

I also wish to acknowledge the help of Dr. Ahmadu Ali and Erelu Bose Ogumuyiwa. I thank the almighty God for using you as a source of blessing to me during this programme.

Finally, I acknowledge my friends and colleagues who supported me in one way or the other.

Table of Contents

List of figures

List of tables

Chapter 1

Introduction

Biometrics can be defined as an automated method of recognising humans based on physiological or behavioural characteristics. Biometric recognition on the other hand, deals with measuring an individual's suitable behavioral and biological characteristics in a recognition inquiry and comparing these data with the biometric reference data which had been stored during a learning procedure, in order to determine the identity of a specific user.

Following from above, a biometric characteristic is a biological or behavioural property of an individual that can be measured and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of individuals. Examples of such characteristics include voice, face image, gait (which is the way of walking), fingerprint, iris, etc. It is from these characteristics that specific features are derived for use by computers as digital representation of persons which the computer can learn and store, as well as recognize when the same features are re-presented to it at a later time. Therefore, biometric features are information extracted from biometric samples which can be used for comparison with a biometric reference. For example, characteristic measures extracted from a face photograph such as eye distance or nose size etc. A biometric sample is the representation, in analog or digital form, of biometric characteristics obtained from a biometric capture device like camera, scanner, microphone etc, prior to the extraction of features process. Examples of biometric samples include electronic face photograph, fingerprint image, voice sample, etc.

In current traditional biometric systems, there exist stages as identified below:

(i) An initial stage of image capture or signal acquisition (i.e. the image or signal that is acquired from a human being and presented to the computer in a machine readable form).

(ii) Feature extraction and processing stage. The aim of the extraction of biometric features from a biometric sample is to remove any superfluous information which does not contribute to biometric recognition. This enables a fast comparison, an improved biometric performance, and may have privacy advantages.

(iii)Template creation and storage. A biometric template is a digital reference of distinct characteristics that has been extracted from a biometric sample. It represents the biometric measurement of an enrolee used by a biometric system for comparison against subsequently submitted biometric samples. The template is generated during the process of feature extraction, which frees the raw data coming from the biometric sensor from irrelevant information. The template is the digital representation of the biometric data like the analysis of the locations of minutia contained in fingerprints or a mathematical summary of the patterns in an iris image or the digital representation of voice prints that is created and stored. These templates contain the unique characteristics of an individual's biometric information to which future biometric data would be compared in order to achieve authentication or verification. When templates are created, they are stored in computers (may be a database in a centralised server), in a token or smart card that can be carried around, on a workstation, or directly on the biometric sensing device.

(iv)Data comparison for the purpose of authentication (identification or verification). The user subsequently provides his/her biometric data for verification / authentication, during which the sample is quickly processed into a

digital template, which is then compared to those existing in the database to determine a match. This process of converting the provided biometric samples into a digital template for comparison is repeated each time the user attempts to use the system.

A typical template-based biometric system is as represented in figure 1.1. below:

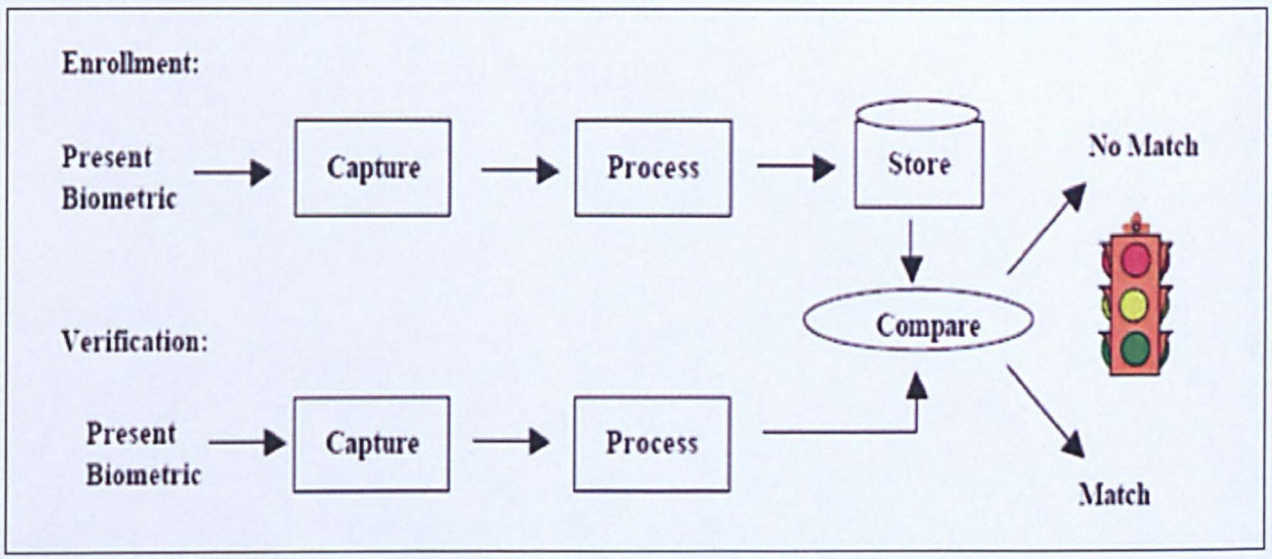

Fig. 1.1: schematic diagram of a template-based biometric system

Stages (i) to (iii) above represent the enrolment process in current biometric systems, which basically obtain an individual's physical and behavioural characteristics and process them by a numerical algorithm to create a digital representation of the obtained biometric and stores it as a template [1]. For the purpose of verification, the same process is followed, except that the new data obtained is compared against the stored template to determine a match.

1.1 Problem Definition

The need to store the biometric data on a medium to be referenced before achieving verification/ authentication has created a potential security risk in biometric technology because the stored data can be stolen, copied, cloned, etc. [2] – [9], [15], [16]. Although it is not easy to do this, it is a major threat that has made the processes in current biometric systems possess the risk of an attacker gaining access to the stored template for fraudulent or unauthorised use. Once biometric systems are successfully compromised, the owner of the biometric as well as the data protected by the biometric is compromised for life because humans cannot ever change their features, and unlike passwords that can be cancelled and reissued if lost or stolen, biometrics cannot be re-issued [10], [11]. In the area of privacy, it has been argued that although technology has improved to the extent that the template cannot be decoded back to the biometric data, it could be used to track the activities of an individual because if there is a database anywhere that ties the user to the unique biometric template, it could be used to perform tracking functions [12]. Public confidence and acceptance of the biometrics technology will depend on the ability of system designers to demonstrate that these systems are robust, have low error rates and are tamper proof. This is therefore the challenge that this research is set out to address.

1.2 Motivation

From section 1.1 above, it has been shown that biometric data stored on templates are susceptible to risks. Jain et al [13] clearly showed that data stored on a template can be attacked and subsequently compromised. As a result of these fears for the safety of biometric data, there have been various attempts at securing such captured biometric measurements [14]. Thus, a new trend in biometric research is in the protection of biometrics systems themselves. Such efforts have looked at revocable biometrics [2] – [9], [15], [16], and broad based Template Security [13], [14], [17]. However, these efforts are still dependent on some form of template storage and as long as template

data are stored somewhere to form the basis for matching, the security of the system will be susceptible to cases of compromise because it largely depends on several other factors. For instance, if the owner of the biometric sensor fails to keep the biometric private, then the confidence in revocable biometrics will be eroded because its security depends on the secure management of the distortion parameters (i.e. the disguised or cancellable parameters), which must be used for enrolment and made available at matching. The storage of the original or distorted information on a template equally makes the system vulnerable because if the individual responsible for the safety of such template deliberately or by error exposes the system to attack, the entire system will be compromised.

It has therefore become justifiable to design biometric systems that will eliminate the need for template storage of data before achieving authentication. In addition, the need for remote authentication using existing infrastructure is ever increasing. Such needs are found in e-banking, e-commerce, smartcards, remote password reset etc., and voice has been found useful in achieving remote authentication. The choice of voice as the modality to employ in this research stems from the fact that it has many advantages over other biometrics such as:

- In many applications, speech may be the main or only modality (e.g. telephone transactions), so users do not consider providing a speech sample for authentication as a separate or intrusive step.

- The telephone system provides a ubiquitous, familiar network of sensors for obtaining and delivering the speech signal. Therefore, in telephone based applications, there is no need for special signal transducers or networks to be installed at application access points since a cell phone gives one access almost anywhere.

- Infrastructure for other non-telephone applications are readily available e.g. sound cards and microphones are low-cost and readily available.

- Speech is a natural signal to produce and users do not consider its provision threatening.

- Speaker recognition area has a long and rich scientific basis with over 30 years of research, development, and evaluations.

- Finally, voice has a higher advantage over other biometrics characteristics because in voice, we can change what password or code that an individual says. Thus it combines the advantage of two factor authentication ('what you are' e.g. your voice and 'what you know' e.g. a password).

Therefore, the challenge that this research seeks to address is in the development of a new approach to biometric encoding which will eliminate the need for a template of pre-captured data being used as a basis for comparison before authentication is achieved, thereby significantly reducing both fraudulent authoring of information and fraudulent access to confidential documents. This technique will exploit the possibility of directly encrypting the biometric data provided by the individual's voice and develop a method of directly generating an encryption key based on the voice features. This will eliminate the need for storing templates used for data validation, therefore increasing the security of the system. The implication is that the system proposed in this research seeks to combine the advantages in voice biometric to build a template-free system that will essentially directly encrypt the biometric data provided by the individual's voice, thus eliminating the need for storing templates used for data validation, and in turn increasing the security of the system.

1.3 Scope of the Research

This research initially presents the processes involved in current biometric systems and the issues of concerns raised by the storage of biometric data on a template. In order to overcome these concerns related to template storage of biometric data as outlined above, this research proposed and investigated the possibility of directly encrypting the biometric data provided by the individual using the potential of the human voice modality. In order to achieve this, the study considered the characteristics that made voice to be useful in biometric recognition and investigated the stable features derivable from the human voice that can be used to directly generate biometric keys. The research subsequently presents the basic operating principles of template-free biometrics and introduced feature concatenation as a novel method of combining the binary information generated from the voice feature sets to build an efficient template-free biometric system.

Bearing in mind that template-free biometrics aims only at eliminating template-based vulnerabilities, and that other vulnerable points in biometric systems can introduce compromises that may affect the keys generated based on template-free biometrics, the research further investigated the techniques used in revocable biometrics with the view to establishing the possibility of using the concept to annul keys generated from template-free biometrics. This is mainly by disguising the biometric information used to generate keys in template-free system; hence a new set of biometric information is produced to annul previously used keys and thus reduces problems of compromise associated with other vulnerable points in biometric systems.

This research scope does not include studies on the voice capture infrastructure like the microphone or the telephone handset and their various types which may introduce variations in the value of the signals introduced into the encryption algorithm. This is because it is expected that the choice of the infrastructure used for implementing voice based template-free systems is made ab-initio.

1.4 Aims and Objectives

The overall aim of this research is to investigate and develop strategies for the novel concept of template-free biometrics using human voice modality.

To achieve this aim, the research targeted the following objectives:

- Evaluating candidate features extracted from the human voice that can be employed in template-free systems.
- Outline the principles of template-free biometrics based on voice strategy
- Introducing feature concatenation as the novel technique for voice feature combination as a means of combining the biometric codes generated from template-free systems.
- Investigating techniques for the integration of revocable biometrics with template-free biometrics in order to enhance security and preserve privacy by taking away the control of biometric system from the hands of either an attacker, the owner of the biometric sensor used for signal/sample capture, or those with access to the algorithm.

1.5 Thesis Outline

Following from the problem definition and introduction of the main focus of this research, this thesis further reports the following:

Chapter 2 reviews existing biometric systems and the human traits that are used, their advantages, limitations and their basic operating principles. It further reviews the challenges associated with the current system which can be potentially solved with template-free systems.

Chapter 3 reports the evaluation of the properties of the human voice that qualifies it as a biometric trait, how the human voice is produced, and the basic operating principles of voice biometric systems, its drawbacks and applications. This chapter also reviews the

existing voice features used for template-based biometrics, an overview of template-free biometric technology based on the human voice and how it proposes to solve problems associated with template-based vulnerabilities, and analyses the suitability of human voice features for employment in template-free biometrics.

Chapter 4 covers an in-depth analysis of the operating principles of template-free biometrics. It reviews the principles behind existing cryptographic systems, introduces the principles of operation of the template-free system based on voice modality and the generation of biometric keys there from. Finally, it introduces a novel key combination method with the overall system yielding feature stability of 65.5%.

Chapter 5 examines existing revocable biometric systems and how it can be integrated with the evolving concept of template-free biometrics. This chapter further discusses how these keys may be revoked as well as an evaluation of the system's performance showing that an attacker will have to carry out up to $8.32e^{+50}$ permutations in order to hack into the system. The concluding part of the work however identified potential challenges to this result and made recommendations for improvement.

Finally, the conclusions from the research were presented while future research directions are given in chapter 6.

1.6 Chapter Summary

This chapter has introduced the subject of the research in template free biometric systems using voice modality. It specifically identified the issues of concern with current biometric systems and how they may be overcome by the technique of template free biometrics. The motivation for using voice modality in this research was also discussed, with the scope ranging from introduction of the subject to the experimental layout to show that voice may potentially form the basis for a practical template-free biometric system. Broadly, this thesis reports the research on the technique that exploits

the possibility of directly encrypting biometric data provided by the individual and therefore eliminates the need for storing templates used for data validation, thus increasing the security as well as users' confidence in the system.

The next chapter broadly reviews extant literature on template-based biometric systems and highlights the economic benefits as well as the drawbacks.

Chapter 2

Overview of current biometric systems

Automatic human identity verification/authentication is becoming very critical due to the advancement in technology like in e-commerce, access control, banking, etc. [10]. The need for automatic recognition has led to the increase in the use of computers to recognize humans from physical and behavioral traits especially since the digital computer evolution of the 1960's [10].

The word 'Biometrics' represent an automated method of recognising humans based on a physiological or behavioural characteristic [10]. Biometrics also has an older meaning/application used in biological studies or biological statistics including forestry. Here it is referred to as the collection, synthesis, analysis and management of quantitative data on biological communities [145] such as forests. However, this research deals with a more recent use of the term which include the study of methods for uniquely recognizing humans based upon one or more intrinsic physiological or behavioural traits. Simply put, a *'biometric trait'* is a physiological or behavioural characteristic of a human being that can distinguish one person from another and that can be used for identification or verification of identity. The broad definition as well as the stages involved in biometrics has been mentioned in the general introduction in chapter 1.

Biometrics deals with measuring an individual's physical features in an authentication inquiry and comparing this data with stored biometric reference data to determine the identity of a specific user. The Authentication process could be either verification or

identification. In the verification mode, the system validates a user's identity by comparing the captured biometric data with the user's own biometric template(s) stored in the system database [18]. Verification systems are used for positive identification and in such a system, an individual who desires to be recognized willingly claims and enrol an identity by choosing to be given a user name, a personal identification number (PIN), or a smart card. The system will usually have several of such user identities stored on it and when a particular user verification is required, the system conducts a one-to-one comparison to determine whether the claim is true or not. In most cases, identity verification is used to prevent multiple people from using the same identity [19]. Examples range from access control into a machine, building like a library or a club, and computer or in international passports.

In the identification mode, the system searches the biometric templates of all the users in the database to determine a match for a particular individual. An example is when the system is used for crime detection and it uses samples lifted from a crime scene to search through a database of known criminals to determine who among the previously enrolled criminals perpetuated the crime. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity [18]. Identification is a critical component in negative recognition applications where the system establishes whether the person is who he or she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities [19]. This is only possible through biometrics, because in traditional passwords or token authentication, a user can have as many identities as possible.

While verification prevents multiple people from using the same identity, identification prevents a single person from using multiple identities. Sometimes, identification may also be used in positive recognition for convenience during which a user is not required to claim an identity. An example is in access to a conference hall or an office building where a user is allowed to enter so long as he or she is enrolled in the database.

As increasing number of biometrics based identification systems are being deployed for many civilian and forensic applications, biometrics and its applications has evoked considerable interest. The current state of affairs is that the technical and technological literature about the overall state-of-the-art in biometrics is dispersed across a wide spectrum of books, journals, and conference proceedings [20]. However, despite decades of research and hundreds of major deployments, the fields of biometrics remains fresh and exciting as new technologies are developed and old technologies are improved and fielded in new applications [10]. Thus, Worldwide over the past few years, there has been a marked increase in both government and private sector interest in large-scale biometric deployments for accelerating human–machine processes, efficiently delivering human services, fighting identity fraud and even combating terrorism[10]. This is because Biometric technologies provides the link between human–machine interface, but like all technologies, by themselves they can provide no value until deployed in a system with support hardware, network connections, computers, policies and procedures, all tuned together to work with people to improve some real business process within a social structure [10]. In order to choose the right human traits and the infrastructure to build an effective biometric security system, it is important to understand the basic requirements of a biometric system as described in the next section.

2.1 Requirements of Biometric Systems

Several human physical or behavioural traits have been used in biometrics. Such physiological or behavioural traits must satisfy the following requirements [13], [18], [20], [21]:

Universality: Every relevant person should have an identifier.

Uniqueness: Each relevant person should have only one identifier, and no two people should have the same identifier. In essence, any two persons should be sufficiently different in terms of the characteristic.

Permanence: The identifier should not change, nor should it be changeable i.e. the

characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.

Indispensability: The identifier should be one or more natural characteristics, which each person has and retains.

Collectability: The characteristic can be measured quantitatively and should be collectible by anyone on any occasion.

Storability: The identifier should be storable in manual and in automated systems.

Exclusivity: No other form of identification should be necessary or used.

Precision: Every identifier should be sufficiently different from every other identifier such that mistakes are unlikely.

Simplicity: Recording and transmission should be easy and not error prone.

Cost: Measuring and storing the identifier should not be unduly costly.

Convenience: Measuring and storing the identifier should not be unduly inconvenient or time-consuming.

Acceptability: Its use should conform to contemporary social standards. This indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives.

Circumvention: This reflects how easily the system can be fooled using fraudulent methods. A good biometric system should have a null or minimal circumvention tendency.

It is therefore important that biometric systems meet all or most of the criteria listed above in order to be considered useful. Since a robust biometric system is a function of the modality used and the infrastructure, we first have to look at the various human traits that are used in biometrics as well as their strengths and weaknesses. A good knowledge of this as well as an understanding of the basic infrastructural requirements will be important for building the right biometric solution for any given scenario. In addition, subsequent sections and chapters will show why voice was chosen as the specific biometric used for this research.

2.2 Human traits used in Biometrics

Some human traits have been identified to meet the criteria listed in section 2.1 above and are therefore employed in biometrics. A practical biometric system should meet the specified recognition accuracy, speed, and resource requirements, be harmless to the users, be accepted by the intended population, and be sufficiently robust to various fraudulent methods and attacks to the system. Based on the preceding requirements, human physiological and behavioural traits commonly used in biometrics include the following:

Physiological traits (these are related to the shape of the body): these include fingerprints (which are the commonest and oldest traits used), face recognition, hand geometry, iris recognition, retina, hand veins, ear canal, facial thermogram, and palm prints [20].

Behavioural traits (the se are related to the behaviour of a person): these include signature, keystroke dynamics, voice, gait (way of walking), odour and scent [20].

Physiological biometrics are based on direct measurements and data derived from measurements of a part of the human body, whereas behavioural biometrics are based on measurements and data derived from human actions, and indirectly measures characteristics of the human body over a period of time. It should be noted that although voice is also a physiological trait which is unique in every human (except a few who cannot speak), the science of voice recognition is mainly based on the study of the way a person speaks, which can be classified as behavioural.

The characteristics of the various traits are described below:

2.2.1 Fingerprints

With the exception of those natural ways that humans recognise each other, fingerprints are about the oldest biometric in use for automatic personal identification and the matching accuracy using fingerprints has been shown to be very high [11]. A fingerprint

is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is determined during the first seven months of foetal development.

According to Jain, et al [20], major representations of the finger are based on the entire image, finger ridges, or salient features derived from the ridges (minutiae). Four basic approaches to identification based on fingerprint are prevalent: (i) the invariant properties of the gray scale profiles of the fingerprint image or a part thereof; (ii) global ridge patterns, also known as fingerprint classes; (iii) the ridge patterns of the fingerprints; (iv) fingerprint minutiae - the features resulting mainly from ridge endings and bifurcations. It is believed that no two persons (including identical twins) share the same fingerprints because the fingerprint patterns are part of a person's phenotype and do not apparently depend on genetics [21], [22]. Fingerprints have been used to identify humans for a long time—there is some evidence that thousands of years ago ancient Chinese were aware of the uniqueness of fingerprints [21] and have used it to distinguish between people. Despite other evidences of pre-historic use of fingerprint technology for human recognition [10], modern application of fingerprint based biometrics gained prominence since the evolution of digital computer and has continued to remain popular in applications like forensics, genetics, Government, civil and commercial. It is perhaps the most widely used biometric trait and there are several write-ups on fingerprint technology available in literature. Recognition performance of fingerprint systems are also very high: 90% [150]; 81.9% [151]; 87.6% [152].

2.2.2 Face Recognition

Like Voice, humans do a lot of face recognition on a daily basis. It seems to be one of the most acceptable biometrics we have (unlike, for example, fingerprints, which are often associated with criminal prosecution). In automatic biometric systems, face recognition refers to an automated or semi-automated process of matching facial images. The image of the face is captured using a scanner and then analysed in order to obtain a biometric "signature" [25]. It is considered as a passive biometric because it does not necessarily require the cooperation of the individual to achieve recognition and the unobtrusive nature of its technology makes it an attractive choice for wide range

surveillance and security applications. For example, an automated face recognition system can use a video camera to capture face images from a distance and detect, track and finally recognize people such as terrorists or drug traffickers. According to Maltoni et al [10], an automated face recognition system includes several related face processing tasks, such as detection of a pattern as a face, face tracking in a video sequence, face verification, and face recognition. Face recognition performance reported in literature include: FFR and FAR of 0% [8]; and EER of 2.5% [42].

The application of facial recognition ranges from a static, controlled "mug-shot" verification to a dynamic, uncontrolled face identification in a cluttered background (e.g., airport) [18]. The most popular approaches to face recognition are based on either: (1) the location and shape of facial attributes such as the eyes, eyebrows, nose, lips and chin, and their spatial relationships, or (2) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces.

2.2.3 Hand Geometry

The physical dimensions of a human hand contain information that is capable of authenticating the identity of an individual [1]. This information has been popularly known as hand or palm geometry. Biometric authentication based on hand geometry is extremely user-friendly. Features measured and used by hand geometry biometrics typically include length and width of fingers, different aspect ratios of palm and fingers, thickness and width of the palm, and so on [21]. These features are extracted from images of a hand and used in the representation.

Jain et al [72] proposed a hand geometry based system with performance of FRR of 15% and FAR of 2% in one scenario and FRR of 4% and FAR of 0% in a second scenario. A summary of another typical performance based on hand geometry is identified in table 2.1 below [152]

Table 2.1 Typical performance of hand geometry based system

	150 dpi	400 dpi	600 dpi	150 - 600dpi
VP (Verification performance)	99.42	99.12	98.09	98.83
IP (Identification performance)	99.42	98.83	89.18	98.25

Table 2.2 is another performance based on hand geometry, showing average identification rate obtained with four methods [153]

Table 2.2: Average identification rate obtained with four methods

Recognition method	Average identification Rate
Minimum Euclidean distance classifier	97.2 %
k-nearest neighbor (k=3)	98.0 %
Neural network	Training: 100 % Generalization: 98.5 %
Support vector machine	99.0 %

Hand geometry based identity verification systems are being widely used in a number of access control, time and attendance, and point-of-sale applications.

2.2.4 Iris Recognition

The iris is the externally-visible, coloured ring around the pupil. Although it is externally visible, it is an internal part of the eye and like fingerprints, the iris image is a part of human phenotype and is believed to be unique in every individual [21]. An iris 'scan' is a high-quality photograph of the iris taken under near-infrared (near-IR) illumination [25]. Iris recognition-based biometric systems are believed to be very reliable and accurate [21]. The accuracy and speed of currently deployed iris-based recognition systems is promising and point to the feasibility of large-scale identification systems based on iris information [25]. Daugman [154] shows a typical recognition performance based on iris in the form of error probabilities for several decision criteria as shown in table 2.3 below:

Table 2.3 Recognition performance based on Iris

	Performance	
HD Criterion	Odds of False Accept	Odds of False Reject
0.25	1 in 13.5 billion	1 in 1490
0.26	1 in 2.04 billion	1 in 2660
0.27	1 in 339 Million	1 in 4850
0.28	1 in 60 Million	1 in 9000
0.29	1 in 12 Million	1 in 17100
0.30	1 in 2.4 Million	1 in 32800
0.31	1 in 603000	1 in 64200
0.32	1 in 151000	1 in 128000
0.33	1 in 39800	1 in 260000
0.34	1 in 11500	1 in 536000
0.35	1 in 3630	1 in 1.12 Million

Daugman [155] also showed an improved recognition result as indicated in table 2.4 below:

Table 2.4: Iris recognition performance

HD Criterion	Observed False Match Rate
0.220	0 (theor: 1 in 5×10^{15})
0.225	0 (theor: 1 in 1×10^{15})
0.230	0 (theor: 1 in 3×10^{14})
0.235	0 (theor: 1 in 9×10^{13})
0.240	0 (theor: 1 in 3×10^{13})
0.245	0 (theor: 1 in 8×10^{12})
0.250	0 (theor: 1 in 2×10^{12})
0.255	0 (theor: 1 in 7×10^{11})
0.262	1 in 200 billion
0.267	1 in 50 billion
0.272	1 in 13 billion
0.277	1 in 2.7 billion
0.282	1 in 284 million
0.287	1 in 96 million
0.292	1 in 40 million
0.297	1 in 18 million
0.302	1 in 8 million
0.307	1 in 4 million
0.312	1 in 2 million
0.317	1 in 1 million

2.2.5 Signature

Signature, which is the way a person signs his or her name, is a characteristic unique to an individual and it enjoys a high degree of acceptance, largely because of their everyday use and familiarity [18]. Although signatures require contact with the writing instrument and an effort on the part of the user, they have been accepted in government, legal, and commercial transactions as a method of verification. Signature is a behavioural biometric, which lack permanence: they may change at the will of a person, or under influence from such factors as illness, mental state, medicines, emotions, or age. Signatures of some people vary substantially: even successive impressions of their signature are significantly different. In addition, professional forgers may be able to reproduce signatures that fool the system. Two subtypes of signature verification systems exist: static signature verification systems, where only the graphical representation (image) of the signature is used, and dynamic signatures, where the

dynamics, pressure, and speed of the movement of a special pen are used for verification [18].

A typical signature verification results from the work of Azlinah Mohamed et al [156] is tabulated in table 2.5 below:

Table 2.5: Typical signature verification performance

Data	Syste m	Questionnaire Result			System Vs Questionnaire
		Ascnd	Strgh	Dscnd	
1	S	8.3%	75%	16.7%	Identical
2	A	87.5%	8.3%	4.2%	Identical
3	S	41.7%	45.8%	12.5%	Identical
4	S	12.5%	70.8%	16.7%	Identical
5	A	79.2%	4.2%	16.7%	Identical
6	S	0 %	100%	0%	Identical
7	S	4.2%	87.5%	8.3%	Identical
8	A	70.8%	0%	29.1%	Identical
9	A	58.3%	41.7%	0 %	Identical
10	S	25.0%	66.7%	8.3%	Identical
11	S	75.0%	12.5%	12.5%	Non Identical
12	S	37.5%	54.2%	8.3%	Identical
13	D	70.8%	12.5%	16.7%	Non identical
14	A	79.2%	8.%	12.5%	Identical
15	A	75%	10%	15%	Identical
16	A	70.8%	25%	4.2%	Identical
17	S	8.3%	87.5%	4.2%	Identical
18	A	70.8%	12.5%	16.7%	Identical
19	A	79.2%	12.5%	8.3%	Identical
20	A	79.2%	4.2%	16.7%	Identical

S – Normally Straight; A – Ascending; D - Descending

In addition, Soedjianto et al [157] reported an average result of signature recognition of 96 % for 20 people and everyone tries the software for 20 times. Another recognition performance [158] is tabulated below:

Table 2.6: Another signature recognition result

Person's name	Accuracy
Mr. X	99%
Mr. Y	72%
Mr. Z	60%
Mr. U	9%
Mr. V	12%
Mr. W	27%

Other recognition performance results include: up to 97.60% in [159], and 78.92% [160].

2.2.6 DNA

Deoxyribonucleic acid (DNA) is currently used in forensic applications for person recognition. Although the DNA patterns of identical twins are similar, it is the one-dimensional (1–D) ultimate unique code for one's individuality [18]. It is associated with three major issues of concern which limits its use in biometric applications. These are:

i) Abuse: it is easy to steal a piece of DNA from an unsuspecting subject that can be subsequently abused for an ulterior purpose;

ii) Automatic real-time recognition issues: the present technology for DNA matching requires cumbersome chemical methods (wet processes) involving an expert's skills and is not geared for on-line non-invasive recognition;

iii) Privacy issues: information about susceptibilities of a person to certain diseases could be gained from the DNA pattern and there is a concern that the unintended abuse of genetic code information may result in discrimination, e.g., in hiring practices [18], [20].

Despite these concerns, DNA is still considered as a biometric modality inasmuch as it involves the use of physiological characteristic for human identification. However, reference to it as a biometric sometimes contested because DNA differs from standard biometrics in several ways:

- In standard biometrics, image impressions (like fingerprint, palm, iris, etc) or pre-recordings (e.g. voice) can be used while DNA requires a tangible physical sample of the individual.

- Most biometric operates in real-time mode, with all stages being automated as against DNA, in which matching is not done in real-time, and currently not all stages of comparison are automated.

- Matching of DNA does not employ templates or use of extracted features. Rather, in DNA, actual samples are compared.

2.2.7 Ear

Ear Biometrics measures the shape of the ear and the structure of the cartilaginous tissue of the pinna [18]. The ear recognition approaches are based on matching the distance of salient points on the pinna from a landmark location on the ear. Biometrics based upon the ear is viable because the ear anatomy is unique to each individual and features based upon measurements of that anatomy are comparable over time. Like face, ear biometrics is passive in nature because it can be captured at a distance and sometimes does not require the active participation of the subject. However, it has more advantage over face because unlike the difficulty with face biometrics like hair growth, cosmetics, ageing, etc, the ear biometrics is robust and simple to extract [20].

Recognition performances in ear based biometrics are high: 98.7% [163]; 89% [164]; and ear recognition performance according to [162] is indicated in table 2.7 below.

Table 2.7: Ear recognition performance

Approach	Ear Image	Ear Database	Recognition Rate
LABSSFEM	2D	77 (training), 77 (test), USTB ear database	85%
Neural Networks	2D	84(training), 28 (validation), 56 (test)	93%
Force Field Transformation	2D	252 (test) XM2VTS face database	99.2%
PCA	2D	197 (training), 88 (registrant) ND Human ID database	71.6%
Moment Invariants	2D	120 (training), 60 (test) USTB ear database	96%
Local Surface Patch	3D	10 (training), 10 (test)	100%
Two-step ICP	3D	30 (training), 30 (test)	93.3%
Improved ICP	3D	302 (training), 302 (test) ND Human ID database	98.8%

2.2.8 Palm Print

Palm print recognition is similar to fingerprint recognition since both are represented by the information presented in a friction ridge impression. This information combines ridge flow, ridge characteristics, and ridge structure of the raised portion of the epidermis. The data represented by these friction ridge impressions allows a determination that corresponding areas of friction ridge impressions either originated from the same source or could not have been made by the same source [18].

Palm print images are easy to capture as they can be acquired by a variety of sensor types (capacitive, optical, ultrasound, and thermal). Like fingerprints, the three main categories of palm matching techniques are minutiae-based matching, correlation-based matching, and ridge-based matching [27]. Minutiae-based matching, the most widely used technique, relies on the minutiae points described above, specifically the location, direction, and orientation of each point. Correlation-based matching involves simply lining up the palm images and subtracting them to determine if the ridges in the two palm images correspond. Ridge-based matching uses ridge pattern landmark features

such as sweat pores, spatial attributes, and geometric characteristics of the ridges, and/or local texture analysis, all of which are alternates to minutiae characteristic extraction. This method is a faster method of matching and overcomes some of the difficulties associated with extracting minutiae from poor quality images.

There are several palm pint recognition systems available in literature and typical performance include: [165] where the overall accuracy of the system is more than 97%, FAR & FRR of 2.4% & 0.8% respectively; and EER (%) of 0.74 [165].

2.2.9 Thermal Sensing

Thermal Sensing investigates the pattern of heat radiated by human body, especially from the facial, hand, and hand vein infrared tissues, and this can be captured by an infrared camera without an active participation of the subject [20]. Therefore, it has the advantage of covert recognition. However, it becomes difficult in some environment where artificial heating is present like room heaters.

2.2.10 Gait

Gait refers to the way of walking of humans, and like face and voice, has been used regularly and naturally by humans to recognise each other. It is one of those biometric traits that can be used to recognize people at a distance [18]. Gait is a behavioural biometric and may change over a long period of time, possibly due to changes in body weight, major injuries involving joints or brain, pain in the leg, the choice of footwear, nature of clothing, walking surface, etc [18]. Most gait recognition algorithms attempt to extract the human silhouette in order to derive the spatio-temporal attributes of a moving individual [22]. Acquisition of gait is similar to acquiring a facial picture and, hence, may be an acceptable biometric. It uses the video-sequence footage of a walking person to measure several different movements of each articulate joint, making it input intensive and computationally expensive. However, it has an advantage in surveillance

scenarios where the identity of an individual can be surreptitiously established. It also offers the possibility of tracking an individual over an extended period of time.

Gait biometrics is an evolving research and several publications are available in literature [29] – [39].

Recognition performance of gait systems published include: EER of 16% [167]. In addition, [168] reported that performance based on shoe type (A vs. B), view (right camera vs. left camera), briefcase (carrying vs. not carrying) and surface (grass vs. concrete), the recognition rates were 78%, 73%, 61% and 32%, respectively.

2.2.11 Keystroke

Keystroke is a behavioural biometric which offers sufficient discriminatory information to permit identity verification [40]. Keystroke dynamics is susceptible to large intra-class variations in a person's typing patterns due to changes in emotional state, position of the user with respect to the keyboard, type of keyboard used, etc [22]. It can be monitored unobtrusively as that person is keying in information and continuously over a session after the person logs in using a stronger biometric such as fingerprint or iris.

Some performances reported on keystrokes include:
[169] reported results for laptop keyboards (99.5% accuracy on 36 users, which decreased to 97.9% on a larger population of 47 users); for desktop keyboards (98.3% accuracy on 36 users, which decreased to 93.3% on a larger population of 93 users)

The overall performance achieved by [170] includes a false acceptance rate (FAR) of 0.0152% and a false rejection rate (FRR) of 4.82%.

2.2.12 Retina Scan

Retina scan technology is claimed to be the most secure biometric measure, as it is almost impossible to change or replicate the blood vessel structure of the eye. It measures the retinal vasculature which is a characteristic of each individual and each eye [18]. The user is required to stand close to the sensor which comprises of a bright light source. However, its acceptability is low because it involves users' full cooperation and participation, entails contact with the eyepiece, requires a conscious effort on the part of the user, and the fear that it might reveal other disease conditions.

Retinal recognition performance was given as 85% by Ravi Das [171]. Farzin etal [172] also had an average result of 99%. Identification result for [173] is also indicated in table 2.8 below:

Table 2.8: Retina recognition performance

No. of training samples	Identification rate
1	86.18%
2	92.63%
3	95.68%
4	97.59%
5	99.09%

The overall advantages and limitations of biometric systems are subsequently enumerated.

2.3 Advantages of Biometric Systems

The use of biometrics in personal authentication has several advantages over other forms of security like password or token based systems. These advantages have made their use popular in several applications as described earlier. A number of these advantages available in literature [10], [18], [19], [20] are described below:

- In Commercial applications, the traditional technologies available to achieve a positive recognition include knowledge-based methods (e.g., PINs and passwords) and token-based methods (e.g., keys and cards). However, these can be easily lost, stolen or forgotten. Biometrics cannot be lost, 'stolen' (in the physical sense of it) or forgotten.

- Biometrics are more secure than passwords which are easy to crack by guessing or by a simple brute force dictionary attack.

- In some applications that require user authentication e.g. a subscription to a Virtual Library or an Internet Service Provider, passwords can be shared among users thereby denying the provider revenue. However, if biometric authentication is required, it is not possible for multiple users to share the same login information.

- Keys and tokens can be shared, duplicated, lost or stolen and an attacker may make a "master" key that may open many locks. It is significantly more difficult to copy, share, and distribute biometrics with as much ease as passwords and tokens.

- It is difficult to forge biometrics and extremely unlikely for a user to disclaim, for example, having accessed a building or a computer network.

- All the users of the system have relatively equal security level and one account is no easier to break than any other (e.g., through social engineering methods).

- Biometrics is more convenient for users because users are no longer required to remember multiple, long and complex frequently changing passwords while maintaining a sufficiently high degree of security. They are also not expected to worry about carrying tokens or keys as they naturally carry around their biometrics.

- Multimodal biometrics allows the use of several combination of biometric modality and makes the system more secure.

- Negative recognition applications are in cases such as employee background checking and preventing terrorists from boarding airplanes.

- In most negative recognition system, personal recognition is required to be performed in the identification mode and the accuracy of identification is less compared to verification due to the large number of comparisons that are required to be performed [18]. Traditional personal recognition tools such as passwords and PINs cannot be applied for negative recognition applications. Background checks and forensic criminal identification are also negative recognition systems.

It is these advantages that have made the use of biometric as a means of identification very popular worldwide. However, despite these advantages and the numerous applications, biometrics does have lots of limitations that are subject of several research. A few of these limitations are described in section 2.4.

2.4 Limitations of biometric systems

There are several limitations associated with biometrics, which have not allowed their use to be completely acceptable worldwide. Overcoming these limitations are still the subject of continuing research, aiming at improving on currently available technologies. Some of these limitations are described below.

- **Noise in sensed data:** Noisy data can result in error in biometrics. Noisy data may include a fingerprint image with a scar or a voice sample altered by cold. Defective or improperly maintained sensors can also result in noisy data. Such defects may include accumulation of dirt on a fingerprint sensor or unfavourable ambient conditions like poor illumination in a face recognition system. When noise is introduced into biometric systems, recognition error may result as the data may not be successfully matched with corresponding templates in the database, resulting in a genuine user being incorrectly rejected [18].

- **Variations in user characteristics:** this refers to changes in an individual's characteristics over a period of time. Also known as Intra-class variations, its examples include the change in the human voice due to stress, ageing, etc or change in hand geometry over time or way of walking due to injury, change of signature over a period of time, and so on. Intra-class variations are more prominent in behavioural traits [18].

- **Similarities in multiple users:** This is also referred to as Inter-class similarity and it refers to the overlap of feature spaces corresponding to multiple individuals. This can lead to false match in a multi user identification system comprising of a large number of enrolled individuals [18].

- **Non-universality:** The biometric system may not be able to acquire meaningful biometric data from a subset of users. A fingerprint biometric system, for example, may extract incorrect minutiae features from the fingerprints of certain individuals, due to the poor quality of the ridges [18].

- **Interoperability issues:** When biometric data obtained from different sensors are used for matching, there may be errors introduced due to the operating characteristics of the capture device. An example is in the voice signals captured by two different handset technologies or face images captured by different camera types.

- **Design flaws in biometric systems**, both in terms of False Reject Rate (FRR) and False Accept Rate (FAR). High FRR causes inconvenience for legitimate users and prompts the system administrator to lower a verification threshold. This inevitably can give rise to FAR, which, in turn, lowers the security level of the system.

Although these limitations exist, biometrics has continued to gain prominence and is currently used in several applications as seen in the last section. These limitations notwithstanding, there are other forms of vulnerabilities associated with biometrics requiring further research to address.

2.5 Security Vulnerabilities of a Biometric System

Despite the numerous advantages of biometrics over knowledge and token based authentication methods, there are some security vulnerabilities associated with biometrics, a few of which are mentioned below. These are mostly in the form of attacks or compromises that are deliberately carried out on the system, in order to undermine it as well as loss of privacy and flaws in the system. Some of them are described below:

Substitution attack: In current biometric systems, the biometric template must be stored as reference for user verification. If an attacker gains access to the stored template, he can overwrite the legitimate user's template with his/her own. Stealing of template records compromises the users for life as they cannot ever change their biometrics [3].

Tampering: In a number of cases, feature sets on verification or in the templates can be modified in order to obtain a high verification score, no matter which image is presented to the system [3], [48], [53].

Spoofing: This refers to the ability to fool a biometric system by applying fake fingerprints, face or iris image. It involves the deliberate manipulation of one's biometric traits in order to avoid recognition or the creation of physical biometric artefacts in order to take on the identity of another person [22], [48], [54].

Replay attacks: This can happen in voice based systems where an attacker can replay a pre-recorded voice print. Also, an attacker can circumvent the biometric sensor by injecting a recorded image in the system input [3], [9], [13], [23], [48], [53].

Masquerade attack- also known as a "spoofing" attack. The most usual masquerade attacks happen when one computer pretends to be another computer in order to gain access to restricted resources or otherwise infiltrate another computer [48].

Trojan horse attacks: This is an attack on the feature extractor module. In this attack, the attacker can replace the feature extractor module with a Trojan horse. A Trojan horse program refers to an executable code that is not a translation of the original program but was added later, usually maliciously, and comes into the system disguised as the original program [11]. Trojan horses in general can be controlled remotely. Therefore, the attacker can simply send commands to the Trojan horse to send to the matcher module feature values selected by him [48].

Overriding the match result: The output of the system is always a binary Yes/No (match/no match) response. If an attacker were able to interject a false Yes response at a proper point of the communication between the biometrics and the application, he could pose as a legitimate user to any of the applications, thus bypassing the biometric part [3], [48].

System and Design Issues: A number of factors need to be considered when designing a biometric system. Some of the most important biometric system design and implementation considerations include security, accuracy, privacy, cost, speed etc [21].

Security: Although biometrics are most times used for security purposes, biometrics itself needs to be secured because it is susceptible to theft, compromise, etc. and a loss of confidence in it will invariable mean a loss of confidence in the system that is being protected with the biometrics. Some of these vulnerabilities have been discussed earlier [21].

Accuracy: Every biometric system is expected to have a high degree of accuracy otherwise the real essence of using it will be lost. The system should correctly tell people apart with minimal False Accept and False Reject Rates [21].

Speed: In some cases, speed is a relative term, it becomes obvious that higher speeds are required when a particular system begins to cause some inconvenience. Therefore, if a biometric system is in an access control, airports or border crossing points where a

large number of people needs to be reliably and quickly identified and authenticated, then speed becomes a major factor of consideration [21].

Exceptions: In many everyday life situations, provision needs be made for exceptions. Therefore, a biometric system should be able to handle exceptions like a person without the required biometric (e.g. someone without fingers or someone who cannot speak) or a person whose biometric may not be usable for some reason. These are a few cases that requires that the system be switched to manual mode to enable such exceptions be handled. However, these will lead to tradeoffs with problems associated with manual processes like speed, accuracy, sincerity etc. [21], [55]. Although this is a major area of research, it is outside the scope of this research.

Cost: Although biometrics introduces several advantages in security system, its use is in mostly commercial, government, and social environment and it needs not be too expensive compared to the system that it is to protect [3], [21].

Privacy: Several factors affects users' confidence in a system but privacy appears to be among the first issue of concern to many people when using biometrics [3], [21].

2.6 Overview of Voice Biometric Systems

Voice can be classified as a combination of physiological and behavioural biometrics. All humans, except a few, can speak and each one's voice is unique. The features of an individual's voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in the synthesis of the sound. These are the physiological part of voice characteristics which are permanent for an individual. The behavioural part of a person's voice changes over time due to age, medical conditions (e.g. cold), and emotional state [18]. Voice recognition systems depend on numerous characteristics of a human voice to identify the speaker. Just like face recognition, humans do voice recognition on a daily basis e.g. recognising the voice of a loved one (or an enemy) on a telephone. Voice recognition holds much potential because it is acceptable and it does not require expensive input devices, unlike some other

biometrics. It is ideal for many practical and widespread telephony applications, and in theory voice recognition systems may even function in the background without forcing the users to go through a separate identification and verification process, saving us from another password to remember.

Voice recognition could be text dependent or text independent. A text-dependent voice recognition system is based on the utterance of a fixed predetermined phrase. A text-independent voice recognition system recognizes the speaker independent of what is voiced out [56].

2.6.1 Basic operating principles of voice biometrics

Voice Biometrics is basically the unique representation of the characteristics that make up an individual's voice. The differing physical components of a human throat and mouth produce a unique sound which can be analysed, measured and stored. This is known as a voice print. In the current methods of voice biometrics, a sample of speech is recorded and analysed as part of an enrolment process [56], [57]. The characteristics extracted from this sample are fed into a complex algorithm which produces information that is encrypted and securely stored on a template. At the verification stage, a new sample of the same individual's voice is recorded and analysed in the same way described above. If the result of the calculation based on the characteristics in the verification sample matches the result obtained during the enrolment then the identity can be verified. To overcome security challenges like ensuring that pre-recorded samples of an individual is not replayed to achieve verification, a process called liveliness detection [11], [179], [180], [181] where the caller is asked to repeat a random phrase or sequence of numbers can be added to the verification process.

Speaker recognition encompasses verification and identification i.e. to identify a particular person or to verify a person's claimed identity. While **Speaker identification** is defined as deciding if a speaker is a specific person or is among a group of persons, **Speaker verification** is defined as deciding if a speaker is who he claims to be [56]. It has been a subject of research since 1974 when Atal [57] reported the use of pattern

matching method to process cepstrum as inputs to do text dependent speaker recognition. Speaker recognition could be text-dependent or text-independent. Text-dependent recognition involves selection and enrolment of one or more voice pass-phrases. In this case the system knows what will be spoken and can perform a pattern match, but does not necessarily have explicit (phonetic) knowledge about the pass-phrases. Text-independent mode would allow free speech for verification where the variability of words and the natural personal variability have to be compensated. In this mode, the verification is performed independently of what is spoken. Explicit knowledge could only be gained after successful speech recognition and possibly language identification [58]. Markel and Davis [59] pioneered text independent speaker recognition in 1979 by using a method that extracts the linear predictive coding (LPC) coefficients from the speech input.

Speaker recognition possesses several advantages over other methods of biometric recognition. These advantages include the following:

- *It delivers remote authentication capabilities* [49], [56]: It is one of the few (in addition to gait and face) biometric that does not require the individual's physical presence during the enrolment or verification process. This makes it ideally suited in the context of communication applications and has the ability to leverage existing telephony infrastructure, standard microphones, as well as web-based applications where remote authentication is required. This makes it possible to support broad-based deployments of voice biometric applications in a variety of settings unlike most other biometrics that requires proprietary hardware such as the vendor's fingerprint sensor or iris-scanning equipment.

- *Its initial investment expense is low:* it represents a low cost authentication solution as no additional end user hardware is required. Following from above, the caller will typically use a standard telephone or a microphone, although sometimes, there are challenges with variable and inferior microphones and telephones which give rise to extreme hoarseness [49], [128].

- It l*everages existing infrastructure:* It complements both automated phone based services and call centre operative-based operations [49], [128].

- *Voice Biometrics facilitates strong two-factor authentication:* Two-factor authentication combines both biometrics and knowledge-based information to deliver remote identity verification. Voice biometrics combines 'something you are' (your voice) with 'something you know' (a pass phrase or shared secret) to deliver a strong two-factor authentication. This provides significantly higher levels of security than a single factor 'PIN' or knowledge based authentication process [49], [128].

- *It is perceived as a non-intrusive technology.* This means that it is an *Intuitive and natural technology since it* uses only spoken words. This is unlike systems that rely on scanners or similar devices. In addition, it requires no end-user training as it is such a natural process. Therefore, it is widely accepted by end users [49], [128].

- It allows for synergy effects in combination with other processes such as speech recognition [49], [128].

- Perhaps, the most significant difference between voice biometrics and other biometrics is that voice biometrics is the only commercial biometrics that process acoustic information. Most other biometrics are image-based [49], [128].

- *Cost reductions in the commercial sector:* Implementation of a voice verification system can reduce administrative and operational costs associated with handling lost/forgotten passwords or PINs [49], [128].

- Digital signature: Voice verification systems can also be used to digitally sign phone or web based transactions [49], [128].

- *Multi- Channelling:* Voice verification can be used seamlessly across multiple direct channels including the Internet. For example, a financial institution that implements voice verification in its call centre could use the same voiceprints to authenticate customers accessing its online services [46], [49], [128].

These advantages have made voice a very important biometric trait that is widely used. In some cases, it is the only biometric that can be applied, especially in remote authentication, telephone based recognition system, and in two-factor authentication. However, despite these advantages, voice biometrics is faced with a number of challenges which are worth mentioning.

2.6.2 Drawbacks of voice based biometric system

Voice based biometrics are vulnerable to some conditions like:

- Background and channel noise: Noise within the environment or noise within the transmission channel can affect the accuracy of voice based biometric systems. In some cases, e.g. in a bus station, stadium, or other noisy environments, it may be impossible to use the voice authentication device [182].

- Variable and inferior microphones and telephones; and extreme hoarseness: these are errors generated by inferior or damaged signal capture device like microphone or telephone. In addition, a biometric system calibrated with a particular type of microphone or telephone may not authenticate well with a different brand whose specifications are significantly different as well as the difference on the networks that they operate. An example is in a situation where a user enrols with a home telephone and tries to authenticate with a mobile telephone [182].

- Fatigue or vocal stress: these factors can affect the signals produced by the individual and may introduce intra class variations in the voice prints [182].

- A few cannot speak: the universality factor may be affected in situations where the dumb or people with other forms of voice disorders or inability to speak are unable to use the system.

- Variation across ageing: voice is one of those human features that changes as an individual ages. It will therefore be difficult to authenticate enrolments made at a younger age.

- Illness (e.g. cold) can affect the signals transmitted to the authentication device and therefore affects its accuracy.

- High false non-matching rates: FNMR is the ratio between numbers truly matching samples, which are not matched by the system and total numbers of tests [18].

- Replay of pre-recorded voice sample or mimicry by humans and tape recorders. In addition, Impostors or Hackers might attempt to play back a pre-recorded voice sample from an authorized user in order to gain access to a voice based biometric protected system. It has been suggested to use challenge response system to thwart this sort of attack [60]. The Challenge response system enables the system to prompt the user to repeat a random set of words or phrases in a specified order before verifying that the voice sample matches, and that the sample contains the requested words and phrases in the correct order.

- The fact that it is still an evolving biometric also makes it less attractive in commercial applications [18].

- Another disadvantage is that it cannot be used in security surveillance applications except in text independent scenario which is more difficult to implement [18].

Despite these disadvantages mentioned above, voice biometrics has continued to be a popular choice in commercial and security applications as enumerated in the next section.

2.6.3 Applications of voice biometrics

Voice biometric systems have found use in several telephony-based applications. Many institutions like Government, healthcare, call centres, banking, e- commerce, etc uses voice authentication systems. A catalogue of some typical current applications is detailed below:

Use of Voice Biometrics in Smart Card Applications

Blythe [177] presented a typical case of the use of voice biometrics in smart card applications. Smart card solutions have been severally used with the sole objective of tightening security for physical and/or logical access to company buildings and resources.

Voice Biometrics for Information Assurance Applications

According to Kang and Lee [61], the United States Government has established an organization within the Department of Defense (DOD) to develop and promulgate biometrics technologies to achieve security in information, information systems, weapons, and facilities. This organization has been tasked to study voice biometrics for applications in which other biometrics techniques are difficult to apply.

Forensic Applications

Fingerprints have previously been used in forensics but voice based systems are increasingly becoming popular because of the increasing number of remote criminal activities. For example, telephone based criminal activities related to drug trafficking, terrorism, kidnapping, and advance fee fraud can only be combated by voice based systems.

Other uses include Forensic evidence in the court of law, Telephone and Internet Banking applications, and Password Reset services.

2.7 Overview of biometric key generation

Cryptographic systems generally uses encryption keys (basically bit strings long enough to be difficult to crack, usually 128 bit or more) which could be symmetric, public, or private. These are in form of long random key that is difficult for a person to remember and it is usually generated, after several steps, from a password or a PIN that can be memorized [48].

The use of password or PIN introduces challenges as the password can be guessed, lost, hacked, or stolen by an attacker. On the other hand, biometrics uses unique characteristics that are fairly permanent and more secure from theft, guessing, etc., and which do not place additional challenge (on the user) of having to memorise information. Therefore, biometrics can be used for password management [48]. Biometric Encryption uses a process that securely binds a PIN or a cryptographic key to a biometric such that neither the key nor the biometric can be retrieved from the stored template. This key is created at the point of enrolment and it is re-created only if the correct live biometric sample is presented on verification.

Research in the generation of encryption keys from biometrics has been ongoing for a while and there are currently a number of publications. Within the context of this research, it is important to review extant literature on biometric based encryption key generation.

In [134], Hoque et al considered the fact that live biometric samples can reliably verify not only user identity but also their physical presence at a remote station. They therefore investigated whether the present two-tier approach can be merged into a one-step process in such a way that encryption key(s) are extracted directly from the biometric samples. Their method is a modification of the Vector Quantisation approach in which the codebook is replaced by a series of partitions induced in the feature subspaces, each created by a subset of feature dimensions and the partitions define a number of cells in these subspaces. Each cell is tagged with a key component (usually its identity). When a live sample is available, it is checked against these partitions to ascertain its

membership of a cell. Each feature subspace (denoted by its own set of partitions) is treated independently and contributes its share of the encryption key. As there are many subspaces, by concatenating these key segments a complete key can be obtained. In this proposition, users do not need to declare individual identities to have access to a secured file. The capability to provide a biometric sample that can decipher the file is an acceptable proof of identity. On the other hand, the partitions are created based on feature-point distribution in the subspace (rather than user identities). Therefore, multiple users may share the same cell space, and their biometrics will lead to the same encryption key. Such unintended impersonation, where an individual tries to access a document secured by his cellmate, is found to be very unlikely.

Lalithamani and Soman [135] proposed an effective scheme for generating irrevocable cryptographic key from cancelable fingerprint templates. Initially the minutiae points are extracted from the fingerprints. Afterwards, cancelable templates are generated and irrevocable keys are extracted from the cancelable templates. As the cryptographic key is generated in an irreversible manner, obtaining cancelable fingerprint templates and original fingerprints from the generated key is impossible.

Chen and Chandran [136] introduced a new method which uses an entropy based feature extraction process coupled with Reed-Solomon error correcting codes that can generate deterministic bit-sequences from the output of an iterative one-way transform. The technique is evaluated using 3D face data and is shown to reliably produce keys of suitable length for 128-bit.

Zheng et al [137] proposed a lattice mapping based fuzzy commitment method for cryptographic key generation from biometric data. The proposed method not only outputs high entropy keys, but also conceals the original biometric data such that it is impossible to recover the biometric data even when the stored information in the system is open to an attacker.

Perhaps, one of the most referenced works in the use of voice data for key generation is that of Monrose et al [138], which proposed a technique to reliably generate a

cryptographic key from a user's voice while speaking a password. The key resists cryptanalysis even against an attacker who captures all system information related to generating or verifying the cryptographic key. In this method, Monrose et al proposes the use of entropy from how a user speaks a password.

Kuan et al [139] also proposed a method of extracting cryptographic key from dynamic handwritten signatures that does not require storage of the biometric template or any statistical information that could be used to reconstruct the biometric data. Also, the keys produced are not permanently linked to the biometric hence, allowing them to be replaced in the event of key compromise. This is achieved by incorporating randomness which provides high-entropy to the naturally low-entropy biometric key using iterative inner-product method.

In [140], Dodis et al proposed an efficient secure technique for (1) turning biometric information into keys usable for any cryptographic application, and (2) reliably and securely authenticating biometric data. The paper proposed two primitives: a fuzzy extractor extracts nearly uniform randomness from its biometric input; the extraction is error-tolerant in the sense that the uniform randomness will be the same even if the input changes, as long as it remains reasonably close to the original. Thus, the randomness can be used as a key in any cryptographic application.

In [40], Monrose et al also used user's typing patterns (e.g. durations of keystrokes, and latencies between keystrokes) in combination with the user's password to generate a hardened password that is convincingly more secure than conventional passwords against both online and offline attacks.

Also, in Monrose et al [143], a scheme that repeat-ably generates cryptographic keys from spoken user input was proposed. In this scheme, a device generate a key (e.g., for encrypting files) upon its user speaking a chosen password (or passphrase) to it. An attacker who captures the device and extracts all information it contains, however, will be unable to determine this key.

Uludag et al [141] proposed various methods that monolithically bind a cryptographic key with the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication.

Lívia et al [142] also developed a scheme that uses a static typing biometrics in user authentication. The inputs are the key down and up times and the key ASCII codes captured while the user is typing a string. Four features (key code, two keystroke latencies and key duration) were analyzed, and, seven experiments were performed combining these features. The results of the experiments were evaluated involving three types of user: the legitimate, the impostor and the observer impostor users. The best results were achieved utilizing all features, obtaining a false rejection rate (FRR) of 1.45% and a false acceptance rate (FAR) of 1.89%.

In [144], Costanzo used feature and parametric aggregation for Biometric cryptographic Key generation. The proposed approach uses a method referred to as Biometric Aggregation in which the encryption process begins with the acquisition of the required biometric samples. Features and parameters are extracted from these samples and used to derive a biometric key that can be used to encrypt a plaintext message and its header information. The decryption process starts with the acquisition of additional biometric samples from which the same features and parameters are extracted and used to produce a "noisy" key as done in the encryption process. Next, a small set of permutations of the "noisy" key are computed. These keys are used to decrypt the header information and determine the validity of the key. If the header is determined to be valid, then the rest of the message is decrypted. The proposed approach eliminates the need for biometric matching algorithms, reduces the cost associated with lost keys, and addresses non-repudiation issues.

Several other biometric key generation schemes exist. However, they are all based on the same principle of using features that are unique to individuals to generate encryption keys for the purpose of data protection and other forms of security. In addition, most of the literatures on key generation described above are template based, requiring storage

of some information (either in its original form or distorted form as in the case of revocable biometrics).

In the area of template-free biometrics, key generation has been addressed in two major researches:

Harmer [130] investigated the direct key generation from biometric samples for implementation in a cryptosystem using the fingerprint modality. The research reported that an encryption key, with 21 effective bits, was reproduced correctly ~80% of the time with 55% unique keys in the resultant key-space.

Papoutsis [131] also examined the possibility of generation of the encryption keys for the desired encryption algorithm directly from properties (or features) of a given hardware (i.e. satellites). In such a way, security will be maximised since access to transmitted data will only be achievable by determining these encoding properties to regenerate the encryption keys or breaking the encryption cipher itself. The additional potential validation of the initiator node of a message will prevent the unauthorized introduction of malicious messages into the network communication spectrum, designed to deliberately corrupt its operation, which is a significant risk for any wireless communication system. This will serve both to minimize the need for key sharing as well as to validate the initiator node in a message.

The reviews above, although not the focus of this research, provide basic background information. It was also important to have mentioned the work done by Harmer and Papoutsis and to state that they are significantly different from this work which deals with the voice modality. While Harmer's work deals with fingerprint images and extracts useful features from it, Papoutsis work is similar to this research as it is signal based. However, it differs in the sense that the signals in Papoutsis work are from IC's and most times generates multiple modes and the subjects do not necessarily have control on the signals that they generate. It is therefore unlike in the case of this research where the subjects are humans who can sometimes choose not to allow the use of their samples, the signals from their samples could be altered by their mood, ailment,

age, etc, as well as the fact that human voice do not generate multiple modes which are considered unusual distributions.

2.8 Introduction to Template-free biometrics

Several recognition and authentication systems based on biometric measurements have been proposed in the last few years owing to the current security and data integrity challenges worldwide [47]. As a result, several algorithms and sensors have been developed to acquire and process many different biometric data sources. The recent introduction of biometric data in electronic documents, such as passports, has further increased the relevance of the secure storage and processing of personal biometric data. Currently, most biometric systems are based on templates and operate by measuring an individual's physical features in an authentication inquiry and comparing this data with biometric reference data stored on a template [62]. As the need for security increases, several concerns about biometrics, especially in the safety of the personal biometric information that is stored on the template have come to the fore [10], [63]. One of these concerns is that once a biometric source has been compromised, it cannot be re-issued, unlike passwords that can be cancelled and reissued if lost or stolen. Therefore, the owner of the biometric as well as the data protected by the biometric is compromised for life because users cannot ever change their features. Although revocable biometrics are in use today [2] – [9], [13] - [17], it is challenged by the integrity of the owner of the biometric sensor who may pre-record biometric samples, and those with access to the algorithm who may have, and can use, privilege rights to decipher measurable values unique to individuals.

A Template-Free biometric system is a novel approach to the security of biometric technology, which eliminates the need to use a template of pre-captured data as a basis for comparison before authentication is achieved. This technique exploits the possibility of directly encrypting the biometric data provided by the individual and therefore eliminates the need for storing templates used for data validation, thus increasing the security, and in turn user's confidence, in the system. Current research into template-

free biometrics seeks to address concerns associated with template storage of an individual's physical features as reference data for authentication/verification [62], [67]. In a template- free biometric system, a user provides samples of the given biometric allowing encryption keys to be generated directly from certain features in the samples. As a result, the proposed system requires no storage of the biometric templates and no storage of any private encryption keys is required. Template-free encryption possesses the significant advantages of removing the need for users to enrol or have personal biometric template data or private keys recorded.

Although an evolving system, research so far on template-free biometrics [68] - [71], [86] – [88], [97] – [100], [108], [109], [115] indicates that it basically operates via a two stage process called Calibration and Operation respectively. The Calibration phase is performed once per application domain and the Operation phase is employed subsequently every time an encryption key is required.

Abstractly, in the **Calibration phase,** a user provides samples of the given biometric to generate a global normal distribution functions or probability density curves formed from the probability distribution of the users' biometric keys within a quantised interval (details of which are described in this chapter). These are called normalisation maps from which encryption keys can be generated directly from certain features in the samples. As a result, the proposed system requires no storage of the biometric templates and no storage of any private encryption keys [87], [109].

In the **Operation phase,** a new set of samples are provided by the same user from which new keys may be generated directly. These are previously unseen samples (that have not been stored anywhere). The system then proceeds as a standard asymmetric encryption system where the message data is encrypted first with the receiver's asymmetric public key and a digest of the message is then encrypted with the sender's asymmetric private key regenerated via new biometric samples to form a digital signature. The encrypted message is then sent to the receiver [87], [109]. Figure 2.1 shows a conceptual key generation system.

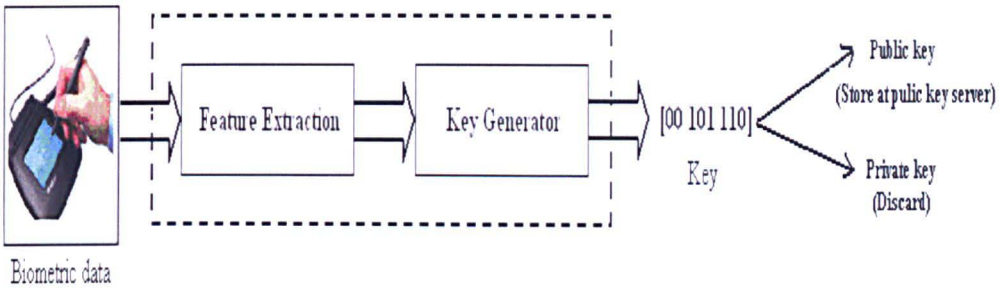

Figure 2.1: A conceptual biometric key generation system

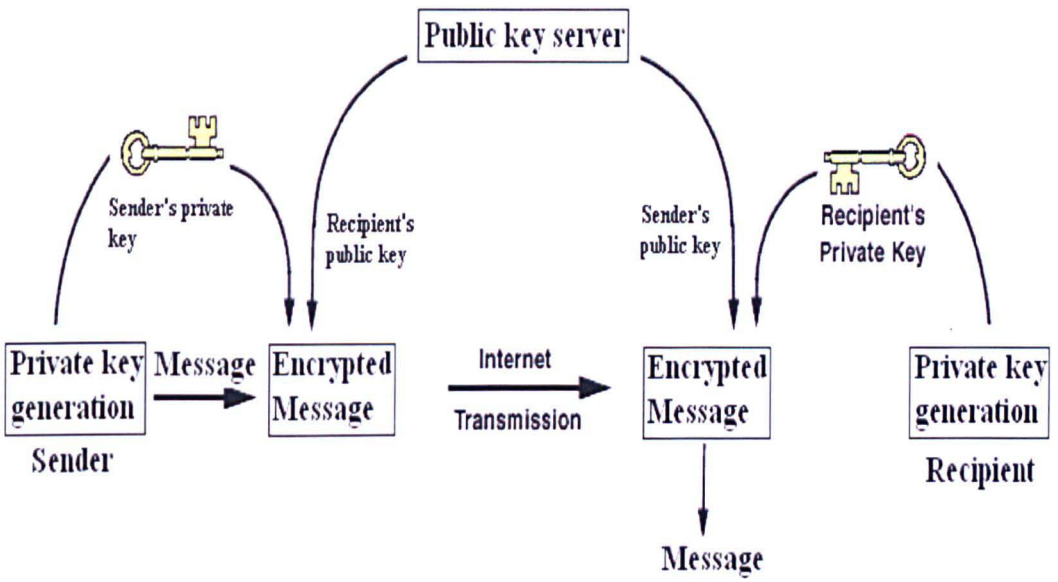

Figure 2.2: Working flow in a standard biometric system

Referring to Figure 2.2, to send a message using the biometric system, the following steps occur:

- Message data is encrypted first with the receiver's asymmetric public key.
- A digest of the message is then encrypted with the sender's asymmetric private key regenerated via new biometric samples to form a digital signature.
- The encrypted message is sent to the receiver.

- The encrypted message is decrypted first with the sender's asymmetric public key to verify the sender.
- The decrypted message is then further decrypted with the receiver's asymmetric private key again regenerated via further biometric samples.

Subsequent chapters will dwell on the details and how this applies to template-free systems.

Figure 2.3 is a block diagram of the calibration phase, depicting an initial single calibration which analyses typical biometric samples to determine the characteristics of the biometric modality in question.

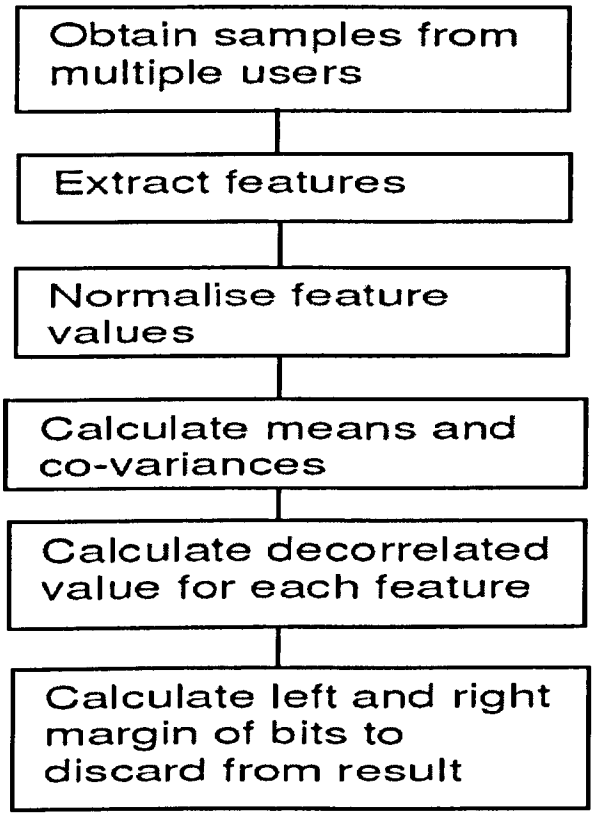

Fig. 2.3: Calibration

In the Operation phase, the encrypted message is decrypted first with the sender's asymmetric public key to verify the sender. Thereafter, the decrypted message is further decrypted with the receiver's asymmetric private key again regenerated via further

biometric samples. From a user perspective, the system may be simply viewed as an entirely self-contained operation as shown in Figure 2.4. It should be noted that no record of any biometric sample or communication with any networked resource is required [87], [109].

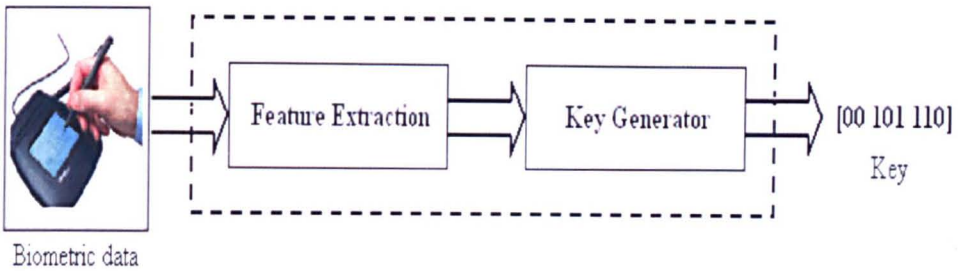

Fig. 2.4: Key generation in the Operation phase

Figure 2.5 is a block diagram of the Operation phase, depicting the Operation phase which is applied whenever keys are required from the system. Thus, ssubsequently, keys may be generated directly for previously unseen user samples as depicted in figure 2.5.

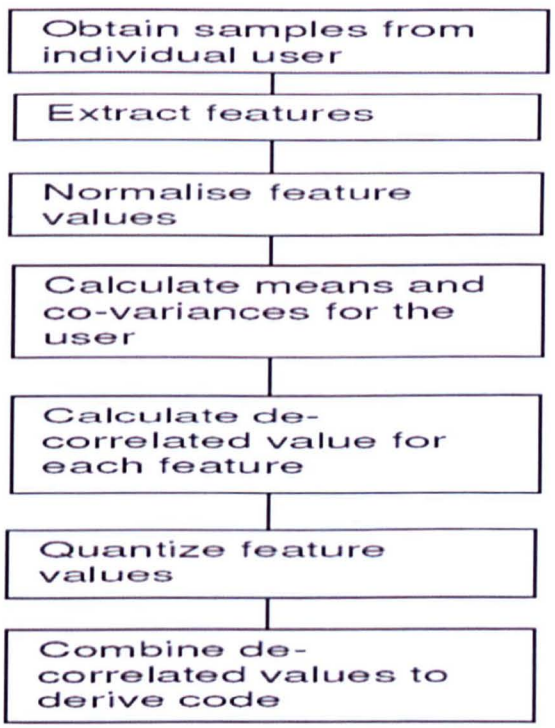

Figure 2.5: Operation

Subsequent chapters will provide more details on this subject and how it relates to the subject of voice based template-free biometrics.
Research in template-free systems has exploited the use of features from fingerprint [67], [130], Voice [62], [86] – [88], [108], [109], [115] and IC (Integrated Circuit) metrics [97] - [100], [131] (which although addressing non human features, but is based on the same principle of not storing template values to achieve authentication).

The novelty of the current proposal lies in the development of techniques for the *direct encryption* of data extracted from biometric samples of the human voice which characterise the identity of the individual. This research has identified a number of features from the human voice that can be useful in template-free biometric system and also introduced novel method of combining the biometric keys generated from the features. Such a system offers the following significant advantages:-

- The removal of the need to store any form of template for validating the user, hence directly addressing the disadvantages of template compromise.

- The security of the system will be as strong as the biometric and encryption algorithm employed (there is no back door). The only mechanisms to gain subsequent access are to provide another sample of the biometric or to break the cipher employed by the encryption technology.

- The (unlikely) compromise of a system does not release sensitive biometric template data which would allow unauthorised access to other systems protected by the same biometric or indeed any system protected by any other biometric templates present.

- A further significant advantage relates to the asymmetric encryption system associated with the proposed technique. Traditional systems require that the private key for decrypting data be stored in some way (memorising a private key is not feasible). With the proposed system, the key will be uniquely associated with the given biometric sample and a further biometric sample will be required to generate

the required private key. As there is no physical record of the key, it is not possible to compromise the security of sensitive data via unauthorised access to the key.

The investigation of voice as a suitable modality for template-free biometric systems is the main subject of this research and a number of publications have been made by the author [62], [86 – 88], [108], [109], [115] , [149]. The research has looked at extractable features in the human voice that can be used in template-free systems and in addition, a number of features and methods currently used in template-based systems were also studied and subsequent chapters will catalogue the success/failures recorded in the use of the various schemes.

2.9 Chapter Summary

This chapter reviewed extant literature on biometrics; the various types and applications. It also presented the economic activities that are generated by this field of research. However, there is paucity of information on template-free biometrics and no information on voice based template-free systems. It is this vacuum that the research reported here found as a niche. This research, which is, in the use of human voice features in a template-free biometric system introduces several novelties that seek to address template-based vulnerabilities in biometric systems.

In the succeeding chapter, this research will examine the suitability of using voice in a template-free system. Template-free system is a new trend in biometric research that aims at protecting the user of the biometric system and the biometric system itself. The next chapter also evaluated a number of human voice features useful for template-free system, and utilised a number of newly identified human voice features useful for template-free systems.

Chapter 3

Strategies for implementing voice features in Template-free Biometrics

The Science of Biometrics has to do with automatically recognising a person using distinguishing traits. Voice possesses very useful features and is considered a suitable biometric measure because it can be obtained from most humans. It is a primary mode of communication that is unique to individuals and can be identified by others (who are familiar with us), either physically or even on the telephone, microphone or across networks.

Voice satisfies the acceptable requirements of a biometric trait because it is robust, distinct, available, acceptable, and accessible. By "robust", we mean changing in a predictable fashion in an individual over time. By "distinctive", we mean showing great variation over the population. By "available", we mean that the entire population should ideally have this measure. By "accessible", we mean easy to measure using electronic sensors. By "acceptable", we mean that people do not object to having this measurement taken from them [18] – [20]. In addition, voice cannot be forgotten or misplaced, unlike knowledge-based (e.g. password) or possession-based (e.g. key) attributes. Specifically, voice has a higher advantage over other biometrics characteristics because in voice, we can change what password or code that an

individual says as well as the fact that it is the only biometric with which authentication can be achieved across a long distance medium like the telephone.

Voice is regarded as a performance biometric because an individual must perform a task to be recognized (in this case, speak). The above attributes qualify voice to be used as a biometric trait. The applications of voice biometrics are found in smartcards, forensics, healthcare, call centres, banking, and a host of other information assurance applications. In commercially available voice biometric systems, a wide range of features as will be described in this chapter are in use.

As described in section 1.2, the choice of voice as the modality to employ in this research stems from the fact that it has many advantages over other biometrics. However, a major thrust of this research is to determine the suitability of the voice modality in a template-free environment. The concept of template-free biometrics has been introduced in the previous chapter and its requirements the key elements in the features generated from voice to determine their suitability in template-free systems will be subsequently discussed. This chapter will describe the detailed analysis of those features from the human voice that are considered useful and how they are measured, indicating how they are distinct between different subjects (humans). Finally, the chapter will present experimental data to support the identification of some voice features that are suitable for template-free biometrics.

3.1 Analysis of voice features for suitability in template-free biometrics

As described earlier, voice is a primary mode of communication that is unique to individuals and can be identified by others, especially those who are close to us, even on the telephone, microphone or across networks. It is a good biometric characteristic because it is robust, distinct, available, acceptable, and accessible [19]. Voice is regarded as a performance biometric because an individual must perform a task to be recognized; in this case, speak. Voice, like other biometrics, cannot be forgotten or

misplaced, unlike knowledge-based (e.g., password) or possession-based (e.g., key) access control methods. Voice possess one more advantage over other biometric characteristics like fingerprint, iris, etc. as we can easily alter the phrase or word spoken which is used as the biometric sample. Therefore, it has the advantage of 2-factor authentication which combines what you have with what you know.

This section focuses on the study of the various characteristics (features) in the human voice which can be useful in directly generating encryption keys without having to store the features on a template, which subsequently improves the security of the data protected by it [62], [86] - [88], [108], [109], [115].

This study has looked at a number of voice features that have some measure of stability as well as distinguishing properties which makes them suitable for a template-free system [62], [86] - [88], hence the stability of biometric keys based on voice. Therefore, a set of criteria needs to be established to determine that features that meet those criteria are suitable. However, before drawing up the criteria, it is important to note a number of statistical properties to look out for in the features and which can be measured over a wide range of subjects to determine their consistency and uniqueness over a wide range of subjects.

For a template-free biometric system, the proposed features ideally need to be distinct to each individual. We therefore propose to investigate the arithmetic mean score of the samples taken from the same individual a number of times as a distinct measure of a feature's score [89], [90]. This is the arithmetic mean defined as "The mean of a list of numbers is the sum of all the members of the list divided by the number of items in the list". For a set of data $X=(x_1, x_2,.....x_n)$, the mean $\bar{x}$ is given by:

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \quad \text{.....(3.1)}$$

where x_i represents the value of each sample

In addition, it is important to investigate the following statistical properties:

- Statistical **variances** between several samples from a user and between different users: The variance of a random variable, probability distribution, or sample is a measure of statistical dispersion, averaging the squares of the deviations of its possible values from its expected value (mean). Campbell [56] says that for speaker recognition, features that exhibit high speaker discrimination power, high inter-speaker variability, and low intra-speaker variability are desired. Therefore, for this system, it is required that the features be fairly stable over a large number of samples of an individual and therefore should have very low intra-sample variances (i.e. the variance between several samples from the same user), but high inter-sample variances (i.e. the variance between the arithmetic mean of samples from different users). Standard variance function is used as given by:

$$\sigma^2 = \frac{\sum_{i=1}^{n}\left(x_i - \bar{x}\right)^2}{n} \qquad \text{.....(3.2)}$$

where x_i represents the value of each sample and $\bar{x}$ is the mean of all the samples and 'n' is the number of samples.

- **Covariance** between the features: Covariance is a measure of how strongly variables are correlated to each other [91]. We used this principle to investigate the relationship between the features like the effect of the change of one feature on another which provides an idea of how much the feature vary from the mean with respect to each other. This is useful in order to investigate if the value of one feature can be guessed from another. If the result of the covariance calculation is zero then the two variables are independent of each other. When the result is positive it signifies that the two variables have moved in the same direction. As the value increases in the positive direction, the more strongly related the two variables are. If the result is negative, then the two variables have a negative relationship with one another, that is, are moving in opposite directions [89], [90]. Covariance is given as:

$$Cov(X,Y) = \frac{1}{n}\sum_{i=1}^{n}\left[\left(X_i - \bar{X}\right)*\left(Y_i - \bar{Y}\right)\right] \quad \text{.....(3.3)}$$

where n=number of samples, $\bar{X}$ =mean of variable X, $\bar{Y}$ =mean of variable Y, X_i =a single sample of variable X, Y_i= a single sample of variable Y.

- The Correlation between the features is also an important factor to consider. **Correlation** is a method for establishing the degree of probability that a linear relationship exists between two measured quantities [89], [90]. When there is no correlation between the two quantities, then there is no tendency for the values of one quantity to increase or decrease with the values of the second quantity. If the value of one feature tends to increase as the value of a second increases, the two features are said to be positively correlated or just correlated. If the value of one feature tends to increase as the value of a second decreases, the two features are negatively or inversely correlated. If the value of one feature has no influence on the value of a second, they are independent or non-correlated. The measure of the correlation between the features was also considered in the choice of the features considered suitable. For two variables X and Y given as x_i and y_i, where i= 1,2,3.....n, the Correlation between X and Y is given as:

$$r_{xy} = \frac{\sum x_i y_i - n\bar{x}\bar{y}}{(n-1)s_x s_y}$$

$$= \frac{n\sum x_i y_i - \sum x_i - \sum y_i}{\sqrt{n\sum x_i^2 - (\sum x_i)^2}\sqrt{n\sum y_i^2 - (\sum y_i)^2}} \quad \text{.....(3.4)}$$

These measurable properties can be applied to potential features and used as the basis for determining the absolute values derivable from the voice signals to form a unique

representation. Considering this general overview on how to ascertain the suitability of the features, we define the criteria for a good feature as shown in table 3.1.

Table 3.1 Criteria for a good feature

1	Intra-sample variance	Low compared to inter sample variance
2	Inter-sample variance	Higher than intra-sample variance
3	Mean Value	Must be distinct
4	Correlation between the features	Should be minimal. Ideal value is 0. Therefore should be as close to zero as possible
5	Covariance between the features	Should be minimal. Ideal value is 0. Therefore should be as close to zero as possible

We therefore measured every characteristics defined in the human voice against the criteria to determine their suitability. In arriving at a good judgement, equations 3.1 – 3.4 and the procedures involved as detailed in this section were used.

As detailed in the experimentation, preliminary investigation of statistical properties of the mean, inter and intra sample variances, the covariance and correlations were employed in order to determine the useful features. Useful features possess distinct mean, low intra-user sample variance, high inter-user variance between user mean values, and almost zero covariance. It is important to note that the investigation was not restricted to features that are already in use in template-based systems since the focus is to look out for features with properties that can be measured without necessarily storing the samples from which the features were determined.

3.1.1 Review of features used in current voice based biometrics

Several strategies are employed to extract features for use in current template-based biometric systems. These schemes include the use of systems that directly extract specific features from the voice samples and those that use statistical methods to identify patterns in the human voice that are user specific.

Since research on speaker recognition became prominent in 1974 [57], various features have been extracted from the human voice for use in automatic identification. These include hidden features of human voice that cannot be directly measured, such as volume (soft or loud), pitch (high or low frequency), but first need to be processed in order to measure the value [76]. Most of the features described in this section are those available in research literature and which may be in use in commercial applications.

Many of the speaker identification systems available in literature use Mel frequency cepstral coefficients (MFCC), and linear predictive cepstral coefficients (LPCC) as features [80], [146]. The Mel-frequency represents a warping of the frequency band that is linear from 0 to 1 kHz and logarithmic at the higher frequencies, and the analysis is performed over this warped axis (in principle). This warping function has its origins in the human perception of tones. The speech signal is constrained to a bandwidth of about 150–3500 Hz for telephone speech and about 50 Hz–8 kHz for broadband communications [183]. The cepstral features are obtained by analyzing the Mel-scaled speech every 0.01 seconds over a time interval of about 20 milliseconds (nominally) in duration. This yields the Mel-scale spectrum and the Fourier coefficients of the logarithm of this function are produced. Depending on the system there are about 12–20 such coefficients produced every 0.01 seconds. These coefficients, MFCCs, are used to generate cepstral derivatives by differencing techniques, resulting in about 24 to 40 features and sometimes second derivatives [10]. One or more normalized energy features also employed to round out the basic feature set. Linear predictive analysis provides both an accurate estimate of the speech parameters and also an efficient computational model of speech. The basic idea behind linear predictive analysis is that a specific speech sample at the current time can be approximated as a linear combination of past speech samples. Through minimizing the sum of squared differences (over a finite interval) between the actual speech samples and linear predicted values a unique set of parameters or predictor coefficients can be determined. These coefficients form the basis for linear predictive analysis of speech. These two features have proved to be very good in speech recognition, but are not necessarily good in speaker identification;

hence currently, some researchers are focusing on improving these two features as well as appending new features to them [146].

Reynolds [102] also listed four features used in different speech and speaker recognition systems reported throughout the literature. The features are melfrequency and linear-frequency filterbank cepstral coefficients, linear prediction cepstral coefficients, and perceptual linear prediction (PLP) cepstral coefficients. Reynolds [102] presented an experimental evaluation of these different features and channel compensation techniques for robust speaker identification using the King speech database. This system used the Gaussian mixture speaker classifier which is a weighted sum of M components densities [121] and which is algebraically given as:

$$p(\vec{x}|\lambda) = \sum_{i=1}^{M} p_i b_i(\vec{x}) \quad \text{.....(3.5)}$$

where $\vec{x}$ is a D-dimensional random vector, $b_i(\vec{x})$, i =1, ..., M are the component densities and p_i, i = 1, ..., M, are the mixture weights. [121].

The best recognition performance based on this method was 92%.

Hirsimaki [77] measured the characteristics of the cochlea, which are its critical bandwidths in frequency domain that are equal to band pass filters with bandwidth spaced linearly at low frequency. The same method was also adopted by [185]

Atal [57] used pattern matching method to process cepstrum as inputs to do text dependent speaker recognition. Under this scheme, Atal reported that several different parametric representations of speech derived from the linear prediction model are examined for their effectiveness for automatic recognition of speakers from their voices. Twelve predictor coefficients were determined approximately once every 50 milliseconds from speech sampled at 10 kHz. The predictor coefficients and other speech parameters derived from them, such as the impulse response function, the autocorrelation function, the area function, and the cepstrum function were used as

input to an automatic speaker-recognition system. The speech data consisted of 60 utterances, consisting of six repetitions of the same sentence spoken by 10 speakers. The identification decision was based on the distance of the test sample vector from the reference vector for different speakers in the population; the speaker corresponding to the reference vector with the smallest distance was judged to be the unknown speaker. In verification, the speaker was verified if the distance between the test sample vector and the reference vector for the claimed speaker was less than a fixed threshold. Among all the parameters investigated, the cepstrum was found to be the most effective, providing an identification accuracy of 70% for speech 50 msec in duration, which increased to more than 98% for a duration of 0.5 sec. Using the same speech data, the verification accuracy was found to be approximately 83% for a duration of 50 msec, increasing to 98% for a duration of 1 sec. In a separate study to determine the feasibility of text-independent speaker identification, an identification accuracy of 93% was achieved for speech 2 sec in duration even though the texts of the test and reference samples were different.

Markel et al [59], while carrying out research on text independent speaker recognition, extracted the linear predictive coding (LPC) coefficients from the speech input.

Abdul Wahab et al [76] identified five features that are used in voice biometrics viz:

(a) Energy of the signal or Log energy which is defined as:

$$E_s = 10\log\left(\varepsilon + \frac{1}{N}\sum_{n=1}^{N} s^2(n)\right) \quad \text{.....(3.6)}$$

where ε is a small positive constant added to prevent the computing of log of zero and s(n) is the amplitude of the sampled signal.

(b) Zero crossing rate of the signal, which is an indicator of the frequency at which the energy is concentrated in the signal spectrum. Voiced speech is produced as a result of excitation of the vocal tract by the periodic flow of air at the glottis and usually shows a low zero crossing count. Unvoiced speech is produced due to excitation of the vocal tract by the noise-like source at a point of constriction in the interior of the vocal tract and shows a high zero crossing count. The zero

crossing count of silence is expected to be lower than for unvoiced speech, but quite comparable to that for voiced speech. Silence in this case means noise at very high SNR (Signal to Noise Ratio) [184].

(c) Normalized autocorrelation coefficient at unit sample delay, C which is defined as:

$$C = \frac{\sum_{n=1}^{N} S(n)S(n-1)}{\sqrt{(\sum_{n=1}^{N} s^2(n))(\sum_{n=0}^{N-1} s^2(n))}} \quad \text{.....(3.7)}$$

where C is the normalized autocorrelation coefficient and S(n) is the amplitude of the sampled signal. This feature is the correlation between adjacent speech samples. Due to the concentration of low frequency energy of voiced sounds, adjacent samples of voiced speech waveform are highly correlated, thus the coefficient is close to 1. On the other hand, the correlation is close to zero for unvoiced speech.

(d) First predictor coefficient: This is derived using the covariance method. It can be shown that this feature is the negative of the Fourier component of the log spectrum at unit sample delay. Since the spectra of the three classes (voiced, unvoiced, silence) differ considerably, so does the first LPC coefficient.

(e) Energy of the prediction error. This is defined as

$$E_p = E_s - 10\,log\,\langle 10^{-6} + \left|\sum_{k=1}^{p} \alpha_k \emptyset\,(0,k) + \emptyset\,(0,0)\right|.\rangle \quad \text{.....(3.8)}$$

$$\emptyset\,(i,k) = \frac{1}{N}\sum_{n=1}^{N} s(n-i)s(n-k) \quad \text{.....(3.9)}$$

where E_s is the log energy as defined in (a) and $\emptyset\,(i,k)$is the (i, k) term of the covariance matrix of the speech samples, α_k is the predictor coefficient and P is the total number of predictor coefficients.

Wahab [76] also reported that most researchers chose features in the frequency domain, such as LPC, pitch, formants, maximum and minimum amplitude frequencies while others use the time domain approach based on the auto correlation, covariance or zero crossing rate (ZCR). The frequency domain approach is also called the quefrency domain, which is derived from the word 'frequency' since the features extracted from this domain are first processed in frequency domain before they are finally converted back to the time domain. Some examples of the features belonging to this domain are real cepstrum and melcepstrum.

Zhu and O'Shaughnessy [79] also used Log-Energy Dynamic Range Normalization for Robust Speech Recognition to improve recognition result by 30.83% over the reference front-end algorithm in clean-condition training.

Abdulla [80] also introduced a feature called perceptual log area ratio (PLAR), which depends on notions from psychoacoustics where the robustness can be assured. Abdulla also identified the log area ratio as an effective feature for recognizing speakers as it embodies the geometry and dynamics of the vocal tract, which are very much person-dependent. This method modeled the speakers' vocal tracts in form of transforming LPC into LAR feature in which the vocal tract of an individual is modeled as a non-uniform acoustic tube. The LAR coeffients are therafter calculated by the equation

$$LAR_i = log\ \frac{A_i}{A_{i+1}} = log\ \left(\frac{1+\alpha_1}{1-\alpha_1}\right), A_{p+1} = 1 \quad \text{.....(3.10)}$$

where α_1 is the ith partial correlation (parcor) coefficient which can be found by

$$\alpha_1 = a_i^{(i)}\ 1 \leq i \leq p$$

where $a_i^{(i)}$ is the ith coefficient calculated by the ith order LP model

Subramanya et al [81] used the following features: (i) the raw likelihoods resulting from each recognizer pass, (ii) the difference between the raw likelihoods (LR), and (iii) the durations. This system used the CUT YOHO corpus with varying lengths of passphrases. The result obtained shows an improvement of 36.41% in EER.

Avci [82] introduced an expert speaker recognition system based on optimum wavelet packet entropy parameter values. Avci [82] further mentioned speech features which are usually obtained via Fourier transforms (FTs), short-time Fourier transforms (STFTs) or linear predictive coding techniques, as well as wavelet and wavelet packet analysis. The classification result obtained from this system is 85%.

Kuwabara and Sagisaka [83] mentioned prosodic features such as the fundamental frequency contour, the duration of words, timing, rhythm, pause, and power levels.

In addition, Kuwabara and Sagisaka [83] identified two types of acoustic characteristics, the voice source and the vocal tract resonance. Voice source comprises of (1) the average pitch frequency, (2) the time-frequency pattern of pitch (the pitch contour), (3) the pitch frequency fluctuation, (4) the glottal wave shape, while Vocal tract resonance comprises of (1) the shape of spectral envelope and spectral tilt, (2) the absolute values of formant frequencies, (3) the time-frequency pattern of formant frequencies (formant trajectories), (4) the long-term average speech spectrum, (5) the formant bandwidth.

Monrose et al [138], proposed a method that uses entropy from the way a user speaks a password. The proposed technique reliably generates a cryptographic key from a user's voice while speaking a password. The key resists cryptanalysis even against an attacker who captures all system information related to generating or verifying the cryptographic key.

Several other features are in use, especially in commercial applications, which are not readily available for listing because of commercial competition reasons. This research reviewed the suitability of the existing features mentioned above in addition to other features suggested in this work as will be detailed in the next section.

3.1.2 Review of additional features proposed in this system

Maximum, Minimum, and Average Power Spectral Densities (PSD)

Power spectral density function (PSD) shows the strength of the variations (energy) as a function of frequency. In other words, it shows at which frequencies variations are strong and at which frequencies variations are weak [186]. The power spectral density (PSD) is intended for continuous spectra. The unit of PSD is energy per frequency (width) and energy can be obtained within a specific frequency range by integrating PSD within that frequency range. Power spectral density is commonly expressed in watts per hertz (W/Hz) or dBm/Hz [92], [187].

From [186], the power spectral density (PSD) of a stationary random process X_n is mathematically related to the autocorrelation sequence (RXX) by the discrete-time Fourier transform. This is given by:

$$P_{xx}(\omega) = \frac{1}{2\pi}\sum_{m=-\infty}^{\infty} R_{xx}(m)e^{-j\omega m} \quad \text{.....(3.11)}$$

Which can be written as a function of physical frequency$\omega = 2\pi f/f_s$; where f_s is the sampling frequency. Therefore,

$$P_{xx}(f) = \frac{1}{f_s}\sum_{m=-\infty}^{\infty} R_{xx}(m)e^{-2\pi jfm/f_s} \quad \text{.....(3.12)}$$

According to Matlab(TM) documentation [188], the integral of the PSD over a given frequency band computes the average power in the signal over that frequency band. Since Matlab was used in many of the experimentation (refer to experiment section), the bitstreams generated from the audio input has a measure of its maximum, minimum, and average values. Consequently, the PSD functions can also be measured in terms of its maximum, minimum, and average values.

Cepstrum Analysis (Maximum, Minimum, and Mean cepstrum)

Bogert et al [93] introduced the term cepstrum. They observed that the logarithm of the power spectrum of a signal containing an echo had an additive periodic component due to echo. Voiced speech generally can be regarded as the response of the vocal tract articulation equivalent filter driven by a pseudo periodic source. Cepstrum analysis is a nonlinear signal processing technique with a variety of applications in areas such as speech and image processing. Thus, it is a potential feature that can be used in voice based template-free biometric system. The Signal Processing Toolbox [183] provides three functions for cepstrum analysis.

1. Complex cepstrum
   - Maximum CCEPS
   - Minimum CCEPS
   - Average CCEPS

2. Inverse Complex cepstrum
   - Maximum ICCEPS
   - Minimum ICCEPS
   - Average ICCEPS

3. Real Cepstrum
   - Maximum RCEPS
   - Minimum RCEPS
   - Average RCEPS

A complex cepstrum can be defined as the inverse Fourier transform of the complex logarithm of a Fourier transform. According to Bogert et al [93], for a sequence x, the complex cepstrum can be calculated by

$$\hat{x}[n] = \frac{1}{2\pi}\int_{-\pi}^{\pi} log\left[X(e^{j\omega})\right]e^{j\omega n}d\omega$$

$$= \frac{1}{2\pi}\int_{-\pi}^{\pi}[\log|X(e^{j\omega})| + j\arg(X(e^{j\omega}))]e^{j\omega n}d\omega \quad \text{.....(3.13)}$$

where arg is the continuous (unwrapped) phase function.

The toolbox function cceps in Matlab is used to perform this operation.

The real cepstrum is used to design an arbitrary length minimum-phase FIR filter from a mixed-phase sequence [192]. The *real cepstrum* of a signal x, is calculated by determining the natural logarithm of magnitude of the Fourier transform of x, then obtaining the inverse Fourier transform of the resulting sequence. It is given by

$$c_x = \frac{1}{2\pi}\int_{-\pi}^{\pi}\log|X(e^{j\omega})|e^{j\omega n}d\omega \quad \text{.....(3.14)}$$

Matlab function 'rceps' performs this operation.

Maximum, Minimum, and Average Fast Fourier Transform (fft)

Fourier Transform (FT) is used in a number of signal and image processing applications. It is a representation of an image as a sum of complex exponentials of varying magnitudes, frequencies, and phases. It can also be described as a wavelet transform with basis vectors defined by trigonometric functions. Defined mathematically [188], if f(m, n) is a function of two discrete spatial variables 'm' and 'n', then the two-dimensional Fourier transform of f(m, n) is defined by the relationship

$$f(\omega_1, \omega_2) = \sum_{m=-\infty}^{\infty}\sum_{n=-\infty}^{\infty} f(m,n)\, e^{-j\omega_1 m}\, e^{-j\omega_2 m} \quad \text{.....(3.15)}$$

Where ω_1, ω_2 are frequency variables; $f(\omega_1, \omega_2)$ is the frequency domain representation of $f(m, n)$.

When signals in time domain are transformed into frequency domain, a special variant of Fourier Transform called Discreet Fourier Transform (DFT) is used i.e. the Discrete Fourier Transform (DFT) is used to produce frequency analysis of discrete non-periodic signals. DFT is usually the FT method used when working with computers because its input and output values are discrete samples, making it convenient for computer manipulation. However, a faster method of computing DFT is the Fast Fourier Transform (FFT). This method can be investigated to determine special properties of the voice signal for biometric purpose.

Mathematically, for a vector of length N, the function X=fft(x) and X=ifft(x) implement the transform and inverse transforms of the vector given by:

$$x(k) = \sum_{j=1}^{N} x(j)\omega_N^{(j-1)(k-1)} \quad \text{.....(3.16)}$$

$$x(j) = (1/N) \sum_{k=1}^{N} x(k)\omega_N^{-(j-1)(k-1)} \quad \text{.....(3.17)}$$

Where

$\omega_N = e^{(-2\pi i)/N}$ is an Nth root of unity [188].

Maximum, Minimum, and Average Hilbert function

The Hilbert transform is useful in calculating instantaneous attributes of a time series, especially the amplitude and frequency [188]. These are signal attributes that have potential uses in voice based biometrics and consequently proposed for investigation in this research. According to Kschischang [189], Hilbert transform $H[g(t)]$ can be defined as

$$H[g(t)] = g(t) * \frac{1}{\pi t} = \frac{1}{\pi}\int_{-\infty}^{\infty} \frac{g(\tau)}{t-\tau}\,\delta\tau = \frac{1}{\pi}\int_{-\infty}^{\infty} \frac{g(t-\tau)}{\tau}\,\delta\tau \quad \text{.....(3.18)}$$

Where the Hilbert Transform of $g(t)$ is the convolution of $g(t)$ with the signal $1/\pi t$

The function x = hilbert(xr) returns a complex helical sequence, sometimes called the analytic signal, from a real data sequence [188]. The analytic signal x = xr + i*xi has a real part, xr, which is the original data, and an imaginary part, xi, which contains the Hilbert transform.

Linear Predictive Coding (LPC)

Linear Predictive Coding (LPC) is a method of measuring speech parameters accurately. It uses a process called inverse filtering to remove the effect of formants from the speech signal and then estimate the intensity and frequency of the remaining signal which is called the residue. The formants and the residue can be estimated accurately in form of integers which are measured as the special characteristics (features) and which are unique to individuals. The application of LPC varies from filter design to speech coding.

According to [188], [a,g] = lpc(x, p) is given by

$$\hat{x}(n) = -a(2)x(n-1) - a(3)x(n-2) - \cdots - a(p+1)x(n-p) \quad \text{.....(3.19)}$$

p is the order of the prediction filter polynomial, a = [1 a(2) ... a(p+1)]. If p is unspecified, lpc uses as a default p = length(x)-1. If x is a matrix containing a separate signal in each column, lpc returns a model estimate for each column in the rows of matrix a and a column vector of prediction error variances g. The length of p must be less than or equal to the length of x.

Cross Correlation

Cross correlation is the method of estimating the similarity of two waveforms. It Is mostly used in pattern recognition, single particle analysis, electron tomographic averaging, cryptanalysis, and neurophysiology. It can be represented as:

$$R_{xy}(m) = E\{x_{n+m}y_n^*\} = E\{x_n y_{n-m}^*\} \quad \text{.....(3.20)}$$

where x_n and y_n are jointly stationary random processes, $-\infty < n < \infty$, and $E\{\cdot\}$ is the expected value operator [188].

Auto Correlation

Autocorrelation is used to identify repeating patterns in a signal. It is like the cross correlation of a signal within itself. Autocorrelation can also be defined as a mathematical representation of the degree of similarity between a signal and its lagged version over consecutive time intervals. Its value usually range from -1 to +1 with an autocorrelation of +1 representing a perfect positive correlation in which case the increase in a time series signal will lead to a proportionate increase in the lagged version of the same signal. On the other extreme, a n autocorrelation of -1 represents a perfect negative correlation in which case the time series signal and its lagged version moves in proportionately opposite direction [190].

Many of these other features used are standard mathematical/ signal processing functions whose details and were measured using functionalities available in Matlab. Their mathematical derivations are not very necessary to provide an understanding of the research.

It is therefore now necessary to show the experimental setup used to determine the suitability of these features.

3.2 Experimental evaluation of suitable features

Experimental evaluations were carried out to ascertain that the proposed features will meet the requirement for a template-free system as summarised in table 3.1. The datasets are described in 3.2.1. All the experiments were conducted using functions available in Matlab. A code was developed to read the audio samples using the Microsoft based 'wave audio format' in combination with the 'wavread' function in Matlab. This acts as a simple algorithm that extracts features from the human voice. The Waveform Audio File Format (WAVE or WAV) is a standard file format for storing an audio bitstream [92]. Matlab 'WAVREAD' function reads Microsoft WAVE (".wav") sound file and returns a sampled value which can be denoted as 'y'. The value of 'y' that returns a new value for each of the functions representing the respective features (fft, cceps, rceps, psd, etc.) which is unique to each individual. Therefore, the steps for testing a feature is as summarized below:

i. Take several voice samples from an individual. (In one of the datasets used in this research, 106 users were evaluated and each provided 5 samples while in the second datasets, there were 4 Enrollment sessions per subject with 24 phrases per session and 10 test sessions per subject with 4 phrases per session
ii. Convert the samples into 'wav' format. This uses existing standard conversion software and need not be dwelt upon.
iii. Use the wavread function to extract the signal values from each of the samples taken. This is the value represented as 'y' above.
iv. Take the average of all the values from the respective samples of the same individual i.e. the average of 'y'.
v. For the various features, use the respective functions to read 'y' in order to obtain the value of that feature i.e. feature= function (y).

To further illustrate the steps above, consider a typical feature to be measured as described below.

Step 1

Take a number of audio samples from a subject and label them as 'sample 1', 'sample 2', 'sample 3' 'sample 4', 'sample 5' ..... 'sample n'

Step 2

Use standard audio conversion tools to convert the samples into wave form with '.wav' extension.

Step 3

Read each sample by applying the 'wavread' function.

Step 4

Take the average of each result obtained from step 3 and apply the function as described in 3.1.2

Step 5

Calculate the mean of the results for all the samples in step 4

Step 5

Take the variance of each value for the samples in step 4

As part of the check for the criteria in table 3.1, steps 6 and 7 below which are basically to investigate the effect of the change of one feature on the other will be considered.

Step 6

Measure the covariances between the features using equations (4.3)

Step 7

Measure the correlations between the features using equations (4.4)

These steps are repeated for each feature to be tested and those that meet the criterion set in table 3.1 are considered useful. A further review of the practical experimentation is detailed subsequently.

3.2.1 Datasets

The experiments were carried out on two main databases - the VALID Datasets and the YOHO Datasets. The two databases comprises of voice samples collected over a period of time from varying subjects with diverse ethnic and gender backgrounds.

The VALID database [94] contains 530 samples (consisting of five recordings for each of 106 individuals over a period of one month), each one uttering the sentence "Joe Took Father's Green Shoebench Out" and the numbers "5 0 6 9 2 8 1 3 7 4". The recordings were acquired across different environments/ background – noisy, real world, and others in office scenario with no control on acoustic noise.

The YOHO speaker verification Database [95] consists of:

- "Combination lock" phrases (e.g., 36-24-36)
- 138 subjects: 108 males, 30 females
- Collected over 3 month period in a real-world office environment
- 4 Enrollment sessions per subject with 24 phrases per session
- 10 Test sessions per subject with 4 phrases per session
- Total of 1932 validated sessions
- 8 kHz sampling with 3.8 kHz analog bandwidth
- 1.2 gigabytes of data (when uncompressed)

3.2.2 Tests

The initial part of the research carried out extensive tests on various features to determine their suitability for template-free system. A number of candidate features were tested (including those that are currently in use in template-based systems) to determine their suitability in template-free system. The tests were carried out to ascertain features with distinct means whose intra sample variances are lower compared to the inter-sample variances between the mean values. The aim is to look out for features that exhibit high speaker discrimination power, high inter-speaker variability, and low intra-speaker variability. Therefore, for this system, it is specifically required that those features are fairly stable over a large number of samples, possessing very low intra-sample variances (i.e. the variance between several samples from the same user), but high inter-sample variances (i.e. the variance between the arithmetic mean of samples from different users). Therefore, we used the criteria outline in Table 3.1 and subjected the features through steps 1 to 7 above. Tables 3.2 to 3.6 are examples of results obtained using this procedure.

According to the proposed criteria for a useful feature, a distinct mean value should be determinable. Secondly, intra-sample variance needs to be smaller in comparison with inter-sample variances. Furthermore, the covariance between the features should show that there is almost zero covariance between the features, except for those within the same domain (e.g. all features from Amplitude domain like minimum, average, and maximum amplitude will normally be correlated). The features that were successfully evaluated are indicated in the next section.

Using the datasets described in 3.2.1, the percentage of subjects with Intra-sample variance value lower compared to inter-sample variance were evaluated for each proposed feature in which it was possible to determine a distinct mean value. Furthermore, the percentage of each feature correlations and covariances with other features (i.e. the number of feature correlations and covariances amongst the useful features) were evaluated. For each of the subjects in the datasets, the proposed features were tested and results obtained are as summarised subsequently.

3.2.3 Results

The system was evaluated against the datasets described in section 3.2.1. The purpose of the experiments was to ascertain the features that are potentially suitable for use in voice based template-free biometric system.

The first step in all cases was to be able to measure a distinct mean value which was possible in all the twenty nine proposed features evaluated. These are typical intra-sample means of the samples from the same subject at varying intervals and locations. In addition, the intra-sample variances between these samples are calculated using the method proposed in equation 3.2 in section 3.1

An example for peak-to-peak amplitude feature is shown in table 3.2, showing typical mean values and intra sample variance of peak-to-peak amplitude for different subjects denoted by x0, x1.....xn.

Table 3.2: samples of intra-sample means and variances for various subjects (x) from the VALID database for peak-to-peak amplitude

Sample	Intra sample Means	Intra sample variances
x0	0.2862	0.0132
x1	0.2478	0.0017
x2	0.2901	0.00061421
x3	0.4201	0.0181
x4	0.3417	0.0056
x5	0.2091	0.0039
x6	0.2476	0.0034
x8	0.4566	0.0031
x9	0.3411	0.0018
x10	0.4029	0.0138

This is pictorially represented in figure 3.1 below which clearly shows the mean of each set of samples (x), and the corresponding value of intra-sample variances.

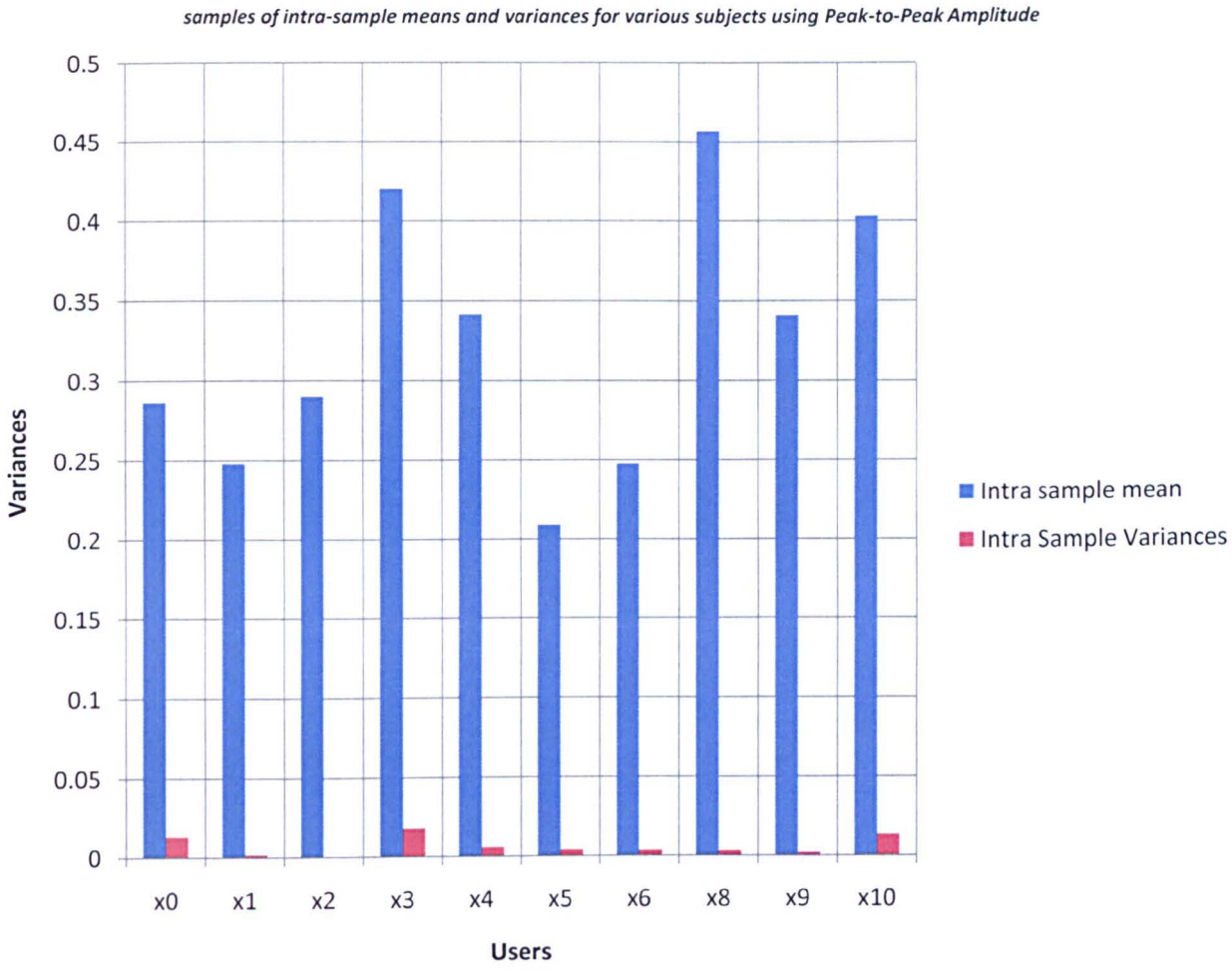

Figure 3.1: comparing intra sample means and variances

The blue bar represents intra-sample mean while the red bar represent intra-sample variances.

Another typical case for maximum power spectral density is shown in Table 3.3. This table shows samples of normalised mean scores with the inter sample variance values for successive users.

Table 3.3: Samples of normalised mean scores and inter-sample variances for maximum power spectral density from the VALID database

User candidate	Mean scores	Inter-sample variables	Inter-sample variances
x0	0.5297	x0-x1	0.003362
x1	0.4477	x1-x2	0.0080264
x2	0.321	x2-x3	0.0369376
x3	0.5928	x3-x4	0.0035617
x4	0.5084	x4-x5	0.007688
x5	0.3844	x5-x6	0.0054184
x6	0.2803	x6-x8	0.049707
x8	0.5956	x8-x9	0.0064752
x9	0.4818	x9-x10	0.0001824
x10	0.5009	x10-x11	0.001245

This table is plotted in figure 3.2 below which clearly shows the comparison between the mean of a set of sample (x), and the corresponding value of intra-sample variances.

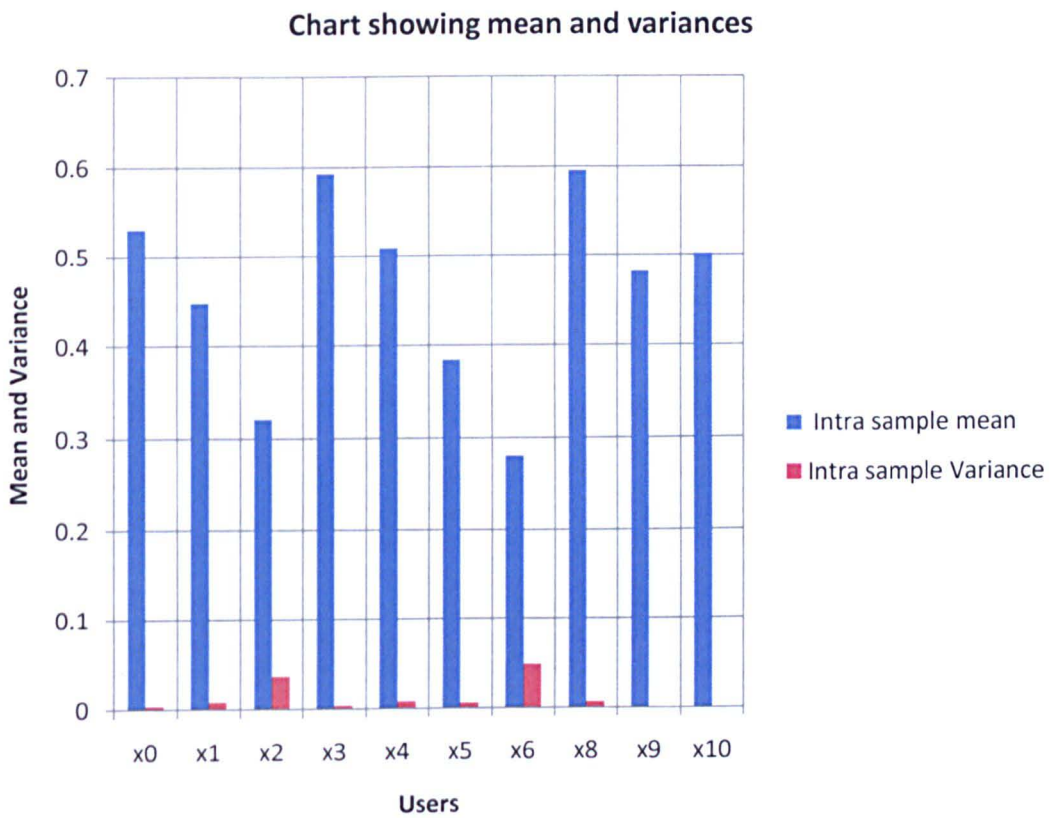

Figure 3.2: comparing mean and inter sample variance values for power spectral density

The sample results in Tables 3.2 and 3.3 as well as figures 3.1 and 3.2 is the first step in every feature evaluation. For any feature to be evaluated for suitability in this research, it should first be measureable, although this measurement is not an indication of whether all other criteria for suitability will be met. The overall result indicates that twenty nine (29) features were measurable and consequently used for further evaluation as detailed subsequently. These include:

1. Maximum Power Spectral Density (PSD)
2. Average Power Spectral Density (PSD)
3. Minimum Power Spectral Density (PSD)
4. Maximum fft
5. Mean fft
6. Minimum fft
7. Maximum Amplitude
8. Peak to Peak Amplitude
9. Mean Amplitude
10. Minimum Amplitude
11. Maximum Cepstrum
12. Minimum Cepstrum
13. Mean Cepstrum
14. Maximum ifft
15. Minimum ifft
16. Mean ifft
17. Maximum hilbert function
18. Minimum hilbert function
19. Mean hilbert function
20. Maximum LPCC
21. Minimum LPCC
22. Mean LPCC
23. Log Energy
24. Maximum Cross Correlation
25. Minimum Cross Correlation
26. Mean Cross Correlation
27. Maximum Auto Correlation
28. Minimum Auto Correlation
29. Mean Auto Correlation

Subsequently, this study experimented to view the difference between the intra and inter sample variances so as to determine criterion 1 and 2 in table 3.1. The twenty nine (29) features above were evaluated to ensure that beyond the possibility of measuring their sample mean values, they can meet the additional criteria specified.

Table 3.4 below is an extract of a typical evaluation of a feature showing that inter-sample variance values are higher compared to intra-sample variances in some of the features.

Table 3.4: Sample mean scores, intra and inter-sample variances, showing higher inter sample variance values for maximum amplitude from the VALID database

User	Mean	intra sample variance	Inter sample variances between successive means	Positive Difference indicating higher inter sample variance
x0	0.2967	0.0021	0.038198	0.036098
x1	0.5731	0.000503	0.023762	0.023259
x2	0.3551	0.005	0.015647	0.010647
x3	0.532	0.0024	0.01234	0.00994
x4	0.3749	0.0011	0.002911	0.001811
x5	0.2986	0.006	0.009814	0.003814
x6	0.4387	0.00065	0.000169	-0.00048
x8	0.4203	0.0029	0.007296	0.004396
x9	0.2995	0.0023	0.036073	0.033773
x10	0.5681	0.0011	0.013613	0.012513
x11	0.4031	0.000317	0.019582	0.019266
x12	0.601	0.0014	0.014878	0.013478
x13	0.4285	0.000985	0.00236	0.001375
x14	0.3598	0.0071	0.015789	0.008689
x16	0.5375	0.0011	0.007357	0.006257
x17	0.4162	0.0011	0.009194	0.008094
x18	0.5518	0.0065	0.029452	0.022952
x19	0.3091	0.001	0.010382	0.009382
x20	0.4532	8.02E-05	0.000293	0.000213

This table can better be represented in figure 3.3 below which clearly shows that for each mean of a set of sample (x), the corresponding value of inter-sample variances between the mean are higher compared with intra-sample variances.

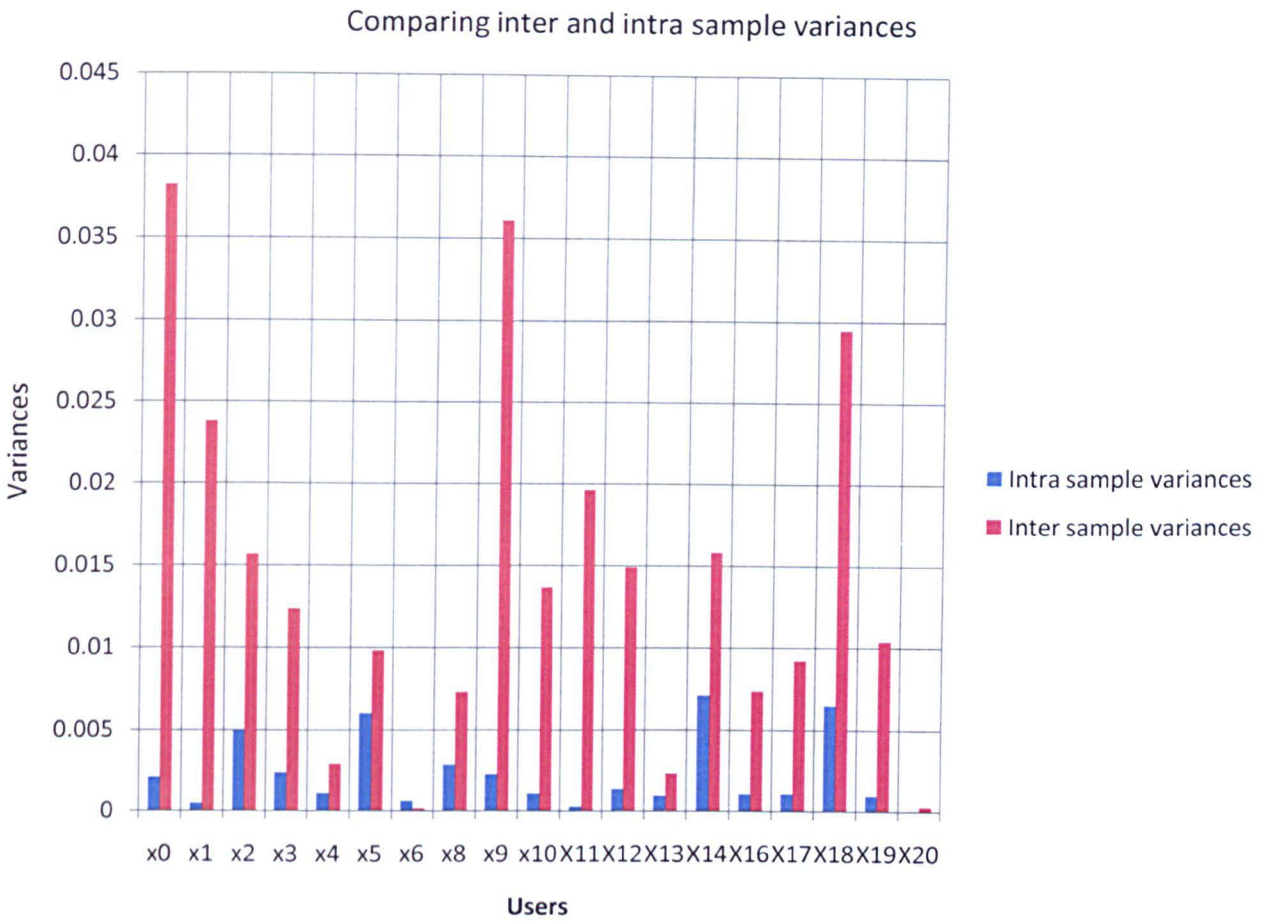

Figure 3.3: Comparing inter and intra sample variance values for respective subjects using Maximum Amplitude

Figure 3.3 graphically explains the comparison between intra-sample and inter-sample variances. The blue bar represents intra-sample variance while the red bar represents inter-sample variances. For a useful feature, it can be seen that inter-sample variance is higher compared to intra-sample variances. From table 3.4, it can be deduced that for each user (x) the intra-sample variances are lower compared to the inter-sample variances for a typical useful feature. Table 3.7 summarises the results of the percentage of users in both the VALID and the YOHO databases in which the inter-sample variance is higher than intra-sample variance and vice versa, and which contributes the use-ability or otherwise of the proposed features.

A further step is to evaluate the useful features to determine the relationships between them in terms of the covariances and correlations. Sample results of feature covariance for features using the VALID database are shown in table 3.5 below. The covariance between the features shows that there is almost zero covariance between the features, except for those within the same domain (e.g. Minimum Amplitude and Maximum Amplitude), which implies that the change in the value of one feature does not affect another feature. Therefore the value of one feature cannot be guessed from the other. In terms of correlation, some of the features tend to be anti-correlated (i.e. have values close to -1 and as such have negative linear relationship) and in some cases tends to be close to 1 (indicating a linear relationship). Thus, there are indications that the values of some features are likely to move in the same direction (for those close to 1) and in diverse direction (for those close to -1).

Table 3.5: Samples of feature covariance for VALID database features

Legend:

X= User
A=Mean Amplitude
B=Maximum Amplitude
C=Minimum Amplitude
D=Peak to Peak Amplitude
E=Mean Frequency
F=Maximum Frequency
G=Minimum Frequency
H=Maximum PSD
I=mean PSD
J=Minimum PSD
K= Maximum Hilbert function
L= Mean Hilbert function
M= Minimum Hilbert function

Covariance Matrix for Speaker x0

	A	B	C	D	E	F	G	H	I	J
A	8.13E-10	-8.28E-07	7.47E-07	-1.58E-06	-1.30E-05	-8.02E-04	3.66E-09	6.71E-10	-1.17E-09	-1.13E-12
B	-8.28E-07	3.30E-03	-3.30E-03	6.60E-03	4.39E-02	2.89E+00	1.62E-05	1.60E-04	6.31E-06	3.32E-09
C	7.47E-07	-3.30E-03	3.30E-03	-6.60E-03	-4.46E-02	-3.14E+00	-1.78E-05	-1.68E-04	-6.41E-06	-3.19E-09
D	-1.58E-06	6.60E-03	-6.60E-03	1.32E-02	8.84E-02	6.03E+00	3.40E-05	3.28E-04	1.27E-05	6.51E-09
E	-1.30E-05	4.39E-02	-4.46E-02	8.84E-02	6.57E-01	6.94E+01	2.15E-04	3.00E-03	9.26E-05	3.54E-08
F	-8.02E-04	2.89E+00	-3.14E+00	6.03E+00	6.94E+01	2.19E+04	1.80E-02	1.03E+00	1.39E-02	-2.36E-06
G	3.66E-09	1.62E-05	-1.78E-05	3.40E-05	2.15E-04	1.80E-02	1.97E-07	1.10E-06	3.48E-08	9.78E-12
H	6.71E-10	1.60E-04	-1.68E-04	3.28E-04	3.00E-03	1.03E+00	1.10E-06	6.27E-05	8.18E-07	-6.52E-11
I	-1.17E-09	6.31E-06	-6.41E-06	1.27E-05	9.26E-05	1.39E-02	3.48E-08	8.18E-07	1.69E-08	4.19E-12
J	-1.13E-12	3.32E-09	-3.19E-09	6.51E-09	3.54E-08	-2.36E-06	9.78E-12	-6.52E-11	4.19E-12	5.10E-15

Covariance Matrix for Speaker x1

	A	B	C	D	E	F	G	H	I	J
A	2.06E-11	-4.21E-08	3.36E-08	-7.57E-08	-3.57E-07	1.15E-04	4.29E-10	3.48E-09	8.25E-11	2.37E-14
B	-4.21E-08	7.44E-04	-3.38E-04	1.10E-03	9.50E-03	8.51E-02	1.22E-05	1.86E-05	6.55E-07	3.68E-10
C	3.36E-08	-3.38E-04	2.50E-04	-5.88E-04	-6.30E-03	9.46E-02	-5.98E-06	2.77E-06	-1.71E-07	-2.15E-10
D	-7.57E-08	1.10E-03	-5.88E-04	1.70E-03	1.58E-02	-9.60E-03	1.82E-05	1.58E-05	8.26E-07	5.84E-10
E	-3.57E-07	9.50E-03	-6.30E-03	1.58E-02	2.52E-01	4.67E+00	3.79E-04	2.79E-04	1.81E-05	1.41E-08
F	1.15E-04	8.51E-02	9.46E-02	-9.60E-03	4.67E+00	9.68E+02	1.63E-02	4.41E-02	1.30E-03	6.09E-07
G	4.29E-10	1.22E-05	-5.98E-06	1.82E-05	3.79E-04	1.63E-02	7.20E-07	9.22E-07	4.01E-08	2.66E-11
H	3.48E-09	1.86E-05	2.77E-06	1.58E-05	2.79E-04	4.41E-02	9.22E-07	2.77E-06	7.29E-08	3.04E-11
I	8.25E-11	6.55E-07	-1.71E-07	8.26E-07	1.81E-05	1.30E-03	4.01E-08	7.29E-08	2.55E-09	1.45E-12
J	2.37E-14	3.68E-10	-2.15E-10	5.84E-10	1.41E-08	6.09E-07	2.66E-11	3.04E-11	1.45E-12	1.01E-15

Covariance Matrix for Speaker x2

	A	B	C	D	E	F	G	H	I	J
A	1.68E-11	7.66E-08	6.19E-09	7.04E-08	-1.05E-06	-1.20E-05	5.48E-10	2.45E-08	4.56E-10	3.75E-15
B	7.66E-08	4.50E-04	-3.51E-05	4.86E-04	-1.70E-03	2.33E-04	1.79E-06	1.30E-04	2.75E-06	4.10E-11
C	6.19E-09	-3.51E-05	9.34E-05	-1.29E-04	-2.60E-03	-1.22E-01	6.14E-07	8.93E-06	5.55E-08	-6.24E-13
D	7.04E-08	4.86E-04	-1.29E-04	6.14E-04	9.44E-04	1.23E-01	1.17E-06	1.21E-04	2.70E-06	4.16E-11
E	-1.05E-06	-1.70E-03	-2.60E-03	9.44E-04	1.65E-01	2.93E+00	-6.15E-05	-1.10E-03	-1.18E-05	3.22E-10
F	-1.20E-05	2.33E-04	-1.22E-01	1.23E-01	2.93E+00	1.74E+02	-6.99E-04	-2.53E-02	-4.53E-04	-1.03E-08
G	5.48E-10	1.79E-06	6.14E-07	1.17E-06	-6.15E-05	-6.99E-04	3.73E-08	8.97E-07	1.53E-08	2.03E-13
H	2.45E-08	1.30E-04	8.93E-06	1.21E-04	-1.10E-03	-2.53E-02	8.97E-07	4.49E-05	9.36E-07	1.66E-11
I	4.56E-10	2.75E-06	5.55E-08	2.70E-06	-1.18E-05	-4.53E-04	1.53E-08	9.36E-07	2.08E-08	4.38E-13
J	3.75E-15	4.10E-11	-6.24E-13	4.16E-11	3.22E-10	-1.03E-08	2.03E-13	1.66E-11	4.38E-13	1.45E-17

Covariance Matrix for Speaker x3

	A	B	C	D	E	F	G	H	I	J
A	6.45E-11	-3.70E-07	3.59E-07	-7.29E-07	-4.94E-06	-2.41E-04	-7.34E-09	1.77E-08	-2.61E-10	-6.06E-13
B	-3.70E-07	4.40E-03	-4.50E-03	8.90E-03	4.19E-02	1.27E+00	6.17E-05	-1.21E-04	4.07E-06	5.27E-09
C	3.59E-07	-4.50E-03	4.70E-03	-9.20E-03	-4.38E-02	-1.39E+00	-5.39E-05	1.37E-04	-3.99E-06	-5.59E-09
D	-7.29E-07	8.90E-03	-9.20E-03	1.81E-02	8.57E-02	2.66E+00	1.16E-04	-2.58E-04	8.06E-06	1.09E-08
E	-4.94E-06	4.19E-02	-4.38E-02	8.57E-02	5.20E-01	3.01E+01	5.82E-04	-1.50E-03	4.26E-05	7.34E-08
F	-2.41E-04	1.27E+00	-1.39E+00	2.66E+00	3.01E+01	4.03E+03	2.06E-02	-1.95E-02	3.50E-03	6.01E-06
G	-7.34E-09	6.17E-05	-5.39E-05	1.16E-04	5.82E-04	2.06E-02	1.39E-06	-1.23E-06	6.25E-08	7.03E-11
H	1.77E-08	-1.21E-04	1.37E-04	-2.58E-04	-1.50E-03	-1.95E-02	-1.23E-06	8.50E-06	-1.10E-08	-1.44E-10
I	-2.61E-10	4.07E-06	-3.99E-06	8.06E-06	4.26E-05	3.50E-03	6.25E-08	-1.10E-08	6.87E-09	7.43E-12
J	-6.06E-13	5.27E-09	-5.59E-09	1.09E-08	7.34E-08	6.01E-06	7.03E-11	-1.44E-10	7.43E-12	1.19E-14

Covariance Matrix for Speaker x4

	A	B	C	D	E	F	G	H	I	J
A	1.89E-11	5.92E-08	1.26E-07	-6.65E-08	-2.18E-06	-5.65E-05	-9.80E-11	-1.87E-09	2.10E-11	-3.52E-13
B	5.92E-08	1.50E-03	-8.84E-04	2.40E-03	1.35E-02	8.21E-01	5.92E-06	7.15E-05	3.13E-06	1.80E-09
C	1.26E-07	-8.84E-04	2.30E-03	-3.20E-03	-3.60E-02	-8.91E-01	-2.33E-06	-9.11E-05	-3.32E-06	-5.57E-09
D	-6.65E-08	2.40E-03	-3.20E-03	5.60E-03	4.95E-02	1.71E+00	8.24E-06	1.63E-04	6.45E-06	7.37E-09
E	-2.18E-06	1.35E-02	-3.60E-02	4.95E-02	5.77E-01	1.77E+01	6.11E-05	1.40E-03	4.88E-05	8.88E-08
F	-5.65E-05	8.21E-01	-8.91E-01	1.71E+00	1.77E+01	1.72E+03	1.64E-02	5.35E-02	1.10E-03	2.18E-06
G	-9.80E-11	5.92E-06	-2.33E-06	8.24E-06	6.11E-05	1.64E-02	2.53E-07	2.64E-07	-2.92E-09	-1.06E-12
H	-1.87E-09	7.15E-05	-9.11E-05	1.63E-04	1.40E-03	5.35E-02	2.64E-07	4.72E-06	1.86E-07	2.12E-10
I	2.10E-11	3.13E-06	-3.32E-06	6.45E-06	4.88E-05	1.10E-03	-2.92E-09	1.86E-07	8.56E-09	7.65E-12
J	-3.52E-13	1.80E-09	-5.57E-09	7.37E-09	8.88E-08	2.18E-06	-1.06E-12	2.12E-10	7.65E-12	1.41E-14

Appendix 1 is the complete result of the covariance matrix for 106 users. From these tables it can be observed that the correlation between the users differ even for the same feature. In some cases, there are positive correlations while there are negative correlations in some cases. This can be considered as a good result because the behavior of successive features cannot be guessed by merely knowing the behavior of one feature because in all cases they do not move in the same direction.

Similarly, samples of correlations between features are shown in table 3.6.

Table 3.6: Samples of feature correlations

User	AB	AC	AD	AE
x0	-0.5071	0.4535	-0.4807	-0.5641
x1	-0.3404	0.4677	-0.4082	-0.1567
x2	0.8812	0.1564	0.6936	-0.6314
x3	-0.6913	0.6531	-0.6747	-0.8527
x4	0.3471	0.6001	-0.204	-0.6605
x5	0.4287	-0.3327	0.3845	-0.1373
x6	0.8677	-0.4858	0.7316	-0.7624
x8	0.9673	0.2218	0.6613	-0.4719
x9	0.8189	-0.5617	0.8063	0.4396

Using the same legend as in table 3.5, we can observe typical correlation relationships between the features indicated in table 3.6. Additional results of correlation between the features for all the 106 users in the VALID database is attached as appendix 2.

Preliminary investigation of statistical properties of the mean, inter and intra sample variances, the covariance and correlations to determine the useful features indicates that some of the features tested met the criteria in table 3.1 and were considered useful. In addition, some of those tested that did not meet the criteria are as shown in table 3.7. The results shown represent the evaluation of all the 29 features that were measurable and those that are useful based on the set criteria are indicated. The steps detailed in this section yielded the results.

Table 3.7: Summary of features that met and those that failed prescribed criteria of table 3.1based on both databases

	Feature	% subjects with Intra-sample variance value lower compared to inter-sample variance	Distinct mean score (Yes/No)	% Feature correlations with other features (i.e. no. of feature correlations out of the 15 useful features). Correlated features are mainly those within the same domain. The closer to zero, the better	% Feature co-variances with other features
1.	Maximum Power Spectral Density (PSD)	93.4%	Yes	16.67 %	16.67 %
2.	Average Power Spectral Density (PSD)	100%	Yes	16.67 %	16.67 %
3.	Minimum Power Spectral Density (PSD)	100%	Yes	16.67 %	16.67 %
4.	Maximum fft	0%	Yes	16.67 %	16.67 %
5.	Mean fft	0.94%	Yes	16.67 %	16.67 %
6.	Minimum fft	100%	Yes	16.67 %	16.67 %
7.	Maximum Amplitude	75.47 %	Yes	22.2%	22.2%
8.	Peak to Peak Amplitude	50 %	Yes	22.2%	22.2%
9.	Mean Amplitude	100%	Yes	22.2%	22.2%
10.	Minimum Amplitude	72.64%	Yes	22.2%	22.2%
11.	Maximum Cepstrum	0%	Yes	Feature not useful	
12.	Minimum Cepstrum	100%	Yes	11.11%	11.11%
13.	Mean Cepstrum	74.53%	Yes	11.11%	11.11%
14.	Maximum ifft	99.06%	Yes	16.67 %	16.67 %
15.	Minimum ifft	100%	Yes	16.67 %	16.67 %
16.	Mean ifft	100%	Yes	16.67 %	16.67 %
17.	Maximum hilbert function	72.64%	Yes	16.67 %	16.67 %
18.	Minimum hilbert function	97.17%	Yes	16.67 %	16.67 %
19.	Mean hilbert function	96.23%	Yes	16.67 %	16.67 %
20.	Maximum LPCC	0%	Yes	Feature not useful	
21.	Minimum LPCC	0%	Yes	Feature not useful	

22.	Mean LPCC	0%	Yes	Feature not useful	
23.	Log Energy	0%	Yes	Feature not useful	
24.	Maximum Cross Correlation	0%	Yes	Feature not useful	
25.	Minimum Cross Correlation	0%	Yes	Feature not useful	
26.	Mean Cross Correlation	0%	Yes	Feature not useful	
27.	Maximum Auto Correlation	0%	Yes	Feature not useful	
28.	Minimum Auto Correlation	0%	Yes	Feature not useful	
29.	Mean Auto Correlation	0%	Yes	Feature not useful	

Table 3.7 above summarises the average results for the features based on the VALID and the YOHO databases. Some features within the same domain have differing percentage of users that meets the suitability criteria. Average Power Spectral Density (PSD), Minimum Power Spectral Density (PSD), Minimum fft, Mean Amplitude, Minimum Cepstrum, Minimum ifft, and Mean ifft have the highest number of subjects in which the intra-sample variances are lower compared to inter-sample variances. Therefore, they are the most useful features by that criteria. Maximum fft, Maximum Cepstrum, Maximum LPCC, Minimum LPCC, Mean LPCC, Log Energy, Maximum Cross Correlation, Minimum Cross Correlation, Mean Cross Correlation, Maximum Auto Correlation, Minimum Auto Correlation, and Mean Auto Correlation do not have any users in which the feature is useful. It can also be deduced from the table 3.7 that the features within the same domain tend to be correlated and they possess the same percentage of users whose features were correlated.

Figure 3.4 compares the various features, showing the percentage of the number of subjects per feature with low intra sample variances compared to high inter sample variances.

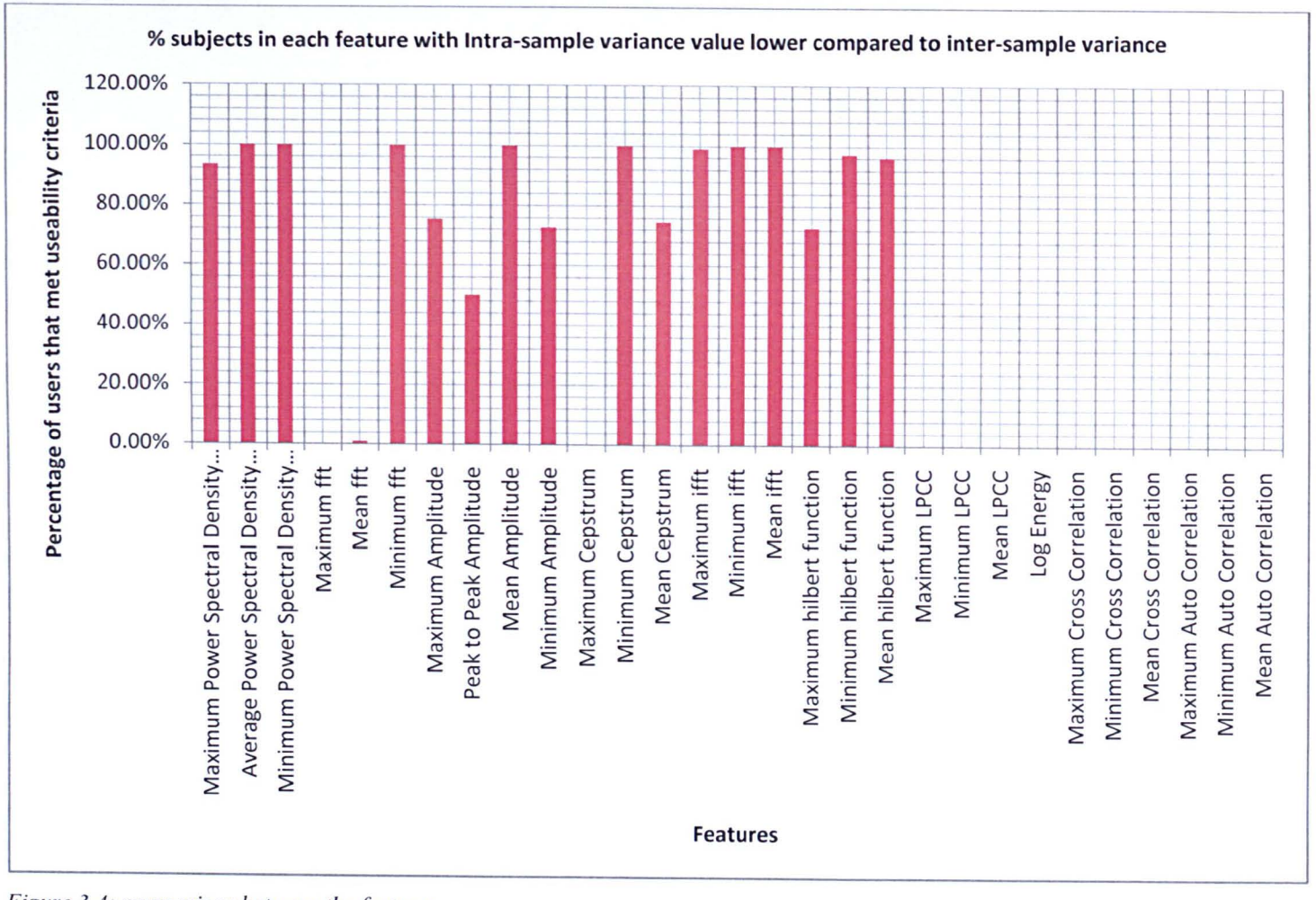

Figure 3.4: comparison between the features

Figure 3.5 also pictorially represent the percentage of feature correlations and co variances with other features.

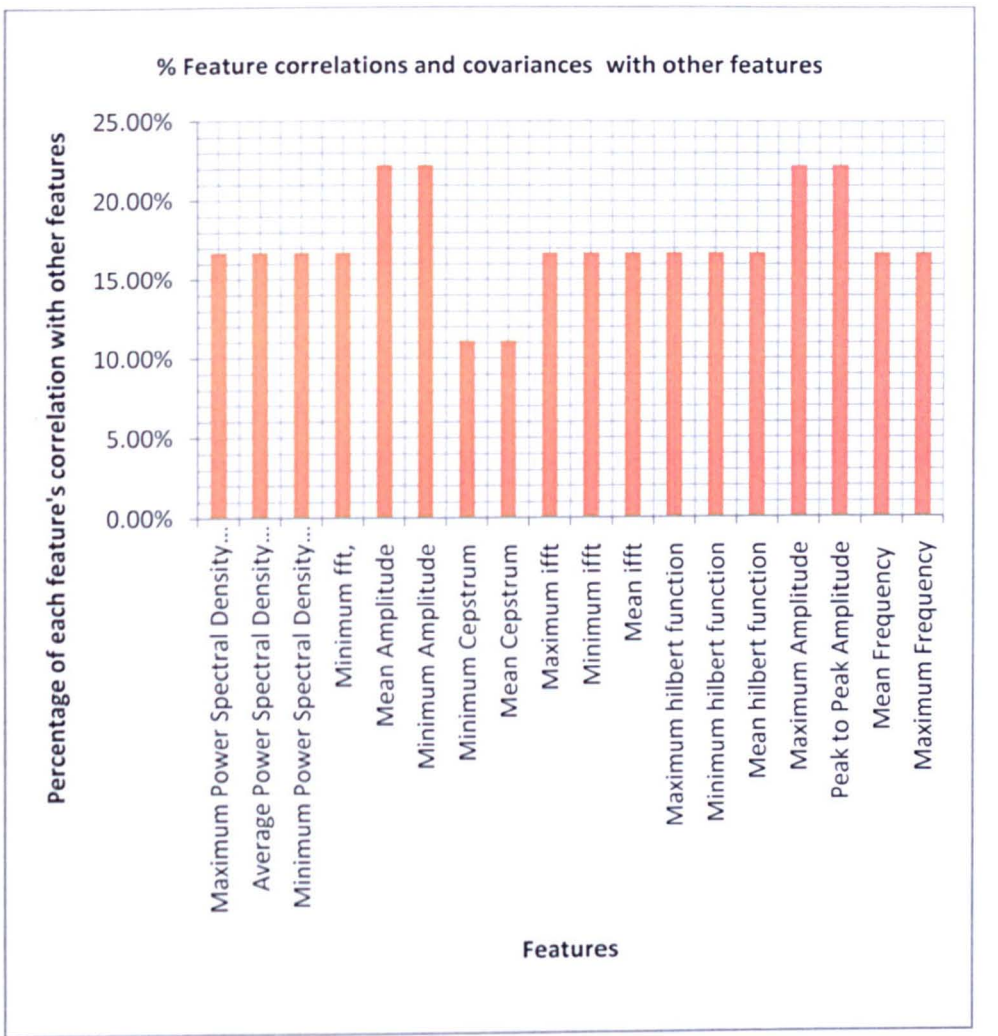

Figure 3.5: comparison between the feature covariance and correlations

It is clear from table 3.7 and figures 3.4 and 3.5 that the features that have proven useful include:

(i) Maximum Power Spectral Density (PSD)
(ii) Average Power Spectral Density (PSD)
(iii) Minimum Power Spectral Density (PSD)
(iv) Minimum fft
(v) Maximum Amplitude
(vi) Mean Amplitude
(vii) Minimum Amplitude
(viii) Minimum Cepstrum
(ix) Mean Cepstrum
(x) Maximum ifft
(xi) Minimum ifft
(xii) Mean ifft
(xiii) Maximum hilbert function
(xiv) Minimum hilbert function
(xv) Mean hilbert function

The evaluated features that did not meet the prescribed criteria include:

(i) Maximum fft
(ii) Mean fft
(iii) Peak to Peak Amplitude
(iv) Maximum Cepstrum
(v) Maximum LPCC
(vi) Minimum LPCC
(vii) Mean LPCC
(viii) Log Energy
(ix) Maximum Cross Correlation
(x) Minimum Cross Correlation
(xi) Mean Cross Correlation
(xii) Maximum Auto Correlation
(xiii) Minimum Auto Correlation
(xiv) Mean Auto Correlation

3.3 Chapter Summary

The chapter reviewed existing features that are commonly extracted and used in current voice based biometrics. The chapter equally explored the suitability of voice features for use in a template-free biometrics and the various characteristics (features) in the human voice which can be used in directly generating encryption keys without having to store the features on a template, which subsequently improves the security of the data protected by it. The distinguishing properties of the candidate voice features are a measure of the various statistical properties outlined (mean, variance, correlation, and covariance), which suggests that for the features to effectively work in a template-free biometric system, they must be distinct in every individual, have less effect of the change of one feature on another and with less probability that a linear relationship exists between two features. The features outlined above meets the stated criteria in table 3.1. The results of the suitability (or otherwise) of the features are tabulated in table 3.7 and are equally listed. These results have shown that the features identified can be theoretically used as a basis for generating template-free biometric keys as will be seen in the next chapter, which looks at the operating principles of template-free biometrics and how voice based keys are generated and reproduced when required, with experimental results shown high performance values.

Voice is one of those recognition traits that humans use on a daily basis to recognise those persons already known to us. Just like face recognition, where we can remotely recognize individuals from their photograph or video, we have the ability of recognising the voice of a loved one (or an enemy) physically or even remotely on a telephone. Voice recognition holds much potential because it is acceptable and it does not require expensive input devices, unlike some other biometrics. It is ideal for many practical and widespread telephony applications, and can even function in the background without forcing the users to go through a separate identification and verification process, saving us from another password to remember. As a result of these advantages, voice is now used in several commercial applications as described in this chapter. However, like

other current biometrics, voice based systems suffer from vulnerabilities associated with templates and has therefore led to the research presented in this report.

Chapter 4

Operating Principles of a Template-free biometrics

The concept of Template-free biometrics has been defined earlier, but in order to understand its basic operating principles and the justification for its operation, it will be helpful to understand the technique of basic cryptographic systems. This chapter will dwell on the core principles of a template-free voice based biometric system and the justification for its operation, as well as report on how encryption keys can be generated from the template-free scheme using voice modality. The evaluation in this chapter is based on the voice features that have been considered useful in chapter 3. The system uses these features to generate keys based on the template-free system to be evaluated in this chapter. To aid the understanding of how the system works, an overview of cryptographic systems has been introduced in the next section. The experimental results show that the system is potentially useful with an accuracy of 65.5% reproducibility of the same users' keys.

4.1 An Overview of Cryptographic systems

Cryptography can be defined as the science of writing in secret code or the conversion of data into scrambled but decipherable codes which can be transmitted across networks or exchanged between several people. It has been in existence for long, with recorded evidence dating back to 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription [96]. There are however modern day uses like diplomatic

communication, war-time battle plans, secret coding, data and telecommunications, ATM cards, computer passwords, electronic commerce, etc [96].

There are basically three types of cryptographic schemes viz: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions. In all cases, the initial unencrypted data is referred to as plaintext. It is this plaintext that is encrypted into ciphertext, and which in turn, is usually decrypted into usable plaintext.

Symmetric Key Cryptography

Symmetric-key cryptography is the encryption methods requiring both the sender and receiver to share the same key [96]. In a symmetric cipher, the sender and the receiver uses the same key for encryption and decryption. This means that the encryption key must be shared between them before any messages can be decrypted. Although symmetric ciphers are significantly faster than asymmetric ciphers, the requirements for key exchange make them difficult to use. The major disadvantage of symmetric key cryptography is the fact that before any two parties can exchange information confidentially, they must agree on a key beforehand [193]. This is usually very difficult, especially in the current internet age. Owing to the inherent difficulty in using symmetric key cryptography, a new method of encryption was developed in the 1970's by Diffie and Hellman called Asymmetric key cryptography [193].

Asymmetric Key Cryptography

Asymmetric cipher is the system in which each person has two keys (i.e. the encryption key and the decryption keys are separate). One key, the public key, is shared publicly while the second key (the private key) is not shared. When a message is sent using asymmetric cryptography, the message is encrypted using the recipient's public key which was previously shared or published. The recipient then decrypts the message using his private key i.e. only the recipient's private key which is known to him/her alone can be used to decrypt the message [96], [193].

The difference between symmetric and asymmetric key cryptography is that Symmetric cryptography uses the same secret (private) key to encrypt and decrypt its data while Asymmetric uses both a public and private key. While symmetric requires that the secret key be known by both the party encrypting the message and the party decrypting the message, Asymmetric allows for the distribution of the public key to the public. Users can then encrypt their message securely and it can only be decoded by the person with the private key. Thus the need to give someone the secret key which can be compromised is avoided.

Hash Functions

A Hash function (also called message digests and one-way encryption) is a transformation that takes in a variable size input and returns a fixed size string that may serve as an index to an array. Unlike in Symmetric and Asymmetric systems, it is an algorithm that uses no key; instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered [96].

This section provides a background to cryptography in order to aid the understanding of the subject of this chapter but is not necessarily the focus of this research. In addition, section 2.7 provides an overview of biometric key generation as a foreword to this chapter. It is important to mention these basic principles before looking at how keys are generated and reproduced in template-free systems for the purpose of encryption and decryption respectively. The next section explains the basic principles of operation of a template-free biometrics.

4.2 Biometric Key Generation and Reproducibility Based on Calibration and Operation Principles

As described earlier, template-free biometric systems operate in two stages-Calibration and Operation. Although still an evolving subject of research there are a number of publications proposing the use of the same two-stage process of calibration and operation [68] - [71], [86] – [88], [97] – [100], [108], [109], [115]. This research pioneered the use of voice based modality in template-free system along with a number of proposed innovations on how the system should operate.

This section describes the detailed technical methods of the calibration and operation in template-free biometrics with specific reference to a voice based system.

4.2.1 Calibration

The initial phase in template-free biometrics is the Calibration phase which begins with the presentation of known biometric samples by the users of the system. Samples could be from voice, fingerprint, iris, etc; however, this research addresses the voice modality. The calibration process is as depicted in Figure 4.1.

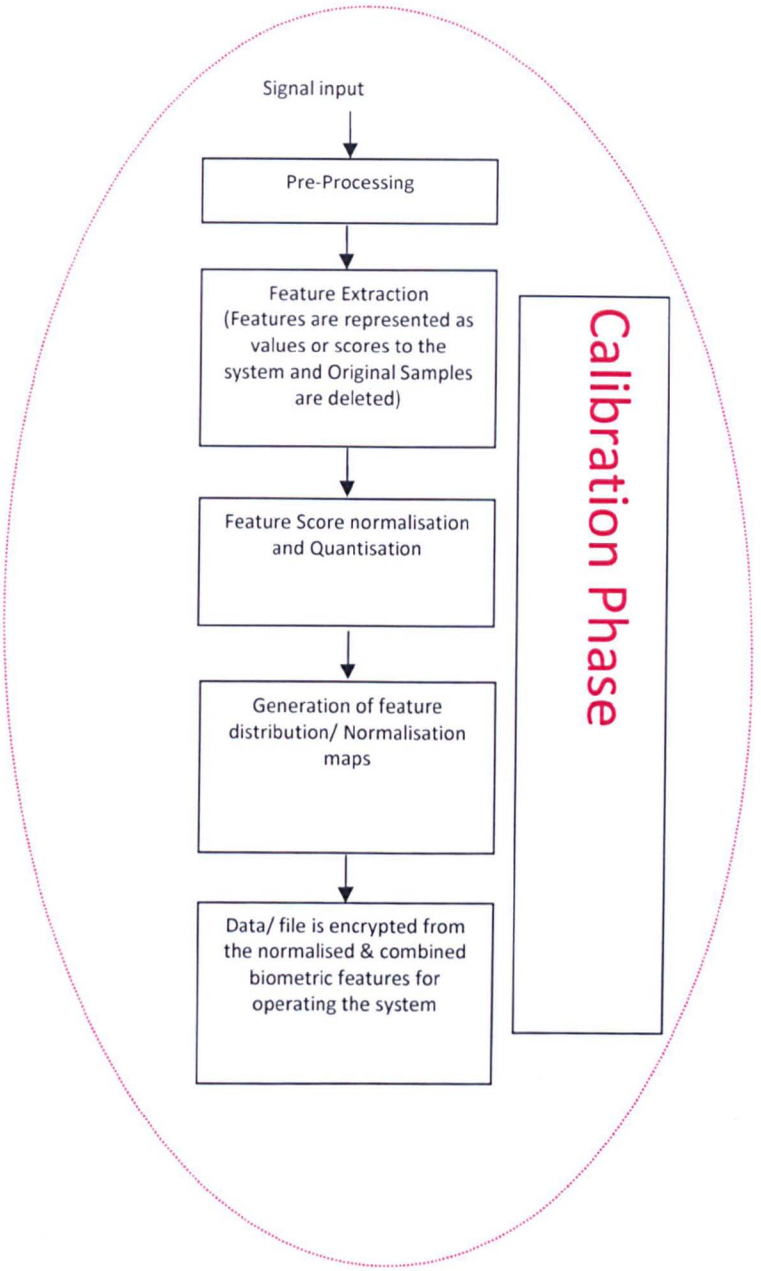

Figure 4.1: Schematic representation of the calibration phase

From the Figure (4.1), it can be shown that the calibration stage consists of six major stages: signal input, pre-processing, feature extraction, normalisation and quantisation, normalisation maps generation, and data encryption. Each of these stages are explained below:

i. Signal input stage

In a voice based system, typical capture device is a standard microphone or a telephone handset. Although the operating parameters differ in some microphones, for experimental purpose those with fixed known parameters are used as the detail technicalities of the operation of the microphone is outside the scope of this research.

ii. Signal pre-processing

As shown, the biometric samples undergo pre-processing (e.g. to determine sampling frequency, the frame etc) and to ensure relative stability/standardisation because of the variances in the capture device. These are standard pre-processing methods used in template-based system and its detailed description may not be relevant in this report.

iii. Feature Extraction

The purpose of feature extraction stage is to extract the features from the speech samples that can uniquely verify the speaker. These are features that met the suitability criteria described in chapter 3. There are several commercially available voice feature extractors. In this research, we used existing Microsoft based 'wave audio format' in combination with the 'wavread' function in Matlab to develop a simple algorithm that extracts features from the human voice.

WAVE or WAV is short for Waveform Audio File Format which is a standard audio file format used for storing an audio bitstream on PCs [92], [191]. A WAV file name has the file extension of '.wav'

In Matlab, the 'WAVREAD' function reads Microsoft WAVE (".wav") sound file using the matlab syntax 'Y=WAVREAD (FILE)' which reads a WAVE file specified by the string FILE, returning the sampled data in Y [188].

Based on the capabilities of the Microsoft Wave file format and the Matlab wavread function, the feature extractor uses standard audio samples from the

VALID and YOHO Databases to generate signals representing feature values which are used for further processing, but discarded later as the system stores no sample values (refer to Figure 4.1 above). The feature extractor accepts pre-processed samples and isolates special characteristics of the human voice which are unique to individuals (also called features) for use in the system. These are extracted and represented in the form of feature scores. The features used in this system were extracted from several samples provided by the same user and the evaluation of those features was presented in chapter 3. The technique of template-free biometrics does not employ the storage of samples; therefore, as soon as the features are extracted, the various samples from which the features were extracted are discarded. These features are taken in form of decimals, making them easier for further manipulation. The manipulations follows the entire calibration procedure described in steps 1 to 8 in the following example to generate feature normalisation maps that are then stored.

iv. Feature score normalization

Normalization is necessary in order to transform the scores of the various features into a single common domain or a common scale [62]. The goal of this is to independently normalize the feature components into the [0,1] range. In this case, normalisation is applied to the feature values of all users within a given feature space in order to reduce the effect of score variability. Some normalisation techniques have been developed as used by Papoutsis et al [97] - [100]. However, these methods were found unusable because they only work well with systems that generate multiple modes, leading to unusual distributions.

The normalisation method employed in this research is one in which for each normalised feature space, the mean and standard deviation for each user are calculated; in this case, we used the min-max normalisation technique since the voice modality to a reasonable extent does not generate unusual distributions (multiple modes). This method can use other existing normalisation schemes to achieve this. They include linear scaling to unit variance or Z-score

normalization, linear scaling to unit range or the min-max normalization, decimal scaling method, median method, transformation to a uniform [0,1] random variable, and rank normalization. Suppose that $x_i = x_1, x_2.....x_n$ is a score to be fused, then each of the normalization technique given as x^1 is described in the equations below:

Min-max method

$$x^1 = \frac{x_i - \max(x_i)}{\max(x_i) - \min(x_i)} \text{ ----------(4.1) [89], [90]}$$

Z-score method

$$x^1 = \frac{x_i - \mu_i}{\sigma_i} \text{ ----------(4.2)}$$

where μ and σ are the mean and the variance respectively [89], [90]

Decimal scaling method

$$x^1 = \frac{x_i}{10^{\log_{10}{}^{\max x_i}}} \text{ .....(4.3) [89]}$$

Median method

$$x^1 = \frac{x_i - median(x_i)}{median(|\, x_i - median(x_i)\,|)} \text{ [89]}$$

The technique adopted in this system takes feature values from the extraction algorithm (as shown in Figure 4.1) and applies the normalisation to each of the extracted value before the samples are deleted. The resultant normalised score is fed into the binarisation algorithm as subsequently described.

v. **Feature Score Binarisation**

The signals content up to the point of generating feature distribution maps in the operation phase, i.e. all the normalised score values are given in decimals.

Binarisation in this case is a process that converts the decimal values into Gray code patterns. It is necessary in order to ensure precision and absolute score stability to the encryption algorithm at every instance of encryption and decryption. In addition, the binarisation process is introduced to convert the probability distribution scores within the quantised intervals into Gray code in order to generate the appropriate key from the feature values to represent the users. Gray code is used because of its single distance code property, which implies that adjacent code words differ by '1' in one digit position only. This property is important because unlike straightforward binary encoding, this avoids the possibility that, when several bits change in the binary representation of a signal, a misread could result from some of the bits changing before others when a requirement of the current system is key stability. Because of this property, the first and last values of the sequence in the signal differ by only one bit.

For the signal to be thus converted to Gray code, the acceptable quantisation intervals used in this case corresponds to the probability distribution values within the range of 10% deviation from the highest probability value (as would be explained subsequently). As part of the design for this system, a section of the algorithm accepts normalised decimal values representing the features and converts them to Gray code as depicted in table 4.1 below:

Table 4.1: Binarisation example

		Max Amplitude			
User Candidate	Sample				
		x	norm(x)	Norm(x) multiplied by a constant	Gray code equivalent of norm (x) multiply a constant
x0	a	0.0712	0.054604	5460361	00000000011110101111100101001101
	b	0.1829	0.309801	30980123	00000001001101001110010000010110
	c	0.1348	0.199909	19990861	00000001101010011000110111101011
	d	0.1205	0.167238	16723783	00000000100000001011100011100100
	e	0.2396	0.439342	43934202	00000011110100010101000100000111
x1	a	0.1133	0.150788	15078821	00000000100101010001111101110111
	b	0.1098	0.142792	14279187	00000000101101010001001100011010
	c	0.1727	0.286498	28649760	00000001011011111101111010110000
	d	0.1644	0.267535	26753484	00000001010101000010010100101010
	e	0.1168	0.158785	15878456	00000000100010110110110110100100
x2	a	0.1885	0.322595	32259539	00000001000110100010001100111010
	b	0.1534	0.242403	24240347	00000001110010010001000010110110
	c	0.1447	0.222527	22252685	00000001111110100100101011001011
	d	0.1464	0.226411	22641078	00000001111101011100010101101101
	e	0.123	0.17295	17294951	00000001100001000001010101010100

Table 4.1 shows the binarisation for a typical feature for 3 users (x0, x1, and x2). Each user produces 5 samples (a,b,c,d, and e) whose score (x) are multiplied by a constant factor (long enough) to eliminate the floating points. This is because Gray codes can not use floating points. Subsequently, the values of samples a,b,c,d, and e, each multiplied by a constant, are converted to the Gray code equivalent. This represents the binarised values. As can be observed from table 4.1, for each user, there is a vertical section where the bits are similar irrespective of the sample. That region represents the unique portion that establishes the portion from which the biometric key can be determined.

The above postulation however needs further strengthening as there are bound to be similarities among users as well as inconsistencies within a user's samples when only one feature is used. Thus, a combination of features is necessary to provide a wide interval from which such uniqueness can be experimentally established. Therefore, a feature combination method that aligns the information from a number of features for the same user is introduced.

vi. Binarised score concatenation

It is required that a long biometric key be generated for each user of the system as the tendency for attack is less with a long key. Therefore, a combination of the bits generated from all the useful features is necessary to generate a very long key which can be used with any of the encryption systems. It therefore means that the length of the key is a function of the number of features used. Feature bits concatenation is a novel method of bit combination introduced in this research. In this case, it is a process of bringing all the feature scores together to form a global bit clusters. As depicted in the table below, F1 to F10 represents the various features while s1 to s5 represents the samples from a particular user.

Table 4.2: Schematic representation of mapped pattern for a typical user

S1	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10
S2	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10
S3	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10
S4	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10
S5	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10

This report proposes that rather than regarding the features as independent components, they are merged along the rows to form a single set of information derivable from the sample 'S'. Thus, table 4.2 above now becomes like the table 4.3 below

Table 4.3: Merged schematic representation of mapped patterns

S1	F1, F2, F2, F3, ...F_n
S2	F1, F2, F2, F3, ...F_n
S3	F1, F2, F2, F3, ...F_n
S4	F1, F2, F2, F3, ...F_n
S5	F1, F2, F2, F3, ...F_n

vii. Setting Quantization intervals and generating Distribution Maps

Quantisation intervals are determined for the users' normalised scores and within this quantised space, the probability distribution function for that users' features are calculated. Two scenarios were employed: quantisation between '0' and '1' at an interval of 0.01 and quantisation between '0' and '100' at an interval of 1. There was no difference in the shape of the distribution curve when plotted on a normal distribution as shown in Figure 4.2. For useful features, the distribution gives a bell shape curve for the users within the quantised interval, but this does not necessarily provide information on the discriminability between users. As a result of this and as shown in Figure 4.3, a plot of the Gaussians for the same feature but from different users shows feature overlaps within the same quantised space.

For each user (x), the signal information is read using the Wavread function described earlier.

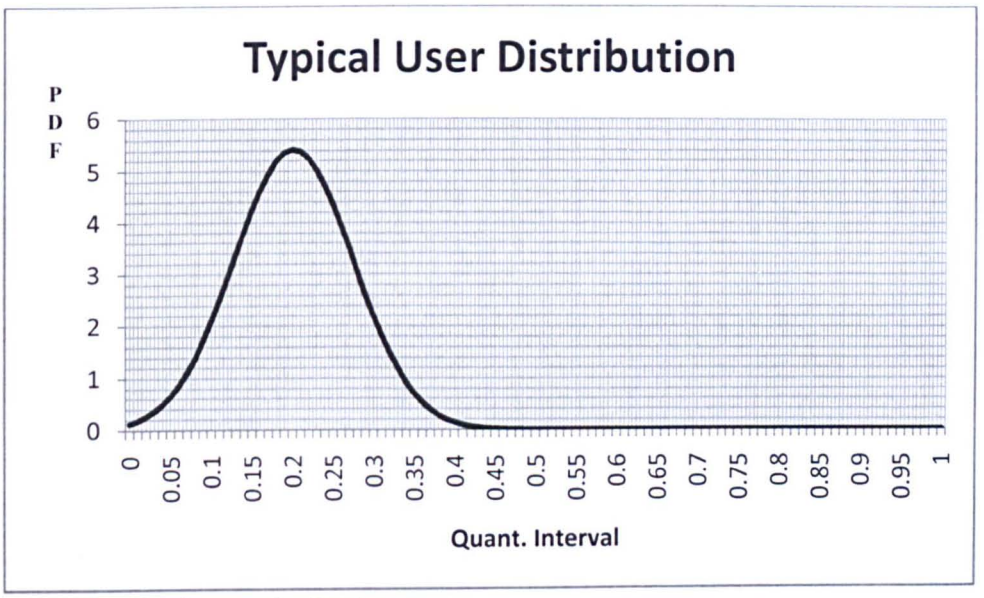

Figure 4.2: Single user distribution map

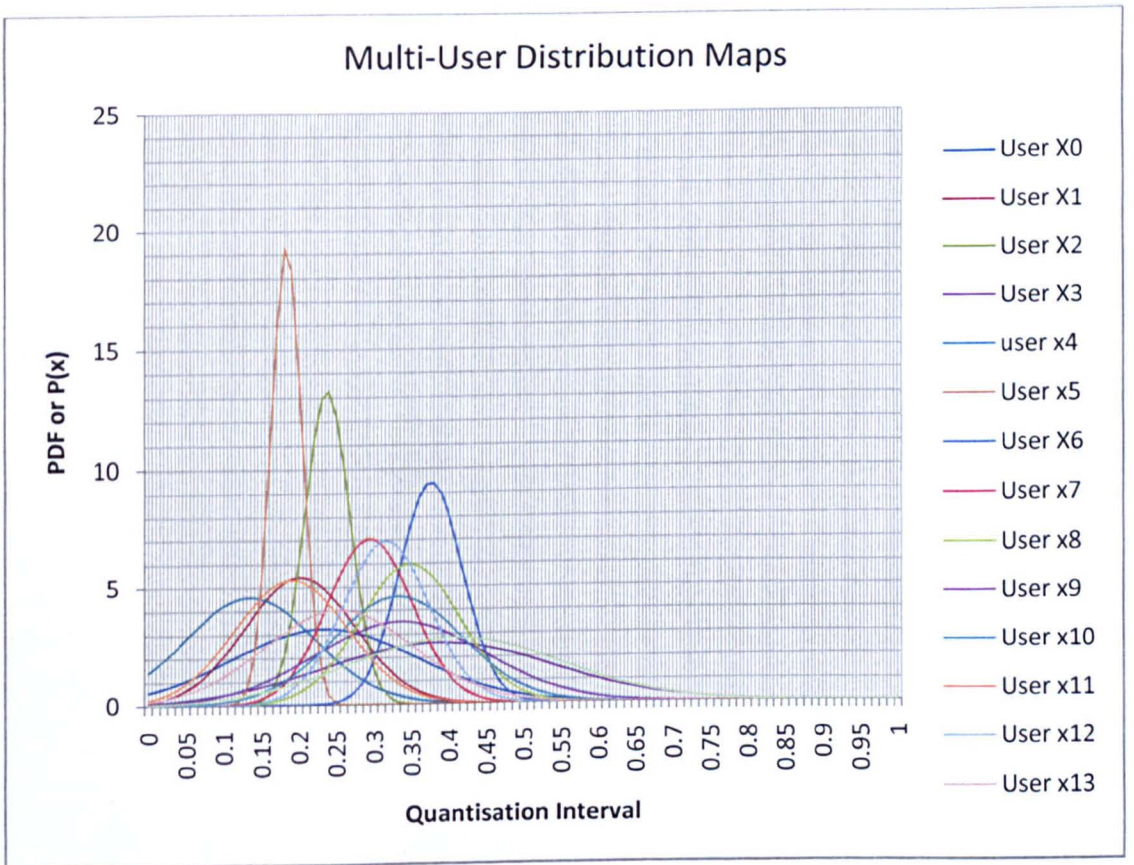

Figure 4.3: Multi users' distribution map showing overlaps

In arriving at this distribution maps, features specific to each user are plotted using the steps outlined below for a typical user calibration:

1. Consider a typical voice feature e.g. average power spectral density denoted by 'x' for a typical user. The min and max sample score values of all users within each feature space are determined.

2. Users' sample values within the feature spaces are normalised, using the min-max normalisation method given by $x^{norm} = \frac{x_i - \min(x_i)}{\max(x_i) - \min(x_i)}$

   where x_i is the individual sample value; $\min(x_i)$ is the smallest value of x in all the users for that feature space, and $\max(x_i)$ is the largest value of x in all the users for that feature space.

3. Calculate the mean (μ) and standard deviation (σ) of the normalised values per user in that feature space.

4. Determine a fixed quantization interval (say between 0 and 1 at an increment of 0.1 or 0.01).

5. For each value in the quantization interval, use the mean μ and standard deviation σ per user calculated in 3 above to determine the normal probability distribution function given by:

$$p(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right),$$

   p(x) provides the probability that the binary bits that is most unique to the user lies within the specific point in the quantisation interval.

6. Plot p(x) against the quantization space as given in Figure 4.3. It should however be noted that there are overlaps in users characteristics increasing the

likelihood of one user's unique information to be similar to that of the others. These overlaps indicate a similarity in the information from the voice samples of various users, however, the peaks in each case differs. Because of these overlaps, the key information contained in each user's feature will be difficult to determine. This research overcame this challenge by not using the entire feature space to generate biometric keys because there will be similarity in any key generated using the entire feature information. Therefore, for the purpose of discriminability, a pre-defined small percentage of the interval from the highest probability value of each user's feature within the quantised space is considered for generating the binary integers used for the biometric keys. From experiments, the limit of pre-defined percentage of the interval from the highest probability is determined from the point at which the unique pattern in the binary integers generated starts to differ. Figure 4.4 shows a fixed interval (k) from the mean within which the specific user biometric keys can be determined. Specifically in this research, the acceptable quantisation intervals used in this case corresponds to the probability distribution values within the range of k= 10% deviation from the highest probability value. Uniqueness of the information and consistency in all users has been found within the region of 10 % deviation from the highest probability as shown in the experiment.

7. Following from step 6, a problem of discriminability is introduced. In order to overcome this, values within the range of an acceptable percentage deviation from the highest probability point are considered most useful for generating the encryption keys for the user from that particular feature.

8. The p(x) values from the acceptable region around the highest probability are further converted into Gray code to provide more specific information needed to build the key in the operation phase.

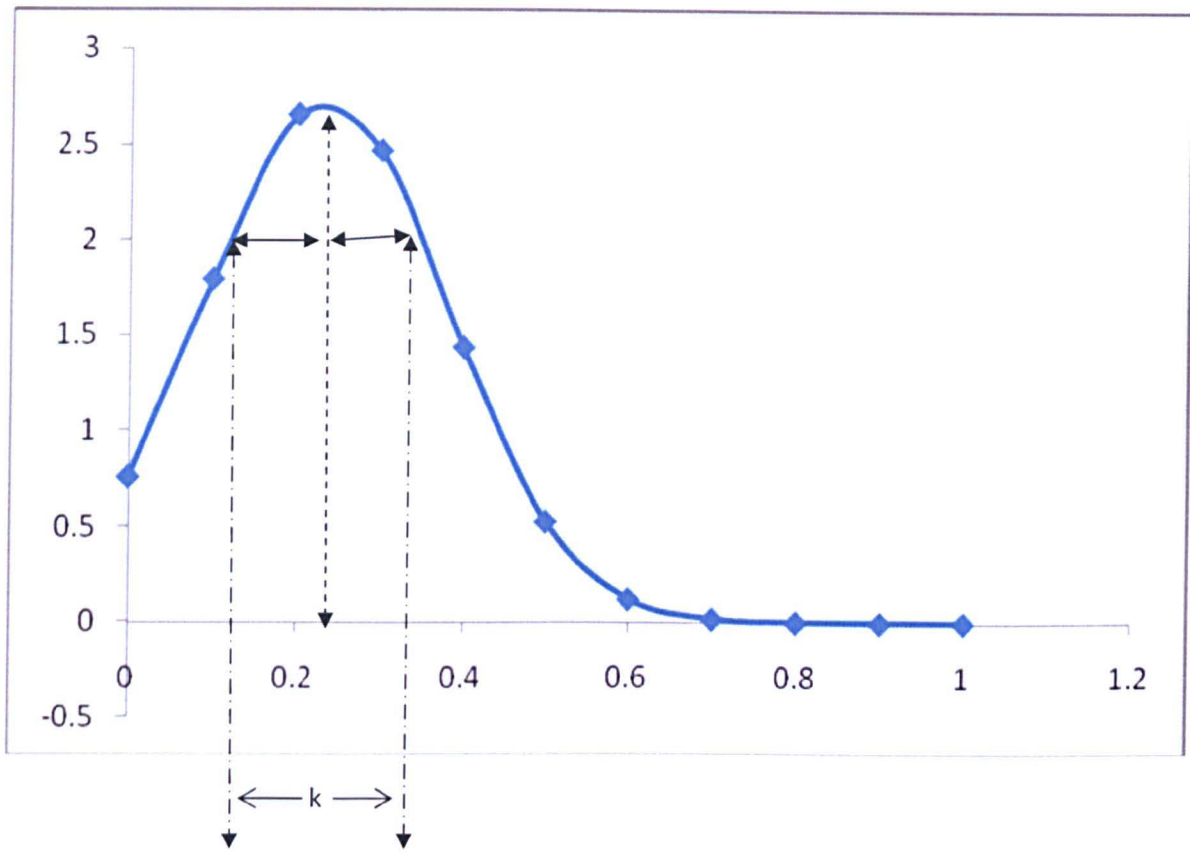

Figure 4.4: Specific user key generation interval

At this stage, the feature distribution maps are stored and calibration process will not be repeated again. It should however be noted that the maps are a completely transformed representation of the users' information obtained directly from the biometric samples which would have been deleted and it is unlike templates from which privacy information can be deduced when the template is compromised.

4.2.2 Operation

The Operation phase is shown in Figure 4.5. The signal pre-processing and feature extraction stage in the operation phase is the same as in the calibration phase. But unlike the Calibration phase which is employed once, the operation phase is employed at each instance that an encryption key is required. Actual biometric keys are generated and reproduced when required by the operation phase and for every instance of key generation, the information obtained from the allowable percentage of deviation from the highest probability as described in step 7 in the example above is converted into binary form.

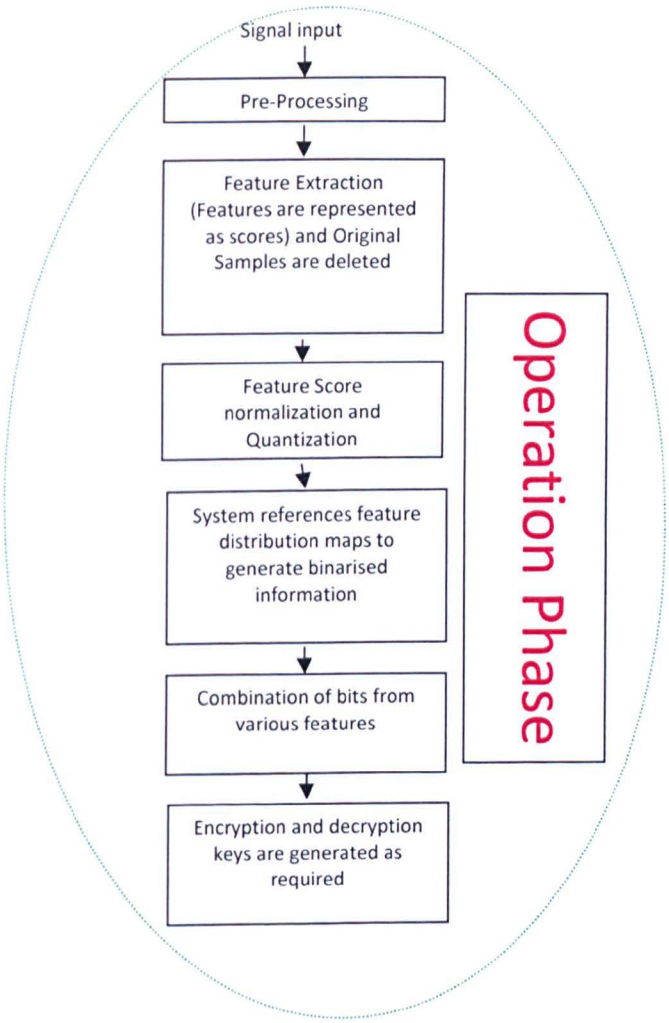

Figure 4.5: Schematic representation of the Operation phase

4.2.2.1 Key Generation

Keys are determined from the region where the bits are equal in all the samples from a particular user. In addition to the actual bits that are generated as keys from concatenated feature spaces, the position(s) at which the stable bits occur holds very useful information from which additional bits serving as keys can be generated. As these keys are the same every time samples from the same candidate are taken, key generation could be based on bits position value or signal pattern that emerges, but a combination of the position and signal pattern as well as the distance between these position (if there are more than one) can effectively generate a very long biometric key that is almost infallible. The signal pattern in this case is the uniform value that is produced when several samples from the user are aligned as illustrated below:

00011100010 for sample 1
00011100010 for sample 2
00011100010 for sample 3

From the above, we can say that the signal pattern is 00011100010

To further illustrate key generation, consider tables 4.4a, 4.4b, and 4.4c below formed from a single feature space (using maximum amplitude).

Table 4.4a: Illustration of signal pattern

Information from a typical feature space
00001000001010011111101010101101
00001001111110011111110101010011
00001111111110100000100111011110
00001100110010111010000011100101

Each row in table 4.4a is formed from samples from the same user used to generate information representing the same feature. For ease of understanding, we separated each column as depicted in tables 4.4b below.

Table 4.4 b: Illustration of signal pattern

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	0	0	0	1	0	0	0	0	0	1	0	1	0	0	1
0	0	0	0	1	0	0	1	1	1	1	1	1	0	0	1
0	0	0	0	1	1	1	1	1	1	1	1	1	0	1	0
0	0	0	0	1	1	0	0	1	1	0	0	1	0	1	1

Table 4.4 b continued

17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	1	1	1	1	0	1	0	1	0	1	0	1	1	0	1
1	1	1	1	1	1	0	1	0	1	0	1	0	0	1	1
0	0	0	0	1	0	0	1	1	1	0	1	1	1	1	0
1	0	1	0	0	0	0	0	1	1	1	0	0	1	0	1

Following the procedure outlined above, for this user, this feature produces absolute stable bits at column numbers 1,2,3,4,5,13,14. This research also considered regions with most probable bit uniformity. In this case for three or more stable bits, we assume that the bits in that region are stable. Therefore, column numbers 7, 9, 11, 16, 17, 19, 21, 23, 25, 26 are equally considered in the key generation. For a typical user denoted by X_0 within a given feature space, the biometric key generation process provides information as below:

From the table, information for biometric key generation is in three ways:

(1) The first way to obtain the biometric key is to use the information derived from the region of stable signal pattern =00001-0-111-1-0-111--1001---1-1.

(2) The second way to obtain the biometric key for the same user within the same feature space will be to use the information derived from the value of the column number within the table which in this case is =1,2,3,4,5, 7, 9, 11, 13,14, 16, 17, 19, 21, 23, 25, 26, The binary equivalent of these position values are represented below:

Table 4.5 a: binary equivalent of the position at which equality occurs

1	2	3
0 0 0 0 0 1	0 0 0 0 1 1	0 0 0 0 1 0

Table 4.5 b

4	5	7
0 0 0 1 1 0	0 0 0 1 1 1	0 0 0 1 0 0

Table 4.5 c

9	11	13
0 0 1 1 0 1	0 0 1 1 1 0	0 0 1 0 1 1

Table 4.5 d

14	16	17
0 0 1 0 0 1	0 1 1 0 0 0	0 1 1 0 0 1

Table 4.5 e

19	21	23
0 1 1 0 1 0	01 11 1 1	0 1 1 1 0 0

Table 4.5 f

25	26
0 1 0 1 0 1	0 1 0 1 1 1

(3) The third way to generate the biometric key will be to use the difference between the values of these positions and in this case, it is given as: 2-1=1; 3-2=1; 4-3=1; 5-4=1; 7-5=2; 9-7=2; 11-9=2; 13-11=2; ,14-13=1; 16-14=2; 17-16=1; 19-17=2; 21-19=2; 23-21=3; 25-23=2; and 26-25=1. This translates to the values: 1,1,1,1,2,2,2,2,1,2,1,2,2,3,2,1 which represent key information.

A further combination of the first, second and third methods of generating the biometric keys described above will increase the number of bits that can be used to build the key and thus strengthen the key representing the user within that feature space. When all the keys so generated from other feature spaces are combined through concatenation, then a single user's biometric key which can be considered as long and stable is generated. The length of the key as proposed here is relative as it is dependent on the number of

features employed. However, stability is not affected as the unused bits outside the allowable percentage from the mean are discarded.

As users must always present their samples every time a key is required, none of the candidate's samples will be recorded. Thus the key that is used for the system are reproduced at every instance of operation, but neither this key nor the samples from which they are derived are stored on any form of template.

4.3 Key combination Method (bit concatenation)

For each user, the keys generated are mostly stable within the region of 10% deviation of the highest probability distribution function within a defined quantisation interval. As discussed in Section 4.1.1, the keys begin to degenerate when bits beyond this range is considered. As a result, the information used to generate the key is more precise but shorter per feature space. Therefore, it is required that as many features as possible be combined to produce a single long key. A novel key combination method (bits Concatenation) was introduced in this research. This follows the same method as in item vi in section 4.2.1 Concatenating the bits from the entire feature space produces a long biometric key. As in the first cycle of the operation phase, in order to generate a long key size, this system considers additional novel ways of building the keys based on a combination of the position and signal values as well as the distances between these positions.

It should be noted that individually, these feature information represents some measure of unique identification. However, as the number of bits produced individually is not very long, the features are combined such that a longer key length can be achieved. The specific advantage of this method of combination includes:

- It yields a longer bit size for the unique representation of the individual
- It forms the basis for randomisation revocation strategy as detailed in chapter 6

- It makes it easier to for the designer to exclude a block of data from a particular feature in cases where the accuracy of the system is affected by any of the feature in use.

4.4 Key reproducibility

Key reproducibility is necessary to ensure that keys are correctly regenerated in the operation phase. It happens when the system further references the feature distribution maps to generate the bits used as biometric keys that represent individual users. The key is then used to encrypt message/ data. For the purpose of decrypting the system, the same process is followed and a new key is generated from previously unseen samples provided by the user. The key generated at this stage forms the basis for decrypting the information.

4.5 Key stability analysis and Performance evaluation

Key stability analysis is carried out to justify the utility of the system. Based on the proposed system, samples from the YOHO speaker verification database [95] was used. There are 138 users (108 males, 30 females) in the database which was collected over a period of three months with a total of 1932 validated sessions.

Samples from a total of 100 users were investigated to establish the consistency in the key from the points of stable bits between various samples of a particular user. The performance evaluation looks more at the number of times a key can be reproduced correctly from the 40 samples per speaker in the test sessions rather than an evaluation against template-based system.

4.6 Evaluating the percentage of success

Consider one feature (in this case maximum amplitude) generated from 10 sets of samples (with a set containing four samples each) from a user. We evaluated the robustness of the key by first normalizing each feature score (a total of 40 scores, with each set of samples comprising of 4 normalised scores). Each score is binarised and values are concatenated. We then evaluated the points in sets 1 to 10 where the number of bits is equal. The experiment shows that each user's bits in the features considered useful have a very high chance of being equal. We further considered each column to see the number of sets where within the same position value (or column number) there are less than 3 out of 4 chances that the bits are equal. Using the columns in which there are predominantly 3 and above chances of bits equality, in some of the features there is at least 96% probability that the system will correctly recognise the user. Using this level of established accuracy this evaluation was repeated for one hundred user samples yielding key reproducibility accuracy for all users between 40.62% in the features with least suitability and 93.75% in the features with most accuracy.

4.7 Strength of the biometric key

Using this system, the strength of the biometric is a function of the number of features and combinations used. Combination in this case refers to the position value and distances between positions as described earlier. A substantial length of key can be achieved using at least two features. As indicated in the experiment, combination of bits from 13 different features yielded an average accuracy of 65.55%. As more features are concatenated, the length of the key increases.

4.8 Performance Evaluation against other voice based biometric systems

Several researches on speaker verification or voice biometric systems are available in literature [80], [101] - [103]. These are all template-based systems which are associated with template related compromises. This system generally has eliminated administrative compromises like template modification, and cloning, improved on the integrity of the enrolment process, reducing compromises due to collusion at enrolment, forced enrolment, and abuse of exception processes. It has also improvement on intrinsic errors which normally lead to false accept and false reject. The focus of this research is not a direct comparison of the performance against template-based system, but rather to show that having eliminated the need for templates and its associated vulnerabilities, this biometric system still possesses a high level of accuracy that can increase users' confidence.

4.9 Experimental Evaluation and testing of Key Generation and key Stability

Following from chapter 3 (table 3.7 and Figures 3.5 and 3.6), a number of features have been theoretically established as useful, haven met the set criteria for a useful feature in table 3.1. The summary of the result indicates that the following features are useful in the context of this research.

(i) Maximum Power Spectral Density (PSD)
(ii) Average Power Spectral Density (PSD)
(iii) Minimum Power Spectral Density (PSD)
(iv) Minimum fft
(v) Maximum Amplitude
(vi) Mean Amplitude
(vii) Minimum Amplitude

(viii) Minimum Cepstrum
(ix) Mean Cepstrum
(x) Maximum ifft
(xi) Minimum ifft
(xii) Mean ifft
(xiii) Maximum hilbert function
(xiv) Minimum hilbert function
(xv) Mean hilbert function

The evaluated features that did not meet the prescribed criteria include:
(i) Maximum fft
(ii) Mean fft
(iii) Peak to Peak Amplitude
(iv) Maximum Cepstrum
(v) Maximum LPCC
(vi) Minimum LPCC
(vii) Mean LPCC
(viii) Log Energy
(ix) Maximum Cross Correlation
(x) Minimum Cross Correlation
(xi) Mean Cross Correlation
(xii) Maximum Auto Correlation
(xiii) Minimum Auto Correlation
(xiv) Mean Auto Correlation

Consequently, subsequent evaluation in this chapter is based on the features that are listed as useful.

4.9.1 Datasets and tests

The experiments were carried out on two main databases- the VALID Datasets and the YOHO Datasets described in chapter 3. In both databases, the identity, ethnicity, or other specific information about the subjects were not disclosed, rather a broad mention of the diversities like the number of males and females, the different backgrounds under recording (noisy, real world, office scenario etc), the period over which data was collected are the information available. Therefore, the results reported did not include details about the identity of the subjects involved, hence the subjects were labelled as X0, X1,.....Xn where X0 represent User 1, X1= User2, and so on. It should be noted that User 1 in VALID Database is not the same as User 1 in the YOHO Database and in each case, the database from which results were obtained has been stated in the experiment section.

The Calibration and Operation tests were carried out using voice features that show some promise in terms of stability and suitability as indicated in chapter 3 and in previous publications [62], [86] – [88], [108], [109], [115]. This follows the steps in the example procedure outlined in section 4.2.1 to generate normalisation maps from the features. For each dataset, the maximum and minimum values were calculated and for each user within the system, the normalised values [norm (x)] are used to calculate the mean and standard deviation per user as shown in table 4.6.

Table 4.6: Example normalisation table as obtained from the VALID Database

		Max Amplitude	
User Candidate	Sample		
		X	norm(x)
x0	a	0.0712	0.054604
	b	0.1829	0.309801
	c	0.1348	0.199909
	d	0.1205	0.167238
	e	0.2396	0.439342
		Mean	0.234179
		Standard deviation	0.146384
		Variance	0.021428
x1	a	0.1133	0.150788
	b	0.1098	0.142792
	c	0.1727	0.286498
	d	0.1644	0.267535
	e	0.1168	0.158785
		Mean	0.201279
		Standard deviation	0.069692
		Variance	0.004857

These normalised values are used to determine the probability values at each point in the quantisation interval per user as detailed in 4.2.1.

A typical user distribution table and graph are in table 4.7 and Figure 4.6 respectively. They are formed from the probabilities at each point in the quantization interval between 0 and 1 using the mean and standard deviation of the normalized values of each user as shown in table 4.7.

Table 4.7: Typical user distribution table as obtained from the VALID Database

Quantization Interval	Normal PDF
0	0.128575
0.1	2.102475
0.2	5.421213
0.3	2.204202
0.4	0.141318
0.5	0.001429
0.6	2.28E-06
0.7	5.72E-10
0.8	2.27E-14
0.9	1.42E-19
1	1.4E-25

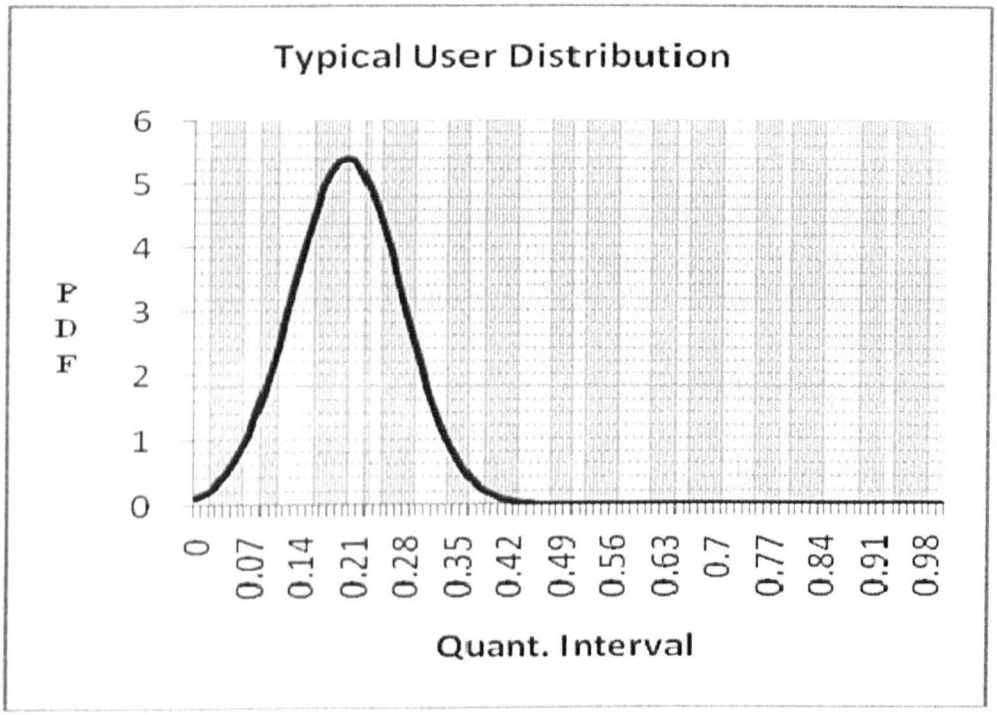

Figure 4.6: Typical user distribution graph

The experiment on 106 users in the VALID database generates unique biometric keys representing the users. The subjects in the VALID database were taken through the outlined procedure in section 4.2.1 to evaluate the codes obtained and in order to ascertain the region within the distribution curve that presents some level of consistency

in the codes. The results for each of the features evaluated are indicated in table 4.8 below.

Table 4.8: Percentage of consistent bits for the subjects in VALID database

Feature	Number of subjects evaluated	Percentage of consistent pattern in the bits from the various samples for the evaluated subjects
Minimum Amplitude	6	20
Mean Amplitude	6	10
Mean Frequency	6	8
Minimum Frequency	6	10
Maximum Frequency	6	8
Minimum PSD	6	10
Mean PSD	6	10
Maximum PSD	6	10
Peak to peak Amplitude	6	10

For the features that are useful, the best results are obtained within the 10% deviation from the highest probability value and consistency in the codes (i.e. its ability to be reproduced correctly) is high. It should be noted that only a few subjects and features were evaluated because a random evaluation of other subjects indicate that it is safe to keep to the 10% range because the data obtained generally becomes inconsistent beyond this range. However, future work may consider additional evaluations. Thus, for all probability values within the quantisation interval in the distribution, values beyond 10% interval from the highest probability are not consistent when binarisation is applied and are therefore not considered useful in generating the keys.

4.9.2 Analysis of Key stability based on the YOHO Database

A typical consistency in the key as established from the points of stable bits between the subjects in the YOHO samples is shown in table 4.9. Since the investigation is studying the feasibility of template-free biometrics, we used only the test sessions in the YOHO database which contains 10 test sessions per subject with 4 phrases per session making a total of 40 samples per speaker in all the 138 subjects. The aim is to reproduce the same biometric key from each sample without referencing any stored template; therefore we disregarded the enrolment sessions. The performance evaluation is not an evaluation against template-based system, but the number of times a key can be reproduced correctly from the 40 samples per speaker in the test sessions.

Table 4.9 contains 16 samples per user and it indicates the consistency in the bits generated from a number of samples belonging to the same user. In these results, the level of consistency in the bits occurs in over 80 % of the bits in the samples and the region of consistency can safely be used to represent the users. It is also noted that the keys generated based on the bits within these region of consistency differs between users as indicated in the bits from user 1 and 2 for example.

Table 4.9: key generation sessions showing consistency in keys from various samples of the same user in YOHO Database.

USER 1

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
S1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	0	1	1	1	1	1	1
S2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1	1	0	0	1	0	1	1	1
S3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1	1	1	0	1	0	1	1	1
S4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1	1	0	0	0	1	1	1	0
S5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	1	1	1	0	0	1	1
S6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	1	0	0	1	0	0	0
S7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	1	1	1	0	1	0	0
S8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	0	1	0	1	1	0	1
S9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1	1	0	1	1	1	0	0	0
S10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1	1	0	0	1	1	1	1	0
S11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1	1	0	1	1	0	1	1	0
S12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	1	0	0	0	1	1	1
S13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1	1	0	1	0	1	0	0	1
S14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	1	1	1	0	1	1	1
S15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1	1	0	0	1	1	0	1	0
S16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	1	1	0	1	1	1	0

Stable bit in User 1 feature 1 = 00000000000000000100 1111
Percentage of bits stable in User 1 feature 1 =80.65%

USER 2

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
S1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	1	0	0	0
S2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	1	1	0	0	0	1
S3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	1	1	1	0
S4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	1	0	1	1
S5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	1	1	0	1
S6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	1	0	1	0
S7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	1	0	0	1
S8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	1	0	1	1
S9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	1	0
S10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	1	0	1	0
S11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	1	1	0	1
S12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0
S13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	1	0	0	0
S14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	0	1	0	0
S15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	0	1	0	1
S16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	1	1	0	0	1	0

bit in User 2 feature 1 = 00000000000000000000011100
Percentage of bits stable in User 2 feature 1 =83.87%

Table 4.9 above is an analysis of key stability for various users using different features. Using all the methods outlined in this chapter, each sample produces 32 separate bits which can be separated in a table as shown above. The essence of representing them in a table is to enable all equivalent bits to be neatly arranged in a column. It can be observed (as shown in the shaded portions) that there is consistency within a large portion of the table, indicating that irrespective of the sample there is some form of consistency within a user's information and this can largely be reproduced correctly when the same user's sample is repeatedly collected. This result however differs between samples i.e. the percentage of consistency or stability in the shaded portion.

Following the pattern in table 4.9, 13 features were evaluated for 138 subjects in the YOHO Database with the following results.

Table 4.10: percentage of stable bits in each feature for subjects in YOHO Database

Feature	**Percentage of stable bits**
Maximum Amplitude	70.96%
Average Amplitude	93.75%
Minimum Amplitude	71.87%
Peak to peak Amplitude	68.75%
Maximum Frequency	43.75%
Minimum Frequency	40.62%
Mean Frequency	62.5%
Maximum PSD	84.37%
Mean PSD	46.87%
Minimum PSD	87.5%
Maximum Hilbert	68.75%
Mean Hilbert	90.62%
Minimum Hilbert function	87.5%

Table 4.11: Overall results for the features and subjects *in YOHO Database*

Average percentage of bit contribution from 13 features	65.55%
Average percentage of stable bits for 138 subjects in 13 features	62%

The results shows the percentage of the stable bits contributed by each feature for each user and the average result in a situation where key generation is based on the 13

features. Mean amplitude and mean Hilbert have the highest percentage of stability while maximum frequency is the least stable. The overall average for the 13 features is 65.55%.

4.9.3 Discriminability Analysis

Discriminability in this case is determined from the value of each bit at a particular position. Following from table 4.9, the bits for user 1 changed at column 19 and changed again in column 20 and then 22. For user 2, the bits changed at columns 22 and 25. When plotted on a graph, the positions of these bit changes can be well appreciated as below.

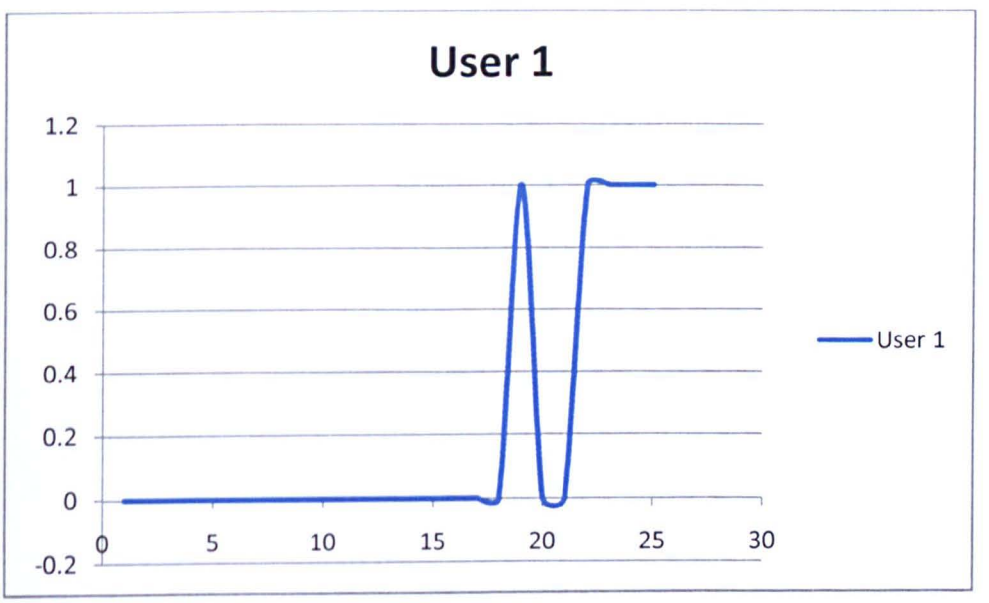

Figure 4.7.: Pattern of change between 0 and 1 in the bits for user 1in YOHO Database

Figure 4.8: pattern of change between 0 and 1 in the bits for user 2 in YOHO Database

With similar changes occurring in all the thirteen features, discriminability can be determined from (i) the values of these bits (ii) the positions at which the changes occur, and (iii) the difference between the positions as described in the operation phase in section 4.2.2.

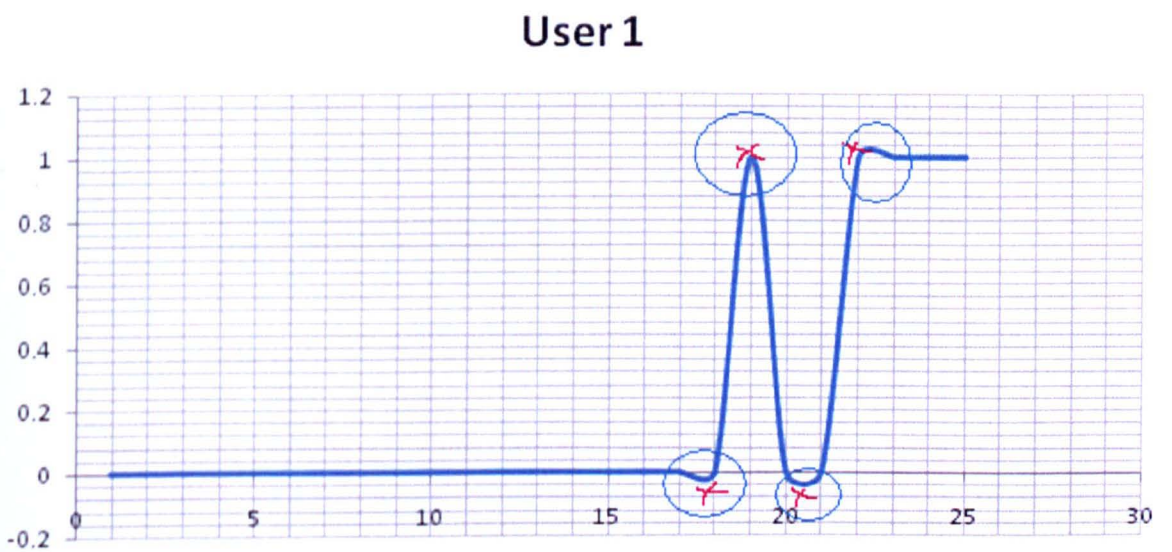

Figure 4.9: The positions at which the bits changes for user 1 in YOHO Database

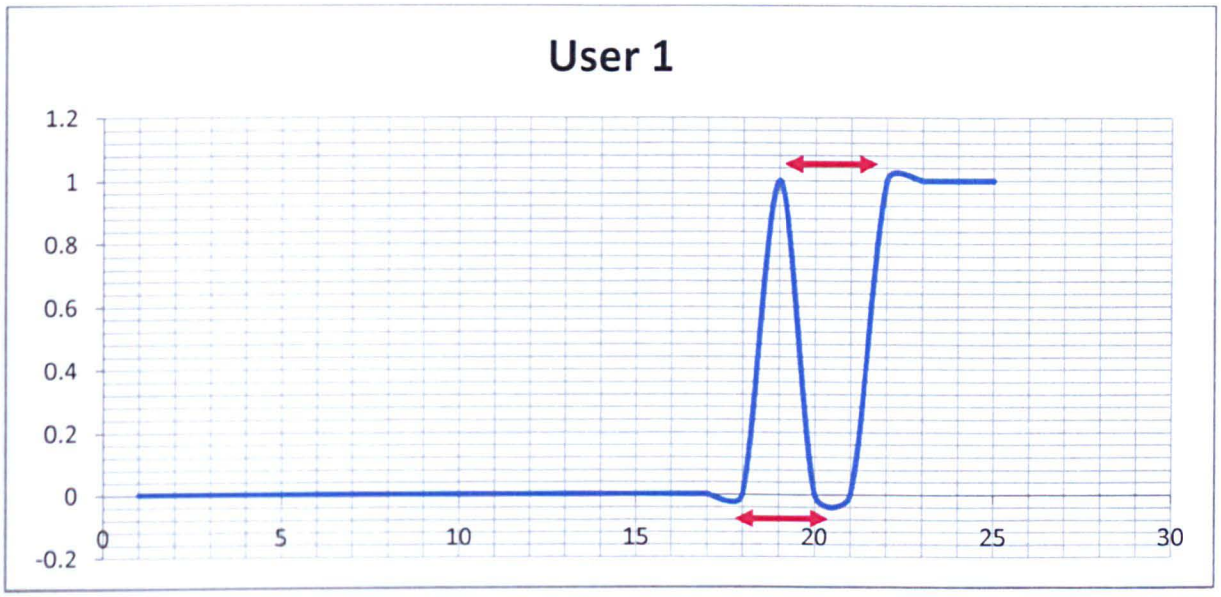

Figure 4.10: Distances between the positions at which the bits changes for user 1 in YOHO Database

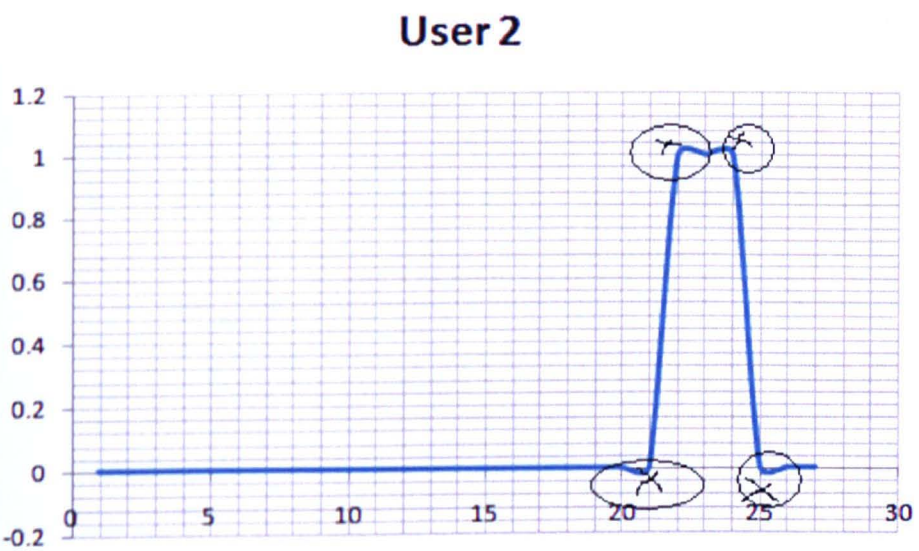

Figure 4.11: The positions at which the bits changes for user 2 in YOHO Database

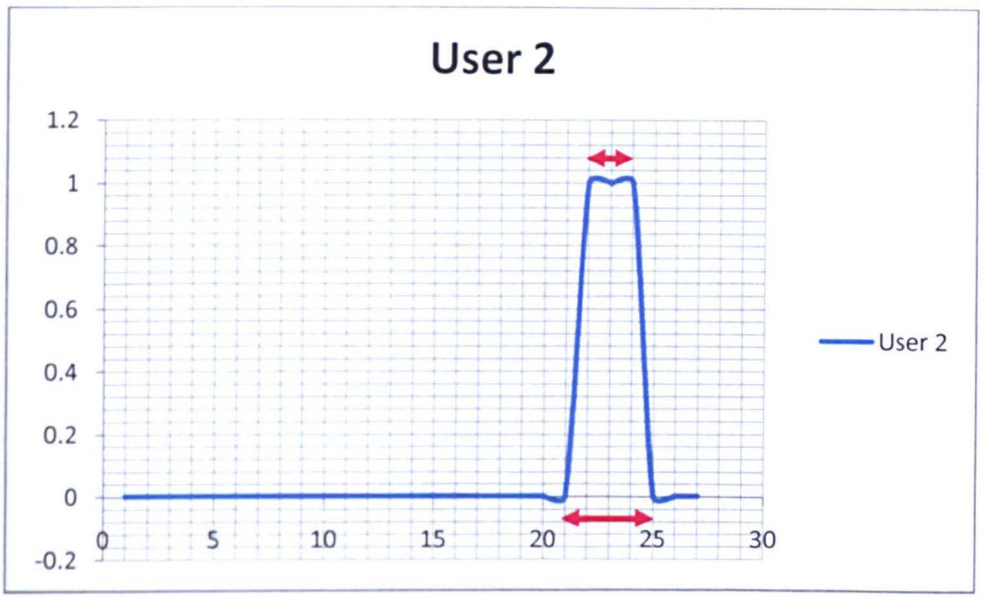

Figure 4.12: Distances between the positions at which the bits changes for user 2 in YOHO Database

From the results for the 13 features in section 4.9.2 above, the positions of bit changes for each feature is indicated in the result below.

Table 4.12: Number of bit changes in each feature for subjects in YOHO Database

Feature	**Column at which bits change**
Maximum Amplitude	23
Average Amplitude	25, 27, 28, 31
Minimum Amplitude	24 and 25
Peak to peak Amplitude	22 and 24
Maximum Frequency	15
Minimum Frequency	14
Mean Frequency	20
Maximum PSD	28
Mean PSD	16
Minimum PSD	29
Maximum Hilbert	23
Mean Hilbert	30
Minimum Hilbert function	28

The concatenation of the thirteen features yielded 18 bit changes, making it robust for individual distinction. This is based on the assumption that in all key generation procedures, there will be up to or close to these number of bit changes which, in

addition to considering the positions at which these changes occur, can form the elements of distinction between the subjects.

In all cases the key is found within the columns where the bits from the samples are equal as shown in table 4.9. This was repeated for 138 subjects in the YOHO database. The results shows that for each feature, the bit changes are consistent for each subject, thus the key is stable within the shaded region but the accuracy of this key as analysed is 93.75% in average amplitude which is the feature with the highest region of stable bits, while it is 40.62% in the feature (Minimum frequency) with the lowest region of stability

This is an improvement over other speaker verification experiments using the same database [40], [80], [101], [107], [120], [121] which are all associated with template-based compromise.

Table 4.13 compares the result of this research to that of other template free systems (non voice based) evaluated so far to the best of our knowledge. These are based on fingerprint and ICMetrics.

Table 4.13: Comparison with results obtained from other template-free systems

Paper reference	Result summary
ICMetrics by Papoutsis [131]	By applying addition combination technique and considering the case at which ICMetrics work with unseen devices, the produced key was 35-bit long with its stability varying from 55.6% to 92.6% depending on the number of samples used (5 and 1000 respectively). By applying concatenation combination technique and considering the case at which ICMetrics work with unseen devices, the produced key's stability varying from 23% to 77% depending on the number of samples used (5 and 1000 respectively).
Fingerprint by harmer [130]	Template free keys reproduced correctly ~80% of the time with 55% unique keys in the resultant key-space
This system (Voice based)	93.75 % in best case; 65.55% average in 13 features

It is expected that future studies will evaluate other modalities like palm print, gait, iris, etc and compare with these results.

4.10 Chapter Summary

This chapter describes the processes involved in Template-free biometrics which are grouped into two broad stages: the Calibration and the Operation stages. The initial Calibration stage is carried out once to build normalisation maps while the Operation phase is carried out whenever encryption keys are required. The chapter shows vividly, examples on the proposed algorithm for template-free biometric systems and demonstrates how key generation takes place in the operation phase at high accuracy (> 65.55% accuracy). Since in this process, raw biometric data are not stored, but keys are directly encrypted from the biometric data provided by the individual, this technique eliminates the need for storing templates and thus increases the security, and in turn user's confidence, in biometric systems. This result was evaluated against other template-based systems as well as the research so far on template-free systems using other biometric modes.

Although template-based compromises have been addressed by this system, concerns about other vulnerable points in biometric systems still exist. In order to ensure that these other vulnerable points do not significantly degrade the performance of this system, we further investigated the revocability of the keys based on template-free systems in the subsequent chapter.

Chapter 5

Revocability of biometric keys generated from a voice based template-free biometric system

There are several advantages and reasons for using biometrics. In the first place, it is a mechanism that has been accepted universally as an automated method of recognising humans based on physiological or behavioural characteristics. It offers many advantages for personal authentication because it cannot be forgotten, stolen, lost, misplaced, guessed or shared among users [14]. In addition, it helps in overcoming the weakness in traditional authentication systems that use tokens, passwords or both (like sharing of passwords, losing tokens, guessable passwords, forgetting passwords etc [10]).

However, protection of Biometric Systems itself is necessary because most current biometric systems are based on templates and operate by measuring an individual's physical features in an authentication inquiry (for identification and verification) and comparing this data with stored biometric reference data. Hence they are associated with risks especially in the safety of the personal biometric information that is stored on the template [10], [14]. As mentioned earlier, once biometric systems are compromised the owner of the biometric as well as the data protected by the biometric is compromised for life, because users cannot ever change their biometric features, and unlike passwords that can be cancelled and reissued if lost or stolen, biometrics cannot be re-issued. Thus, a new trend in biometric research is in the protection of biometrics systems itself. Previous efforts at protecting biometrics have looked at revocable

biometrics [2] – [9], Template Security [14], [13], [17], and lately, Template-free Biometrics [62], [67], [87], [88], [97] - [100], [102], [115].

5.1 Need for cancelling template-free keys

Elimination of all risk factors associated with biometric templates is possible in template-free systems. However, biometrics generally are associated with several vulnerable points other than templates. Therefore, some possible cases of compromise may still exist and have to be mentioned.

- Administration (insider) attack due to the integrity of the system managers who may pre-record the voice passphrase used and attempt to replay it in order to regenerate the key of the operation phase.
- Utilisation attack: In this case, a beneficiary at the operation phase (who had witnessed a file that needed to be unlocked before use) may secretly place a recorder within the interface to capture the passphrase and attempt to replay it subsequently.
- Privacy and safety of biometric sensor: if the owner of the biometric sensor fails to keep the biometric private.

Although there is so far no evidence in literature to support these possibilities in template-free system (since they are not template associated risks), they are however worth guarding against whilst designing a template-free biometric system since those vulnerable points are also part of the template-free process. We however, need to bear in mind that these scenarios are only possible if the system accepts such spoofed biometric trait. The following sections iterate possible techniques for addressing these issues. Their effectiveness will be evaluated in the subsequent sections.

While pioneering the research into template-free biometrics, we could theoretically conclude that the elimination of all risk factors associated with biometric templates is possible using template-free systems. This may also apply to cancellable or revocable

biometrics to a certain extent. However, Ratha et al. [3] identified several different levels of attacks that can be launched against a biometric system as listed below:

i. a fake biometric trait such as an artificial finger may be presented at the sensor,
ii. illegally intercepted data may be resubmitted to the system,
iii. the feature extractor may be replaced by a Trojan horse program that produces pre-determined feature sets,
iv. legitimate feature sets may be replaced with synthetic feature sets,
v. the matcher may be replaced by a Trojan horse program that always outputs high scores thereby defying system security,
vi. the templates stored in the database may be modified or removed, or new templates may be introduced in the database,
vii. the data in the communication channel between various modules of the system may be altered, and
viii. The final decision output by the biometric system may be overridden.

Thus we recognise that biometrics generally is associated with several vulnerable points other than templates; therefore, some possible cases of compromise may still exist, especially at points like the signal capture stage or at the point of data decryption. Other non template-based vulnerabilities like the integrity of the owner of the biometric sensor who may pre-record biometric samples, the owner of the algorithm who may have, and use, privilege rights to decipher measurable values unique to individuals or an attacker, as well as those with access to the algorithm to decipher biometric key from a previously unlocked information or data are some broad based fears to bear in mind. It is in consideration of these fears that this research introduces a new concept that essentially disguises the biometric information generated based on the method used in a template-free system; does not store any template values, thereby eliminating all template associated risks; and reverses cryptographic information when necessary through randomisation of feature distribution maps and introduction of deliberate distortions in feature and pass phrase, thus cancelling previously generated (but disguised) biometric information from the same user candidate.

This chapter explores revocation strategies for biometric keys generated from a voice based template-free biometric system using five generic approaches listed below, whose details are described later in this chapter:

i. *Randomisation of feature distribution maps prior to key re-generation in the operation phase to annul previous user keys*
ii. *Complete replacement of the set of features*
iii. *Partial replacement of some of the features*
iv. *Alteration of the spoken phrase*
v. *Deliberate introduction of distortions in the user distribution maps.*

In the next section, this research will briefly look at existing revocable biometric systems to understand how it can leverage on the evolving concept of template-free biometrics that this research has pioneered. This will be better understood within the context of the reader's comprehension of the previous chapter which provides an in-depth of how keys are generated in template-free biometrics from individual features as well as a novel concept of key combination. The last section in this chapter hypothesizes how these keys can be revoked and an evaluation of the system's performance.

5.2 Evaluation of previous works on Revocable Biometric System

Revocable or Cancellable biometrics is a way of building protection into biometrics, making it possible to re-issue biometric keys or features. Essentially, the original features are kept hidden and never exposed to any risk as a distortion of the features is carried out before matching. The variability in the distortion parameters provides the cancellable nature of the scheme. Revocable biometrics were first introduced by Bolle et al. [55], and several other related works have been performed on the subject. Maltoni

et al [11] stated some principal objectives of revocable biometrics. Davida et al [107] worked on iris data without stored references, Monrose et al [40] used keystroke dynamics which uses the duration of the keys and the latency between each pair of keys. Souter et al [111] also used identification code recovery from the optical integral correlation of fingerprint data. Its principal objectives are: Diversity, Reusability, Non-invertibility, and Performance [2].

Other template protection schemes that can be found in literature are in two broad categories: feature transformation and biometric cryptosystem [13] [14].

5.2.1 Feature transformation

In feature transformation, a fixed transformation function (e.g. a random key or a password) is applied to the template and the transformed template is stored. The same transformation function is introduced to the matching phase to obtain a transformed query that can be matched against the transformed template. Some examples of feature transformation scheme are:

Salting: this is also known as Bio-hashing [2] [112] - [114]. A user specific key or password is introduced as a transformation function to distort the original features. The introduction of the key or password as an additional information further strengthens the biometric system. It also reduces the tendency for false accept and since the key is user specific, multiple templates of the same user can be created by simply changing the keys or password. The problem here is that the key or password needs to be remembered and securely stored. Loss of this key presents a lot of challenges as the system will be difficult to operate without it. Also, theft of this key will compromise the system as the original template can be deduced by 'reversibility'. In addition, this form of distortion may introduce intra user variations which can reduce the recognition performance.

2-N discretization: This is a method proposed by Yip et al [114] to guard against the storage of biometric information that may be reconstructed to decode the original biometric data. This method produces keys that are not permanently linked to the biometric information and it works incorporating randomness, hence, a compromised key can be easily replaced. [114]. In this scheme, it is computationally infeasible to recover the underlying biometric data from the output. This method incorporates the inner product-based mixing with random token, multiple-bit discretization and permutation to result in replaceable cryptographic keys, in addition to a longer and unpredictable key space. The improvement that this brings to the fore over other methods of revocable biometrics include (i) It uses population-wide instead of user specific boundaries for multiple-bits discretization, (ii) It forces the number of segments in discretization space to be of be 2^n so that an adversary has to search all possible space, (iii) It permutates the pre-keys to deter multiple keys attack, and (iv) It uses error correction codes to compensate for the loss of accuracy due to (i) and (ii).

Dynamic Quantisation Transform: [17] uses a technique which converts biometrics into bitstring, allowing authentication to take place in the transformed domain rather than the original biometric feature space, thereby having the advantage of template security. Another advantage is that this method simultaneously satisfies the four major requirement of a revocable template protection scheme which are: accuracy, non-invertibility, privacy, and auxiliary data secrecy. However, this is still an evolving scheme with little information in literature to support its utility.

Non invertible transform: this method is a one way function that is easy to compute but irreversible or when possible, may be very difficult to invert [13]. The scheme is designed such that even if the key or transformed template is known, it is computationally difficult to recover the original template. This makes the scheme very secure. Also, revocability is made possible by using application or user specific transformation function [13]. However, the challenge in this scheme is in the trade-off between discriminability and non-invertibility of the transformation function [13] since

it will be difficult to design a transformation function that satisfies both discriminability and non-invertibility simultaneously.

5.2.2 Biometric cryptosystem scheme

This method works with a helper data to serve as a template protection scheme. Helper data are public information about biometric data that are stored and used to extract cryptographic key from the database during matching [13]. The validity of the extracted key forms the basis for the matching [13]. An example of biometric cryptosystem scheme is Key binding. In a key binding system, the template is secured by binding it with a key within a cryptographic framework. A helper data is used to bind the key and the template which is then securely stored, but the helper data is unable to reveal any information about the template or key. Examples of this scheme include fuzzy commitment [122], fuzzy vault [123], shielding function [124], distributed source coding [125], and Fuzzy extractor [126]. The major advantage of this scheme is that it is tolerant to intra-user variations in biometric data and this tolerance is determined by the error correcting capability of the associated codeword [13]. The major draw backs according to [13] include: (i) Reduced probability of matching accuracy since matching has to be done using error correction schemes and does not use sophisticated matchers developed specifically for matching the original biometric template (ii) In general, biometric cryptosystems are not designed to provide diversity and revocability (iii) The helper data needs to be carefully designed; it is based on the specific biometric features to be used and the nature of associated intra-user variations.

According to Nandakumar et al [127], the Summary of biometric template protection approaches is shown in the table 5.1 below:

Table 5.1: Summary of Biometric Template protection schemes available in literature

Template Protection Approaches	**Methodology**	**Advantages**	**Limitations**
Encryption	Template is encrypted using well-known cryptographic techniques	Matching algorithm and accuracy are unaffected	Template is exposed during every authentication attempt
Non-invertible transform	One-way function is applied to the biometric features	Since transformation occurs in the same feature space, matcher need not be redesigned	Usually leads to increase in the False reject Rate (FRR)
Hardening/ Salting	User-specific external randomness is added to the biometric features.	Increases the entropy of biometric features resulting in low False Accept rate (FAR)	If the user-specific random information is compromised, there is no gain in entropy
Key generation	A key is derived directly from biometric features	Most efficient and scalable approach	Tolerance to intra-user variations is limited, resulting in high FRR
Secure sketch	A sketch is derived from the template; sketch is secure because template can be reconstructed only if a matching biometric query is presented	More tolerant to intra-user variations in biometric data; can be used for securing external data such as cryptographic keys	Template is exposed during successful authentication. Non-uniform nature of biometric data reduces security
Fuzzy vault	A hybrid approach where the biometric features are hardened (using password) before a secure sketch (vault) is constructed	Hardening increases the entropy thereby improving the vault security; also enhances user privacy	Not user-friendly; user needs to provide both the password and the biometric during authentication

Although, revocable biometrics represents a very promising approach to address template-based biometric security, there are still several concerns about the security of such schemes [11], [107]. In addition, if the owner of the biometric sensor fails to keep the biometric private, then the confidence in revocable biometrics will be eroded because its security depends on secure management of the distortion parameters, which must be used for enrolment and made available at matching. The storage of the original

or distorted information on a template equally makes the system vulnerable, hence the justification for this chapter.

The next section will look at the proposed revocation schemes and explain the reasons for using it.

5.3 Proposed Key Cancellation Technique

The main focus is to enhance the security of biometric systems and increase confidence. By using template-free systems, we have eliminated the need to store biometric samples on templates. The next focus is to completely remove inherent problems associated with non template vulnerabilities e.g. information extracted at the signal pre-processing stage as well as concerns with the integrity of individuals for whom the system had been decrypted using specific biometric information, passphrases as the case may be. This is just in case such individuals or an eavesdropper copies the information at the point of decryption and tries to re-use it illegally. Revocability is introduced at the key building stage by disguising the binarised biometric information used for cryptography in such a way that it can be cancelled after use, but preserving the actual biometric information on the individual. To fully appreciate this section, it is important to understand how keys may be generated in template-free system as elaborated in chapter 4.

5.3.1 Randomisation of feature distribution maps

Randomisation of feature distribution maps prior to key re-generation can annul previous user keys. Randomisation in this case is achieved by alteration of feature positions and (consequently) distances between the positions. Since this key combination method is based on bit concatenation, the pattern of the key changes if the successive feature positions within the algorithm are altered. This also automatically changes the position value used as additional key building technique. As an illustration, and following from key generation scheme outlined in chapter 4, consider a biometric key generated from a set of features as below:

Table 5.2: Illustration of feature randomisation

Feature A	Feature B	Feature D	Feature C
111101	100110	101011	001100

=111101100110101011001100

Note that these keys are not stored anywhere but for a template-free system, the keys needs to be the same at all instances of re-generation This key becomes completely different if we change the order of feature occurrence as below:

Table 5.3: Illustration of feature randomisation

Feature D	Feature A	Feature C	Feature B
101011	111101	001100	100110

= 101011111101001100100110

The implication of this revocation strategy is that there will be a complete re-calibration to interweave the features used for building the maps i.e. the order of feature occurrence before generating the distribution maps is altered to consequently annul previously generated keys based on the operation phase.

However, there are some weaknesses in this scheme as follows:

(i) The randomisation process cannot be automated because once the algorithm is compromised, it may be possible to predict how the maps will be reordered. The solution to this will be for the randomisation scheme to be external to the system and be unpredictable. The proposed option is to build a randomisation algorithm that can be resident on a server or the features can be tied to random numbers that can be chosen by the user. It should be noted that remembering these random numbers may not necessarily become a challenge because the user only needs to choose them once and not bother about remembering them.

(ii) In order to ensure proper association of the keys to individual users, the new key needs to relate to the original key, and this brings up the need for some form of storage with the associated risks with storage of biometric information. The solution to this is to incorporate 'time stamps' and 'liveness detection' which are subjects for future research.

(iii) If the same features are used at all times and are merely reordered, then the system can be exhaustively attacked easily since it will contain the same number of '0's and '1's and which reduces the search space significantly. This will therefore make the sole use of this scheme not reliable but it can be used in combination with other schemes.

5.3.2 Complete and fraction feature replacement

If a set of features A, B, C, and D are used at the first instance, new sets of features D, E, F, G, H, and I can be used subsequently. (Note that these are selected from the features discussed in Chapter 3). This is a case of complete replacement of features from the same user. In another scenario, a partial replacement can also be made. In this case, the introduction of an additional feature alters the entire feature distribution maps and consequently, key configuration. This scheme is also prone to challenges as follows:

- The need to relate the new key with the original key.
- The need to use a medium external to the system to select the new sets of features to be used.

  The fact that the system can run out of features after several revocations are carried out.

5.3.3 Alteration of spoken phrase

The spoken word or phrase fed into the system also affects the configuration of keys generated as representation of the individuals. A simple alteration of the pass phrase or spoken word from which the features are derived will completely alter the keys. Getting the users to speak a particular phrase reduces intra sample variations and makes the system stronger. In addition, the spoken phrase becomes another level of password. The challenges in this scheme include the common challenges to voice biometrics like cold, variation as the individual ages, background and channel noise, variable and inferior

microphones and telephones; and extreme hoarseness, fatigue or vocal stress, and it is not suitable for use by individuals who cannot speak (e.g. the deaf and dumb).

5.3.4 Introduction of Transformation function

This scheme allows addition of a transformation function to the feature distribution maps and the same transformation function at the operation phase. This follows the same principle as in BioHashing, but it is applied to the feature distribution maps as against the stored template in BioHashing. A user specific key or password is introduced as a transformation function to distort the feature distribution maps and the same distortion measure used at the Operation Phase when keys are being re-built from previously unseen user samples. In addition to this, and depending on the type of biometric modality being used, helper data can be introduced deliberately to change the property of the keys generated by a fixed measure. The problem here is that storage of the helper data is required and will make it vulnerable to template-based attack. Despite these challenges, the use of this method in combination with others proposed above will reduce the probability of successfully attacking the system.

5.3.5 Hybridization of several cancelling schemes

Hybridization in this case combines a number of options to deliberately alter the biometric key, making it difficult to re-create for fraudulent purpose. The proposed scheme can use a distortion value; combined with phrase alteration, helper data, randomisation of distribution maps and so on. The performance of the hybrid scheme is a function of the strength of the various schemes employed.

5.4 Non invertibility

The essence of revocable biometrics is to protect the original biometric data belonging to individuals. This system has proposed a number of schemes that can be used to cancel keys generated from a template-free biometric system. Such a scheme should however not allow the original biometric information to be deduced from the keys, even if the transformation parameters are known.

According to Kong et al [7], for any invertible transform $y = f(x)$; $x = f^{1}(y)$ can be derived, where $f^{1}(y)$ is the inverse of f. Within the concept of this system, the codes obtained from the system should be such that it is non invertible i.e. the inverse $g^{1}(x)$ should not be deduced from the transform $y = g(x)$.

Considering that this system does not store template information, this research therefore proposed to use feature domain quantisation and the transformation from measurable feature values to normalisation maps as described in chapter 4 to guard against the reversibility of the scheme.

5.5 Performance evaluation

The primary difference between this system and other revocable biometric systems is that while revocable biometrics disguises or transforms template information from the original template safely stored, this system completely eliminates storage of templates. This system principally annuls biometric keys generated based on the referenced normalisation maps at the operation phase. This approach eliminates all vulnerabilities associated with template-based system, and defeat other attacks based on administrative, technical and enrolment process.

Initial examination of this system against existing revocable biometrics system shows the following possibilities:

i) There are less opportunities for compromise in this system than in traditional revocable biometric system as the number of vulnerable points are greatly reduced.

ii) Unlike this system, traditional revocable biometrics are still subject to intrinsic failure which are due to limitations in the sensing device, which leads to false accept/reject.

iii) The integrity of the enrolment process in revocable biometrics introduces a weak point that can be exploited e.g. collusion at the point of enrolment, forced enrolment, and abuse of exception processing [13].

iv) Modification of template records and operating parameters are other administrative abuses possible in traditional biometric systems, but which have been eliminated based on this system.

5.6 Challenges to the proposed system

This system is based on voice biometrics, an evolving biometric modality which is susceptible to environmental interferences. Another issue of concern is the high instability of voice systems over a given period in an individual's life, e.g. between childhood to Adolescent to old age, and in periods of illnesses. This can possibly result to high intra class variability of the voice samples used within the different periods. Although the effect of these changes on voice as a biometric modality is outside the scope of this research, it is noteworthy for future work.

These techniques offer advantages over existing revocable biometrics systems because they use a method that incorporates a number of advantages drawn from both template-free and revocable biometrics. The basic operating principle (which will be described in detail later) is as follows:

(i) It uses keys generated from a template-free biometric system and then incorporates revocability, therefore having all the advantages of template-free system.

(ii) It does not store any template values as a basis for comparison, therefore eliminating template associated risks that are still possible in traditional revocable systems.

(iii) It disguises the biometric information used for cryptography by using the values of feature positions and distances rather than the actual biometric samples, and

(iv) It can reverse information passed from a user to a cryptographic algorithm at every instance of the operation phase in a template-free system through randomisation of feature distribution maps, deliberate introduction of distortions in features and pass phrase, thus cancelling previously generated (but disguised) biometric information from the same user candidate.

5.7 Experimental analysis of revocation strategies

The experimentation in this Chapter follows from the keys generated from suitable features used in the template-free system (during the operation phase) as described in previous Chapters and using the VALID and YOHO Datasets already described in chapters 3 and 4. It follows from the identified voice features that met the template-free criteria as detailed in previous publications [62], [86] - [88], [115], [108], [109]. Some examples include: Maximum Power Spectral Density (PSD), Average Power Spectral Density (PSD), Minimum Power Spectral Density (PSD), Minimum fft, Mean Amplitude, Minimum amplitude, minimum cepstrum, mean cepstrum, maximum ifft, minimum ifft, mean ifft, maximum hilbert function, minimum hilbert function, mean hilbert function, Maximum Amplitude; Peak to Peak Amplitude; Mean Frequency; Maximum Frequency. These features are used in [108] to establish that the results for template-free biometric system based on the voice modality produces keys for all the subjects tested at an average of 65.55% accuracy. These are the keys that form the basis

for the experiments under the revocation strategies outlined in this chapter. The experimental evaluation of each strategy is outlined subsequently.

Randomisation of feature distribution maps Strategy

The main aim of the investigation of this particular revocation strategy is to show that there is a lot of difference between the code that is generated based on the traditional template-free scheme and the code based on a random feature distribution.

Keys produced from samples taken from 130 users from the YOHO database were investigated. These are keys based on the concatenated features for individual subjects as in the previous chapter. The sequence of the bits (made up of '0's and '1's) and the points at which they change between the '0's and '1's were noted (they are a function of the specific feature from which they were generated) as illustrated in tables 5.2 and 5.3. A typical illustration is the result for user 101 in the YOHO database indicated in table 5.4 below. In this table, the points at which the bits changes between '0' and '1' have been underlined. Although the number of bits in the original code and the randomized codes are the same, when the key generation method outlined in Chapter 4 is taken into consideration, it will be noted that the points at which these bits changed between '0's and '1's is a significant method of distinction. Hence, even though the codes belong to the same subject, it has been altered to provide a sense of revocation and re-issue.

Table 5.4: An example of random feature distributions using samples of user 101 in YOHO database showing that the original codes are different from the transformed code.

User	Codes based on regular template-free scheme	Same user code based on random feature distributions
101	0000000000000000000000100000000000 0000000000001000000000000000000010 0110000000000000000000000010000000 0000000100000000000000010100000000 0000000000110000000000000000000000 0000000100000000000000110000000000 0000001100000000000000000000001100 0000000000000000000000001100000000 00000000001	0000000000000000000000010000000000000 0000000001000000000000000000110000000 0000000000000001100000000000000000000 0000000010000000000000001100000000000 0000001001100000000000000000000001000 0000000000001100000000000001010000000 0000000001000000000000001000000000000 000000000000000110

Note the points at which the bit changes from '0' to '1' in all cases. For this particular case, the bits changed at 23, then the next change from point 23 occurred at 19, then at 2, 24, 15, 15, 2, 19, 29, 15, 16, 22, 26, 18 for the left hand row while it is at points 23, 24, 19,24, 29,15, 19, 3, 22, 16, 13 , 16,15 an 26 for the right side. In order to better understand this table the Figures below shows the shape of the distribution when plotted on a scale for the region between bits 65 and 92.

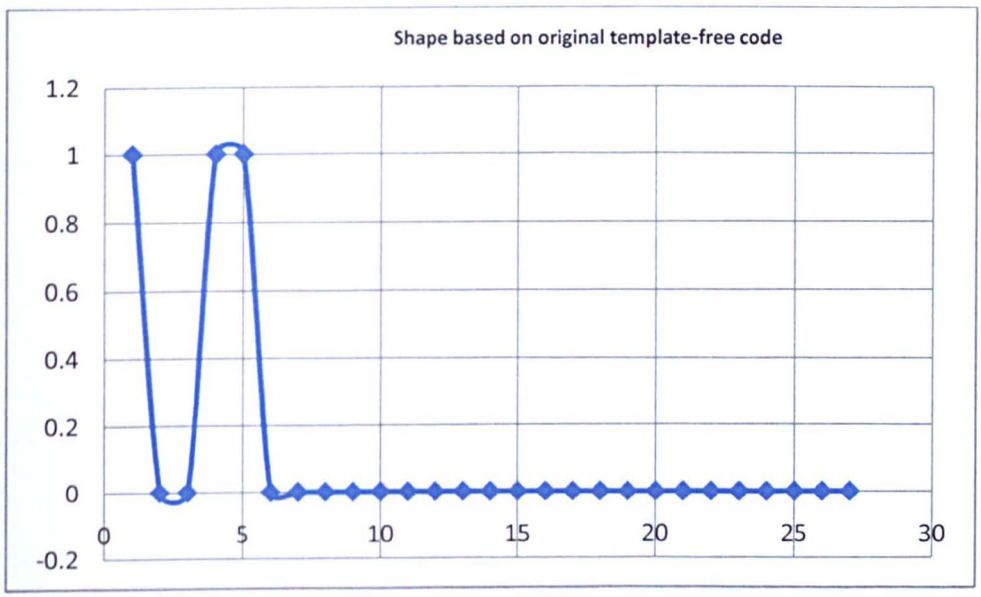

Fig.5.1 Shape based on regular template-free scheme

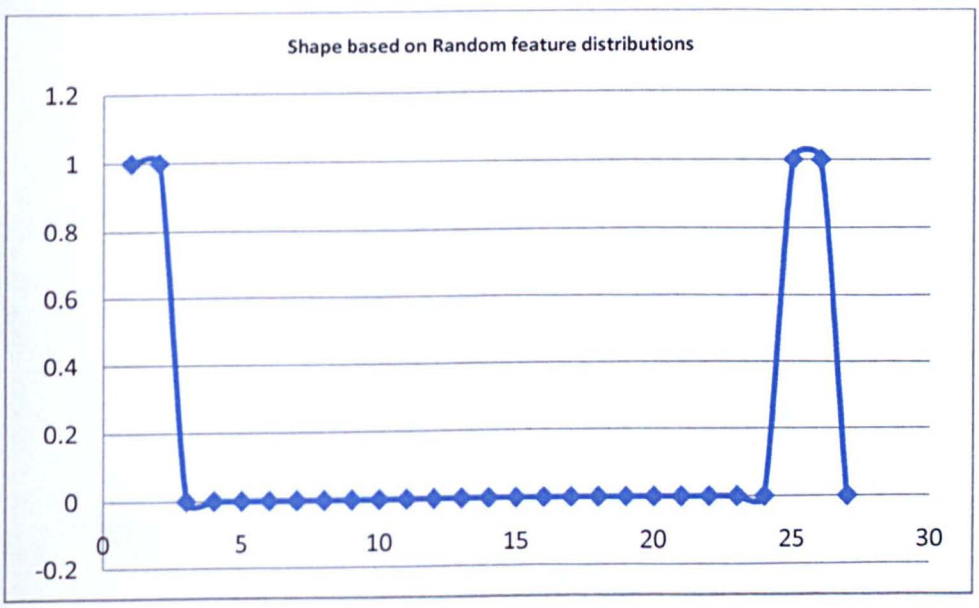

Figure 5.2: Same user's shape based on random feature distributions

The graphical illustration in Figures 5.1 and 5.2 shows the points on a scale where the bits changed between '0' and '1' for the same user but based on different structures of the normalisation maps. This means that the sequence of the features within the map affects the value of the bits contributed to form the key and a random re-ordering of the map will change the sequence and consequently the entire structure as illustrated between Figures 5.1 and 5.2.

The import of this scheme is that in an automated process, using several samples and features from the same subject, a significant bit re-ordering can be achieved to create multiple keys representing the same identity.

This evaluation was repeated for 130 subjects and it was observed that for each change in the positions of the features in the distribution maps at the calibration phase, the code changes and these changes differ between individual users. However, since the same features are used in this case, the number of '0's and '1's that make up the code are equal between the original code and the new code. Therefore, to attack the system, a hacker needs to carry out a number of permutations to obtain all the possible arrangements between the old and the new code. This can be achieved by the knowledge of the number of 'n' bits taken 'k' at a time denoted by

$$^{n}P_{k} = \frac{n!}{(n-k)!} \quad \ldots\ldots\ldots \quad 5.1$$

Since the permutation of a number of objects is the number of different ways they can be ordered; i.e. which is first, second, third, etc, we chose the number of 1's in the bits generated taking cognisance of the positions of the 1's. In a typical case evaluated, there are 21 bit changes (1's) out of the 276 bits. Therefore, the number of permutations (reordering) that an attacker needs to do to obtain the new key from the compromised key is

$$^{276}P_{21} = \frac{276!}{(276-21)!}$$

$$= 8.320514302514807557576141904178 6e^{+50} = 8.32 \times 10^{50}$$

=832,051,430,251,480,000,000,000,000,000,000,000,000,000,000,000,000 number of possible combinations.

Therefore, for the random feature distribution scheme, the number of times an attacker can make an attempt before recovering the new code, granted that the old code is compromised is
832,051,430,251,480,000,000,000,000,000,000,000,000,000,000,000,000 times.

The overall result for this scheme and other schemes are as shown in table 5.9.

Complete or Partial replacement of some of the features

In this scheme, even though the same features were used, the revocable code is dependent on the fraction of the features used. The scheme is as outlined in section 5.3.2. As in the previous scheme, 130 subjects were evaluated. A set of features were selected to form the normalization maps and subsequently, keys were generate based on these features. At a second instance, a different set of features from the same subjects were used and the sequence of the bits (made up of '0's and '1's) and the points at which they change between the '0's and '1's were noted for both instances.

Using the codes generated for user 101 as illustrated in table 5.5, the keys based on a fraction of the features and another fraction is shown.

Table 5.5: Fraction feature replacement using codes of user 101 in YOHO database

User	Codes based on regular template-free scheme	Same user code based on fraction feature replacement
101	000000000000000000000001000000 000000000000000001000000000000 000000010011000000000000000000 000001000000000000010000000000 000000101000000000000000000011 000000000000000000000000000001 000000000000001100000000000000 001100000000000000000000001100 000000000000000000000000011000 000000000000001	000000000000000000000100000000 000000000000001000000000000000 000110000000000000000000000110 OR 000000000000000000000000001000 000000000011000000000000000110 00000000000000000000110

A further illustration for user 103 the code generated using the respective features are as indicated below:

Maximum Amplitude	Minimum Amplitude	Average Frequency	Max Hilbert
0000000000000000 0000001	0000000000000000 000000110	0000000000000000 00011	0000000000000000 0000001

The code for this user based on a fraction of the feature distributions

0000000000000000 000001	0000000000000000 000000110	0000000000000000 00011	0000000000000000 0000001

The above translates to a code for this user as shown below:
00000000000000000000001000000000000000000000011000000000000000000000110
000000000000000000001

When another set of the features for the same subject are used it will produce a different code as follows:

Maximum PSD	Minimum PSD	Average PSD	Max Hilbert
0000000000000000 00000000000010	0000000000000000 00000000000001	0000000000000000 10	0000000000000000 0000001

The above now translates to the code for the same user as shown below:
00000000000000000000000000001000000000000000000000000000000010000000000
000000100000000000000000000001.

In each resultant code, the order of the bits and their respective values should be noted. The advantage of this scheme is that the system is re-calibrated with new sets of features and so the user or the system needs not remember or know the feature. These features can be selected randomly and the code produced from each set differs from the initial code and also differs between users. Thus it is difficult to work out the initial code from just a fraction of the revoked code or a completely new set of the features which produces a new code. For an attacker to successfully work out the original code, a user must have used all the possible combinations of features and all the combinations would have to have been compromised and this may not happen over an individual's

lifetime. In addition, the attacker must also overcome the hurdle of cracking a template-free scheme to first of all have sufficient knowledge of the initial code. The evaluation for this scheme for 130 subjects is also reported in table 5.9

Deliberate introduction of distortions in the user distribution maps

Table 5.6 is for the addition of a transformation function. In order to attack the system based on this scheme, the attacker needs to:

i. Know the transformation function added to the code,
ii. Be able to crack the template-free code, a possibility that is yet to be proven
iii. Decode the features that were used and their respective order of occurrence and be able to re-arrange them to work out the new code as well as obtain the transformation function.

The problem here is that the transformation function will need to be stored or be in the form of a password; therefore the transformation function is only as secured as the password. However, the user only needs to type in the password or the random number used as a helper data just once to avoid the issues with remembering the transformation function.

Table 5.6: Addition of a transformation function to the code of user 101 in YOHO database

User	Codes based on regular template-free scheme	Same user code based on addition of a transformation function
101	0000000000000000000000100000000000000 0000000001000000000000000000100110000 0000000000000000001000000000000001000 0000000000010100000000000000000011000 0000000000000000000000000100000000000 0001100000000000000011000000000000000 0000001100000000000000000000000000110 00000000000000001	simply a case of the code on the left + a fixed function which is only known to the user

For this scheme, 130 subjects were evaluated and in each case a fixed value was added in all cases. For experimental purpose, this known fixed value yielded the same bits and

in all the subjects, the code changed by the value of the fixed distortion added and when the distortion value is changed, the code automatically changed. Thus the code was successfully altered in 100% of the users as indicated in table 5.9. It should however be noted that when another method of distortion other than a fixed value is used, the success rate maybe less as such distortion parameter may introduce some margin of error. This was however not investigated as it is out of scope of the research.

Alteration of the spoken phrase

This scheme was the most difficult to evaluate as all the inherent problems associated with voice based systems had a role to play. For each phrase altered, the values are not 100 % the same. Table 5.7 is an illustration of user 101 codes for the case of altering the spoken phrase in which case the phrase becomes the password for the system. Tables 5.7 and 5.8 shows that for each phrase spoken by the same user, there is a difference in the resultant codes generated.

Table 5.7: Alteration of spoken phrase using user 101 of YOHO database

User	Codes based on regular template-free scheme	Same user code based on altered phrase
101	000000000000000000000010000000000000000000000000 100000000000000000010011000000000000000000000000 100000000000000100000000000000101000000000000000 000001100000000000000000000000000010000000000 000011000000000000001100000000000000000000011 000000000000000000000000001100000000000000001	see table 5.8

Table 5.8: User 101 based on altered phrase (Note the positions at which the bits changes between '0' and '1').

Uttered phrase	Code for the same user			
	Maximum Amplitude	Average Amplitude	Minimum Amplitude	Peak to peak Amplitude
27_82_39	0000000000000 0000000001001 100001	000000000000 000000100110 10111111	0000000000000 0000000001110 011100	0000000000000 0000000010111 110101
61_75_53	0000000000000 0000000001010 000011	000000000000 000000100111 10010111	0000000000000 0000000001110 100010	0000000000000 0000000011100 100111
62_91_59	0000000000000 0000000001101 110100	000000000000 000000100111 11010111	0000000000000 0000000001100 110111	0000000000000 0000000011001 000011
75_43_34	0000000000000 0000000011000 100011	000000000000 000000100111 10001110	0000000000000 0000000001110 000101	0000000000000 0000000010010 101101

Table 5.8 shows how the codes changes for the different phrases from the same user. In all the 130 subjects evaluated, the code was correctly revoked (while still representing the same user) in 70 % of the subjects. This level of accuracy could be attributed to the inherent problems associated with voice biometric systems as each sample from the different phases contributes some form of errors that reduces the level of accuracy.

Analysis of revocability rates of the various schemes

Table 5.9 shows the summary of the percentage of key revocability and reliability of the various schemes based on the YOHO datasets for 130 users. It also shows the possible weakness of each scheme.

Table 5.9: Analysis of revocability rates of the various schemes

Number of subjects	Revocability scheme	Percentage of key revocability per 130 users	Weakness	Remarks
130	Randomised distribution maps	100%	See section 5.3.1	
130	Complete and fraction feature replacement	100%	See section 5.3.2	
130	Alteration of spoken phrase	70%	See section 5.3.3 Also, it is useful only in text dependent systems. Cannot be used if spoken phrase is not the basis for key generation in the first place	
130	Introduction of Transformation function	100%	See section 5.3.4	
130	Hybridization of several cancelling scheme	100%		This is the most suitable technique which will benefit from all the advantages of the various schemes and can still do well even with the disadvantage of any of the schemes

Tables 5.4 to 5.9 indicates that for each of the proposed schemes, the value of the codes generated for the same individual differs, implying that using a number of possible combination of the schemes, new codes can be created to replace previously used codes as many times as necessary.

Overall, the proposed revocation strategies enhances security and preserves privacy by taking away the control of biometric system from the hands of either an attacker, the owner of the biometric sensor used for signal/sample capture, or those with access to the algorithm.

5.8 Chapter summary

It is important to note that the various schemes outlined in this chapter are postulations based on which this chapter establishes the possibility of integrating the concept of revocable biometrics with ongoing research in template-free biometrics. By disguising the biometric information used to generate keys in template-free system, a new set of biometric information can be produced to annul previously used keys. This can help to reduce problems of compromise associated with all vulnerable points in biometric systems. The system revokes biometric keys generated from the operation phase of a voice based template-free system using four approaches viz:

(i) Randomisation of feature distribution maps prior to key re-generation in the operation phase to annul previous user keys
(ii) Complete replacement of the set of features
(iii) Partial replacement of some of the features
(iv) Changing the spoken phrase

This method introduces several novelties as follows:

- does not store any template values as a basis for comparison,
- disguises the biometric information used for cryptography by using the values of feature positions and distances rather than the actual biometric samples, and
- reverses cryptographic information when necessary through randomisation of feature distribution maps and introduction of changes in feature and pass phrase,

thus cancelling previously generated (but disguised) biometric information from the same user candidate.

This chapter makes some contribution to addressing non template-based vulnerabilities and the result of the experiments represents some credible solution to this problem.

Chapter 6

Conclusions

This chapter summarises the work done on the strategies for template-free biometrics using features from the human voice as well as a discussion on the major research findings and suggestions for future research. The conclusion reviews the entire research report to ascertain if the aims and objectives were met. As stated in the introductory chapter, the overall aim of this research was to investigate and develop strategies for the novel concept of template-free biometrics using human voice modality. Towards achieving this aim, the research targeted a number of objectives like:

- Evaluating candidate features extracted from the human voice that can be employed in template-free systems.
- Outline the principles of template-free biometrics based on voice strategy
- Introducing feature concatenation as the novel technique for voice feature combination as a means of combining the biometric codes generated from template-free systems.
- Investigating techniques for the integration of revocable biometrics with template-free biometrics in order to enhance security and preserve privacy by taking away the control of biometric system from the hands of either an attacker, the owner of the biometric sensor used for signal/sample capture, or those with access to the algorithm.

In terms of the specific objective, this research evaluated a number of features (both in use for template-based application and a set of new ones) and identified those that meet set criteria for use in a template-free system. In addition, an overall strategy for template-free biometric was introduced, with further evaluation of how the voce features can be used to develop a template-free application. The results also show how template-free biometric keys can be revoked and re-generated using a number of revocation strategies.

In terms of a final reflection on the aims and objectives of the research, the overall aim of investigating strategies for the novel concept of template-free biometrics using human voice modality was achieved but a lot of further work is required to develop a practical system based on the pragmatic appraisals in the next section.

6.1 Summary of contributions

This research has introduced a new concept in biometric technology in which biometric keys are generated from a combination of information derived from a number of newly identified human voice features without referencing a stored biometric template. The following summarises the main contributions of the research.

- A set of criteria for evaluating voice features suitable in template-free biometrics was developed based on references to standard biometric evaluation criteria and previous work on template-free systems based on fingerprint and ICMetrics.

- A number of candidate voice features were found to possess useful characteristics that can be used in a template-free biometric system. These are features that met the set criteria above and they include existing features used in voice biometrics as well as newly identified features detailed in chapter 3.

- Following from an initial review of cryptographic systems and biometric encryption, the research further suggested a new method of generating

encryption keys from the human voice in a template-free scenario. In doing this, the research addressed the two main phases in template-free biometric systems – the Calibration and Operation phases and introduced nine steps involved in the voice calibration process which are carried out once per application domain while the operation phase is employed subsequently every time an encryption key is required.

- Furthermore, a new method of feature combination called 'Feature concatenation' was introduced. It was used as a means of combining the features as well as a basis for further evaluations and generation of the normalization maps.

- The research was the first to investigate the possibility of integrating the concept of revocable biometrics with template-free biometrics in order to combine the strengths of the two concepts. The findings lay the foundation for eliminating problems of compromise associated with all vulnerable points in biometric systems as it postulates a system that (i) does not store any template values as a basis for comparison, (ii) disguises the biometric information used for cryptography by using the values of feature positions and distances rather than the actual biometric samples, and (iii) reverses cryptographic information when necessary through using five newly identified revocation strategies.

- The research also identified five new strategies for revoking biometric keys and reproducing them at high accuracies (depending on the number of schemes combined). Thus, a system that will require an attacker to make 832, 051, 430, 251, 480, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000 attempts before recovering the code from an exposed biometric was theoretically developed. This is based on the results obtained as the percentage of revocation per user tabulated in chapter 5.

In addition to cataloguing these contributions, it is important to note a number of challenges that were encountered which will form the basis for future research on this subject. These include:

- The use of normalization maps is associated with some concerns because though substantial evaluations established that the elimination of templates as a source of reference data can be achieved, this system still stores some form of distorted or scrambled reference called normalization maps which are available for attack.

- The research has also shown that the length of the biometric key produced is necessarily a function of the number of features employed as fewer features produces less possibilities of consistent bits that can be used for biometric keys. Thus, the need to further research into identifying more features is obvious in order to provide a sufficient length of biometric key that cannot be exhaustively attacked.

- Unfortunately, voice is still an evolving biometric and there are very few voice databases with the required flexibility for evaluations. This therefore limited the scope of evaluations to a few databases. Therefore some research thoughts like the performance of the system across various ethnic background could not be tested. Other thoughts include the behavior of the system using samples taken when a subject is well and when he or she is sick; the samples taken from the same subject as he or she ages; and so on. Since there are no voice databases that addresses peculiar situations like these, it was impossible to address such research thoughts.

- Voice is still associated with the tendency for high inter-class similarities and intra-class variations depending on the environment, the state of health of the subject, the hardware, and several other factors that makes voice more difficult to evaluate compared to other biometric modes. Therefore, this research was

unable to test the effect of using the system in varying environments with different background noise and weather conditions. Furthermore, the effect of variable microphones or capture device on the system was another resecrh thought that could not be exploited due to lack of suitable data. This is important to note because the hardware may introduce distortions that may yield varying results for the same candidate.

Based on the pragmatic appraisal in this section, it can be concluded that this research makes some initial contribution as well as lays the basic foundation towards building a voice based template-free biometric system. It can also be concluded that given an improved result, the practical application of the system when integrated with alternative security systems can bring about a solution to template-based compromises in biometric systems. In addition, the proposed revocation strategies will revolutionise biometric security by ensuring that stolen or exposed biometric data does not necessarily mean a life time of compromise to the subject especially as it currently stands when users cannot change a compromised biometric.

This research can form the basis for building a system that eliminates administrative compromises like template modification and cloning; and improve on the integrity of the enrolment process, reducing the potential for compromise due to collusion at enrolment, forced enrolment, and abuse of exception processes.

The potential application of the system range from secure document exchange over electronic media to instant encryption of mobile telephone conversations based on the voice samples provided by the speaker, access control systems, banking, etc. Thus, it is important to recommend further evaluations as detailed in the next section.

6.2 Recommendations for Future Work

The advantages introduced by this research can be further improved upon. The recommendations for improving on the various strategies outlined in future research include:

- The main goal of building a system that will not store any form of reference data (including the normalization maps) still remains to be achieved and hence is recommended as future research challenge.

- Future research needs to further look at 'feature concatenation' as an alternative method of feature combination with a view to establishing that it is a superior form of feature combination.

- It is a well known fact that there are common challenges to voice biometrics like high inter-class similarities and intra-class variations, cold (ill-health), variation as the individual ages, background and channel noise, susceptibility to environmental interferences, variable and inferior microphones and telephones; and extreme hoarseness, fatigue or vocal stress, and it is not suitable for use by individuals who cannot speak (e.g. the deaf and dumb). Future research needs to address these basic challenges.

- It has been shown in this research that the strength of the biometric is a function of the number of features used to build the key. Therefore, evaluation and generation of more features to strengthen the keys as well as to provide enough codes for use in the revocation strategies could also be explored further.

- There is also the need to improve on the accuracy of the keys which is currently at 65.55% accuracy in this research.

- In terms of the revocation strategies, opportunities exist for a lot of further research. In a practical scenario, the system must be automated; however, further research is required as currently, the randomisation process in the revocation scheme cannot be automated because once the algorithm is compromised, it may be possible to predict how the maps will be reordered. In addition, further research is required to develop a sch eme that will ensure proper association of the keys to individual users because the new key needs to relate to the original key, and this brings up the need for some form of storage with the associated risks with storage of biometric information. The proposal to addressing this could be to incorporate 'time stamps' and 'liveness detection' which are subjects for future research. Furthermore, if the same features are used at all times and are merely reordered, then the system can be exhaustively attacked easily since it will contain the same number of '0's and '1's and which reduces the search space significantly. This will therefore make the sole use of this scheme not reliable but it can be used in combination with other schemes which requires further research to develop the integration. Finally, the revocation strategy requiring deliberating introduction of distortions in the distribution maps is a bit challenging. The problem here is that storage of the helper data is required and will make it vulnerable to template-based attack.

- There is the need to research into developing the right metrics for template-free biometrics as the current metrics used in template-based biometrics do not sufficiently represent measurements in template-free systems. Suggestions on such metrics which may be addressed by future research include comparative time, calibration error, margin of useful deviation from the mean to build normalization map, concatenation error, normalization map distortion coefficient, etc.

References

[1] J. L. Wayman, Technical testing and evaluation of biometric identification devices, in A. Jain, et al. (eds) Biometrics: Personal Identification in Networked Society. Kluwer Academic Press, 1999.

[2] Andrew B.J. Toeh et al, Random Multispace Quantisation as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs, IEEE transactions on pattern analysis and machine intelligence, vol. 28, No. 12, December 2006.

[3] N.K. Ratha, J.H. Connell, and R.M. Bolle, Enhancing security and privacy in biometrics based authentication systems, IBM Systems Journal Vol 40, No 3, 2001, pp. 614-634

[4] Loris Nanni, Alessandra Lumini, Random subspace for an improved BioHashing for face authentication, Pattern Recognition Letters 29 (2008) 295-300

[5] A.B.J. Teoh, Yip Wai Kuan, Sangyoun Lee, Cancellable biometrics and annotations on BioHash, the journal of the pattern recognition society 41 (2008) 2034-2044

[6] A.B.J. Teoh, D.N. Chek Ling, and A. Goh, BioHashing: two factor authentication featuring fingerprint data and tokenized random number, the journal of the pattern recognition society 37 (2004) 2245-2255

[7] A. kong, K. Cheung, D. Zhang, M. Kamel, and J. You, An analysis of BioHashing and its variants, the journal of the pattern recognition society 39 (2006) 1359-1368

[8] Y. Pang, A.T.B Jin, and D.N.C. Ling, Binarized Revocable Biometrics in Face Recognition, in Computational Intelligence and Security Volume 3802/2005 pp 788-795, Springer Berlin / Heidelberg, 2005

[9] Anil K. Jain, Umut Uludag, Hiding biometric Data, IEEE transactions on pattern analysis and machine intelligence, vol. 25, No. 11, November 2003

[10] Maltoni, Anil, Wayman, Dario (Editors), Biometric Systems: Technology, Design and Performance Evaluation, Springer-Verlag 2002 ISBN 1852335963

[11] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, pp. 301-307. Springer, 2003.

[12] Andrew Patrick & Sabrina Mu, Usability and Acceptability of Biometric Security Devices, National Research Council of Canada, Updated September 10, 2004

[13] A.K. Jain, K. Nandakumar, and A. Nagar, Biometric Template security, EURASIP Journal on Advances in Signal Processing Vol 2008

[14] Anil K. Jain, Arun Ross, and Umut Uludag, Biometric template security: Challenges and solutions. In Proceedings of the 14th European Signal Processing Conference (EUSIPCO), Antalya, Turkey, September 2005.

[15] C. S. Chin, A. T. B. Jin, and D. N. C. Ling, "High security iris verification system based on random secret integration," Computer Vision and Image Understanding, vol. 102, no. 2, pp. 169–177, 2006.

[16] T. Connie, A. B. J. Teoh, M. Goh, and D. C. L. Ngo, "Palm Hashing: a novel approach for cancellable biometrics," Information Processing Letters, vol. 93, no. 1, pp. 1–5, 2005.

[17] T.S Ong, A.B.J. Teoh, S.E. Khor, and T. Connie, Reliable template protection technique for biometric authentication, IEICE Electronic express, Vol. 5, No. 8, 278-284

[18] A.K. Jain, S Prabakar and A Ross, An Introduction to Biometric Recognition, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004

[19] J. Wayman, Fundamentals of biometric authentication technologies. Int. J. Imaging and Graphics, **1**(1), 2001.

[20] A. Jain, et al. (eds) Biometrics: Personal Identification in Networked Society. Kluwer Academic Press, 1999.

[21] Edgar Danielyan, The Lures of Biometrics, The Internet Protocol Journal - Volume 7, Number 1, March 2004

[22] A.A. Ross, K. Nandakumar et al., Handbook of Multibiometrics Vol. 6, 2006, ISBN: 978-0-387-22296-7

[23] N. K. Ratha, A. Senior and R. M. Bolle, ICAPR tutorial on automated biometrics, IBM T. J. Watson Research Center, Hawthorne, NY 10532

[24] Anil Jain, Umut Uludag and Arun Ross, Biometric Template Selection: A Case Study in Fingerprints, Appeared in Proceedings of 4th International Conference on Audio- and Video-Based Person Authentication (AVBPA), LNCS 2688, pp. 335-342, Guildford, UK, June 9-11, 2003.

[25] Ioannis Maghiros et al, Biometrics at the Frontiers: Assessing the Impact on Society, Technical report series for the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), 2005

[26] D. J. Hurley, B. Arbab-Zavar, and M. S. Nixon, The ear as a biometric, 15th European Signal Processing Conference (EUSIPCO 2007), Poznan, Poland, September 3-7, 2007.

[27] Palmprint Recognition [online]. Available: http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Palm%20Print%20Recognition.pdf

[28] F. J. Prokoski, "NC-TEST: noncontact thermal emissions screening technique for drug and alcohol detection," in *Proc. SPIE: Human Detection and Positive Identification: Methods and Technologies* (L. A. Alyea and D. E. Hoglund, eds.), Vol. 2932, pp. 136-148.

[29] Stuart D. Mowbray and Mark S. Nixon, Automatic Gait Recognition via Fourier Descriptors of Deformable Objects in J. Kittler and M.S. Nixon (Eds.): AVBPA 2003, LNCS 2688, pp. 566–573, 2003. c Springer-Verlag Berlin Heidelberg 2003.

[30] A. Kale, A. Sundaresan, A. N. Rajagopalan, N. P. Cuntoor, A. K. Roy Chowdhury, V. Kruger, and R. Chellappa, "Identification of humans using gait," IEEE Trans. Image Process., vol. 13, no. 9, pp. 1163- 1173, Sep. 2004.

[31] Sudeep Sarkar , P. Jonathon Phillips , Zongyi Liu , Isidro Robledo Vega , Patrick Grother , Kevin W. Bowyer, The Human ID Gait Challenge Problem: Data Sets, Performance, and Analysis, IEEE Transactions on Pattern Analysis and Machine Intelligence, v.27 n.2, p.162-177, February 2005.

[32] M. S. Nixon and J. N. Carter, "Automatic recognition by gait," Proc. IEEE, vol. 94, no. 11, pp. 2013-2024, Nov. 2006.

[33] Zongyi Liu , Sudeep Sarkar, Improved Gait Recognition by Gait Dynamics Normalization, IEEE Transactions on Pattern Analysis and Machine Intelligence, v.28 n.6, p.863-876, June 2006.

[34] David K. Wagg, Mark S. Nixon, Automated markerless extraction of walking people using deformable contour models: Research Articles, Computer Animation and Virtual Worlds, v.15 n.3-4, p.399-406, July 2004.

[35] C. Yam, M. Nixon, and J. Carter, "Automated person recognition by walking and running via model-based approaches," Pattern Recognition., vol. 37, no. 5, pp. 1057-1072, May 2004.

[36] A. I. Bazin and M. S. Nixon, "Probabilistic combination of static and dynamic gait features for verification," in Proc. Biometric Technol. Human Identification II, SPIE Defense Security Symp., 2005, vol. 5779, pp. 23-30.

[37] James B. Hayfron-Acquah , Mark S. Nixon , John N. Carter, Automatic gait recognition by symmetry analysis, Pattern Recognition Letters, vol.24 no.13, pp.2175-2183, September 2003.

[38] G. Veres, L. Gordon, J. N. Carter, and M. Nixon, "What image information is important in silhouette-based gait recognition?" in Proc. IEEE Conf. Comput. Vis. Pattern Recog., 2004, vol. 2, pp. 776-782.

[39] L. Wang , T. Tan , H. Ning, W. Hu, Silhouette Analysis-Based Gait Recognition for Human Identification, IEEE Transactions on Pattern Analysis and Machine Intelligence, v.25 n.12, p.1505-1518, December 2003.

[40] F. Monrose, M.K. Reiter, and S. Wetzel, Password Hardening Based on Keystroke Dynamics, International Journal of Information Security Volume 1, Number 2 / February, 2002, pp. 69-83.

[41] E. S. Bigun, J. Bigun, B. Duc, and S. Fischer, "Expert conciliation for multi-modal person authentication systems by Bayesian statistics," In Proceedings Int. Conf. On Audio Video-Based Personal Authentication, pp. 327-334, Crans-Montana, Switzerland, 1997.

[42] R. Brunelli and T. Poggio, "Face recognition: Features versus templates," IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 15, No. 10,pp. 1042-1052, 1993.

[43] U. Dieckmann, P. Plankensteiner, and T. Wagner, "SESAM: A biometric person identification system using sensor fusion," Pattern Recognition Letters, Vol. 18, No. 9, pp. 827-833, 1997.

[44] J. Kittler, Y. Li, J. Matas, and M. U. Sanchez, "Combining evidence in multimodal personal identity recognition systems," In Proceedings International Conference on Audio Video-Based Personal Authentication, pp. 327-344, Crans-Montana, Switzerland, 1997.

[45] Claus Vielhauer, Funda mentals in Biometrics: Automated Processing of Bodily Measurements 1568-2633 Volume 18, in Advances in Information Security, Springer US, Pages11-31.

[46] L. Rila, Denial of Access in Biometrics-Based Authentication Systems, in G. Davida, Y. Frankel and O. Rees (Eds.): InfraSec 2002, LNCS 2437, pp. 19–29, 2002.

[47] Arun Ross and Anil Jain, Biometric Sensor Interoperability: A Case Study in Fingerprints Appeared in Proc. of International ECCV Workshop on Biometric Authentication (BioAW), (Prague, Czech Republic), LNCS Vol. 3087, pp. 134-145, Springer Publishers, May 2004.

[48] Ann Cavoukian, Alex Stoianov, Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security and Privacy, March 2007.

[49] Bimbot et al, A Tutorial on Text-Independent Speaker Verification, EURASIP Journal on Applied Signal Processing 2004:4, 430–451.

[50] Juliet Lodge, eJustice, Security and Biometrics: the EU's Proximity Paradox, European Journal of Crime, Criminal Law and Criminal Justice, Vol. 13/4, 533–564, 2005.

[51] Ishwar K Sethi, Biometrics: Overview and Applications in, Katherine Jo Strandburg, Daniela Stan Raicu (Eds.) Privacy and technologies of identity: a cross-disciplinary conversation 2006, XV, 383 (pp 117 - 134).

[52] Businesswire,[online].Available: http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20091217005401&newsLang=en

[53] Nalini K. Ratha, Jonathan H. Connell, Ruud M. Bolle, Biometrics break-ins and band-aids, Pattern Recognition Letters 24 (2003) 2105–2113

[54] Anil K. Jain and Arun Ross, Multibiometric Systems, Communications of the ACM, January 2004/Vol. 47, No. 1.

[55] R.M. Bolle, J.H. Connell and N.K. Ratha, Biometric perils and patches, *Pattern Recognition Vol 35, No12* December 2002.

[56] J. P. Campbell, "Speaker Recognition: A Tutorial." Proceedings of the IEEE, Vol. 85, No.9, pp. 1437-1462, 1997

[57] B.S. Atal, Effectiveness of linear prediction characteristics of the speech wave for automatic speaker identification and verification, J. Acoust. Soc. Am. 55 (Part 6) (1974) 1304–1312

[58] Stephan Grashey and Matthias Schuster, Multiple Biometrics: in SmartKom: Foundations of Multimodal Dialogue Systems, Springer Berlin Heidelberg, ISBN 978-3-540-23732-7 (Print) 978-3-540-36678-2 (Online), pp 181-193

[59] J.D. Markel, S.B. Davis, Text-independent speaker recognition from a large linguistically unconstrained time-spaced database, IEEE Trans. Acoust. Speech Signal Process. ASSP-27 (1) (1979) 74–82

[60] Lisa Myers, An Exploration of Voice Biometrics, SANS institute, 2004

[61] George S. Kang, Yvette Lee, Voice Biometrics for Information Assurance Applications, Naval Research Laboratory, Washington, DC 20375-5320, NRL/FR/5550--02-10,044, December 5, 2002

[62] J.A. Atah, Gareth Howells, Score Normalisation of Voice Features for Template Free Biometric Encryption, the 2008 Multi-Conference in Computer Science, Information Technology, Computer Engineering, Control and Automation Technology, Orlando, Fl, USA, July 2008

[63] K. Nandakumar, Integration of multiple cues in biometric systems, PhD thesis, Michigan State University, 2005.

[64] F. Deravi and M. Lockie "Biometric Industry Report - Market and Technology Forecasts to 2003", *Elsevier Advanced Technology*, December 2000.

[65] W. G. J. Howells, H. Selim, S. Hoque, M. C. Fairhurst, and F.Deravi. An Autonomous Document Object (ADO) Model. *In Proceedings of the 6th International Conference on Document Analysis and Recognition* (ICDAR 2001), 977-981, Seattle, Washington, USA. September 2001.

[66] S. Hoque, H. Selim, G. Howells, M. C. Fairhurst, and F. Deravi. "SAGENT: A Novel Technique for Document Modeling for Secure Access and Distribution. *In Proceedings of the 7th International Conference on Document Analysis and Recognition* (ICDAR 2003), Edinburgh, Scotland, UK.

[67] W. Sheng, G. Howells, M.C. Fairhurst,and F. Deravi, Template-free Biometric Key Generation by means of Fuzzy Genetic Clustering, Information Forensics and Security, Vol. 3, No. 2. (2008), pp. 183-191.

[68] G. Howells, H. Selim, M. C. Fairhurst, F. Deravi, and S. Hoque. "SAGENT: A Model for Security of Distributed Multimedia". *Submitted to IEEE Transactions on System, Man and Cybernetics.*

[69] A. F. R. Rahman and M .C. Fairhurst: "Enhancing multiple expert decision combination strategies through exploitation of a priori information sources", *IEE Proc. on Vision, Image and Signal Processing*, 146, 1-10, 1999

[70] K.Sirlantzis, S.Hoque, and M.C.Fairhurst, "Trainable multiple classifier schemes for handwritten character recognition, Proc. *3rd Int. Workshop on Multiple Classifier Systems*, Cagliari, Italy, 169-178

[71] C.C. Chibelushi, J.S.D Mason and F.Deravi, "Audio-Visual Person Recognition: An Evaluation of Data Fusion Strategies", *Proc. European Conference on Security, London*, 28-30 April 1997, IEE, pp 26-30

[72] A.K. Jain, S Prabakar and A. Ross, Biometrics Based Web Access. *Technical Report TR98-33*, Michigan State University, 1998.

[73] G.I.Davida et al, On the relation of error correction and cryptography to an offline biometric based identification scheme. *In Proceedings of WCC99, Workshop on Coding and Cryptography*, 1999.

[74] M Peyravian, S M Matyas, A Roginsky and N Zunic, Generating user-based cryptographic keys and random numbers, *Computers and Security*, Vol 18, No 7, pp 619-626, 1999.

[75] H.O. Nyongesa, S. Al-Khayatt, S.M. Mohamed and M. Mahmoud, Fast robust fingerprint fe ature extraction and classification, Journal of Intelligent and Robotic Systems 40 (1): 103-112 May 2004.

[76] Abdul Wahab, Gock See Ng, Romy Dickiyanto, Speaker authentication system using soft computing approaches, Neurocomputing Volume 68, October 2005, Pages 13-37.

[77] T. Hirsimaki, A Decoder for Large-Vocabulary Continuous Speech Recognition, Master's Thesis, Helsinki University of Technology, 2002, pp. 11–15.

[78] Cochran, W et al, What is the fast Fourier transform?, in: IEEE Transactions on Audio and Electroacoustics, Volume 15 Issue 2, Jun 1967, pp: 45 - 55

[79] *Weizhong Zhu and Douglas O'Shaughnessy,* Log-Energy Dynamic Range Normalizaton for Robust Speech Recognition, INRS-EMT, University of Quebec 800 De la Gauchetiere West, Montreal, Quebec, H5A 1K6, Canada.

[80] Waleed H. Abdulla, Robust speaker modelling using perceptually motivated feature, Pattern Recognition Letters 28 (2007) 1333–1342.

[81] A. Subramanya, Zhengyou Zhang, A.C. Surendran, P. Nguyen, Narasimhan, M.; Acero, A. (2007). A Generative-Discriminative Framework using Ensemble Methods for Text-Dependent Speaker Verification, in IEEE International Conference on Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. Volume 4, 15-20 April 2007 Page(s): IV-225 - IV-228.

[82] Engin Avci, A new optimum feature extraction and classification method for speaker recognition, Expert Systems with Applications Volume 32, Issue 2, February 2007, Pages 485-498

[83] Hisao Kuwabara and Yoshinori Sagisaka, Acoustic characteristics of speaker individuality: Control and conversion, Speech Communication 16 (1995) 165-173.

[84] Lindsay I Smith, A Tutorial on Principal Components Analysis, February 26, 2002.

[85] Jonathon Shlens, A Tutorial on Principal Component Analysis, Systems Neurobiology Laboratory, Salk Institute for Biological Studies La Jolla, CA 92037 and Institute for Nonlinear Science, University of California, San Diego La Jolla, CA 92093-0402, December 10, 2005; Version 2.

[86] J.A. Atah, Gareth Howells, Combining normalised voice features for use in efficient template - free biometric security system, the 2008 World Congress in Computer Science, Computer Engineering, and Applied Computing, Las Vegas, Nevada USA.

[87] J.A. Atah, Gareth Howells, Analysis of binary information in a voice based template-free biometric security system, International Association for development of information Society (IADIS) conference 2009, Algarve, Portugal.

[88] J.A. Atah, Gareth Howells, Mapping of Information in Voice Features for use in an Efficient Template - Free Biometric Security System, the 2009 International Conference on Information Security and Privacy (ISP-09), Orlando, FL, USA.

[89] Norman Poh, Samy Bengio, a study of the effect of score normalization prior to fusion in Biometric Authentication Tasks, December 2004.

[90] Deborah Rumsey (2003), *Statistics for Dummies,* Indiana: Wiley publishing Inc.

[91] A. koutsoyiannis, *Theory of Econometrics*, 2nd ed, New York: Palgrave.

[92] Multimedia Programming Interface and Data Specifications 1.0 Issued as a joint design by IBM Corporation and Microsoft Corporation August 1991

[93] B.P. Bogert, M.J.R. Healy, J.W. Tukey, The frequency analysis of time-series for echoes, Proc. Symp. Time Series Analysis (1963) 209–243.

[94] The Realistic Multi-modal VALID database, University College, Dublin [online]. Available: http://ee.ucd.ie/validdb/datasets.html

[95] YOHO Speaker Verification, Linguistic Data Consortium, University of Pennsylvania[Online]. Available:http://www.ldc.upenn.edu/Catalog/CatalogEntry.jsp?catalogId=LDC94S16

[96] Gary C. Kessler, An Overview of Cryptography, in Handbook on Local Area Networks, Auerbach (September 1998)

[97] E. Papoutsis, G. Howells, A. Hopkins, K. McDonald-Maier, Integrating Multimodal Circuit Features Within an Efficient Encryption System, 3rd International Symposium on Information Assurance and Security, 2007

[98] G. Howells, E. Papoutsis, A. Hopkins, K. McDonald-Maier, Normalizing Discrete Circuit Features with Statistically Independent Values for Incorporation within a highly Secure Encryption System, 2nd NASA/ESA conference on Adaptive Hardware and Systems (AHS), 2007

[99] E. Papoutsis, G. Howells, A. Hopkins, K. McDonald-Maier, Ensuring data integrity via ICmetrics based security infrastructure, 2nd NASA/ESA conference on Adaptive Hardware and Systems (AHS), 2007

[100] E. Papoutsis, G. Howells, A. Hopkins, K. McDonald-Maier, Key Generation for secure Inter-Satellite Communication, 2nd NASA/ESA conference on Adaptive Hardware and Systems (AHS), 2007

[101] Fernando Huenupa'n, Nestor Becerra Yoma, Carlos Molina, Claudio Garreto'n, Confidence based multiple classifier fusion in speaker verification, Pattern Recognition Letters 29 (2008) 957–966

[102] Douglas A. Reynolds, Experimental Evaluation of Features for Robust Speaker Identification, IEEE transactions on speech and audio processing. vol. 2, no. 4, October 1994

[103] George R. Doddington, Speaker Recognition- Identifying People by their Voices, proceedings of the IEEE, VOL 73, NO. 11, NOVEMBER 1985

[104] A. J. Menezes, P. C. van Oorschot and Scott A. Vanstone: Handbook of Applied Cryptography. CRC Press, 1996.

[105] C. Ellison, C Hall, R Milbert and B Schneier, "Protecting secret keys with personal entropy", *Future Generation Computer Systems*, Vol 16, No 4, pp 311-318, February 2000.

[106] B Schneier, Applied Cryptography, 2nd Edition, John Wiley & Sons Inc., 1996.

[107] G. Davida, Y. Frankel, and B.J. Matt, On Enabling Secure Applications through off-Line Biometrics Identification, Proc. Symp. Privacy and Security, pp. 148-157, 1998.

[108] J.A. Atah, Gareth Howells, Calibration and Operation in a Voice Based Template Free Biometric Security System, to appear in EURASIP journal of signal processing.

[109] J.A. Atah, Gareth Howells, Key Generation in a Voice Based Template Free Biometric Security System, Joint COST 2101 & 2102 International Conference on Biometric ID Management and Multimodal Communication 2009, Madrid, Spain, September 2009.

[110] R. M. Bolle, J.H. Connell and N.K. Ratha, Biometric perils and patches, Pattern Recognition Volume 35, Issue 12, December 2002, Pages 2727-2738

[111] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B.V.K. Vijaya Kumar, "Biometric Encryption," ICSA Guide to Cryptography, McGraw-Hill, 1999

[112] P. N. Belhumeur, et al, "Eigenfaces versus fisherfaces: recognition using class specific linear projection," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 9, no. 7, pp. 711–720, 1997.

[113] M. Savvides and B. V. K. Vijaya Kumar, "Cancellable biometric filters for face recognition," in Proceedings of the IEEE International Conference Pattern Recognition (ICPR '94), vol. 3, pp. 922–925, Cambridge, UK, August 2004.

[114] W.K. Yip, A. Gog, A. Goh, D.C.L. Ngo, and A.B.J. Teoh, Cryptographic keys from Dynamic Hand Signatures with Biometric secrecy preservation and replaceability, fourth IEEE International conference on Automatic Identification Advanced technology pp. 27- 31, 2005.

[115] J.A. Atah, Gareth Howells, Integrating Revocable Biometrics within a voice based Template-Free Biometric Security System, the 2009 International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV '09), World Congress in Computer Science, Computer Engineering, and Applied Computing, Las Vegas, Nevada USA.

[116] N. A. Fox, B. O'Mullane, & R. B. Reilly, The realistic multi-modal VALID database and visual speaker identification comparison experiments. Paper presented at the 5th International Conference on Audio and Video-Based Biometric Person Authentication, (2005).

[117] Derek J. Shiell, Louis H. Terry, Petar S. Aleksic, Aggelos K. Katsaggelos, An automated system for visual biometrics, Forty-Fifth Annual Allerton Conference Allerton House, UIUC, Illinois, USA September 26-28, 2007

[118] Reilly R.B, Fox N.A. Conference (International) June 2005, Speaker Identification based on Automatic Crossmodal Fusion of Audio and Visual Data, Proceedings of the 6th Annual Meeting of International Multisensory Research Forum, Trento, Italy

[119] Fox N Mullane B., Reilly R.B Conference, Audio-Visual Speaker Identification via Automatic Fusion using Reliability Estimates of both Modalities (International) July 2005, Proc. of the 5th International Conference on Audio-and Video-Based Biometric Person Authentication, Tarrytown, New York.

[120] Nestor Becerra Yoma, Tarciano Facco Pegoraro, Robust speaker verification with state duration modeling, Speech Communication 38 (2002) 77–88

[121] Douglas A. Reynolds and Richard C. Rose, Robust Text-Independent Speaker Identification Using Gaussian Mixture Speaker Models, IEEE transactions on speech and audio processing, vol. 3, NO. 1. January 1995

[122] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proceedings of 6th ACM Conference on Computer and Communications Security (ACM CCS '99)*, pp. 28–36, Singapore, November 1999.

[123] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proceedings of the IEEE International Symposium on Information Theory*, p. 408, Piscataway, NJ, USA, June-July 2002.

[124] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G.-J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis, "Practical biometric authentication with template protection," in *Proceedings of the 5th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA '05)*, vol. 3546 of *Lecture Notes in Computer Science*, pp. 436–446, Hilton Rye Town, NY, USA, July 2005.

[125] S. C. Draper, A. Khisti, E.Martinian, A. Vetro, and J. S. Yedidia, "Using distributed source coding to secure fingerprint biometrics," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '07)*, vol. 2, pp. 129–132, Honolulu, Hawaii, USA, April 2007.

[126] X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky, and A. Smith, Secure remote authentication using biometric data, advances in Cryptology EUROCRYPT, 2005.

[127] K. Nandakumar, A. Nagar, and A. K. Jain, "Hardening fingerprint fuzzy vault using password," in Proceedings of 2nd International Conference on Biometrics, pp. 927–937, Seoul, South Korea, August 2007.

[128] 2006 Frost and Sullivan, *Leading European Financial Institution Implements Voice Verification Biometrics to Enrich Customer Experience.* [online]. Available: http://www.frost.com/srch/content-search.do?srchid=191687796

[129] http://biosecure.it-sudparis.eu/AB/

[130] Karl Harmer, Evaluation of Candidate Fingerprint Features for Employment within Template-Free Biometric Cryptosystems, PhD. Thesis, University of Kent, 2009

[131] Evangelos Papoutsis, Investigation of the potential of generating encryption keys for ICmetrics, PhD. Thesis, University of Kent, 2010

[132] Gérard Maral (2003), VSAT Networks, John Wiley and Sons. ISBN 0470866845

[133] MyCrypto.net. Encryption Algorithms. Online. Available: http://www.mycrypto.net/encryption/crypto_algorithms.html (June 11, 2004)

[134] S. Hoque, M. Fairhurst, G. Howells and F. Deravi, Feasibility of generating biometric encryption keys, ELECTRONICS LETTERS 17th March 2005 Vol. 41 No. 6

[135] N. Lalithamani and K.P. Soman, An Effective Scheme for Generating Irrevocable Cryptographic Key from Cancelable Fingerprint Templates, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.3, March 2009

[136] B. Chen and V. Chandran, Biometric Based Cryptographic Key Generation from Faces, 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, pp:394 - 401, 3-5 Dec, 2007

[137] Gang Zheng, Wanqing Li and Ce Zhan, Cryptographic Key Generation from Biometric Data Using Lattice Mapping, The 18th International Conference on Pattern Recognition (ICPR'06

[138] Fabian Monrose Michael K. Reiter Qi Li Susanne Wetzel, Cryptographic Key Generation from Voice (Extended Abstract), In Proceedings of the 2001 IEEE Symposium on Security and Privacy, May 2001

[139] Yip Wai Kuan, Alwyn Goh, David Ngo CL, Andrew Teoh BJ, Cryptographic Keys from Dynamic Hand-signatures with Biometric Secrecy Preservation and Replaceability, Fourth IEEE Workshop on Automatic Identification Advanced Technologies, 2005.

[140] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith, Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data, EUROCRYPT 2004, LNCS 3027, pp. 523–540, 2004. © International Association for Cryptologic Research 2004

[141] Umut Uludag, Sharath Pankanti, Salil Prabhakar, and Anil k. Jain, Biometric Cryptosystems: Issues and Challenges, Proceedings of the IEEE, vol. 92, No. 6, June 2004

[142] Lívia C. F. Araújo, Luiz H. R. Sucupira Jr., Miguel G. Lizárraga, Lee L. Ling, and João B. T. Yabu-uti, User Authentication through Typing Biometrics Features in D. Zhang and A.K. Jain (Eds.): ICBA 2004, LNCS 3072, pp. 694-700, 2004. © Springer-Verlag Berlin Heidelberg 2004

[143] *Fabian Monrose, Michael K. Reiter, Qi Li, Susanne Wetzel,* Using Voice to Generate Cryptographic Keys, In Proc. of Odyssey 2001, The Speaker Verification Workshop

[144] C. R. Costanzo. Biometric cryptography: Key generation using feature and parametric aggregation. Online Technical Report, 2004.

[145] R. N. Forthofer, E.S. Lee, M. Hernandez, Biostatistics: A Guide to Design, Analysis, and Discovery, 2007 Elsevier, ISBN 13:978-0-12-369492-8

[146] S. Sanderson, Automatic Person Verification Using Speech and Face Information, PhD thesis, Griffith University, Brisbane, Australia, 2002

[147] Biometrics in Healthcare [online]. Available: http://www.findbiometrics.com/health-care

[148] Alice Osborn, How biometric technology is used in video surveillance, [online]. Available: http://www.video-surveillance-guide.com/biometric-technology.htm, August 17, 2005

[149] J.A. Atah, Gareth Howells, Revocability of biometric keys generated from a voice based template-free biometric system, to appear in Engineering Letters Manuscript Number: EL_2009_12_17a. Manuscript submitted 17 December 2009, accepted 20 April 2010, final camera ready copy submitted 19 June 2010

[150] Michel Neuhaus and Horst Bunke, An Error-Tolerant Approximate Matching Algorithm for Attributed Planar Graphs and Its Application to Fingerprint Classification, in A. Fred et al. (Eds.): SSPR&SPR 2004, LNCS 3138, pp. 180–189, 2004, Springer-Verlag Berlin Heidelberg 2004

[151] Jiangang Cheng, Jie Tian, Hong Chen, Qun Ren, Xin Yang, Fingerprint Enhancement Using Oriented Diffusion Filter, in J. Kittler and M.S. Nixon (Eds.): AVBPA 2003, LNCS 2688, pp. 164-171, 2003. (c) Springer-Verlag Berlin Heidelberg 2003

[152] G. Fouquier, L. Likforman, J. Darbon, and B. Sankur, "The biosecure geometry-based system for hand modality", Proc. IEEE ICASSP, Honolulu, Hawai, USA, 2007, pp. I801-I804.

[153] Juan Manuel Ramirez-Cortes et al, A Feature Extraction Method Based on the Pattern Spectrum for Hand Shape Biometry, in Proceedings of the World Congress on Engineering and Computer Science 2008, WCECS 2008, October 22 - 24, 2008, San Francisco, USA

[154] John Daugman, High confidence visual recognition of persons by a test of statistical independence, IEEE transactions on pattern analysis and machine intelligence, vol. 15, No. 11, November 1993

[155] John Daugman, New Methods in Iris Recognition, IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics, vol. 37, no. 5, October 2007

[156] Azlinah Mohamed et al, Baseline Extraction Algorithm for Online Signature Recognition, WSEAS transactions on systems, Issue 4, Volume 8, April 2009

[157] Felicia Soedjianto1, Lukas Dwi Kristianto, Rudy Adipranata, Signature Recognition with Dominant Point Method,

[158] Md. Itrat Bin Shams, Signature Recognition by Segmentation and Regular Line Detection, TENCON 2007 - 2007 IEEE Region 10 Conference, Oct. 30 2007-Nov. 2 2007

[159] Reza Ebrahimpour, Ali Amiri, Masoom Nazari and Alireza Hajiany, Robust Model for Signature Recognition Based on Biological Inspired Features, International Journal of Computer and Electrical Engineering, Vol. 2, No. 4, August, 2010, 1793-8163

[160] H. B. Kekre, V. A. Bharadi, and A. A. Ambardekar, "Novel and simple contour technique for signature recognition,"National Conference of Communication and Signal Processing 2007 (NCCSP 2007), Mumbai, India, 2007

[161] Usability Doroteo T. Toledano et al, evaluation of multi-modal biometric verification systems, Interacting with Computers 18 (2006) 1101–1122

[162] Li Yuan, Zhichun Mu, and Zhengguang Xu, Using Ear Biometrics for Personal Recognition, in S.Z. Li et al. (Eds.): IWBRS 2005, LNCS 3781, pp. 221–228, 2005. © Springer-Verlag Berlin Heidelberg 2005

[163] P. Yan and K. Bowyer, "Empirical evaluation of advanced ear biometrics," Proc. IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshop, pp. 41–48, 2005.

[164] Mahbubur Rahman et al, Person Identification Using Ear Biometrics, International Journal of The Computer, the Internet and Management Vol. 15#2 (May - August, 2007) pp 1 – 8

[165] Nageshkumar.M et al, An Efficient Secure Multimodal Biometric Fusion Using Palmprint and Face Image, IJCSI International Journal of Computer Science Issues, Vol. 2, 2009

[166] Michael Goh Kah Ong, Connie Tee and Andrew Teoh Beng Jin, Touch-Less Palm Print Biometric System, VISAPP 2008 - International Conference on Computer Vision Theory and Applications

[167] Davrondzhon Gafurov, Einar Snekkenes, and Tor Erik Buvarp, Robustness of Biometric Gait Authentication Against Impersonation Attack, R. Meersman, Z. Tari, P. Herrero et al. (Eds.): OTM Workshops 2006, LNCS 4277, pp. 479–488, 2006.

[168] Davrondzhon Gafurov, A Survey of Biometric Gait Recognition: Approaches, Security and Challenges, NIK-2007 conference

[169] Mary Villani et al, Keystroke Biometric Recognition Studies on Long-Text Input under Ideal and Application-Oriented Conditions, Proceedings of Student/Faculty Research Day, CSIS, Pace University, May 5th, 2006

[170] Ahmed Awad E Ahmed, Issa Traore, Ahmad Almulhem, Digital Fingerprinting Based on Keystroke Dynamics, Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008)

[171] Ravi Das, Retinal recognition: Biometric technology in practice, Keesing Journal of Documents & Identity, issue 22, 2007

[172] Hadi Farzin, Hamid Abrishami-Moghaddam, and Mohammad-ShahramMoin, A Novel Retinal Identification System, EURASIP Journal on Advances in Signal Processing, Volume 2008

[173] Li Ma, Yunhong Wang, Tieniu Tan, Iris Recognition Based on Multichannel Gabor Filtering, ACCV2002: The 5th Asian Conference on Computer Vision, 23--25 January 2002, Melbourne, Australia.

[174] Timothy J. Hazen, Eugene Weinstein, Bernd Heisele, Alex Park, and Ji Ming, Multi-Modal Face and Speaker Identification for Mobile Devices in Face Biometrics for Personal Identification: Multi-Sensory Multi-Modal Systems, edited by R. I. Hammoud, B. R. Abidi and M. A. Abidi., Springer, Berlin 2007.

[175] Engin Erzin, Yücel Yemez,, and A. Murat Tekalp, Multimodal Speaker Identification Using an Adaptive Classifier Cascade Based on Modality Reliability, IEEE Transactions on Multimedia, VOL. 7, NO. 5, October 2005

[176] J. Montalvao Filho and E. Freire, "Multimodal biometric Fusion- Joint typist (keystroke) and speaker verification," in Telecommunications Symposium, 2006 International, 2006, pp. 609–614.

[177] P. T. Blythe, Improving public transport ticketing through smart cards, Proceedings of the Institution of Civil Engineers, Municipal Engineer 157, March 2004 Issue ME1, Pages 47–54

[178] T. Parsons, Voice and Speech Processing, Communications and Signal Processing, S. Director, Series Ed. New York: McGraw-Hill, 1987.

[179] Hyung-Keun Jee, Sung-Uk Jung, and Jang-Hee Yoo, Liveness Detection for Embedded Face Recognition System, World Academy of Science, Engineering and Technology 18 2006

[180] Bori Toth, Deloitee, Biometric Liveness Detection, Information Security Bulletin, Volume 10, October 2005

[181] Xiaoyang Tan, Yi Li, Jun Liu and Lin Jiang, Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model, COMPUTER VISION – ECCV 2010, Lecture Notes in Computer Science, 2010, Volume 6316/2010, 504-517

[182] Judith A. Markowitz, Voice Biometrics, Communications of the ACM, September 2000/Vol. 43, No. 9

[183] Brian E. D. Kingsbury, Perceptually Inspired Signal-processing Strategies for Robust Speech Recognition in Reverberant Environments, PhD thesis, University of California, Berkeley, 1989

[184] Giridharan, K.; Smolenski, B.Y.; Yantorno, R.E., Statistical and model based approach to unvoiced speech detection, in Proceedings of 2004 International Symposium on Intelligent Signal Processing and Communication Systems, 2004. ISPACS 2004. pp 816 – 821

[185] E. Givelberg, J. J. Bunn, and M. Rajan. Detailed simulation of the cochlea: Recent progress using large shared memory parallel computers. In Proceedings of the 2001 International Mechanical Engineering Congress, New York, November 2001.

[186] Mohamad O. Diab, Amira El-Merhie, Nour El-Halabi, Layal Khoder, Classification of uterine EMG signals using supervised classification method, J. Biomedical Science and Engineering, 2010, 3, 837-842

[187] Kaveh Mollazade, Hojat Ahmadi, Mahmoud Omid, Reza Alimardani, An Intelligent Combined Method Based on Power Spectral Density, Decision Trees and Fuzzy Logic for Hydraulic Pumps Fault Diagnosis, International Journal of Intelligent Systems and Technologies 3:4 2008

[188] Matlab Documentation (http://www.mathworks.com)

[189] Frank R. Kschischang, The Hilbert Transform, The Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, October 22, 2006

[190] NIST/SEMATECH e-Handbook of Statistical Methods, http://www.itl.nist.gov/div898/handbook/

[191] Herong Yang, Herong's Tutorial Notes on CD/DVD, Version 2.14, 2007

[192] S.C. Pei and H.S. Lin, "Minimum-phase fir filter design using real cepstrum," Circuits and Systems II: Express Briefs, IEEE Transactions on, vol. 53, no. 10, pp. 1113–1117, October 2006.

[193] Neil Daswani, Christoph Kern, and Anita Kesavan, Foundations of Security: What every programmer needs to know, ISBN 1590597842

Appendix 1

10 X 10 Covariance Matrix for the 106 samples

	A	B	C	D	E	F	G	H	I	J
A	5.89E-11	2.96E-08	4.02E-08	-1.06E-08	-1.19E-06	-1.18E-04	-1.35E-09	3.79E-09	1.13E-10	-1.88E-13
B	2.96E-08	2.33E-03	-1.72E-03	4.06E-03	2.15E-02	3.98E-01	1.02E-05	2.56E-04	8.88E-06	1.47E-09
C	4.02E-08	-1.72E-03	2.41E-03	-4.13E-03	-3.23E-02	-1.23E+00	-1.95E-05	-2.23E-04	-8.83E-06	-3.21E-09
D	-1.06E-08	4.06E-03	-4.13E-03	8.19E-03	5.37E-02	1.63E+00	2.97E-05	4.78E-04	1.77E-05	4.68E-09
E	-1.19E-06	2.15E-02	-3.23E-02	5.37E-02	7.09E-01	3.15E+01	4.22E-04	3.65E-03	1.53E-04	7.23E-08
F	-1.18E-04	3.98E-01	-1.23E+00	1.63E+00	3.15E+01	1.23E+04	2.08E-02	6.07E-01	1.23E-02	2.57E-06
G	-1.35E-09	1.02E-05	-1.95E-05	2.97E-05	4.22E-04	2.08E-02	1.19E-06	9.71E-07	5.49E-08	1.04E-10
H	3.79E-09	2.56E-04	-2.23E-04	4.78E-04	3.65E-03	6.07E-01	9.71E-07	1.19E-04	2.69E-06	1.09E-10
I	1.13E-10	8.88E-06	-8.83E-06	1.77E-05	1.53E-04	1.23E-02	5.49E-08	2.69E-06	7.69E-08	9.02E-12
J	-1.88E-13	1.47E-09	-3.21E-09	4.68E-09	7.23E-08	2.57E-06	1.04E-10	1.09E-10	9.02E-12	4.09E-14

Covariance Matrix Table

AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ
BA	BB	BC	BD	BE	BF	BG	BH	BI	BJ
CA	CB	CC	CD	CE	CF	CG	CH	CI	CJ
DA	DB	DC	DD	DE	DF	DG	DH	DI	DJ
EA	EB	EC	ED	EE	EF	EG	EH	EI	EJ
FA	FB	FC	FD	FE	FF	FG	FH	FI	FJ
GA	GB	GC	GD	GE	GF	GG	GH	GI	GJ
HA	HB	HC	HD	HE	HF	HG	HH	HI	HJ
IA	IB	IC	ID	IE	IF	IG	IH	II	IJ
JA	JB	JC	JD	JE	JF	JG	JH	JI	JJ

Legend

A=Mean Amplitude
B=Maximum Amplitude
C=Minimum Amplitude
D=Peak to Peak Amplitude
E=Mean Frequency
F=Maximum Frequency
G=Minimum Frequency
H=Maximum PSD
I=mean PSD
J=Minimum PSD

Covariance Matrix for Speaker x0

	A	B	C	D	E	F	G	H	I	J
A	8.13E-10	-8.28E-07	7.47E-07	-1.58E-06	-1.30E-05	-8.02E-04	3.66E-09	6.71E-10	-1.17E-09	-1.13E-12
B	-8.28E-07	3.30E-03	-3.30E-03	6.60E-03	4.39E-02	2.89E+00	1.62E-05	1.60E-04	6.31E-06	3.32E-09
C	7.47E-07	-3.30E-03	3.30E-03	-6.60E-03	-4.46E-02	-3.14E+00	-1.78E-05	-1.68E-04	-6.41E-06	-3.19E-09
D	-1.58E-06	6.60E-03	-6.60E-03	1.32E-02	8.84E-02	6.03E+00	3.40E-05	3.28E-04	1.27E-05	6.51E-09
E	-1.30E-05	4.39E-02	-4.46E-02	8.84E-02	6.57E-01	6.94E+01	2.15E-04	3.00E-03	9.26E-05	3.54E-08
F	-8.02E-04	2.89E+00	-3.14E+00	6.03E+00	6.94E+01	2.19E+04	1.80E-02	1.03E+00	1.39E-02	-2.36E-06
G	3.66E-09	1.62E-05	-1.78E-05	3.40E-05	2.15E-04	1.80E-02	1.97E-07	1.10E-06	3.48E-08	9.78E-12
H	6.71E-10	1.60E-04	-1.68E-04	3.28E-04	3.00E-03	1.03E+00	1.10E-06	6.27E-05	8.18E-07	-6.52E-11
I	-1.17E-09	6.31E-06	-6.41E-06	1.27E-05	9.26E-05	1.39E-02	3.48E-08	8.18E-07	1.69E-08	4.19E-12
J	-1.13E-12	3.32E-09	-3.19E-09	6.51E-09	3.54E-08	-2.36E-06	9.78E-12	-6.52E-11	4.19E-12	5.10E-15

Covariance Matrix for Speaker x1

	A	B	C	D	E	F	G	H	I	J
A	2.06E-11	-4.21E-08	3.36E-08	-7.57E-08	-3.57E-07	1.15E-04	4.29E-10	3.48E-09	8.25E-11	2.37E-14
B	-4.21E-08	7.44E-04	-3.38E-04	1.10E-03	9.50E-03	8.51E-02	1.22E-05	1.86E-05	6.55E-07	3.68E-10
C	3.36E-08	-3.38E-04	2.50E-04	-5.88E-04	-6.30E-03	9.46E-02	-5.98E-06	2.77E-06	-1.71E-07	-2.15E-10
D	-7.57E-08	1.10E-03	-5.88E-04	1.70E-03	1.58E-02	-9.60E-03	1.82E-05	1.58E-05	8.26E-07	5.84E-10
E	-3.57E-07	9.50E-03	-6.30E-03	1.58E-02	2.52E-01	4.67E+00	3.79E-04	2.79E-04	1.81E-05	1.41E-08
F	1.15E-04	8.51E-02	9.46E-02	-9.60E-03	4.67E+00	9.68E+02	1.63E-02	4.41E-02	1.30E-03	6.09E-07
G	4.29E-10	1.22E-05	-5.98E-06	1.82E-05	3.79E-04	1.63E-02	7.20E-07	9.22E-07	4.01E-08	2.66E-11
H	3.48E-09	1.86E-05	2.77E-06	1.58E-05	2.79E-04	4.41E-02	9.22E-07	2.77E-06	7.29E-08	3.04E-11
I	8.25E-11	6.55E-07	-1.71E-07	8.26E-07	1.81E-05	1.30E-03	4.01E-08	7.29E-08	2.55E-09	1.45E-12
J	2.37E-14	3.68E-10	-2.15E-10	5.84E-10	1.41E-08	6.09E-07	2.66E-11	3.04E-11	1.45E-12	1.01E-15

Covariance Matrix for Speaker x2

	A	B	C	D	E	F	G	H	I	J
A	1.68E-11	7.66E-08	6.19E-09	7.04E-08	-1.05E-06	-1.20E-05	5.48E-10	2.45E-08	4.56E-10	3.75E-15
B	7.66E-08	4.50E-04	-3.51E-05	4.86E-04	-1.70E-03	2.33E-04	1.79E-06	1.30E-04	2.75E-06	4.10E-11
C	6.19E-09	-3.51E-05	9.34E-05	-1.29E-04	-2.60E-03	-1.22E-01	6.14E-07	8.93E-06	5.55E-08	-6.24E-13
D	7.04E-08	4.86E-04	-1.29E-04	6.14E-04	9.44E-04	1.23E-01	1.17E-06	1.21E-04	2.70E-06	4.16E-11
E	-1.05E-06	-1.70E-03	-2.60E-03	9.44E-04	1.65E-01	2.93E+00	-6.15E-05	-1.10E-03	-1.18E-05	3.22E-10
F	-1.20E-05	2.33E-04	-1.22E-01	1.23E-01	2.93E+00	1.74E+02	-6.99E-04	-2.53E-02	-4.53E-04	-1.03E-08
G	5.48E-10	1.79E-06	6.14E-07	1.17E-06	-6.15E-05	-6.99E-04	3.73E-08	8.97E-07	1.53E-08	2.03E-13
H	2.45E-08	1.30E-04	8.93E-06	1.21E-04	-1.10E-03	-2.53E-02	8.97E-07	4.49E-05	9.36E-07	1.66E-11
I	4.56E-10	2.75E-06	5.55E-08	2.70E-06	-1.18E-05	-4.53E-04	1.53E-08	9.36E-07	2.08E-08	4.38E-13
J	3.75E-15	4.10E-11	-6.24E-13	4.16E-11	3.22E-10	-1.03E-08	2.03E-13	1.66E-11	4.38E-13	1.45E-17

Covariance Matrix for Speaker x3

	A	B	C	D	E	F	G	H	I	J
A	6.45E-11	-3.70E-07	3.59E-07	-7.29E-07	-4.94E-06	-2.41E-04	-7.34E-09	1.77E-08	-2.61E-10	-6.06E-13
B	-3.70E-07	4.40E-03	-4.50E-03	8.90E-03	4.19E-02	1.27E+00	6.17E-05	-1.21E-04	4.07E-06	5.27E-09
C	3.59E-07	-4.50E-03	4.70E-03	-9.20E-03	-4.38E-02	-1.39E+00	-5.39E-05	1.37E-04	-3.99E-06	-5.59E-09
D	-7.29E-07	8.90E-03	-9.20E-03	1.81E-02	8.57E-02	2.66E+00	1.16E-04	-2.58E-04	8.06E-06	1.09E-08
E	-4.94E-06	4.19E-02	-4.38E-02	8.57E-02	5.20E-01	3.01E+01	5.82E-04	-1.50E-03	4.26E-05	7.34E-08
F	-2.41E-04	1.27E+00	-1.39E+00	2.66E+00	3.01E+01	4.03E+03	2.06E-02	-1.95E-02	3.50E-03	6.01E-06
G	-7.34E-09	6.17E-05	-5.39E-05	1.16E-04	5.82E-04	2.06E-02	1.39E-06	-1.23E-06	6.25E-08	7.03E-11
H	1.77E-08	-1.21E-04	1.37E-04	-2.58E-04	-1.50E-03	-1.95E-02	-1.23E-06	8.50E-06	-1.10E-08	-1.44E-10
I	-2.61E-10	4.07E-06	-3.99E-06	8.06E-06	4.26E-05	3.50E-03	6.25E-08	-1.10E-08	6.87E-09	7.43E-12
J	-6.06E-13	5.27E-09	-5.59E-09	1.09E-08	7.34E-08	6.01E-06	7.03E-11	-1.44E-10	7.43E-12	1.19E-14

Covariance Matrix for Speaker x4

	A	B	C	D	E	F	G	H	I	J
A	1.89E-11	5.92E-08	1.26E-07	-6.65E-08	-2.18E-06	-5.65E-05	-9.80E-11	-1.87E-09	2.10E-11	-3.52E-13
B	5.92E-08	1.50E-03	-8.84E-04	2.40E-03	1.35E-02	8.21E-01	5.92E-06	7.15E-05	3.13E-06	1.80E-09
C	1.26E-07	-8.84E-04	2.30E-03	-3.20E-03	-3.60E-02	-8.91E-01	-2.33E-06	-9.11E-05	-3.32E-06	-5.57E-09
D	-6.65E-08	2.40E-03	-3.20E-03	5.60E-03	4.95E-02	1.71E+00	8.24E-06	1.63E-04	6.45E-06	7.37E-09
E	-2.18E-06	1.35E-02	-3.60E-02	4.95E-02	5.77E-01	1.77E+01	6.11E-05	1.40E-03	4.88E-05	8.88E-08
F	-5.65E-05	8.21E-01	-8.91E-01	1.71E+00	1.77E+01	1.72E+03	1.64E-02	5.35E-02	1.10E-03	2.18E-06
G	-9.80E-11	5.92E-06	-2.33E-06	8.24E-06	6.11E-05	1.64E-02	2.53E-07	2.64E-07	-2.92E-09	-1.06E-12
H	-1.87E-09	7.15E-05	-9.11E-05	1.63E-04	1.40E-03	5.35E-02	2.64E-07	4.72E-06	1.86E-07	2.12E-10
I	2.10E-11	3.13E-06	-3.32E-06	6.45E-06	4.88E-05	1.10E-03	-2.92E-09	1.86E-07	8.56E-09	7.65E-12
J	-3.52E-13	1.80E-09	-5.57E-09	7.37E-09	8.88E-08	2.18E-06	-1.06E-12	2.12E-10	7.65E-12	1.41E-14

Covariance Matrix for Speaker x5

	A	B	C	D	E	F	G	H	I	J
A	1.42E-11	5.06E-08	-4.02E-08	9.08E-08	-1.89E-07	1.78E-05	-7.37E-10	2.70E-09	5.70E-11	-9.38E-15
B	5.06E-08	9.81E-04	-9.60E-04	1.90E-03	9.50E-03	8.44E-01	-5.13E-08	1.77E-05	1.20E-06	1.14E-10
C	-4.02E-08	-9.60E-04	1.00E-03	-2.00E-03	-9.80E-03	-9.52E-01	-1.84E-06	-2.15E-05	-1.28E-06	-2.32E-11
D	9.08E-08	1.90E-03	-2.00E-03	3.90E-03	1.94E-02	1.80E+00	1.79E-06	3.92E-05	2.48E-06	1.38E-10
E	-1.89E-07	9.50E-03	-9.80E-03	1.94E-02	1.33E-01	9.04E+00	4.31E-05	7.89E-05	1.22E-05	1.80E-09
F	1.78E-05	8.44E-01	-9.52E-01	1.80E+00	9.04E+00	1.48E+03	2.20E-03	4.80E-03	8.42E-04	2.43E-07
G	-7.37E-10	-5.13E-08	-1.84E-06	1.79E-06	4.31E-05	2.20E-03	6.89E-08	2.61E-10	2.53E-09	-1.06E-12
H	2.70E-09	1.77E-05	-2.15E-05	3.92E-05	7.89E-05	4.80E-03	2.61E-10	1.31E-06	3.62E-08	-1.29E-11
I	5.70E-11	1.20E-06	-1.28E-06	2.48E-06	1.22E-05	8.42E-04	2.53E-09	3.62E-08	1.80E-09	-1.25E-13
J	-9.38E-15	1.14E-10	-2.32E-11	1.38E-10	1.80E-09	2.43E-07	-1.06E-12	-1.29E-11	-1.25E-13	2.56E-16

Covariance Matrix for Speaker x6

	A	B	C	D	E	F	G	H	I	J
A	1.96E-11	1.29E-07	-5.90E-08	1.88E-07	-5.66E-07	8.62E-06	8.11E-10	3.11E-08	5.78E-10	8.35E-15
B	1.29E-07	1.10E-03	-7.44E-04	1.90E-03	-4.70E-03	4.87E-01	5.56E-06	2.83E-04	5.29E-06	-1.00E-11
C	-5.90E-08	-7.44E-04	7.53E-04	-1.50E-03	2.10E-03	-6.24E-01	-2.54E-06	-2.00E-04	-3.90E-06	1.42E-10
D	1.88E-07	1.90E-03	-1.50E-03	3.40E-03	-6.80E-03	1.11E+00	8.10E-06	4.83E-04	9.19E-06	-1.52E-10
E	-5.66E-07	-4.70E-03	2.10E-03	-6.80E-03	2.81E-02	-3.73E-01	-2.44E-05	-1.10E-03	-2.03E-05	-5.07E-10
F	8.62E-06	4.87E-01	-6.24E-01	1.11E+00	-3.73E-01	1.15E+03	1.10E-03	1.46E-01	2.60E-03	-9.26E-08
G	8.11E-10	5.56E-06	-2.54E-06	8.10E-06	-2.44E-05	1.10E-03	3.46E-08	1.35E-06	2.47E-08	4.66E-13
H	3.11E-08	2.83E-04	-2.00E-04	4.83E-04	-1.10E-03	1.46E-01	1.35E-06	7.19E-05	1.35E-06	-8.68E-12
I	5.78E-10	5.29E-06	-3.90E-06	9.19E-06	-2.03E-05	2.60E-03	2.47E-08	1.35E-06	2.56E-08	-2.82E-13
J	8.35E-15	-1.00E-11	1.42E-10	-1.52E-10	-5.07E-10	-9.26E-08	4.66E-13	-8.68E-12	-2.82E-13	8.08E-17

Covariance Matrix for Speaker x8

	A	B	C	D	E	F	G	H	I	J
A	3.67E-11	2.69E-07	4.54E-08	2.24E-07	-1.71E-06	-2.50E-03	-3.53E-09	3.54E-11	-9.59E-14	-1.81E-13
B	2.69E-07	2.10E-03	6.32E-05	2.10E-03	-1.06E-02	-1.85E+01	-1.88E-05	-1.14E-05	3.00E-07	-9.21E-10
C	4.54E-08	6.32E-05	1.10E-03	-1.10E-03	-1.61E-02	-4.52E+00	-3.27E-05	6.78E-05	-7.50E-07	-1.48E-09
D	2.24E-07	2.10E-03	-1.10E-03	3.10E-03	5.50E-03	-1.40E+01	1.40E-05	-7.92E-05	1.05E-06	5.59E-10
E	-1.71E-06	-1.06E-02	-1.61E-02	5.50E-03	3.60E-01	2.67E+02	6.38E-04	1.70E-03	4.58E-05	2.68E-08
F	-2.50E-03	-1.85E+01	-4.52E+00	-1.40E+01	2.67E+02	4.04E+05	4.80E-01	4.78E+00	7.12E-02	2.13E-05
G	-3.53E-09	-1.88E-05	-3.27E-05	1.40E-05	6.38E-04	4.80E-01	1.26E-06	2.56E-06	8.23E-08	5.72E-11
H	3.54E-11	-1.14E-05	6.78E-05	-7.92E-05	1.70E-03	4.78E+00	2.56E-06	1.10E-04	1.48E-06	9.47E-11
I	-9.59E-14	3.00E-07	-7.50E-07	1.05E-06	4.58E-05	7.12E-02	8.23E-08	1.48E-06	2.27E-08	3.43E-12
J	-1.81E-13	-9.21E-10	-1.48E-09	5.59E-10	2.68E-08	2.13E-05	5.72E-11	9.47E-11	3.43E-12	2.73E-15

Covariance Matrix for Speaker x9

	A	B	C	D	E	F	G	H	I	J
A	3.11E-11	1.03E-07	-8.58E-08	1.88E-07	1.27E-06	1.32E-04	-6.79E-10	6.28E-08	1.34E-09	-3.19E-13
B	1.03E-07	5.03E-04	-2.50E-04	7.53E-04	2.20E-03	-2.47E-01	-3.93E-06	1.35E-04	3.67E-06	-2.91E-09
C	-8.58E-08	-2.50E-04	7.50E-04	-1.00E-03	-1.33E-02	-1.64E+00	-5.29E-06	-3.77E-04	-6.24E-06	-4.34E-09
D	1.88E-07	7.53E-04	-1.00E-03	1.80E-03	1.54E-02	1.40E+00	1.36E-06	5.13E-04	9.91E-06	1.43E-09
E	1.27E-06	2.20E-03	-1.33E-02	1.54E-02	2.69E-01	2.51E+01	1.35E-04	6.30E-03	9.97E-05	4.62E-08
F	1.32E-04	-2.47E-01	-1.64E+00	1.40E+00	2.51E+01	1.06E+04	1.18E-02	1.30E+00	1.81E-02	4.26E-05
G	-6.79E-10	-3.93E-06	-5.29E-06	1.36E-06	1.35E-04	1.18E-02	1.37E-07	1.40E-06	4.17E-09	4.95E-11
H	6.28E-08	1.35E-04	-3.77E-04	5.13E-04	6.30E-03	1.30E+00	1.40E-06	2.49E-04	4.17E-06	3.66E-09
I	1.34E-09	3.67E-06	-6.24E-06	9.91E-06	9.97E-05	1.81E-02	4.17E-09	4.17E-06	7.54E-08	3.91E-11
J	-3.19E-13	-2.91E-09	-4.34E-09	1.43E-09	4.62E-08	4.26E-05	4.95E-11	3.66E-09	3.91E-11	2.08E-13

Covariance Matrix for Speaker x10

	A	B	C	D	E	F	G	H	I	J
A	8.01E-11	2.29E-07	-3.37E-07	5.65E-07	-3.49E-07	-1.79E-04	1.29E-09	-1.21E-09	3.56E-10	-1.49E-13
B	2.29E-07	5.00E-03	-3.10E-03	8.10E-03	6.50E-03	-2.93E+00	3.76E-06	4.98E-05	8.71E-06	-1.50E-09
C	-3.37E-07	-3.10E-03	2.50E-03	-5.70E-03	-1.90E-03	1.97E+00	-5.81E-06	-2.79E-05	-5.47E-06	1.18E-09
D	5.65E-07	8.10E-03	-5.70E-03	1.38E-02	8.40E-03	-4.91E+00	9.57E-06	7.77E-05	1.42E-05	-2.68E-09
E	-3.49E-07	6.50E-03	-1.90E-03	8.40E-03	9.47E-02	-1.04E+01	-7.17E-05	-2.80E-03	-2.66E-05	-8.51E-09
F	-1.79E-04	-2.93E+00	1.97E+00	-4.91E+00	-1.04E+01	2.43E+03	2.80E-03	2.42E-01	-1.50E-03	1.68E-06
G	1.29E-09	3.76E-06	-5.81E-06	9.57E-06	-7.17E-05	2.80E-03	7.55E-08	2.37E-06	3.79E-08	3.69E-12
H	-1.21E-09	4.98E-05	-2.79E-05	7.77E-05	-2.80E-03	2.42E-01	2.37E-06	1.10E-04	1.56E-06	2.87E-10
I	3.56E-10	8.71E-06	-5.47E-06	1.42E-05	-2.66E-05	-1.50E-03	3.79E-08	1.56E-06	3.50E-08	1.41E-12
J	-1.49E-13	-1.50E-09	1.18E-09	-2.68E-09	-8.51E-09	1.68E-06	3.69E-12	2.87E-10	1.41E-12	1.41E-15

Covariance Matrix for Speaker x11

	A	B	C	D	E	F	G	H	I	J
A	5.96E-11	-3.36E-07	2.44E-07	-5.80E-07	-4.68E-06	-1.27E-04	-1.96E-09	-9.14E-09	-6.08E-10	-4.66E-13
B	-3.36E-07	2.40E-03	-2.30E-03	4.70E-03	4.07E-02	9.63E-01	3.10E-05	8.51E-05	5.31E-06	3.70E-09
C	2.44E-07	-2.30E-03	2.90E-03	-5.20E-03	-4.69E-02	-1.12E+00	-3.79E-05	-8.12E-05	-5.53E-06	-3.67E-09
D	-5.80E-07	4.70E-03	-5.20E-03	9.90E-03	8.76E-02	2.08E+00	6.89E-05	1.66E-04	1.08E-05	7.37E-09
E	-4.68E-06	4.07E-02	-4.69E-02	8.76E-02	7.97E-01	1.72E+01	6.88E-04	1.70E-03	1.02E-04	6.26E-08
F	-1.27E-04	9.63E-01	-1.12E+00	2.08E+00	1.72E+01	5.82E+02	1.30E-02	1.85E-02	1.80E-03	2.12E-06
G	-1.96E-09	3.10E-05	-3.79E-05	6.89E-05	6.88E-04	1.30E-02	1.80E-06	2.86E-06	1.34E-07	1.37E-10
H	-9.14E-09	8.51E-05	-8.12E-05	1.66E-04	1.70E-03	1.85E-02	2.86E-06	6.72E-06	3.04E-07	1.83E-10
I	-6.08E-10	5.31E-06	-5.53E-06	1.08E-05	1.02E-04	1.80E-03	1.34E-07	3.04E-07	1.57E-08	1.06E-11
J	-4.66E-13	3.70E-09	-3.67E-09	7.37E-09	6.26E-08	2.12E-06	1.37E-10	1.83E-10	1.06E-11	1.54E-14

Covariance Matrix for Speaker x12

	A	B	C	D	E	F	G	H	I	J
A	7.13E-11	8.26E-09	-2.96E-09	1.12E-08	-2.82E-06	-3.80E-04	-1.44E-09	-4.69E-08	-9.28E-10	-9.82E-13
B	8.26E-09	1.10E-03	-8.08E-05	1.20E-03	2.00E-03	-1.08E+00	4.33E-06	3.57E-05	2.75E-06	-2.50E-09
C	-2.96E-09	-8.08E-05	2.85E-04	-3.66E-04	-1.03E-02	-1.43E-01	-4.05E-06	-7.07E-05	-1.93E-06	6.53E-10
D	1.12E-08	1.20E-03	-3.66E-04	1.50E-03	1.23E-02	-9.38E-01	8.38E-06	1.06E-04	4.68E-06	-3.16E-09
E	-2.82E-06	2.00E-03	-1.03E-02	1.23E-02	5.20E-01	2.86E+01	3.47E-04	5.30E-03	1.22E-04	4.58E-08
F	-3.80E-04	-1.08E+00	-1.43E-01	-9.38E-01	2.86E+01	5.24E+03	4.74E-02	5.01E-01	7.90E-03	1.52E-05
G	-1.44E-09	4.33E-06	-4.05E-06	8.38E-06	3.47E-04	4.74E-02	9.14E-07	6.70E-06	1.39E-07	1.66E-10
H	-4.69E-08	3.57E-05	-7.07E-05	1.06E-04	5.30E-03	5.01E-01	6.70E-06	7.61E-05	1.64E-06	1.37E-09
I	-9.28E-10	2.75E-06	-1.93E-06	4.68E-06	1.22E-04	7.90E-03	1.39E-07	1.64E-06	3.93E-08	2.05E-11
J	-9.82E-13	-2.50E-09	6.53E-10	-3.16E-09	4.58E-08	1.52E-05	1.66E-10	1.37E-09	2.05E-11	5.14E-14

Covariance Matrix for Speaker x13

	A	B	C	D	E	F	G	H	I	J
A	1.64E-11	2.78E-07	-7.39E-08	3.52E-07	1.11E-06	2.57E-05	3.32E-10	4.58E-09	3.08E-10	3.82E-14
B	2.78E-07	6.00E-03	-9.25E-04	6.90E-03	7.53E-04	-1.03E+00	-2.44E-05	-9.66E-06	3.95E-06	-2.01E-10
C	-7.39E-08	-9.25E-04	5.37E-04	-1.50E-03	-1.45E-02	-8.46E-01	-8.84E-06	-4.52E-05	-2.04E-06	-2.18E-10
D	3.52E-07	6.90E-03	-1.50E-03	8.40E-03	1.52E-02	-1.81E-01	-1.55E-05	3.55E-05	5.98E-06	1.68E-11
E	1.11E-06	7.53E-04	-1.45E-02	1.52E-02	5.42E-01	3.87E+01	4.87E-04	1.70E-03	5.43E-05	9.68E-09
F	2.57E-05	-1.03E+00	-8.46E-01	-1.81E-01	3.87E+01	3.00E+03	4.08E-02	1.27E-01	3.20E-03	7.87E-07
G	3.32E-10	-2.44E-05	-8.84E-06	-1.55E-05	4.87E-04	4.08E-02	9.36E-07	2.58E-06	4.52E-08	2.99E-11
H	4.58E-09	-9.66E-06	-4.52E-05	3.55E-05	1.70E-03	1.27E-01	2.58E-06	8.18E-06	1.98E-07	8.31E-11
I	3.08E-10	3.95E-06	-2.04E-06	5.98E-06	5.43E-05	3.20E-03	4.52E-08	1.98E-07	8.36E-09	1.49E-12
J	3.82E-14	-2.01E-10	-2.18E-10	1.68E-11	9.68E-09	7.87E-07	2.99E-11	8.31E-11	1.49E-12	1.24E-15

Covariance Matrix for Speaker x14

	A	B	C	D	E	F	G	H	I	J
A	9.70E-12	-2.66E-08	7.20E-08	-9.86E-08	-1.43E-06	-5.89E-06	-3.02E-09	-5.74E-09	-1.40E-10	-1.36E-13
B	-2.66E-08	6.50E-04	-8.60E-04	1.50E-03	1.52E-02	6.13E-01	1.61E-05	7.43E-05	2.62E-06	1.74E-09
C	7.20E-08	-8.60E-04	1.90E-03	-2.70E-03	-3.47E-02	-1.37E+00	-3.55E-05	-1.36E-04	-4.61E-06	-2.99E-09
D	-9.86E-08	1.50E-03	-2.70E-03	4.30E-03	4.99E-02	1.99E+00	5.16E-05	2.10E-04	7.22E-06	4.74E-09
E	-1.43E-06	1.52E-02	-3.47E-02	4.99E-02	6.44E-01	2.41E+01	6.67E-04	2.50E-03	8.29E-05	5.43E-08
F	-5.89E-06	6.13E-01	-1.37E+00	1.99E+00	2.41E+01	1.43E+03	1.58E-02	9.10E-02	3.50E-03	1.99E-06
G	-3.02E-09	1.61E-05	-3.55E-05	5.16E-05	6.67E-04	1.58E-02	1.09E-06	2.74E-06	8.14E-08	6.43E-11
H	-5.74E-09	7.43E-05	-1.36E-04	2.10E-04	2.50E-03	9.10E-02	2.74E-06	1.05E-05	3.52E-07	2.37E-10
I	-1.40E-10	2.62E-06	-4.61E-06	7.22E-06	8.29E-05	3.50E-03	8.14E-08	3.52E-07	1.24E-08	7.98E-12
J	-1.36E-13	1.74E-09	-2.99E-09	4.74E-09	5.43E-08	1.99E-06	6.43E-11	2.37E-10	7.98E-12	5.46E-15

Covariance Matrix for Speaker x16

	A	B	C	D	E	F	G	H	I	J
A	3.00E-11	1.47E-08	-4.96E-08	6.42E-08	-9.76E-07	-6.59E-05	1.25E-09	1.95E-08	4.40E-10	-3.57E-14
B	1.47E-08	2.90E-03	-1.50E-03	4.40E-03	7.30E-03	-4.83E-01	4.08E-07	3.39E-04	1.00E-05	-9.69E-11
C	-4.96E-08	-1.50E-03	1.70E-03	-3.20E-03	-6.60E-03	-2.03E-01	-6.17E-06	-2.35E-04	-6.81E-06	1.41E-10
D	6.42E-08	4.40E-03	-3.20E-03	7.60E-03	1.39E-02	-2.80E-01	6.58E-06	5.74E-04	1.68E-05	-2.38E-10
E	-9.76E-07	7.30E-03	-6.60E-03	1.39E-02	9.09E-02	7.10E+00	-8.24E-06	5.98E-04	2.04E-05	6.33E-10
F	-6.59E-05	-4.83E-01	-2.03E-01	-2.80E-01	7.10E+00	1.27E+03	2.40E-03	-3.78E-02	-1.20E-03	4.24E-08
G	1.25E-09	4.08E-07	-6.17E-06	6.58E-06	-8.24E-06	2.40E-03	8.21E-08	1.05E-06	2.45E-08	-1.76E-12
H	1.95E-08	3.39E-04	-2.35E-04	5.74E-04	5.98E-04	-3.78E-02	1.05E-06	5.39E-05	1.49E-06	-3.48E-11
I	4.40E-10	1.00E-05	-6.81E-06	1.68E-05	2.04E-05	-1.20E-03	2.45E-08	1.49E-06	4.18E-08	-8.60E-13
J	-3.57E-14	-9.69E-11	1.41E-10	-2.38E-10	6.33E-10	4.24E-08	-1.76E-12	-3.48E-11	-8.60E-13	4.72E-17

Covariance Matrix for Speaker x17

	A	B	C	D	E	F	G	H	I	J
A	2.53E-11	1.24E-07	-4.07E-08	1.65E-07	5.47E-07	6.50E-05	8.17E-10	2.06E-08	5.07E-10	1.08E-13
B	1.24E-07	2.30E-03	-2.00E-03	4.30E-03	3.52E-02	1.55E+00	8.12E-06	1.32E-04	5.85E-06	2.28E-09
C	-4.07E-08	-2.00E-03	2.00E-03	-3.90E-03	-3.77E-02	-1.38E+00	-9.96E-06	-4.64E-05	-4.28E-06	-2.03E-09
D	1.65E-07	4.30E-03	-3.90E-03	8.20E-03	7.29E-02	2.93E+00	1.81E-05	1.78E-04	1.01E-05	4.31E-09
E	5.47E-07	3.52E-02	-3.77E-02	7.29E-02	7.95E-01	2.45E+01	3.24E-04	-3.36E-04	6.37E-05	4.46E-08
F	6.50E-05	1.55E+00	-1.38E+00	2.93E+00	2.45E+01	1.06E+03	4.60E-03	8.04E-02	3.80E-03	1.48E-06
G	8.17E-10	8.12E-06	-9.96E-06	1.81E-05	3.24E-04	4.60E-03	3.47E-07	-1.19E-06	7.51E-09	2.11E-11
H	2.06E-08	1.32E-04	-4.64E-05	1.78E-04	-3.36E-04	8.04E-02	-1.19E-06	3.07E-05	6.17E-07	1.74E-11
I	5.07E-10	5.85E-06	-4.28E-06	1.01E-05	6.37E-05	3.80E-03	7.51E-09	6.17E-07	1.88E-08	4.35E-12
J	1.08E-13	2.28E-09	-2.03E-09	4.31E-09	4.46E-08	1.48E-06	2.11E-11	1.74E-11	4.35E-12	3.07E-15

Covariance Matrix for Speaker x18

	A	B	C	D	E	F	G	H	I	J
A	1.07E-10	1.65E-07	-1.51E-07	3.16E-07	2.27E-07	2.57E-05	-5.49E-09	3.96E-08	8.88E-10	-1.92E-13
B	1.65E-07	1.10E-03	-4.42E-04	1.50E-03	1.24E-02	4.34E-01	6.36E-06	1.13E-04	3.19E-06	-1.00E-10
C	-1.51E-07	-4.42E-04	4.67E-04	-9.09E-04	-8.80E-03	-1.11E+00	-8.68E-06	-1.28E-04	-2.99E-06	-3.18E-12
D	3.16E-07	1.50E-03	-9.09E-04	2.40E-03	2.11E-02	1.54E+00	1.50E-05	2.42E-04	6.18E-06	-9.70E-11
E	2.27E-07	1.24E-02	-8.80E-03	2.11E-02	4.92E-01	4.63E+01	4.51E-04	4.10E-03	1.00E-04	1.43E-08
F	2.57E-05	4.34E-01	-1.11E+00	1.54E+00	4.63E+01	6.11E+03	5.94E-02	4.64E-01	1.04E-02	1.62E-06
G	-5.49E-09	6.36E-06	-8.68E-06	1.50E-05	4.51E-04	5.94E-02	1.41E-06	1.69E-06	4.60E-08	2.46E-11
H	3.96E-08	1.13E-04	-1.28E-04	2.42E-04	4.10E-03	4.64E-01	1.69E-06	5.23E-05	1.19E-06	6.42E-11
I	8.88E-10	3.19E-06	-2.99E-06	6.18E-06	1.00E-04	1.04E-02	4.60E-08	1.19E-06	2.78E-08	1.52E-12
J	-1.92E-13	-1.00E-10	-3.18E-12	-9.70E-11	1.43E-08	1.62E-06	2.46E-11	6.42E-11	1.52E-12	8.40E-16

Covariance Matrix for Speaker x19

	A	B	C	D	E	F	G	H	I	J
A	2.71E-11	-3.14E-08	1.27E-07	-1.58E-07	-1.36E-06	-6.44E-05	-1.78E-09	1.64E-09	2.74E-11	-4.87E-14
B	-3.14E-08	3.17E-04	-3.47E-04	6.64E-04	1.03E-02	9.85E-02	1.09E-05	1.43E-05	9.80E-07	6.24E-10
C	1.27E-07	-3.47E-04	7.99E-04	-1.10E-03	-1.35E-02	-5.13E-01	-1.57E-05	-1.12E-06	-5.95E-07	-6.72E-10
D	-1.58E-07	6.64E-04	-1.10E-03	1.80E-03	2.38E-02	6.11E-01	2.66E-05	1.54E-05	1.57E-06	1.30E-09
E	-1.36E-06	1.03E-02	-1.35E-02	2.38E-02	3.83E-01	9.22E+00	3.26E-04	5.16E-04	3.65E-05	2.16E-08
F	-6.44E-05	9.85E-02	-5.13E-01	6.11E-01	9.22E+00	9.54E+02	3.70E-03	2.77E-04	5.51E-04	3.56E-07
G	-1.78E-09	1.09E-05	-1.57E-05	2.66E-05	3.26E-04	3.70E-03	5.21E-07	9.22E-08	1.78E-08	2.01E-11
H	1.64E-09	1.43E-05	-1.12E-06	1.54E-05	5.16E-04	2.77E-04	9.22E-08	1.81E-06	9.05E-08	3.23E-11
I	2.74E-11	9.80E-07	-5.95E-07	1.57E-06	3.65E-05	5.51E-04	1.78E-08	9.05E-08	5.10E-09	2.20E-12
J	-4.87E-14	6.24E-10	-6.72E-10	1.30E-09	2.16E-08	3.56E-07	2.01E-11	3.23E-11	2.20E-12	1.29E-15

Covariance Matrix for Speaker x20

	A	B	C	D	E	F	G	H	I	J
A	5.94E-11	-8.29E-08	7.81E-08	-1.61E-07	-4.98E-06	-6.76E-04	-5.49E-09	-3.29E-08	-1.08E-09	-6.52E-13
B	-8.29E-08	1.40E-03	-1.50E-03	2.90E-03	3.71E-02	3.29E+00	2.47E-05	3.17E-04	1.05E-05	8.14E-09
C	7.81E-08	-1.50E-03	1.90E-03	-3.50E-03	-4.47E-02	-3.78E+00	-2.37E-05	-3.13E-04	-1.12E-05	-1.11E-08
D	-1.61E-07	2.90E-03	-3.50E-03	6.40E-03	8.17E-02	7.08E+00	4.84E-05	6.29E-04	2.17E-05	1.92E-08
E	-4.98E-06	3.71E-02	-4.47E-02	8.17E-02	1.24E+00	1.08E+02	7.90E-04	7.00E-03	2.71E-04	2.70E-07
F	-6.76E-04	3.29E+00	-3.78E+00	7.08E+00	1.08E+02	1.71E+04	9.46E-02	1.43E+00	3.97E-02	2.51E-05
G	-5.49E-09	2.47E-05	-2.37E-05	4.84E-05	7.90E-04	9.46E-02	8.06E-07	8.13E-06	2.42E-07	1.20E-10
H	-3.29E-08	3.17E-04	-3.13E-04	6.29E-04	7.00E-03	1.43E+00	8.13E-06	1.66E-04	4.11E-06	1.58E-09
I	-1.08E-09	1.05E-05	-1.12E-05	2.17E-05	2.71E-04	3.97E-02	2.42E-07	4.11E-06	1.12E-07	6.09E-11
J	-6.52E-13	8.14E-09	-1.11E-08	1.92E-08	2.70E-07	2.51E-05	1.20E-10	1.58E-09	6.09E-11	7.41E-14

Covariance Matrix for Speaker x21

	A	B	C	D	E	F	G	H	I	J
A	8.54E-11	1.88E-08	2.60E-07	-2.41E-07	-3.37E-06	-3.77E-04	-3.59E-09	-2.64E-08	-5.60E-10	2.97E-14
B	1.88E-08	9.85E-04	-5.48E-04	1.50E-03	1.35E-02	4.78E-01	1.85E-05	7.61E-05	2.68E-06	6.62E-11
C	2.60E-07	-5.48E-04	1.30E-03	-1.90E-03	-2.51E-02	-1.79E+00	-2.39E-05	-1.63E-04	-4.25E-06	-1.37E-10
D	-2.41E-07	1.50E-03	-1.90E-03	3.40E-03	3.86E-02	2.27E+00	4.24E-05	2.39E-04	6.94E-06	2.04E-10
E	-3.37E-06	1.35E-02	-2.51E-02	3.86E-02	5.95E-01	3.90E+01	4.36E-04	3.60E-03	9.62E-05	6.83E-09
F	-3.77E-04	4.78E-01	-1.79E+00	2.27E+00	3.90E+01	4.13E+03	1.81E-02	2.41E-01	5.90E-03	4.43E-08
G	-3.59E-09	1.85E-05	-2.39E-05	4.24E-05	4.36E-04	1.81E-02	6.14E-07	2.84E-06	8.30E-08	2.91E-12
H	-2.64E-08	7.61E-05	-1.63E-04	2.39E-04	3.60E-03	2.41E-01	2.84E-06	2.19E-05	5.82E-07	3.40E-11
I	-5.60E-10	2.68E-06	-4.25E-06	6.94E-06	9.62E-05	5.90E-03	8.30E-08	5.82E-07	1.61E-08	9.78E-13
J	2.97E-14	6.62E-11	-1.37E-10	2.04E-10	6.83E-09	4.43E-08	2.91E-12	3.40E-11	9.78E-13	2.94E-16

Covariance Matrix for Speaker x22

	A	B	C	D	E	F	G	H	I	J
A	6.57E-12	-1.95E-08	3.22E-08	-5.17E-08	-6.86E-07	-3.81E-05	-1.14E-09	1.54E-08	2.53E-10	2.23E-13
B	-1.95E-08	7.10E-03	-5.90E-03	1.30E-02	1.37E-01	-9.57E+00	5.79E-05	-7.23E-05	1.76E-05	-3.44E-09
C	3.22E-08	-5.90E-03	5.00E-03	-1.09E-02	-1.22E-01	5.95E+00	-5.33E-05	3.86E-05	-1.49E-05	-1.86E-10
D	-5.17E-08	1.30E-02	-1.09E-02	2.39E-02	2.59E-01	-1.55E+01	1.11E-04	-1.11E-04	3.25E-05	-3.26E-09
E	-6.86E-07	1.37E-01	-1.22E-01	2.59E-01	3.53E+00	-9.28E+01	1.30E-03	4.80E-03	5.02E-04	4.26E-07
F	-3.81E-05	-9.57E+00	5.95E+00	-1.55E+01	-9.28E+01	3.05E+04	-3.30E-02	5.22E-01	-1.46E-02	3.73E-05
G	-1.14E-09	5.79E-05	-5.33E-05	1.11E-04	1.30E-03	-3.30E-02	6.91E-07	-2.10E-06	1.10E-07	-2.22E-11
H	1.54E-08	-7.23E-05	3.86E-05	-1.11E-04	4.80E-03	5.22E-01	-2.10E-06	9.21E-05	2.00E-06	4.68E-09
I	2.53E-10	1.76E-05	-1.49E-05	3.25E-05	5.02E-04	-1.46E-02	1.10E-07	2.00E-06	9.72E-08	1.13E-10
J	2.23E-13	-3.44E-09	-1.86E-10	-3.26E-09	4.26E-07	3.73E-05	-2.22E-11	4.68E-09	1.13E-10	3.20E-13

Covariance Matrix for Speaker x23

	A	B	C	D	E	F	G	H	I	J
A	3.25E-11	-5.57E-08	1.30E-07	-1.86E-07	-1.74E-06	-2.35E-04	-1.87E-09	-3.73E-08	-8.84E-10	1.48E-13
B	-5.57E-08	1.10E-03	-1.30E-03	2.40E-03	3.23E-02	1.13E+00	1.81E-05	2.33E-04	7.58E-06	3.28E-09
C	1.30E-07	-1.30E-03	2.30E-03	-3.70E-03	-5.26E-02	-2.37E+00	-3.60E-05	-3.85E-04	-1.21E-05	-4.97E-09
D	-1.86E-07	2.40E-03	-3.70E-03	6.10E-03	8.49E-02	3.50E+00	5.41E-05	6.18E-04	1.97E-05	8.24E-09
E	-1.74E-06	3.23E-02	-5.26E-02	8.49E-02	1.29E+00	5.57E+01	8.32E-04	7.90E-03	2.60E-04	1.34E-07
F	-2.35E-04	1.13E+00	-2.37E+00	3.50E+00	5.57E+01	4.10E+03	4.13E-02	4.25E-01	1.18E-02	3.60E-06
G	-1.87E-09	1.81E-05	-3.60E-05	5.41E-05	8.32E-04	4.13E-02	5.90E-07	5.58E-06	1.76E-07	7.89E-11
H	-3.73E-08	2.33E-04	-3.85E-04	6.18E-04	7.90E-03	4.25E-01	5.58E-06	7.56E-05	2.20E-06	5.53E-10
I	-8.84E-10	7.58E-06	-1.21E-05	1.97E-05	2.60E-04	1.18E-02	1.76E-07	2.20E-06	6.73E-08	2.22E-11
J	1.48E-13	3.28E-09	-4.97E-09	8.24E-09	1.34E-07	3.60E-06	7.89E-11	5.53E-10	2.22E-11	1.78E-14

Covariance Matrix for Speaker x24

	A	B	C	D	E	F	G	H	I	J
A	3.59E-11	-1.09E-07	2.70E-07	-3.79E-07	-3.57E-06	-1.51E-04	-1.26E-09	8.09E-09	-1.59E-11	-2.67E-13
B	-1.09E-07	1.10E-03	-8.56E-04	1.90E-03	8.60E-03	4.77E-01	-5.82E-06	3.79E-05	1.84E-06	1.99E-10
C	2.70E-07	-8.56E-04	2.20E-03	-3.00E-03	-3.06E-02	-8.82E-01	-7.77E-06	6.81E-05	-3.68E-07	-4.40E-09
D	-3.79E-07	1.90E-03	-3.00E-03	5.00E-03	3.92E-02	1.36E+00	1.95E-06	-3.02E-05	2.20E-06	4.60E-09
E	-3.57E-06	8.60E-03	-3.06E-02	3.92E-02	4.85E-01	6.33E+00	9.99E-05	-1.30E-03	4.78E-07	9.07E-08
F	-1.51E-04	4.77E-01	-8.82E-01	1.36E+00	6.33E+00	1.29E+03	1.02E-02	-5.60E-03	-1.09E-04	-2.03E-06
G	-1.26E-09	-5.82E-06	-7.77E-06	1.95E-06	9.99E-05	1.02E-02	2.21E-07	-8.75E-07	-2.25E-08	1.57E-11
H	8.09E-09	3.79E-05	6.81E-05	-3.02E-05	-1.30E-03	-5.60E-03	-8.75E-07	8.07E-06	1.35E-07	-2.45E-10
I	-1.59E-11	1.84E-06	-3.68E-07	2.20E-06	4.78E-07	-1.09E-04	-2.25E-08	1.35E-07	4.46E-09	2.19E-12
J	-2.67E-13	1.99E-10	-4.40E-09	4.60E-09	9.07E-08	-2.03E-06	1.57E-11	-2.45E-10	2.19E-12	5.61E-14

Covariance Matrix for Speaker x25

	A	B	C	D	E	F	G	H	I	J
A	2.69E-11	-1.38E-07	1.27E-07	-2.66E-07	-1.58E-06	-4.25E-05	1.06E-09	1.06E-08	1.07E-10	-3.52E-13
B	-1.38E-07	6.50E-03	-5.30E-03	1.18E-02	7.40E-02	1.47E+00	7.55E-05	-1.19E-04	4.72E-06	1.52E-08
C	1.27E-07	-5.30E-03	5.10E-03	-1.04E-02	-6.57E-02	-1.33E+00	-6.68E-05	1.40E-04	-3.72E-06	-1.18E-08
D	-2.66E-07	1.18E-02	-1.04E-02	2.21E-02	1.40E-01	2.81E+00	1.42E-04	-2.58E-04	8.44E-06	2.70E-08
E	-1.58E-06	7.40E-02	-6.57E-02	1.40E-01	1.36E+00	1.11E+01	9.21E-04	-1.70E-03	9.79E-05	3.08E-07
F	-4.25E-05	1.47E+00	-1.33E+00	2.81E+00	1.11E+01	4.51E+02	1.69E-02	-3.53E-02	3.72E-04	1.47E-06
G	1.06E-09	7.55E-05	-6.68E-05	1.42E-04	9.21E-04	1.69E-02	1.24E-06	-8.34E-07	7.91E-08	1.72E-10
H	1.06E-08	-1.19E-04	1.40E-04	-2.58E-04	-1.70E-03	-3.53E-02	-8.34E-07	6.66E-06	-2.75E-08	-2.93E-10
I	1.07E-10	4.72E-06	-3.72E-06	8.44E-06	9.79E-05	3.72E-04	7.91E-08	-2.75E-08	9.29E-09	2.36E-11
J	-3.52E-13	1.52E-08	-1.18E-08	2.70E-08	3.08E-07	1.47E-06	1.72E-10	-2.93E-10	2.36E-11	7.63E-14

Covariance Matrix for Speaker x26

	A	B	C	D	E	F	G	H	I	J
A	9.72E-11	-4.87E-08	-1.22E-07	7.34E-08	2.10E-06	2.97E-05	-1.00E-08	1.96E-08	7.31E-10	9.33E-13
B	-4.87E-08	1.00E-03	-1.10E-03	2.10E-03	2.01E-02	5.58E-01	2.78E-05	1.38E-04	4.93E-06	3.66E-09
C	-1.22E-07	-1.10E-03	2.00E-03	-3.10E-03	-2.92E-02	-8.80E-01	-1.22E-05	-1.82E-04	-6.62E-06	-5.89E-09
D	7.34E-08	2.10E-03	-3.10E-03	5.30E-03	4.93E-02	1.44E+00	4.00E-05	3.20E-04	1.16E-05	9.55E-09
E	2.10E-06	2.01E-02	-2.92E-02	4.93E-02	7.18E-01	2.35E+01	3.89E-04	4.50E-03	1.59E-04	1.42E-07
F	2.97E-05	5.58E-01	-8.80E-01	1.44E+00	2.35E+01	8.51E+02	1.56E-02	1.35E-01	4.70E-03	4.24E-06
G	-1.00E-08	2.78E-05	-1.22E-05	4.00E-05	3.89E-04	1.56E-02	1.62E-06	1.96E-06	6.51E-08	1.82E-11
H	1.96E-08	1.38E-04	-1.82E-04	3.20E-04	4.50E-03	1.35E-01	1.96E-06	3.08E-05	1.09E-06	9.59E-10
I	7.31E-10	4.93E-06	-6.62E-06	1.16E-05	1.59E-04	4.70E-03	6.51E-08	1.09E-06	3.86E-08	3.40E-11
J	9.33E-13	3.66E-09	-5.89E-09	9.55E-09	1.42E-07	4.24E-06	1.82E-11	9.59E-10	3.40E-11	3.14E-14

Covariance Matrix for Speaker x27

	A	B	C	D	E	F	G	H	I	J
A	2.75E-11	6.33E-09	8.78E-09	-2.45E-09	-2.04E-07	-1.12E-04	3.79E-09	-3.15E-09	-3.87E-11	-7.78E-14
B	6.33E-09	8.02E-05	-7.97E-05	1.60E-04	1.50E-03	5.56E-02	5.81E-06	8.43E-06	1.20E-07	6.50E-11
C	8.78E-09	-7.97E-05	1.43E-04	-2.23E-04	-3.40E-03	-1.54E-01	-6.46E-06	-9.60E-06	-1.16E-07	-4.06E-10
D	-2.45E-09	1.60E-04	-2.23E-04	3.83E-04	4.90E-03	2.10E-01	1.23E-05	1.80E-05	2.36E-07	4.71E-10
E	-2.04E-07	1.50E-03	-3.40E-03	4.90E-03	9.07E-02	3.21E+00	1.48E-04	1.89E-04	2.30E-06	9.28E-09
F	-1.12E-04	5.56E-02	-1.54E-01	2.10E-01	3.21E+00	5.84E+02	-8.70E-03	2.03E-02	2.31E-04	7.89E-07
G	3.79E-09	5.81E-06	-6.46E-06	1.23E-05	1.48E-04	-8.70E-03	9.49E-07	9.41E-08	1.25E-09	8.56E-12
H	-3.15E-09	8.43E-06	-9.60E-06	1.80E-05	1.89E-04	2.03E-02	9.41E-08	1.52E-06	2.21E-08	2.53E-12
I	-3.87E-11	1.20E-07	-1.16E-07	2.36E-07	2.30E-06	2.31E-04	1.25E-09	2.21E-08	3.44E-10	-2.32E-13
J	-7.78E-14	6.50E-11	-4.06E-10	4.71E-10	9.28E-09	7.89E-07	8.56E-12	2.53E-12	-2.32E-13	3.50E-15

Covariance Matrix for Speaker x28

	A	B	C	D	E	F	G	H	I	J
A	2.16E-11	-4.36E-08	8.56E-08	-1.29E-07	-2.17E-06	-1.21E-04	-1.31E-09	2.05E-09	-4.26E-11	-1.20E-13
B	-4.36E-08	2.45E-04	-3.78E-05	2.83E-04	3.60E-03	1.98E-01	-8.59E-07	-1.43E-05	-5.50E-07	2.63E-10
C	8.56E-08	-3.78E-05	4.66E-04	-5.04E-04	-8.90E-03	-4.82E-01	-9.17E-06	-4.32E-06	-7.12E-07	-4.38E-10
D	-1.29E-07	2.83E-04	-5.04E-04	7.87E-04	1.25E-02	6.80E-01	8.31E-06	-9.96E-06	1.62E-07	7.01E-10
E	-2.17E-06	3.60E-03	-8.90E-03	1.25E-02	3.10E-01	9.10E+00	1.40E-04	-4.15E-04	7.91E-06	9.42E-09
F	-1.21E-04	1.98E-01	-4.82E-01	6.80E-01	9.10E+00	1.06E+03	3.90E-03	-1.28E-02	4.01E-04	9.15E-07
G	-1.31E-09	-8.59E-07	-9.17E-06	8.31E-06	1.40E-04	3.90E-03	2.48E-07	3.85E-07	1.67E-08	4.16E-12
H	2.05E-09	-1.43E-05	-4.32E-06	-9.96E-06	-4.15E-04	-1.28E-02	3.85E-07	2.35E-06	3.52E-08	-1.37E-11
I	-4.26E-11	-5.50E-07	-7.12E-07	1.62E-07	7.91E-06	4.01E-04	1.67E-08	3.52E-08	2.66E-09	1.36E-13
J	-1.20E-13	2.63E-10	-4.38E-10	7.01E-10	9.42E-09	9.15E-07	4.16E-12	-1.37E-11	1.36E-13	8.38E-16

Covariance Matrix for Speaker x29

	A	B	C	D	E	F	G	H	I	J
A	2.91E-11	1.58E-08	1.79E-09	1.40E-08	-5.42E-07	-1.44E-04	3.77E-10	6.16E-09	2.58E-10	-3.59E-14
B	1.58E-08	1.60E-03	-5.83E-04	2.20E-03	7.40E-03	-5.77E-01	6.04E-06	5.51E-05	3.60E-06	6.91E-10
C	1.79E-09	-5.83E-04	3.92E-04	-9.76E-04	-8.50E-03	7.47E-02	-6.80E-07	-4.98E-05	-1.69E-06	-3.37E-10
D	1.40E-08	2.20E-03	-9.76E-04	3.10E-03	1.60E-02	-6.52E-01	6.72E-06	1.05E-04	5.29E-06	1.03E-09
E	-5.42E-07	7.40E-03	-8.50E-03	1.60E-02	2.46E-01	1.20E+00	2.93E-05	8.35E-04	1.95E-05	9.19E-09
F	-1.44E-04	-5.77E-01	7.47E-02	-6.52E-01	1.20E+00	1.25E+03	-1.21E-02	1.17E-02	-1.30E-03	-3.86E-07
G	3.77E-10	6.04E-06	-6.80E-07	6.72E-06	2.93E-05	-1.21E-02	2.15E-07	-9.44E-07	-6.74E-09	1.05E-11
H	6.16E-09	5.51E-05	-4.98E-05	1.05E-04	8.35E-04	1.17E-02	-9.44E-07	1.37E-05	3.48E-07	-2.01E-11
I	2.58E-10	3.60E-06	-1.69E-06	5.29E-06	1.95E-05	-1.30E-03	-6.74E-09	3.48E-07	1.31E-08	4.32E-13
J	-3.59E-14	6.91E-10	-3.37E-10	1.03E-09	9.19E-09	-3.86E-07	1.05E-11	-2.01E-11	4.32E-13	8.46E-16

Covariance Matrix for Speaker x30

	A	B	C	D	E	F	G	H	I	J
A	8.27E-12	-3.52E-09	9.88E-08	-1.02E-07	-1.83E-06	-1.45E-05	-1.14E-09	1.24E-09	-1.07E-10	-1.76E-13
B	-3.52E-09	6.75E-04	-4.49E-04	1.10E-03	2.01E-02	9.44E-01	8.02E-05	7.23E-05	3.33E-06	2.00E-08
C	9.88E-08	-4.49E-04	1.60E-03	-2.00E-03	-3.27E-02	-1.00E+00	-7.55E-05	-4.57E-05	-3.58E-06	-1.72E-08
D	-1.02E-07	1.10E-03	-2.00E-03	3.20E-03	5.28E-02	1.94E+00	1.56E-04	1.18E-04	6.91E-06	3.72E-08
E	-1.83E-06	2.01E-02	-3.27E-02	5.28E-02	9.70E-01	2.71E+01	2.40E-03	1.70E-03	1.18E-04	5.71E-07
F	-1.45E-05	9.44E-01	-1.00E+00	1.94E+00	2.71E+01	2.11E+03	1.54E-01	1.36E-01	5.00E-03	3.80E-05
G	-1.14E-09	8.02E-05	-7.55E-05	1.56E-04	2.40E-03	1.54E-01	1.17E-05	1.04E-05	4.15E-07	2.90E-09
H	1.24E-09	7.23E-05	-4.57E-05	1.18E-04	1.70E-03	1.36E-01	1.04E-05	1.01E-05	3.64E-07	2.58E-09
I	-1.07E-10	3.33E-06	-3.58E-06	6.91E-06	1.18E-04	5.00E-03	4.15E-07	3.64E-07	1.84E-08	1.01E-10
J	-1.76E-13	2.00E-08	-1.72E-08	3.72E-08	5.71E-07	3.80E-05	2.90E-09	2.58E-09	1.01E-10	7.23E-13

Appendix 2

Additional correlation results for users in the VALID Database

User	AB	AC	AD	AE	AF	AG	AH	AI	AJ	BA	BC	BD	BE
x0	-0.5071	0.4535	-0.4807	-0.5641	-0.1904	0.2886	0.003	-0.3154	-0.5543	-0.5071	-0.9962	0.999	0.9446
x1	-0.3404	0.4677	-0.4082	-0.1567	0.8139	0.1113	0.4613	0.36	0.1644	-0.3404	-0.7839	0.9707	0.6936
x2	0.8812	0.1564	0.6936	-0.6314	-0.2233	0.6926	0.8939	0.7724	0.2407	0.8812	-0.1712	0.9232	-0.1969
x3	-0.6913	0.6531	-0.6747	-0.8527	-0.4724	-0.7758	0.7548	-0.3928	-0.6918	-0.6913	-0.9837	0.9958	0.8724
x4	0.3471	0.6001	-0.204	-0.6605	-0.3136	-0.0448	-0.1978	0.0523	-0.6811	0.3471	-0.4678	0.8233	0.4535
x5	0.4287	-0.3327	0.3845	-0.1373	0.1233	-0.745	0.6249	0.357	-0.1555	0.4287	-0.9548	0.9884	0.8336
x6	0.8677	-0.4858	0.7316	-0.7624	0.0576	0.986	0.8308	0.8181	0.2102	0.8677	-0.8077	0.9603	-0.837
x8	0.9673	0.2218	0.6613	-0.4719	-0.6544	-0.5195	5.57E-04	-1.05E-04	-0.5704	0.9673	0.0407	0.7976	-0.3845
x9	0.8189	-0.5617	0.8063	0.4396	0.2303	-0.3292	0.7133	0.8723	-0.1252	0.8189	-0.4061	0.8016	0.1853
x10	0.3629	-0.7473	0.5384	-0.1266	-0.4069	0.5239	-0.0129	0.2127	-0.4427	0.3629	-0.8853	0.9799	0.2997
x11	-0.8925	0.5869	-0.756	-0.6796	-0.6793	-0.1895	-0.4565	-0.6277	-0.4858	-0.8925	-0.8753	0.965	0.9359
x12	0.0296	-0.0208	0.0339	-0.4632	-0.6208	-0.1789	-0.6363	-0.5537	-0.5128	0.0296	-0.1449	0.905	0.0822
x13	0.8887	-0.7884	0.9509	0.3714	0.1157	0.0848	0.3959	0.8334	0.2677	0.8887	-0.5167	0.9762	0.0132
x14	-0.3347	0.5324	-0.4853	-0.5705	-0.05	-0.9274	-0.5703	-0.4034	-0.5916	-0.3347	-0.7758	0.9074	0.7424
x16	0.0501	-0.2226	0.1344	-0.591	-0.3376	0.7955	0.4836	0.3924	-0.9471	0.0501	-0.7133	0.9451	0.4539
x17	0.5106	-0.1812	0.3605	0.1219	0.3975	0.2759	0.7383	0.7355	0.3881	0.5106	-0.9101	0.979	0.8174
x18	0.4859	-0.6767	0.6206	0.0314	0.0318	-0.4482	0.5301	0.5159	-0.6436	0.4859	-0.6224	0.9392	0.5369
x19	-0.3387	0.8626	-0.715	-0.4212	-0.4004	-0.4739	0.2348	0.0736	-0.2609	-0.3387	-0.6896	0.8766	0.9369
x20	-0.2913	0.2323	-0.262	-0.5796	-0.6708	-0.7934	-0.3312	-0.4205	-0.3107	-0.2913	-0.9598	0.9881	0.8996
x21	0.065	0.7762	-0.4482	-0.4726	-0.6351	-0.4956	-0.6117	-0.4776	0.1877	0.065	-0.4814	0.838	0.5565
x22	-0.09	0.1776	-0.1306	-0.1425	-0.085	-0.5334	0.6241	0.3163	0.1535	-0.09	-0.9782	0.9955	0.8631
x23	-0.2939	0.4716	-0.4162	-0.2684	-0.6436	-0.4264	-0.7537	-0.5977	0.1946	-0.2939	-0.8341	0.9401	0.8541
x24	-0.5518	0.9677	-0.897	-0.8544	-0.7005	-0.4484	0.4747	-0.0397	-0.1883	-0.5518	-0.5581	0.8369	0.3734
x25	-0.3305	0.3435	-0.3441	-0.2605	-0.3856	0.1832	0.789	0.2146	-0.2458	-0.3305	-0.9136	0.9808	0.7874
x26	-0.1528	-0.2741	0.1025	0.251	0.1032	-0.7956	0.3591	0.3777	0.5343	-0.1528	-0.7477	0.9106	0.733
x27	0.1348	0.14	-0.0239	-0.1294	-0.8806	0.7422	-0.4876	-0.398	-0.2508	0.1348	-0.7438	0.9126	0.5536
x28	-0.5989	0.8528	-0.9907	-0.8378	-0.7993	-0.5649	0.2873	-0.1776	-0.894	-0.5989	-0.1117	0.6442	0.4171

x30	0.0739	0.0168	0.0464	-0.2024	-0.7555	0.1504	0.3087	0.4176	-0.2286	0.0739	-0.7439	0.9716	0.3795
x31	-0.0471	0.8646	-0.634	-0.6477	-0.1099	-0.1163	0.1358	-0.2745	-0.0722	-0.0471	-0.4342	0.7701	0.7838
x32	0.2783	0.4469	-0.0431	-0.3823	-0.0554	-0.7553	0.5512	0.5216	-0.6827	0.2783	-0.6587	0.9324	0.3262
x33	0.5888	0.2932	-0.0197	-0.4466	-0.4044	-0.2422	0.8125	0.5829	-0.6221	0.5888	-0.0793	0.4758	-0.2154
x34	0.8038	0.5737	0.4669	-0.6979	-0.7952	-0.2172	-0.9134	-0.8432	-0.8577	0.8038	0.5729	0.7031	-0.4649
x35	0.5532	-0.7393	0.6704	-0.2347	-0.8396	-0.0413	0.7497	0.8407	-0.2875	0.5532	-0.7958	0.959	-0.7921
x36	0.093	0.2563	0.0097	-0.8407	-0.1026	-0.3662	-0.9092	-0.9238	0.0154	0.093	-0.425	0.9692	-0.5677
x37	-0.0473	0.1325	-0.091	-0.3431	-0.2924	-0.0612	-0.3428	-0.3575	-0.1792	-0.0473	-0.7866	0.955	0.8212
x38	0.5762	-0.6727	0.6319	0.3939	-0.3659	0.409	0.8067	0.8079	0.1961	0.5762	-0.9332	0.9853	0.8776
x40	0.5902	-0.5884	0.596	0.4668	0.18	0.0454	0.4713	0.492	0.7732	0.5902	-0.9537	0.9852	0.9566
x41	-0.4489	0.2414	-0.3307	-0.3777	0.6869	-0.5707	0.5585	0.0668	-0.433	-0.4489	-0.9301	0.9748	0.9595
x42	-0.9863	0.8211	-0.9487	-0.8712	-0.7975	0.4482	-0.866	-0.8958	-0.8066	-0.9863	-0.8284	0.9599	0.8823
x43	0.7181	0.2615	0.3958	0.6887	0.4172	-0.3326	0.8244	0.7522	0.3534	0.7181	-0.3702	0.8984	0.7101
x44	-0.4078	0.2482	-0.3162	-0.6291	0.4572	-0.598	0.0169	-0.4507	-0.7362	-0.4078	-0.9363	0.9765	0.9334
x46	0.4149	-0.3383	0.3756	0.1644	0.0692	-0.9722	0.1564	0.1851	-0.1026	0.4149	-0.9532	0.9847	0.9035
x48	0.1326	-0.2824	0.2144	0.5909	-0.4276	0.8213	0.2758	0.6922	0.229	0.1326	-0.5529	0.9323	0.402
x49	-0.1013	-0.0023	-0.0608	-0.3616	-0.3062	-0.3095	0.1864	0.1128	-0.1208	-0.1013	-0.8422	0.9726	0.5809
x50	0.0721	0.573	-0.3864	-0.4526	-0.5461	-0.8991	0.3801	0.2701	-0.9241	0.0721	-0.4033	0.7435	0.3511
x52	0.2023	-0.1526	0.1773	0.2107	0.2912	0.4078	0.3864	0.3616	0.2471	0.2023	-0.997	0.9992	0.9695
x53	-0.0166	0.123	-0.0552	-0.4962	-0.2399	0.0381	0.8731	0.5844	0.405	-0.0166	-0.6017	0.9608	-0.0662
x56	-0.5521	0.5969	-0.6193	-0.7745	-0.3299	-0.3516	0.0054	-0.307	-0.4298	-0.5521	-0.7363	0.9064	0.8063
x57	-0.3013	0.7774	-0.612	-0.3235	0.33	-0.7169	0.3847	0.2039	-0.4699	-0.3013	-0.7717	0.9205	0.6251
x58	-0.636	0.9827	-0.9304	-0.8739	-0.5357	-0.4429	-0.581	-0.6701	-0.9248	-0.636	-0.5727	0.8624	0.2788
x59	0.5282	0.0852	0.1707	0.1757	0.2192	0.0919	0.7927	0.5789	0.4359	0.5282	-0.6255	0.8516	0.645
x60	0.1108	0.2413	-0.0647	-0.5914	-0.6244	-0.5137	-0.2589	-0.3883	-0.5284	0.1108	-0.8392	0.9605	0.6412
x61	0.8269	-0.6257	0.8168	-0.3703	0.1054	-0.3751	0.6161	0.8784	-0.7917	0.8269	-0.6878	0.9618	0.0035
x62	-0.5765	0.3929	-0.491	-0.4107	-0.1261	0.4585	-0.1626	-0.299	-0.2827	-0.5765	-0.8545	0.9527	0.8758
x63	0.5348	0.0931	0.0779	-0.3053	-0.0758	0.611	0.075	0.0272	-0.58	0.5348	-0.6007	0.7673	0.4929
x64	0.0707	0.6629	-0.399	-0.8551	-0.3483	-0.404	0.4134	-0.2546	-0.6212	0.0707	-0.0579	0.7376	-0.1456
x65	0.0912	-0.1282	0.1091	-0.163	0.1171	0.2704	0.2826	0.3009	0.1607	0.0912	-0.9837	0.9964	0.4757
x67	0.8523	-0.724	0.8352	0.9228	0.5134	-0.276	0.7454	0.7822	0.2906	0.8523	-0.8655	0.9854	0.9106

x68	0.1103	0.1031	0.0154	0.0962	0.5077	-0.8014	0.1531	0.1814	-0.2292	0.1103	-0.6702	0.9306	-0.1871
x69	0.6069	-0.1831	0.6749	0.2601	0.3977	-3.73E-04	0.6304	0.6861	0.1642	0.6069	0.5281	0.9925	-0.3585
x70	-0.3814	0.1191	-0.2247	-0.1621	-0.6341	-0.4079	-0.0431	-0.1933	0.4814	-0.3814	-0.8839	0.9544	0.7495
x71	0.5771	-0.6695	0.6741	0.5441	-0.3316	-0.3753	0.0297	0.2426	0.7198	0.5771	-0.7824	0.8801	0.6228
x72	0.8548	-0.9541	0.9102	0.6828	-0.182	0.3431	0.8558	0.9102	-0.451	0.8548	-0.96	0.9913	0.5886
x73	0.846	-0.7768	0.9215	0.8333	-0.1052	0.2771	0.282	0.554	-0.6996	0.846	-0.5456	0.9488	0.4793
x74	0.2854	-0.11	0.1818	-0.3807	0.3747	-0.8216	0.4412	0.0558	-0.5597	0.2854	-0.8554	0.9419	0.5687
x75	0.7914	-0.6698	0.762	-0.1025	0.5211	-0.3927	0.6279	0.6105	0.1636	0.7914	-0.8461	0.9628	0.5013
x76	-0.2457	0.6282	-0.5301	-0.8953	-0.5791	-0.4396	0.0481	0.0649	-0.3094	-0.2457	-0.8708	0.9342	0.5557
x77	-0.1116	0.4932	-0.3821	0.2126	0.77	-0.0675	0.8511	0.6291	0.5527	-0.1116	-0.89	0.9474	0.9166
x78	0.7215	-0.5885	0.6737	0.083	0.2675	-0.3557	0.9057	0.9373	-0.1034	0.7215	-0.9682	0.995	0.1697
x79	-0.0107	0.5057	-0.3217	-0.4645	0.444	-0.6723	0.6041	0.5308	-0.5879	-0.0107	-0.5993	0.8655	0.3504
x81	0.7697	-0.4488	0.7077	-0.6609	0.2667	-0.8124	0.9772	0.6475	-0.6357	0.7697	-0.8153	0.9861	-0.4107
x82	0.8088	-0.5341	0.8563	0.8017	0.1759	-0.2175	0.9391	0.9064	0.0233	0.8088	-0.332	0.9503	0.9162
x83	0.3072	-0.3403	0.3237	0.2771	0.114	0.1965	0.0345	0.0699	0.5106	0.3072	-0.9236	0.9917	-0.7987
x85	0.0781	-0.1564	0.1219	0.3739	-0.2067	-0.3654	0.3237	0.4893	0.1746	0.0781	-0.9585	0.9877	0.9142
x86	0.8627	-0.9227	0.9003	0.3815	0.8198	0.7884	0.7151	0.8525	-0.3549	0.8627	-0.9838	0.9948	0.4322
x87	0.0795	0.5985	-0.1428	0.6543	-0.0897	0.7019	-0.2051	-0.0644	0.2363	0.0795	-0.4199	0.9496	0.1123
x88	-0.7741	0.7276	-0.7721	-0.0544	-0.3413	-0.8181	0.8699	0.7977	0.1197	-0.7741	-0.8102	0.9019	0.6665
x89	-0.0394	0.2966	-0.1431	-0.8072	-0.4394	0.2278	-0.3476	-0.2888	-0.2791	-0.0394	-0.9563	0.9931	0.5749
x90	0.4052	0.6825	-0.1606	-0.667	-0.0543	-0.0756	-0.3952	-0.1512	-0.2806	0.4052	-0.2663	0.8048	-0.5225
x91	-0.0652	0.2816	-0.1537	-0.7909	-0.1108	-0.659	-0.4391	-0.664	-0.089	-0.0652	-0.9263	0.9884	0.5099
x92	0.3074	0.5953	-0.28	-0.8194	-0.9188	0.0873	-0.67	-0.869	0.4701	0.3074	0.2826	0.54	-0.6409
x94	0.5591	-0.2876	0.4551	-0.3162	-0.8974	0.7772	-0.8111	-0.4676	-0.88	0.5591	-0.846	0.9686	0.4852
x95	0.4731	0.8353	-0.3535	-0.756	-0.7344	-0.4095	0.2872	-0.0017	-0.9279	0.4731	-0.0836	0.655	0.1575
x96	0.3681	-0.2356	0.3097	-0.147	0.6425	-0.554	0.8155	0.7145	-0.5467	0.3681	-0.9174	0.98	0.7405
x98	0.4045	-0.0062	0.2575	-0.64	0.1823	-0.5703	0.8867	0.5834	-0.6585	0.4045	-0.8702	0.9802	-0.2838
x99	0.537	-0.34	0.4732	0.553	0.6805	-0.3106	0.4202	0.7974	0.7862	0.537	-0.8603	0.9767	0.9136
x100	-0.2618	0.3216	-0.302	-0.4304	0.0669	0.4171	0.0787	-0.1458	-0.7142	-0.2618	-0.855	0.9652	0.7634
x101	0.4273	-0.475	0.4948	-0.408	0.1897	-0.7714	0.2401	-0.1692	-0.1488	0.4273	-0.6551	0.9175	0.3975
x102	0.2438	0.3524	-0.0466	-0.4881	-0.37	-0.8652	-0.171	-0.1672	-0.6636	0.2438	-0.7405	0.9378	0.5032

x103	-0.124	0.1288	-0.1319	-0.364	0.5674	-0.0586	0.8099	0.6387	-0.4335	-0.124	-0.8238	0.9675	0.2357
x104	-0.7881	0.8277	-0.8209	-0.7431	0.2002	-0.5318	0.891	0.5893	-0.894	-0.7881	-0.944	0.9836	0.9925
x105	0.0528	0.1089	-0.0163	-0.4507	0.1538	-0.8176	0.5497	0.7329	-0.2371	0.0528	-0.7697	0.9584	0.5722
x106	0.4289	-0.357	0.4044	-0.1158	0.2512	0.1986	0.2038	0.1696	0.2969	0.4289	-0.9311	0.9868	0.7938
x107	0.668	0.1523	0.3703	-0.682	-0.7382	-0.8813	-0.6633	-0.5299	-0.7629	0.668	-0.5498	0.9198	-0.0332
x108	-0.6572	0.5339	-0.6043	-0.6685	0.103	-0.9109	0.8085	0.5948	-0.613	-0.6572	-0.9327	0.9822	0.7186
x110	0.0628	0.4748	-0.3023	-0.7823	-0.5584	-0.2964	-0.6345	-0.5653	-0.3993	0.0628	-0.4882	0.7938	0.3981
x111	-0.4697	0.1064	-0.2543	-0.1115	0.1346	-0.8581	0.108	0.0266	0.5133	-0.4697	-0.8298	0.9323	0.8652
x113	0.8197	0.8665	0.1786	-0.5416	-0.8129	-0.2251	0.7123	0.6727	-0.3483	0.8197	0.6041	0.6499	-0.5921
x114	-0.015	0.1732	-0.1002	-0.6453	-0.8901	-0.048	-0.5459	-0.4331	0.2244	-0.015	-0.8727	0.9652	0.6104
x115	0.2747	0.2177	0.103	-0.6689	-0.5271	-0.9083	-0.5688	-0.4523	-0.2927	0.2747	-0.7294	0.9643	0.2814
x116	-0.6084	0.799	-0.74	-0.769	-0.489	-0.8185	-0.3723	-0.4658	-0.5076	-0.6084	-0.8709	0.9579	0.9284
x117	0.1043	0.0657	0.0038	-0.4974	-0.9499	-0.9557	-0.5571	-0.5872	-0.7737	0.1043	-0.7365	0.9032	0.611
x118	0.6778	-0.6977	0.7053	0.3112	0.7084	0.5172	0.76	0.7432	-0.6121	0.6778	-0.8881	0.9813	0.1487
x119	-0.5675	0.392	-0.6546	-0.3803	-0.8311	0.7543	-0.6408	-0.4524	0.3703	-0.5675	-0.1184	0.847	-0.1992
x121	0.8846	-0.8398	0.8826	0.5448	0.6789	-0.0554	0.9662	0.949	-0.6088	0.8846	-0.9315	0.9912	0.6764
x122	-0.0132	0.0679	-0.0511	-0.0426	0.4962	0.6908	0.3543	0.1605	0.2718	-0.0132	-0.2989	0.7963	-0.3956

User	BF	BG	BH	BI	BJ	CA	CB	CD	CE	CF	CG	CH	CI
x0	0.3411	0.6355	0.3526	0.8472	0.8112	0.4535	-0.9962	-0.9991	-0.9521	-0.3678	-0.6942	-0.3665	-0.8545
x1	0.1002	0.526	0.4096	0.4752	0.426	0.4677	-0.7839	-0.9101	-0.7976	0.1923	-0.4456	0.1054	-0.2147
x2	8.34E-04	0.4356	0.9108	0.8998	0.5067	0.1564	-0.1712	-0.5367	-0.6732	-0.96	0.3285	0.1378	0.0398
x3	0.3003	0.7856	-0.6239	0.7377	0.7248	0.6531	-0.9837	-0.996	-0.8858	-0.3186	-0.668	0.6838	-0.702
x4	0.5051	0.2999	0.8389	0.863	0.3868	0.6001	-0.4678	-0.8869	-0.984	-0.446	-0.0959	-0.87	-0.7454
x5	0.7014	-0.0062	0.4926	0.9014	0.2283	-0.3327	-0.9548	-0.9889	-0.8386	-0.7718	-0.2189	-0.5862	-0.942
x6	0.4283	0.8908	0.9939	0.9863	-0.0332	-0.4858	-0.8077	-0.9401	0.4628	-0.671	-0.4972	-0.8589	-0.8878
x8	-0.6325	-0.3638	-0.0237	0.0433	-0.383	0.2218	0.0407	-0.5703	-0.7937	-0.2106	-0.8636	0.1913	-0.1472
x9	-0.1068	-0.474	0.3825	0.5964	-0.2838	-0.5617	-0.4061	-0.8719	-0.9325	-0.5825	-0.5225	-0.8725	-0.8296
x10	-0.8461	0.1944	0.0673	0.6616	-0.5667	-0.7473	-0.8853	-0.9603	-0.1203	0.795	-0.4203	-0.0528	-0.5811
x11	0.8189	0.4752	0.6737	0.8684	0.611	0.5869	-0.8753	-0.9714	-0.9761	-0.86	-0.5253	-0.5818	-0.8195
x12	-0.4515	0.137	0.1238	0.4197	-0.3338	-0.0208	-0.1449	-0.5521	-0.849	-0.1169	-0.2508	-0.4799	-0.5754
x13	-0.2425	-0.3259	-0.0437	0.5585	-0.0737	-0.7884	-0.5167	-0.6901	-0.8489	-0.6668	-0.3943	-0.6817	-0.9607
x14	0.6346	0.6041	0.9007	0.9223	0.9246	0.5324	-0.7758	-0.9691	-0.9958	-0.8348	-0.782	-0.9644	-0.9523
x16	-0.254	0.0267	0.8646	0.9163	-0.2641	-0.2226	-0.7133	-0.9032	-0.5395	-0.14	-0.5299	-0.7867	-0.8187
x17	0.9898	0.2858	0.4929	0.8851	0.8529	-0.1812	-0.9101	-0.9754	-0.9484	-0.9483	-0.3791	-0.1877	-0.6999
x18	0.1692	0.1632	0.477	0.5831	-0.1054	-0.6767	-0.6224	-0.8534	-0.578	-0.6563	-0.3382	-0.8211	-0.8284
x19	0.1793	0.85	0.5961	0.7709	0.9773	0.8626	-0.6896	-0.953	-0.7734	-0.5869	-0.7689	-0.0296	-0.2945
x20	0.6808	0.743	0.6658	0.8462	0.8092	0.2323	-0.9598	-0.9915	-0.9168	-0.6617	-0.6052	-0.5559	-0.7683
x21	0.2372	0.7527	0.5187	0.6736	0.123	0.7762	-0.4814	-0.8817	-0.8968	-0.7677	-0.8411	-0.9593	-0.9225
x22	-0.6479	0.8234	-0.0891	0.6687	-0.0719	0.1776	-0.9782	-0.9935	-0.9171	0.4809	-0.9068	0.0568	-0.6754
x23	0.5294	0.7081	0.8055	0.8792	0.7392	0.4716	-0.8341	-0.9722	-0.9565	-0.7665	-0.9691	-0.9162	-0.9664
x24	0.4015	-0.375	0.4042	0.8332	0.0254	0.9677	-0.5581	-0.9213	-0.9462	-0.5272	-0.3555	0.516	-0.1188
x25	0.8614	0.8407	-0.5708	0.6073	0.6827	0.3435	-0.9136	-0.9754	-0.7894	-0.8775	-0.8408	0.7582	-0.5405
x26	0.5919	0.6749	0.769	0.7771	0.6385	-0.2741	-0.7477	-0.9553	-0.7621	-0.668	-0.2115	-0.7283	-0.7468
x27	0.257	0.666	0.7643	0.7226	0.1227	0.14	-0.7438	-0.952	-0.9504	-0.5326	-0.5539	-0.6509	-0.5225
x28	0.3874	-0.1101	-0.5941	-0.681	0.5793	0.8528	-0.1117	-0.832	-0.7397	-0.6842	-0.8524	-0.1303	-0.6397
x30	-0.4122	0.3288	0.3768	0.7944	0.6	0.0168	-0.7439	-0.881	-0.8674	0.1067	-0.074	-0.6802	-0.7459
x31	0.7915	0.9023	0.876	0.9446	0.9055	0.8646	-0.4342	-0.909	-0.8361	-0.5474	-0.5553	-0.3623	-0.6641

x32	0.2542	0.3637	0.7124	0.8437	-0.1607	0.4469	-0.6587	-0.886	-0.2413	0.0503	-0.7994	-0.4465	-0.523
x33	-0.0445	-0.6858	0.9481	0.8645	-0.7562	0.2932	-0.0793	-0.9145	-0.5428	-0.9708	-0.426	0.0411	-0.4278
x34	-0.3484	-0.5718	-0.7388	-0.5751	-0.4662	0.5737	0.5729	-0.18	-0.9026	-0.5491	-0.4202	-0.4488	-0.766
x35	-0.6972	-0.4047	0.9142	0.8853	-0.6838	-0.7393	-0.7958	-0.9348	0.3519	0.5475	0.6148	-0.7111	-0.7718
x36	-0.2752	-0.1324	0.0725	-0.08	-0.1949	0.2563	-0.425	-0.6348	0.0861	0.3738	0.7281	-0.3412	-0.2304
x37	0.6948	0.8048	0.6863	0.8003	0.8781	0.1325	-0.7866	-0.9343	-0.9684	-0.9731	-0.9922	-0.9688	-0.9687
x38	-0.2408	0.3907	0.6415	0.9188	0.122	-0.6727	-0.9332	-0.9809	-0.825	0.5395	-0.567	-0.6927	-0.9419
x40	0.7851	0.774	0.9783	0.9714	0.8707	-0.5884	-0.9537	-0.9912	-0.9591	-0.7636	-0.7428	-0.9344	-0.8963
x41	-0.7001	0.9695	-0.3537	0.5591	0.9137	0.2414	-0.9301	-0.9886	-0.8832	0.6229	-0.8447	0.4042	-0.4293
x42	0.8689	-0.4331	0.9359	0.9565	0.7568	0.8211	-0.8284	-0.9523	-0.9898	-0.8024	0.2959	-0.7322	-0.8014
x43	-0.2807	-0.0924	0.7422	0.9283	-0.3051	0.2615	-0.3702	-0.7406	-0.3577	0.863	-0.52	0.2254	-0.2312
x44	-0.5321	0.8224	-0.4519	0.363	0.7074	0.2482	-0.9363	-0.99	-0.8745	0.2114	-0.6967	0.2194	-0.4919
x46	0.8618	-0.4193	0.924	0.934	0.0511	-0.3383	-0.9532	-0.9913	-0.98	-0.9572	0.3834	-0.9817	-0.9868
x48	0.1968	0.1537	0.6336	0.6993	-0.5057	-0.2824	-0.5529	-0.8169	-0.9275	-0.5517	-0.5109	-0.0465	-0.6695
x49	0.6867	0.6527	0.4389	0.6812	0.5992	-0.0023	-0.8422	-0.9445	-0.7283	-0.9112	-0.1474	-0.6352	-0.8468
x50	0.6045	-0.2092	0.2524	0.5068	0.0136	0.573	-0.4033	-0.9118	-0.391	-0.821	-0.1787	0.5714	0.4137
x52	0.9645	0.9643	0.8654	0.8919	0.8835	-0.1526	-0.997	-0.9993	-0.9725	-0.9658	-0.9438	-0.862	-0.8885
x53	-0.7329	-0.7052	0.3394	0.6238	-0.7718	0.123	-0.6017	-0.7996	-0.6761	0.7021	-0.1121	-0.369	-0.7028
x56	0.6259	0.6141	-0.4291	-0.1767	0.2982	0.5969	-0.7363	-0.9532	-0.8849	0.0041	-0.0473	0.7104	0.2609
x57	0.0936	0.703	-0.2442	0.0268	0.8327	0.7774	-0.7717	-0.9588	-0.6053	0.3868	-0.7581	0.6296	0.3479
x58	-0.1008	-0.198	0.2479	0.4466	0.8603	0.9827	-0.5727	-0.9089	-0.8289	-0.5282	-0.5723	-0.469	-0.5518
x59	0.3828	0.4072	0.8359	0.8608	0.3739	0.0852	-0.6255	-0.9416	-0.894	-0.5885	-0.6219	-0.1577	-0.6669
x60	0.6673	0.7422	0.8534	0.7783	0.7638	0.2413	-0.8392	-0.9574	-0.9133	-0.8578	-0.8012	-0.8091	-0.9178
x61	-0.4603	-0.5653	0.299	0.9279	-0.6801	-0.6257	-0.6878	-0.8603	-0.4728	0.3418	0.7819	0.2248	-0.4352
x62	0.3885	-0.2848	0.603	0.896	0.7204	0.3929	-0.8545	-0.9719	-0.9951	0.1071	-0.2032	-0.1675	-0.6278
x63	0.7864	0.6002	0.8165	0.7326	0.1568	0.0931	-0.6007	-0.9736	-0.875	-0.8743	-0.6232	-0.9448	-0.9707
x64	0.2713	-0.6989	0.7828	0.6541	-0.3959	0.6629	-0.0579	-0.7168	-0.8774	-0.8146	0.0131	-0.1393	-0.7144
x65	0.9939	0.1106	0.9688	0.9664	-0.4424	-0.1282	-0.9837	-0.9954	-0.3813	-0.9616	-0.1547	-0.9405	-0.94
x67	0.6023	-0.4979	0.9744	0.9838	-0.2392	-0.724	-0.8655	-0.9382	-0.8824	-0.8645	0.0431	-0.9228	-0.9258
x68	0.042	-0.0724	0.8798	0.9369	0.8178	0.1031	-0.6702	-0.8954	-0.4767	0.6461	0.2287	-0.2403	-0.3907
x69	-0.2505	-0.2583	0.9295	0.8901	-0.6794	-0.1831	0.5281	0.4203	-0.9728	-0.1878	-0.6973	0.4481	0.1718

x70	0.9377	0.4326	0.7787	0.8937	-0.2288	0.1191	-0.8839	-0.9832	-0.9113	-0.7066	-0.6664	-0.8029	-0.971
x71	0.3893	0.1378	0.4149	0.563	0.5097	-0.6695	-0.7824	-0.9843	-0.9472	-0.3709	-0.2969	-0.5488	-0.7221
x72	-0.6184	0.155	0.648	0.8471	-0.3019	-0.9541	-0.96	-0.9885	-0.704	0.4281	-0.3166	-0.7289	-0.8739
x73	-0.2501	0.0673	0.2238	0.4467	-0.4766	-0.7768	-0.5456	-0.7825	-0.8648	-0.2208	-0.3147	-0.5205	-0.6895
x74	0.1248	-0.146	-0.5467	0.6954	0.3087	-0.11	-0.8554	-0.9797	-0.794	-0.475	-0.2123	0.2968	-0.9292
x75	0.6485	-0.6307	0.7353	0.8199	-0.2421	-0.6698	-0.8461	-0.9587	-0.3104	-0.6564	0.4086	-0.7661	-0.8229
x76	0.8778	0.862	0.9433	0.9073	0.986	0.6282	-0.8708	-0.9889	-0.7668	-0.9676	-0.862	-0.6764	-0.5947
x77	0.1565	0.795	0.2265	0.6908	0.7653	0.4932	-0.89	-0.9891	-0.6364	0.0695	-0.5898	0.064	-0.3058
x78	-0.1892	-0.8555	0.8165	0.9123	-0.7458	-0.5885	-0.9682	-0.9884	0.0033	0.2439	0.8211	-0.7834	-0.8312
x79	0.6179	-0.2087	0.7459	0.8191	0.3977	0.5057	-0.5993	-0.9197	-0.9501	-0.4927	-0.233	0.0157	-0.1594
x81	0.03	-0.4081	0.8137	0.8824	-0.7094	-0.4488	-0.8153	-0.9002	0.2248	0.2708	-0.1245	-0.5581	-0.9686
x82	0.7156	0.1963	0.9542	0.9689	-0.2175	-0.5341	-0.332	-0.6092	-0.6716	0.1847	0.8391	-0.3687	-0.3059
x83	-0.711	-0.3384	-0.6648	-0.6311	-0.4246	-0.3403	-0.9236	-0.9653	0.6413	0.4549	0.1933	0.3334	0.2922
x85	0.5589	0.8529	0.8391	0.8611	0.8805	-0.1564	-0.9585	-0.9913	-0.9712	-0.7183	-0.7297	-0.9433	-0.9198
x86	0.5703	0.6445	0.8022	0.974	-0.3367	-0.9227	-0.9838	-0.997	-0.5129	-0.6848	-0.6566	-0.7345	-0.9409
x87	0.0996	0.3991	0.2227	-0.0096	-0.6626	0.5985	-0.4199	-0.6832	0.1467	-0.3349	-0.1404	-0.6682	-0.6531
x88	0.1222	0.9787	-0.7251	-0.3819	0.4797	0.7276	-0.8102	-0.9839	-0.4192	-0.4393	-0.7573	0.4589	0.1695
x89	-0.3758	-0.9364	0.2266	0.7701	-0.7711	0.2966	-0.9563	-0.984	-0.7471	0.3229	0.9114	-0.323	-0.8165
x90	-0.4852	-0.4789	-0.3292	-0.0366	-0.4833	0.6825	-0.2663	-0.7864	-0.2235	-0.0972	0.5046	-0.5175	-0.5008
x91	-0.8685	-0.3183	-0.4582	0.1135	-0.1581	0.2816	-0.9263	-0.9728	-0.6961	0.9088	0.3206	0.5502	-0.0256
x92	-0.3001	-0.3862	-0.3797	-0.3498	-0.5989	0.5953	0.2826	-0.6547	-0.3551	-0.4221	0.0365	-0.0373	-0.1434
x94	-0.3325	0.6295	-0.0205	0.437	-0.2063	-0.2876	-0.846	-0.952	-0.8153	0.0309	-0.4838	-0.172	-0.5136
x95	-0.3473	-0.1703	0.892	0.851	-0.6443	0.8353	-0.0836	-0.8077	-0.9475	-0.5579	-0.3436	-0.259	-0.5402
x96	0.7327	0.0637	0.6514	0.8653	0.2442	-0.2356	-0.9174	-0.9783	-0.9141	-0.473	-0.3174	-0.381	-0.6686
x98	-0.7926	0.4346	0.1777	0.3298	-0.18	-0.0062	-0.8702	-0.9506	-0.0378	0.9803	-0.6145	0.1324	-0.1661
x99	0.6343	0.6101	-0.0466	0.9236	0.7965	-0.34	-0.8603	-0.9496	-0.8751	-0.1727	-0.6502	0.4137	-0.6764
x100	0.3039	0.5495	0.8174	0.8851	0.6775	0.3216	-0.855	-0.9609	-0.4911	-0.7106	-0.2263	-0.8036	-0.78
x101	0.8542	-0.5954	0.2832	0.7171	0.6544	-0.475	-0.6551	-0.9016	-0.3859	-0.1704	0.1073	0.3675	-0.0919
x102	0.7094	0.1221	0.8673	0.8839	0.0714	0.3524	-0.7405	-0.9277	-0.9351	-0.7841	-0.5757	-0.9172	-0.964
x103	-0.6925	0.1046	-0.0017	0.4221	0.3833	0.1288	-0.8238	-0.9405	-0.6727	0.7993	-0.6036	0.2193	-0.4723
x104	0.2897	0.4859	-0.4355	0.0174	0.7748	0.8277	-0.944	-0.988	-0.9401	-0.3562	-0.5491	0.5445	0.1556

x105	0.5245	0.1443	-0.4151	0.3627	-0.5293	0.1089	-0.7697	-0.9199	-0.9136	-0.8881	-0.5625	-0.0208	-0.5234
x106	0.5307	0.9024	0.8989	0.9236	0.9552	-0.357	-0.9311	-0.9779	-0.8854	-0.6308	-0.984	-0.941	-0.9406
x107	-0.2456	-0.7615	0.0669	0.276	-0.4202	0.1523	-0.5498	-0.8335	-0.7701	-0.2874	0.0695	-0.6001	-0.8446
x108	0.3101	0.3289	-0.2423	-0.062	0.6471	0.5339	-0.9327	-0.9839	-0.841	-0.5998	-0.209	0.062	-0.0941
x110	0.6746	0.2308	0.6789	0.705	0.5302	0.4748	-0.4882	-0.9183	-0.9115	-0.9271	-0.8896	-0.7678	-0.8453
x111	-0.6448	0.7092	-0.6067	-0.207	0.4535	0.1064	-0.8298	-0.9754	-0.8673	0.2582	-0.2446	0.407	0.0061
x113	-0.5003	-0.1991	0.3002	0.3586	-0.5382	0.8665	0.6041	-0.2131	-0.7295	-0.578	-0.3104	0.571	0.4953
x114	-0.2969	0.013	0.7195	0.7426	-0.4417	0.1732	-0.8727	-0.97	-0.8009	-0.0352	-0.474	-0.839	-0.8446
x115	-0.8482	0.1121	0.3571	0.5803	-0.8988	0.2177	-0.7294	-0.8846	-0.8343	0.2723	-0.41	-0.7899	-0.8937
x116	0.2027	0.1014	0.706	0.9505	0.1509	0.799	-0.8709	-0.9754	-0.9909	-0.4563	-0.4508	-0.756	-0.8225
x117	-0.0494	-0.2043	-0.6212	-0.0056	0.4754	0.0657	-0.7365	-0.9556	-0.8979	-0.2016	0.0435	0.0533	-0.6109
x118	0.5978	-0.0375	0.7447	0.673	-0.698	-0.6977	-0.8881	-0.96	-0.5859	-0.8791	-0.3324	-0.7314	-0.8025
x119	0.1187	-0.8623	0.7449	0.6041	-0.5713	0.392	-0.1184	-0.6282	-0.9131	-0.7026	0.1786	-0.7505	-0.8331
x121	0.7944	-0.0101	0.9743	0.9762	-0.3296	-0.8398	-0.9315	-0.9714	-0.8772	-0.6592	-0.2414	-0.9057	-0.9572
x122	-0.2803	-0.5471	0.9114	0.4311	-0.4147	0.0679	-0.2989	-0.8153	-0.5023	0.1133	0.6654	-0.4189	-0.8329

Legend:
X= User
A=Mean Amplitude
B=Maximum Amplitude
C=Minimum Amplitude
D=Peak to Peak Amplitude
E=Mean Frequency
F=Maximum Frequency
G=Minimum Frequency
H=Maximum PSD
I=mean PSD
J=Minimum PSD
K= Maximum Hilbert function
L= Mean Hilbert function
M= Minimum Hilbert function