DISCRETE FRACTIONAL COSINE TRANSFORM BASED ONLINE HANDWRITTEN SIGNATURE VERIFICATION SYSTEM

A thesis submitted in the partial fulfillment of the requirement

for the award of degree of

Master of Engineering

In

Electronics and Communication

Submitted by:

Mohit Arora

Roll no:-801161031 (ECED)

Under the guidance of:

Dr. Kulbir Singh

Assistant Professor (ECED)

T.U, Patiala

ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

(Established under the section 3 of UGC Act, 1956)

PATIALA-147004(PUNJAB)

CONTENTS

CERTIFICATE

I, Mohit Arora, hereby certify that the work which is being presented in this dissertation entitled "**Discrete Fractional Cosine Transform based Online Hand Written Signature Verification**" by me in partial fulfillment of the requirements for the award of degree of Master of Engineering in Electronics and Communication Engineering from Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of **Dr. Kulbir Singh Associate Professor, ECED** and refers other researcher's works which are duly listed in the reference section.

The matter presented in this dissertation has not been submitted in any other University/Institute for the award of any other degree.

Date: 15/7/13

Mohit Arora
Roll No. 801161031

It is certified that the above statement made by the student is correct to the best of our knowledge and belief.

Date: 15/7/13

(Dr. Kulbir Singh)
Associate Professor
(ECED)
Thapar University, Patiala

Countersigned by:

Professor and HEAD ECED
Thapar University, Patiala

Dean of Academic Affairs
Thapar University, Patiala

i

ACKNOWLEDGEMENT

I would like to express my gratitude to **Dr. Kulbir Singh**, Associate Professor, Electronics and Communication Engineering Department, Thapar University, Patiala for his patience guidance and support throughout this dissertation. I am truly very fortunate to have the opportunity to work with him. He has provided me help in technical writing and presentation style, and I found this guidance to be extremely valuable.

I am very thankful to the Head of the Department, **Dr. Rajesh Khanna**, for his encouragement, support and providing the facilities for the completion of this dissertation.

I am also thankful to entire faculty and staff members of Electronics and Communication Engineering Department for their unyielding encouragement.

Last but not the least I am greatly indebted to my parents, sister, and my brother and all my friends, who have graciously applied themselves to the task of helping me with ample morale support and valuable suggestions. Finally, I would like to extend my gratitude to all those persons who directly or indirectly helped me in process and contribute towards this work.

(Mohit Arora)

ii

ABSTRACT

Several biometric modalities are currently being tested for identity verification, but amongst all the possible biometric modalities, the handwritten signature has been used for the longest period of time as a means of identification. It is commonly found in commerce and banking transactions, credit card payments, cheque authentication and, in general, all types of legal documents. Therefore, considering all the different biometric modalities, the signature is undoubtedly the most accepted for the majority of different scenarios. Advancing progress in identification applications has led to widespread demand for new generation ID documents, such as electronic passports and citizen cards, which contain additional biometric information required for more accurate user recognition. The image of the user's handwritten signature is already incorporated into ID documents. However, current error rates in verifying signature images are not yet sufficient for massive deployment. This can be overcome by embedding dynamic features of signature along with the static features within the documentation. This problem and the increasing demand for standardized signature verifications systems have motivated the research work performed in present study.

Accuracy of the hand written signature verification system depends on how these dynamic features are extracted. In literature several methodologies have been given to extract these features and since this field of signature verification is still under development phase, many methodologies are yet to be explored. One such unexplored methodology based on Fractional Transform is presented in this study. Fractional Transforms are generalization of classical transforms with an additional parameter which gives us an added degree of freedom.

There is a close relationship between the conventional Discrete Cosine Transform (DCT) and the Discrete Fractional Cosine Transform (DFrCT).The DFrCT share many useful properties of the regular cosine transform, and has a free parameter, its fraction. When the fraction is zero, we get the cosine modulated version of the input signal. When it is unity, we get the conventional DCT. As the fraction changes from 0 to 1 we get different forms of the signal which interpolate between the cosine modulated form of the signal and its DCT representation. Thus, DFrCT is a general form of DCT which has an additional free parameter, and with this free parameter it may find its place in many applications more efficiently as compare to where DCT is found to be useful.

A new method for an online handwritten signature verification based on finite impulse response (FIR) system is proposed by utilizing discrete fractional cosine transformation (DFrCT) for feature extraction. Various characteristics of the hand-written signature are used to extract different features of the signature by optimizing the value of the fractional order. The system for the hand-written signature verification is realized by characterizing three FIR systems. The impulse responses of FIR systems are used to calculate Euclidean norm. The signature can be verified by evaluating the difference between the average of Euclidean norms of reference signatures and the Euclidean norm of signature to be verified. The equal error rate (EER) is calculated to compare the efficiency of the proposed method. It has been verified through simulation results that the DFrCT tool achieves much better results as compared to discrete cosine transform (DCT) for extracting the features. The signature verification experiment was performed on SVC2004 signature database.

CONTENTS

List of Abbreviation

ID	Identity
DTW	Dynamic Time Warping
HMM	Hidden Markov Model
DCT	Discrete Cosine Transform
PDA	Personal Digital Assistant
ATM	Automated Teller Machine
PCs	Personal Computers
FT	Fourier Transform
CT	Cosine Transform
ST	Sine Transform
FrFT	Fractional Fourier Transform
DFrFT	Discrete Fractional Transform Fourier
DFrCT	Discrete Fractional Cosine Transform
DFrST	Discrete Fractional Sine Transform
SVM	Support Vector Machine
ANN	Artificial Neural Network
FIR	Finite Impulse Response
EPW	Extreme points warping
PCA	Principal Component Analysis
AFT	Affine Fourier Transform
DAFT	Discrete Affine Transform
POS	Point of Scale
dpi	Dots Per Inch
BiSP	Biometric smart pen
SFS	Sequential Forward Search
SBS	Sequential Backward Search
ICDR	Inter-intra class distance radio

NN	Neural Networks
GA	Genetic Algorithm
BPN	Back Propagation Network
RBF	Radial Basis Function
MCA	Minor Component Analysis
LR	Linear Regression
PA	Polygonal Approximation
EP	Extreme Points
MLP	Multilayer Perceptrons
FAR	False Acceptance Rate
FRR	False Rejection Rate
EER	Equal Error Rate

List of Figures

List of Tables

Chapter 1
Introduction

1.1 Preamble

The need to accurately and automatically verify claimed identities of users has become an important issue when considering new and upcoming techniques of performing electronic transactions. Unfortunately, such transactions have also increased the opportunities for fraudulent claims and “identity theft”.

The security requirements of the today’s society have placed biometrics at the center of a large debate, as it is becoming a key aspect in a multitude of applications. The term biometrics refers to individual recognition based on a person’s distinguishing characteristics. While other techniques use the possession of a token (i.e., badge, ID card, etc.) or the knowledge of something (i.e., a password, key phase, etc.) to perform personal recognition, biometric techniques offer the potential to use the inherent characteristics of the person to be recognized to perform this task. Thus, biometric attributes do not suffer from the disadvantages of either the token-based approaches, whose attributes can be lost or stolen and knowledge-based approaches, whose attributes can be forgotten.

The characteristics that are captured essentially need to be [1]:

a) **Universal:** Every person must possess the characteristic. It must be one that is seldom lost to accident or disease.
b) **Invariant:** It should be constant over long period of time.
c) **Singular:** It must be unique to individual.
d) **Inimitable:** It should be reproducible by other means.
e) **Reducible and comparable:** It should be capable of being reduced to a format that is easy to handle and digitally comparable to others.
f) **Reliable and temper-resistant:** It should be impractical to mask or manipulate.

Depending on the personal traits considered, two types of biometrics can be defined: physiological or behavioral. [2] The former are based on the measurement of biological traits of users, like, for instance, fingerprint, face, hand geometry, retina, and iris. The latter consider behavioral traits of users, such as voice or handwritten signature.

Although a wide set of biometrics has been considered so far, it is worth noting that no trait is able to completely satisfy all the desirable characteristics required for a biometric system. Thus, the assessment of a biometric trait is strongly dependent on the specific application since it involves not only technical issues but also social and cultural aspects.[2]
A biometric system can either use for verification or identification.

1.1.1Verification Based on Biometrics

During verification the user presents the biometric data to the system (data capture subsystem) and at the same time, his/her claimed identity. This biometric raw data captured is then processed (signal processing subsystems) while the biometric reference data, for the identity claimed, is retrieved from the data storage subsystem. Both elements, the features that represent the biometrics data presented by the user and the biometric reference data retrieved from the Data Storage, are compared (comparison subsystem) obtaining a similarity degree between them, generally referred to as "comparison score". This score is taken by the decision subsystem which verifies, based on a predetermined threshold level, if the claim regarding the user's identity is positive. The verification decision outcome will be successful if a true claim is accepted and a false claim is rejected. The outcome will be considered erroneous if either a false claim is accepted or a true claim is rejected.

1.1.2 Identification Based on Biometrics

Alike the verification process, during identification the user also supplies his/her biometric data to the data capture subsystem, however, in this case the claimed identity is not provided. The biometric system processes the raw data coming from the sensor and extracts the features (signal processing subsystem) and compares it to all the biometric references stored in the data storage subsystems. The biometric system attempts to locate the identifier for the users, providing a candidate list of enrolled based on the comparison scores achieved.
The outcome of this process is successful when the user is enrolled in the biometric system and his/her identity is included on the candidate list of enrolment records. Otherwise, the identification process outcome will be considered erroneous, i.e. when the user is not

enrolled and the candidate list is not empty, or the user identity is not included on the candidate list.

1.1.3 Advantages of a Biometrics System

- Increase security - Provide a convenient and low-cost additional tier of security.
- Reduce fraud by employing hard-to-forge technologies and materials. For example minimizes the opportunity for ID fraud, buddy punching.
- Eliminate problems caused by lost IDs or forgotten passwords by using physiological attributes. For example it prevents unauthorized use of lost, stolen or "borrowed" ID cards.
- Reduce password administration costs. Replace hard-to-remember passwords which may be shared or observed.
- Integrate a wide range of biometric solutions and technologies, customer applications and databases into a robust and scalable control solution for facility and network access.
- Offer significant cost savings or increasing return of investment in areas such as Loss Prevention or Time & Attendance.
- Unequivocally link an individual to a transaction or event.

1.1.4 Disadvantages of a Biometrics System

Biometric system also has some of disadvantages that can be given as:

- The finger prints of those people, who working in Chemical industries are often affected. Therefore those companies should not use the finger print mode of authentication.

- It is found that with age, the voice of a person changes. Also when the person has flu or throat infection the voice changes or if there are too much noise in the environment this method may not work correctly. Therefore this method of verification is not workable all situations.

- For those people, who affected with diabetes, the eyes get affected resulting in differences.

Despite of these disadvantages, biometric system is employed to accomplish current verification requirements. This technology provides high levels of security and is both convenient and comfortable for the user. Biometrics has already been deployed in many different scenarios, where one of the most common applications is in new generation identification documents, such as citizen ID cards and electronic passports.

1.2 Signature Verification

Several biometric modalities are currently being tested for identity verification, but amongst all the possible biometric modalities, the handwritten signature has been used for the longest period of time as a means of identification. It is commonly found in commerce and banking transactions, credit card payments and, in general, all types of legal documents. Therefore, considering all the different biometric modalities, the signature is undoubtedly the most accepted for the majority of different scenarios. The image of the user's handwritten signature is already incorporated into ID documents. However, current error rates in verifying signature images are not yet sufficient for massive deployment.

In a signature verification system, the individuals can be recognized by measuring the activity of signing, which includes information regarding the pressure applied by the pen or its speed, in addition to the visual aspect of the signatures. Being part of everyday life, signature based authentication is perceived as a non-invasive and non-threatening process by the majority of the users. Furthermore, the written signature has a high legal value. On the other hand, the signature can be influenced by physical and emotional conditions, and therefore exhibits a significant variability which must be taken into account in the authentication process. In such a system the objective is to detect three types of forgeries, which are related to intra and inter-personal variability.[3] The first type, called random forgery, is usually represented by a signature sample that belongs to a different writer of the signature model. The second one, called simple forgery, is represented by a signature sample with the same shape of the genuine writer's name the last type is the skilled forgery, represented by a suitable imitation of the genuine signature mode as shown in Figure 1.1.

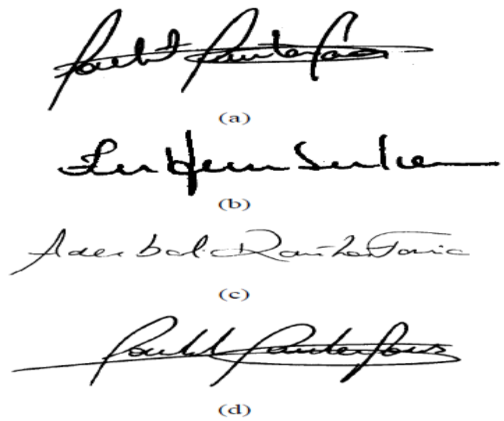


Figure. 1.1 Type of forgeries: (a) genuine signature; (b) random forgery; (c) simulated simple forgery; (d) simulated skilled forgery [3]

The possibility of incorporating dynamic features, which are unique characteristics of every user, during the act of signing, can provide additional verification mechanisms to be embedded into modern ID documents. By improving the error rates using these added characteristics, the handwritten signature will become a viable verification option for users of online processes such as e-banking and e-commerce.

1.2.1 Modes of Verification

Signature Verification Systems are generally split into two main groups: offline (commonly referred to as static) and online (referred to as dynamic). [4] The difference between these groups is based on the information acquired.

1.2.1.1 Offline Mode of Verification

In general, Offline signature verification is a challenging problem. In an offline signature verification system, a signature is acquired as an image. This image represents a personal style of human handwriting. Consequently, an offline verification system has to cope with a significant amount of errors and uncertainties in the recovered data. These difficulties are not present in the online case. [5] The problem of offline signature verification has been faced by taking into account three different types of forgeries: random forgeries, produced without knowing either the name of the signer nor the shape of his signature; simple forgeries, produced knowing the name of the signer but without having an example of his signature;

and skilled forgeries, produced by people who, looking at an original instance of the signature, attempt to imitate it as closely as possible [6]

The common approaches to offline signature verification have been to exploit the static features of the handwriting, treating the complete signature as a single entity. These techniques involve the analysis and comparison of image projections, gradient features, geometric features shadow-code descriptors, transform features, and moment features etc.

1.2.1.2 Online Mode of Verification

Online signature verification uses special hardware, such as a digitizing tablet or a pressure sensitive pen, to record the pen movements during writing. In addition to shape, the dynamics of writing are also captured in online signatures, which is not present in the 2-D representation of the signature and hence it is difficult to forge. The online signature verification methods proposed in literature can be distinguished into three main categories, which differ in the information extracted from the available data [7]:

- Global approaches, where a set of global parametric features (i.e. signature total duration, number of pen-ups, and so on) are extracted from the acquired signatures, and used to train a classifier.
- Local function based approaches, where the time functions extracted from different signatures are directly matched by using elastic distance measures, such as Dynamic Time Warping (DTW), instead to be used as features for a classifier.
- Regional function based approaches, where the acquired signatures are analyzed by estimating some regional properties, which are then employed to train a given classifier. The best regional approaches model online signatures with Hidden Markov Models (HMMs). Moreover, signatures are decomposed employing wavelet transforms, and the Discrete Cosine Transform (DCT) is applied to the resulting approximation coefficients.

1.2.2 Advantages of Signature Verification

In the point of view of adaption in the market place, signature verification presents three likely advantages over other biometrics techniques.

- It is a socially accepted verification method already in use in banks and credit card transaction.
- It is useful for most of the new generation of portable computers and personal digital assistants (PDAs) use handwriting as the main input channel.
- A signature may be changed by the user. Similarly to a password while it is not possible to change finger prints iris or retina patterns.

Therefore, automatic signature verification has the unique possibility of becoming the method of choice for identification in many types of electronic transactions, not only electronics but also for other industries.

1.2.3 Applications of Signature Verification

Signature verification has been and is used in many applications ranging from governmental use to commercial level to forensic applications. A few of them are discussed below:

- **Security for Commercial Transactions*:*** Nowadays signature verification used for commercial use. It can be used for authentication on ATMs, for package delivery companies. The internationally recognized courier service UPS has been using signature verification for many years now for personnel identification.
- **Secure computer system authentication:** Logging on to PCs can be done with a combination of signature verification system and fingerprint identification system to achieve a higher level security in a sensitive area. We can also use a combination of password and signature verification system. This would allow the users to have a higher level of security and confidentiality for their clients and protection of their work.
- **Cheque Authentication:** Signatures have been using for decades for cheque authentication in banking environment. But even experts on forgeries can make mistakes while identifying a signature. In general, offline signature verification can be used for cheque authentication in commercial environment.
- **Forensic Applications:** Signature verification techniques have been used for cheque fraud and forensic applications.

1.3 General Model for Signature Verification

The modules of signature verification system are shown in Figure 1.2. During enrollment of a new user, input to the system is a set of input signatures produced by that user. The input data is preprocessed and the features are extracted. This data is then saved in a database together with a unique identifier (ID) that is used to retrieve the signatures during matching. In addition, a threshold on the matching score is derived from the training data. For verification, a test signature along with the claimed writer identity is input to the system. The same preprocessing and feature extraction methods are applied. The signature is then compared to each of the reference (input) signatures which are retrieved from the database based on the writer identifier. The resulting difference values are combined and, based on the individual threshold for the writer; the signature is accepted as genuine or rejected as a forgery.

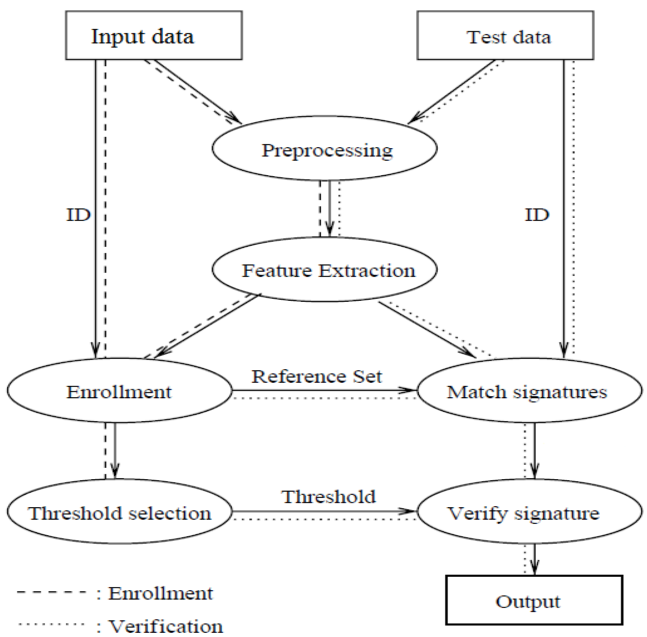


Figure. 1.2 General Model for Signature Verification [8]

1.3.1 Database Management

This module handles the process of data acquisition and maintenance of signature images and other parameters for each user. It handles the various aspects of database management like creation, modification and deletion for a signature instance. Data acquisition of static features is carried out using high resolution scanners. And the dynamic features are acquired using special devices called digitizers. The information regarding a particular signature is stored in database as a feature vector where the entire static features are stored against each user's ID.

1.3.2 Noise Removal and Preprocessing

In the preprocessing phase, the enhancement of the input data is generally based on techniques originating from standard signal processing algorithms. When offline signatures are considered, typical preprocessing algorithms concern signature extraction noise removal by median filters and morphological operators signature size normalization binarization thinning and smearing.

Typical preprocessing algorithms for online signature verification involve filtering, noise reduction, and smoothing. For this purpose, Fourier transform, mathematical morphology, and Gaussian functions have been used. Signature normalization procedures using global reference systems (center of mass and principal axes of inertia) and Fourier transform have been considered to standardize signatures in the domain of position, size, orientation, and time duration [4].

1.3.3 Feature Extraction

Two types of features can be used for signature verification: functions or parameters [9]. When function features are used, the signature is usually characterized in terms of a time function whose values constitute the feature set. When Parameter features are used, the signature is characterized as a vector of elements, each one representative of the value of a feature. In general, function features allow better performance than parameters, but they usually require time-consuming procedures for matching. Furthermore, parameters are generally classified into two main categories: global and local. Global parameters concern the whole signature; typical global parameters are total time duration of a signature, number of pen lifts, number of components, global orientation of the signature, coefficients obtained by mathematical transforms, etc. Local parameters concern features extracted from specific parts of the signature. Depending on the level of detail considered, local parameters can be divided into component-oriented parameters, which are extracted at the level of each component (i.e., height to width ratio of the stroke, relative positions of the strokes, stroke orientation, etc.), and pixel-oriented parameters, which are extracted at pixel level (i.e., grid-based information, pixel density, gray-level intensity, texture, etc.)

1.3.4 Learning

This module uses the extracted features to calculate various defined parameters such as mean, standard deviation etc for each feature. These values are placed as a vector and stored in the database against the entered identification number. The higher the number of learning samples the higher would be the accuracy.

1.3.5 Verification

This module compares the different features obtained from the test signature given to signature verification system with the features stored in the database against the given identification number. Based on this comparison, it either accepts the signature instance as being genuine or rejects it.

1.4 Fractional transform

The Fourier transform is the most important tool used in signal processing and image processing. The fractional Fourier transform is representation of time and frequency domain.
The FrFT, which is a generalization of the ordinary Fourier transform (FT), was introduced 75 years ago, but only in the last two decade it has been actively applied in signal processing, optics and quantum mechanics. The Fourier Transform (FT) is undoubtedly one of the most valuable and frequently used tools in signal processing and analysis. Little need be said of the importance and ubiquity of the ordinary Fourier transform in many areas of science and engineering. A generalization of Fourier Transform, the Fractional Fourier Transform (commonly referred as FrFT in available literature) was introduced in 1980 by Victor Namias [10] and it was established in the same year that the other transforms could also be fractionalized [11]. McBride and Keer explored the refinement and mathematical definition in 1987 [12]. In a very short span of time, FrFT has established itself as a powerful tool for the analysis of time varying signals [13]. Furthermore, a general definition of FrFT for all classes of signals (one-dimensional & multidimensional, continuous & discrete and periodic & non-periodic) was given by Cariolario et al. in. But when FrFT is analyzed in discrete domain there are many definitions of Discrete Fractional Fourier Transform [14], [19], [37]. It is also established that none of these definitions satisfies all the properties of continuous FrFT. Santhanam and McClellan first reported the work on DFrFT in 1995.

Also the cosine transform can be generalized into fractional cosine transform (FrCT). The one-sided FrCT is much more efficient when dealing with the even functions. Since it can be substituted for the FRFT under many conditions, it is believed that it will also become a useful signal processing tool in the future. By far, there have been several definitions of FRCT and discrete algorithms correspondingly. Lohmann [59] *et al.* derived FRCT by taking the real part of the kernel of FRFT. In 2001, S. C Pei [55] proposed the fractional versions of DCT by generalizing the eigenvalues into fractional order. The kernel matrix was constructed using even eigenvectors of DFT Hermite matrix, and this computation would take order $O(N2)$ complexity.

1.5 Organization of Dissertation

This dissertation consists of 6 chapters which are organized as below:

Chapter 1: Introduction, in this chapter concept of biometrics along with signature verification has been introduced. Modes of signature verification and general model for verification have also been discussed in this chapter.

Chapter 2: Literature review, in this chapter study the work which has been done regarding for designing various methods for online/offline signature verification. Along with it work related to fractional transform is also discussed in this chapter.

Chapter 3: Automatic signature verification, discusses the steps involved in signature verification. Various methods for steps involved in verification have been discussed.

Chapter 4: Fractional transforms, this chapter describes the fractional transforms i.e. fractional Fourier and fractional Cosine transform and their applications.

Chapter 5: Signature verification System using discrete fractional cosine transform is proposed and is compared with the one using DCT in this chapter.

Chapter 6: Conclusion, in this chapter whole work has been concluded, on the basis of observations and also future scope has been discussed

Chapter 2

Literature Survey

2.1 Introduction

This chapter overviews the work which has been done regarding Online/Offline signature verification system and Fractional transform along with their various design methods from time to time. On the basis of literature survey various areas of work which are still to be explored are discussed and finally the objective for dissertation has been given at the end of this chapter.

2.2 Offline Signature Verification

The contribution to signature verification considering different forgery types in an HMM framework has been reported by **E. J. R. Justino** *et al.*[3]. The work comprised of three main processes: pre-processing, segmentation and feature extraction. During the preprocessing, they proposed the horizontal segmentation to divide the written area into three zones: upper zone (ascenders), medium zone (main body) and lower zone (descends), then followed by vertical segmentation which involving the use of scales with square cells, which presented a learning process based on HMM for the segmentation. An automatic derivation process of the decision threshold was used in the matching process.

B. Fang *et al.*[15] explained, two methods to track the variations in a signature. Given the set of training signature samples, the first method measures the positional variations of the one-dimensional projection profiles of the signature patterns; and the second method determines the variations in relative stroke positions in the two-dimension signature patterns. The statistics on these variations are determined from the training set. Given a signature to be verified, the positional displacements are determined and the authenticity is decided based on the statistics of the training samples. For the purpose of comparison, two existing methods proposed by other researchers were implemented and tested on the same database.

An offline signature verification and recognition system using the global, directional and grid features of signatures has been presented by **M. E. Karslıgil** *et al.*[16]. Support Vector Machine (SVM) was used to verify and classify the signatures and a classification ratio of 0.95 was obtained. As the recognition of signatures represents a multiclass problem SVM's one-against-all method was used. We also compare our methods performance with Artificial Neural Network's (ANN) back propagation method.

A model-based method has been proposed by **K. Huang** *et al.*[5]. In this method, statistical models are constructed for both pixel distribution and structural layout description. In addition to simple geometric handwriting features, it is proposed to use the directional frontier feature as a structural descriptor of the signature. The statistical verification algorithm based on the geometric handwriting feature is used to accept signatures which closely resemble the reference samples, and to reject random and less skilled forgeries. For the questionable signatures for which the pixel feature judgment is inconclusive, the structural feature verification algorithm is invoked. This algorithm compares the detailed structural correlation between the input and reference signatures in an attempt to detect skilled forgeries.

I. S. I. Abuhaiba *et al.*[6] discusses a signature verification method based on the raw binary pixel intensities is presented. The method looks at the signature verification problem as a graph matching problem. The method is tested using genuine and forgery signatures produced by five subjects. A positive property of our algorithm is that the false acceptance rate of random forgeries vanishes at the point of equal false rejection and skilled forgery false acceptance rates. Keeping the normalization size at 32×64 pixels makes the verification time in the two seconds range.

Displacement extraction method in which a questionable signature is compared with a corresponding authentic one has been proposed by **Y. Mizukami** *et al.*[17]. The optimum displacement function for any pair of signatures is extracted using minimization of a functional defined as the weighted sum of the squared Euclidean distance between two signatures and a penalty term requiring smoothness of the displacement function. A coarse-to-fine search methods applied to avoid stopping at a local minimum, i.e. the two signatures are first transformed into coarse images by Gaussian filtering. The optimum displacement function is incorporated such that the system measures the dissimilarity between a questionable signature and the corresponding authentic one. The questionable signature is accepted as genuine only if the observed dissimilarity is below a threshold determined using the dissimilarity between two authentic signatures multiplied by a threshold coefficient.

The method proposed by **I. Guler** *et al.*[18] relies on global features that summarize different aspects of signature shape and dynamics of signature production. For designing the algorithm, it has been tried to detect the signature without paying any attention to the thickness and size of it. The results have shown that the correctness of our algorithm detecting the signature is more acceptable. In this method, first the signature is pre-processed and the noise of sample signature is removed. Then, the signature is analyzed and specification of it is extracted and saved in a string for the comparison. At the end, using adapted version of the dynamic time warping algorithm, signature is classified as an original or a forgery one.

In this paper an offline signature verification and recognition system based on a combination of features extracted such as global features, mask features and grid feature is being discussed by **B. Schafer** *et al.*[20] . The system is trained using a database of signatures. For each person, a centroid feature vector is obtained from a set of his/her genuine samples using the features that were extracted. The centroid signature is then used as a template which is used to verify a claimed signature. To obtain a satisfactory measure of similarity between template signature and the claimed signature, the Euclidean distance was used in the feature space.

2.3 Online Signature Verification

An online signature authentication system based on an ensemble of local, regional, and global matchers has been presented by **L. Nanni** *et al.*[7]. Specifically, the following matching approaches are taken into account: the fusion of two local methods employing Dynamic Time Warping, a Hidden Markov Model based approach where each signature is described by means of its regional properties, and a Linear Programming Descriptor classifier trained by global features.

A method for online handwritten signature verification where signatures are acquired using a digitizing tablet which captures both dynamic and spatial information of the writing was proposed by **A. K. Jain** *et al.*[8]. After preprocessing the signature, several features are extracted. The authenticity of a writer is determined by comparing an input signature to a stored reference set (template) consisting of three signatures. The similarity between an input signature and the reference set is computed using string matching and the similarity value is compared to a threshold.

T. Matsuura *et al.*[21] discussed FIR filter design method for signature verification. The impulse response of the FIR filter can be determined by finding the autocorrelation functions of the handwriting velocities in the horizontal and vertical directions are respectively regarded as the input and output sequences of the FIR filter and the impulse response of the FIR filter is determined from the input and output sequences The resulting impulse response can fully describe the dynamics of a given signature.

A novel method of online signature verification that analyzes both the shape of the signature and the dynamic of the writing process by have been presented by **C. Schmidt** *et al.*[22]. This approach automatically determines characteristic features of the writing image and combines these shape features with features from the writing dynamic. For establishing a writing characteristic template for one signer the signature is separated into characteristic segments. The segmentation algorithm extracts writing points which would give a forgery the appearance of the original. For these significant points local extreme values, which identify writing segments are calculated. Subsequently, dynamic features are computed for the segments. The developed system needs three signatures of one person for the establishment of a personalized template.

An online signature verification scheme based on similarity measurement of logarithmic spectrum has been discussed by **Q. Z. Wu** *et al.*[23]. The principal components of the logarithmic spectrum of each signature are extracted. The similarity of logarithmic spectrum between input signature and the reference template were computed. By comparing the similarity of logarithmic spectrum with the verification threshold, the authenticity of the input signature was determined.

A. Zimmer *et al.*[24] proposes a new hybrid handwritten signature verification system where the online reference data acquired through a digitizing tablet serves as the basis for the segmentation process of the corresponding scanned offline data. Local foci of attention over the image are determined through a self-adjustable learning process in order to pinpoint the feature extraction process. Both local and global primitives are processed and the decision about the authenticity of the specimen is defined through similarity measurements. The global performance of the system is measured using two different classifiers.

There are two common methodologies to verify signatures: the functional approach and the parametric approach. **H. Feng** *et al.*[25] proposes a new warping technique for the functional approach in signature verification. The commonly used warping technique is dynamic time warping (DTW). It was originally used in speech recognition and has been applied in the field of signature verification with some success since two decades ago. The new warping technique we propose is named as extreme points warping (EPW). It proves to be more adaptive in the field of signature verification than DTW, given the presence of the forgeries. Instead of warping the whole signal as DTW does, EPW warps a set of selected important points.

The re-evaluatation of algorithm using the database SVC2004 and the effectiveness of pen pressure, azimuth and altitude has been discussed by **D. Muramatsu** *et al.*[26]. Experimental results show that even though these features are not so effective when they are used by themselves, they improved the performance when used in combination with other features.

An approach to identify the authenticity of signatures based on the variance was reported by **L. Liu** *et al.* [27]. They combine the variance and Dynamic Time Warping algorithm to calculate the intra-class distance (between real signatures) and inter-class distance (between real-forged signatures).The results show that the former is far less than the later, so a conclusion was drawn that the deviation between real signatures is smaller than the real-forged ones when people signature. The method in this paper is simple and efficient; it also has strong stability and good recognition rate.

A camera-based online signature verification system has been proposed by **D. Muramatsu** *et al.*[28]. One web camera is used for data acquisition, and a sequential Monte Carlo method is used for tracking a pen tip. Several distances are computed from an online signature, and a fusion model combines the distances and computes a final score. Preliminary experiments were performed by using a private database.

Finite impulse response (FIR) system characterizing velocity and direction change of barycenter trajectory for signature verification has been reported by **T.Matsuura** *et al.*[29]. First, the discrete cosine transforms (DCTs) of the characteristics are used to reduce fluctuation and extract the feature of handwriting in signing process. Then the signature verification system is realized by the three FIR subsystems. The obtained impulse responses of the three FIR subsystems are used as the individual feature for signature verification. Signature can be verified by evaluating the difference between the impulse responses of the FIR subsystems for a reference signature and the signature to be verified.

S. Emerich *et al.*[30] discusses, a new online signature verification system. Firstly, the pen-position parameters of the online signature are decomposed into multi-scale signals by using the wavelet transform technique. A TESPAR DZ based method is employed to code the approximation and details coefficients, in which the waveform is divided into periods determined by successive passes through zero of the signal, thus maintaining the time information combined with a simple approximation of the waveform in-between two successive passes through zero. Thus, for each analyzed time function, a fixed dimension feature vector is obtained. The models were trained and tested with the Support Vector Machine classifier.

S. Shirato *et al.*[31] Uses a camera-based online signature verification system. Time-series images are obtained from a camera while a signature is being written. Then, online signature data are obtained by tracking the pen tip from these images with a particle filter (sequential Monte Carlo). The proposed system has an advantage that special devices such as an electronic tablet are not necessary. In this system, the signature shape obtained by tracking pen tip changes depending on the camera position because the pen tip position in the image is used. Thus, different camera positions might have an effect on verification accuracy.

A method in which the use of trajectories in isolation by first decomposing the pressure and velocity profiles into two partitions and then extracting the underlying horizontal and vertical trajectories has been reported by **M. T. Ibrahim** *et al.*[32]. So the overall process can be thought as the process which exploits the inter-feature dependencies by decomposing signature trajectories depending upon pressure and velocity information and performs verification on each partition separately. As a result, it is possible to extract eight discriminating features and among them the most stable discriminating feature is used in verification process. Further Principal Component Analysis (PCA) has been proposed to make the signatures rotation invariant. Experimental results demonstrate superiority of our approach in online signature verification in comparison with other techniques.

The algorithm for signature verification system using dynamic parameters of the signature: pen pressure, velocity and position has been discussed by **C. T. Yuen** *et al.*[33]. The system is proposed to read, analyze and verify the signatures from the SUSig online database. Firstly, the testing and reference samples will have to be normalized, re-sampled and smoothed through pre-processing stage. In verification stage, the difference between reference and testing signatures will be calculated based on the proposed threshold standard deviation method. A probabilistic acceptance model has been designed to enhance the performance of the verification system.

2.4 Fractional Transform

V. Namias [10] Introduced the concept of Fourier transforms of fractional order, the ordinary Fourier transform being a transform of order 1. The integral representation of this transform can be used to construct a table of fractional order Fourier transforms. A generalized operational calculus is developed, paralleling the familiar one for the ordinary transform. Its application provides convenient technique for solving the certain class of ordinary and partial differential equations which arise in quantum mechanics from classical quadratic Hamiltonians. The method of solution is first illustration its application to the free and to the force quantum mechanical harmonics oscillator. The corresponding Green's functions are obtained in closed form. The new techniques are extended for 3-dimensional problems and applied to the quantum mechanical description of motion of electrons in a constant magnetic field. The stationary states, energy level and evolution of initial wave are packet is obtained by systematic application rules of generalized operational calculus.

S. C. Pei *et al*.[14] explored the continuous fractional Fourier transform (FrFT) represents a rotation of signal in time-frequency plane, and it becomes an important tool for signal analysis. A discrete version of fractional Fourier transform has been developed but its results do not match those of continuous case. In this paper, authors propose a new version of discrete fractional Fourier transform (DFrFT). This new DFrFT will provide similar transforms as those of continuous fractional Fourier transform and also hold the rotation properties. This DFrFT provide a method for implementing DFrFT in digital electronic system.

Introduction to FrFT and number of its properties and some new results: interpretation as the rotation in time frequency plane and the FrFT's relationship with the time-frequency representation such as the Wigner distribution, ambiguity function, the short time Fourier transform and its spectrogram has been discussed by **L. B. Almeida** [34]. The relationship has very simple and natural form and supports the FrFT's interpretation as rotation operation. In this paper some examples of FrFT of simple signals are given. And also explain the example of its applications, showing how the use of FrFT allows a treatment of swept-frequency filters that is very similar to classical treatment of shift-invariant filter with the Fourier transform. The author presented the extension of Fourier transform which is designated as fractional Fourier transform. The linear transform depends upon the parameter alpha and can be interpreted as a rotation by angle alpha in time frequency plane.

A consolidate a definition of the discrete fractional Fourier transform that generalizes the discrete Fourier transform (DFT) in the same sense that the continuous fractional Fourier transform generalizes the continuous ordinary Fourier transform was given by **C. Candan** *et al.*[35]. This definition is based on a particular set of eigenvectors of the DFT matrix, which constitutes the discrete counterpart of the set of Hermite–Gaussian functions. The definition is exactly unitary, index additive, and reduces to the DFT for unit order. One of the most interesting avenues for future research is the establishment of the relationship of the discrete fractional Fourier transform with the discrete Wigner distribution. It might expect the study of the relationship of the Wigner distribution with the fractional Fourier transform to contribute to the establishment of a definitive definition of the discrete Wigner distribution, leading to a consolidation of the theory of discrete time-frequency analysis.

J. J. Ding *et al*. [36] Introduced a new type of DFrFT, which are unitary, reversible, and flexible; in addition, the closed-form analytic expression can be obtained. The discrete fractional Fourier transform (DFrFT) is the generalization of discrete Fourier transform. Many types of DFrFT have been derived and are useful for signal processing applications. It works in performance similar to the continuous fractional Fourier transform (FrFT) and can be efficiently calculated by FFT. Since the continuous FrFT can be generalized into the continuous affine Fourier transform (AFT) so-called canonical transform, they also extend the DFRCT into the discrete affine Fourier transform (DAFT). They will derive two types of the DFrFT and DAFT. Type 1 will be similar to the continuous FRFT and AFT and can be used for computing the continuous FrFT and AFT. Type 2 is the improved form of type 1 and can be used for other applications of digital signal processing. Meanwhile, many important properties continuous FrFT and AFT are kept in closed-form DFrFT and DAFT, and some applications, such as the filter design and pattern recognition, will also be discussed.

Fractional cosine and sine transforms that are additive on the index and preserve the similar relationships with the FrFT as the ordinary cosine and sine transforms (CT, ST) have with the FT was stated by **T.Alieva** *et al.*[54]. They derive the main properties of the fractional cosine transform (FrCT) and fractional sine transforms (FrST) and show, as examples, the FrCT and FrST of some selected signals. Although there are different ways for the fractionalization of cyclic transforms like the FT, the CT, and the ST, in this paper they consider the fractional CT and ST in relation to the fractional FT, which is more useful for signal analysis because the fractional FT corresponds to a rotation of the Wigner distribution and the ambiguity function.

S.C Pei *et al.*[55] Defines the discrete fractional cosine transform (DFrCT) and the discrete fractional sine transform (DFrST). The definitions of DFrCT and DFrST are based on the Eigen decomposition of DCT and DST kernels. This is the same idea as that of the discrete fractional Fourier transform (DFrFT); the Eigen value and eigenvector relationships between the DFrCT, DFrST, and DFrFT can be established. The computations of DFrFT for even or odd signals can be planted into the half-size DFrCT and DFrST calculations.

2.5 Comparison Table

Table 2.1: Comparison Table of Literature Review

Year	Researchers	Technique	Method
1996	T. Matsuura *et.al.*	Online	FIR filter design
1997	C. Schmidt *et al.*	Online	Establishment of Personalized Templates
1998	Q.Z.Wu *et.al.*	Online	Based on logarithmic spectrum
2000	E.J. R.Justino *et.al.*	Offline	Hidden Markov Model
2001	Y. Mizukami *et.al.*	Off line	Extracted Displacement Function
2002	A. K. Jain *et el.*	Online	String Matching
2002	K. Huang *et al.*	Offline	Statistical model
2003	A. Zimmer *et al.*	Offline/Online	Segmentation of signature
2003	B. Fang *et al.*	Offline	Tracking of feature and stroke positions
2003	H.Feng *et al.*	Online	Extreme points warping technique
2005	M. E.Karslıgil *et al.*	Offline	Support vector machine
2007	D.Muramatsu *et al.*	Online	Effectiveness of Pen Pressure, Azimuth, and Altitude Features

2007	I.S. I. Abuhaiba	Offline	Graph matching
2008	I.Guler *et al.*	Offline	dynamic time warping
2009	L. Liu *et al.*	Online	Combined variance with dynamic time warping
2009	B.Schafer *et al.*	Offline	Euclidean distance
2009	D.Muramatsu *et al.*	Online	Sequential Monte Carlo
2010	T.Matsuura *et al.*	Online	Based on DCT
2010	S.Emerich *et al.*	Online	Wavelet transforms technique**.**
2010	S.Shirato *et al.*	Online	Sequential Monte Carlo
2010	L.Nanni *et al.*	Online	Dynamic Time Warping, a Hidden Markov Model
2010	M.T. Ibrahim *et al.*	Online	Velocity and pressure-based partitions of horizontal and vertical trajectories
2011	C.T. Yuen *et al.*	Online	Probabilistic Model

2.6 Gaps in Study

Many design methodologies for hand written signature verification system have been developed till date, whether they are online verification schemes such as Sequential Monte Carlo, extreme points warping technique, Wavelet transforms technique etc. Or offline verification schemes such as Hidden Markov Model, Euclidean distance, Graph matching etc. since this field of signature verification is still under development phase, many methodologies are yet to be explored. One such unexplored methodology is Discrete Fractional Cosine Transform with an additional parameter which gives us an added degree of freedom; it may find its place in signature verification system more efficiently as compare to various methods.

2.7 Objective

On the basis of literature review of existing Hand Written Signature Verification system and gaps identified, following are the objectives of this study:

I. To study the existing online signature verification technique.

II. To develop a technique based on DFrCT

III. To compare the technique based on DCT with that of DFrCT.

Chapter 3
Automatic Signature Verification

3.1 Introduction

Handwritten signatures occupy a very special place in this wide set of biometric traits. This is mainly due to the fact that handwritten signatures have long been established as the most widespread means of personal verification. Signatures are generally recognized as a legal means of verifying an individual's identity by administrative and financial institutions. Moreover, verification by signature analysis requires no invasive measurements and people are familiar with the use of signatures in their daily life. Unfortunately, a handwritten signature is the result of a complex process depending on the psychophysical state of the signer and the conditions under which the signature apposition process occurs. Therefore, although complex theories have been proposed to model the psychophysical mechanisms underlying handwriting and the ink-depository processes, signature verification still remains an open challenge since a signature is judged to be genuine or a forgery only on the basis of a few reference specimens. [4]

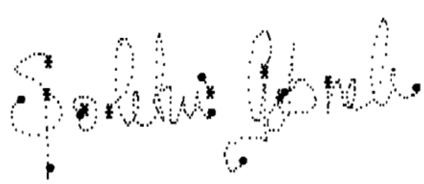
There are three main phases of automatic signature verification: data acquisition and preprocessing, feature extraction, and classification. During enrolment phase, the input signatures are processed and their personal features are extracted and stored into the knowledge base. During the classification phase, personal features extracted from an inputted signature are compared against the information in the knowledge base, in order to judge the authenticity of the inputted signature. Automatic signature verification involves aspects from disciplines ranging from human anatomy to engineering, from neuroscience to computer science and system science [38]. Because of this fact, in recent years, studies on signature verification have attracted researchers from different fields, working for universities and companies, which are interested in not only the scientific challenges but also the valuable applications this field offers. In conjunction with the recent and extraordinary growth of the Internet, automatic signature verification is being considered with new interest. The creation of specific laws and regulations, which have been approved in many countries, and the attention that several national associations and international institutes have given to the standardization of signature data interchange formats are evidence of the renewed attention in this field. The aim of these efforts is to facilitate the integration of signature verification technologies into other standard equipment to form complete solutions for a wide range of commercial applications such as banking, insurance, health care, ID security, document management, e-commerce, and retail point-of-sale (POS).

This chapter presents the main aspects related to data acquisition and preprocessing, discusses the feature extraction phase and describes activities concerning the classification phase.

3.2 Data Acquisition and Management

On the basis of the data acquisition method, two categories of systems for handwritten signature verification can be identified: offline systems and online systems as shown in Figure 3.1. In offline system acquisition devices perform data acquisition after the writing process has been completed. In this case, the signature is represented as a gray level image $\{S(x,y)\}_{0\leq x\leq X, 0\leq y\leq Y}$ where $S(x,y)$ denotes the gray level at the position (x,y) of the image. Instead, dynamic systems use online acquisition devices that generate electronic signals representative of the signature during the writing process. In this case, the signature is represented as a sequence $\{S(n)\}_{n=0,1,\ldots..N}$, where $S(n)$ is the signal value sampled at time $n\Delta t$ of the signing process, Δt being the sampling period.

(a)



(b)

Figure 3.1 (a) Offline Signature. (b) Online Signature [4]

(“∗”: pen-down; “•”: pen-up)

The most traditional online acquisition devices are digitizing tablets. In Figure 3.2 and Figure 3.3 some examples of digital tablets are shown.

Figure 3.2: Genius Tablet [58]

Figure 3.3: Wacom Tablets [58]

In general, digital tablets are connected to a computer via the USB interface. The tablet has a sensitive surface, which captures the movements from the stylus and transmits them to the computer. Tablets transmit temporal series vectors such as x and y position, pressure and, the more sophisticated tablets include inclination and azimuth. The space resolution commonly referred to as dots per inch (dpi), range from 1000 to 5000 dpi. The pressure, if present, typically ranges from 256 to 2048 levels. The inclination and azimuth angles have a resolution of approximately +/- 0.5º. These signals are sampled at frequencies ranging from 50Hz to 200Hz.

In Figure 3.4 a graphical description of the different signals captured by a digital tablet used as a signature input device is presented.

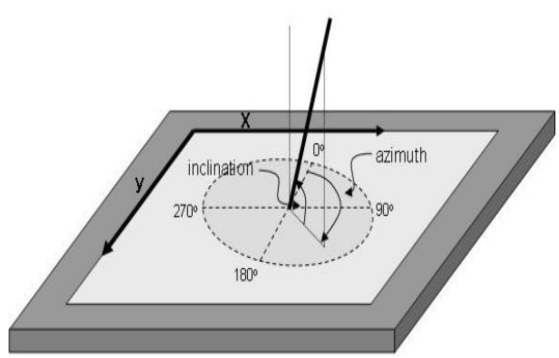


Figure 3.4: Signals Acquired by Digital Tablets [58]

As an example, the tablet used for capturing the SVC2004 database was a Wacom Intuos 2 A6, where the following signals were captured:

- X axis position
- Y axis position
- Time stamp
- Button status
- Pressure
- Azimuth angle
- Altitude

The use of these devices in industry as signature input devices is constantly growing, where their new manufacturing process follows designs which suit online signature verification specifications. These devices are widely accepted by users, and several offer interactive information for the user on the built-in screen. But in the last couple of years, new touch-screen devices have become a reality. These devices have become very popular, reaching a massive portion of the technology market. These products are: smart phones, tablets-pc and tablets as shown in Figure. 3.5. All they incorporate touch-sensitive screen.

(a) Smart-Phone **(b) Tablet PC** **(c) Tablet**

Figure 3.5: Touch-sensitive screen devices than can be used for signature acquisition

These new devices, due to their remarkable widespread coverage, are expected to play an important role in the near future of signature verification systems. Even though digital tablets are still the most used signature input device, there have been some attempts at developing a stylus capable of capturing signature dynamics without the requirement for any additional equipment.

For example, the Biometric Smart Pen (BiSP) [39] describes a stylus composed of optical sensors for recording the x and y movements, pressure sensors that record the pressure in 3 directions and also tilt sensors to measure angles [Figure.3.6]. Another stylus input device composed of accelerometers, a pressure transducer and orientations by sensing gravitational acceleration is shown in Figure 3.7.

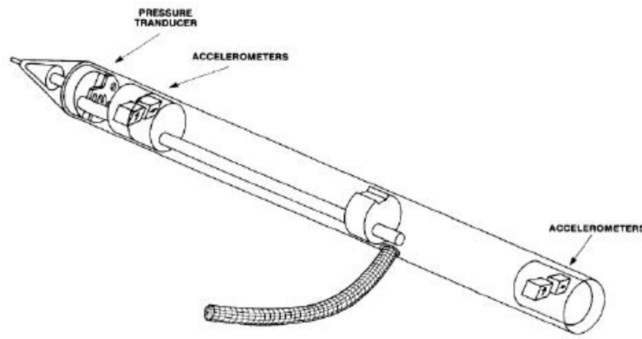


Figure 3.6: Biometric Smart Pen [39] **Figure 3.7: Accelerometer Pen [39]**

Once the features corresponding to a signature are acquired, the information regarding a particular signature is stored in database as a feature vector where the entire static features are stored against each user's ID.

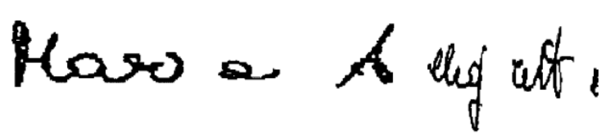
3.3 Noise Removal and Preprocessing

A crucial preprocessing step, that strongly influences all the successive phases of signature verification, is segmentation. Signature segmentation is a complex task since different signatures produced by the same writer can differ from each other due to local stretching, compression, omission or additional parts. In general, some segmentation techniques derive from specific characteristics of handwritten signatures and reflect specific handwriting models [41]. Other techniques provide segmentation results well suited for particular techniques used for signature verification. Table 3.1 [4] reports some of the most relevant techniques for signature segmentation.

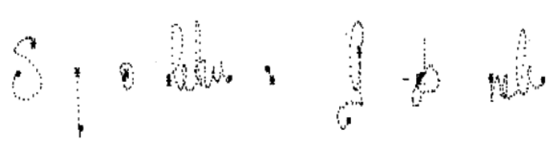
Table 3.1: Segmentation Techniques

Technique	Category
Segmentation by Pen-down/Pen-up Signals	Online
Segmentation by Velocity Signal Analysis	Online
Segmentation by Perceptually Relevant points	Online
Segmentation by Dynamic Time Warping	Online
Segmentation by Connected Components	Offline
Segmentation by Tree Structure Analysis	Offline
Segmentation by Statistics of Directional Data	Offline

The simplest segmentation approaches for offline signatures derive from structural descriptions. Some approaches perform structural analysis through the identification of connected components obtained by contour-following algorithms. Figure 3.8(a) shows the signature in Figure. 3.1(a) segmented into connected components. Other approaches describe a signature by a tree structure, obtained through the analysis of horizontal and vertical projection histograms, which identifies fundamental segments in the static image. Offline signature segmentation by statistics of directional data has also been considered. This approach permits the extraction of textured regions that are characterized by local uniformity in the orientation of the gradient, evaluated with the Sobel operator.



(a)



(b)

Figure 3.8: Examples of signature segmentation. (a) Offline signature segmentation by connected components. (b) Online signature segmentation by components (“∗” : pen-down; “•” : pen-up) [4]

Concerning online signatures, some segmentation techniques have been derived directly from the acquired signals representative of the input signature. A widespread segmentation technique that uses pressure information is based on the consideration that the signature can be regarded as a sequence of writing units, delimited by abrupt interruptions; writing units are the regular parts of the signature, while interruptions are the singularities of the signature. Thus, pen-up/pen-down signals are used to segment a signature into components, where each component is a piece of the written trace between a pen-down and a pen-up movement. Furthermore, only a finite set of components can be generated by each writer, as demonstrated by the experimental evidence that singularities can occur only in definite positions in the signature of an individual. Figure 3.8(b) shows the signature of Figure 3.1(b) segmented into components [42]. Other approaches exclusively use pen-up strokes for signature verification, since pen-up strokes can be memorized by the computer but are invisible to humans. Hence, possibility of imitating these strokes deliberately is low.

Other segmentation techniques use curvilinear and angular velocity signals. In other cases, signature segmentation is performed by the analysis of the velocity signals, also using static features, when necessary.

A different segmentation technique is based on the detection of perceptually important points of a signature [44]. The importance of a point depends on the change of the writing angle between the selected point and the neighbor. A modified version of this technique considers the end points of pen- down strokes as significant splitting points. Other approaches use perceptually important points for segmenting signatures while consider the evolutionary-distance measure, based on arc length distance, for segment association.

In order to allow the segmentation of two or more signatures into the same number of perfectly corresponding segments, dynamic time warping (DTW) has been widely used for signature segmentation [41]. After the splitting of a first signature, according to uniform spatial criteria or the position of geometric extremes, DTW is applied to determine the corresponding set of points on other specimens. A model-guided segmentation technique has also been proposed. This uses DTW to segment an input signature according to its correspondence with the reference model.

3.4 Feature Extraction

As shown in Figure 3.9 features used for signature verification are of two types: functions or parameters [44]. While using function features, the signature is usually characterized in terms of a time function whose values constitute the feature set. When parameter features are used, the signature is characterized as a vector of elements, each one representative of the value of a feature. Parameters are generally classified into two main categories: global and local. Global parameters concern the whole signature; typical global parameters are total time duration of a signature, number of pen lifts, number of components, global orientation of the signature, coefficients obtained by mathematical transforms, etc. Local parameters concern features extracted from specific parts of the signature.[4] Depending on the level of detail considered, local parameters can be divided into component-oriented parameters, which are extracted at the level of each component (i.e., height to width ratio of the stroke, relative positions of the strokes, stroke orientation, etc.), and pixel-oriented parameters, which are extracted at pixel level (i.e., grid-based information, pixel density, gray-level intensity, texture, etc.). It is worth noting that some parameters, which are generally considered to be global features, can also be applied locally, and vice versa. For instance, contour-based features can be extracted at global level or at local level

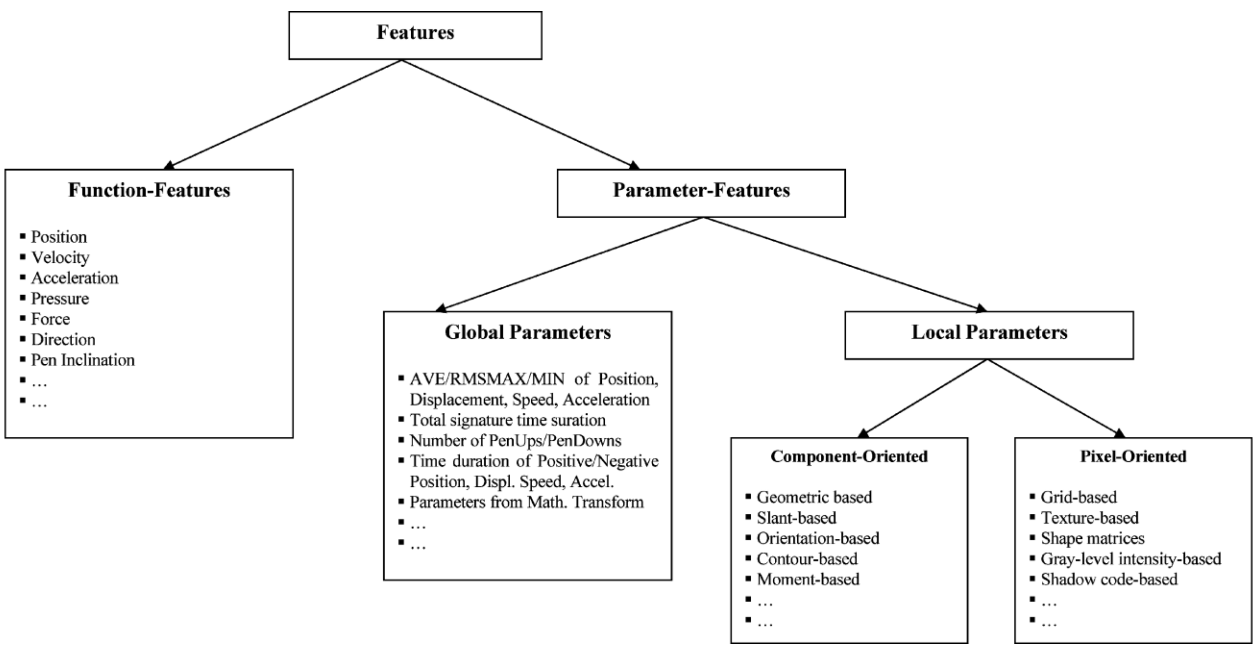


Figure 3.9: features categories for signature verification [4]

Table 3.2 [4] presents some of the most common function features being used. Position, velocity, and acceleration functions are widely used for online signature verification. Position function is conveyed directly by the acquisition device whereas velocity and acceleration functions can be provided by both the acquisition device and numerically derived from position. In recent years, pressure and force functions have been used frequently and specific devices have been developed to capture these functions directly during the signing process. In particular, pressure information, which can be registered with respect to various velocity bands, has been exploited for signature verification in order to take advantage of inter-feature dependencies. Furthermore, direction of pen movement and pen inclination have also been successfully considered to improve the performance in online signature verification, whereas pen trajectory functions have been extracted from offline signatures, in order to exploit the potential of dynamic information for offline signature verification as well. Recent studies also demonstrate that signature verification can be successfully performed by means of “motif” series, which are characteristic subsequences extracted from function features.

Table 3.2: Function Features

Functions	Category
Position	Online/Offline
Velocity	Online
Acceleration	Online
Pressure	Online
Force	Online
Direction of pen movement	Online
Pen inclination	Online

In general, position, velocity, and pen inclination functions are considered among the most consistent features in online signature verification, when a distance-based consistency model is applied. This model starts from the consideration that the characteristics of a feature must also be estimated by using the distance measure associated to the feature itself.

Table 3.3 shows some parameter features that have been widely considered for automatic signature verification [4]. Some parameters are specifically devoted to online signature verification. This is the case of some global parameters that describe the signature apposition process, as the total signature time duration , the pen-down time ratio and the number of pen lifts (pen-down, pen-up). Other parameters are numerically derived from time functions representative of a signature, like, for instance, the average (AVE), the root mean square (rms), and the maximum (MAX) and minimum (MIN) values of position, displacement, speed, and acceleration . In other cases, the parameters-that have been used for both offline and online signature verification are determined as coefficients obtained from mathematical tools as Fourier, Hadamard, cosine, wavelet and Radom transforms.

Table 3.3: Parameter features [4]

Parameters	**Category**
Total signature time duration	Online
Pen-down time ratio	Online
Number of pen Ups/Pen Down	Online/Offline
AVE/RMS/MAX/MIN of position, displacement, speed ,acceleration	Online
Time duration of positive/negative position, displacement, speed ,acceleration	Online
X-Y correlation of position , displacement, speed ,acceleration	Online
Fourier Transform	Online/Offline
Hadamard Transform	Online
Cosine Transform	Online
Wavelet Transform	Online/Offline
Random Transform	Offline
Fractal Transform	Offline
Direction-based	Online/Offline
Geometric-based	Offline
Curvature-based	Online/Offline
Structure-based	Offline
Graphometric-based	Offline
Peripheral-based	Offline
Projection-based	Offline
Slant-based	Offline
Orientation-based	Offline
Contour-based	Offline
Grid-based	Offline
Moment based	Online/Offline
Texture-based	Offline
Shape Matrices	Offline
Gray-level intensity-based	Offline
Shadow code-based	Offline
Smoothing- based	Offline
Pattern spectrum	Offline

Other parameters in Table 3.3 are more widely used for offline signature verification, when dynamic information is not available. For example, typical local features extracted from a signature at the component level are geometric-based parameters, such as signature image area, signature height and width, length to width ratio, middle zone width to signature width radio, number of characteristic points (end points, cross-points, cusps, loops, etc.), and so on. Other well-known parameters based on slant orientation, contour, direction, and curvature have also been considered. Conversely, typical parameters extracted at pixel level are grid-based features. When grid-based parameters are used, the signature image is divided into rectangular regions and well-defined image characteristics, such as ink-distribution or normalized vector angle, are evaluated in each region. Grid features and global geometric features are used to build multi-scale verification functions. Texture features have also been extracted based on the co-occurrence matrices of the signature image, shape matrices, and gray-level intensity features that provide useful pressure information.

The extended shadow code has been considered as a feature vector to incorporate both local and global information into the verification decision. A morphological shape descriptor used in signature verification is the pecstrum, which is computed by measuring the result of successive morphological openings of the image, as the size of the structuring element increases. The sequences of openings so obtained are called granulometries. A smoothness index has been used for detecting skilled forgeries in offline signature verification. This technique was inspired by expert examiners who observed that well-forged signatures are generally less smooth on a detailed scale than the genuine ones. According to an expert forensic approach, Graphometric-based parameters have also been considered, including static features (caliber, proportionality, etc.) and pseudo-dynamic features (apparent pressure, stroke, curvature, and regularity). For instance, starting from an offline signature image, pseudo-dynamic features can be used to extract information on the dynamics of the underlying signing process. This is considered by forensic experts to be a fundamental aspect concerning the authorship of the sample in question.

In general, although not every feature analyzed by a forensic examiner can easily be represented as a parameter feature extracted by a computer program—and *vice versa*, it is quite easy to find close relationships between many parameter features and some of the main features used by forensic experts.

Whatever feature set is considered, the evidence that an individual's signature is unique has led many researchers to devote specific attention to the selection of the most suitable features for a signer. Indeed, signatures from different writers generally contain very few common characteristics, and thus, the use of a universally applied feature set is not effective. Feature selection in the domain of signature verification is also required because system efficiency, processing cost, and memory requirement are strictly dependent on the cardinality of the feature set. Therefore, the smaller the feature vector, the greater the number of individuals that can be enrolled in the system and the faster speeds that can be achieved in the verification process. In recent years, several techniques have been proposed for feature selection based on principal component analysis (PCA) and self-organizing feature map, sequential forward search/sequential backward search (SFS/SBS), inter–intra class distance radios (ICDRs), and analysis of feature variability. Forgery based feature analysis has also been proposed to select feature sets well suited for random and skilled forgery, respectively. This approach has been motivated by evidence that some features are best suited for distinguishing skilled forgeries from genuine signatures whereas other features are better at distinguishing random forgeries [45].

Other approaches use the same features set for each person and face the problem of personalized feature selection by assigning a different weight to each feature. Neural networks (NNs) and genetic algorithms (GAs) have been widely used for determining genetically optimized weighted parameters, as well as for selecting optimal functions, personalized parameters, or signature strokes to be used for verification [46].

3.5 Verification

In the verification process, the authenticity of the test signature is evaluated by matching its features against those stored in the knowledge base developed during the enrolment stage. This process produces a single response (Boolean value) that states the authenticity of the test signature. The verification process involves many critical aspects that ranges from the technique for signature matching to the strategy used for the development of the knowledge base.

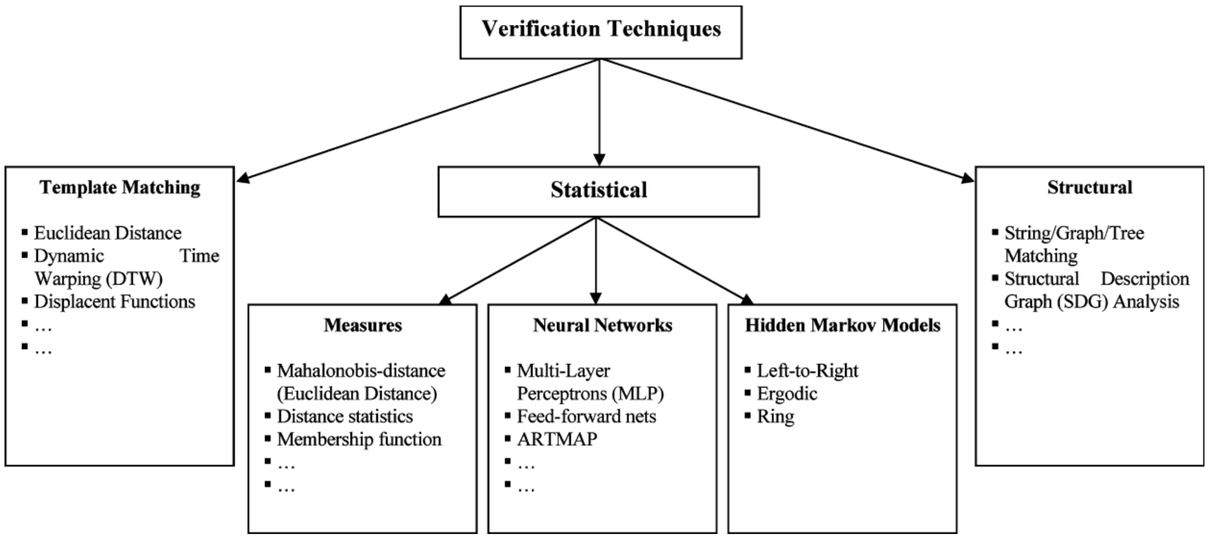


Figure 3.10 Signature verification techniques [4]

Figure.3.10 shows some of the most relevant approaches to signature verification, although blended solutions can be adopted in several cases [4]. When template matching techniques are considered, a questioned sample is matched against templates of authentic/forgery signatures. In this case, the most common approaches use DTW for signature matching. When statistical approaches are used, distance-based classifiers can be considered. NNs have also been widely used for signature verification, due to their capabilities in learning and generalizing. More recently, special attention has been devoted to the use of hidden Markov models (HMMs) for both offline and online signature verification.

The classification techniques most commonly used are reported in Table 3.4 [4]. When functions are considered, the matching problem can be complicated by random variations, due to the writer's pauses or hesitations.

DTW allows the compression or expansion of the time axis of two time sequences representative of the signatures to obtain the minimum of a given distance value. More precisely, let $T : (T_{1,} T_{2,} T_{3,} \dots, T_{N_T})$ and $R : (R_{1,} R_{2,} R_{3,} \dots, R_{N_R})$ be two online signatures, the DTW is used to determine the optimal warping function $W^*(T,R)$ minimizing a well-defined dissimilarity measure $D_{W(T,R)} = \sum_{k=1}^{K} d(c_k)$, where $c_k = (i_k, j_k)$, $(1 \le i_k \le N_T,\ 1 \le j_k \le N_R)$ and $d(c_k) = d(T_{i_k}, T_{j_k})$ is a distance measure between the samples of T and R.

Table 3.4 Comparison Techniques [4]

Technique		Category
Euclidean distance		Online/Offline
Mahalanobis Distance		Offline
Pattern Matching		Offline
Membership Function		Online
Distance Statistics		Offline
Dynamic Similarity Measure		Online
Dynamic time Warping (DTW)	Continuous	Online
	Parallel	Online
	GA-based	Online
	PCA-based	Online
	MCA-based	Online
	LR-based	Online
	PA-based	Online
	EP-based	Online
	Random-based	Online
	asymmetric	Online
Dynamic Programming		Online/Offline
Correlation		Online
Relaxation Matching		Offline
Bayesian Approach		Offline
Split and Merge		Online
String/Graph/Tree Matching		Online/Offline
Structural Description Graph		Online/Offline
Displacement Function		Offline
Support Vector Machine (SVM)		Online/Offline
Neural Network(NN)	Bayesian	Online/Offline
	Multi-Layer Perceptions (MLP)	Online/Offline
	Time-Delay	Online/Offline
	ARTMAP	Online/Offline
	Back propagation Network (BPN)	Online/Offline
	Self-Organizing Map	Online/Offline
	Fuzzy Nets	Online/Offline
	Radial Basis Functions (RBF)	Online/Offline
Hidden Markov Models (HMM)	Left-to-Right Topology	Online/Offline
	Ergodic Topology	Online/Offline
	Ring Topology	Offline

In the field of automatic signature verification, although the superiority of DTW has not been proven with respect to other comparison techniques, such as regional correlation and skeletal tree matching, DTW has been extensively used and continuous and parallel implementations have been investigated. In addition, several techniques for signature data reduction based on, Minor Component Analysis (MCA), Linear Regression (LR), Polygonal Approximation (PA), Extreme Points (EPs), and random selection have been considered. Stroke-based DTW has also been investigated. This process starts from the consideration that a comparison between the complete time sequences will not only result in higher computational load but also lead to a loss of the information related to the structural organization of the signatures. In order to avoid deformation of reference signatures when matched against test specimens, a well-suited form of asymmetric DTW was defined [47]. Other template matching approaches can use well-defined distortion measures, similarity measures, displacement functions, relaxation matching, accumulated position and velocity distances based on split-and-merge mechanisms fuzzy logic and pattern matching.

When parameters are used as features, statistical-based techniques are generally chosen. The most common approaches use Mahalanobis and Euclidean distances: Mahalanobis distance is used when the full covariance matrix is available for each signature class; Euclidean distance is considered when only the mean vector of the class is known. Membership functions and other distance statistics have also been used [48].

NNs have been widely used for automatic signature verification for a long time, as demonstrates. Table 3.4 shows some of the NN models that have been used recently: Bayesian NNs, multilayer perceptrons (MLPs), time-delay NNs, ARTMAP NNs, back propagation neural networks (BPNs), self-organizing maps, and radial basis functions (RBFs). Fuzzy NN, which combine the advantages of both NNs and fuzzy rule-based systems, has also been considered [49]. A transform can reproduce a time-series pattern assuming a constant linear velocity to model the temporal characteristics of the signing process; another transform can map the signal onto a horizontal versus vertical velocity plane, where the variation of the velocities over time is represented as a visible shape. Instead, other approaches first modify the test signature to the template signature by dynamic programming (DP) matching, and then, use an NN to compare dynamic information along the matched points of the signatures. Although NNs have demonstrated good capabilities in generalization, they require large amounts of learning data that are not always available. Recently, intensive research has been devoted to HMMs [50]. These models have found to be well suited for signature modeling since they are highly adaptable to personal variability. Strictly speaking, a HMM is a double stochastic approach in which one underlying yet unobservable Process may be estimated through a set of processes that produce a sequence of observations. Concerning the field of signature verification, various HMM topologies have been considered so far, as Figure 3.11 shows. Most approaches use the left-to-right HMM topology, since it is considered well suited for signature modeling. Ergodic topology has also been considered for both online and offline signatures verification. Furthermore, in order to guarantee invariance to signature rotation, ring topology has been adopted, which is equivalent to left-to-right topology and a transition from the last state to the first state is allowed. However, independent of the topology used, HMM [50] seem to be superior to other signature modeling techniques based on structural descriptions and fuzzy approaches. Some results have also demonstrated that HMM-based systems for offline signature verification can outperform human verifiers.

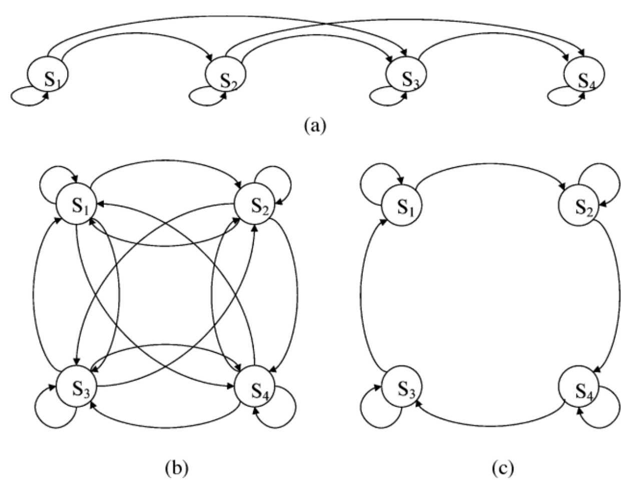
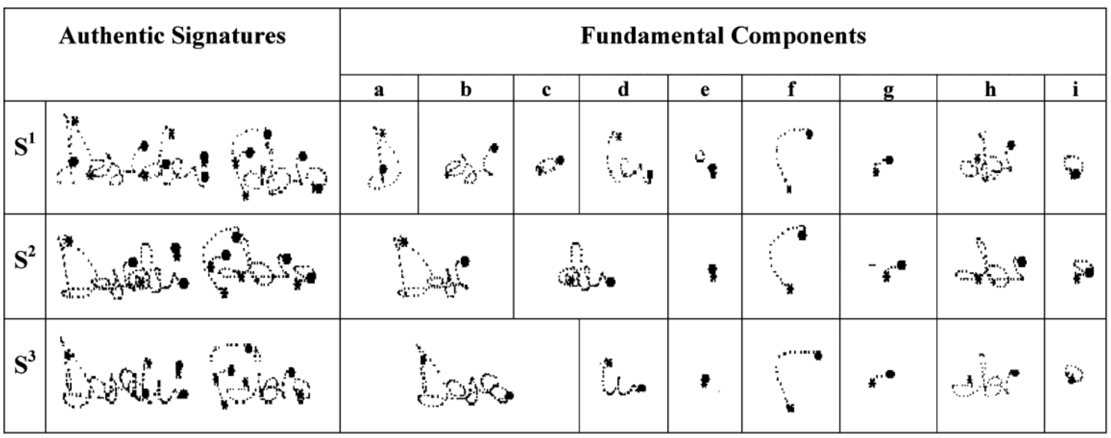


Figure 3.11: HMM topologies. (a) left-to right. (b) Ergodic. (c) Ring [4]

Furthermore, recent approaches use HMM in combination with autoregressive models while the signature is decomposed into pseudo-stationary segments and represented by a one-dimension spatial stochastic sequence. The effect of interpersonal and intrapersonal variability on HMM has also been investigated, as well as the possibility of automatically and dynamically deriving various author-dependent parameters by cross-validation.

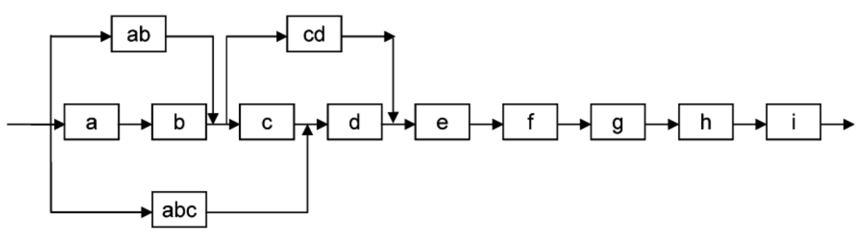
Support vector machines (SVMs) are another promising statistical approach to signature verification [51]. An SVM is a new classification technique in the field of statistical learning theory and it has been successfully applied in many pattern recognition applications. An SVM can map input vectors to a higher dimensional space in which clusters may be determined by a maximal separating hyper plane. SVMs have been used successfully in both offline and online signature verification.

Structural approaches [52] mainly concern string, graph, and tree matching techniques and are generally used in combination with other techniques. For instance, string matching is used not only for signature verification but also for signature identification purposes, via advanced local associative indexing. In other cases, the structural description graph is used to verify the structural organization of a questioned signature, as Figure. 3.12 illustrates.



(a)

S^1 = ("a", "b", "c", "d", "e", "f", "g", "h", "i"); S^2 = ("ab", "cd", "e", "f", "g", "h", "i"); S^3 = ("abc", "d", "e", "f", "g", "h", "i")



(b)

Figure 3.12 Structural description of signatures. (a) Description of authentic signatures by components. (b) Structural description graph [4]

Furthermore, the verification at stroke level can be performed by DTW, also considering multiple function features for stroke representation (like position, velocity, and acceleration) in order to verify both the shape and dynamics of each part of the signature.

Along with the matching techniques, attention has been given to knowledge-base development also in relation to learning strategies and signature modeling techniques. In particular, special attention has been given to writer-dependent learning strategies using only genuine specimens. In this case, a first approach uses a single prototype of genuine signatures for each writer, and several techniques have been proposed for the development of the optimal average prototype for a signer, including shape and dynamic feature combination, time- and position-based averaging, or selecting the genuine specimen with the smallest average difference, when compared to the other true signatures available. After the prototype has been determined, the decision threshold is generally defined on the basis of the difference values that can be determined from the genuine signatures. A second approach uses a set of genuine signatures for reference. In this case, a crucial problem concerns the selection of the optimal subset of reference signatures, among the specimens available. When offline signature verification is considered, the validity of the reference model has been evaluated according to specific quality criteria, as for instance, intra-class variability that should be as low as possible. In Online signature verification, the selection of the best subset of reference signatures has been performed on the basis of the analysis of variance within samples or by considering the stability regions in the signatures, determined by a well-defined analysis of local stability. The selection of the best subset of reference signatures can be avoided at the cost of using multiple models for signature verification. Furthermore, knowledge-base development involves the problem of having a lack of sufficient reference data to characterize a given signature class, as is generally the case of many practical applications. Thus, specific research has been devoted to feature modeling, also using regularization techniques that estimate the statistical significance of small-size training sets. Other approaches propose the generation of additional training samples from the existing ones by convolutions, elastic matching and perturbations [4].

Chapter 4
Fractional Transforms

4.1 Introduction

In recent years, the concept of fractional operator and measure has been investigated extensively in many engineering applications and science. Four typical examples are described as follows. The first is that the fractional derivative and integral are defined by many mathematicians and applied to solve some physical problems. The second is that the fractional Fourier transform has been studied in the optical community and signal processing area. The third is that the fractional dimension is used to measure some real-world data such as coastline, clouds, dust in the air, and networks of neurons in the body. The fractional dimension has been applied widely to pattern recognition and classification. The last is that the fractional lower order moment has been used to analyze non-Gaussian signals, which is more realistic than the Gaussian model in signal processing applications.

The fractional Fourier transform (FrFT) is a generalized Fourier transform, in addition, the FrFT is a special case of the more general linear canonical transform, and it provides a tool to compute the mixed time and frequency components of signals. The interpretation of the FrFT is a rotation of signals in the time–frequency plane. The FrFT is a generalization of the ordinary Fourier transform with an order parameter 'a' and is identical to the ordinary Fourier transform when this order α is equal to $\pi/2$ [34]. Since the ordinary Fourier transform and related techniques are of importance in various different areas like communications, signal processing and control systems, it is natural to expect the FrFT to find many applications in these fields as well. The FrFT belongs to the class of time–frequency representations that have been extensively used by the signal processing community. In all the time–frequency representations, one normally uses a plane with two orthogonal axes corresponding to time and frequency. If we consider a signal x(t) to be represented along the time axis and its ordinary Fourier transform X(f) to be represented along the frequency axis, then the Fourier transform operator (denoted by F) can be visualized as a change in representation of the signal corresponding to a counter clockwise rotation of the axis by an angle $\pi/2$ [11].

This is consistent with some of the observed properties of the Fourier transform (FT). For example, two successive rotations of the signal through π/2 will result in an inversion of the time axis. Moreover, four successive rotations will leave the signal unaltered since a rotation through 2π of the signal should leave the signal unaltered. The FrFT is a linear operator that corresponds to the rotation of the signal through an angle which is not a multiple of π/2, i.e. it is the representation of the signal along the axis u making an angle α with the time axis.

4.2 Fractional Fourier Transform

The FrFT $F^{\alpha}(\mu)$ of a function $f(x)$ is defined as [34]

$$F^{\alpha}(u) = R_F^{\alpha}[f(x)](u) \tag{4.1}$$

$$F^{\alpha}(\mu) = \frac{1}{2}\int_{-\infty}^{\infty} k_{\alpha}(x,u) f(x)\, exp\left(-\frac{jux}{sin\ \alpha}\right) dx, \tag{4.2}$$

where α is the rotation angle, $k_{\alpha}(x,u)$ is the kernel and is given by

$$k_{\alpha}(x,u) = \frac{exp(j\frac{1}{2}\alpha)}{\sqrt{j\ sin\ \alpha}}\, exp\left[\frac{1}{2} j(x^2+u^2)\, cot\ \alpha\right] \tag{4.3}$$

Note that for $\alpha = \frac{1}{2}\pi$, for which $k_{\frac{\pi}{2}}(x,u) = 1$. We have the normal FT. while for $\alpha = 0$ we have the identity transformation: $F^0(x) = f(x)$. Moreover note that for $k_{\alpha+\pi}(x,u) = k_{\alpha}(x,u)$, and hence $F^{\alpha+\pi}(u) = F^{\alpha}(-u)$, and that $k_{-\alpha}(x,u) = k_{\alpha}^{*}(x,u)$, and that $k_{\alpha}(x,u) = k_{\alpha}(u,x)$. and that $k_{\alpha}(\pm x,u) = k_{\alpha}(x,u) = k_{\alpha}(x,\pm u)$.

From the linearity of the FrFT and the reversion property [54]

$$R_F^{\alpha}[f(-x)](u) = R_F^{\alpha}[f(x)](-u) = F^{\alpha}(u). \tag{4.4}$$

We have

$$R_F^{\alpha}[f(x) \pm f(-x)](u) = F^{\alpha}(u) \pm F^{\alpha}(-u), \tag{4.5}$$

And it is concluded that the FrFT of an even function is even. While the FrFT of an odd function is odd.

4.3 Fractional Cosine Transform

We now restrict ourselves to a one-sided function $f(x)$, with $f(x) = 0$ for $x < 0$, and define the FrCT as [54]

$$F_c^{\alpha}(u) = R_c^{\alpha}[f(x)](u) \tag{4.6}$$

$$F_c^\alpha(u) = R_F^\alpha[f(x) + f(x)](u) \tag{4.7}$$

$$F_c^\alpha(u) = F^\alpha(u) + F^\alpha(-u) \qquad (u \geq 0) \tag{4.8}$$

$$F_c^\alpha(u) = \sqrt{\frac{2}{\pi}} \int_0^\infty k_\alpha(x,u) f(x) \cos\left(\frac{ux}{\sin\alpha}\right) dx\,, \tag{4.9}$$

Which reduces to normal CT for $\alpha = \frac{1}{2}\pi$. To express in a different way, the relationship between the FrFT of a causal, one-sided function and the FrCT of this function, we can write the kernels of the fractional transform R^α

$$R_F^\alpha : \left(\frac{1}{\sqrt{2\pi}}\right) k_\alpha(x,u) \exp\left(-\frac{jux}{\sin\alpha}\right), \tag{4.10}$$

$$R_c^\alpha : \left(\frac{2}{\sqrt{2\pi}}\right) k_\alpha(x,u) \cos\left(\frac{ux}{\sin\alpha}\right), \tag{4.11}$$

We can say that R_c^α is related to the even part of R_F^α. In general to determine the FrCT of a causal, one-sided function $f(x)$, one can determine the FrFT of evenly extended two-sided function $f(x) + f(-x)$.

4.4 Eigen Functions and Eigen Values

With $\psi_n(x)$ the Hermite-Gauss functions [54]

$$\psi_n(x) = \left(\sqrt{\pi} 2^n n!\right)^{-\frac{1}{2}} \exp\left(-\frac{x^2}{2}\right) H_n(x), \tag{4.12}$$

Where $H_n(x)$ are the Hermite polynomials, we have

$$R_F^\alpha = \left(\frac{1}{\sqrt{2\pi}}\right) k_\alpha(x,u) \exp\left(-\frac{jux}{\sin\alpha}\right), \tag{4.13}$$

$$R_F^\alpha = \frac{\exp\left(j\frac{1}{2}\alpha\right)}{\sqrt{j \sin\alpha}} \exp\left[\frac{1}{2} j(x^2 + u^2)\cot\alpha\right] \exp\left(-\frac{jux}{\sin\alpha}\right), \tag{4.14}$$

$$R_F^\alpha = \sum_{n=0}^\infty \psi_n^*(x)\, \psi_n(u) \exp(-jn\alpha), \tag{4.15}$$

Thus

$$R_c^\alpha = \left(\frac{2}{\sqrt{2\pi}}\right) k_\alpha(x,u) \cos\left(\frac{ux}{\sin\alpha}\right), \tag{4.16}$$

$$R_c^\alpha = \left(\frac{1}{\sqrt{2\pi}}\right) k_\alpha(x,u) \left[\exp\left(-\frac{jux}{\sin\alpha}\right) + \exp\left(\frac{jux}{\sin\alpha}\right)\right], \tag{4.17}$$

$$R_c^\alpha = \left(\frac{1}{\sqrt{2\pi}}\right) [k_\alpha(x,u) + k_\alpha(x,-u) \exp(-j(-u)ux/\sin\alpha)], \tag{4.18}$$

$$R_c^\alpha = \sum_{n=0}^\infty \psi_n^*(x)\, \psi_n(u) \exp(-jn\alpha) + \sum_{n=0}^\infty \psi_n^*(x)\, \psi_n(-u) \exp(-jn\alpha), \tag{4.19}$$

$$R_c^\alpha = \sum_{n=0}^\infty \psi_n^*(x) [\psi_n(u) + \psi_n(-u)] \exp(-jn\alpha)\,, \tag{4.20}$$

$$R_c^\alpha = 2 \sum_{n=0}^\infty \psi_{2n}^*(x)\, \psi_{2n}(u) \exp(-j2n\alpha), \tag{4.21}$$

Thus it is concluded that, while Hermite-Gauss functions $\psi_n(x)$ are the Eigen functions of the FrFT with Eigen values $exp(-jn\alpha)$, the even-order Hermite-Gauss functions $\sqrt{2\psi_{2n}(x)}$ are the Eigen functions of the FrCT. The FrCT Eigen functions $\sqrt{2\psi_{2n}(x)}$ are orthonormal on the half range,

$$2\int_0^\infty \psi_{2n}(x)\psi_{2m}(x)\,dx = \delta_{n,m} \tag{4.22}$$

4.5 Basic Properties

From the general observations made in the previous section, we conclude that many properties [54] of the FrFT immediately translate to the FrCT. In particular, for all fractional transforms the *additive property* for the angle α holds,

$$R^{\alpha_1}R^{\alpha_2}[f(x)](u) = R^{\alpha_1+\alpha_2}[f(x)](u), \tag{4.23}$$

from which we conclude that the inverse of any fractional transform corresponds to the transform with the negative angle.

With $tan\,\beta = \lambda^2\,tan\,\alpha$ (and with the additional condition $\lambda > 0$ in the case of fractional CT) And with C defined as

$$C = \sqrt{cos\beta/\,cos\alpha}\,\frac{exp\left(\frac{j\alpha}{2}\right)}{exp\left(\frac{j\beta}{2}\right)}exp\left[\frac{ju^2}{2}cot\,\alpha\left(1-\frac{cos^2\beta}{cos^2\alpha}\right)\right], \tag{4.24}$$

Scaling property for FrCT is as that for FrFT

$$R_c^\alpha[f(\lambda x)](u) = CR_c^\beta[f(x)]\left(\frac{usin\beta}{\lambda sin\alpha}\right), \tag{4.25}$$

If we shift a causal, one sided function $f(x)$ away from the origin $f(x) \rightarrow f(x-x_o)$ we have the same *shifting property* for the FrCT

$$R^\alpha[f(x-x_o)](u) = exp\left[-jx_o sin\alpha\left(u-\frac{1}{2}x_o cos\alpha\right)\right]\times R^\alpha[f(x)](u-x_o cos\alpha), \tag{4.26}$$

As far as *modulation or shifting* in the u domain is concerned for the FrFT we have

$$R_F^\alpha[f(x)](u-u_o sin\alpha) = exp\left[-ju_o cos\alpha\left(u-\frac{1}{2}u_o sin\alpha\right)\right]\times R_F^\alpha[f(x)\,exp(ju_o x)](u), \tag{4.27}$$

For the FrCT we have

$$R_c^\alpha[f(x)](u-u_o sin\alpha) = exp\left[-ju_o cos\alpha\left(u-\frac{1}{2}u_o sin\alpha\right)\right]\times R_c^\alpha[f(x)\,cos(u_o x)](u), \tag{4.28}$$

Fractional transforms satisfy the *symmetry relation* i.e.

$$R^{-\alpha}[f(x)](u) = \{R^\alpha[f^*(x)](u)\}^* \tag{4.29}$$

And while the FrFT is *periodic* in α with period 2π and satisfies the half-period relation

$$R_F^{\alpha+\pi}[f(x)](u) = R_F^{\alpha}[f(x)](-u) \tag{4.30}$$

The FrCT is *periodic* with period π:

$$R_c^{\alpha+\pi}[f(x)](u) = R_c^{\alpha}[f(x)](u), \tag{4.31}$$

4.6 Applications of Fractional Transform

- FrFT has many applications in optics, especially in wave and beam propagation, wave field reconstruction, phase-space tomography.
- It has also been used for study of time- or space – frequency distributions.
- Its application in biometrics for iris verification is also reported.
- In signal processing applications this transform is basically used for filtering, signal recovery, signal reconstruction, signal synthesis, beam forming, signal detectors, correlators, image recovery, pattern recognition and matched filtering.
- It can also be used for multistage and multi channel filtering, multiplexing in fractional Fourier domains and adaptive windowed FrFT

In general, the FrFT is likely to have something to offer in every area in which FT and related concepts are used.

Chapter 5

Signature Verification System using DFrCT

5.1 Implemented Technique

In this dissertation, an online signature verification method based on DFrCT is proposed. A previously implemented technique based on DCT [29] has been taken as reference to develop the proposed signature verification system. In place of DCT in the block diagram DFrCT is employed to extract the features as shown in Figure 5.1. The method is based on three FIR systems. In first of the above three mentioned FIR systems, Discrete fractional cosine transformation (DFrCT) [55] of barycenter trajectory in the horizontal and vertical direction are used as the input and the output of the system. In the second FIR system, the DFrCTs of the direction change and the magnitude of velocity of the barycenter trajectory are used as the input and the output of the system. Lastly, in the third FIR system, the DFrCTs of the areal velocity and the displacement are used as the input and the output of the system, respectively. The impulse responses of FIR systems are used as features in order to verify a signature.

5.2 Overview of the System

System purposed for online hand written signature verification system shown in Figure 5.1 consists of following steps:

- **Input signature**: Here a standard database SVC2004 [56] is used for experimentation. Corresponding to each user, 40 signatures are provided, out of which 20 signatures are genuine and 20 signatures are forgery.
- **Preprocessing process**: In order to remove the fluctuations, signature is firstly being preprocessed by normalizing the size, location and trajectory of barycenter of a given signature
- **Features extraction**: After preprocessing of a given signature, of many described features six features namely horizontal pen point movement, vertical pen point movement, areal velocity, displacement from trajectory of barycenter, magnitude of

velocity, change of angle trajectory of barycenter have been extracted. DFrCT of these features are used to define three FIR systems to characterize a given signature.

- **Signature verification**: To verify a given signature, impulse responses of FIR systems are used. All impulse response are combined together to form a feature vector. Euclidean norm of this vector is used to set the threshold level for a given signature. To verify a given signature threshold level of the signature is compared to the reference signature, if difference of reference signature and given signature is less than the threshold, the given signature is genuine else it is a forgery.

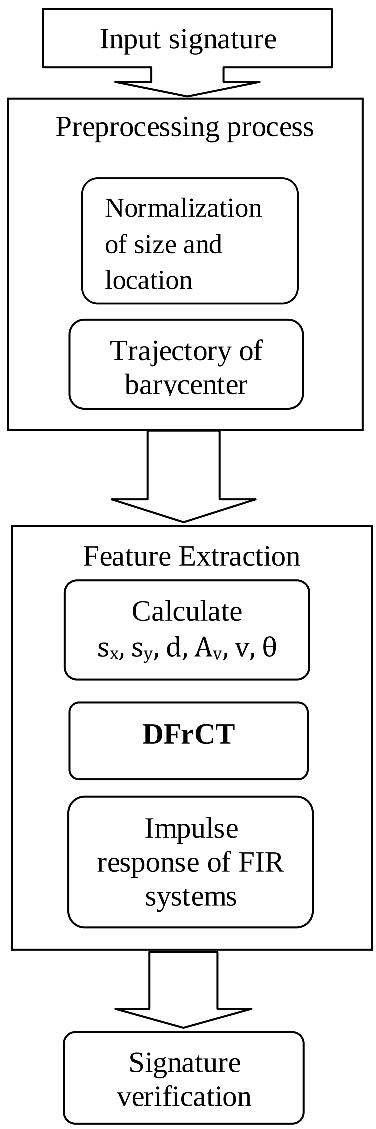


Figure 5.1: Overview of the system

5.3 Database: SVC2004

The SVC2004 database was released in 2003 to assist participants develop and test algorithms for the first signature verification contest (SVC2004). The capture device was a Wacom Intuos 2 A6 tablet, acquiring x and y position, pressure and 2 angles (inclination and azimuth) from each user. Every user contributed 20 genuine signatures during 2 different sessions. For privacy reasons, the signers were advised not to use their real signatures. Instead, they were recommended to design a new signature specifically for the database. Another 20 forgery signatures were provided by at least four other users. In order to forge the signatures, forgers had the opportunity to see the genuine signatures to be copied using a software application. This software application allowed forgers to replay the writing sequence of a signature. Forgers were advised to practice skilled forgeries until they were confident of their reproduction.

This database contains signatures from Chinese users, who could choose to sign in either Latin characters or Chinese characters.

5.4 Preprocessing Process

It is known that a graphical tablet has been used to collect the horizontal and vertical components, $x(t_n)$ and$y(t_n)$, of pen point movement at a time t_n. Since the signatures signed by same person can never be precisely the same so it is considered as fluctuations of handwriting in signing process. Such fluctuations can be reduced as follows [29]:

5.4.1 Normalization of Size

By making a standard size of signatures will reduce the fluctuations related to the size of the signature as:

$$\hat{a}(t_n) = \frac{a(t_n) - a_{min}}{a_{max} - a_{min}}, \tag{5.1}$$

Where,$a = x, y$, $a_{min} = min\, a(t_n)$, $a_{max} = max\, a(t_n)$

5.4.2 Normalization of Location

Fluctuations related to location of signature can be reduced by shifting the coordinates of center point of signature to the origin as follows:

$$c_a = \frac{1}{N}\sum_{n=0}^{N-1} \hat{a}(t_n), \tag{5.2}$$

$$\tilde{a} = \hat{a}(t_n) - c_a\,, \quad (n = 0,1,2,3 \dots\dots N-1),$$

Where, c_a is the center point of signature and N is the total number of sampled points of pen point movement.

5.4.3 Trajectory of Barycenter

Trajectory of barycenter is used to reduce the fluctuation of pen-point movement. It is determined from the center point of signature and two adjacent pen-point positions with respect to time. Trajectory of barycenter of a signature is calculated as:

$$s_a(t_n) = \frac{\tilde{a}(t_n)+\tilde{a}(t_{n+1})}{3} \tag{5.3}$$

5.5 Feature Extraction

Dataset Out of many features possessed by an online signature, following six features have been considered for verification process [29].

- Horizontal component of pen-point movement.
- Vertical component of pen point movement.
- Areal velocity $A_v(t_n)$ along the trajectory of signature.

$$A_v(t_n) = \frac{1}{2}\begin{vmatrix} s_x(t_{n-1}) & s_y(t_{n-1}) \\ s_x(t_n) & s_y(t_n) \end{vmatrix} \tag{5.4}$$

- Displacement $d(t_n)$ which is the from the center of signature to barycenter trajectory at time t_n

$$d(t_n) = \sqrt{s_x(t_n)^2 + s_y(t_n)^2} \tag{5.5}$$

- Velocity $v(t_n)$ of barycenter trajectory at time t_n

$$v(t_n) = \sqrt{u_x(t_n)^2 + u_y(t_n)^2} \tag{5.6}$$

where

$u_x(t_n) = s_x(t_{n+1}) - s_x(t_n)$

$u_y(t_n) = s_y(t_{n+1}) - s_y(t_n)$

- The direction change $\theta(t_n)$ of barycenter trajectory.

$$\theta(t_n) = tan^{-1} \frac{s_y(t_{n+1}) - s_y(t_n)}{s_x(t_{n+1}) - s_x(t_n)} \tag{5.7}$$

Furthermore, in order to extract individual features, discrete fractional cosine transform (DFrCT) $G_x(m)$, $G_y(m)$, $G_d(m)$, $G_{Av}(m)$, $G_v(m)$, and $G_\theta(m)$ of the $s_x(t_n)$, $s_y(t_n)$, $d(t_n)$, $A_v(t_n)$, $v(t_n)$ and $\theta(t_n)$ respectively is calculated [57] as

$$G^\alpha(m) = A_\alpha \sum_{n=0}^{N-1} K_p\,(m,n) g(n) \tag{5.8}$$

$$(n = 0,1,2,3 \ldots \ldots N-1)$$

where, $g(n)$ is individual characteristics of the signature, α is the rotation angle, the parameter A_α and the kernel $K_p(m,n)$ are given as follows:

$$K_p(m,n) = exp(\frac{i(m^2+n^2)\pi cos\alpha}{N}) \cos(\frac{2\pi mn}{N})$$

$$(m,n = 0,1,2,3 \ldots \ldots N-1)$$

$$A_\alpha = \sqrt{\frac{2 - i2\cot\alpha}{\pi}} \sqrt{\frac{2\pi\sin\alpha}{N}}$$

Signature verification system consisting of three FIR systems [29] is introduced in order to characterize the individual features of signature. In first system in order to characterize the relation between the horizontal and vertical components of barycenter trajectory, the DFrCTs $G_x(m)$ and $G_y(m)$ are used as the input and the output of the FIR system as

$$G_y(m) = \sum_{m=0}^{M} h_1(m) G_x(k-m) \tag{5.9}$$

In second system in order to characterize the relation between direction change and velocity, the DFrCTs $G_\theta(m)$ and $G_v(m)$ are used as the input and the output of the FIR system as

$$G_v(m) = \sum_{m=0}^{M} h_2(m) G_\theta(k-m) \tag{5.10}$$

In third system in order to characterize the relation between areal velocity and displacement, the DFrCTs $G_{Av}(m)$ and$G_d(m)$ are used as the input and the output of the FIR system as

$$G_d(m) = \sum_{m=0}^{M} h_3(m) G_{Av}(k-m) \tag{5.11}$$

Where $h_1(m),\ h_2(m),\ h_3(m)$ are the impulse responses of the corresponding FIR systems, M is the order of system, $\hat{G}_y(k)$, $\hat{G}_v(k)$, and $\hat{G}_d(k)$ are approximations of $G_y(m)$, $G_v(m)$ and $G_d(m)$ respectively. By minimizing the least-square error at M the impulse responses $h_1(m),\ h_2(m),\ h_3(m)$ can be obtained as follows:

$$E_1 = \sum_{k=0}^{M-1} \left[G_y(k) - \hat{G}_y(k)\right]^2 \tag{5.12}$$

$$E_2 = \sum_{k=0}^{M-1} \left[G_v(k) - \hat{G}_v(k)\right]^2 \tag{5.13}$$

$$E_3 = \sum_{k=0}^{M-1} \left[G_d(k) - \hat{G}_d(k)\right]^2 \tag{5.14}$$

5.6 Signature Verification

The impulse responses so far obtained are used to verify the signature and the algorithm [29] for the same is given below:

Step 1: Feature vectors of the signatures from the impulse responses of FIR systems are defined as

$$h_1^{'} = [h_1(0), h_2(0), h_3(0), \dots \dots .. h_1(m)] \tag{5.15}$$

$$h_2^{'} = [h_1(0), h_2(0), h_3(0), \dots \dots .. h_1(m)] \tag{5.16}$$

$$h_3^{'} = [h_1(0), h_2(0), h_3(0), \dots \dots .. h_1(m)] \tag{5.17}$$

Step 2: Combine the feature vectors to form a single feature vector corresponding to a signature as

$$h^{'} = [h_1^{'}\ h_2^{'}\ h_3^{'}] \tag{5.18}$$

Step 3: The Euclidean norm of feature vector of signature to be verified is compared with the Euclidean norm of the reference signature. If this difference is less then threshold of a particular signature then the signature is consider to be genuine otherwise it is a forge signature i.e.

$$\text{If } \left|\left|h^{ref} - h\right|\right| > \eta \qquad \text{true}$$

$$\text{Otherwise,} \qquad \text{false}$$

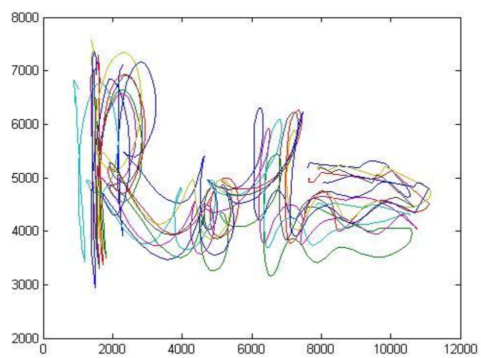
where $\|\,.\,\|$ is Euclidean norm and η is a threshold value for a particular signature.

5.7 Simulation Results

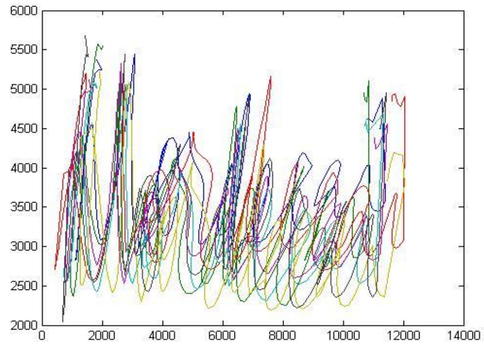
Few examples of the simulated results are discussed in this section. Various extracted features and characteristics corresponding to a given signature are shown graphically over here.

Original and Normalized Signatures

Figure 5.2 shows the original signatures of two users, it can be seen from the Figure that all signatures from same user are different, i.e. the fluctuations due to size and location can be seen.



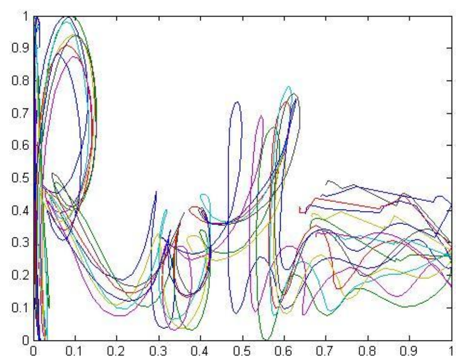
(a) Original signatures of user 1



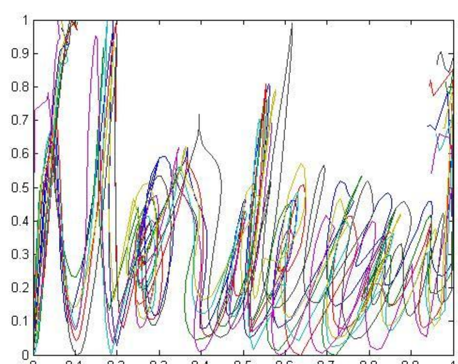
(b) Original signatures of user 2

Figure 5.2: original signatures

To reduce the fluctuations due to size and location normalization of signatures is done. Figure 5.3 show the signatures two users after normalization of size and Figure 5.4 show the signatures after location normalization.

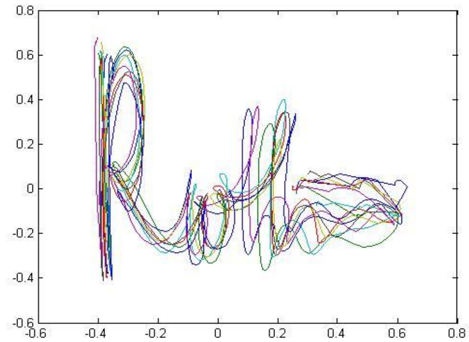


(a) Signatures of user 1 after size normalization

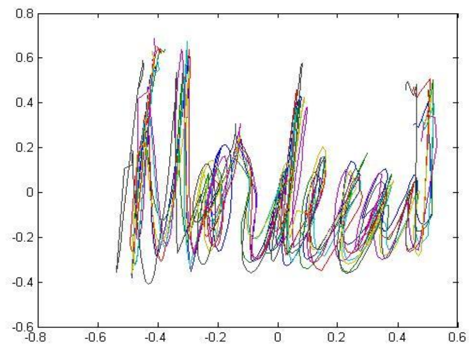


(b). Signatures of user 2 after size normalization

Figure 5.3: Signatures after size normalization



(a) Signatures of user 1 location normalization

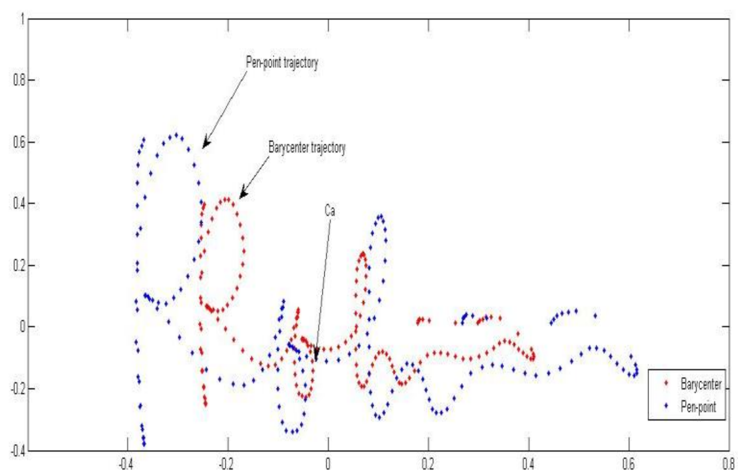


(b) Signatures of user 2 location normalization

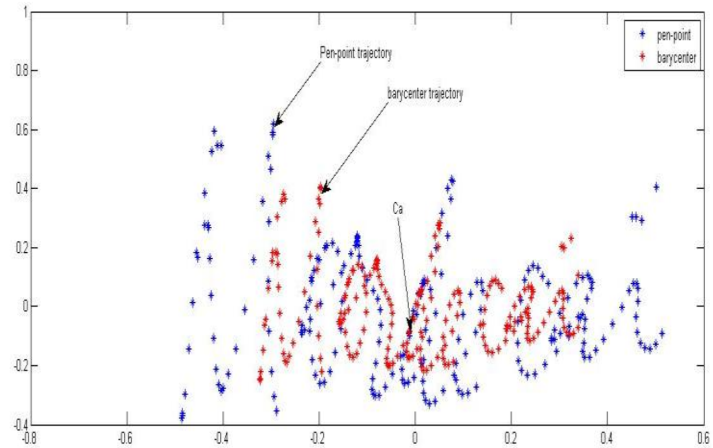
Figure 5.4: Signatures after location normalization

Trajectory of Barycenter

To reduce the fluctuations due to pen-point movement trajectory of barycenter is calculated and is show in Figure 5.5



(a) Trajectory of barycenter of signature of user 1



(b) Trajectory of barycenter of signature of user 2

Figure 5.5: Trajectories of pen-point position and barycenter of signature

Features of Signatures

Various features extracted out of given signatures are shown in Figure 5.6 & Figure 5.7 corresponding to user 1 and user 2 respectively. A comparison between features of genuine and forgery signatures are shown here.

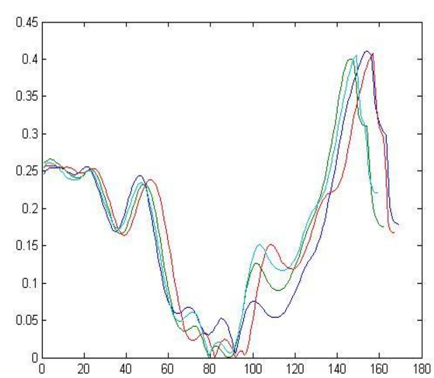
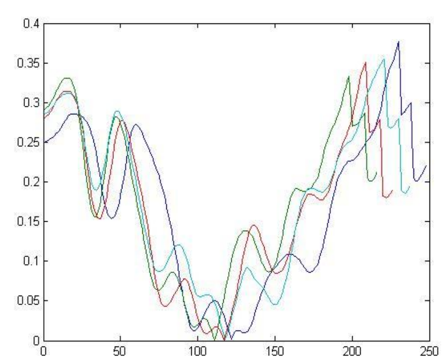
	Features of signatures of user 1	
	Genuine signature	**Forgery signature**
Horizontal component	 **(a)**	 **(b)**

Figure 5.6: Feature of signatures of user 1(contd.)

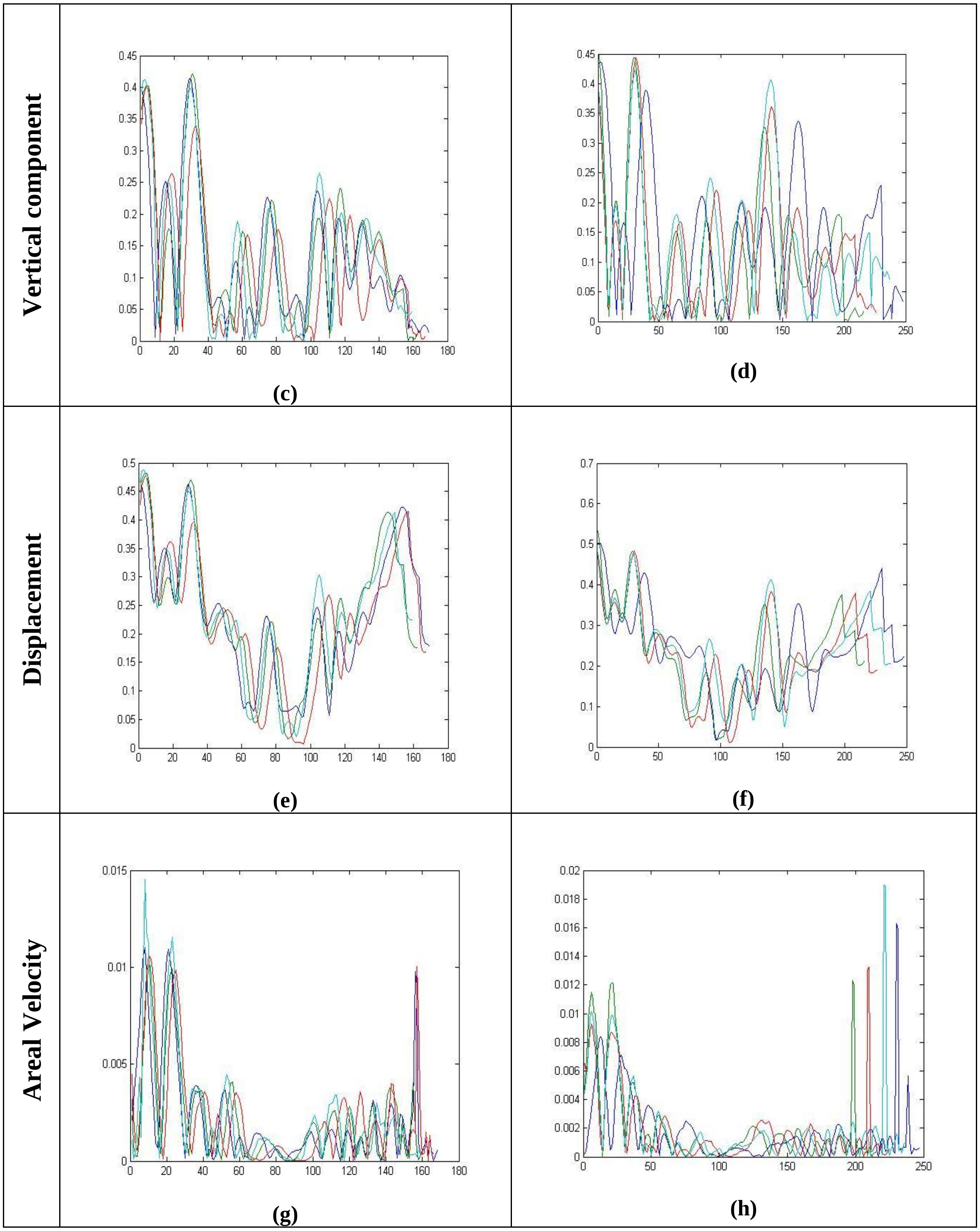


Figure 5.6: Feature of signatures of user 1(contd.)

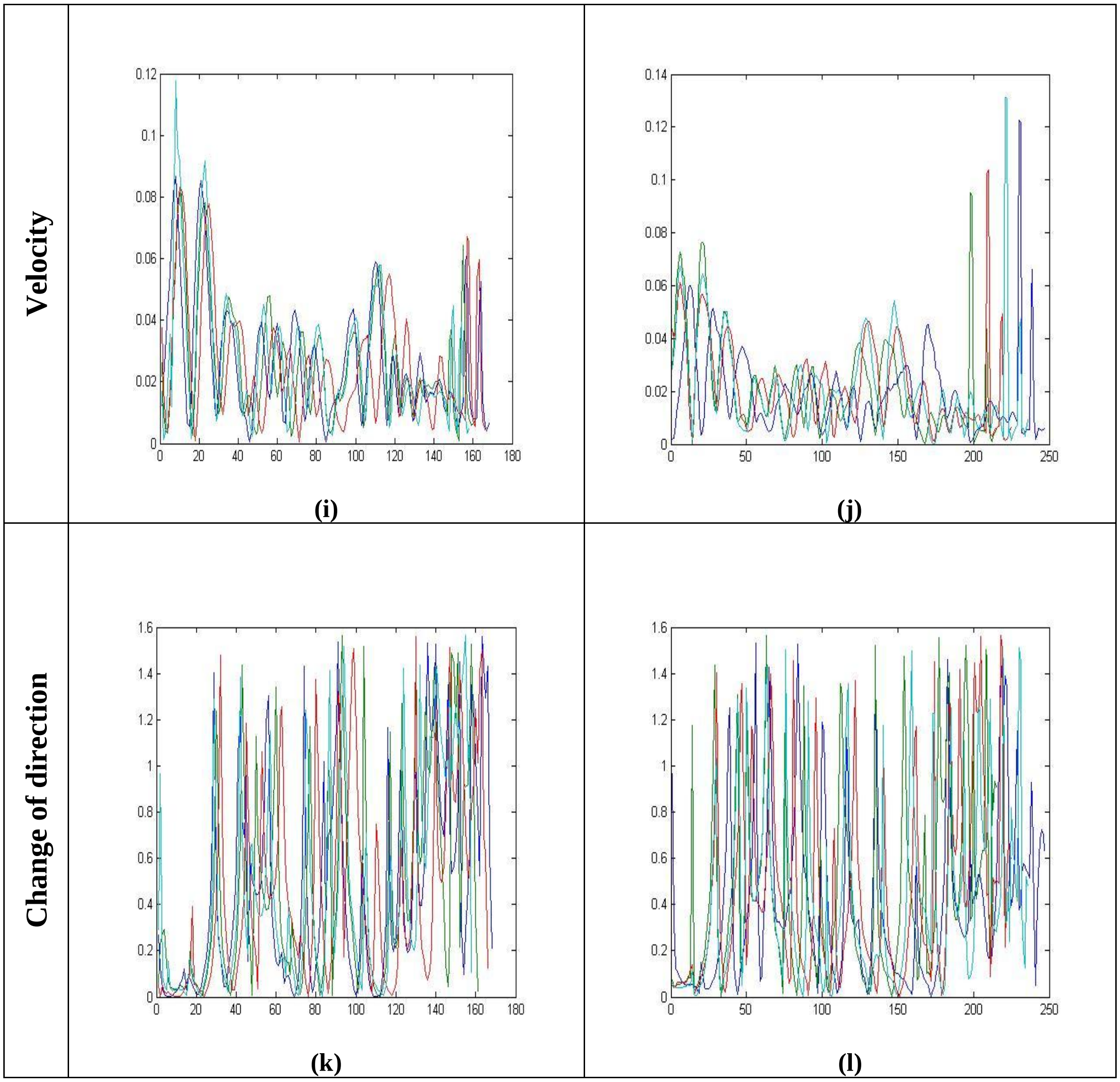


Figure 5.6: Feature of signatures of user 1

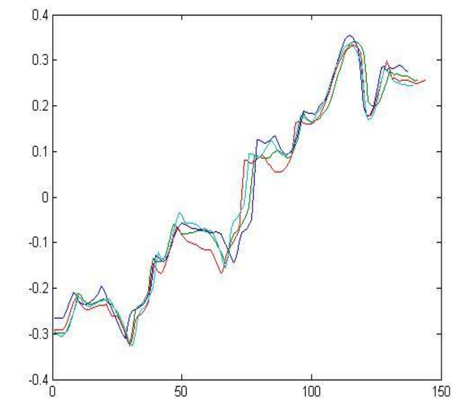
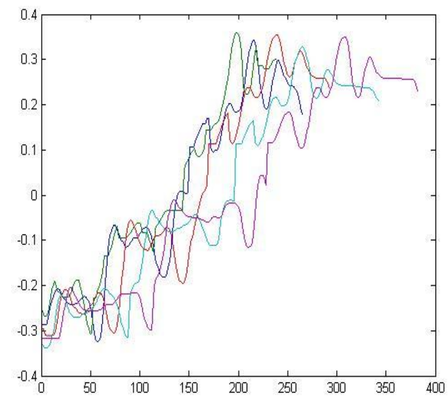
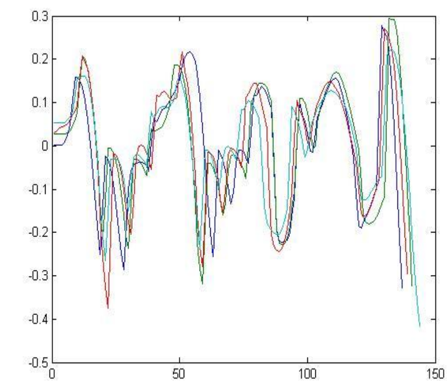
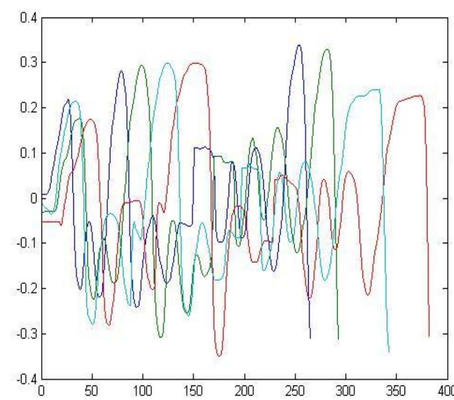
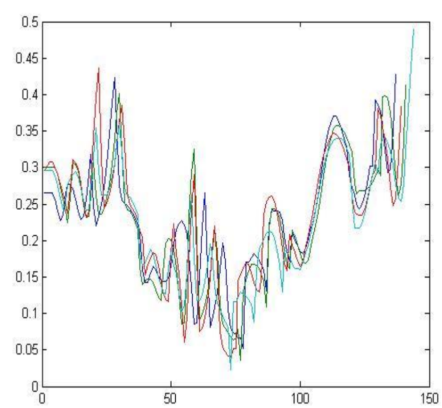
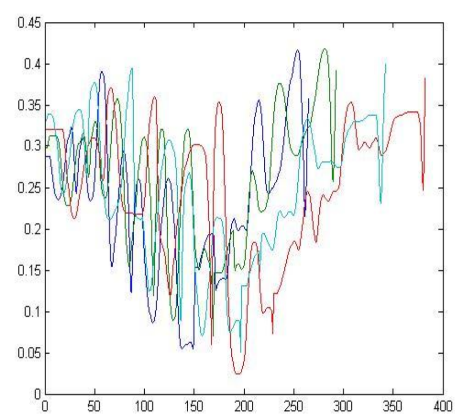
	Features of signature of user 2	
	Genuine signature	**Forgery signature**
Horizontal component	 **(a)**	 **(b)**
Vertical component	 **(c)**	 **(d)**
Displacement	 **(e)**	 **(f)**

Figure 5.7: Feature of signatures of user 2 (contd.)

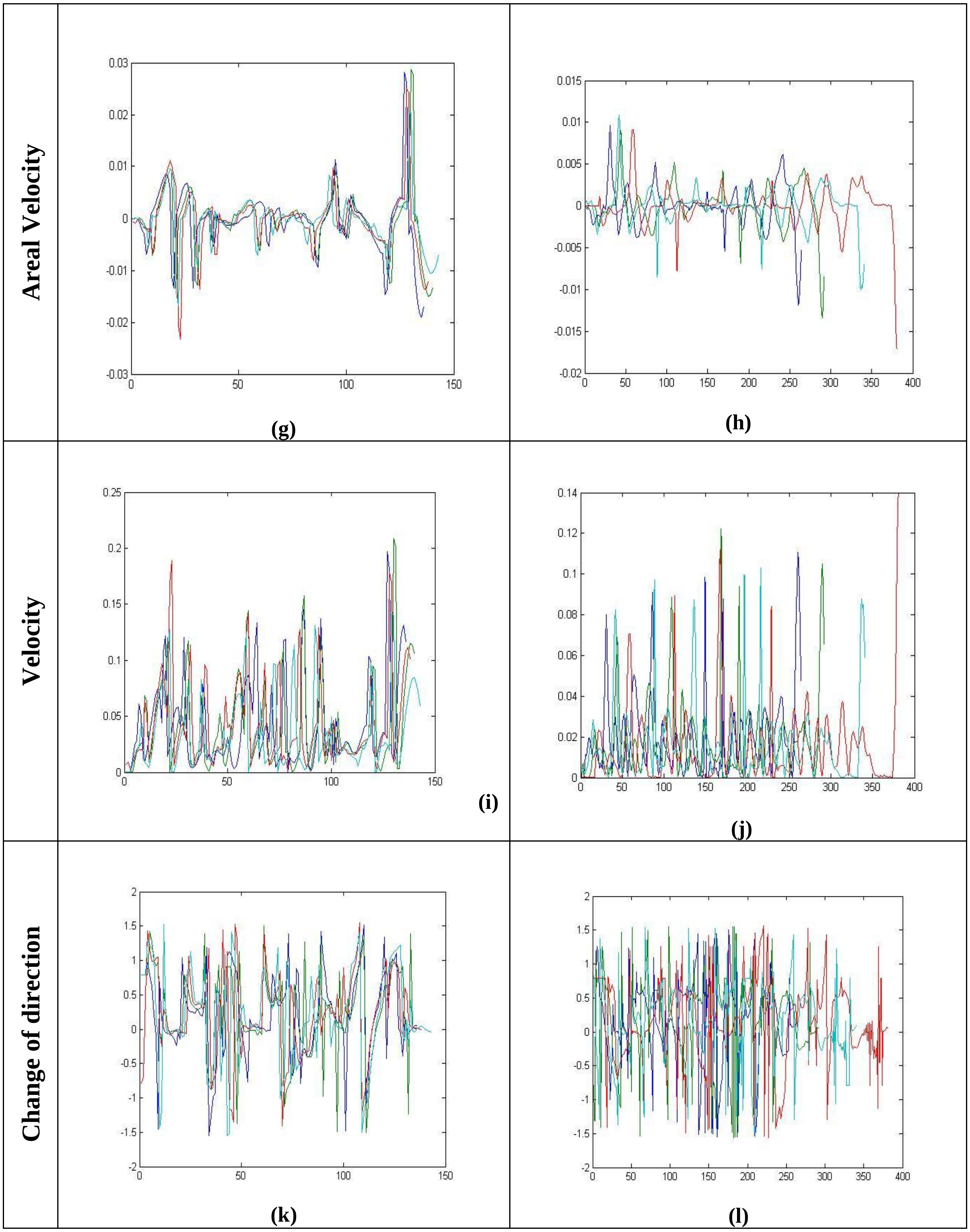


Figure 5.7: Feature of signatures of user 2

DFrCT of Features of Signatures

Figure 5.8 & Figure 5.9 shows the DFrCT's of various extracted features corresponding to the signatures of user 1 and user 2. Graphically it can be visualized the difference in profile of genuine and forge signature.

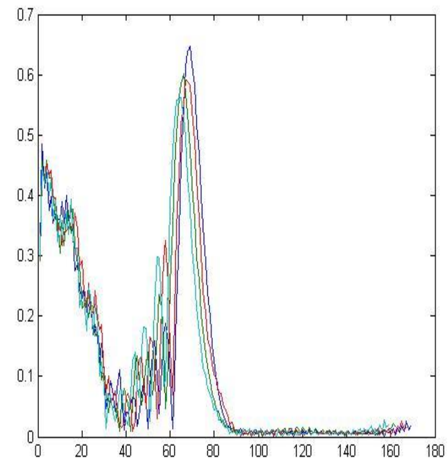
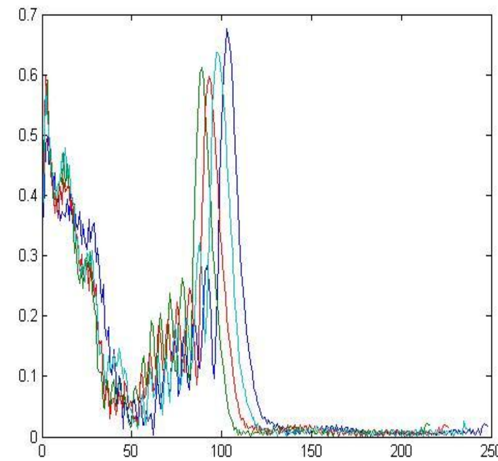
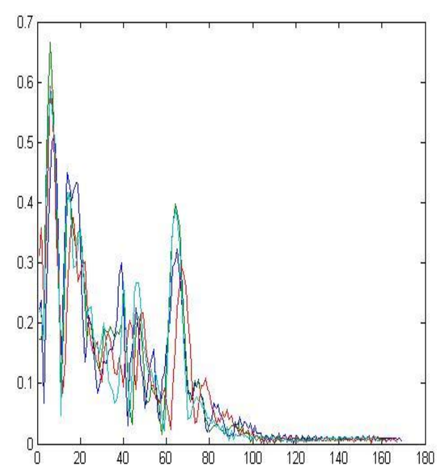
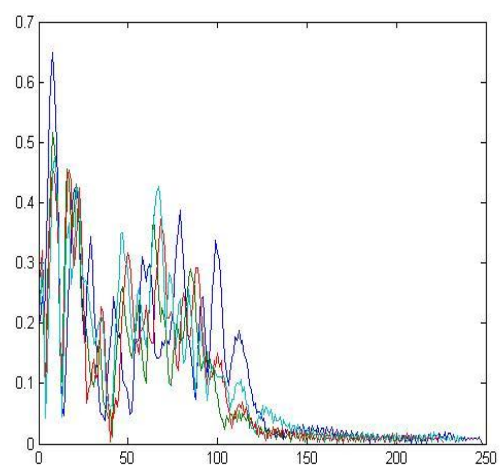
	DFrCT of Features of signature of user 1	
	Genuine signature	**Forgery signature**
DFrCT of Horizontal component	 **(a)**	 **(b)**
DFrCT of Vertical component	 **(c)**	 **(d)**

Figure 5.8: DFrCT of features of signatures of user 1 with 'α'=.76 (contd.)

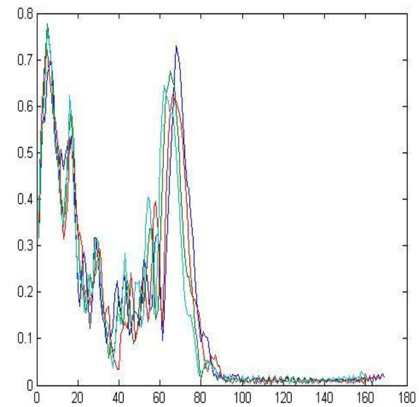
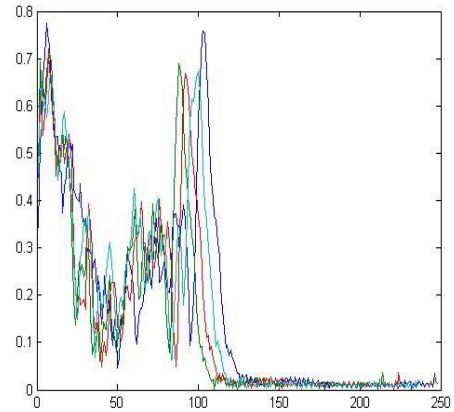
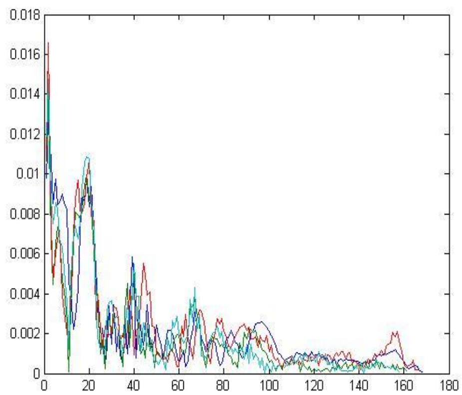
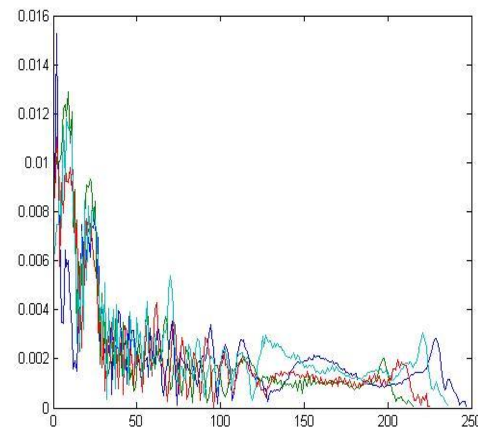
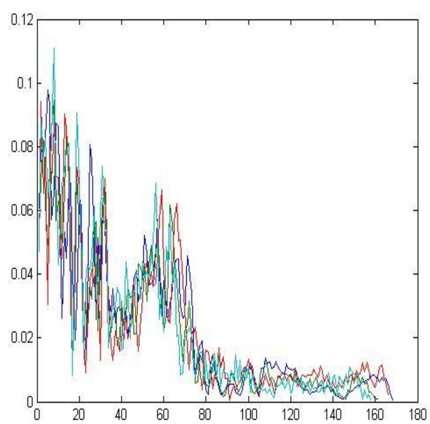
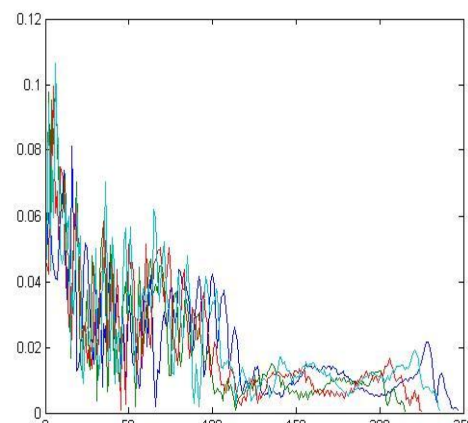
DFrCT of Displacement	 **(e)**	 **(f)**
DFrCT of Areal Velocity	 **(g)**	 **(h)**
DFrCT of Velocity	 **(i)**	 **(j)**

Figure 5.8: DFrCT of features of signatures of user 1 with ‘α’=.76 (contd.)

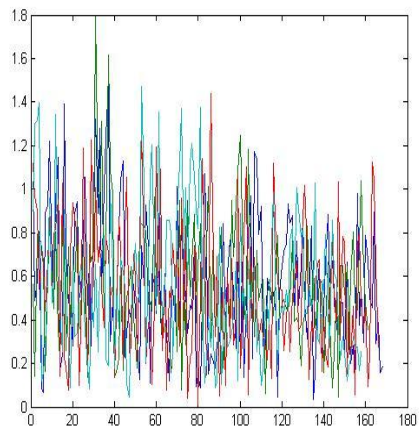
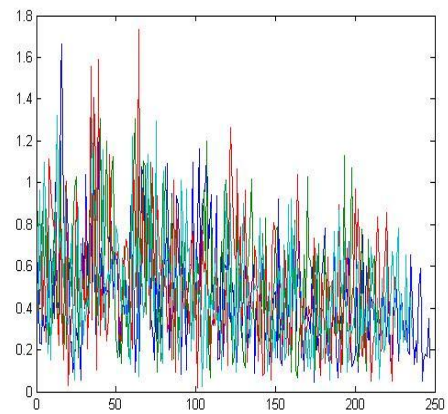
DFrCT of Change of direction	 **(k)**	 **(l)**

Figure 5.8: DFrCT of features of signatures of user 1 with ‘α’=.76

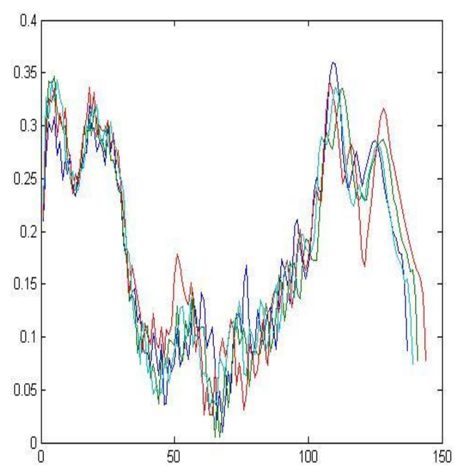
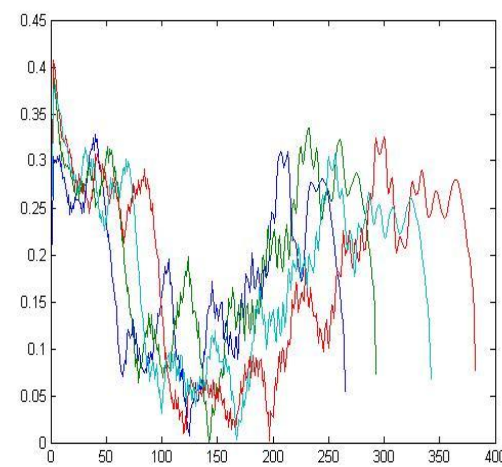
	DFrCT of Features of signature of user 2	
	Genuine signature	**Forgery signature**
DFrCT of Horizontal component	 **(a)**	 **(b)**

Figure 5.9: DFrCT of features of signatures of user 2 with ‘α’=.92 (contd.)

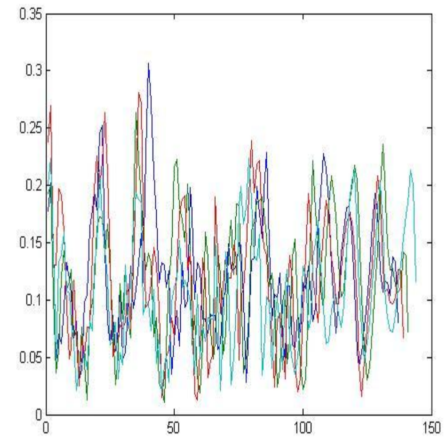
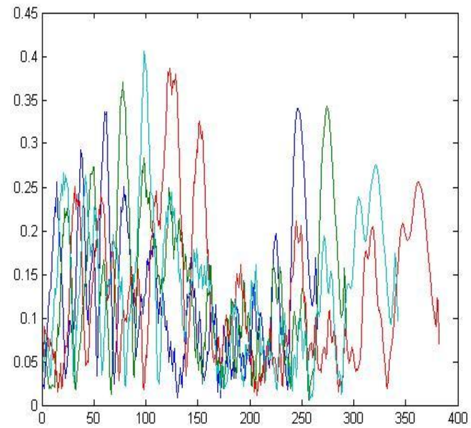
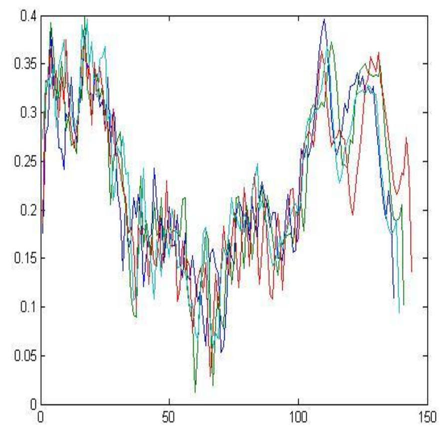
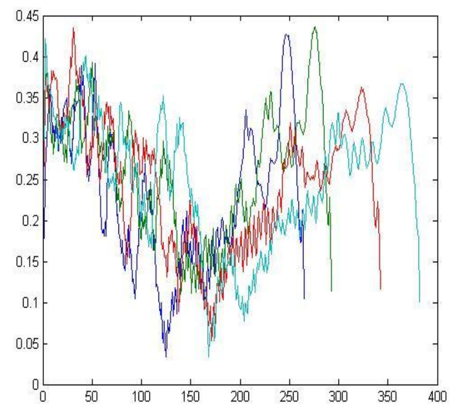
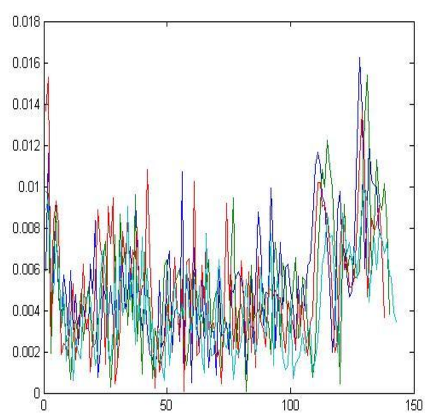
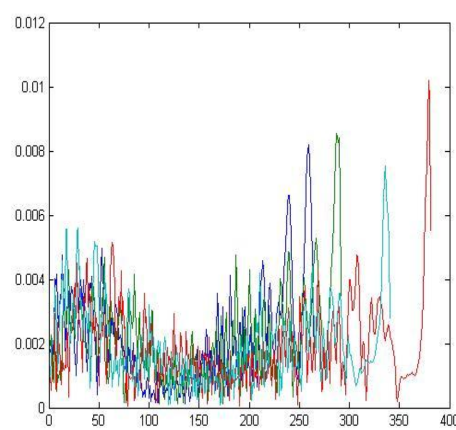
DFrCT of Vertical component	 **(c)**	 **(d)**
DFrCT of Displacement	 **(e)**	 **(f)**
DFrCT of Areal Velocity	 **(g)**	 **(h)**

Figure 5.9: DFrCT of features of signatures of user 2 with 'α'=.92 (contd.)

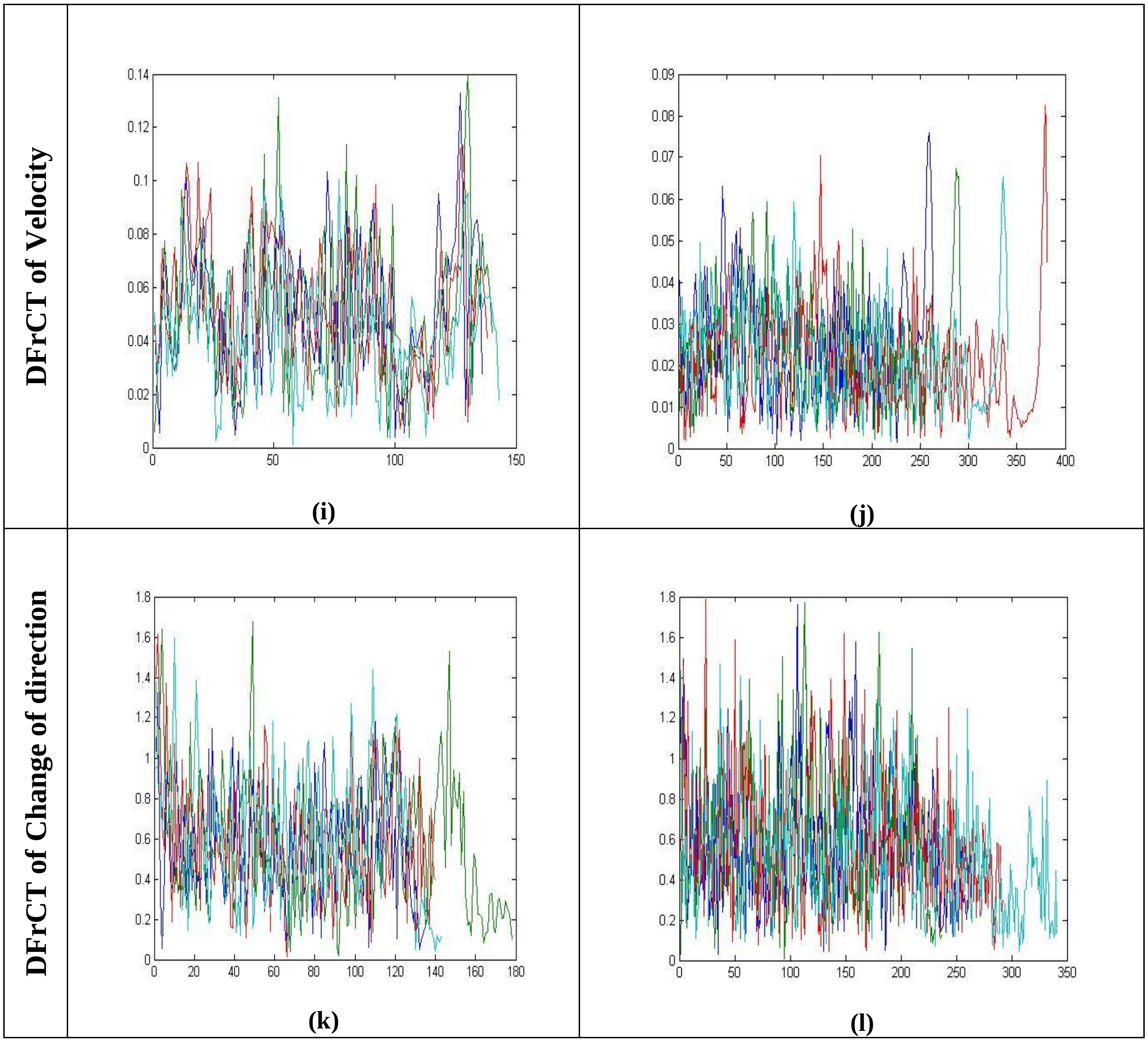


Figure 5.9: DFrCT of features of signatures of user 2 with 'α'=.92

5.8 Experimental Results of Verification system

The performance of signature verification systems is typically described on terms; the false accept rate (FAR) and a corresponding false reject rate (FRR). A false acceptance occurs when the system allows a forger's sign is accepted. A false reject ratio represents a valid user is rejected from gaining access to the system. These two errors are directly correlated, where a change in one of the rates will inversely affect the other. A common alternative to describe the performance of system is to calculate the equal error rate (EER). EER corresponds to the point where the false accept and false reject rates are equal. In order to visually comment the performance of a signature verification system, receiver operating characteristic (ROC) curves are drawn.

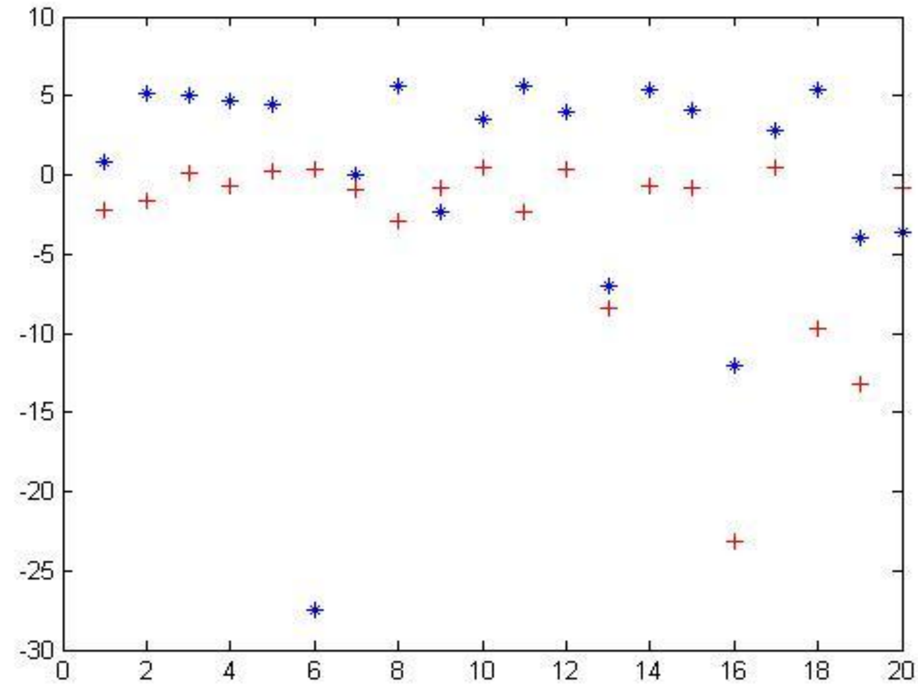
The SVC2004 database was used in the experiment. Corresponding to each user there are 20 genuine signatures and 20 forgery signatures. In the experiment, 5 users were selected from the database. Thus, there were 200 signatures in total for this experiment.

Signature verification system generates Euclidean norm corresponding to each test signature. Difference between the reference Euclidean norm and that of test signature is used for verification. This difference is compared with the threshold to make a decision of rejecting or accepting the user. The threshold value can be changed in order to obtain various FAR and FRR combinations.

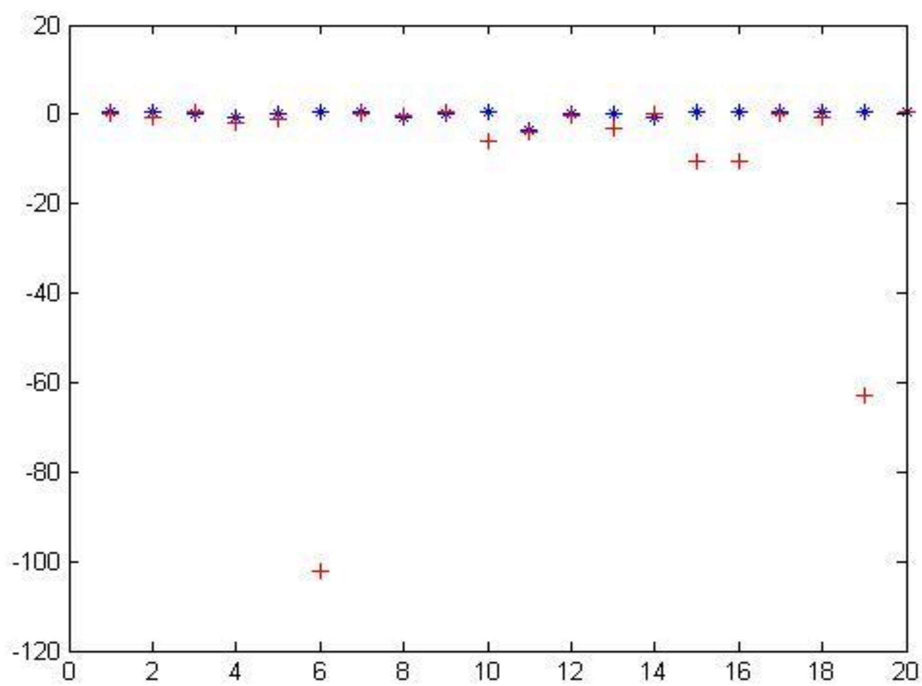
The signature verification system is trained by 5 genuine signatures corresponding to each user. Euclidean norm of each signature is calculated and mean of their Euclidean norms is treated as reference norm. In this study a performance comparison has been made in between results obtained by the method using DFrCT for feature extraction to that of one using DCT for feature extractions for signature verification. The evaluation criteria opted here is Equal Error Rate (EER).

While using DFrCT, the optimum value of α can be achieved by varying its value in between 0 to 1 and repeating the algorithm until a minimum EER corresponding to the user is achieved. Although this is more time consuming as compare to DCT but due to this flexibility we get different forms of the signal which interpolate between the cosine modulated form of the signal and its DCT representation resulting in better system performance.

Figure 5.10 show some examples of the plots of Euclidean norm of genuine signatures and forge signatures using DCT for feature extraction. Figure 5.11 show some examples of the plots of Euclidean norm of genuine signature and forge signatures using DFrCT for its optimum values of α. Red points in the plot refer to the forge signatures and blue points correspond to the genuine signatures. More is the separation between the points lesser will be the error rate.

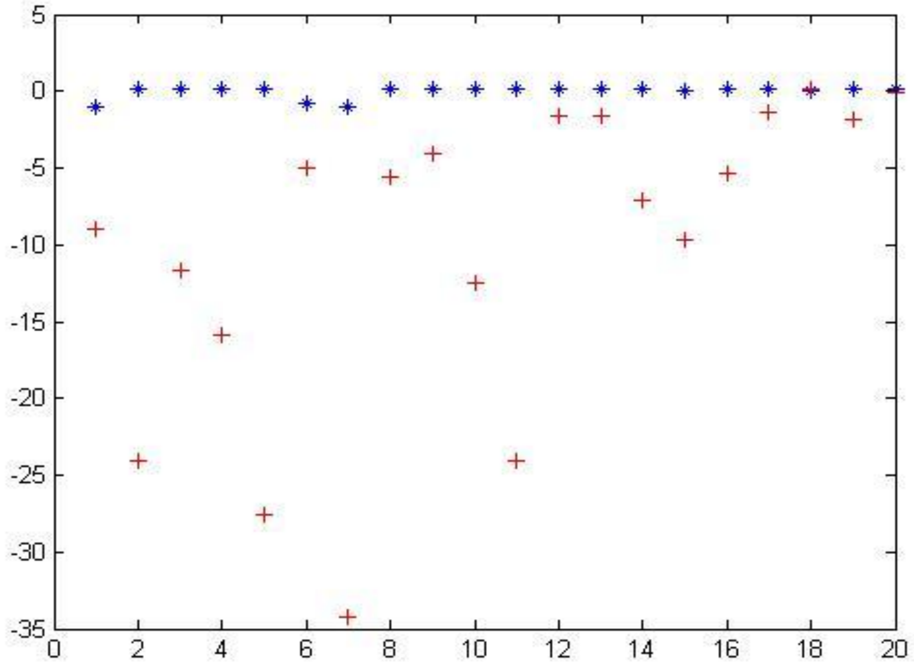


(a)

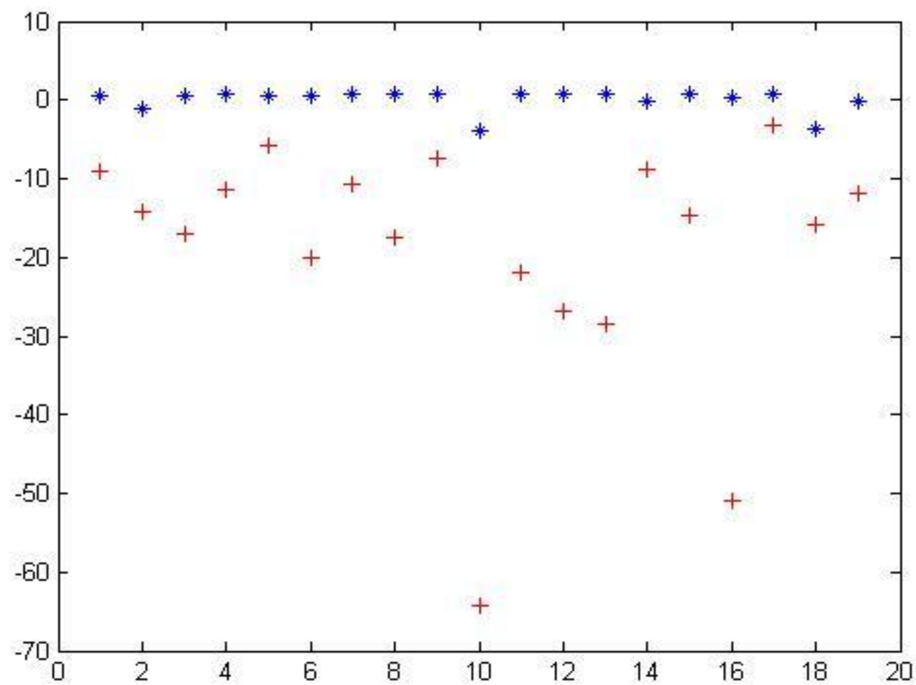


(b)

Figure 5.10: The plot of Euclidean distances obtained for Genuine signatures and Forgeries Using DCT



(a) α=0.445



(b) α=0.195

Figure 5.11: The plot of Euclidean Distances Obtained for Genuine Signatures and Forgeries Using DFrCT

5.8.1 Analysis of System Using DCT Method

Table 5.1 shows the difference between the Euclidean norm of test signature and the Euclidean norm of the reference signature. Table 5.2 shows number of false accepted and false rejected signatures corresponding to various threshold levels. Table 5.3 shows the FAR and FRR corresponding to various threshold levels. Figure 5.12 shows a plot of FAR versus FRR.

Table 5.1: Difference of Euclidean Norm of Reference and Test Signature Using DCT

Sign	User 1		User 2		User 3		User 4		User 5	
	Forge	Genuine	Forge	Genuine	Forge	Genuine	Forge	Genuine	Forge	Genuine
1	0.6047	0.019	-2.2117	0.8238	0.9718	2.8576	0.0274	0.4373	-0.4002	0.5248
2	0.6053	-1.016	-1.6526	5.0974	-3.5617	2.7861	-0.4797	0.4231	-6.8166	0.5077
3	0.5843	0.5415	0.066	5.0441	2.905	2.5756	0.3814	0.3004	-3.1902	0.3605
4	-0.9555	0.6173	-0.672	4.6703	2.5065	2.9502	-1.8012	-0.7587	0.4253	-0.9104
5	-0.1471	0.4871	0.2756	4.4976	2.2535	2.9487	-1.1262	0.1195	-2.3699	0.1434
6	0.3031	0.5452	0.3926	-27.4459	0.6871	1.9684	-102.177	0.4261	-0.1952	0.5113
7	0.5276	0.6128	-0.8809	0.0403	1.6983	2.7848	0.3479	0.4163	-3.0046	0.4996
8	-1.7708	0.617	-2.9482	5.5688	-7.1916	1.8212	-0.3947	-0.7899	0.2125	-0.9479
9	0.3145	0.6006	-0.8287	-2.3356	2.0235	2.951	0.4231	0.3022	-13.2149	0.3626
10	0.6215	0.6176	0.4785	3.4612	-1.0346	0.7073	-5.7972	0.4454	-0.2656	0.5344
11	-2.6113	0.6125	-2.3493	5.6123	-20.351	0.3821	-3.7626	-3.5686	- 3.057	-4.2823
12	-0.5446	0.6157	0.3623	4.0133	2.4784	2.8059	-0.3621	0.3324	0.3622	0.3989
13	-2.7983	0.582	-8.4009	-7.0403	2.7909	1.9258	-3.1458	0.1121	-1.977	0.1345
14	-0.2433	0.5668	-0.7506	5.3482	1.9852	2.8233	0.0453	-0.8074	0.3701	-0.9689
15	-0.4261	0.0571	-0.8319	4.0995	1.2786	2.8994	-10.4594	0.3965	-3.043	0.4758
16	0.2706	0.5735	-23.1969	-12.1047	2.5641	2.5393	-10.5868	0.462	-1.0599	0.5545
17	-0.1449	-4.8909	0.4876	2.8142	2.9396	1.9671	0.2173	0.456	-0.3864	0.5472
18	-2.0542	-0.0433	-9.7607	5.3378	-0.5137	2.8715	-0.605	0.4634	-0.9467	0.5561
19	-2.5989	-0.0975	-13.1987	-3.9201	2.9467	0.6706	-62.7096	0.4309	-2.0509	0.517
20	-0.2959	-1.6181	-0.7999	-3.5821	2.6233	-0.0775	0.4063	0.4009	-7.7041	0.4811

Table 5.2: Number of False Accepted (FA) and False Rejected (FR) Signatures corresponding to Each User for Various Threshold (THD) Levels Using DCT

User 1			User 2			User 3			User 4			User 5			Total	
THD	**FA**	**FR**	**THD**	**FA**	**FR**	**THD**	**FA**	**FR**	**THD**	**FA**	**FR**	**THD**	**FA**	**FR**	**FA**	**FR**
.5415	4	8	0.8238	0	7	2.7848	4	7	0.3965	2	9	0.3989	1	8	11	39
.4871	5	7	0.0403	6	6	2.5756	5	9	0.3004	4	6	0.3626	2	7	22	28
-.0975	8	3	-0.6720	7	6	2.5393	6	8	0.1121	5	4	0.3605	3	6	26	27
-1.6181	15	1	-7.0403	16	2	1.9258	11	5	-0.8074	11	1	-0.9689	9	1	55	10

Table 5.3: False Accept Rate and False Reject Rate using DCT

Threshold level	False Accept Rate (FAR)%	False Reject Rate (FRR)%
1	5.5	19.5
2	11	14
3	13	13.5
4	27.5	5

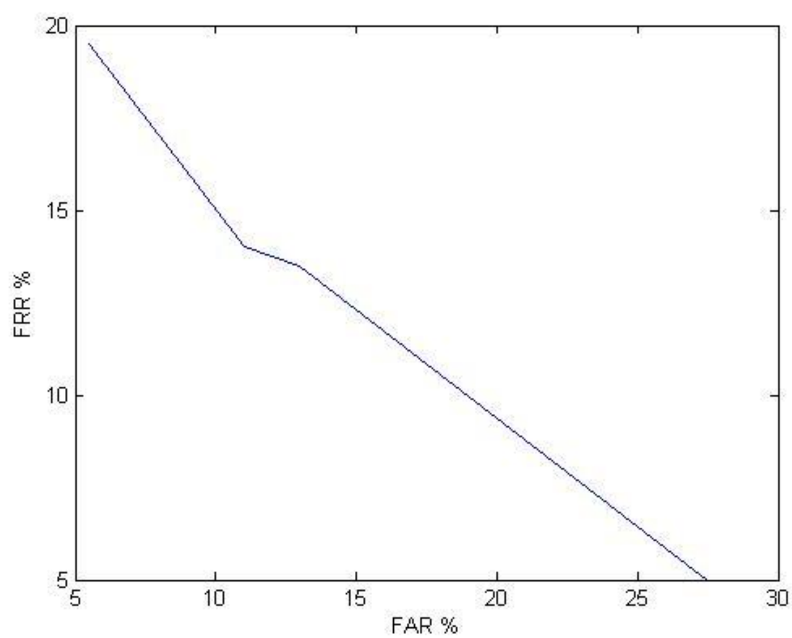


Figure 5.12: FAR versus FRR Using DCT

5.8.2 Analysis of System Using DFrCT Method

Table 5.4 shows the difference between the Euclidean norm of test signature and the Euclidean norm of the reference signature corresponding to optimal values of α, which is achieved by varying this factor in between 0 and 1 and repeating the algorithm until a minimum EER is achieved. Table 5.5 shows number of false accepted and false rejected signatures corresponding to various threshold levels. Table 5.6 shows the FAR and FRR corresponding to various threshold levels. Figure 5.13 shows a plot of FAR versus FRR.

Table 5.4: Difference of Euclidean Norm of Reference and Test Signature Using DFrCT

Sign	User 1 (optimum α=0.76)		User 2 (optimum α=0.61)		User 3 (optimum α=0.445)		User 4 (optimum α=0.195)		User 5 (optimum α=0.6)	
	Forge	Genuine	Forge	Genuine	Forge	Genuine	Forge	Genuine	Forge	Genuine
1	0.3405	-6.4839	0.0453	0.1053	-8.925	-1.0419	-9.1799	0.4531	0.1905	0.1955
2	-0.5854	0.4116	-2.3341	0.1148	-24.0868	0.197	-14.308	-1.1339	0.1905	0.1929
3	-2.3235	0.4236	-0.0658	-1.1786	-11.6916	0.1702	-16.961	0.6221	-1.947	0.1705
4	-1.8158	0.3418	-0.064	0.0913	-15.8328	0.1963	-11.5024	0.7202	-6.302	0.1022
5	-5.1189	0.3412	0.1049	0.0997	-27.6109	0.1888	-5.7588	0.5518	-2.4324	0.0413
6	-4.8678	-0.7057	-0.066	0.1143	-4.9626	-0.8192	-20.0481	0.616	-5.1425	-0.2466
7	-1.7452	0.4373	0.0246	0.1126	-34.1937	-1.0246	-10.6765	0.7395	-21.4591	0.0445
8	-0.42	0.4545	0.0841	0.0656	-5.588	0.1972	-17.5722	0.7443	-7.9945	0.1745
9	-1.4163	0.3829	0.0985	0.0673	-4.0789	0.1974	-7.3223	0.7334	-2.1727	0.0845
10	0.3948	0.3948	0.0535	0.0926	-12.5172	0.1954	-64.1874	-3.8534	-15.5746	0.1018
11	-3.9684	0.2752	0.0289	0.0991	-24.0454	0.1955	-22.0044	0.7178	-17.2141	0.1917
12	-2.0277	0.4366	-0.1395	0.1079	-1.6014	0.1973	-26.8906	0.6659	-9.5119	0.1228
13	-3.222	0.4541	0.0645	0.1057	-1.5869	0.1963	-28.5301	0.6834	-5.5129	-1.8134
14	-1.6865	0.4523	-0.0822	-0.6175	-7.0599	0.1957	-8.8903	-0.1182	-2.4035	0.1567
15	-5.4898	0.3552	0.0549	0.107	-9.6345	0.0857	-14.7167	0.6465	-14.505	0.1942
16	-0.4331	0.4505	0.0527	0.1071	-5.3474	0.1945	-50.8478	0.3727	-1.4667	0.1557
17	-0.736	0.4539	0.0621	0.0908	-1.3396	0.1974	-3.3252	0.7539	-1.2801	-0.2477
18	-1.4079	0.3999	-0.2132	0.0975	0.1154	0.0843	-15.9247	-3.6592	-5.8708	0.1887
19	-1.1168	0.3536	0.0689	0.1092	-1.8787	0.1966	-11.8127	-0.256	-3.1843	0.1903
20	-5.2555	0.3706	0.0825	0.1085	-0.1044	0.1936	-7.836	0.5786	0.0252	0.1438

Table 5.5: Number of False Accepted and Rejected Signatures Corresponding to Each User for Various Threshold Levels Using DFrCT

User 1 (optimum α=.76)			User 2 (optimum α=.61)			User 3 (optimum α=.445)			User 4 (optimum α=0.195)			User 5 (optimum α=.6)			Total	
THD	FA	FR	THD	FA	FR	THD	FA	FR	THD	FA	FR	THD	FA	FR	FA	FR
0.3418	1	4	0.0926	1	8	0.0843	1	3	-1.1339	0	3	0.0445	2	4	5	18
0.3412	1	3	0.0913	2	5	-0.8192	2	2	-0.2560	0	2	0.0413	2	3	7	12
0.2752	2	2	0.0908	2	4	-1.0246	2	1	-3.6592	1	1	0.2477	3	1	10	9
-0.7057	5	1	0.0656	5	2	-1.0419	2	0	-3.8534	1	0	-1.8134	5	0	13	3

Table 5.6: False Accept Rate and False Reject Rate using DFrCT

Threshold level	False Accept Rate (FAR)%	False Reject Rate (FRR)%
1	2.5	9
2	3.5	6
3	5	4.5
4	6.5	1.5

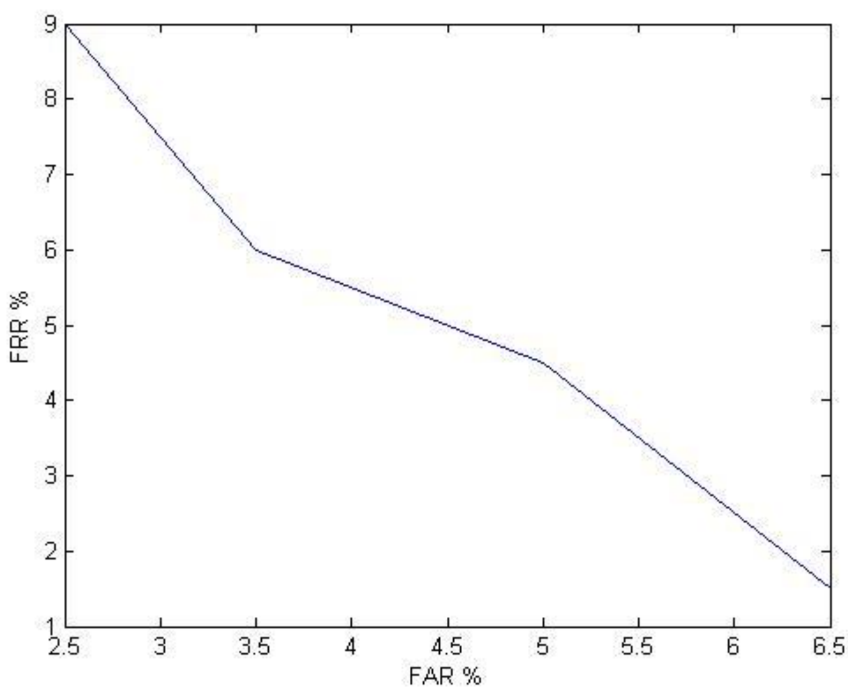


Figure 5.13: FAR versus FRR Using DFrCT

A graphical comparison of performance of DFrCT based system and DCT based system is shown in Figure 5.14, it can be easily seen that both FAR and FRR in case of proposed method is far less as compare to the one based on DCT. A minimum FAR of 2.5 % is attained as compare to 5.5% and maximum FAR is limited to 6.5% as compare to 27.5% with the proposed methodology.

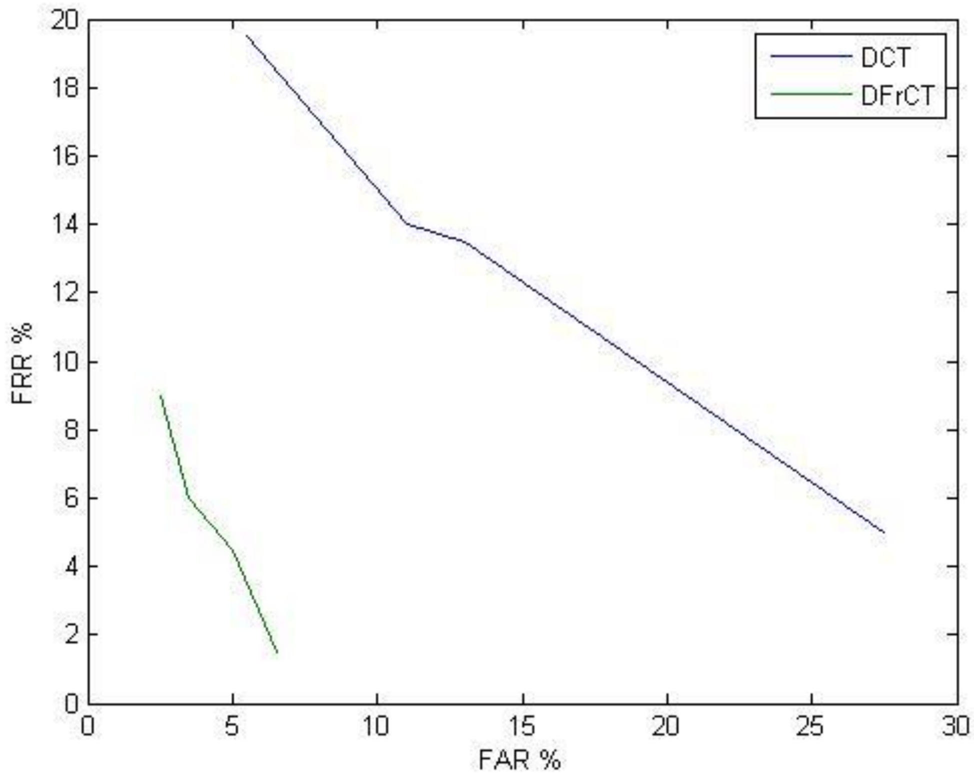


Figure 5.14: Comparison of DFrCT based System with DCT based System

Also from the above results and analysis it is observed that an EER of 5% was achieved with the use of DFrCT as compare to EER of 13.5% when DCT was used for feature extraction. Hence we can say that DFrCT with is free parameter α provides a better option for features extraction for signature verification system as compare to the one extracted by using DCT.

Chapter 6
Conclusion and Future Scope

6.1 Conclusion

Signatures can be categorized as offline signature where only the image of signature is given and online signature where certain dynamic parameters which cannot be seen by eyes such as velocity of signature, acceleration, movement with respect to time, altitude, pressure, azimuth etc. are also recorded.

Now a day's with developing progress in identification applications has increase the demand for new generation ID documents, which contain additional biometric information required for more accurate user recognition. The image of the user's handwritten signature is already incorporated into ID documents. Hence the trend is shifting towards online handwritten signatures incorporating along with other information. Challenging part is to standardize the method of features extraction worldwide in order to be in synchronism. Various methods have been purposed for features extraction and being at developing stage many more methodologies are expected to be purposed. One such effort has been put up in this study to extract features for a given signature. Use of DFrCT which according to literature was yet to be explored has been discussed in this study.

DFrCT is a powerful tool of signal processing with a free parameter, its fraction. With optimization of this parameter for feature extraction has given far better results when compare with one of the existing methodology in literature based on DCT. An EER of only 5% was achieved as compare to the EER of 13.5% when DCT was used. Difference in result clearly proves the superiority of DFrCT over DCT.

6.2 Future Scope

In this study single value of α was optimized for all the features, in future to improve the performance of the system different values of α can be optimized for different parameters to further increase the efficiency of the system.

References

[1] A. K. Jain, “Biometrics, Personal Identification In Networked Society: Personal Identification in Networked Society,” *Kluwer Academic Publishers Norwell*, MA, USA, 1998.

[2] K. W. Boyer, V. Govindaraju, and N. K. Ratha, Eds, “Special Issue on Recent Advances in Biometric Systems,” *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 37, No. 5, pp. 1091–1095, 2007.

[3] E. J. R.Justino, F. Bortolozzi and R.Sabourin. “Offline Signature Verification Using Hmm for Random, Simple and Skilled Forgeries,” *Document Analysis and Recognition. Proceedings. Sixth International Conference.* 2000, pp.1031-1034.

[4] D. Impedovo and G. Pirlo “Automatic Signature Verification System: The State of the Art,” *IEEE Trans. Syst. Man, and Cybern.*, vol. 38, No. 5, pp. 609 – 635, 2008.

[5] K. Huang and H. Yan. “Offline Signature Verification Using Structural Feature Correspondence,” *Pattern Recognition*, vol. 35, No. 11, pp. 2467–2477, 2002.

[6] I. S. I. Abuhaiba. “Offline Signature Verification Using Graph Matching,” *Turk. J. Elec. Eng. & Comp. Sci.*, vol. 15, No. 1, pp. 89-104, 2007.

[7] L. Nanni, E. Maiorana, A. Lumin and P.Campisi. “Combining Local, Regional and Global Matchers for a Template Protected Online Signature Verification System,” *Expert Systems with Applications.*, vol. 37, No. 5, pp. 3676-3684, 2010.

[8] A. K. jain, F. D.Griess and S. D. Connell. “Online Signature Verification,” *Pattern recognition*, vol. 35, No. 12, pp. 2963-2972, 2002.

[9] R. Plamondon and G. Lorette, “Automatic Signature Verification and Writer Identification– The State of the Art,” *Pattern Recognition*, vol. 22, No. 2, pp. 107–131, 1989.

[10] V. Namias, “The Fractional Order Fourier Transform and its Application to Quantum Mechanics,” *Journal of Institute of Mathematics and its Applications*, vol. 25, No. 3, pp. 241-265, 1980.

[11] V. Namias, “Fractionalization of Hankel Transforms,” *IMA Journal of the Institute of Math Applications*, vol. 26, No. 2, pp. 187-197, 1980

[12] A. C. McBride and F. H. Keer, “On Namia's Fractional Fourier Transform,” *IMA Journal of Applied Mathematics*, vol. 39 No. 2, pp. 159-175, 1987

[13] D. Mendlovic and H. M. Ozaktas, " Fractional Fourier Transforms and their Optical Implementation-I," *Journal of Optical Society of America-A*, vol. 10, No. 9, pp. 1875-1881, 1993.

[14] S. C. Pei and M. H. Yeh, "A Method for the Discrete Fractional Fourier Transform Computation," *IEEE International Symposium on Circuits and Systems*, vol. 2, pp. 536-539, 1996.

[15] B. Fang, C. H. Leungb, Y. Y. Tangc, K. W. Tseb, P. C. K.wokd and Y.K.Wonge. "Offline Signature Verification by the Tracking of Feature and Stroke Positions," *Pattern Recognition*, vol. 36, No.1, pp. 91-101, 2003.

[16] E. Orzgunduz, T. Senturk and M. E. Karsligil. "Offline Signature Verification and Recognition By Support Vector Machine," *proc. EUSPICO*, 2005.

[17] Y. Mizukami, M. Yoshimura, H. Miike and I. Yoshimura. "An Offline Signature Verification System Using An Extracted Displacement Function," *Pattern Recognition*, vol. 23, No. 13, pp. 1569-1577, 2001.

[18] I. Guler and M. Meghdadib. "A Different Approach to Offline Handwritten Signature Verification Using the Optimal Dynamic Time Warping Algorithm," *Digital Signal Processing*, vol. 18, No. 6, pp. 940-950, 2008.

[19] A. W. Lohmann, D. Mendlovic, Z. Zalevsky and R.G. Dorsch, "Some important fractional transformations for signal processing," *Optical Communication*, vol. 125, No. 3 pp. 18-20, 1996

[20] B. Schafer and S. Viriri. "An Offline Signature Verification System," *IEEE International Conference on Signal and Image Processing Applications*, pp. 95-100, 2009.

[21] T. Matsuura and S. Okamura. "On FIR Filter for Signature Verification," *Circuits and Systems, Proceedings of the 38th Midwest Symposium*, vol.1, pp. 366-369, 1996.

[22] C. Schmidt and K. E. Kraiss. "Establishment of Personalized Templates for Automatic Signature Verification," *Document Analysis and Recognition, Proceedings of the Fourth International Conference*, vol. 1, pp. 263-267, 1997.

[23] Q .Z. Wu, S. Lee and I. Jou."Online Signature Verification Based on Logarithmic Spectrum," *pattern recognition*, vol. 31, No. 12, pp. 1865-1871, 1998.

[24] A. zimmer, L. L. ling. "A Hybrid On/Offline Handwritten Signature Verification

System," *Document Analysis and Recognition, Proceedings. Seventh International Conference*, pp.424-428, 2003.

[25] H. Feng and C. C. Wah. "Online Signature Verification Using A New Extreme Points Warping Technique," *Pattern Recognition*, vol. 24, No. 16, pp. 2943-2951, 2003.

[26] T. Matsumoto and D. Muramatsu. "Effectiveness of Pen Pressure, Azimuth, and Altitude Features for Online Signature Verification," *Advances in biometrics International conference, proceedings. Springer-Verlag Berlin Heidelberg*, LNCS 4642, pp. 503–512, 2003.

[27] L. Liu, H. Duan. "The Research of Handwritten Signatures," *IT in Medicine & Education. IEEE International Symposium*, pp. 1066-1069, 2009.

[28] D. Muramatsu, K. Yasuda and T. Matsumoto. "Biometric Person Authentication Method Using Camera-Based Online Signature Acquisition," *Document Analysis and Recognition, ICDAR. 10th International Conference*, pp. 46-50, 2009.

[29] P. Thumwarin, J. Pemwong, N. Wakayaphattaramanus, and T. Matsuura. "Online Signature Verification Based on FIR System Characterizing Velocity and Direction Change of Barycenter Trajectory," *Progress in Informatics and Computing, IEEE International Conference*, pp. 30-34, 2010.

[30] S. Emerich, E. Lupu and Corneliu Rusu. "Online Signature Recognition Approach Based on Wavelets and Support Vector Machines," *Automation Quality and Testing Robotics (AQTR), IEEE International Conference.* vol. 3, pp. 1-4, 2010.

[31] S.Emerich, E.Lupu, Corneliu Rusu. "Online Signature Recognition Approach Based on Wavelets and Support Vector Machines," *Automation Quality and Testing Robotics (AQTR), IEEE International Conference*, pp. 1-4, 2010.

[32] M. T. Ibrahim, M. A. Khan, K. S. Alimgeer, M. K .Khan, I. A. Taj and L. Guan. "Velocity and Pressure-Based Partitions of Horizontal And Vertical Trajectories For Online Signature Verification," *Pattern Recognition*, vol. 43, No. 8, pp. 2817-2832, 2010.

[33] C. T.Yuen, W. L.Lim, C. Tan, B. Goi, X. Wang and J .Ho. "Probabilistic Model for Dynamic Signature Verification System," *Applied Sciences, Engineering and Technology*, pp. 1320-1324, 2011.

[34] L. B. Almeida, "The Fractional Fourier Transform and Time-Frequency

Representation," *IEEE Transaction on Signal Processing,* vol. 42, No. 11, pp. 3084-3091, 1994.

[35] C. Candan, M. A. Kutay and H.M. Ozaktas, " Discrete Fractional Fourier Transform," *IEEE Transactions on Signal Processing,* vol. 48, No. 5, pp. 1329-1337, 2000.

[36] S. C. Pei and J. J. Ding, "Closed-Form Discrete Fractional and Affine Fourier Transforms," *IEEE Transactions On Signal Processing,* vol. 48, No. 5, pp. 1338-1353, 2000

[37] H.M.Ozaktas, O.Arikan, M.A.Kutay, and G.Bozdagi. "Digital Computaion Of Fractional Fourier Transform," *IEEE Transactions On Signal Processing,* vol 44, No. 9, pp.2141-2150, 1996

[38] B. Miller, "Vital Signs of Identity," *IEEE Spectr.,* vol. 31, No. 2, pp. 22–30, Feb. 1994.

[39] C. Gruber, and C. Hook, "A Flexible Architecture for Online Signature Verification Based on a Novel Biometric Pen," *IEEE Mountain Workshop on Adaptive and Learning Systems,* pp. 110-115, 2006.

[40] D. J. Hamilton, J. Whelan, A. McLaren, I. Macintyre, and A. Tizzard, "Low Cost Dynamic Signature Verification System," *Proc. Eur. Convention Secur. Detection,* pp. 202–206, 1995.

[41] G. Dimauro, S. Impedovo, and G. Pirlo, "Online Signature Verification by A Dynamic Segmentation Technique," *in Proc. 3rd Int.Workshop Front. Handwriting Recognit. (IWFHR-3), Buffalo, NY,* pp. 262–271, 1993,

[42] Y. Xuhua, T. Furuhashi, K. Obata, and Y. Uchikawa, "A Study on Signature Verification Using a New Approach to Generic Based Machine Learning," *IEEE Int. Conf. Syst., Man, Cybern., Intell. Syst. 21st Century,* vol. 5, pp. 4383–4386, 1995.

[43] J. J. Brault and R. Plamondon, "Segmenting Handwritten Signatures at their Perceptually Important Points," *IEEE Trans. Pattern Anal. Mach. Intell.,* vol. 15, No. 9, pp. 953–957, 1993

[44] R. Plamondon and G. Lorette, "Automatic Signature Verification and Writer Identification-The State Of The Art," *Pattern Recognition,* vol. 22, No. 2, pp. 107–131, 1989.

[45] T. H. Rhee, S. J. Cho, and J. H. Kim, "Online Signature Verification Using Model-

Guided Segmentation And Discriminative Feature Selection For Skilled Forgeries," in *Proc. 6th Int. Conf.Doc. Anal. Recognition. (ICDAR-6)*, Seattle, WA, pp. 645–649, 2001.

[46] C. Vielhauer, "A Behavioural Biometrics," *Public Service Rev.: Eur.Union*, vol. 20, No. 9, pp. 113–115, 2005.

[47] R. Martens and L. Claesen, "Online Signature Verification By Dynamic Time-Warping," in *Proc. 13th Int. Conf. Pattern Recog. (ICPR96)*, pp. 38–42, 1996.

[48] M. K. Kalera, S. Srihari, and A. Xu, "Offline Signature Verification and Identification Using Distance Statistics," *Int. J. Pattern Recognit. Artif. Intell. (IJPRAI)*, vol. 18, No. 6, pp. 1339–1360, 2004.

[49] C. Quek and R. W. Zhou, "Anti-Forgery: A Novel Pseudo-Outer Product Based Fuzzy Neural Network Driven Signature Verification System," *Pattern Recognition*, vol. 23, No. 14, pp. 1795–1816, 2002.

[50] L. R. Rabiner and B. H. Juang, "An Introduction To Hidden Markov Models," *IEEE ASSP Mag.*, vol. 3, No. 1, pp. 4–16, 1986.

[51] C. J. C. Burges, "A Tutorial On Support Vector Machines For Pattern Recognition," *Data Mining Knowl. Discov.*, vol. 2, pp. 121–167, 1998.

[52] Y. Chen and X. Ding, "Online Signature Verification Using Direction Sequence String Matching," *Proc. SPIE*, pp. 744–749, 2002.

[53] L. Bovino, S. Impedovo, G. Pirlo, and L. Sarcinella, "Multi-Expert Verification of Hand-Written Signatures," in *Proc. 7th Int. Conf. Doc. Anal. Recognit. (ICDAR-7), IEEE Comput. Soc.*, Edinburgh, U.K., pp. 932–936, 2003.

[54] T. Alieva, M. J. Bastiaans, "Fractional Cosine and Sine Transforms In Relation To The Fourier and Hartley Transforms*", Signal Processing and Its Applications*, pp. 561-564, 2003.

[55] S. S. Pie, M. H. Yeh. "The Discrete Fractional Cosine And Sine Transform", *IEEE Transactions on Signal Processing*, vol. 49, No. 6, pp. 1198-1207, 2001.

[56] D. Y. Yeung, *et al.*, "SVC2004: First International Signature Verification Competition" in Proceedings Biometric Authentication, pp. 16-22, 2004.

[57] Y. Yang, L .Qi. "Study on the Algorithm of the Fractional Cosine Transform Based on Adaptive LMS Algorithm." *9th International Conference on Signal Processing*, pp.

100-103, 2008.

[58] O. M. Hurtado, “Online Signature Verification Algorithms and Development of Signature International Standards” Ph.D. dissertation, Univ. of Carlos III, 2001

[59] A. W.Lohmann, D. Mendlovic, Z. Zalevsky, and R.G. Dorsch,“Some Important Fractional Transforms for Signal Processing,” *Optics Communications*, vol.125, pp.18-20, 1996.

LIST OF PUBLICATIONS

[1] M. Arora, K.Singh, "Discrete Fractional Cosine based Online Handwritten Signature Verification System," Communicated to International Journal of Computer Application.