Improved online signature verification system using Discrete Fractional Cosine Transform

A dissertation Submitted in the partial fulfillment of requirement

for the award of degree of

Master of Engineering

In

Wireless Communication

Submitted by

Sahil Mantrao

Roll No: 801263024

Under the guidance of

Dr. Kulbir Singh

Associate Professor

ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

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

PATIALA – 147004 (PUNJAB)

DECLARATION

I, hereby declare that the work which is being presented in the dissertation entitled, **"Improved Online Signature Verification System using Discrete Fractional Cosine Transform "** in partial fulfillment of the requirement for the award of degree of Master of Engineering in Wireless Communication submitted in Electronics and Communication Engineering Department of 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 work 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 degree.

Date: 17/7/2014

Sahil Mantrao

(SAHIL MANTRAO)

Roll No: 801263024

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

(Dr. KULBIR SINGH)

Associate Professor

ECED, Thapar University

Countersigned by:

Head

ECED, Thapar University

Patiala-147004

Dean of Academic Affairs

Thapar University

Patiala- 147004

ACKNOWLEDGEMENT

First of all, I would like to express my gratitude to **Dr. Kulbir Singh**, **Associate Professor**, Electronics & Communication Engineering Department, Thapar University, Patiala for his guidance and support throughout this thesis work. I am really very fortunate to have the opportunity to work with him. I found his guidance to be extremely valuable.

I am thankful to the **Head of Department, Professor (Dr.) Sanjay Sharma** of Electronics & Communication Engineering Department for their encouragement and inspiration for the execution of this thesis work.

I am also thankful to the entire faculty and staff of Electronics & Communication Engineering Department for the help and moral support which went along the way for the successful completion of this thesis work.

My greatest thanks are to all who wished me success especially my parents. Above all I render my gratitude to the Almighty who bestowed self-confidence, ability and strength in me to complete this work for not letting me down at the time of crisis and showing me the silver lining in the dark clouds. I do not find enough words with which I can express my feelings of thanks to my friends for their help, inspiration and moral support which went a long way in successful competition of the present study.

Sahil Mantrao

801263024

ABSTRACT

The rapid development and increasing use of computer terminals, automatic tellers, and data banks has engendered the need to protect sensitive information. The Biometric technology uses behavioral characteristics of people such as fingerprints, face, iris, hand geometry, retina, voice etc. in an automated way to provide security while accessing computers and automated banking and personal identification. But the most popular modality is handwritten signature used in banking and commerce, transaction, credit card payments, cheque authentication for longer time.

There are two ways for handwritten signature verification i.e. offline and online signature verification. In offline signature verification, signatures are scanned after it has been written. A more useful and attractive approach is to generate electric signals representative of the signature during the signing process known as online signature verification. The advantage of this approach is that signature verification is based on the dynamics of the signature, which are not visible and, therefore, are very difficult to forge or copy.

In the present work, an online signature verification system based on FIR system is designed using discrete fractional cosine transform (DFrCT). The DFrCT has extra degree of freedom to extract the feature of test signatures. The test signatures are preprocessed and then eight features horizontal movement, vertical movement, areal velocity, displacement, velocity, direction change, area pressure, motion pressure are extracted using DFrCT. The impulse responses of four FIR systems are used to calculate Euclidean norm. The signature can be verified by evaluating the difference between the average of Euclidean norms of genuine and forgery signatures. The equal error rate (EER), false acceptance rate (FAR), false rejection ratio (FRR) is calculated to compare the efficiency of the present work with the previous work. In the present work, the minimum EER of 3.5%, minimum FAR of 1.5% and minimum FRR of 2% is achieved to verify above statement. However, the use of four FIR systems and extraction of eight features has increased the complexity. The accuracy and security can be increased by extracting more than eight feature in future.

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 Perceptron’s
FAR	False Acceptance Rate
FRR	False Rejection Rate
EER	Equal Error Rate

List of Figures

List of Tables

List of Symbols

t_n	Duration of pen movement
$x(t_n)$	Horizontal component
$y(t_n)$	Vertical Component
C_q	Center point of the signature
E_q	Trajectory of Barycenter
$E_x(t_n)$	Horizontal movement of signature
$E_y(t_n)$	Vertical movement of signature
$a_v(t_n)$	Areal velocity of signature
$d(t_n)$	Displacement of signature
$v(t_n)$	Velocity of signature
$\theta(t_n)$	Change in angle of signature
$ap(t_n)$	Area pressure of signature
$dp(t_n)$	Motion pressure of signature
$H_x(m)$	Horizontal movement using DFrCT
$H_y(m)$	Vertical movement using DFrCT
$Ha_v(m)$	Areal velocity using DFrCT
$H_d(m)$	Displacement using DFrCT
$H_v(m)$	Velocity using DFrCT
$H_\theta(m)$	Change in angle using DFrCT
$H_{ap}(m)$	Area pressure using DFrCT
$H_{dp}(m)$	Motion pressure using DFrCT
α	Rotation angle
h_1, h_2, h_3, h_4	Impulse response of FIR system
h^{ref}	Euclidean norm of reference signature
h	Euclidean norm of test signature
η	Threshold

1. INTRODUCTION

1.1 PREAMBLE

Signature is a unique hand writing feature used by a person for his identification through ages. An increasing number of communications, especially financial, are being authorized via signatures. Research into signature verification has been vigorously pursued as it is an important biometric for authenticating the identity of person. Biometric identification is the measure of human physical characteristics to identify or verify certain user [1]. This process of verification is favored over other traditional methods like passwords protection and PIN numbers for its accuracy and case sensitiveness. A biometric process is basically a pattern recognition system which makes a personal identification on the basis of its specific physiological or behavioral characteristic possessed by the user. The characteristics of a particular user can never be duplicable. Thus, biometric attribute can never be lost or stolen and can never be forgotten. Biometric technologies are divided into two types:

(i)Anatomical Biometrics**:** Anatomical biometric includes the use of human body parts such as finger prints, face, iris, DNA, heartbeat, hand geometry, retina etc. for purpose of identification [2].

(ii)Non-Anatomical Biometrics**:** Non-Anatomical biometric includes human behavior characteristics such as human speech, handwritten signature etc. are used for identification [2].

The characteristics that are captured essentially need to be [16]

- Universal: Every person must possess the characteristic. It must be one that is seldom lost to accident or disease.
- Invariant: It should be constant over long period of time.
- Singular: It must be unique to individual.
- Inimitable: It should be reproducible by other means.
- Reducible and comparable: It should be capable of being reduced to a format that is easy to handle and digitally comparable to others.
- Reliable and temper-resistant: It should be impractical to mask or manipulate. In certainty there are many kinds of biometric characteristics which can be used to verify a user. Each of these methods has their own characteristic way of

operating. Although biometric tools are differ in many ways, but their basic operation model is the same.

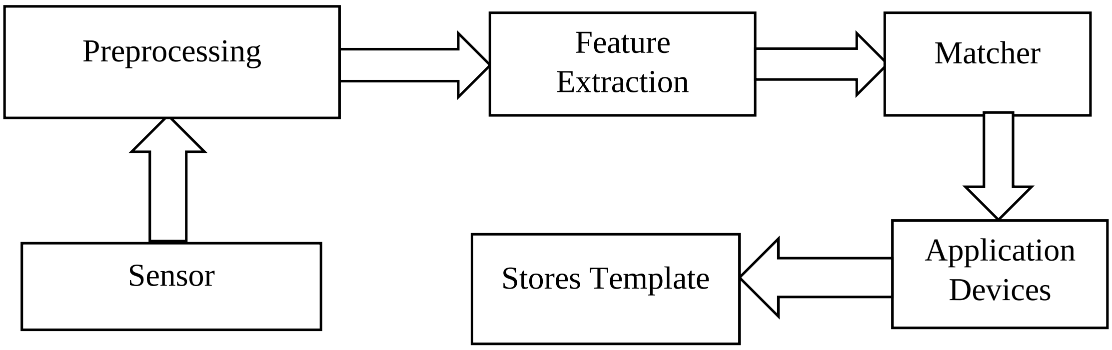


Figure 1.1: Biometric System

The biometric system consists of two types, identify and verifying users.

a) Verification Process based on Biometric

In verification process, Biometric data or claimed identity is retrieved from user and is compared with the Biometric data present in the data base of the system and a degree of similarity is obtained known as "comparison score". A decision subsystem is used which uses a predefined threshold to verify user's identity. Verification is correct if a true claim is accepted and false claim is rejected and is incorrect if either a true claim is rejected or a false claim is accepted [2].

b) Identification Process based on Biometric

Identification process is similar to verification process except that during identification claimed identity is not provided only biometric data of the user is supplied to the data capture subsystem. This data coming from sensor is then processed by extracting the features and comparing them with biometric references stored in data storage system. The biometric system generates a candidate list of enrolled based on the degree of similarity. The results obtained are correct when user is enrolled in the system and his/her identity is included on the candidate list of records otherwise the results are incorrect [1].

Nowadays, Biometric systems are widely used in many kind of industries, banks, colleges etc. The Biometric system provides a very high level of security and is very comfortable for the users. The present work is on online signature verification system using DFrCT.

1.2 SIGNATURE VERIFICATION

Signature verification is a common behavioral biometric to identify human beings for purposes of verifying their identity. Even if skilled forgers can accurately reproduce the shape of signatures, but it is unlikely that they can simultaneously reproduce the dynamic properties as well [51].

Signature verification is split into two categories according to the available input data.

(a) Offline (Static): The input of offline signature verification system is the image of a signature. The offline signatures are verified using various techniques such as hidden markov model (HMM), segmentation of signature, support vector machine (SVM) [20, 30, 36]. The application of offline signature is found on bank checks and documents.

(b) Online (Dynamic): Signatures that are captured by data acquisition devices like pressure-sensitive tablets and webcam. These devices extract dynamic features of a signature in addition to its shape (static). The online signatures are verification using various techniques such as finite impulse response (FIR), personalized template, logarithmic spectrum [12, 37, 49].

The applications of online signatures can be used in real time like credit card transactions, protection of small personal devices (PDA), authorization of computer users for accessing sensitive data or programs, and authentication of individuals for access to physical devices or buildings.

1.3 GENERAL SIGNATURE VERIFICATION SYSTEM

A dynamic signature verification system gets its input from data acquisition device like a digital tablet or other, dynamic input device. The signature is then represented as time-varying signals. The verification system focuses on how the signature is being written rather than how the signature was written. This provides a better means to grasp the individuality of the writer but fails to recognize the writing itself.

In general online signature verification system has different phases. These phases are treated as an individual processes. The general signature verification system diagram is shown Figure 1.2. The figure shows the process used for development of system. Input is taken from a digitizer or such kind of device like webcam. This input is in the form of signal.

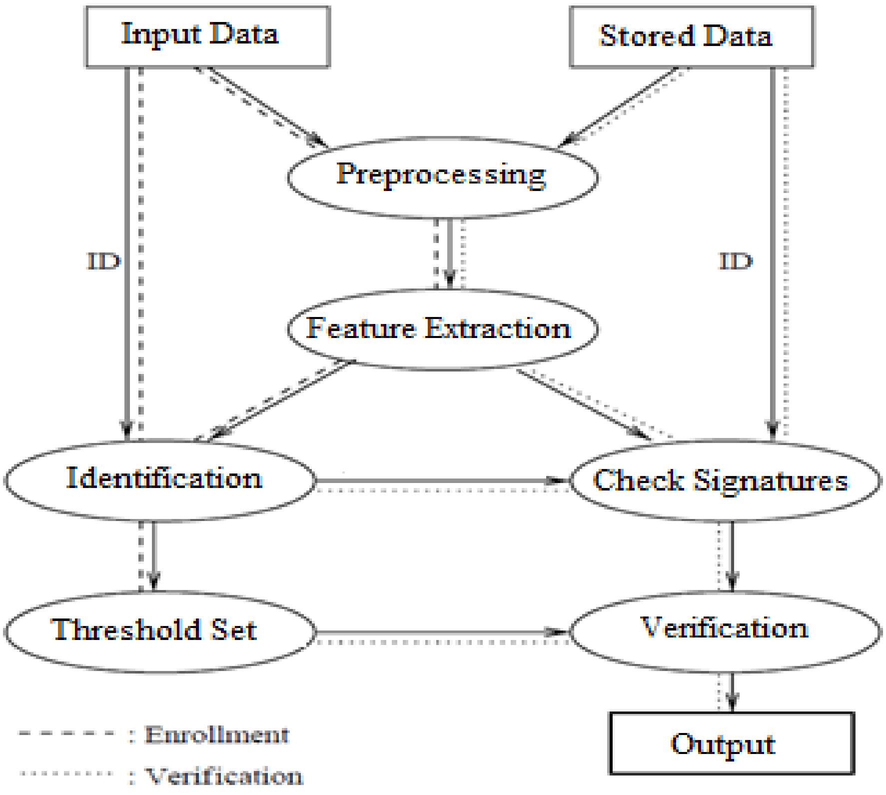


Figure 1.2: General Signature verification system

1.3.1 Input

For an on-line signature verification system, input is dynamic. This input is normally captured through a digital tablet or like other device. This input is digitized and fed for processing. First of all pre-processing is done on the input received and then some features are extracted from the captured online data on the basis of which the signature is validated [31].

1.3.2 Preprocessing

There are some common preprocessing steps, aimed to improve the performance of a verification system. These include size normalization, smoothing of the trajectory and re-sampling of the signature data. Low resolution tablet or low sampling rates tablets may give signatures that have jaggedness which is commonly removed using smoothing techniques. In the systems where tablets of different active areas are used, signature size normalization is a frequently used as preprocessing technique. Comparing of two signatures having the same shape but of different sizes would result in low similarity scores. Size normalization is applied to remove that affect. Modern digital tablets have a sampling rate of more than 100 trajectory points per second. In some of the previous methods, re-sampling, as a preprocessing step, was used to remove possibly redundant data. After successful re-sampling, shape related features were reliably extracted [50].

1.3.3 Feature Extraction

Feature extraction stage is one of the crucial stages of an on-line signature verification system. Features cans be classified as global or local, where global features represents signature's properties as a whole and local ones correspond to properties specific to a sampling point. The global features examples are signature bounding box, trajectory length or average signing speed, and distance or curvature change between consecutive points on the signature trajectory are local features. The signature authentication has various features types [15]It is important to implement identity verification modality which provides high degree in performance and is still acceptable by a majority of users. A signature can be authenticated using either static (off-line) or dynamic (on-line) verification.

1.3.3.1 Static (off-line): The signature is written either on a piece of paper and then scanned or directly on the computer using devices such as the digital pad. The shape of the signature is then compared with the enrolled (reference) signature. The difficulty with this technique is that a good forger will be able to copy the shape of the signature [51].

The selection of features for extraction is difficult for the performance of a bio-metric authentication system. The features extracted must have able to describe the signature, separable between classes and also invariant within the same class. Two types of features can be extracted are both dynamic and static feature sets. For both dynamic and static feature sets, they are parameter based features and function based features. In general, function based features give better performance than parameters, but they usually time-consuming matching procedures. Parameter based features are easily computed and matched because of its simplicity.

When creating a system, it is important task is to take into account different external factors. For example like a bank or teller application, the retrieval of features and computation of matching has to be fast as well as accurate for feasibility for such an application. For daily access control depending on the level of security, speed is an issue. The cost of creating a system is also an issue for certain applications. Certain criterions have to be established during feature extraction to obtain the suitability of the feature set. The list of the criteria shown below, which act as a guideline to obtain the appropriate features [33].

- Selected features must have a high inter-personal variance to ensure that the signatures are separable based on different classes. This allows for low equal error rates during verification.
- It is must to have a low intra-personal variance for the selected features. This will allow the same type of signatures to group together, enabling better performance for the system.
- The features set extraction should be fast, quite simple and easy to compute in order to have a system which has low computational power.
- The amount of features extracted has to be small enough to be stored in a smart card. The number of features should be small, will in turn allow for quicker and faster computation.
- The number of features should be large enough to ensure that the signatures of different users are distinguishable with minimum computational risk.
- Selected features cannot be reverse-engineered to get the original sketch of the signature. This is to ensure that even if the features were to be obtained, the original knowledge of the signature is still unknown.

1.3.3.2 Dynamic (on-line): The user's signature is acquired in real-time. By using this dynamic data, further feature such as acceleration, velocity, and instantaneous trajectory angles and displacements can be extracted [33].

The dynamic feature set describes how the signature is being signed rather than how it seems. Dynamics of the signature are very difficult to forge because these not only have the information of the overall shape of the signature, but also dynamic information of signature. When the user sign on a data acquisition module, it needs to be scanned at a rate high enough to capture this information, and from this dynamic data, relevant features are extracted.

The dynamic feature set extracted consists of global parameter based features which allows us for easy and quick computing. This feature set requires less computational power and is of more cost efficient although it might not perform as well with compare to function based feature sets. The list of dynamic feature set is as follows:

- Total signing time (1 digit): This feature represents the time taken to sign the signature. This is extracted by counting the number of coordinates recorded while the individual is signing. Each obtained coordinate is sampled at a constant rate.
- Number of pen ups (1 digit): The recorded feature shows the number of times the pen leaves the data acquisition screen during signing time is called the number of pen-ups occurred during signing.
- Total length of the sign (1 digit): The total length of the signature calculated by adding the distance between each of the coordinates.
- Maximum velocity (1 digit): While signing the maximum velocity found between two consecutive coordinates.
- Minimum velocity (1 digit): While signing the minimum velocity found between two consecutive coordinates.
- Duration of Horizontal movement: The total time that the pen is moving from left to right is indicated by this feature. It is obtained by adding up the amount of times that the pen is moving from left to right between two consecutive coordinates.
- Duration of Vertical movement: The total time that the pen is moving from down to up. It is obtained by adding up the amount of times that the pen is moving from down to up between two consecutive coordinates.
- Length of signature horizontal: This feature describes the width of the signature. It can be found by subtracting the maximum x coordinate value with the minimum x- coordinate value.
- Length of signature vertical: This feature describes the height of the signature. It can be found by subtracting the maximum y coordinate value with the minimum y-coordinate value.
- Area of signature: It can be found by multiplying both the length of the signature vertically and the length of the signature horizontally [51].

1.3.4 Verification

During the verification stage, a signature to be tested and an ID of a claimed user are submitted to the system. The test signature is compared with the template of reference signatures enrolled in the data base. A threshold value is defined and the test signature is classified as genuine or forged depending on the threshold value [14].

1.3.5 Identification

During the identification stage, only the test signature and no ID are submitted to the system. The unknown test signature is compared with every template signature enrolled in the database. The signature is identified which it belonging to in the database to which it is closest to [14].

1.3.6 Output

The output obtained from an online signature verification system is a decision if the person providing the signature is authorized or not [38]. The performance of biometric verification systems is typically described based 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 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 biometric system, receiver operating characteristic (ROC) curves are drawn. Biometric systems generate matching scores that represent how similar (or dissimilar) the input is compared with the stored template. This score is compared with a threshold to make the decision of rejecting or accepting the user. The threshold value can be changed in order to obtain various FAR and FRR combinations. The ROC curve represents how the FAR changes with respect to the FRR and vice-versa. The genuine accept rate is obtained by simply one minus the FRR [16]. The signatures verification has been performed using various techniques String Matching [1], Monte Carlo technique [15], Hidden Markov method [18], Support Vector Machine [20], DFrCT [31], Dynamic Time Warping [39], Wavelet Transform Technique [44] etc.

1.4 FRACTIONAL TRANSFORMS

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 [50] and it was established in the same year that the other transforms could also be fractionalized [7]. In a very short span of time, FrFT has established itself as a powerful tool for the analysis of time varying signals [52]. 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 [42], [45], [56]. 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. In 2001, S. C Pei [43] 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.

1.5 ORGANIZATION OF DISSERTATION

This dissertation consists of 4 chapters including the introduction. The concept of biometrics along with signature verification is briefly introduced. The signature verification and general model for verification have also been discussed.

Chapter 2: Literature review, in this chapter the study on existing signature verification system is discussed. The designing methods for online/offline signature verification have been also discussed. Being motivated from gaps in literature, the objectives have been also defined in this chapter.

Chapter 3: Signature verification System using discrete fractional cosine transform (DFrCT) with FIR system has been discussed. The simulation results for feature extraction for signature verification using DFrCT have been given in this chapter.

Chapter 4: Conclusion, in this chapter the present work has been concluded, on the basis of observations and also future scope has been given.

2. LITERATURE REVIEW

The history of research work on signature verification and fractional transforms is given in this chapter. In the literature survey, various techniques of signature verification with their applications has been discussed. The gaps of literature review motivated to define the objectives given at the end of this chapter.

2.1 ONLINE AND OFFLINE SIGNATURE VERIFICATION TECHNIQUES

Many techniques are presented by researchers [1, 15, 18, 20, 39, 44] from time to time for online as well as offline signature verification. These are:

- Dynamic Time Warping
- FIR system
- Monte Carlo technique
- Hidden Markov Model
- String Matching
- Support vector machine
- Wavelet Transform technique
- Some other techniques.

2.1.1 Dynamic Time Warping

A technique based on DTW (Dynamic Time Warping) for online signature verification system was proposed in 1996 [39]. This algorithm was originally used for speech recognition which is applied to signature verification. In this algorithm large numbers of reference pattern are observed to extract different features of signature. To deal with this extra information efficiently DTW stage and feature extraction process are carried out separately.

In this paper, a method for the automatic handwritten signature verification (AHSV) is described. The method was proposed in 2008 [23] the system 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 the 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.

This method developed an approach to identify the authenticity of signatures based on the variance and is proposed in 2009 [28]. Experimental dataset was taken from SVC2004 Database, variance and Dynamic Time Warping algorithm were combined 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.

In this paper an on-line signature verification system based on an collaborative of local, area, and over-all matchers is offered proposed in 2010 [29]. Definitely, the resulting identical methodologies are taken into justification: the merging of two local approaches using Dynamic Time Warping, Hidden Markov Model based methodology where each signature is defined by means of its regional things, and a Lined Encoding descriptor classifier skilled by universal features.

Proposed an approach named Bio convolving to ensure security and renewability of biometric templates in 2010 [19]. In order to generate multiple transformed versions of templates, a set of noninvertible transformed are introduced in this technique. Moreover retrieving original data from the transformed data is become quite easy with this method. This technique is employed on online signature verification and its performance is evaluate using MCYT database on the basis of two parameters i.e. authentication rate and renewability capacity.

2.1.2 FIR Filter system

This method is based on finite impulse response (FIR) system characterizing velocity and direction change of barycenter trajectory proposed in 1996 [49]. 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 sub systems for a reference signature and the signature to be verified.

2.1.3 Monte Carlo Technique

A new algorithm called Monte Carlo based Bayesian scheme for signature verification proposed in 2006 [15]. This system consists of two phase of testing in the first phase i.e. learning phase and the second is testing phase. In the first phase semi-parametric models are trained using Markov Chain Monte Carlo (MCMC) to draw posterior samples. In the second phase i.e. testing phase these signatures are tested and tells the signature is genuine or forgery. The proposed work achieves better EER.

A camera-based online signature verification system is proposed in this paper in [2009] [14]. 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 trained by using Ada Boost combines the distances and computes a final score. Preliminary experiments were performed by using a private database. The proposed system yielded an equal error rate (EER) of 4.0%.

2.1.4 Hidden Markov Model

This work reports the involvement to signature authentication considering dissimilar forgery types in an HMM structure 2000 [18]. The works involved of three main methods: pre-processing, division and feature extraction. During the preprocessing, they suggested the horizontal division to divide the inscribed part into three sectors: upper sectors (ascenders), medium sectors (main body) and lower sectors (descends), then designed by perpendicular separation which including the use of balances with rectangular cells, which existing a learning method based on HMM for the division. An automatic source process of the decision threshold was used in the identical method.

2.1.5 String Matching

This is a work for on-line handwritten signature authentication. The signatures are developed using a digitizing tablet which imprisonments both lively and latitudinal information of the text 2002 [1]. After preprocessing the signature, numerous features are take out. The validity of a writer is examined by equating an input signature to a reference one containing of three signatures. The resemblance between an input signature and the reference signature is calculated using string matching and the resemblance value is equated to a threshold.

2.1.6 Support Vector Machine

This work presents an off-line signature verification and retort system using the universal, guiding and grid parameters of signatures proposed in 2005 [20]. Here Support Vector Machine (SVM) was used to authenticate and organize the signatures and a procedure ratio of 0.95 was obtained. As the acknowledgement of signatures indicates a multiclass problem SVM's one-against-all method was used. This scheme performance is also compared with Artificial Neural Network’s (ANN) back propagation system.

2.1.7 Wavelet Transform Technique

In this work, a new on-line signature verification system is proposed in 2010 [44]. 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. 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.

2.1.8 Other Techniques

A new approach is developed for signature verification. In this technique the signature is assumed as vector random process with component x, y coordinates and instantaneous velocity is proposed in 1995 [32]. This process is represented with VAR (vector auto regression) model to approximate the changes in complex contour. In order to extract distinct features correlation between signature sequences is calculated by the vector structure. Model matrix are used to get features vectors which tells the verification of the users identity.

This work presents a novel method of on-line signature verification that analyzes both the shape of the signature and the dynamic of the writing process in 1997 [12]. 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.

In this paper, an on-line signature verification scheme based on similarity measurement of logarithmic spectrum was proposed in 1998 [37]. 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. Based on the experimentation, the rates of false rejection errors and false acceptance errors are as low as 1.4 and 2.8%, respectively.

This paper proposed a weighted multi expert strategy for online handwritten Chinese signature verification system in 1998 [6]. In this paper seven features are used for verify seven expert. Imitative signature are used to compare genuine and imitative writer. Now a final decision is made by combining the partial results a weighted multi expert system is proposed. The propose multi expert system analyze the discriminative ability and give different weight values to specified person. Lower discriminative shows lower weight value for a person.

This paper proposes an off-line signature verification system based on a displacement extraction method in which a questionable signature is compared with a corresponding authentic one in 2001 [54]. 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. An experiment was performed to evaluate the effectiveness of the proposed system, with resultant error rates being as low as 24.9% a level much better than that obtained by a method utilizing no displacement function.

This work presents an off-line signature authentication technique using a model-based methodology in 2002 [25]. In this process, arithmetic models are built for both pixel distribution and structural arrangement description. In addition to modest geometric handwriting parameters, it is proposed to use the directional frontier parameter as a basic descriptor of the signature. The arithmetical verification procedure based on the geometric handwriting parameter is used to accept signatures which thoroughly look like the reference signature, and to reject random and less trained forgeries. For the doubtful signatures for which the pixel parameter decision is unconvincing, the basic feature verification algorithm is invoked. This procedure compares the complete structural correlation between the input and reference signatures.

There are two common methodologies to verify signatures: the functional approach and the parametric approach. In this paper, a new warping technique for the functional approach in signature verification is proposed in 2003 [22]. 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 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. With the use of EPW, the equal error rate is improved by a factor of 1.3 and the computation time is reduced by a factor of 11.

In this work, two approaches are suggested to path the differences. Given the set of prepared signatures sections, the initial process measures the positional deviations of the one-dimensional projection outlines of the signature designs; and the second technique defines the differences in comparative stroke locations in the two-dimension signature designs in 2003 [4]. The figures on these variations are determined from the training set. Assumed a signature to be tested, the positional displacements are determined and the realism is decided based on the data of the training models. For the purpose of judgment, two current approaches proposed by other scholars were applied and verified on the same databank.

The re-evaluation of algorithm using the database SVC2004 and the effectiveness of pen pressure, azimuth and altitude is discussed and is proposed in 2003 [14].

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. When pen pressure and inclination features were considered, an EER of 3.61%was achieved, compared to an EER of 5.79% when these features were not used.

In this work, a simple and actual signature authentication method that depends only on the rare binary pixel intensities and avoids using difficult sets of features is extended 2007 [24]. The process looks at the signature authentication problem as a graph matching problem. The technique is verified using genuine and forgery signatures shaped by five subjects. An equal error rate of 26.7% and 5.6% was succeeded for skilled and random forgeries, respectively. A positive property of the procedure is that the false acceptance rate (FAR) of random forgeries disappears at the point of identical false rejection and skilled forgery false acceptance rates. Keeping the standardization size at 32 × 64 pixels makes the authentication time in the two seconds range.

This paper is based on Singular Value Decomposition (SVD) in finding the single vector sensing the maximal energy of glove matrix a, called principal subspace 2008 [35]. The effective dimensionality of A can be reduced. The signature authentication is performed by finding the angle between the different subspaces. The SVD based signature verification technique is tested and its performance is shown through EER.

In this paper an off-line signature verification and recognition system based on a combination of features extracted such as global features, mask features and grid features is proposed in 2009 [5]. 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. The results were very promising and a success rate of 84.1% was achieved using a localized threshold.

A new technique i.e. LCSS (Longest Common Sub Sequences) detection algorithm for online signature verification 2010 [9]. This technique measures the similarity in the signature time series into a kernel function for SVM (Support Vector Machine). The local variability of the signature such as Force of pen, Time stamp of tip, Change in angle etc. are measured by LCSS. Proposed technique is better than existing technique. SVM-LCSS is significantly better and more reliable than with SVM-DTW.

A technique Viterbi path and signature Log Likelihoods is used to analyze the effect of set choice of features on performance of verification of generative model based online signature verification 2012 [17]. Moreover higher order dynamic information, pressure and inclination angles. Information are included to obtain better results. Viterbi path shows better results for both user-specific hidden markov model (US-HMM) and user adaptive universal background models (UA-UBM) systems.

A technique on FPGA (Field Programmable Gate Arrays) of an embedded system is proposed in 2014 [33]. This algorithm consists of three stages. In the first stage preprocessing on signature for noise removal and normalization information related to horizontal and vertical positions. In the second stage DTW algorithm is applied on previously stored template. In final stage, feature extraction is carried out and pass through Gaussian mixture model to calculate degree of similarities between signatures. The algorithm is testing using vector floating point unit (VFPU) along with Microprocessor to accelerate the floating point computation in Biometric Modality.

This paper verifies the signature using touch interface mobile devices in 2014 [34]. An online signature is represented with a discriminative features vector derived from attributes of several histograms that can be computed in linear time. The resulting signature is compact and requires constant space.

In this paper, a new method for online signature verification system is proposed based on DFrCT (Discrete Fractional Cosine Transform) is proposed in 2014 [31]. In this technique three FIR filter are used to Euclidean norm of the system. To verify the efficiency of the proposed method EER is calculate and verified through simulation results which shows better results as compared to DCT.

There is a close relationship between the conventional Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT). Here, introduce another transform, the (DFrCT), which has a similar relationship with the Discrete Fractional Fourier Transform (DFrFT). The DFrCT share many useful properties of the regular cosine transform, and has a free parameter, its fraction. The extra degree of freedom provided by fraction transform is its benefit to signature verification. When the fraction is zero, the cosine modulated version of the input signal. When it is unity, the conventional DCT is achieved. As the fraction changes from 0 to 1 the different forms of the signal which interpolate between the cosines 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 where DCT is found to be useful.

2.2 FRACTIONAL FOURIER TRANSFORM

The FrFT belongs to the class of time-frequency representations that have been extensively used by the signal processing community [7]. In all the time-frequency representations, one normally uses a plane with two orthogonal axes corresponding to time and frequency. If 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 counterclockwise rotation of the axis by an angle $\pi/2$. This is consistent with some of the observed properties of the Fourier transform. For example, two successive rotations of the signal through $\pi/2$ 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 $\pi/2$, i.e. it is the representation of the signal along the axis u making an angle a with the time axis [42]. With the advent of FrFT and related concept, it is seen that the properties and applications of the ordinary Fourier transform are special cases of those of the FrFT. The FrFT is defined with the help of the transformation kernel $K\alpha,$ as [7]

$$K_\alpha(t,u) = \begin{cases} \delta(t-u) \\ \delta(t-u) \\ \sqrt{\frac{1-jcot\alpha}{2\pi}}\, e^{j((u^2+t^2)/2)cot\alpha - jutcosec(\alpha)} \end{cases} \tag{2.1}$$

Another useful form of writing the square root factor preceding the transformation kernel K_α can be obtained using the relation [51]

$$\sqrt{\frac{1-jcot\alpha}{2\pi}} = \sqrt{\frac{-je^{j\alpha}}{2\pi sin\alpha}} \tag{2.2}$$

Let F_α denote the operator corresponding to the FrFT of angle a. Under this notation, some of the important properties of the FrFT operator are listed below [7]

- For a =a=0 do get the identify operator: F^0= F 4 = I
- For a = π /2; i.e. a=1,we get the Fourier operator: F^1 = F
- For a =π; i.e. a=2, the reflection operator is: F^2= FF = I
- For a = $3\pi/2$; i.e. a=3,we get the inverse Fourier operator: F^3 = FF^2= F

2.2.1 DISCRETE FRACTIONAL FOURIER TRANSFORM (DFrFT)

The fractional Fourier transform is a member of a more general class of transformations that are sometimes called linear canonical transformations or quadratic-phase transforms. Members of this class of transformations can be broken down into a succession of simpler operations, such as chirp multiplication, chirp convolution, scaling, and ordinary Fourier transformation [52].

The one-dimensional FrFT is useful in processing single-dimensional signals such as speech waveforms. For analysis of two-dimensional (2D) signals such as images, need a 2D version of the FrFT. For a $M \times N$ matrix, the 2D FrFT is computed in a simple way: The 1D FrFT is applied to each row of matrix and then to each column of the result. Thus, the generalization of the FrFT to two-dimension is given by S.C. Pie et.al. and C.Candan et.al. [7, 43]

$$X_{\alpha,\beta}(u,s) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} K_{\alpha,\beta}(u,s;t,r)x(t,r)dtdr \tag{2.3}$$

$$K_{\alpha,\beta}(u,s;t,r) = k_\alpha(u,t)k_\beta(s,r) \tag{2.4}$$

In the case of the two-dimensional FrFT in this have to consider two angles of rotation $\alpha = a\pi/2$ and $\beta = b\pi/2$. If one of these angles is zero, the 2D transformation kernel reduces to the 1D transformation kernel. The FrFT can be extended for higher dimensions as:

$$X_{(\alpha_{1---}\alpha_n)}(u_{1---}u_n) = \int_{-\alpha}^{\alpha} -- \int_{-\alpha}^{\alpha} k_{\alpha_{1---}\alpha_n}(u_{1---}u_2; t_{1,---}t_n)k(t_{1,---}t_n)dt_{1---}dt_n \tag{2.5}$$

2.2.2 DISCRETE COSINE TRANSFORM

In particular, a DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the

Fourier transform of a real and even function is real and even), where in some variants the input and/or output data are shifted by half a sample. There are eight standard DCT variants, of which DCT-II is mostly used and is discussed below [56]

Formally, the discrete cosine transform technique (DCT) is a linear invertible function $f:\mathbb{R}^N \to \mathbb{R}^N$ (where $\mathbb{R}$ denotes the set of real numbers), or equivalently an invertible $N \times N$ square matrix. There are several variants of the DCT with slightly modified definitions. The N real numbers $x_{0,.....}, x_{N-1}$ are transformed into the N real numbers $X_{0,,.....}, X_{N-1}$ according to one of the formulas [56]

DCT-II

$$X_k = \sum_{n=0}^{N-1} x_n cos\left[\frac{\pi}{N}\left(n+\frac{1}{2}\right)k\right] \quad k = 0,.....,N-1 \tag{2.6}$$

The DCT-II is probably the most commonly used form, and is often simply referred to as the DCT.

This transform is exactly equivalent (up to an overall scale factor of 2) to a DFT of $4N$ real inputs of even symmetry where the even-indexed elements are zero. That is, it is half of the DFT of the $4N$ inputs y_n, where $y_{2n} = 0$, $y_{2n+1} = x_n$ for $0 \le n < N$, $y_{2N} = 0$, and $y_{4N-n} = y_n$ for $0 < n < 2N$ [54].

Some authors further multiply the $X0$ term by $1/\sqrt{2}$ and multiply the resulting matrix by an overall scale factor of $\sqrt{2/N}$ (see below for the corresponding change in DCT-III). This makes the DCT-II matrix orthogonal, but breaks the direct correspondence with a real-even DFT of half-shifted input [56].

The DCT-II implies the boundary conditions: x_n is even around $n = -1/2$ and even around $n = N - 1/2$; X_k is even around $k = 0$ and odd around $k = N$.

2.2.3 DISCRETE FRACTIONAL COSINE TRANSFORM

DFrCT basically involves rotation of a discrete signal by an angle α in the time-frequency plane. But for analysis of 2D signals such as images, a two dimensional version of DFrCT is required. For an matrix, the 2D DFrCT is computed in an unpretentious way. The 1D DFrCT is applied to each row of given matrix and then same is applied to each column of the result matrix. Thus, the generalization of the DFrCT to 2D is given by taking the DFrCT of the rows of the matrix i.e. image in a fractional domain and then taking the DFrCT of the subsequent column wise. In case of 2D DFrCT, two angles of rotation $\alpha = \ \pi/2 \ and\ \beta = \pi/2$ have to be taken. It has been recently observed that DFrCT can be used in the field of image processing .The vital feature of Discrete Fractional Cosine domain Image compression aids from its extra degree of freedom that is provided by its fractional orders. DCT-I is chosen & used in developing DFrCT [23].The four types of DCT [56]

DCT-I $$C^{I}_{N+1} = \sqrt{2/N}\,[K_m K_n cos(mn\pi/N)] \quad (2.7)$$

$$for\ m,n = 0,1,\dots N$$

DCT-II $$C^{II}_{N} = \sqrt{2/N}\left[K_m cos\left(m(n+\tfrac{1}{2})\pi/N\right)\right] \quad (2.8)$$

$$for\ m,n = 0,1,\dots N\text{-}1$$

DCT-III $$C^{III}_{N} = \sqrt{2/N}\left[K_n cos\left((m+\tfrac{1}{2})n\pi/N\right)\right] \quad (2.9)$$

$$for\ m,n = 0,1,\dots N\text{-}1$$

DCT-IV $$C^{IV}_{N} = \sqrt{2/N}\left[K_m cos\left((m+\tfrac{1}{2})(n+\tfrac{1}{2})\pi/N\right)\right] \quad (2.10)$$

$$for\ m,n = 0,1,\dots N\text{-}1$$

where, $K_m and\ K_n$

$$K_m = \begin{Bmatrix} \frac{1}{\sqrt{2}}\ for\ m = 0\ and\ m = N \\ 1\ otherwiswe \end{Bmatrix} \quad (2.11)$$

The DCT-I kernel has symmetric structure and is periodic with period 2. The periodicity means that repeated application of DCT-I would give the original sequence. DCT-IV is the same as DCT-I for symmetry and periodicity, but DCT-II and DCT-III operators are the forward and inverse transform pair of each other and are non-periodic.

$C_N^1 =$

$$\begin{bmatrix} \frac{1}{2} & \frac{1}{\sqrt{2}} & \cdots & \frac{1}{\sqrt{2}} & \frac{1}{2} \\ \frac{1}{\sqrt{2}} & \cos\frac{\pi}{N-1} & & \cos\frac{(N-2)\pi}{N-1} & \frac{1}{\sqrt{2}}\cos\frac{(N-1)\pi}{N-1} \\ \vdots & & \ddots & & \vdots \\ \frac{1}{\sqrt{2}} & \cos\frac{(N-2)\pi}{N-1} & & \cos\frac{(N-2)^2\pi}{N-1} & \frac{1}{\sqrt{2}}\cos\frac{(N-2)(N-1)\pi}{N-1} \\ \frac{1}{2} & \frac{1}{\sqrt{2}}\cos\frac{(N-1)\pi}{N-1} & \cdots & \frac{1}{\sqrt{2}}\cos\frac{(N-2)(N-1)\pi}{N-1} & \cos\frac{(N-1)^2\pi}{N-1} \end{bmatrix}$$

(2.12)

To develop the DFrCT, the eigenvalues and eigenvectors of DCT-I kernel matrix are needed to be well studied [56]-[45]. In [42], S.C Pei made five propositions which leads to the development of DFrCT.

1. The DFT kernel matrix has only four distinct eigenvalues : $\{1, -1, j, -j\}$ and its multiplicities are summarized in Table I. Because the DFT has only four distinct eigenvalues, the DFT eigenvectors will constitute four eigenspaces. It is trivial to find that any vector spanned by the DFT eigenvectors corresponding to the same eigenvalue is still a DFT eigenvector. Therefore, there exist infinite eigenvectors for the DFT kernel matrix. The multiplicities of DFT eigenvalues are just the dimensions of eigenspaces.

Table 2.1 Eigenvalue multiplicities of the DFT kernel matrices

N	Multiplicity of 1	Multiplicity of -j	Multiplicity of -1	Multiplicity of j
4m	m+1	m	m	m-1
4m+1	m+1	m	m	m
4m+2	m+1	m	m+1	m
4m+3	m+1	m+1	m+1	m

2. All the DFT eigenvectors are even or odd. The even eigenvectors are with the eigenvalues 1 or 1; in addition, the odd eigenvectors correspond to the eigenvalues $j, -j$. This proposition is very important for the development of

DFRCT; therefore, a review it here. In the following discussion, study the eigenvalues and eigenvectors for the DCT and the DST and establish the relationships with the conventional DFT.

3. The DCT-I eigenvectors can be attained from the DFT eigenvectors. If $v = [v_{0,} v_1 \ldots \ldots . v_{N-2}, v_{N-1,} v_{N-2,} \ldots \ldots . v_1]$ is an even eigenvector of the $(2N-2)$ Point DFT kernel matrix$F_{2N-2} v = \lambda\, v$, where $(\lambda = 1, -1)$. Then

$$\hat{v} = [v_0, \sqrt{2} v_1, \ldots \ldots, \sqrt{2} v_{N-2}, v_{1N-1}] \quad (2.13)$$

4. The eigenvalues of DCT-I kernel matrices are only 1 and -1. Their multiplicities are shown in Table 2.2.

Table 2.2 Eigenvalue multiplicities of the DCT-I kernel matrices

N	Multiplicity of 1	Multiplicity of -1
Even	*N*/2	*N*/2
Odd	(*N*+1)/2	(*N*-1)/2

Regardless of N is even or odd, the sum of multiplicity of 1 and multiplicity of -1 is equal to *N*. Thus, the DCT-I eigenvectors obtained from the DFT even eigenvectors can result in a full-rank DCT-I kernel matrix. All the DCT-I eigenvectors can be obtained from the DFT even eigenvectors.

5. The orthogonally in DCT-I and DST-I eigenvectors can be inherited from that in DFT eigenvectors. If v_m and v_n $(m \neq n)$ are both the even and orthogonal DFT eigenvectors, the DCT-I eigenvectors $\widehat{v_m}$ and $\widehat{v_n}$ will also be orthogonal.

$$v_m^T \widehat{v_n} = v_m^T v_n = 0 \quad (2.14)$$

This tells us that the DFT orthogonal eigenvectors can be used to generate the DCT-I orthogonal eigenvectors

From the previous discussions, came to know that all the DFT and DCT transform kernels have infinite eigenvectors. Because the DFRFT defined with these DFT Hermite eigenvectors can have similar output as continuous FRFT and will have the properties of unitarily, additivity, and reversibility, the DFT Hermite eigenvectors will be used in developing DFRCT as reasonable choices. The eigenvector $\widehat{v_n}$ will have the eigenvalue $e^{-jka} (k\ is\ even)$ for the DFrCT kernel matrix. Such an assignment rule will result in a DCT kernel for $\alpha = {}^{\pi}/_{2}$. Similar to the DFRFT, the N-point DFrCT kernel can be defined [45]

$$C_{N,\alpha} = V_N \widehat{D_N^{2\alpha/\pi}} \widehat{v_N^T} \tag{2.15}$$

where, $$\widehat{D_N^{2\alpha/\pi}} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & e^{-j2\alpha} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & e^{-j2(N-1)\alpha} \end{bmatrix} \tag{2.16}$$

and, $$\widehat{v_N} = \{\widehat{v_0} | \widehat{v_1}\} \dots . \{\widehat{v_{N-1}}\} \tag{2.17}$$

$\widehat{v_k}$ is the DCT-I eigenvector obtained from the K-order DFT Hermite eigenvector. While, $\alpha = {}^{\pi}/_{2}$ the DFRCT will become the conventional DCT-I. When, $\alpha = 0, C_{N,\alpha}$ is an identity matrix. The steps for constructing the *N*-point DFRCT kernel with angular parameter α are summarized as [45]

- Step-1: Compute the *M*-point DFT Hermite even eigenvectors. $M = 2(N - 1)$
- Step-2: Use (2.13) to compute the DCT-I eigenvectors from the DFT Hermite even eigenvectors.
- Step-3: Determine the DFRCT transform kernel from (2.15).

For the sake of simplicity, let us take the 8-point, type I forward DCT as an example. The corresponding matrix [55] can be expressed as

$$C = \sqrt{\frac{2}{8-1}} * \left[k_m k_n \cos\left(\frac{mn\pi}{8-1}\right)\right] \tag{2.18}$$

where, $m = 0,1,2, \dots ..7 \ and \ n = 0,1,2 \dots \dots 7$

$$k_m = \begin{Bmatrix} \frac{1}{\sqrt{2}} for \ m = 0 \\ 1 \ otherwise \end{Bmatrix} \tag{2.19}$$

$$k_n = \begin{Bmatrix} \frac{1}{\sqrt{2}} for \ n = 0 \\ 1 \ otherwise \end{Bmatrix} \tag{2.20}$$

It can be diagonalized by

$$C = UVU^T \tag{2.21}$$

where U is an orthonormal matrix obtained from the eigenvectors of C , V is a diagonal matrix composed of the corresponding eigenvalues, and U^T is the transpose matrix of U . The square of the DCT matrix can be written as

$$C^2 = C * C = UV^2U^T \tag{2.22}$$

Similarly,

$$C^\alpha = C * C = UV^\alpha U^T \tag{2.23}$$

$V^\alpha and\ V$ are given as follows:

$$V^\alpha = \begin{bmatrix} \lambda_1^\alpha & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda_2^\alpha & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_3^\alpha & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda_4^\alpha & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda_5^\alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda_6^\alpha & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda_7^\alpha & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_8^\alpha \end{bmatrix}$$

$$V = \begin{bmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

2.3 GAPS IN STUDY

Many hand written signature verification systems have been developed till date, for online verification schemes such as Probabilistic Model, Sequential Monte Carlo, String Matching, Log likelihood method, Wavelet transforms technique, Dynamic Time Warping etc. and or for offline verification schemes such as Hidden Markov Model, Euclidean distance, Statistical Model, Graph matching etc. Still, there was a need of system with minimum EER, FAR and FRR.

One such existing method is Discrete Fractional Cosine Transform which has extra degree of freedom to optimize the six extracted features of signatures. But, this method use same rotation angle for all features using three FIR filters. So, there was a necessity that more than six features should be extracted for accuracy and different rotation angles for different features should be used for security.

2.4 OBJECTIVES

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

1. To implement existing online signature verification technique.
2. To develop the algorithm with eight features and four FIR systems for online signature verification using DFrCT.
3. Comparison of presented algorithm with existing one based on parameters EER, FAR, and FRR.

2.5 SUMMARY

In this paper, various signature verification techniques developed over years have been reviewed. The discrete fractional fourier transforms and discrete fractional cosine transform is also discussed. Based on the gaps in the literature study, the objectives have been defined. The presented algorithm implementation and simulation results are given in the next chapter.

3.1 INTRODUCTION

The presented algorithm of online signature verification using DFrCT is based on Four FIR systems. The discrete fractional cosine transformation (DFrCT) [31] of barycenter trajectory in the horizontal and vertical direction are used as the input and the output of the system in first of the four mentioned FIR systems. The second FIR system has used 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. The third FIR system has used the DFrCTs of the areal velocity and the displacement are used as the input and the output of the system, respectively. Then in the fourth FIR system, the DFrCT of the area pressure and motion pressure are used as the input and output of the system. The impulse responses of FIR systems are used as features in order to verify a signature.

3.2 BLOCK DIAGRAM OF PRESENTED ONLINE SIGNATURE VERIFICATION SYSTEM

The block diagram of online signature verification system is shown in Figure 3.1. It consists of following steps:

- Input signature: A standard database of SVC2004 is used for testing. Corresponding to each user, 40 signatures are used, out of which 20 signatures are genuine and 20 signatures are forgery.
- Preprocessing process: In order to remove the fluctuations in the signature, the 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, feature extraction of the signature is done. The present algorithm extracts eight features namely horizontal pen point movement (Ex), vertical pen point movement (Ey), areal velocity (av), displacement from trajectory of barycenter (d), magnitude of velocity (v), change of angle trajectory of barycenter (θ), area pressure of the pen point movement (ap), motion pressure of the pen point movement (dp) have been extracted. The signature is described with DFrCT of these features used to define four FIR systems. The optimized free parameter (α) of DFrCT

increase accuracy in results. The optimization value of (α) is different for different features

- Signature Verification: The impulse responses of four FIR systems are used to verify a signature. The impulse response of all FIR systems are combined together to form a feature vector. The threshold level of signature verification is set with Euclidean norm of this vector. The different value between the reference signatures is calculated. The given signature is genuine if the difference value is less than threshold.

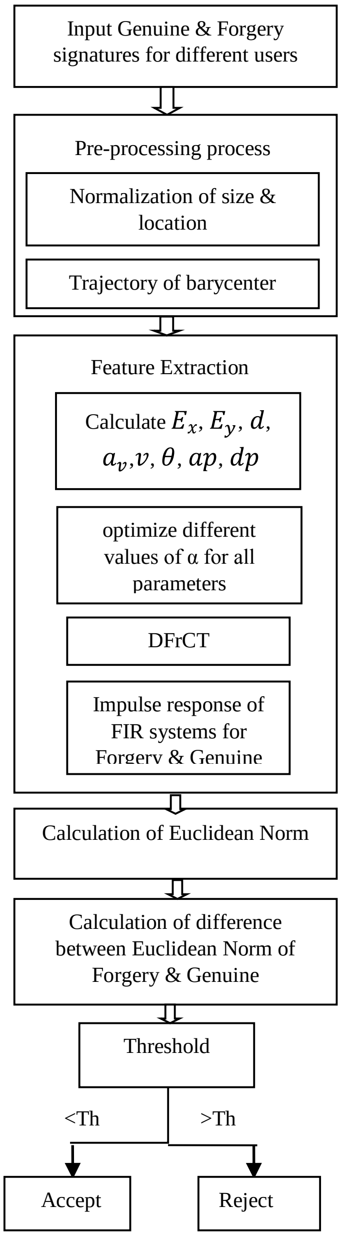


Figure 3.1: Block diagram of presented online signature verification system

3.3 PREPROCESSING

The horizontal and vertical components $x(t_n)$ and $y(t_n)$ are composed from a graphical tablet of a pen point movement at time(t_n). But the signature signed from the same user can never be same so there are some variations in the signature which are reduced in preprocessing process [31, 49].

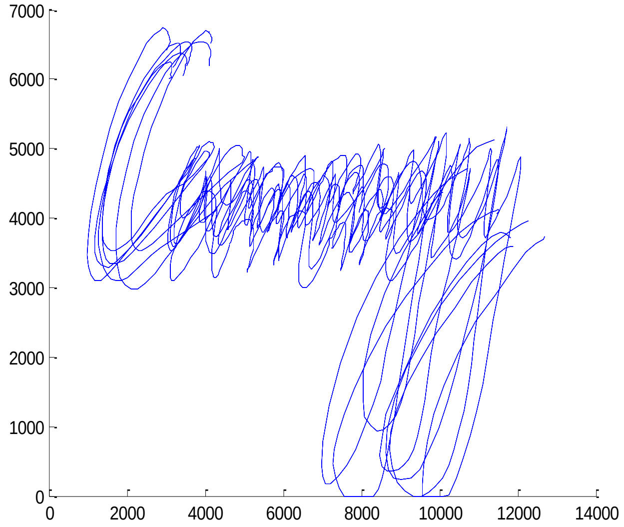


Figure 3.2: Original Signature of User 1

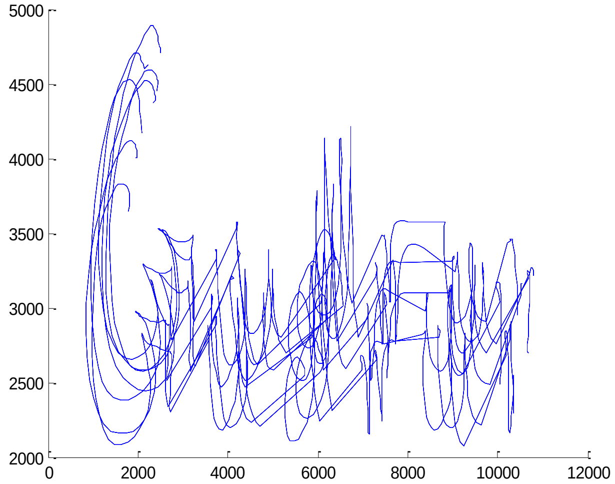


Figure 3.3: Original Signature of User 2

It has been observed from Figures 3.2 and 3.3 that signatures of user 1 and user 2 have fluctuations due to size and location.

3.3.1 Normalization of Size

The variations in the signature due to its size are normalized by making the average size of the signature as:

$$\hat{q}(t_n) = \frac{q(t_n) - q_{min}}{q_{max} - q_{min}} \tag{3.1}$$

where, $q = x, y, p\, q_{min} = \min q(t_n)\, q_{max} = \max q(t_n)$

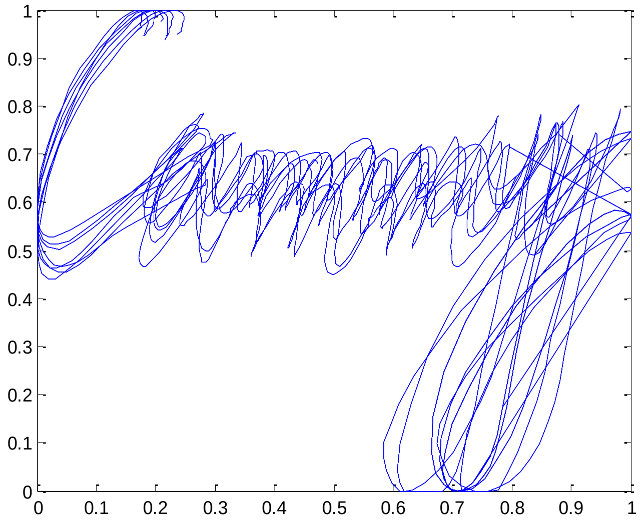


Figure 3.4: Normalization of size of User 1

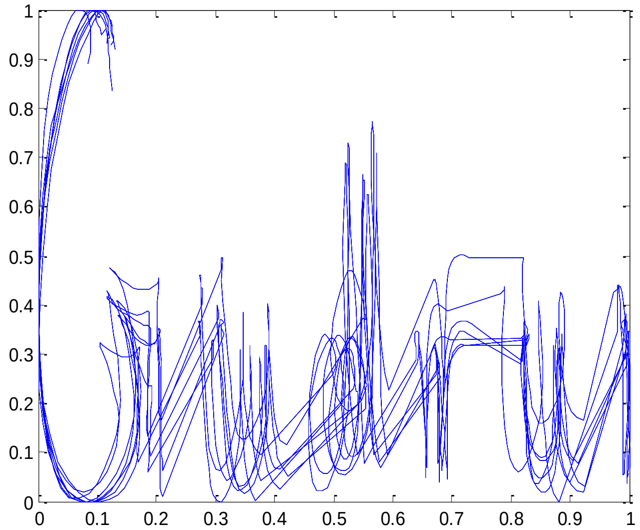


Figure 3.5: Normalization of size of User 2

The normalization of signature is done to reduce the size and location. The normalization of size is shown in Figures 3.4 and 3.5. The location normalization is shown in Figures 3.6 and 3.7.

3.3.2 Normalization of Location

The variations in the signature due to its location are normalized by calculating the coordinates of the center point (c_x, c_y, c_z) and then shifting to its origin as

$$c_q = \frac{1}{N}\sum_{n=0}^{N-1}\hat{q}(t_n) \tag{3.2}$$

where, $\tilde{q} = \hat{q}(t_n) - C_q$, $(n = 0,1,2,3 \ldots \ldots N - 1)$

where, c_q is the center point of the given signature and N is all the points during the pen point movement.

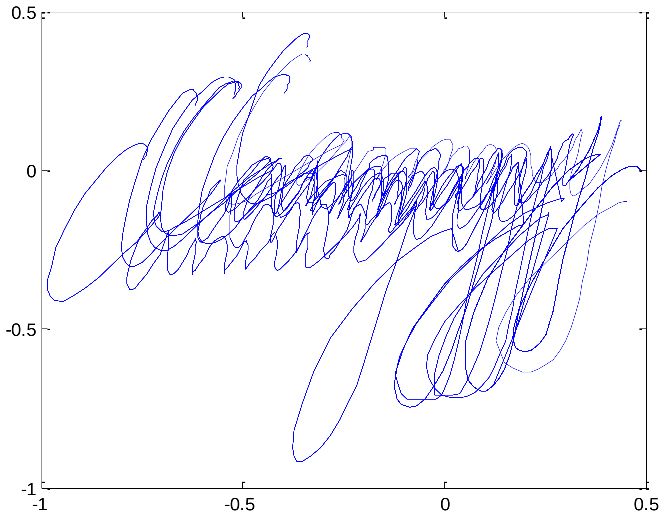


Figure 3.6: Normalization of Location of User 1

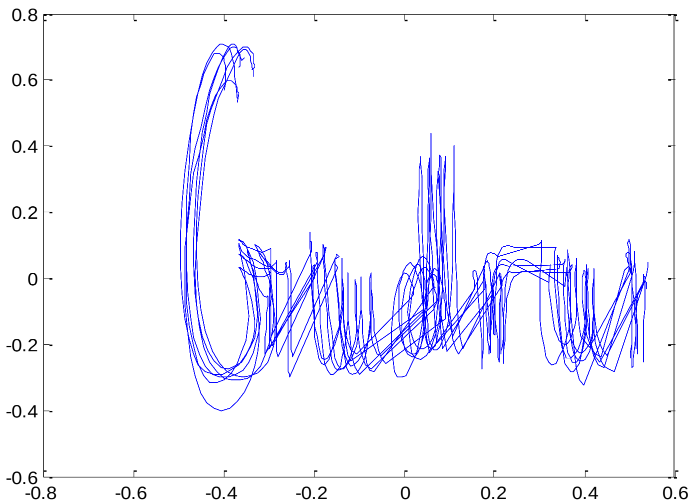


Figure 3.7: Normalization of Location of User 2

The normalization of size and location removes the fluctuations and helps in verifies the signature.

3.3.3 Trajectory of Barycenter

The variations related to pen point movement can be reduced with trajectory of barycenter. Trajectory of barycenter is designed from the center point of signature with two adjacent pen-point positions with respect to time. It can be calculated as:

$$E_q(t_n) = \frac{\hat{q}(t_n) + \hat{q}(t_n + 1)}{3} \tag{3.3}$$

To reduce the fluctuations due to pen point trajectory and barycenter trajectory is calculated. Figures 3.8, 3.9, 3.10 and 3.11 show pen point movement and barycenter trajectory for user 1 and 2.

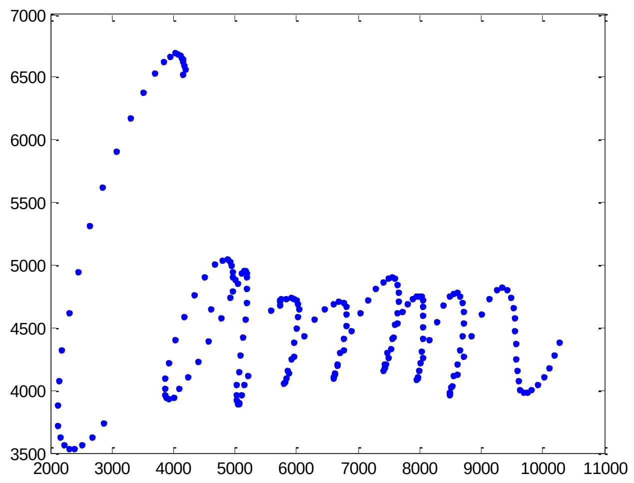


Figure 3.8: Pen Point Trajectory of User 1

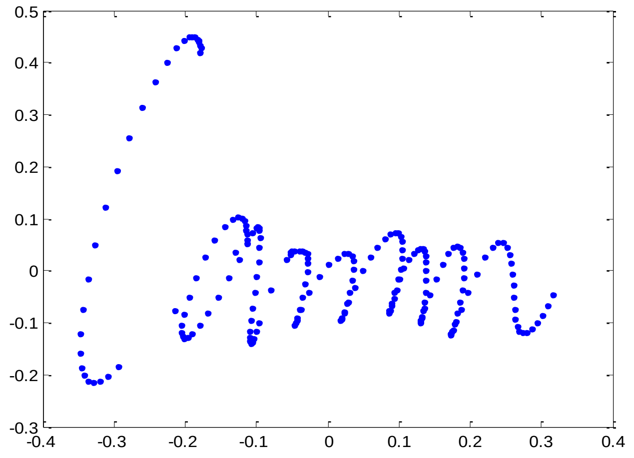


Figure 3.9: Barycenter Trajectory of User 1

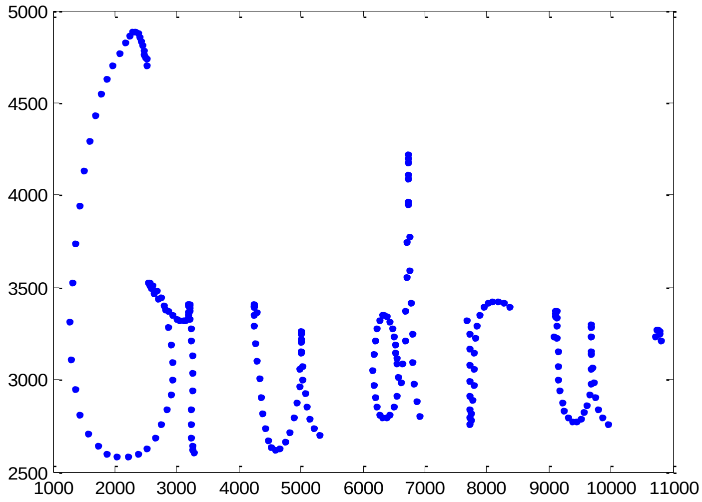


Figure 3.10: Pen Point Trajectory of User 2

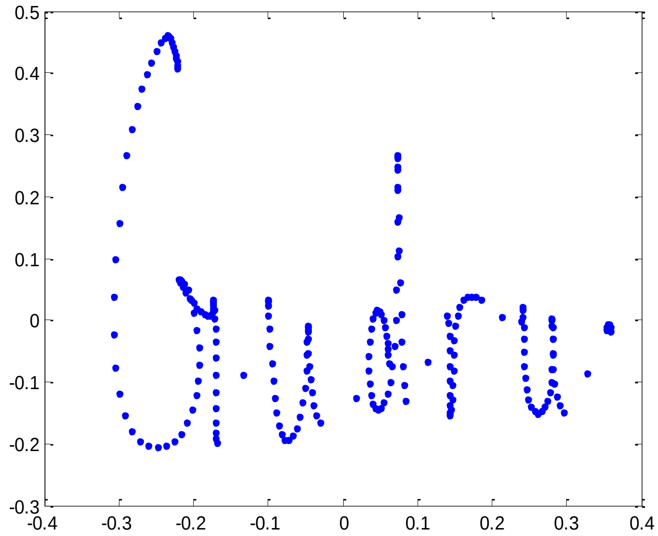


Figure 3.11: Barycenter Trajectory of User 2

Figures shows pen point trajectory and Barycenter Trajectory the variations related to pen movement are removed.

3.4 FEATURE EXTRACTION

The eight parameters that are considered for feature extraction in present work as [31]:

- Horizontal movement (E_x) of the pen-point for the period of signing
- Vertical movement (E_y) of the pen-point for the period of signing
- Areal velocity $a_v(t_n)$ is the area swept by a pen-point as it moves along the trajectory of signature

$$a_v(t_n) = \frac{1}{2}\begin{vmatrix} E_x(t_{n-1}) & E_y(t_{n-1}) \\ E_x(t_n) & E_y(t_n) \end{vmatrix} \qquad (3.4)$$

- Displacement $d(t_n)$ is the shortest distance between the centers of signature to barycenter trajectory at time (t_n)

$$d(t_n) = \sqrt{E_x(t_n)^2 + E_y(t_n)^2} \qquad (3.5)$$

- Velocity $v(t_n)$ can be calculated

$$v(t_n) = \sqrt{f_x(t_n)^2 + f_y(t_n)^2} \qquad (3.6)$$

where, $f_x(t_n) = E_x(t_{n+1}) - E_x(t_n)$

$$f_y(t_n) = E_y(t_{n+1}) - E_y(t_n)$$

- Direction change $\theta(t_n)$ of barycenter trajectory can be calculated

$$\theta(t_n) = \tan^{-1}\frac{E_y(t_{n+1}) - E_y(t_n)}{E_x(t_{n+1}) - E_x(t_n)} \qquad (3.7)$$

- Area pressure $ap(t_n)$ of barycenter trajectory is the pressure applied by a pen per unit time. It can be calculated

$$ap(t_n) = \frac{1}{2}P_1(t_n)\sqrt{E_x(t_n)^2 + E_y(t_n)^2} \qquad (3.8)$$

where, $P_1 = \frac{p(t_n) - p_{min}}{p_{max} - p_{min}}$

- Motion pressure $dp(t_n)$ of barycenter trajectory is calculated

$$dp(t_n) = p(t_{n+1}) - p(t_n) \qquad (3.9)$$

where, $p(t_n) = P_1(t_n) - C_q$

$$c_q = \frac{1}{N}\sum_{n=0}^{N-1}\hat{q}(t_n)$$

Now, in order to compute the separate feature, the technique discrete fractional cosine transform (DFrCT) $H_x(m)$,$H_y(m)$, $H_{av}(m)$, $H_v(m)$, $H_\theta(m)$,$H_d(m)$, $H_{ap}(m)$, and

$H_{dp}(m)$ of the $E_x(t_n)$,$E_y(t_n)$,$a_v(t_n), d(t_n), v(t_n), \theta(t_n), ap(t_n), and\ dp(t_n)$ is extracted [33]

$$H^q(m) = L_q \sum_{n=0}^{N-1} K_p(m,n)\, g(n) \tag{3.10}$$

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

where, K_p is the kernel (m, n) , $g(n)$ is the individual characteristics of the signature,$L_q$is the parameter and α is rotation angle is calculated as:

$$K_p(m,n) = \exp\left(\frac{i\left(m^2+n^2\right)\pi cos\alpha}{N}\right)\cos\left(\frac{2\pi mn}{N}\right) \tag{3.11}$$

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

$$L_q = \sqrt{\frac{2-i2cot\alpha}{\pi}}\sqrt{\frac{2\pi sin\alpha}{N}} \tag{3.12}$$

Additionally, four FIR systems [31] are used to describe the specific features of given signature. The relation between the features horizontal and vertical component of barycenter trajectory is considered in First FIR system. The DFrCT of $H_x(m)$ and $H_y(m)$ are taken as the input and output of this system

$$H_y(m) = \sum_{m=0}^{M} h_1(m) H_x(K-m) \tag{3.13}$$

The second FIR system considers the relation between the directional change and velocity is taken. The DFrCT of $H_\theta(m)$ and $H_v(m)$ are taken as the input and output of this system

$$H_v(m) = \sum_{m=0}^{M} h_2(m) H_\theta(K-m) \tag{3.14}$$

The third FIR system calculates the relation between the features areal velocity and displacement is taken the DFrCT of $H_{av}(m)$ and $H_d(m)$ are taken as the input and output of this system

$$H_d(m) = \sum_{m=0}^{M} h_3(m) H_{av}(K-m) \tag{3.15}$$

The fourth FIR system gives the relation between the features areal area pressure and motion pressure. The DFrCT of $H_{ap}(m)$ and $H_{dp}(m)$ is taken as the input and output of the fourth FIR system

$$H_{dp}(m) = \sum_{m=0}^{M} h_4(m) H_{ap}(K - m) \tag{3.16}$$

where, the $h_1(m)$, $h_2(m)$, $h_3(m)$, $h_4(m)$ are the impulse response of the FIR systems, here M is the order of the system $H_y(k)$, $H_v(k)$, $H_d(k)$, $H_{dp}(k)$ are approximations of $H_y(m), H_v(m), H_d(m), H_{dp}(m)$. By reducing the least-square at M the impulse response of $h_1(m)$, $h_2(m)$, $h_3(m)$, $h_4(m)$ can be calculated

$$E_1 = \sum_{K=0}^{M-1} \left[H_y(k) - H_y(\mathrm{K}) \right]^2 \tag{3.17}$$

$$E_2 = \sum_{K=0}^{M-1} \left[H_v(k) - H_v(\mathrm{K}) \right]^2 \tag{3.18}$$

$$E_3 = \sum_{K=0}^{M-1} \left[H_d(k) - H_d(\mathrm{K}) \right]^2 \tag{3.19}$$

$$E_4 = \sum_{K=0}^{M-1} \left[H_p(k) - H_p(\mathrm{K}) \right]^2 \tag{3.20}$$

3.5 SIGNATURE VERIFICATION

The four impulse responses obtained from the FIR system can be represented in the vector form [31]

$$h_1' = \left[h_1(0), h_2(0), h_3(0) \ldots\ldots\ldots\ldots h_1(m) \right] \tag{3.21}$$

$$h_2' = \left[h_1(0), h_2(0), h_3(0) \ldots\ldots\ldots\ldots h_1(m) \right] \tag{3.22}$$

$$h_3' = \left[h_1(0), h_2(0), h_3(0) \ldots\ldots\ldots\ldots h_1(m) \right] \tag{3.23}$$

$$h_4' = \left[h_1(0), h_2(0), h_3(0) \ldots\ldots\ldots\ldots h_1(m) \right] \tag{3.24}$$

Combining above impulse responses to form a single feature vector corresponding to a signature as in equation:

$$h' = \left[h_1' h_2' h_3' h_4' \right] \tag{3.25}$$

The Euclidean norm of feature vector of signature vector is compared with the Euclidean norm of the test signature. The difference value should be less than threshold of reference signature in genuine case and is given as:

$$\| h^{ref} - h \| > \eta \quad (3.26)$$

where, η is predefined threshold value. Euclidean norm is compared with this threshold to validate signatures.

3.6 FEATURES OF SIGNATURES

The extracted features of user 1 and user 2 are shown in Figures 3.12 and 3.13.

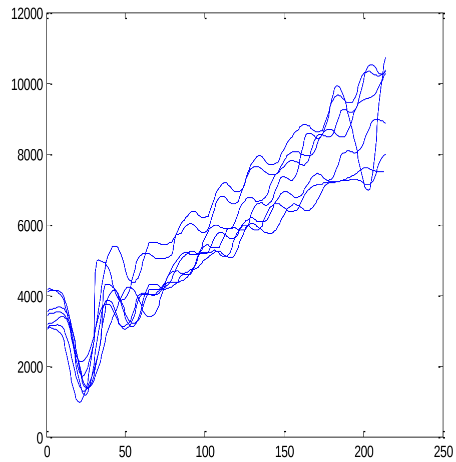
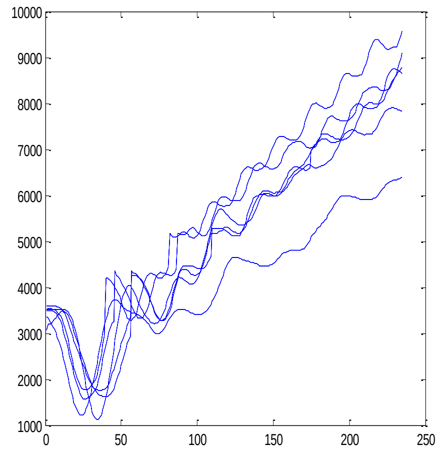
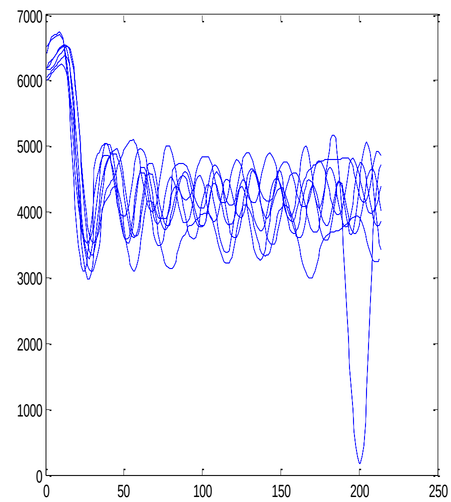
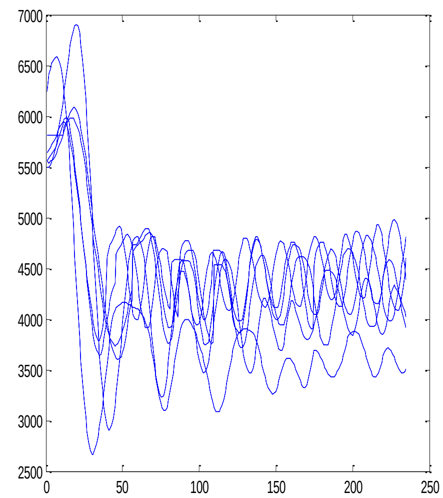
	Features of signature for user 1	
	Genuine signature	**Forgery signature**
Horizontal Component		
Vertical component		

Figure 3.12: Features of signature for user 1 (cont.)

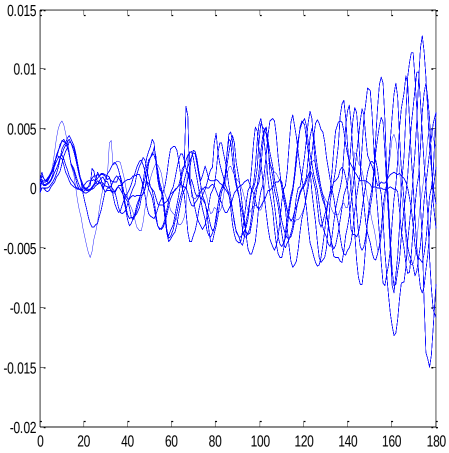
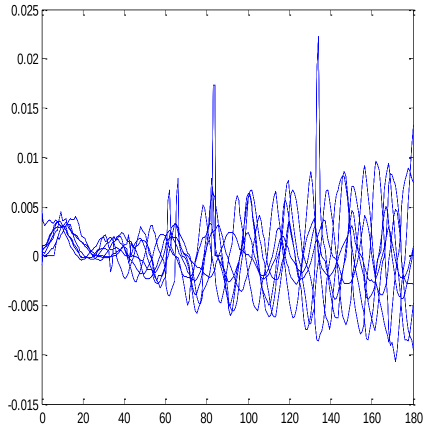
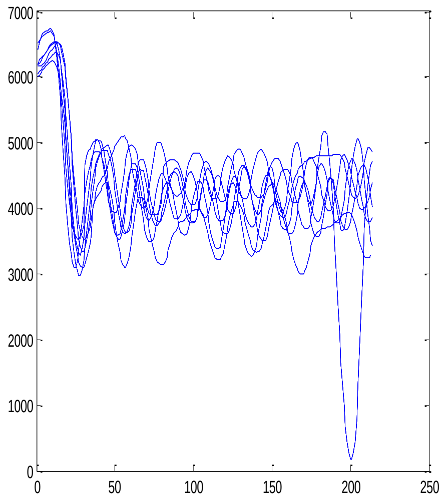
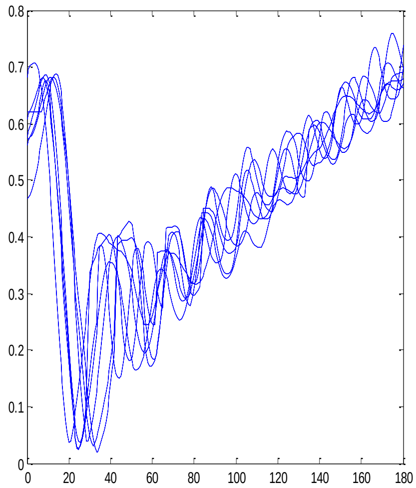
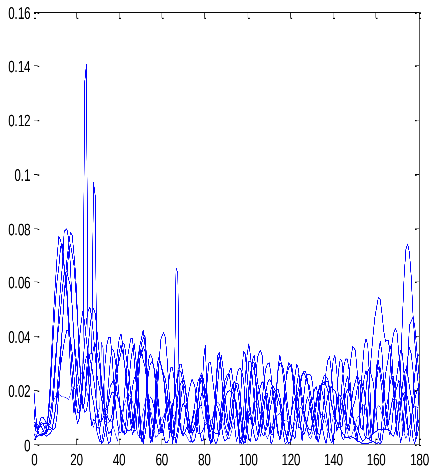
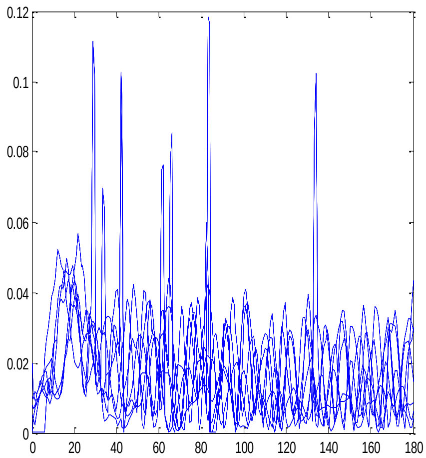
	Features of signature for user 1	
	Genuine signature	**Forgery signature**
Areal velocity		
Displacement		
Velocity		

Figure 3.12: Features of signature for user 1 (cont.)

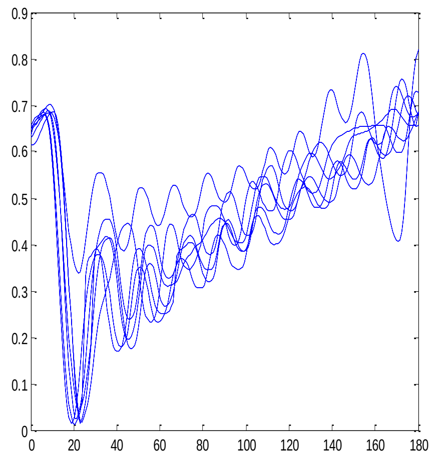
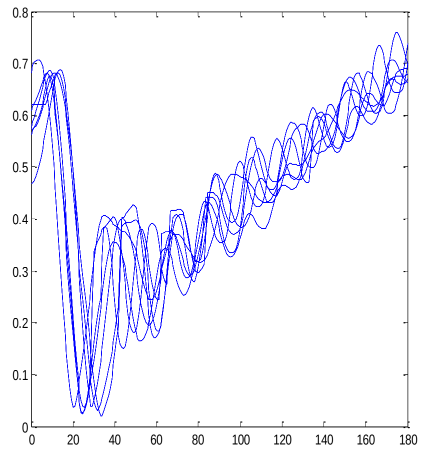
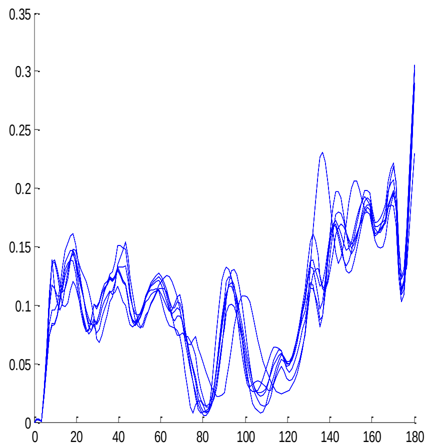
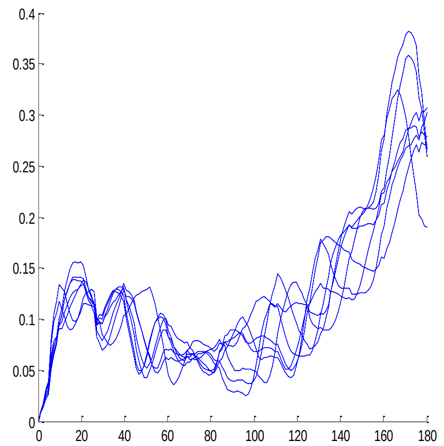
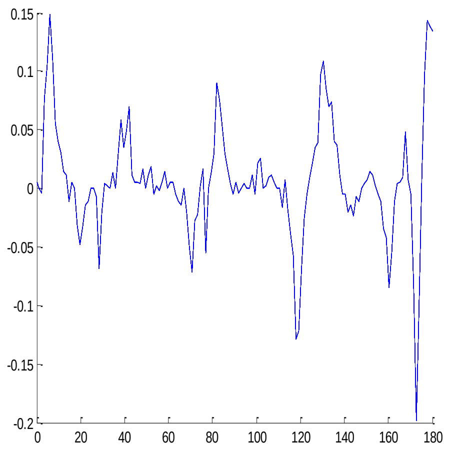
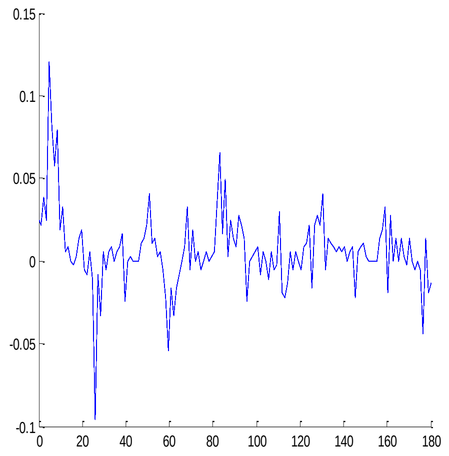
	Features of signature for user 1	
	Genuine signature	**Forgery signature**
Displacement		
Area pressure		
Motion Pressure		

Figure 3.12: Features of signature for user 1

From Figure 3.12 various features are extracted for user 1 it has been observed that genuine signatures are isolate from forgery signatures.

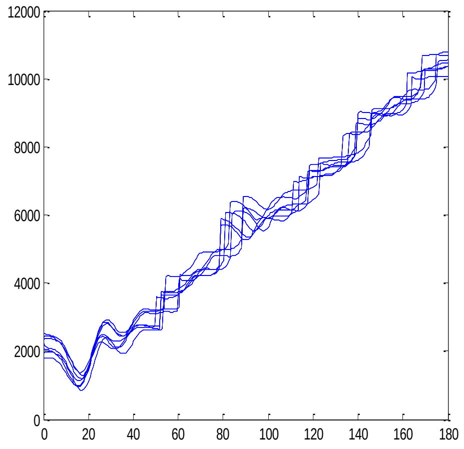
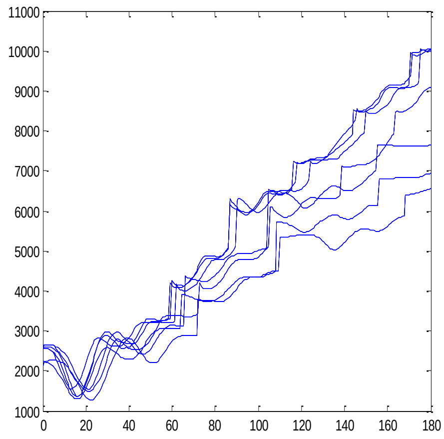
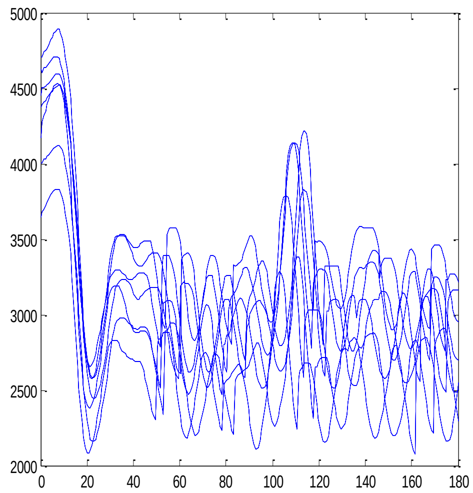
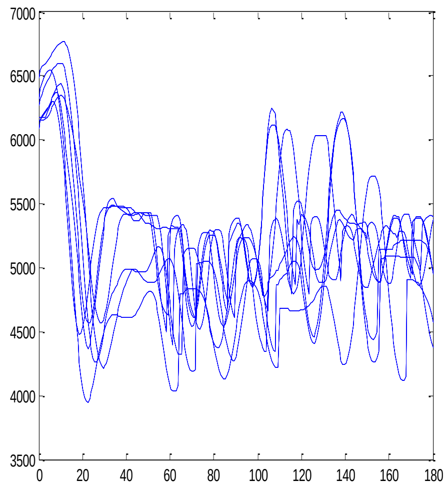
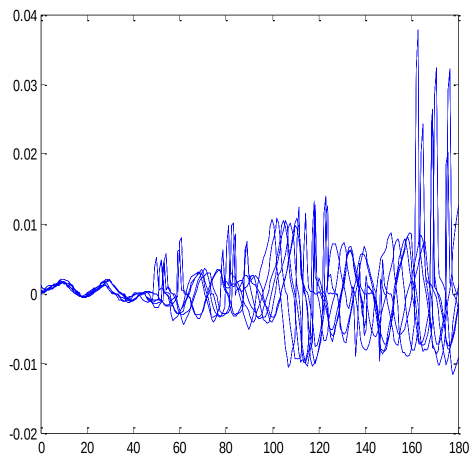
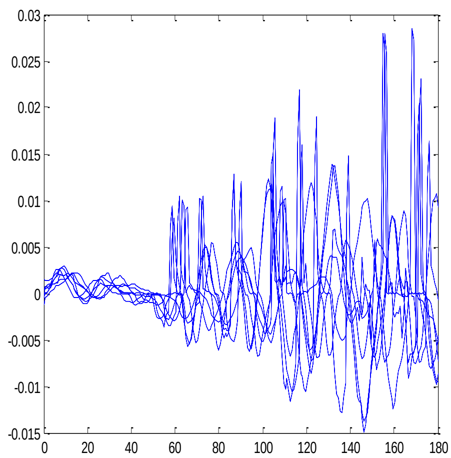
	Features of signature for user 2	
	Genuine signature	**Forgery signature**
Horizontal Component		
Vertical component		
Areal velocity		

Figure 3.13: Features of signature for user 2 (cont.)

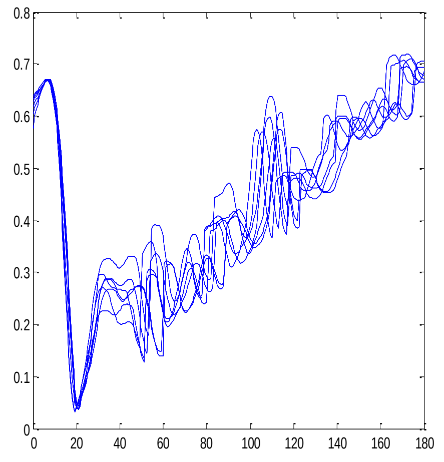
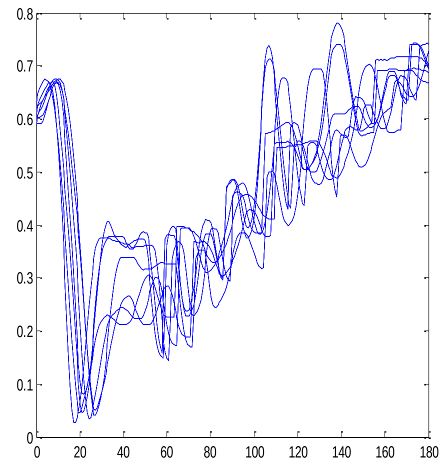
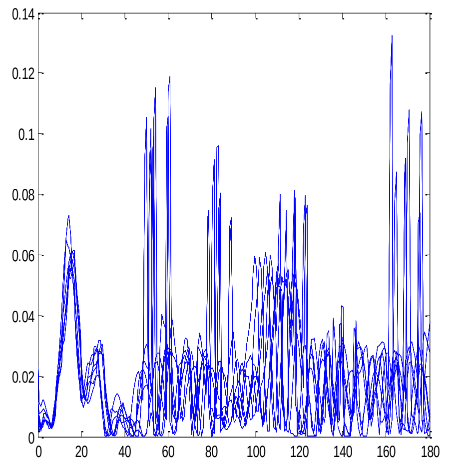
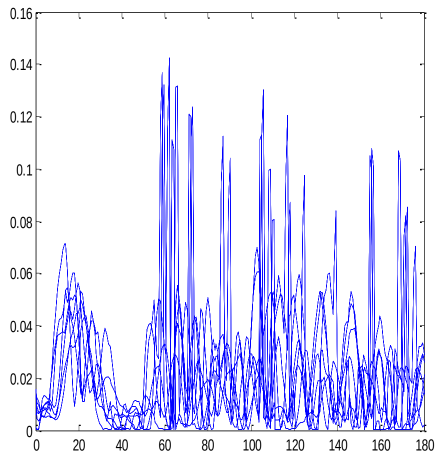
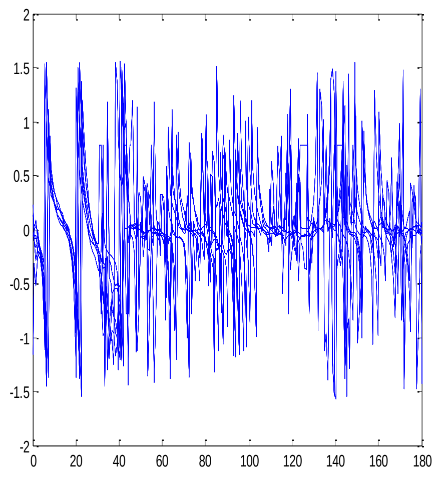
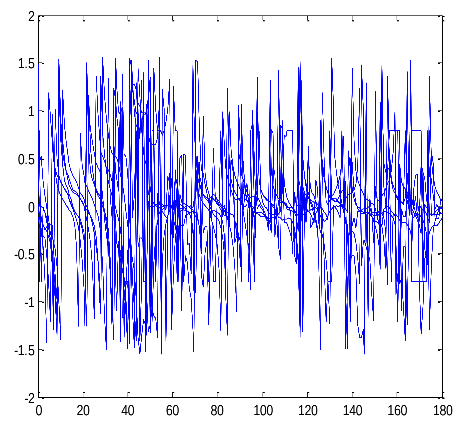
	Features of signature for user 2	
	Genuine signature	**Forgery signature**
Displacement		
Velocity		
Change in Direction		

Figure 3.13: Features of signature for user 2 (cont.)

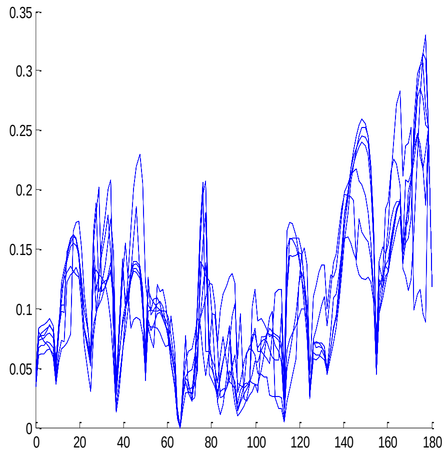
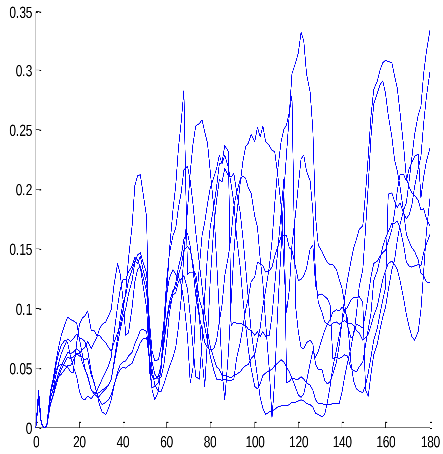
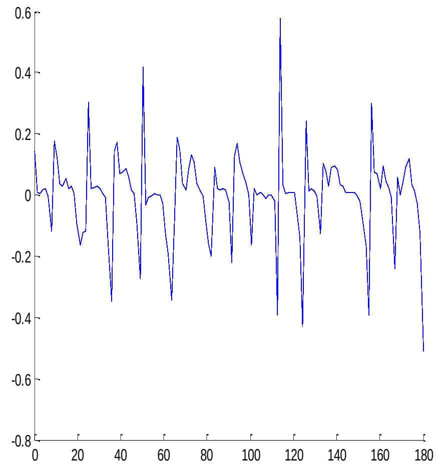
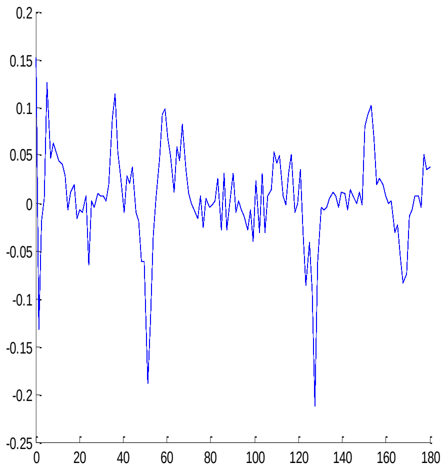
	Features of signature for user 2	
	Genuine signature	**Forgery signature**
Area pressure		
Motion Pressure		

Figure 3.13: Features of signature for user 2

From Figure 3.13 various features are extracted for user 2 it has been observed that genuine signatures are isolate from forgery signatures.

3.7 FEATURES OF SIGNATURES USING DFrCT

Figure 3.14 & Figure 3.15 shows the DFrCTs 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 signatures.

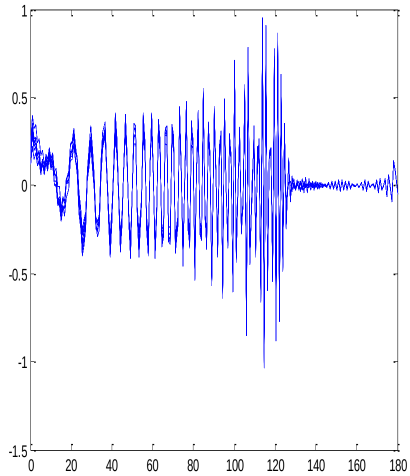
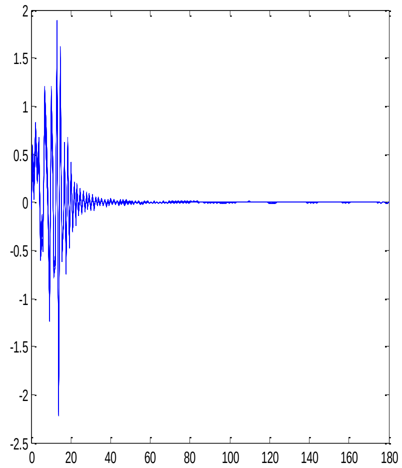
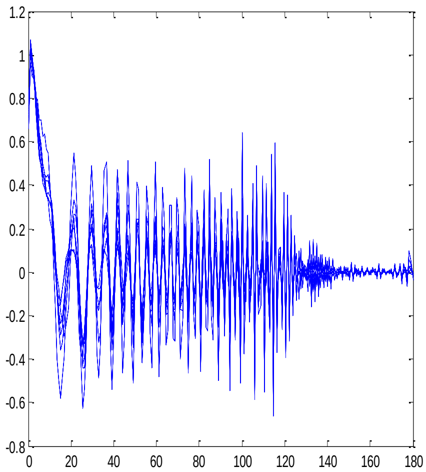
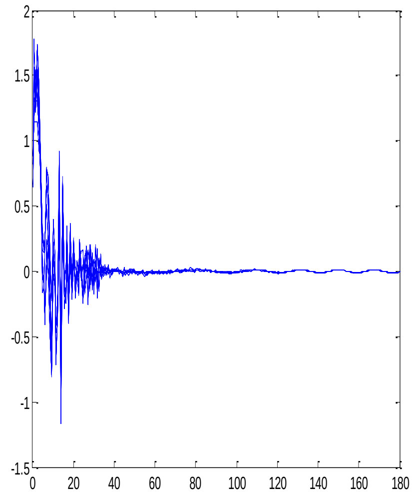
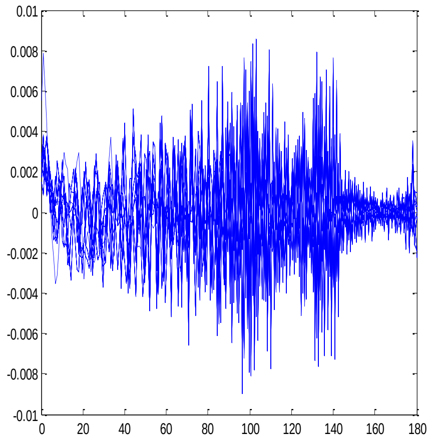
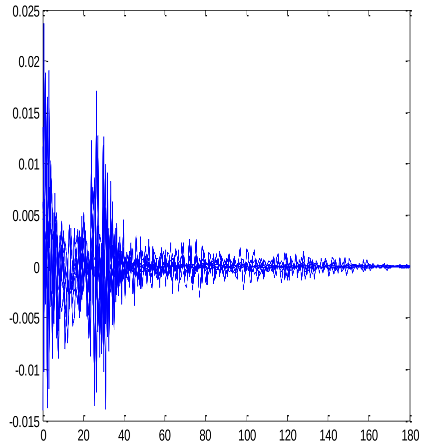
	Features of signature for user 1 using DFrCT	
	Genuine signature	**Forgery signature**
DFrCT of Horizontal Component		
DFrCT of Vertical component		
DFrCT of Areal velocity		

Figure 3.14: Features of signature using DFrCT for user 1 (cont.)

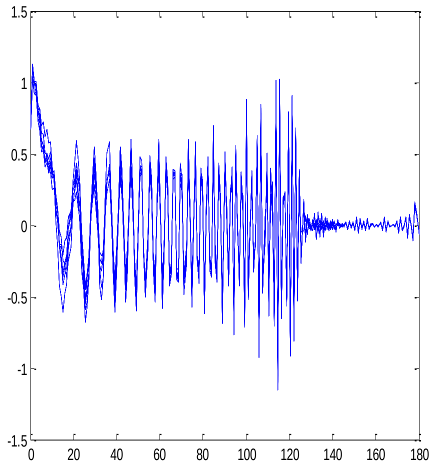
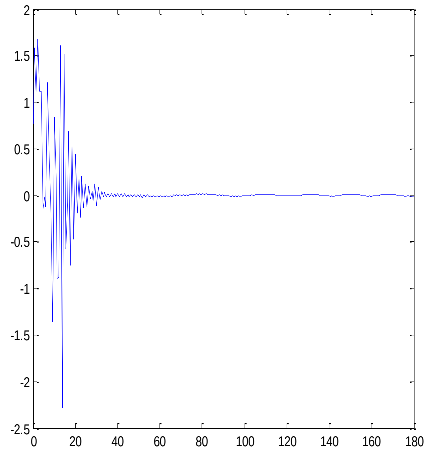
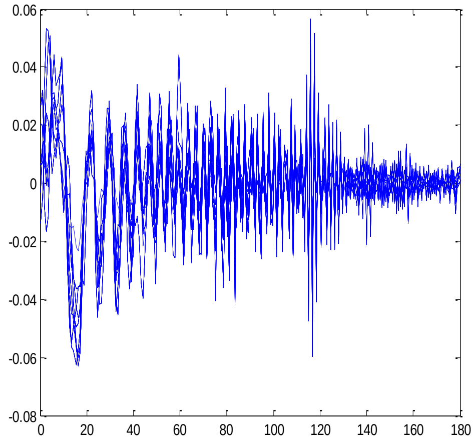
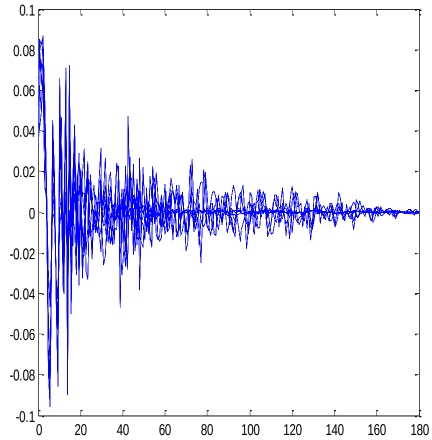
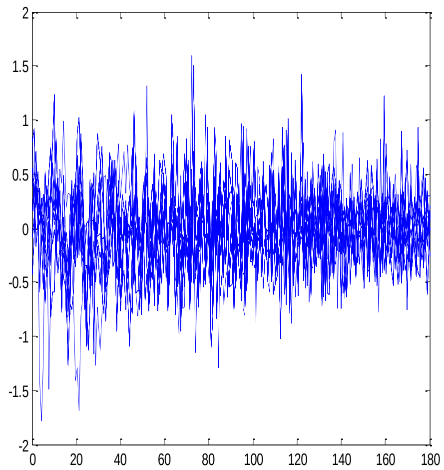
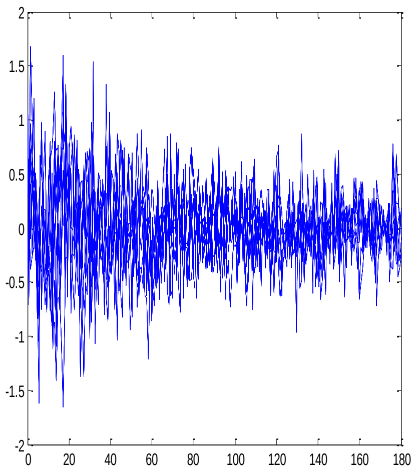
<table>
<tr><td></td><td colspan="2">Features of signature for user 1 using DFrCT</td></tr>
<tr><td></td><td>Genuine signature</td><td>Forgery signature</td></tr>
<tr><td>DFrCT of Displacement</td><td>
</td><td>
</td></tr>
<tr><td>DFrCT of Velocity</td><td>
</td><td>
</td></tr>
<tr><td>DFrCT of Change in Direction</td><td>
</td><td>
</td></tr>
</table>

Figure 3.14: Features of signature using DFrCT for user 1 (cont.)

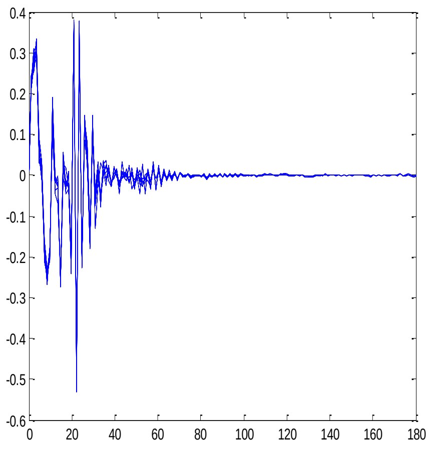
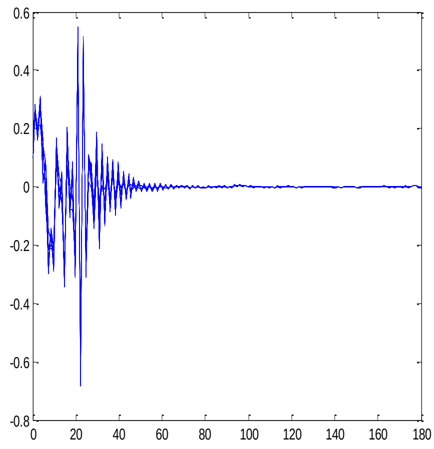
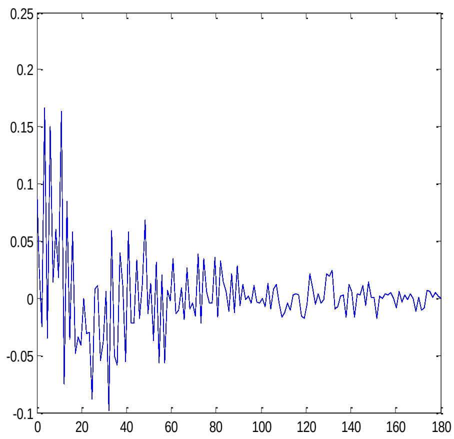
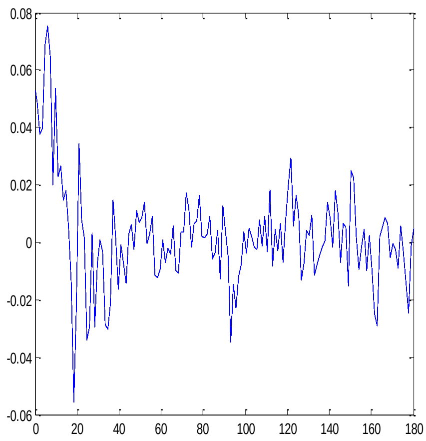
	Features of signature for user 1 using DFrCT	
	Genuine signature	**Forgery signature**
DFrCT of Area pressure		
DFrCT of Motion Pressure		

Figure 3.14: Features of signature using DFrCT for user 1

From Figure 3.14 various features are extracted for user 1 using DFrCT it has been observed that genuine signatures are isolating more properly from forgery signatures with different and optimize value of (α). The figure shows various features like horizontal movement of the signature, vertical movement of the signature, areal velocity, displacement, velocity, change in direction of the signature, area pressure and motion pressure. All the features are taken using different rotation angle for different features and the optimize value of α is taken by repeating the procedure until better results are achieved.

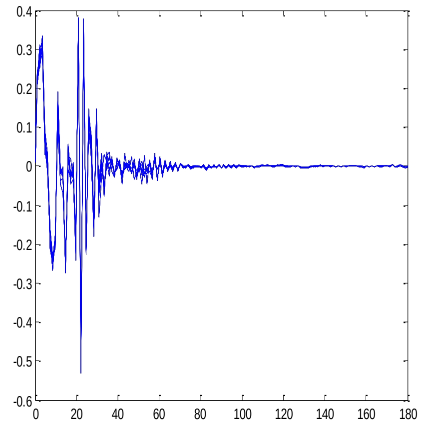
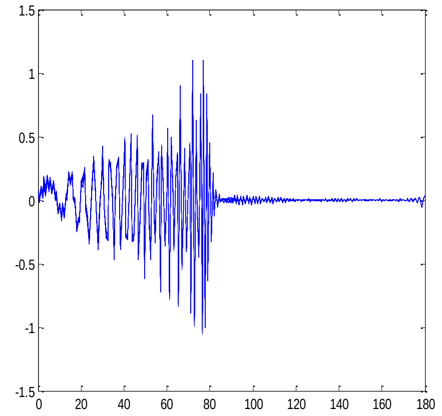
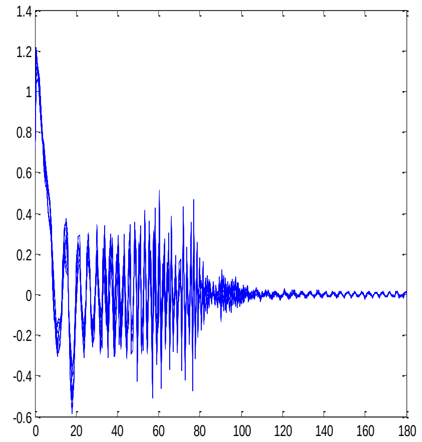
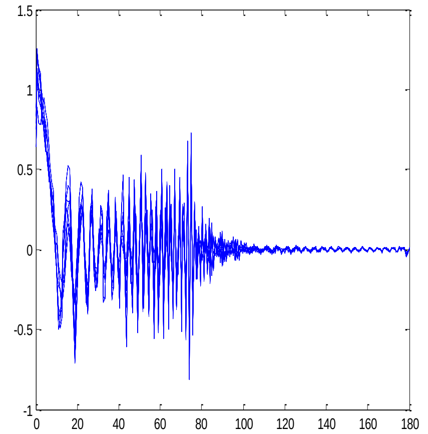
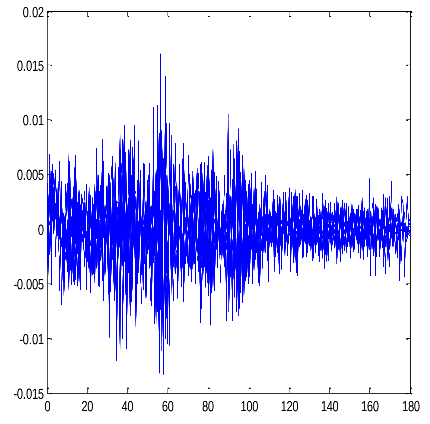
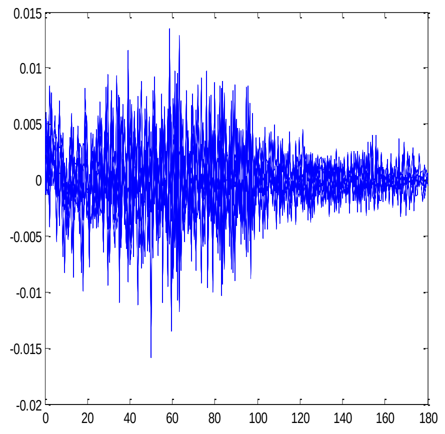
	Features of signature for user 2 using DFrCT	
	Genuine signature	**Forgery signature**
DFrCT of Horizontal component		
DFrCT of Vertical component		
DFrCT of Areal velocity		

Figure 3.15: Features of signature using DFrCT for user 2 (cont.)

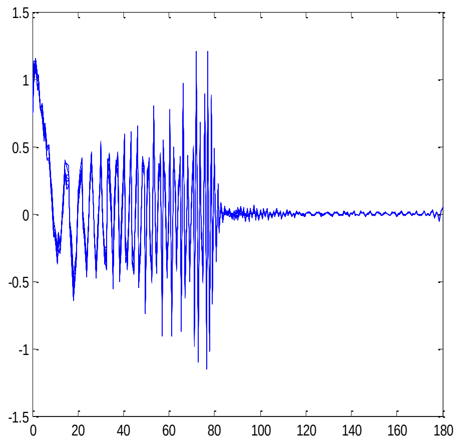
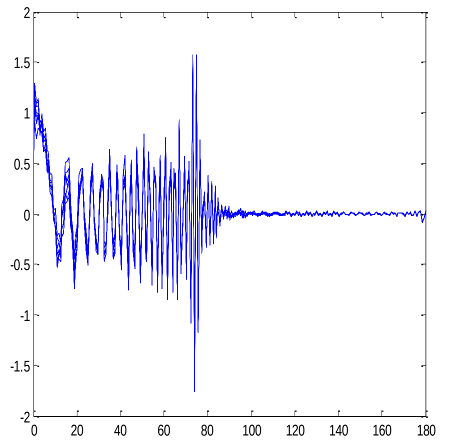
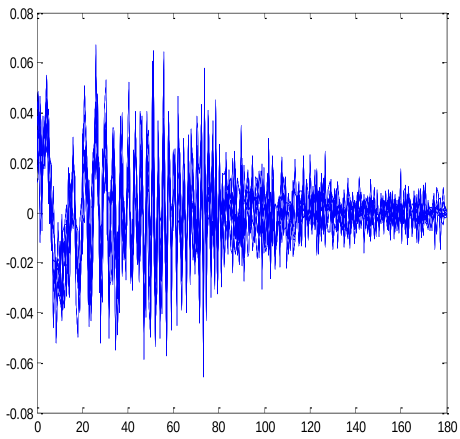
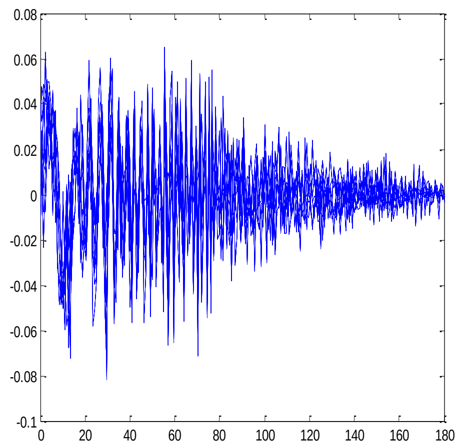
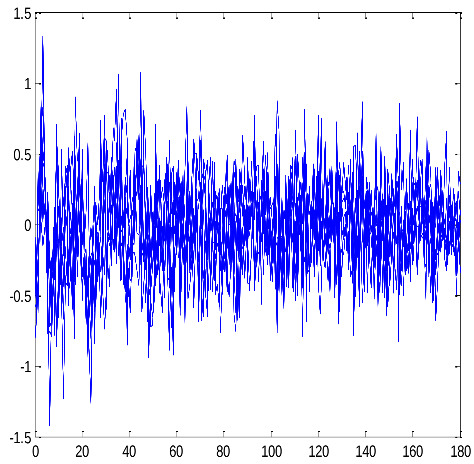
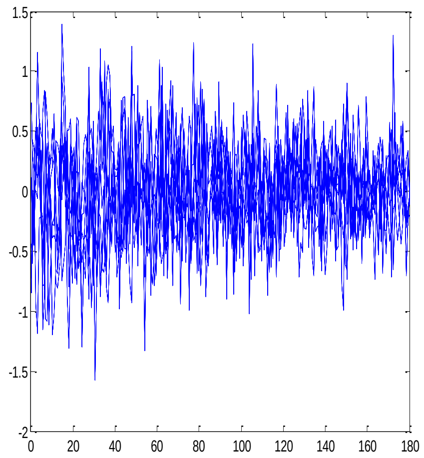
	Features of signature for user 2 using DFrCT	
	Genuine signature	**Forgery signature**
DFrCT of Displacement		
DFrCT of Velocity		
DFrCT of Change in Direction		

Figure 3.15: Features of signature using DFrCT for user 2 (cont.)

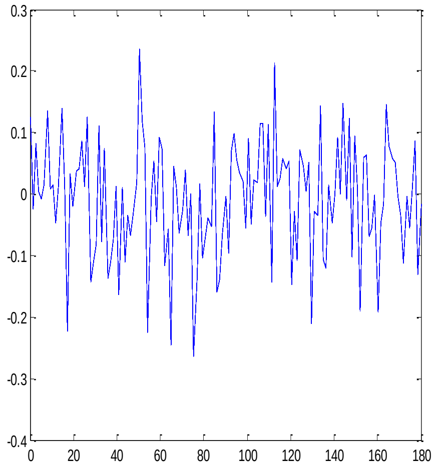
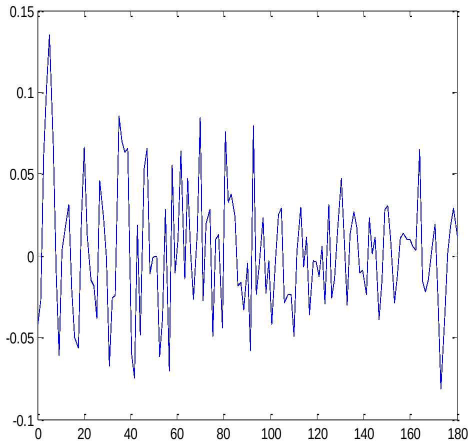
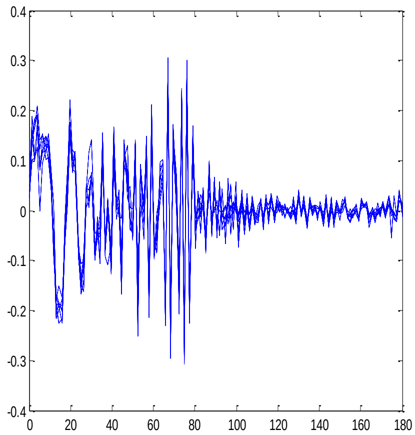
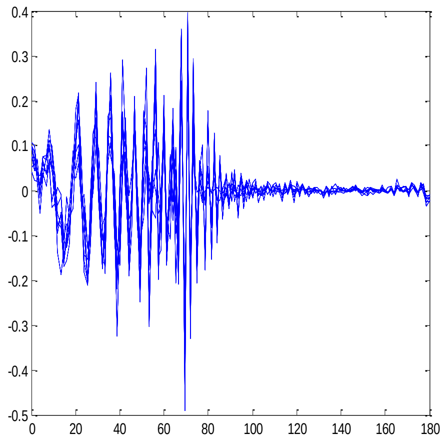
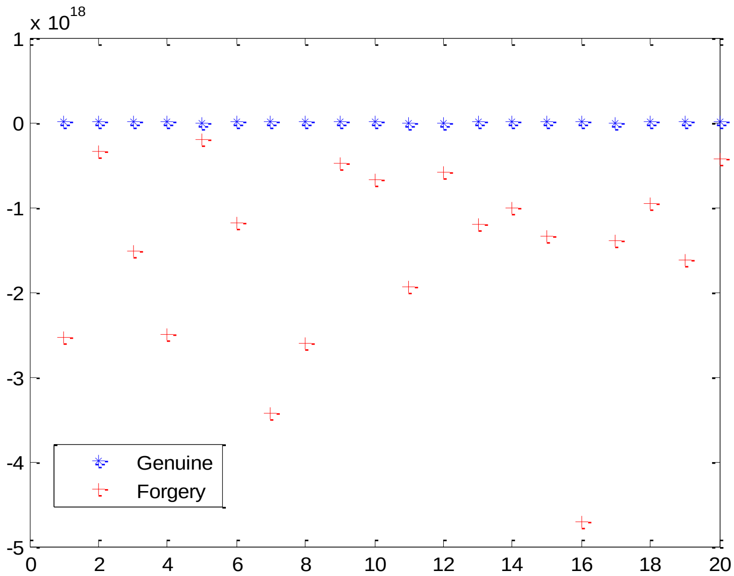
	Features of signature for user 2 using DFrCT	
	Genuine signature	**Forgery signature**
DFrCT of Motion Pressure		
DFrCT of Area pressure		

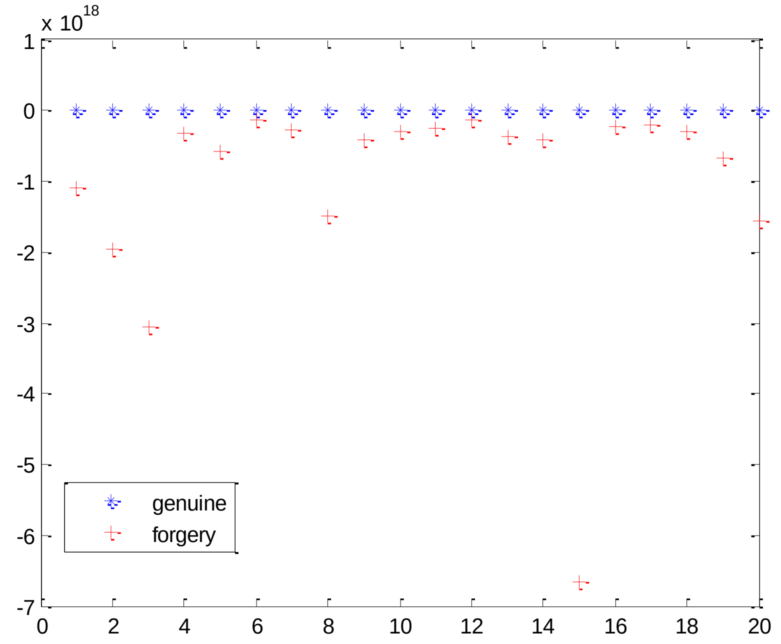
Figure 3.15: Features of signature using DFrCT for user 2

3.8 SIMULATIONS RESULTS FOR SIGNATURE VERIFICATION

The performance of signature verification systems is characteristically described with parameters; the false accept rate (FAR) and 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 interrelated, 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. The SVC2004 database was used in the experiment. Corresponding to each user there are twenty genuine signatures and twenty forgery signatures. In the experiment, five users were selected from the database. Thus, there were two hundred 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 five 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 with different and optimize value of α for all the features and by using four FIR filters to that of one using DFrCT for feature extractions same optimize α for all the features for signature verification. The evaluation criteria chosen 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. Figure 3.16 shows some examples of the plots of Euclidean norm of genuine signatures and forge signatures using DFrCT [31] for feature extraction for optimize (α) for all the features. Figure 3.17 shows some examples of the plots of Euclidean norm of genuine signature and forge signatures using DFrCT for its different and optimum values of (α) for all features. 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.

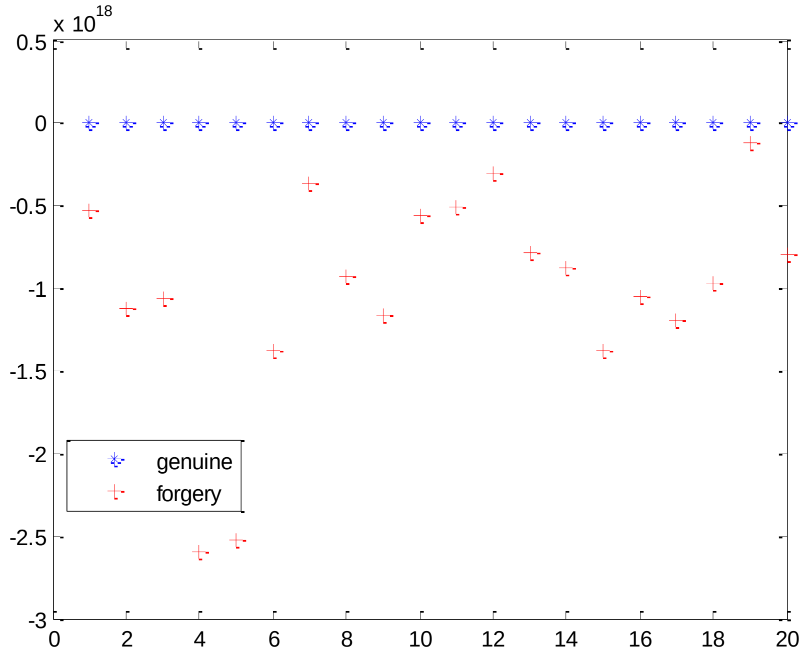


(a) Rotation angle (α) = 0.445

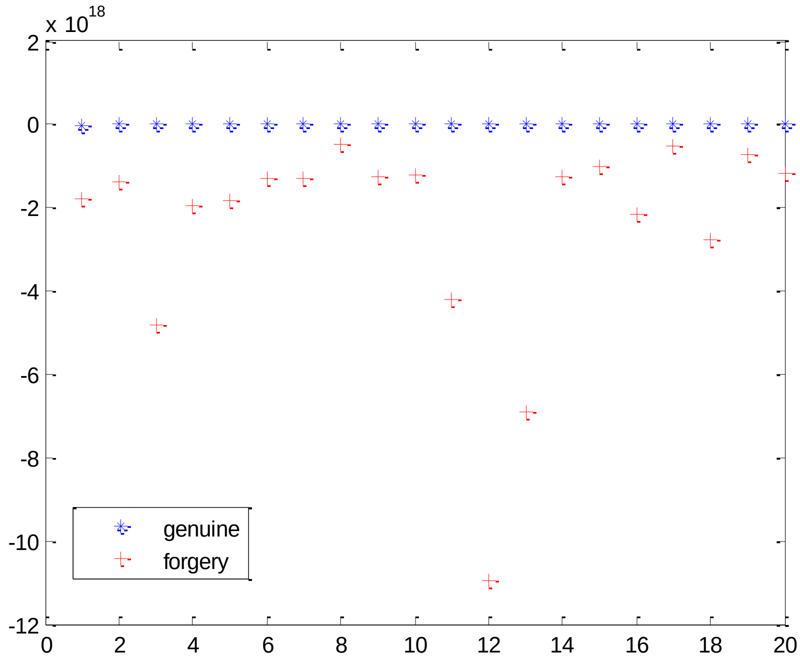


(b) Rotation angle (α) = 0.195

Figure 3.16: The plot of Euclidean Distances obtained for Genuine Signatures and Forgeries using DFrCT for (a) user 1 (b) user 2



(a) Rotation angle (α) = 0.655,0.389,0.478,0.345,0.256,0.545,0.964,0.562



(b) Rotation angle (α) = 0.656, 0.778, 0.545, 0.345, 0.845, 0.545, 0.889, 0.755

Figure 3.17: The plot of Euclidean Distances obtained for Genuine Signatures and Forgeries signatures using DFrCT with different and optimize α [Present work] for (a) user 1 (b) user 2

From Figures 3.17 it is observed that there is more distance between genuine and forgery signatures then in Figures 3.16 [31] and more the separation lesser will be the EER and lesser will be the results better are the results achieved.

3.8.1 Analysis of System Using DFrCT

Table 3.1 shows the difference between the Euclidean norm of test signature and the Euclidean norm of the reference signature corresponding to optimal values of α [31]. The optimized α is achieved by varying it in between 0 and 1 and repeating the algorithm until a minimum EER is achieved. Here, single value of α is taken for all the parameters like for user 1 the value of α is 0.76. Table 3.2 shows number of false accepted and false rejected signatures corresponding to various threshold levels. Table 3.3 shows the FAR and FRR corresponding to various threshold levels and these FAR and FRR are used to calculate EER for the signatures and lesser the EER better will be the results.

Table 3.1: Difference of Euclidean Norm of Reference and Test Signature Using DFrCT method

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

Table 3.2: Number of False Accepted and Rejected Signatures Corresponding to each user for Various Threshold Levels using DFrCT method

THRESHOLD	USER 1		THRESHOLD	USER 2		THRESHOLD	USER 3		THRESHOLD	USER 4		THRESHOLD	USER 5		TOTAL	
	FA	FR		FA	FR		FA	FR		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	-0.8192	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

Table 3.3: False Accept Rate and False Reject Rate using DFrCT method

THRESHOLD LEVEL	FALSE ACCEPT RATE (FAR)%	FALSE REJECT RATE (FRR)%
1	2.5	9
2	3.5	6
3	5	4.5

When using same optimize alpha for all the features a min. FAR of 2.5% is achieved where max. FAR is 5% and min. FRR is 4.5% and max. FRR is 9% is achieved and EER is of 5% is achieved. EER is calculated by taking firstly the percentage of FAR and FRR and the value of EER is calculated where the FAR and FRR are approximately same. So in Table FAR and FRR is approximately same on 3 no. so we take maximum value as our EER.

3.8.2 Analysis of System using Improved DFrCT Method

Table 3.4 shows the difference between the Euclidean norm of test signature and the Euclidean norm of the reference signature corresponding to optimal values of α different for different features, which is achieved by varying this factor in between 0 and 1 and repeating the algorithm until a minimum EER is achieved. Table 3.5 shows number of false accepted and false rejected signatures corresponding to various threshold levels. Table 3.6 shows the FAR and FRR corresponding to various threshold levels. The different value of α for different features is for user 1 α for horizontal movement is 0.655, for vertical direction α is 0.389, for areal velocity α is 0.478, for displacement α is 0.345, for velocity α is 0.256, for change in direction α is 0.545, for area pressure α is 0.964 and for motion pressure α is 0.562. These are the values of α for various features for user 1 for other users the values of α are given in the Table 3.4. Various values of Euclidean norm for test signatures and Euclidean norm of reference signatures are calculated a threshold is set from the test signatures and compare it with the test signatures to get FAR and FRR and these FAR and FRR are used to calculate EER for the signatures and lesser the EER better will be the results.

Table 3.4: Difference of Euclidean Norm of Reference and Test Signature using improved DFrCT method

user 1 optimum α = 0.655,0.389,0.478,0.345,0.256,0.545,0.964,0.562)		user 2 optimum α = 0.656,0.778,0.545,0.345,0.845,0.545,0.889,0.755)		user 3 optimum α = 0.682,0.658,0.845,0.656,0.545,0.778,0.889,0.755)		user 4 optimum α = 0.382,0.658,0.845,0.656,0.764,0.778,0.857,0.452)		user 5 optimum α = 0.455,0.389,0.478,0.545,0.256,0.345,0.264,0.621)	
Genuine	**Forgery**	**Genuine**	**Forgery**	**Genuine**	**Forgery**	**Genuine**	**Forgery**	**Genuine**	**Forgery**
0.5579	-0.5926	0.3961	-2.9729	0.0891	-0.5941	1.3918	-1.3776	0.6859	-0.9364
0.5735	-0.9791	-2.0495	-2.8301	0.1128	-0.3231	1.2112	-4.1415	0.755	-2.5099
0.3435	-2.6932	-0.36	-1.4651	0.1127	-0.2595	-1.9126	-0.222	0.7605	-0.3793
0.0479	-1.3433	0.4477	-0.9331	0.4113	-0.4085	1.5277	-4.6914	0.718	-1.5532
6.7799	-3.1699	0.4363	-0.4208	0.111	-0.2234	1.5379	-1.1476	0.7604	-0.13
-0.5924	-1.9493	0.5601	-2.1791	0.0996	-1.5057	1.5404	-0.7321	-0.0807	-0.8319
0.4593	-8.2102	-3.1115	-0.473	0.1122	-0.3513	1.5414	-0.3986	-6.479	-0.5219
0.3005	-4.4139	-1.1034	-0.9647	0.1111	-0.4848	1.5313	-1.2057	0.7599	-0.1839
0.5938	-1.3167	-0.2196	-1.1429	0.1129	-0.4965	-8.3266	-1.3813	0.716	-0.6182
0.5722	-2.1194	0.6929	-1.2579	0.7028	-0.4169	-0.3466	-5.4325	0.7573	-1.3195
0.4983	-1.7541	0.6402	-1.1164	0.0996	-1.4258	-1.2189	-1.4481	0.7417	-1.1306
0.4686	-2.8248	0.6249	-0.9249	0.0811	-1.2755	1.5378	-1.342	0.76	-2.3978
1.1821	-1.4538	-0.3782	-1.9457	0.1036	-2.3682	1.324	-3.2573	0.7054	-3.8393
0.3248	-1.234	0.6097	-1.0295	0.111	-1.3191	0.9259	-6.683	0.7216	-7.3975
0.4814	-2.359	0.6265	-3.5121	0.0856	-1.0026	0.9188	-2.6439	0.7605	-1.5992
0.4596	-4.0608	0.6194	-1.2652	0.1089	-0.2378	15387	-2.3217	0.7605	-0.1368
0.5472	-1.2288	0.585	-0.6783	0.1088	-2.0094	1.5401	-1.2867	0.7488	-0.4034
0.4998	-7.4873	0.7413	-4.8308	-1.9969	-0.5689	-2.2888	-1.7715	0.7599	-4.8198
0.4757	-1.0128	-0.0129	-1.1242	0.113	-1.0718	-5.4617	-0.5586	0.7062	-0.6794
-0.0139	-7.5903	0.255	-0.5898	0.1098	-0.1649	1.4881	-1.1592	-6.0183	-1.0884

Table 3.5: Number of False Accepted and Rejected Signatures Corresponding to Each User for Various Threshold Levels using improved DFrCT method

THRESHOLD	USER 1		THRESHOLD	USER 2		THRESHOLD	USER 3		THRESHOLD	USER 4		THRESHOLD	USER 5		TOTAL	
	FA	FR		FA	FR		FA	FR		FA	FR		FA	FR		
0.5722	0	2	0.7413	2	2	0.7028	1	2	1.5414	0	2	0.7605	0	2	3	10
0.5579	0	1	0.6194	1	1	0.1122	1	1	1.3918	2	1	0.7417	2	2	7	6
0.4983	1	0	0.5601	2	1	-1.997	0	2	0.9259	2	1	0.7216	1	0	6	4

Table 3.6: False Accept Rate and False Reject Rate using improved DFrCT method

THRESHOLD LEVEL	FALSE ACCEPT RATE (FAR)%	FALSE REJECT RATE (FRR)%
1	1.5	5
2	3.5	3
3	3	2

When using different optimize alpha for all the features a min. FAR of 1.5% is achieved where max. FAR is 3.5% and min. FRR is 2% and max. FRR is 5% is achieved and EER of 3.5% is achieved. Also from the above results and analysis it is observed that an EER of 3.5% was achieved with the use of DFrCT with different and optimize α as compare to EER of 5% when DFrCT for same optimize α was used for feature extraction. Hence it can be say that DFrCT with its free parameter α different for different features provides a better option for features extraction for signature verification system as compare to the one extracted by using DFrCT with same α.

Table 3.7: Comparison of online signature verification (presented work) and existing algorithms

Parameters	DCT [48]	DFrCT [31]	Proposed work
Min. FAR %	5.5%	2.5%	1.5%
Max. FAR%	15.5%	5%	3.5%
Min. FRR%	5%	4.5%	2%
Max. FRR%	12.5%	9%	5%
EER%	10.5%	5%	3.5%
Features Extracted	6	6	8
FIR Filter used	3	3	4
Rotation angle (α)	Not used	Same for different features	Different for different features

3.9 SUMMARY

The presented algorithm block diagram for online signature verification system and simulation results have been given in this chapter. The presented algorithm includes four main steps: preprocessing, feature extraction, DFrCT implementation and threshold calculation. Finally, performance of the implemented technique is measured by EER for different values of free parameter. With the present technique min. FAR is 1.5% and min. FRR is 2% and EER is 3.5% is achieved. In the next chapter conclusion and future scope has been discussed.

4.1 CONCLUSION

The present research work is online signature verification used for personal authentication. Signature samples were captured using WACOM Intuos 2A6 tablet and stored in SVC 2004 database. Corresponding to each user, 40 signatures were used out of which 20 signatures were genuine and 20 were forgery. These signatures were pre-processed by normalizing the size, location and trajectory of barycenter in order to remove the fluctuations in the signature. After pre-processing, the features horizontal pen movement, vertical pen movement, areal velocity, displacement from trajectory of barycenter, magnitude of velocity, change of angle of trajectory of barycenter, area pressure and motion pressure were extracted. Then DFrCT of these signatures was carried out with the use of different values of optimize free parameter (α) for each feature. Impulse responses of four FIR filters were calculated and combined to form a feature vector. Euclidean of this vector was calculated to set the threshold level. To verify a given signature, threshold level of the signature was compared to the reference signature. To measure the performance of the present technique EER, FAR and FRR were calculated. The value of minimum EER 3.5% has been achieved which is 1.5% improvement than the existing method. The existing method has extracted six features and used three FIR filters. The minimum FAR 1.5% and minimum FRR 2% has been calculated in the present technique. The improvement of 1% in. FAR and 2.5% in FRR is also achieved in the presented technique. The complexity of present work increased by extracting eight features and using four FIR system.

The use of different value of optimized free parameter (α) for each feature has also increased the security in comparison of existing system. The existing method has used same optimize free parameter (α) for all six features.

4.2 FUTURE SCOPE

The fractional order (α) has been optimized for eight features individually. In future, it will be in interest of research to consider more number of feature such as altitude, azimuth and Button status etc. to get better results.

REFERENCES

[1] A. K. Jain, F. D. Griess and S. D. Connell, “Online Signature Verification,” *Pattern Recognition*, vol. 35, no. 12, pp. 2963-2972, 2002.

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

[3] 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.

[4] 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.

[5] B. Schafer and S. Viriri, “An Offline Signature Verification System,” in Proc. *International Conference on Signal and Image Processing Applications*, pp. 95-100, 2009.

[6] C. C. Hsu, L. F. Chen, P. C. Chang and B. S. Jeng, “Online signature verification based on Multi expert strategy”, in Proc. *thirty Second Annual International Carnahen Conference on Security Technology*, pp.169-173, 1998.

[7] C. Candan, M. A. Kutay and H. M. Ozaktas, “The Discrete Fractional Fourier Transform”, *IEEE Trans. on Signal Process*, vol. 48, no.5, pp.1329-1337, 2000.

[8] 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.

[9] C. Gruber, T. Gruber, S. Krinninger and B. Sick, “Online signature verification with support vector machine based on LCSS kernel function”, *IEEE Trans. on System, Man and Cybernetics*, vol. 40, no. 4, pp. 1088-1100, 2010.

[10] C. J. C. Burges, “A Tutorial on Support Vector Machines for Pattern Recognition,” *Data Mining Knowledge Discover*, vol. 2, pp. 121-167, 1998.

[11] 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.

[12] C. Schmidt and K. E. Kraiss, “Establishment of Personalized Templates for Automatic Signature Verification,” in Proc. *fourth International Conference on Document Analysis and Recognition*, vol.1, pp. 263-267, 1997.

[13] D. Impedovo and G. Pirlo, “Automatic Signature Verification System: The State of the Art”, *IEEE Trans. on Systems, Man and Cybernetics, Part-C*, vol. 38, no. 5, pp. 609 - 635, 2008.

[14] D. Muramatsu, K. Yasuda and T. Matsumoto, “Biometric Person Authentication Method Using Camera-Based Online Signature Acquisition,” in Proc. *tenth International Conference on Document Analysis and Recognition*, pp. 46-50, 2009.

[15] D. Muramatsu, M. Kanda, M. Sasaki, S. Tachibana and T. Matasumoto, “A Markov chain Monte Carlo Algorithm for Bayesian dynamic signature verification”, *IEEE Trans. on Information Forensic and Security*, vol. 1, no. 1, pp. 22-34, 2006.

[16] D. Y. Yeung, “SVC2004: First International Signature Verification Competition,” in Proc. *on Biometric Authentication*, pp. 16-22, 2004.

[17] E. A. Rau and J. L. A. Castro, “Online signature based on Generative Model,” *IEEE Trans. on system, Man and Cybernetics*, vol. 42, no. 4, pp. 1231-1242, 2012.

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

[19] E. Maiorana, P. Campisi, J. Fierrez and J. O. Garcia, “Cancellable Template for sequence base Biometric with Application to Online signature Recognition”, *IEEE Trans. on Systems, Man, And Cybernetics, Part A: Systems and Humans*, vol. 40, no. 3, 2010.

[20] E. Orzgunduz, T. Senturk and M. E. Karsligil, “Offline Signature Verification and Recognition by Support Vector Machine,” in Proc. *thirteenth European Signal Processing Conference on Vector Machine, EUSPICO*, 2005.

[21] G. Dimauro, S. Impedovo and G. Pirlo, "Online Signature Verification by a Dynamic Segmentation Technique," in Proc. *third International Workshop on Front. Handwriting Recognition* (*IWFHR-3), Buffalo, NY,* pp. 262-271, 1993.

[22] 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.

[23] 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.

[24] I. S. I. Abuhaiba, "Offline Signature Verification Using Graph Matching," *Journal of Electric Engineering and Computer Science*, vol. 15, no. 1, pp. 89-104, 2007.

[25] K. Huang and H. Yan, "Offline Signature Verification Using Structural Feature Correspondence," *Pattern Recognition*, vol.35, no.11, pp. 2467-2477, 2002.

[26] K. W. Boyer, V. Govindaraju and N. K. Ratha, Eds, "Special Issue on Recent Advances in Biometric Systems", *IEEE Trans. on Systems, Man and Cybernetics Part-B,* vol. 37, no. 5, pp. 1091-1095, 2007.

[27] L. B. Almeida, "The Fractional Fourier Transform and Time-Frequency Representation", *IEEE Trans. on Signal Processing,* vol. 42, no. 11, pp. 3084-3091, 1994.

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

[29] 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.

[30] L. R. Rabiner and B. H. Juang, "An Introduction to Hidden Markov Models," *IEEE ASSP Magazine,* vol. 3, no.1, pp. 4-16, 1986.

[31] M. Arora, K. Singh and G. Mander, “Discrete Fractional Cosine Transform based Online Handwritten Signature Verification,” *Recent Advances in Engineering and Computational Sciences*, pp. 1-6, 2014.

[32] M. J. Paulik, N.M. Krishan and M. Nikiforuk, “A time varying Autogression model for signature verification,” in proc. *thirty seventh Midwest Symposium on Circuits and Systems*, pp. 1395-1398, 1995.

[33] M. L. Garcia, R. R. Lara, M. Hurtado and E. C. Navarro, “Embedded system for Biometric online signature verification”, *IEEE Trans. of Industrial Informatics*, vol. 10, no. 1, pp. 491-501, 2014.

[34] N. S. Bae and N. Memon, “Online signature verification on mobile devices”, *IEEE Trans. of Information Forensic and Security*, vol. 9, no. 6, pp. 933-947, 2014.

[35] N. S. Kamel, S. Sayeed and G. A. Ellis, “Glove based approach to online signature verification”, *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 30, no. 30, pp. 1109-1113, 2008.

[36] O. M. Hurtado, “Online Signature Verification Algorithms and Development of Signature International Standards,” Ph.D. Dissertation, University of Carlos III, 2001.

[37] 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.

[38] R. Martens and L. Claesen, “Online signature verification by Dynamic Time wraping,” in Proc. *thirteenth International Conference on Pattern Recognition*, pp. 38-42, 2003.

[39] R. Martens and L. Claesen, “Online Signature Verification by Dynamic Time Warping,” in Proc. *third International Conference on Pattern Recognition*, pp. 38-42, 1996.

[40] R. Martens and L. Claesen, “Online signature verification,” in Proc. *fourth International Conference on Pattern Recognition* , vol. 4, pp. 657-660, 1997.

[41] 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.

[42] S. C. Pei and J. J. Ding, “Closed-Form Discrete Fractional and Affine Fourier Transforms”, *IEEE Trans. on Signal Processing*,vol.48, no.5, pp. 1338-1353, 2000.

[43] S. C. Pei and M. H. Yeh, “A Method for the Discrete Fractional Fourier Transform Computation,” *IEEE International Symposium on Circuits and Systems*, vol. 51, no. 3, pp. 889-891, 2003.

[44] S.Emerich, E.Lupu and C. Rusu, “Online Signature Recognition Approach Based on Wavelets and Support Vector Machines,” in Proc. *Int. Conference on Automation Quality and Testing Robotics*, pp. 1-4, 2010.

[45] T. Alieva and M. J. Bastiaans, “Fractional Cosine and Sine Transforms in Relation to the Fourier and Hartley Transforms,” in Proc. *seventh International Symposium on Signal Processing and its Applications*, pp. 561-564, 2003.

[46] T. H. Rhee, S. J. Cho and J. H. Kim, “Online Signature Verification Using Model 79 Guided Segmentation And Discriminative Feature Selection For Skilled Forgeries,” in Proc. *sixth International Conference on Document Analysis and Recognition*, Seattle, WA, pp. 645–649,2001.

[47] T. Matsumoto and D. Muramatsu, “Effectiveness of Pen Pressure, Azimuth, and Altitude Features for Online Signature Verification,” in Proc. *Springer-Verlag Berlin Heidelberg on Advances in Biometrics International Conference* LNCS, pp. 503-512, 2003.

[48] T. Matsuura, J. Pemwong, N. Wakayaphattaramanus, and P. Thumwarin. “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.

[49] T. Matsuura and S. Okamura, “On FIR Filter for Signature Verification,” in Proc. *thirty Eight Midwest Symposium on Circuits and Systems*,vol.1,pp. 366-369, 1996.

[50] 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.

[51] V. S. Nalwa, “Automatic online signature verification,” in Proc. *of IEEE AT and T Bell Labs, Holmdel, NJ, USA*, vol. 85, no. 2, pp. 215-239, 1997.

[52] W. L. Hsue and S. C. Pei, “Random Discrete Fractional Fourier Transform,” *IEEE Signal Processing letters*, vol. 16, no. 12, pp. 1015-1018, 2009.

[53] Y. Chen and X. Ding, “Online Signature Verification Using Direction Sequence String Matching,” in Proc. *second International Conference on Image and Graphics*, pp. 744-749, 2002.

[54] 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.

[55] Y. Xuhua, T. Furuhashi, K. Obata and Y. Uchikawa. “A Study on Signature Verification Using a New Approach to Generic Based Machine Learning”, *IEEE Trans. on Systems, Man and Cybernetics Intelligence System 21st Century*, vol. 5, pp. 4383-4386, 1995.

[56] Y. Yang and L .Qi. “Study on the Algorithm of the Fractional Cosine Transform Based on Adaptive LMS Algorithm.” in Proc. *ninth International Conference on Signal Processing*, pp. 100-103,2008.

LIST OF PUBLICATION

[1] S. Mantrao and K. Singh, "Improved Online Signature Verification System using Discrete Fractional Cosine Transform," Communicated to International Journal of Electronics, Taylor and Francis.