Distance Based Online Signature Verification with Enhanced Security

[1] Harshdeep Kaur,[2] Er. Rajnish Kansal
[1]Research Scholar,[2]Assistant Professor
[1]CSE Department
[1,2] Asra College of Engineering and Technology Sangrur (Pb.) India

Abstract: Handwritten signature is the most widely accepted biometric to identity verification. There is considerable interest in authentication based on online signature verification system as it is the cheapest way to authenticate a person. The proposed online handwritten signature verification system consists mainly of three phases: Signal preprocessing, feature extraction, and feature matching. Feature extraction and feature selection had an enormous effect on accuracy of signature verification. Feature extraction was a difficult phase of signature verification systems due to different shapes of signatures and different situations of sampling. So we have to take care about the security of biometric template because we can't modify our biometric feature due to its uniqueness. In this case, the performance can be measured in terms of TAR (True Acceptance Rate) and FAR (False Acceptance Rate) for each and every user separately according to the desirable false rejection rate (FRR). In the results, it is shown that the TAR vs FAR graph for the proposed method has improved upon the current method.

Keyword: Online signature, verification, TAR, FAR

I. INTRODUCTION

Signature verification is a general behavioral biometric to discover human beings for purpose of verifying their identity. Here in on-line system verification system our aim is to verify the input signature that's to spot whether or not the input signature is real signature or solid signature. However on the opposite hand we've got to require into consideration the very fact that there will be intrapersonal variations within the signature that's variation within the signature of an equivalent person and for this thesis ought to be minimum chance of rejecting the real signature. Furthermore we've got to come up with a feature vector which has all the options that has been accounted for the system [2]. additional the options non-inheritable additional are going to be the accuracy of the system however the limitation lies within the proven fact that system has restricted area to store these options and additional the parameters additional are going to be process complexness. So we've got to create the system which can be reliable and conjointly economical.

A signature may be changed by the user. Similarly to a password while it is not possible to change finger prints iris or retina patterns. Therefore, automatic signature verification has the unique possibility of becoming the method of choice for identification in many types of electronic transactions, not only electronics but also for other industries.

Signature verification has been used in number of applications such as governmental uses and used for commercial level to forensic applications. A few of them are discussed below: Nowadays signature verification used for commercial use. It can be used for authentication on ATMs, for package delivery companies. The internationally recognized courier service UPS has been using signature verification for many years now for personnel identification. Logging on to PCs can be done with a combination of signature verification system and fingerprint identification system to achieve a higher level security in a sensitive area. We can also use a combination of password and signature verification system. This would allow the users to have a higher level of security and confidentiality for their clients and protection of their work. Signatures have been using for decades for cheque authentication in banking environment. But even experts on forgeries can make mistakes while identifying a signature. In general, Off-line signature verification can be used for cheque authentication in commercial environment. Signature verification techniques have been used for cheque fraud and forensic applications. The requirements for authenticating the identity of the sender and ensuring the content integrity in printed paper documents have been growing. Paper documents are still used in the various secure transactions. Manual verification of large amount of documents to authenticate the sender and the content was difficult. The existing technologies make use of image processing techniques for creating and verifying digital signatures and are vulnerable to physical conditions of the document. Another currently available method takes whole content of the document to achieve the requirement and requires more complex procedures for implementation. A novel scheme was presented for securing the authenticity and originality of certificates issued by an authority by implementing unique digital signatures created from the selected contents (words or characters) of the documents. The method assures the content integrity and sender identity authentication. The proposed method was ensured the authentication and content integrity for certificates printed in paper in a simple and cost effective manner. Some words or characters that make the certificate unique were chosen and were processed to create the on-paper digital signature. The verifier must know the words chosen at the sender side and the position of words selected to create OPDS was provided to the verifier by the signing authority during verification process. An authentication mechanism was provided to authorize the verifier and ensured that only the authorized users can be verified the certificates. The verification of certificates can be done online by anyone who was authorized to do the same. Optical character recognition was applied to the scanned image of the certificate to select the specified words used at the creation process. The verification procedure compares the message digest obtained from QR code and the message digest obtained by hashing the result of OCR. Due to the fact that OCR was not accurate always, a provision for manual verification was made at the verification process. The method used simple and less number of steps and provided easier implementation than the existing technologies. The physical condition of the document does not have much effect on the proposed method compared to the image based techniques for paper document authentication. The analysis showed that the proposed system provided minimum error rate and hence good performance .Highlighting the digital signature mechanisms & its certifications to implement it easily in mobile devices to protect from MIM and fraudulent access to any confidential data or information. Mobile devices are easily accessible to everyone. Mobile technology is upgrading every day hence data transfer security is the basic threat, for which highly secured mechanism is required to avoid fraudulent access to any confidential data or information. Like e-mail broadcast, e-commerce or some financial transactions it was required that both sender and receiver of the data or information should sign the document and convert it digitally, making data transfer more reliable. It indicates that security can be confirmed using signature creation and its verification in android mobile devices when connected in a wired network. With wired networks it was also mandatory to ensure the same security using the same mechanism in wireless network.

Approaches to signature verification be 2 classes in step with the acquisition of the data: On-line [3] and Off-line. On-line information records the motion of the stylus whereas the signature is created, and includes location, and presumably speed, acceleration and pen pressure, as functions of your time. On-line systems use this data captured throughout acquisition. These dynamic characteristics square measures specific to every individual and sufficiently stable similarly as repetitive. Off-line information may be a 2-D image of the signature. Process Off-line is complicated owing to the absence of stable dynamic characteristics. Problem conjointly lies within the proven fact that it's exhausting to section signature strokes owing to extremely fashionable and unconventional writing designs. The non-repetitive nature of variation of the signatures, due to age, illness, geographic location and maybe to some extent the spirit of the person, accentuates the matter. These coupled along cause massive intra-personal variation. a sturdy system must be designed that mustn't solely be ready to contemplate these factors however conjointly notice numerous varieties of forgeries. Signature verification has the following benefits over biometric systems.

1. Nowadays it is a socially accepted verification method already in use in banks and credit card transaction.
2. It is useful for most of the new generation of portable computers and personal digital assistants (PDAs) use handwriting as the main input channel.

II. RLEATED WORK

Plamondon, Réjean et al. [1] in this paper, online signature verification has been proposed and studies the significant feature of signature generation and modeling. The major problems associated to the improvement of proposed system are addressed and the various approaches have been presented in this work.

Sae-Bae, Napa et al. [2] proposed a simple and efficient technique for online signature verification. The template of signature needed constant space and is very compact. This proposed algorithm is implemented on MCYT-100 and SUSIG data sets. The result analysis indicates that the proposed algorithm is very simple, efficient and better in comparison with other techniques. Moreover, proposed approach has been tested on finger drawn signatures on touch devices and then data set has been gathered from an uncontrolled environment and over multiple sessions. The results according to this data set verify the efficiency of the presented algorithm in mobile settings.

Parodi, Marianela et al. [3] proposed Legendre polynomials depends on the feature extraction for online signature verification. In order to model the signatures, the coefficients of expansion in these series are used as features and to evaluate the verification system performance signature database should be considered. In this paper, two classifiers such as SVM and random forests are used for the verification system. t he performance of proposed approach indicates that there is better correlation among the consistency factor and the verification error. These values of consistency factor can be utilized to choose the optimal feature combination.

Lopez-Garcia, Martin, Rafael et al. [4] in this work, implementation of FPGA of an embedded system for online signature verification. This proposed algorithm uses a pre-processing, dynamic time warping algorithm and Gaussian Mixture Model. This work is verified by using database of 100 public users, and achieving a high recognition rates for both original and fake signatures. Furthermore, the implemented system also involves a microprocessor that is related with vector floating-point unit. The proposed system has ability to complete the verification in less than 68 ms with a clock rated at 40 MHz. The results have been compared with the systems depending on ARM Cortex-A8 and performance demonstrated that number of clock cycles is accelerated by a factor of ×4.8 and ×11.1.

Griechisch, Erika et al. [5] Online signature verification technique study the dynamics of the handwriting process to choose whether a signature is almost certainly authentic or fake. Most of the formerly resented technique for online signature verification apply Neural Networks, or HMM for classification. In this paper, a non-parametric statistical test has been applied for association of features and the verification of signatures.

Kudłacik et al. [6] proposed a novel fuzzy technique to *off-line* handwritten signature recognition. In this paper, fuzzy model is produced which is commonly known as the fuzzy signature and it may be evaluated during the phase of verification. It is required to be highlighted that the stored data in the verification system will not be used to re establish the real structure gathered at enrolment phase. Therefore, the proposed approach may be easily used in application where FAR coefficient must be less and most significantly than FRR ratio.

Malik, Muhammad Imran et al. [7] proposed an analysis of signature stability depending on the signature's local / part-based features. In this work, SURF can be utilized for the analysis that provides several evidence about the area from whom the features should be extracted. Furthermore, local stability analysis has been proposed which helps to calculate the data set of the system which carries real, fake and hidden signatures. The presented system attained an EER of 15% that is much lower than others. Additionally, comparisons of the presented system have been done with some other earlier reported systems. Based on the comparison it can be concluded that the presented system performs better among other previously described system

Jarad, Mujahed, Nijad Al-Najdawi et al. [8] this paper discussed an ANN based Back-propagation algorithm. This proposed algorithm is utilized for the verification and recognition. To verify the performance of the proposed system, FAR, FRR and EER have been evaluated. The system is being verified with 400 test signature samples, that includes real, fake or hidden signatures of 20 different people. The major goal of this system is to limit the computer singularity in selecting whether the signature is fake or not. This technique agrees to judging the signature accuracy, and attaining more effective results.

Arora, Manish, Karam Singh et al. [9] in this paper, novel technique for verification of online handwritten signature depending on DFrCT used for extracting feature. Several a new features of hand-written signature are utilized to extract distinct features of signature. The proposed system is realized by the 3 FIR system and the impulse responses of FIR system are useful for the evaluation of Euclidean norm. The signature may be tested by calculating the difference between the average of Euclidean norms of reference signatures and the Euclidean norm of signature to be verified. In order to evaluate the effectiveness of presented approach, the EER can be evaluated. It can be tested during simulations that the DFrCT tool attains better results in comparison with DCT for feature extracting. The simulation result has been conducted on SVC2004 signature database.

Houmani, Nesma et al. [10] in this paper, entropy-based measures has been proposed. In this paper, the proposed measures have been studied measures for an automatic writer categorization on various databases. This paper indicates that such category retrieve separately on one hand degraded data and on the other hand good quality signatures. Finally, the degradation of signatures due to mobile acquisition conditions is quantified by our entropy-based measures

Tolosana, Ruben, Ruben Vera-Rodriguez et al. [11] proposed a dynamic signature recognition approach in this paper which is applied to forensic scenarios. This proposed approach utilizing hybrid partitioning for the verification of signature. Partitioning can be done with two phases. In the first phase signing process have high velocity and in second phase signing process have low pressure. In this paper, global recognition system or automatic featured-based is used for the extracting the features by FDE. A system consist of 117 global features is presented and calculated with Bio Secure DS2 database. Moreover, the subset of 40 features is chosen by SFFS approach as the optimal feature vector in the development phase. The result analysis is attaining 10.6 % of equal error rate for skilled forgeries that develop former results using the same techniques. Additionally, a set of features is being analyzed for real and fake signature to get significant information which can be utilized by the forensic experts.

III. PROPOSED METHODOLOGY

The Hadamard transform-based signature template satisfies the needs of non invertibility and diversity for biometrics. More so, the method is efficient and saves space of memory for saving resultant transformed templates and the parameter key. The proposed method is evaluated with using public databases SUSIG dataset. The results displays the new technique performs satisfactorily in comparison with existing alignment-free templates. The proposed Hadamard transform-based approach can be argued as a special case of dynamic projection for the biometrics; however, compared to conventional projection, the method gives a simple yet effective way of secure transformation during retaining mostly recognition performance.

In this section, discuss the Hadamard transform-based signature template design. Firstly, introduce the preliminaries on Hadamard transform. Then, next apply the partial Hadamard transform to binary string's frequency-domains. So, wrap up the section with signature template matching in transformed domain.

A. *Preliminary*

The Hadamard transform is a orthogonal transformation non-sinusoidal whose base is created with Walsh functions. These Walsh functions are square or rectangular waveforms with the values of +1 or -1. The Hadamard transform contains no multipliers in real because the amplitude of Walsh functions is only two values, +1 or -1. A Hadamard matrix is defined a matrix elements are ±1 and row vectors pair wise orthogonal. In this case when m is a power of 2, an $m \times m$Hadamard matrix is made by means of recursion:

$$\mathrm{H}_2 = \begin{matrix} 1 & 1 \\ 1 & -1 \end{matrix} \qquad \mathrm{H}_{2\mathrm{m}} = \begin{matrix} H_m H_m \\ H_m\text{-}H_m \end{matrix}$$

The Hadamard matrix is orthogonal and symmetrical. Hence,

$$H^T{}_m H_m = {}_m I_m \qquad \text{eq. (3.6)}$$

Where $I_m$is an $m \times m$ identity matrix. With the binary components ±1, the Hadamard method transform a low computational load because it contains no multiplication only addition and subtraction.

B. *Secure Signature Template creation with using Partial Hadamard Transform*

However, a full-order Hadamard matrix is reversible, a sub matrix is formed by randomly opting a subset of rows from full-order Hadamard matrix is column rank-deficient, non-invertible. We explain the partial Hadamard matrix to run on the binary string's on frequency-domain samples. The derivations of binary string's frequency-domain samples are in detailed.

Let H_N denotes partial technique Hadamard matrix, which is created by opting S (S=244 in this case) rows of an $N\times N$ full-order Hadamard matrix H_N, with $S< N$ and $N = 2^n$. Clearly, rank(¯ H_N) = S and therefore the partial Hadamard matrix H_N is column rank-deficient. That is, H_N has no invertible or pseudo-inverse. Now, apply following transformation to creating the resultant template T :

$H_N\, B = T$ eq. (3.7)

Generally, Hadamard matrices are called square matrices, whose entries are +1 or −1 and the rows are orthogonal. Geometrically, it means every two distinct rows in Hadamard matrix display two perpendicular vectors, where the combinatorial terms show which every two distinct rows contains matching entries in correctly half of the columns and unmatched entries in remaining columns. Conversely, a Hadamard matrix contains maximal determinant with these matrices entries of absolute value less than 1 and thus it may be considered as external solution of Hadamard's maximum determinant problem. Hadamard matrices are reduced to the subtraction and addition of the operations. This lets the use of easier hardware to compute the transform or improve the speed of retraining because of less complexity.

Algorithm

A. Template generation
1. Preprocessing
2. Feature extraction
3. Create hadamard matrix

$$H_2 = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$

$$H_4 = \begin{bmatrix} H_2 & H_2 \\ -H_2 & H_2 \end{bmatrix}$$

4. Select random rows
5. Quantize the feature

$$q^u(i) = \beta \sqrt{\left(\frac{1}{S}\right)\left(\sum_{j=1}^{S} f^{Sj}\,(i) - \mu_{f(i)}(u)\right)}$$

6. Generate and Save template for enrolled user
7. Select threshold with minimum EER

B. Testing
   1. Preprocessing
   2. Feature extraction
   3. Create hadamard matrix

$$H_2 = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$

$$H_4 = \begin{bmatrix} H_2 & H_2 \\ -H_2 & H_2 \end{bmatrix}$$

   4. Select random rows
   5. Quantize the feature

$$q^u(i) = \beta \sqrt{\left(\frac{1}{S}\right)\left(\sum_{j=1}^{S} f^{Sj}\,(i) - \mu_{f(i)}(u)\right)}$$

   6. Match the final feature with template

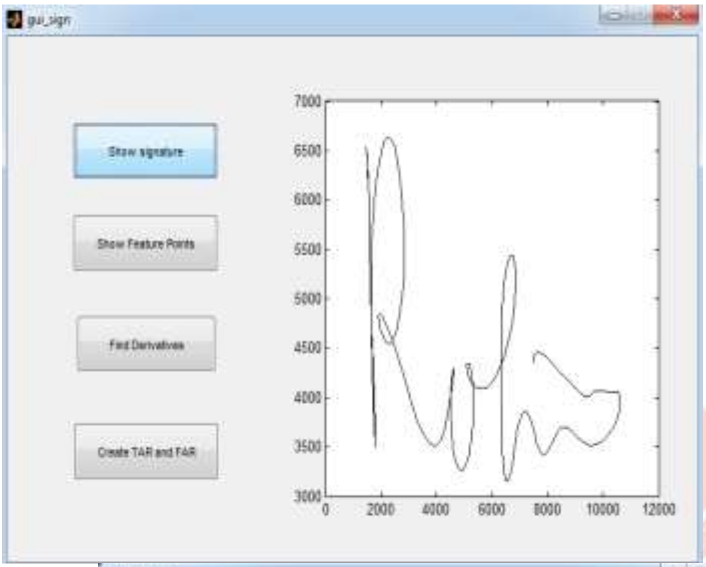
$$Score = \sum_{i=1}^{M} |\hat{F}^{(t|u)} - \ddot{f}^{u}(i)|$$

7. Give output based on verification

IV. RESULT AND DISCUSSION

For the results, adaptive thresholding is implemented for TAR and FAR graph generation. In adaptive thresholding, the distributions of scores of biometric samples are differing from user to user. The false acceptance ratio wrt to same threshold is dissimilar for each user. Moreover, FAR (false acceptance ratio) should be very low for every user in order to check security. In this case, the performance can be taken by changing the threshold for each and every user separately according to the desirable false rejection rate (FRR). In practical applications, it is showed that empirical decision threshold can be calculated by using the pool of signatures in the database where every signature is signified by a feature vector.

The results are shown as below:



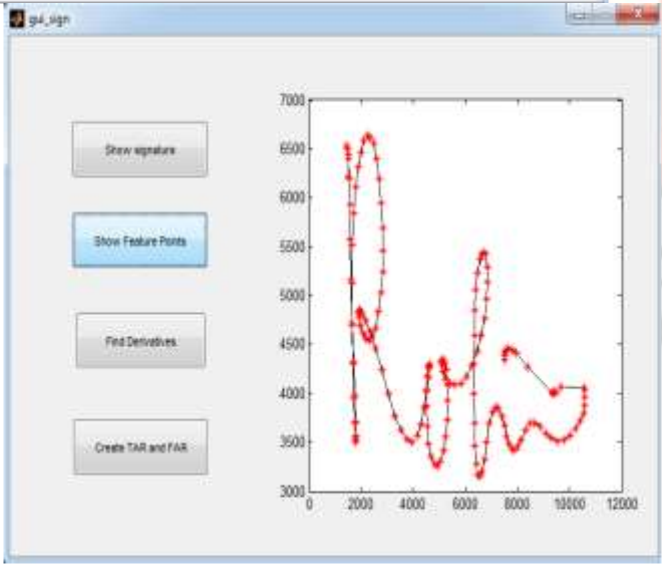


Fig.1: A sample signature from the dataset

Fig.2: Feature points extracted from the sample signature.

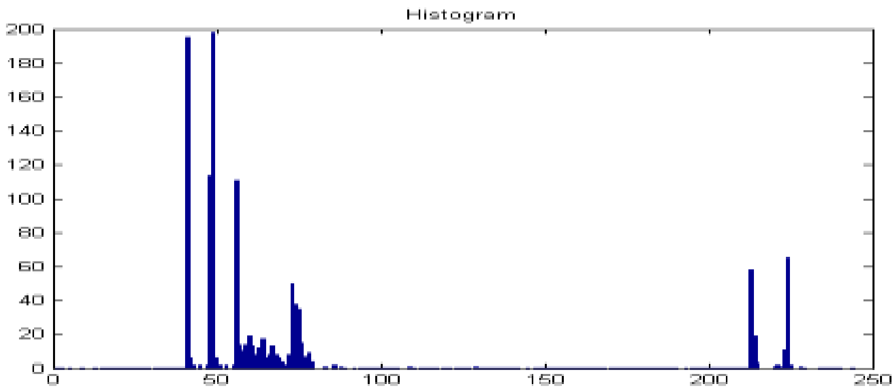


Fig.3: Histogram of all the features.

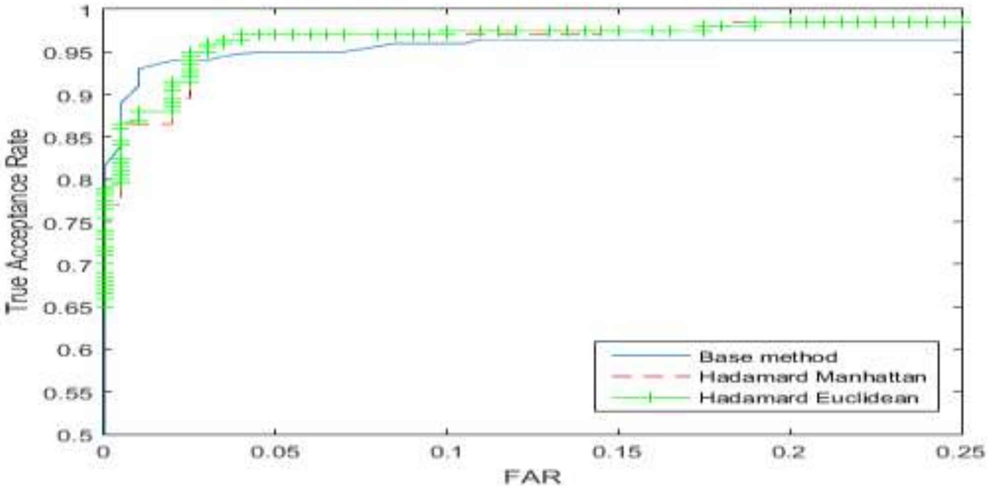
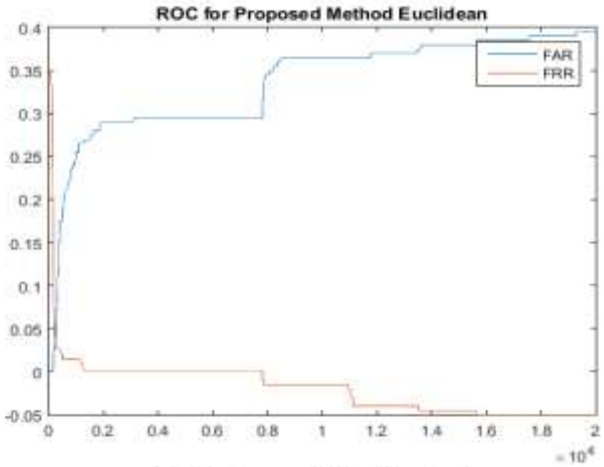


Fig. 4: TAR vs FAR Graph.



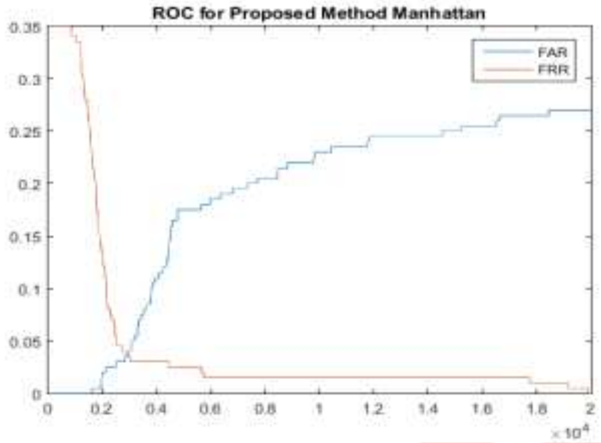


Fig. 5 (a)

Fig. 5 (b)

Fig. 5 (a) ROC Curve for proposed method with Euclidean with low EER. **Fig. 5(b)** ROC Curve for proposed method with Manhattan with low EER than base and higher than Euclidean

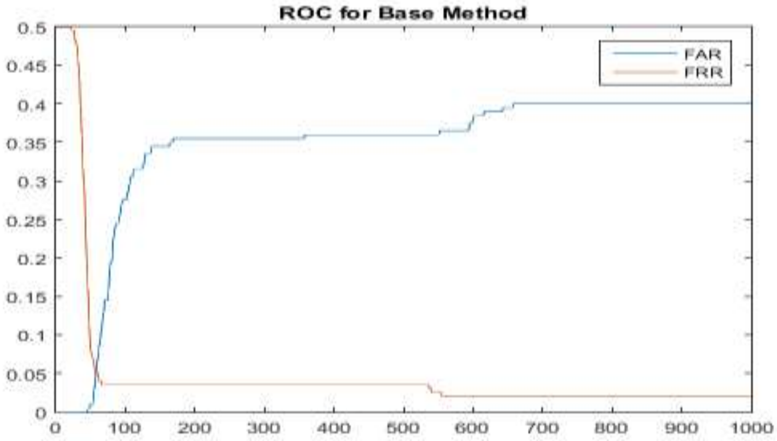


Fig. 6: ROC Curve for base method with high EER

The results presented here, show that the GAR is improved in a much better way in comparison to the previous method. But due to the inclusion of partial Hadamard matrix, the security of the system is increased. This is because the applied partial Hadamard matrix transforms the template into non-invertible domain. This also adds up to the diversity as many number of templates can be generated using the different combination of the partial hadamard matrix. And hence the security also gets increased for the template as well as the biometric system.

Table 1

	Base Method	Proposed Method Manhattan	Proposed Method Euclidean
TAR	**0.94**	**0.945**	**0.95**
FAR	**0.0275**	**0.0275**	**0.0275**

Table 2

	Base Method	Proposed Method Manhattan	Proposed Method Euclidean
EER	**0.05**	**0.03**	**0.025**

V. CONCLUSION

By the help of results, we can conclude that the proposed method enhances the security of the system to a great extent thereby improving the system and also increasing the accuracy of the system as the TAR for the proposed with Euclidean distance system is higher and EER is lower than that of the earlier system. The future work can be dealt in the area to further improve the accuracy so as to further decrease the cases of false acceptance.

In our study we analyze the challenges in the security of the biometric extracted data. The different problem that we found during the recognition of biometric template are: un matching of the signatures, feature extracted from the person with the database stored there are two basic aspect to evaluate the recognition accuracy of the biometric identification system namely FRR(fault rejection rate) and FAR(fault acceptance rate).

1. FRR = Number of fault rejection/ total no of genuine attempts.
2. FAR= Number of fault acceptance/ total no of imposter attempts

We can solve this problem of error in the biometric feature extracted data with the help of the multi model biometric system (fusion of multiple sources) and it helps to increase the recognition accuracy of the biometric template. These techniques help in bringing the false acceptance rate and fault rejection rate low and make the mobile commerce payment transactions highly secure and reliable. The future scope may attract the work to be done in field to reduce the complexity of the systems further so as to increase the reach of the these systems to as many people as possible. Hence, these systems can be made available to the people in order to increase their personal secure environment and improve their privacy quotient.

REFERENCE

[1] Plamondon, Réjean, Giuseppe Pirlo, and DonatoImpedovo. "Online signature verification." In *Handbook of Document Image Processing and Recognition*, Springer London, 2014, pp. 917-947.
[2] Sae-Bae, Napa, and NasirMemon. "Online signature verification on mobile devices." *Information Forensics and Security, IEEE Transactions on* 9, no. 6 (2014): 933-947.
[3] Parodi, Marianela, and Juan C. Gómez. "Legendre polynomials based feature extraction for online signature verification. Consistency analysis of feature combinations." *Pattern Recognition* 47, no. 1 (2014): 128-140.
[4] Lopez-Garcia, Martin, Rafael Ramos-Lara, Oscar Miguel-Hurtado, and Enrique Cantó-Navarro. "Embedded system for biometric online signature verification." *Industrial Informatics, IEEE Transactions on* 10, no. 1 (2014): 491-501
[5] Kudłacik, Przemysław, and PiotrPorwik. "A new approach to signature recognition using the fuzzy method." *Pattern Analysis and Applications* 17, no. 3 (2014): 451-463.
[6] Malik, Muhammad Imran, Marcus Liwicki, Andreas Dengel, Seiichi Uchida, and VolkmarFrinken. "Automatic signature stability analysis and verification using local features."In *Frontiers in Handwriting Recognition (ICFHR), 2014 14th International Conference on*, pp. 621-626.

[7] Jarad, Mujahed, Nijad Al-Najdawi, and Sara Tedmori. "Offline handwritten signature verification system using a supervised neural network approach." In *Computer Science and Information Technology (CSIT), 2014 6th International Conference on*, pp. 189-195.
[8] Arora, Manish, Karam Singh, and GuneetMander. "Discrete fractional cosine transform based online handwritten signature verification." In *Engineering and Computational Sciences (RAECS), 2014 Recent Advances in*, pp. 1-6.
[9] Houmani, Nesma, and Sonia Garcia-Salicetti. "Quality Measures for Online Handwritten Signatures."In *Signal and Image Processing for Biometrics*, pp. 255-283.
[10] Tolosana, Ruben, Ruben Vera-Rodriguez, Julian Fierrez, and Javier Ortega-Garcia. "Feature-based dynamic signature verification under forensic scenarios." In *Biometrics and Forensics (IWBF), 2015 International Workshop on*, pp. 1-6.