International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

Secure Template Generation Using Non-Invertible Transform for Online Mobile Signature Verification

Sonika Sharma[1], Swati Bhasin[2]

[1]M.Tech. Scholar, Geeta Institute of Management and Technology Engineering, Kurukshetra, India
[2]Assistant Professor, Department of ECE, Geeta Institute of Management And Technology Engineering, Kurukshetra, India

Abstract: *The theme possesses the novel property of being strong against AN adjust chosen-message attack: AN somebody UN agency receives signatures for messages of his alternative (where every message could also be chosen during a manner that depends on the signatures of antecedently chosen messages) cannot later forge the signature of even one further message. Therefore target is to construct a signature theme with such properties supported the existence of a "claw-free" combine of permutations--a doubtless weaker assumption than the trait of number factoring.*

1. INTRODCUTION

The term "biometrics" comes from the Greek words bio (life) and metric (to measure). Bioscience means that the automated identification of someone supported his/her physiological or behavioral characteristics. This methodology of verification is most popular over ancient ways involving passwords and PIN numbers for its accuracy and case sensitiveness. A biometric system is actually a pattern recognition system that makes a private identification by crucial the legitimacy of a particular physiological or behavioral characteristic possessed by the user. These characteristics square measure measurable and distinctive. These characteristics mustn't be consistent. A vital issue in coming up with a sensible system is to work out however a private is known. Reckoning on the context, a biometric system shown in Figure one will be either a verification (authentication) system or Associate in identification system.

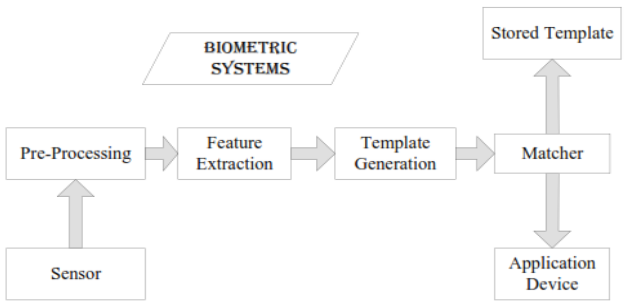

Figure 1.1 Biometric System

There is perpetually a desire for the reliable and economical system for biometric identification. Many biometric options are studied and verified helpful, together with signature, fingerprint, face, speech, iris, and tissue layer pattern. Among them written signature verification methodology has been well accepted for a protracted time. Written signature verification system comes underneath the analysis space of signal process. There square measure 2 varieties of signature verification systems: offline and on-line systems. Before the event within the pc era we have a tendency to be victimization solely the offline system however with the technological advancements man has developed the system of on-line verification. In Associate in Nursing offline system, image of the signature of the user should be non-heritable not the opposite options however in an internet system, different options of the signature have to be compelled to be non-heritable that square measure like x-y coordinates, pressure, variety of strokes, altitude etc. so we will say on-line system is a lot of correct and reliable than that of offline system. However on the opposite hand there's perpetually a scope for the higher results and conjointly to check the one methodology of feature extraction with the opposite. Therefore still lots a lot of work will be done on this analysis topic.

Online signature verification system includes many steps: Signature input, Preprocessing, Feature extraction and matching (verification). Preprocessing is needed to get rid of the fluctuations within the linguistic communication method. Feature extraction techniques square measure needed to induce the distinctive options of each signature and subsequently a novel feature vector is to be created. Here completely different feature extraction techniques will be used like bar graph, separate trigonometric function remodel, Fourier remodel etc. In matching, score is to be deciding that's a threshold is to be predefined with that the input signature is to be verified with the reference (stored) signature. Matching techniques will be of various sorts like Manhattan distance, geometer distance etc.The performance of signature verification system is measured in terms of false rejection rate (FRR), false acceptance rate (FAR) and equal error rate (EER).Feature extraction may be a important step in on-line signature verification. The feature extraction method begins by changing the time-series information of a

signature in to a sequence of philosopher vectors and attributes, similarly as their derivatives. Then, every philosopher vector is additionally reborn to a vector within the coordinate system.A user guide is generated throughout the enrollment method wherever multiple signatures square measure noninheritable from a user and a feature set is computed from every of the samples.

In the verification method once the user provides the input , this input signature is to be verified by matching with the keep reference signal. The matching method will be done by activity the Manhattan distance that is employed within the projected on-line signature verification system. If the distinction between the check signature and therefore the reference signature but the predefined worth then signature are going to be taken as real however if the distinction between the 2 is over the predefined threshold then the check signature are going to be taken as solid.
Verification performance is one in every of the key factors that influence the usability of associate degree authentication system. Particularly, false rejection will result in either a rise within the variety of authentication makes an attempt or user rejection and temporary resistance. Whereas each cause usability problems, the recovery effort of the latter is additional time- overwhelming than the previous. Assumptive that 3 failing makes an attempt square measure allowed before rejecting and quickly protection out users, rejections of real signatures square measure classify into 2 classes.

2. RELATED WORK

Boutellaa, Elhocine, MessaoudBengherabi et al. [1] projected a revolutionary theme for on-line verification of the signature by introducing a replacement user-specific score social control strategy. A most a Posteriori Adaptation technique is employed here to enhance the results. Pirlo, Giuseppe, and **Donato Impedovo** [2], have used the optical flow technique so as to develop the system however eventually it's a computationally valuable approach. **Wibowo, CanggihPuspo,** [3] projected a replacement options referred to as the forward and backward variances of signature for on-line signature verification. At the most recent, **Sae-Bae, Napa, and Nasir Memon** [4] evolved a method that uses position similarly as pressure terms for secure guide that uses a mixture of 1D and 2nd histograms.In this paper, Wei Tian et al. [5] developed a whole fingerprint recognition system embedded on FPGA that was ten times quicker than its equivalent computer code implementation on associate degree Intel Core2Duo micro chip clocked at 1.8 GHz.
In this paper, **YasmineGuerbai** et al. [6] proposed the implementation on field-programmable gate arrays of associate degree embedded system for on-line signature verification. The popularity algorithmic program primarily consists of 3 stages.

In this paper, **Jinjing** Shi et al. [7] proposed the fluctuation of handwriting, the restricted variety of coaching knowledge and also the problem of extracting stable feature of signatures are some issues that has to be Janus-faced in signature verification. Several works in on-line signature verification are exhausted order to search out the correct methodology.In this paper, **Miguel A Ferrer** et al. [8] proposed the signature verification system ought to extract the distinctive options of what has been signed. Essentially biometric authentication deals with characteristic someone whereas verification deals with police investigation whether or not the signature is real or forgery. In this paper, **Mandeep Kaur** et al. [9] proposed the One of the foremost evident effects of the quality of signature generation and implementation processes is that the great deal of non-public variability that may be measured in written signatures, even once dead by an equivalent signer.

In this paper, **Muhammad Reza** et al. [10] proposed the A client-entropy live has been planned to cluster and characterize dynamic signatures in classes that may be associated with signature variability.In this paper, **Srikanta pal** et al. [11] proposed the planned Multi-script offline signature identification within which the signatures of Bengali, Hindi and English are thought of for Identification method.In this paper, **MdAsraful** et al. [12] proposed the planned add that they need used one-class SVM for hand written signature verification. Usually bi-c1ass SVM are accustomed distinguish between real and solid signature. During this work the authors have planned a technique to research the utilization of one-class SVM for written signature verification system.**G. Pirlo** et al. [13] proposed the proposed a technique on foreground and back ground features for the identification of scripts from bi-lingual off-line signatures. Gradient based method is used to extract features of foreground as well as back ground components.In this paper, **V. Di Lecce** et al. [14] proposed the GPU-based SVM classifier, by extending our previous work on Multi-Threaded parallel CPU standalone SVM version, which builds from scratch an implementation of the Sequential Minimal Optimization algorithm.In this paper, **G. Dimauro** et al. [15] proposed the scope of biometric analysis; an important problem is to distinguish between genuine and forged signatures, which are a hard task. in this paper we present a GPU based effective model selection methodology that contributes to circumvent this problem and a robust classifier capable of handling many different groups of features.This paper propose offline schemes for signature verification with the algorithmic program for affine registration of true and

false signatures 2nd purpose sets, artificial immune system's pertinency for written signature verification and form based mostly geometric options and additional significantly focuses on the gap based parameters like the continuity of the signature textural options square measure computed and concatenated with coefficients of contourlet remodel to make the ultimate feature vector severally for the verification system.

3. 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.

3.1 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:

$$H_{2x2} = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$

$$H_{4x4} = \begin{bmatrix} H_{2x2} & H_{2x2} \\ -H_{2x2} & H_{2x2} \end{bmatrix}$$

The Hadamard matrix is orthogonal and symmetrical. Hence,

$$H^T{}_m H_m = {}_m I_m$$

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.

3.2 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($\bar{}$ 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 :

$$H_N B = T$$

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.

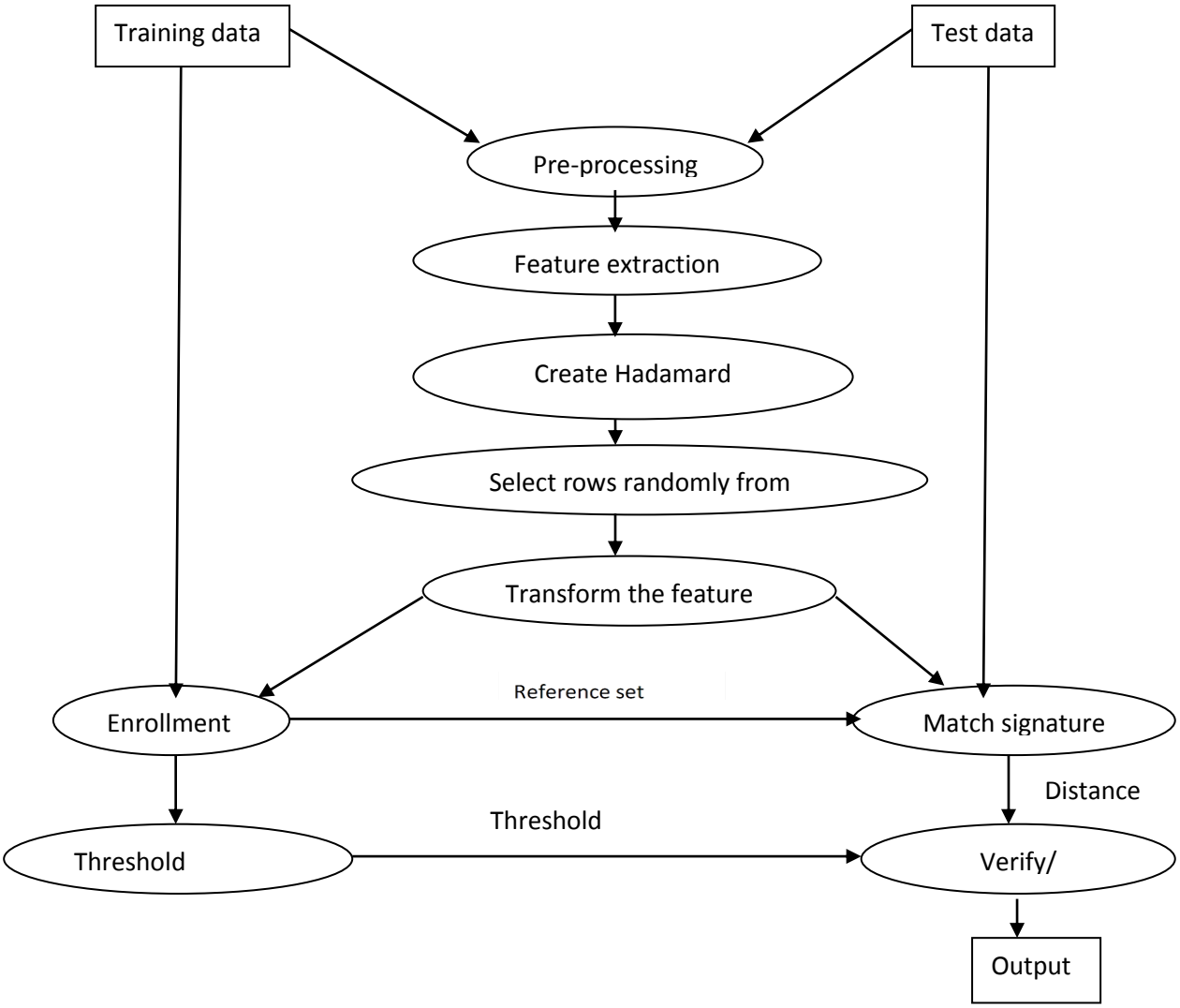

Fig 2. Flow Chart of the proposed Method

4. RESULTS

The results for the proposed method are as follows.

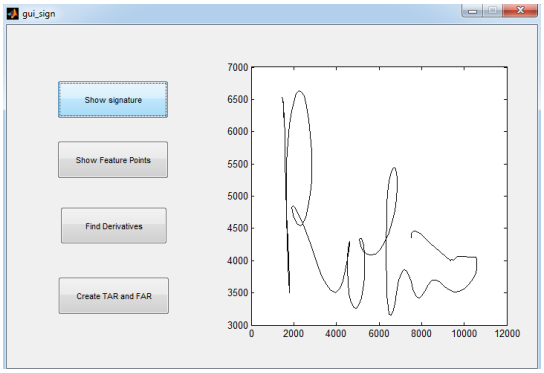

Fig 3.Sample signature

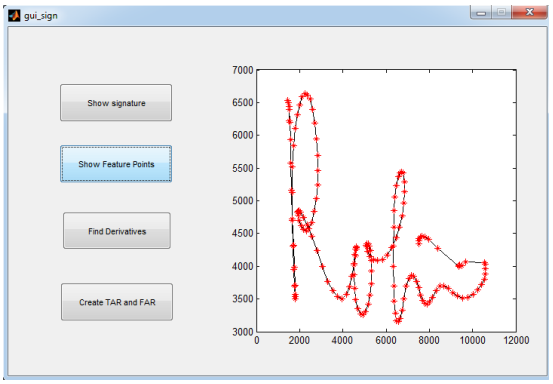

Fig 4.Sample signature features

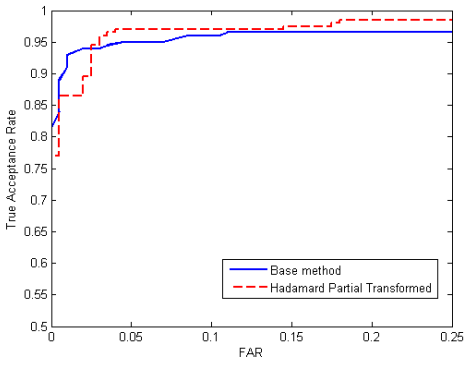

Fig 5.TAR vs FAR Graph.

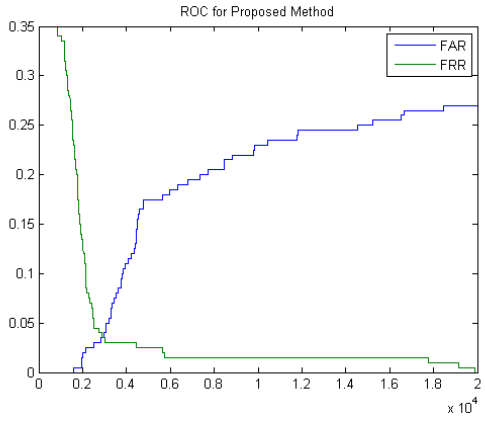

Fig 6. ROC Curve for proposed method with low EER

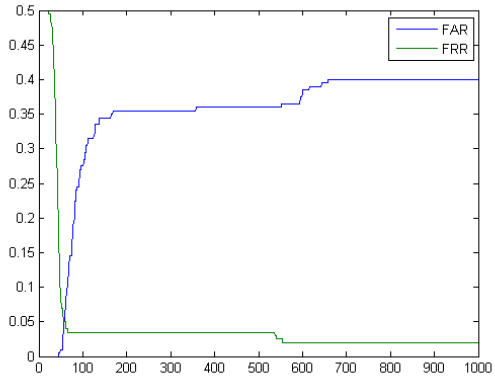

Fig 7 ROC Curve for base method with high EER

5. 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 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.

REFERENCES

[1] Boutellaa, Elhocine, MessaoudBengherabi, and FaridHarizi. "Improving online signature verification by user-specific likelihood ratio score normalization."Systems,

Signal Processing and their Applications (WoSSPA), 2013 8th International Workshop on. IEEE, 2013.

[2] D. Impedovo and G. Pirlo, "On-line signature verification by stroke-dependent representation domains," in Proc. 12th ICFHR, Kolkata, India, Nov. 2010, pp. 623–627,16–18.

[3] Wibowo, CanggihPuspo, PitakThumwarin, and Takenobu Matsuura. "On-linesignatureverification based on forward and backward variances of signature."InformationandCommunication Technology, Electronic and Electrical Engineering (JICTEE), 2014 4th Joint International Conference on. IEEE, 2014

[4] Sae-Bae, Napa, and Nasir Memon. "Online Signature Verification on Mobile Devices."(2014): 1-1.

[5] Wei Tian and JingyuanLv"A New affine registration algorithm applied to off-line signature verification" International Conference on Information and Automation Shenyang, China, pp 806-810, June 2012.

[6] YasmineGuerbai, YoucefChibani and Nassim Abbas, "One-class versus Bi-Class SVM classifier for off-line signature verification", IEEE International Conference on Multimedia Computing and Systems, pp 206-210, 2012.

[7] Miguel A Ferrer, J Fransciscovargas, Aythami Morales and Aaron OrdonDez Robustness of offline signature verification based on grey level features" IEEE Transaction on Information Forensics and Security,voI.7,No.3,June 2012.

[8] Jinjing Shi, Danping Xu, Guoxiang Xu and Moon Ho Lee "Quantum communication scheme for blind signature with two-particle entangled quantum-trits", IEEE 14th International Conference on Advanced Communication Technolgy, pp 558-561, 2012.

[9] Mandeep Kaur Randhawa, A K Sharma, R K Sharam"Off-line signature verification with concentric squares and slope based features using support vector machine", 3rd IEEE International Advance Conference (IACC),pp 600-604,2013.

[10] Muhammad Reza Pourshahabi, Mohamad HoseynSigari and Hamid Reza Pourreza, "Offline handwritten signature identification and verification using contourlettransform", IEEE International Conference on soft computing and pattern recognition, pp 670-673, 2009.

[11] Srikanta Pal, A1aei Blumenstein,"Multi script International Conference 240,2012. Alireza, Umapadapal and Michael offline signature identification" 12th IEEE on Hybrid Intelligent system, pp 236,2012.

[12] MdAsrafulHaque and Tofik Ali, "Improved offline signature verification method using parallel block analysis", IEEE International Conference on Recent Avances in Computing and Software System, pp 119-123, 2012.

[13] G. Pirlo, "Algorithms for Signature Verification," in Proc. NATO-ASI Series Fund. Handwriting Recognit., S. Impedovo, Ed., Berlin, Germany, 1994, pp. 433–454, Springer-Verlag.

[14] V. Di Lecce, G. Dimauro, A. Guerriero, S. Impedovo, G. Pirlo, and A. Salzo, "A multi expert system for dynamic signature verification," in Proc. 1st Int.Workshop,Multiple Classifier Syst. (MCS 2000), J. Kittler and F. Roli, Eds., Cagliari, Italy, Jun. 2000, vol. 1857, Series: Lecture Notes Comput. Sci., pp. 320–329, Springer-Verlag Berlin Heidelberg.

[15] G. Dimauro, S. Impedovo, M. G. Lucchese, R. Modugno, and G. Pirlo, "Recent advancements in automatic signature verification," in Proc. 9th Int. Workshop Frontier Handwriting Recognit., Oct. 2004, pp. 179–184, IEEE Comput. Society Press.