Non-Invertible Online Signature Verification System Using Hadamard Transform

[1]Harleen,[2]Dr. Raghuvinder
[1]M.Tech Scholar,[2] Assistant Professor
[1,2]Department of Computer Science and Applications
[1,2]Chaudhary Devi Lal University, Sirsa, Haryana, India

ABSTRACT: **In this paper, online verification approach is proposed by using non- invertible transform. It is found that the proposed method improves the security of the system to a great extent so enhancing improving the system. Moreover, ever-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.**

Keywords: **Hadamard, matrix, biometric, EER, verification, feature, template, Error Rate, signature.**

I. INTRODCUTION

The fingerprints of those people, who are working in Chemical industries, are often affected. Therefore those companies should not use the finger print mode of authentication. Human affected with disease like diabetes, for those persons the eyes get affected resulting in differences. In spite of these demerits, presently biometric systems are widely utilized in numerous types of industries. If one can get required accuracy, then no other thing can take its place.
Several biometric options are discussed and verified simultaneously along with signature, face, eyes; speech etc. amongst all written signature verification process is being accepted for some time. This written verification system comes below the analysis space of signal process. There are two modes of verifications. One is online verification system and other one is offline verification process.

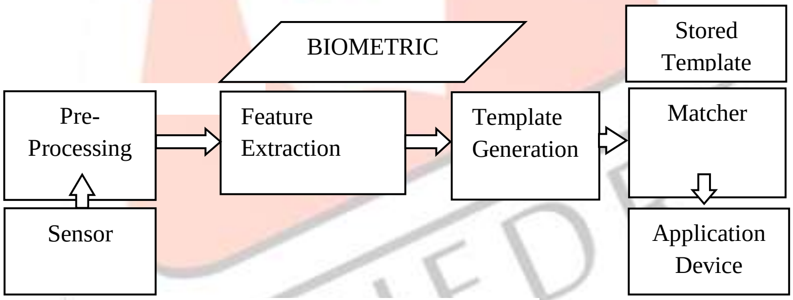

Figure 1.1 Biometric System

In the online system, dynamic information of signature has been discovered at the time when signatures are made. But in the case of offline system, it operates on the scanned images of a signature. Offline systems are bit complex as compared to online system because stable dynamic characteristics are not present in the offline systems. More so, in offline system highly untraditional writing style make it difficult to use. Therefore, easy and reliable system is being designed that must be discovering several kinds of forgeries. Thus, this paper discussed architecture for off-line signature verification.

This proposed method utilizes runtime signature as a replacement for of scanned images for recognition. This proposed offline system utilizes set of shape depending on the geometric features and significantly it focuses on the distance based parameters like continuity of the signature, matching of signature curves produced at some crucial points of particular signature by analyzing polynomial.
When the user gives the input in the verification method, then this this input is matching with the given reference signal for verification. The process of matching is done by the Manhattan distance which is employed within the projected on-line signature verification system. The comparison between verified signature and the given reference signal has been done in order to verify the signature. The verification is the only factor which affects the usability of authentication system. Specifically, forged rejection gives outcomes in either a growth within the variety of authentication makes an attempt or user rejection and temporary resistance.

II. RELATED WORK

In this paper, Jacques Swan poet al. [1] proposed the problem of handwritten signature recognition is considered significant in biometrics, in particular for determining the validity of official documents. The rationale consists of creating an offline classifier to discriminate between fake and genuine digitalized signatures. In such applications containing thousands of samples machine learning techniques such as Support Vector Machines play a preponderant role in overcoming the challenges inherent to this problematic. However, to deal with the computational burden of calculating the large Gram matrix, approaches such as Graphics Processing Units computing are required for efficiently processing big image biometric data.

In this paper, first, we present an empirical study for efficient feature selection concerning the signature identification problem. Second, GPU-based SVM classifier that integrates a component of the open source Machine Learning Library supporting several kernels is developed. Third, we ran several experiments with improved performance over baseline approaches. From our study, we gain insights in both performance and computational cost under a number of experimental conditions, and conclude that the most appropriate model is usually a trade-off between performance and computational cost for a given experimental setup and dataset.

In this paper, Sheikh Faisal et al. [2] proposed a verification function is achieved based on a difference between the points which can be determined by an unknown rotation. In order to archive the rotation, two-step algorithm is employed. We first reduce the affine registration problem to a rigid registration problem, and the unknown rotation is then computed using the coefficients of these polynomials. The algorithms have shown promising results while dealing with random forgeries and simple forgeries, also it gives better recognition rates in a public signature database.

In this paper, Karam Singh et al. [3] proposed novel technique for verification of online handwritten signature depending on DFrCT used for extracting feature. 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. 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. 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.

In this paper, Krzyszt et al. [4] presented a novel technique to recognize the verification depending on the dynamic signature. Portioning has been utilized for the proposed method. In the categorization method of the partitions, the user produced most stable reference signatures during acquisition phase. 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. If dynamics features of the signature are considered then efficiency of signature verification enhances the proposed method has several significant characteristics. Moreover, the results of two presently existing databases of dynamic signatures.

In this paper, Zhihua Yang et al. [5] presented an online signature verification approach depending on the sparse representation and DCT. Also, new property of discrete transforms that may be utilized to acquire a representation of online signature. It leads with simple process of matching and creating an efficient choice to deal with time series of different lengths. Moreover, novel approach has been presented to apply sparse representation to online signature verification and sparse characteristics are extracted. The result demonstrates that the presented process confirms person very reliably with a verification performance which is better than other methods on the same databases.

In this paper, Muhammad Imran et al. [6] 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.

In this paper, Miguel A Ferrer et al. [7] 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. [8] 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.

III. PROPOSED METHODOLOGY

The proposed verification approach is calculated by utilizing public databases SUSIG dataset. The outcome indicates that the novel approach performs suitably in contrast with previously existing alignment-free templates. The presented Hadamard transform-based technique may be squabbled as an exceptional case of dynamic projection for the biometrics; though, 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.

A. Preliminary

The Hadamard transform is an 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 × 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 m × 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× 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.

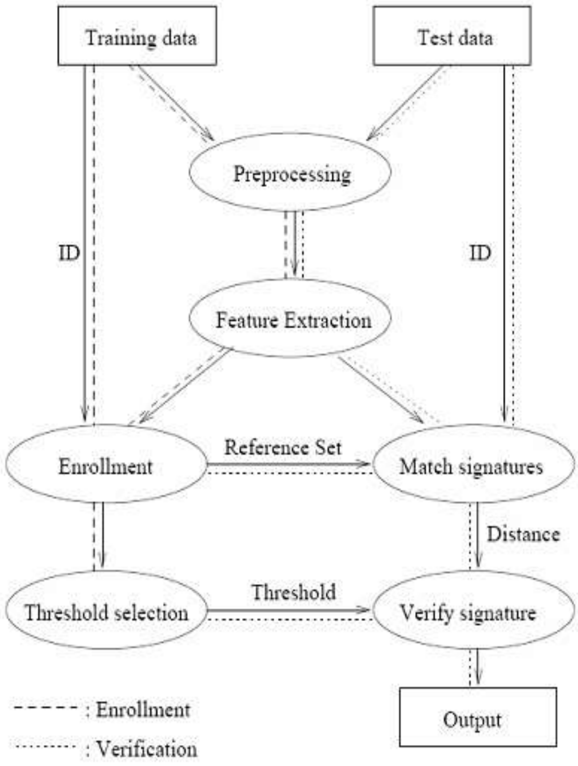

Fig 2: Flow Chart of the proposed Method

IV. RESULTS

The results for the proposed method are as follows.

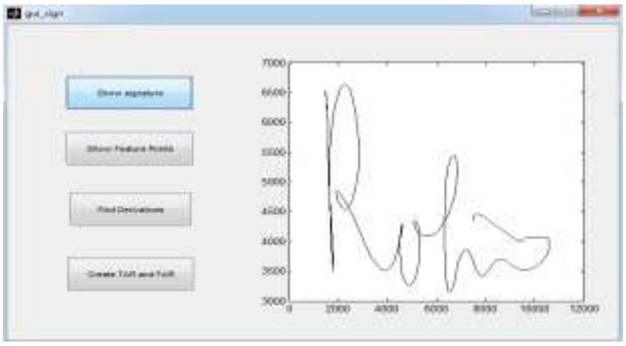

Fig 3: Sample signature

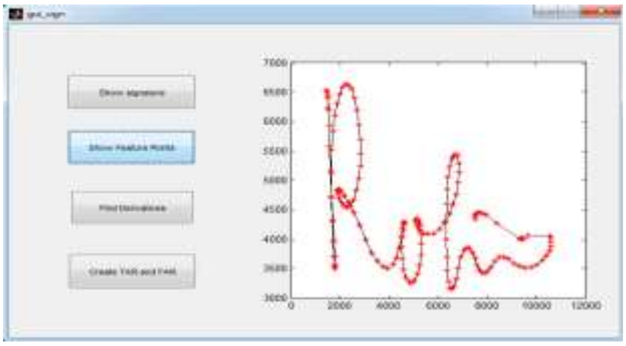

Fig 4: Sample signature features

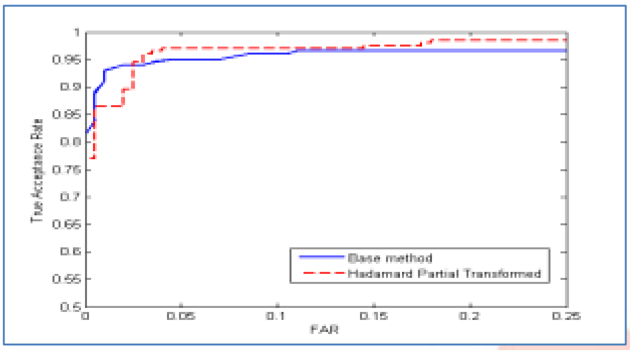

Fig 5: TAR vs. FAR Graph

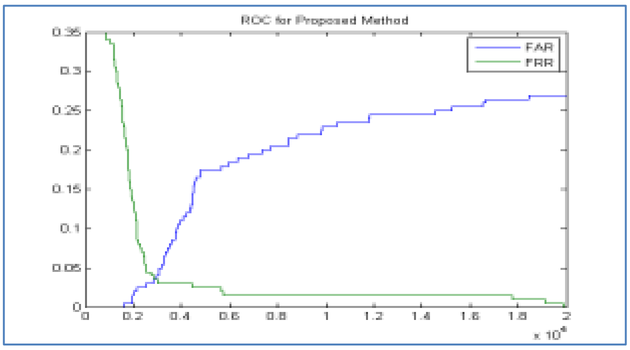

Fig 6: ROC Curve for proposed method with low EER

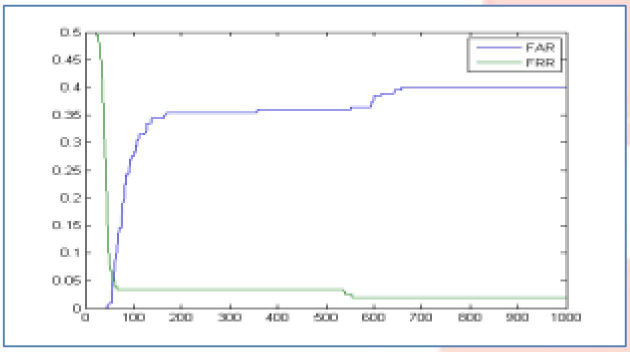

Fig 7: ROC Curve for base method with high EER

	Base Method	Proposed Method
TAR	**0.95**	**0.97**
FAR	**0.05**	**0.05**

Table 1: TAR & FAR of Base Method and Purposed Method

	Base Method	Proposed Method
EER	**0.05**	**0.03**

Table 2: EER of Base Method and Purposed Method

V. CONCLUSION

In this paper, it can be concluded that the proposed approach increases the system security to great extent. Thus modifying the system and also enhancing the accuracy of the system. It can be noted that EER is less than the existing system and TAR of the system is higher. The future work may be deal in area to enhance precision so as to further reduce the cases of false acceptance.

VI. REFERENCES

[1] Jacques Swanepoel and Johanner Coetzer, "Writer-specific dissimilarity normalisation for improved writer-independent off-line signature verification", IEEE International Conference on Frontiers in Handwriting Recognition, pp 393-398, 2012.
[2] Sheikh Faisal Misskhat, Mahamud Ridwan, Ehtesham Chowdhury, Saami Rahman and M. Ashraful Amin, "Profound impact of artificial neural networks and gaussian SVM kernel on distinctive feature set for offline signature verification", IEEE International Conference on Informatics, Electronics and Vision, pp 940-945, 2012.

[3] Karam Singh, and Guneet Mander. "Discrete fractional cosine transform based online handwritten signature verification." In Engineering and Computational Sciences (RAECS), 2014 Recent Advances in, pp. 1-6. IEEE, 2014.

[4] Krzysztof, and Marcin Zalasiński. "On-line signature verification using vertical signature partitioning." Expert Systems with Applications 41, no. 9 (2014): 4170-4180.

[6] Zhihua Yang, and Lihua Yang. "Online signature verification based on dct and sparse representation." Cybernetics, IEEE Transactions on 45, no. 11 (2015): 2498-2511.

[7] Muhammad Imran, Marcus Liwicki, Andreas Dengel, Seiichi Uchida, and Volkmar Frinken. "Automatic signature stability analysis and verification using local features." In Frontiers in Handwriting Recognition (ICFHR), 2014 14th International Conference on, pp. 621-626. IEEE, 2014.

[8] 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. IEEE, 2015.

[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 Hoseyn Sigari and Hamid Reza Pourreza, "Offline handwritten signature identification and verification using contourlet transform", 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] Md Asraful Haque 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.