OPTIMIZED MULTI MODEL SYSTEM FOR ONLINE SIGNATURE VERIFICATION

Poonam Chaudhary[1], Vijay Kumar Singh[2]

[1] *Student, Computer Science and Engineering Department, SIET Sunder Nagar, H.P., India*
[2]*Assistant Professor, Computer Science and Engineering Department, SIET Sunder Nagar, H.P., India*

Abstract

Handwritten signature is the most widely accepted biometric to identity verification. The proposed online handwritten signature verification system consists mainly of three phases: Signal preprocessing, feature extraction, and feature matching. Steps for verifying online handwritten signature in this system start with extracting dynamic data (x and y positions) of points that forming the signature. Pen-movement angles and speed are then derived from pen position data. To reduce variations in pen-position and pen-movement angles dimensionality, data is normalized. After that all the parameters are to be put in a single vector. Here in the proposed system five parameters are taken in to account. Features of the signature can be extracted using proposed feature extraction method. Corresponding to every signature a unique feature will be extracted and this will be quantized using quantization step size vector. Both the feature vector and quantization vector are to be stored using template generator. Further, during the matching phase, a different distance measuring algorithm has been implemented known as Minkowski distance which is helpful in improving the results.

Keywords: *Signal Processing, Feature Extraction, Signature Verification, Minkowski Distance.*

----------***----------

1. INTRODUCTION

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.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.

2. OBJECTIVE

The theme possesses the novel property of being strong against AN adjust chosen-message attack: A 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.

3. PROBLEM STATEMENT

To develop 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.

4. RESEARCH METHODOLOGY

4.1 Preprocessing

Preprocessing of the net signature is needed to get rid of the variations bestowed at the time of the signature was taken from the user. These variations will be owing to the lower resolution of the pill or the digital device that is employed to

accumulate the signature of an individual. These will be owing to the explanation if the reference signatures of the person square measure taken in numerous settings that square measure in dynamic or static environment.

4.2 Feature Extraction

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.

4.3 Guide Generation

A user guide is generated throughout the enrollment method wherever multiple signatures square measure non inheritable from a user and a feature set is computed from every of the samples. A pair comprising of step size vector and its associated feature vector guide is then keep and later wont to verify a claimed signature of the user u.

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

$$\mu_{f(i)}(u) = \left(\frac{1}{S}\right)\sum_{j=1}^{S} f^{Sj}(i) \tag{2}$$

$$\hat{f}^{(S_j|u)}(i) = \left[\frac{f^{Sj}(i)}{q^u + \epsilon}\right], \quad i = 1, \ldots, M \tag{3}$$

$$\bar{f}^u(i) = \frac{\sum_{j=1}^{S}\left(\hat{f}^{(S_j|u)}(i)\right)}{S}, \quad i = 1, \ldots, M \tag{4}$$

4.4 Signature Verification

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. Throughout verification, only if t is claimed to be an internet signature sample from user u, $\hat{F}^{(t|u)}$ is calculated exploitation Q^u. Then the system derives a dissimilar score exploitation Manhattan distance between $\bar{f}^u(i)$ and $\hat{F}^{(t|u)}$ as,

$$Score = \Sigma_i (i = 1)^{\dagger} M \overline{\equiv} \left[|F^{\dagger}(t|u) \right] - (f^{\dagger} u)^{\cdot\cdot}(i)| \tag{5}$$

4.5 Signature Authentication

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. These square measure failing makes an attempt and user rejections. This kind results in a rise in average variety of makes an attempt for prospering authentication whereas the second results in a rise in user rejection rate.

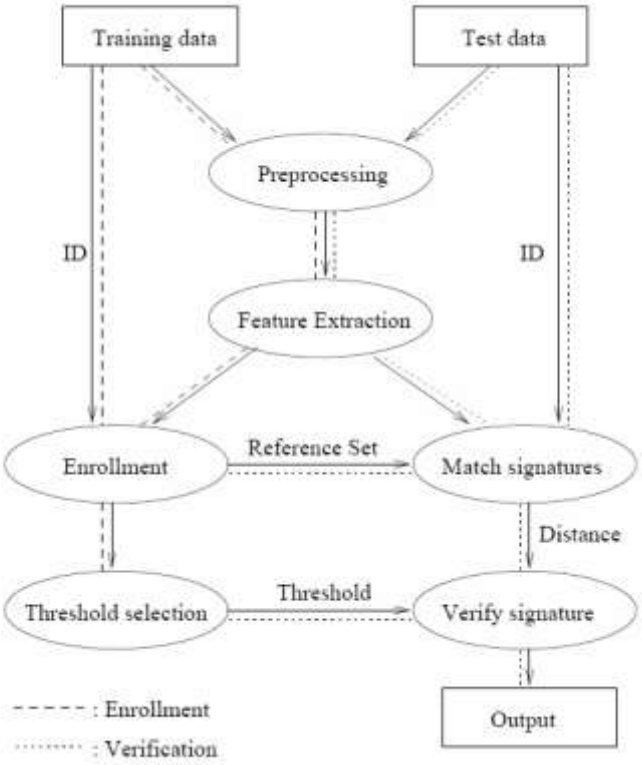

Fig. 1 Flow chart of the approach

5. PROPOSED METHODOLOGY

The distance measures are helpful techniques that are employed in a good vary of applications like fuzzy pure mathematics, multi criteria higher cognitive process, business choices, etc. Among the nice style of the distances, the mathematician distance represents a generalization to a good vary of them like the acting distance, the geometrician distance, the geometric distance and also the harmonic distance.

The mathematician distance may be a metric during a normed vector area which might be thought-about as a generalization of each the geometrician distance and also the Manhattan distance.

The mathematician distance of order p between 2 points.

$$X = (x_1, x_2, \ldots, x_n) \text{ and } Y = (y_1, y_2, \ldots, y_n) \in \mathbb{R}^n \quad (6)$$

Is defined as

$$\left(\sum_{i=1}^{n} |x_i - y_i|^p \right)^{1/p} \quad (7)$$

For p > 1, the mathematician distance may be a metric as a result of the Minkowski difference. When p<1, the space between (0,0) and (1,1) is 21/p>;2, however the purpose (0,1) is at a distance one from each of those points. Since this violates constellation difference, for p & 1 it's not a metric.

Minkowski distance is usually used with p being one or two. The latter is that the geometrician distance, whereas the previous is typically referred to as the Manhattan distance. Within the limiting case of p reaching time, we have a tendency to get the Chebyshev distance:

$$\lim_{p \to \infty} \left(\sum_{i=1}^{n} |x_i - y_i|^p \right)^{\frac{1}{p}} = \max_{i=1}^{n} |x_i - y_i|. \quad (8)$$

Similarly, for p reaching negative time, we have:

$$\lim_{p \to -\infty} \left(\sum_{i=1}^{n} |x_i - y_i|^p \right)^{\frac{1}{p}} = \min_{i=1}^{n} |x_i - y_i|. \quad (9)$$

The mathematician distance can even be viewed as a multiple of the facility mean of the component-wise variations between P and Q.

6. RESULTS

The results are shown as below:

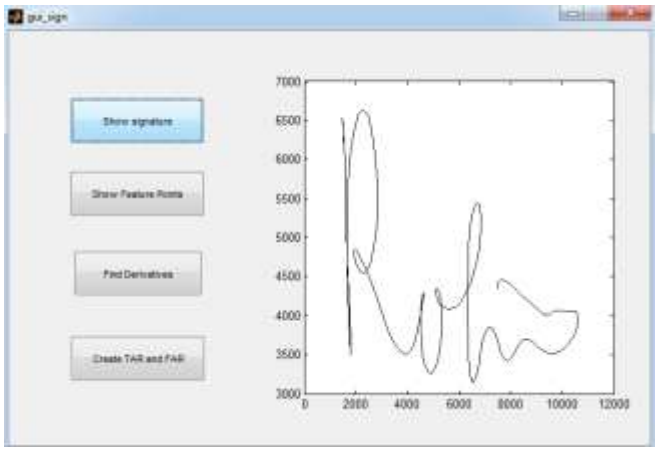

Fig 2. A sample signature from the dataset

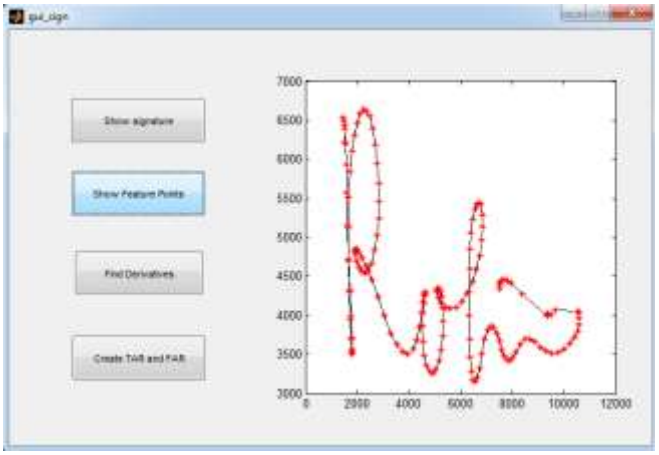

Fig 3. Feature points extracted from the sample signature.

In the figure 4.2, the features has been extracted of sample signature to further processing. The feature extraction algorithm has been applied to extract the features of sample signature.

The below figures shows the result after applying the proposed methodology in various terms.

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.

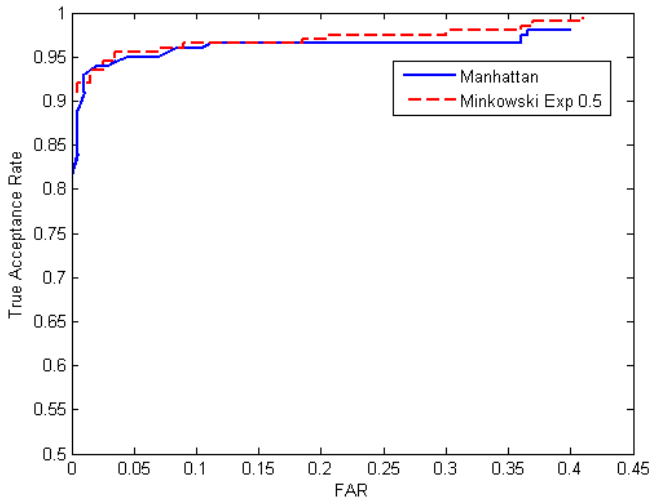

Fig 4 Results comparison of Original and Proposed methodology in terms of TAR vs. FAR Graph plot

7. CONCLUSION

In our study we analyze the challenges in the recognition accuracy 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 fauls acceptance rate and fault rejection rate low and make the mobile commerce payment transactions highly secure and reliable.

8. FUTURE SCOPE

The future scope of this work is to increase the performance of the proposed algorithm with the help of multi biometric system.

REFERENCES

[1]. ArgonesRua, Enrique, and José Luis Alba Castro. "Online signature verification based on Generative models." *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on* 42.4 (2012): 1231-1242.

[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]. 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 Frontier Handwriting Recognit., Oct. 2004, pp. 179–184, IEEE Comput. Society Press.

[4]. Jacques Swanepoel and JohannerCoetzer, "Writer-specific dissimilarity normalisation for improved writer-independent off-line signature verification", IEEE International Conference on Frontiers in Handwriting Recognition, pp 393-398, 2012.

[5]. Liu, Yishu, Zhihua Yang, and Lihua Yang. "Online Signature Verification Based on DCT and Sparse Representation." (2014).

[6]. Muhammad Reza Pourshahabi, MohamadHoseynSigari 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.

[7]. Shah, Vaibhav, UmangSanghavi, and Udit Shah. "Off-line signature verification using curve fitting algorithm with neural networks." *Advances in Technology and Engineering (ICATE), 2013 International Conference on*. IEEE, 2013.

[8]. 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.

[9]. G. Dimauro, S. Impedovo, M. G. Lucchese, R. Modugno, and G. Pirlo, “Recent advancements in automatic signature verification,” in Proc. 9th Int. Workshop