EPH - International Journal of Science And Engineering
ISSN (Online): 2454 2016
Volume 03 Issue 01 March 2017

DOI: https://doi.org/10.53555/eijse.v3i1.43

ONLINE SIGNATURE VERIFICATION SYSTEM ON MOBILE DEVICES FOR EFFECTIVE AND SECURE BIOMETRIC

Sandeep Singh[1]*, Sandeep Kaur[2]
*[1,2]*Department of Electronics & Communication Engineering GVIET, Ramnagar,Banur, Punjab, India*
[2]*Email: Sandeepbhullar647@gmail.com*

Corresponding Author:-
Email: Gillsandeep419@gmail.com

Abstract:-
Handwritten signature is that the most generally accepted biometric to biometric identification. The projected on-line written signature verification system consists principally of 3 phases: Signal preprocessing, feature extraction, and have matching. Steps for confirming on-line written signature during this system begin with extracting dynamic knowledge (x and y positions) of points that forming the signature. Pen-movement angles and speed square measure then derived from pen position knowledge. To scale back variations in pen-position and pen-movement angles spatial property, knowledge is normalized. Options of the signature will be extracted victimization projected feature extraction methodology. Such as each signature a novel feature are extracted and this can be amount victimization quantization step size vector. To verify the check signature Manhattan distance (score) are taken between the check signature and therefore the reference signature. If score is a smaller amount than the predefined threshold then the check signature same is claimed to be real signature and if score is over the predefined threshold then it's said to be cast signature.

Keywords: - *Signal preprocessing, feature extraction, Biometric signature*

I. 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 must n'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.

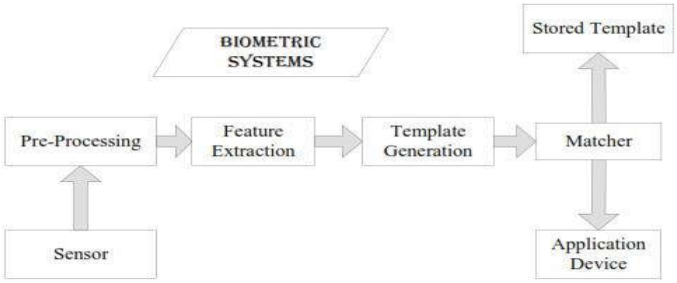

Figure1. Biometric System

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). In the point of view of adaption in the market place, signature verification presents three likely advantages over other biometrics techniques.

1. 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.
3. 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. 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.

Off-line signatures systems usually may have noise, because of scanning hardware or paper background, and contain less discriminative information since only the image of the signature is the input to the system. While genuine signatures of the same person may slightly change, the differences between a forgery and a genuine signatures may be difficult, which make automatic off-line signature verification be a very challenging pattern recognition problem. In addition, the difference in pen widths and unpredictable change in signature's aspect ratio are other difficulties of the problem. It is worth to notice the fact that even professional forensic examiners perform at about 70% of correct signature classification rate (genuine or forgery).Unlike offline, On-line signatures are more unique and difficult to forge than their counterparts are, since in addition to the shape information, dynamic features like speed, pressure, and capture time of each point on the signature trajectory are available to be involved in the classification. As a result, on-line signature verification is more reliable than the off-line.

Biometric system also has some of demerits and this system of verification is nor workable in all kind of circumstances. Some demerits are given as:

1. Biometric system is a costly identification solution.
2. Biometric system may not correctly work in the environment where there is too much noise. Additionally, it is noted that voice of human being changes at different level of ages and it also changes due some throat infection or flu infection. Due to this variation in voice, biometric system will not accurately work.
3. The finger prints of those people, who working in Chemical industries are often affected. Therefore those companies should not use the finger print mode of authentication.
4. 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, than no other thing can take its place.

II LITERATURE REVIEW

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 [1]. 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.

Approaches to signature verification are 2 classes in step with the acquisition of the data: On-line [2] 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 [3, 4, 5]. 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 [1, 6]. The system ought to neither be too sensitive nor too coarse. It ought to have a suitable trade-off between an occasional False Acceptance Rate (FAR) and an occasional False Rejection Rate (FRR). The false rejection rate (FRR) and therefore the false acceptance rate (FAR) square measure used as quality performance measures. The FRR is that the magnitude relation of the amount of real check signatures rejected to the full number of real check signatures submitted. The way is that the magnitude relation of the quantity of forgeries accepted to the full number of forgeries submitted. Once the choice threshold is altered thus on decrease the FRR, the way can invariably increase, and contrariwise.

Argones Rua, Enrique, and José Luis Alba socialist [1] and Rodríguez-Serrano, José A., associate degreed Florent Perronnin [3] bestowed an approach exploitation the hidden Markov models (HMMs) in 2 completely different modes: user-specific HMM (US-HMM) and user-adapted universal background models (UBMs) (UA-UBMs) and Comparisons to alternative progressive systems, from the ESRA 2011 signature analysis contest, also are rumored. Tian, Wei, and Jingyuan cardinal [2], Nemmour, Hassiba, and Youcef Chibani [4], Shah, Vaibhav, Umang Sanghavi, and Udit monarch [5], Pushpalatha, K. N., A. K. Gautam, and K. B. Kumar [5] 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.

Boutellaa, Elhocine, Messaoud Bengherabi, and Farid Harizi [5] 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. A comparative study is projected by Zareen, Farhana Javed, and Suraiya Jabin [6] for the prevailing ways. Pirlo, Giuseppe, and Donato Impedovo [7], have used the optical flow technique so as to develop the system however eventually it's a computationally valuable approach. Smejkal, Vladimir, and Jindrich Kodl [9], Liu, Yishu, Zhihua rule, and Lihua rule [10], Ribeiro, Bernardete, Noel Lopes, and Joao Goncalves [11], and López-García, Mariano, et al. [12] approached to a additional real time implementation with the employment of techniques like GPU, embedded systems and alternative hardwares. Wibowo, Canggih Puspo, Pitak Thumwarin, and Takenobu Matsuura [14] 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 [15] evolved a method that uses position similarly as pressure terms for secure guide that uses a mixture of 1D and 2nd histograms.

III. Experiment and result

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 with respect 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:

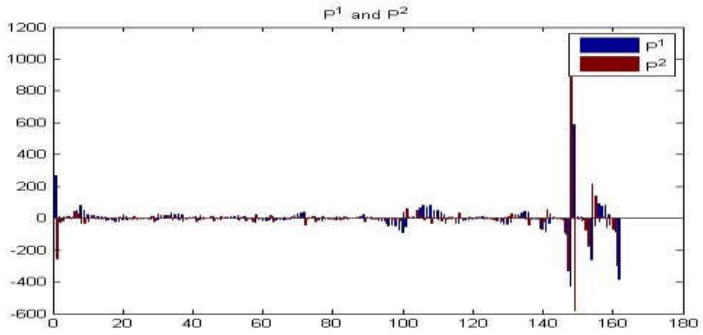

Figure 4.1: Derivative for pressure

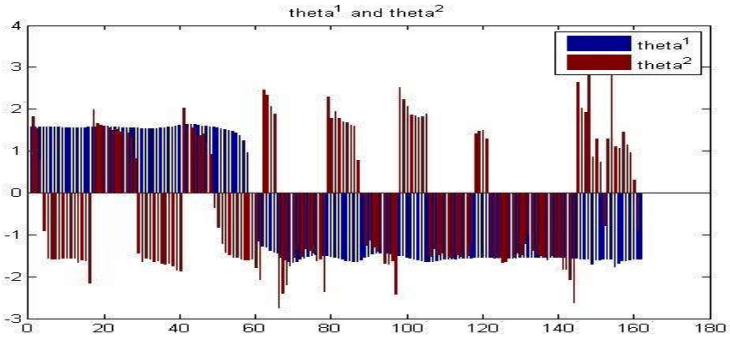

Figure 4.2: Derivative for Theta

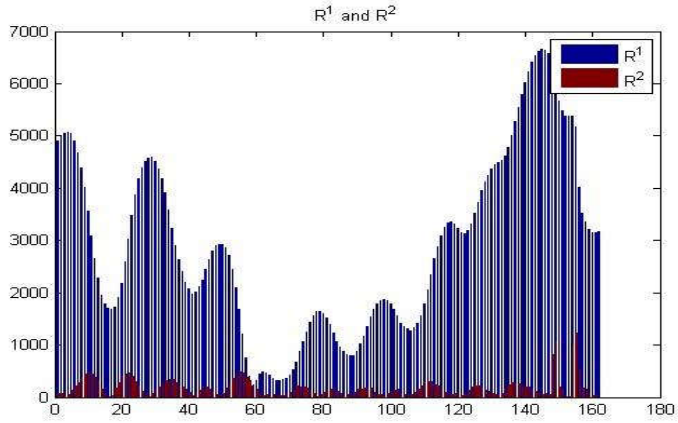

Figure 4.3: Derivative for velocity

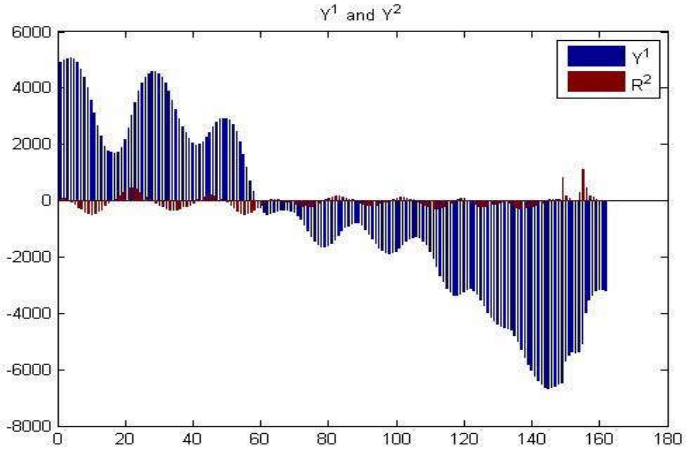

Figure 4.4: Derivative for Y coordinate

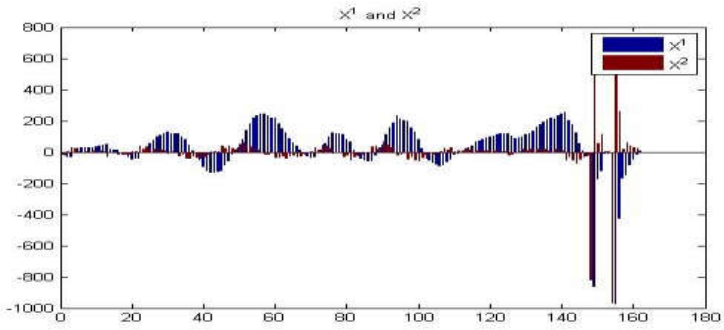

Figure 4.5: Derivative for X coordinate

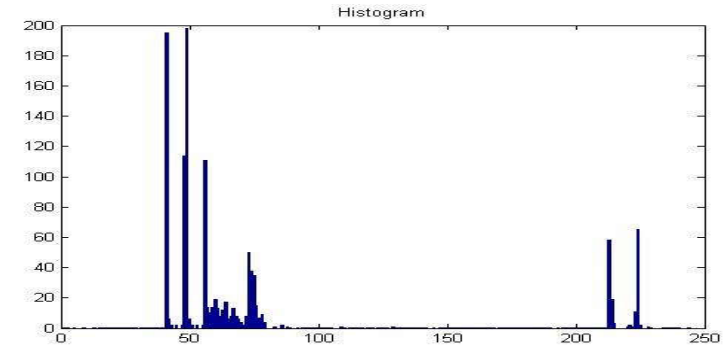

Figure 4.6: Histogram of all the features.

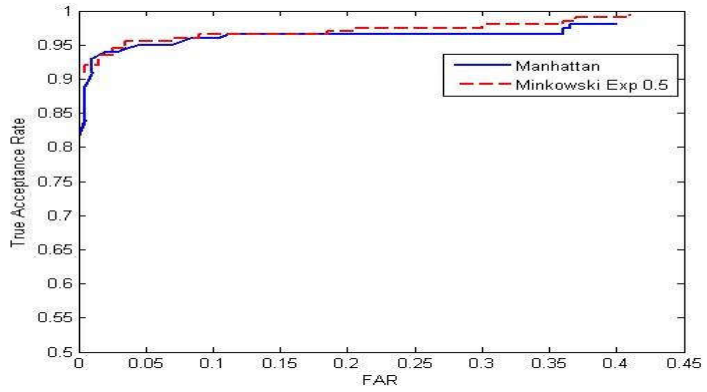

Fig. 4.7 Tru Acceptance rate vs FAR

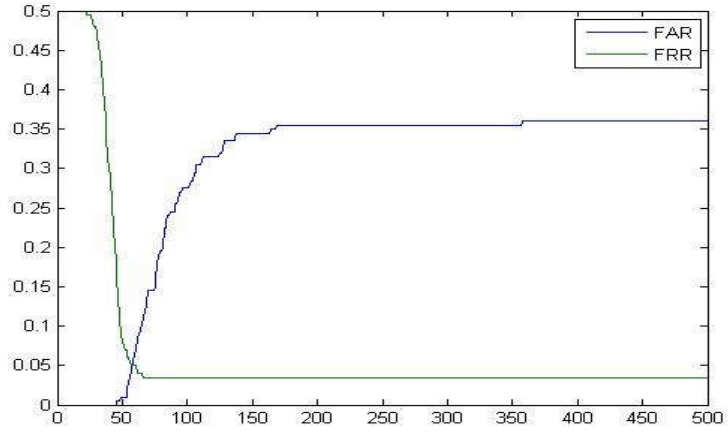

Fig. 4.8 FAR and FRR compared.

The results presented here, show that the GAR is improved in a better way in comparison to the previous method due to the inclusion of Minkowski distance for similarity measure. This also adds up to the diversity as many number of templates can be generated using the different combination and hence their similarity can be measured using the new method. This increases the overall efficiency of the system.

Table 1. TAR/GAR comparison

	Base Method	Proposed Method
TAR	**0.94**	**0.955**
FAR	**0.05**	**0.05**

IV CONCLUSION AND FUTURE SCOPE

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. 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.

V. REFERENCE

[1]. Argones Rua, 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]. Tian, Wei, and Jingyuan Lv. "A new affine registration algorithm applied to off-line signature verification." Information and Automation (ICIA), 2012 International Conference on. IEEE, 2012.

[3]. Rodríguez-Serrano, José A., and Florent Perronnin. "A model-based sequence similarity with application to handwritten word spotting." Pattern Analysis and Machine Intelligence, IEEE Transactions on 34.11 (2012): 21082120.

[4]. Nemmour, Hassiba, and Youcef Chibani. "Off-line signature verification using artificial immune recognition system." Electronics, Computer and Computation (ICECCO), 2013 International Conference on. IEEE, 2013.

[5]. Boutellaa, Elhocine, Messaoud Bengherabi, and Farid Harizi. "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.

[6]. Zareen, Farhana Javed, and Suraiya Jabin. "A comparative study of the recent trends in biometric signature verification." Contemporary Computing (IC3), 2013 Sixth International Conference on. IEEE, 2013.

[7]. Pirlo, Giuseppe, and Donato Impedovo. "Verification of static signatures by optical flow analysis." Human Machine Systems, IEEE Transactions on 43.5 (2013): 499-505.

[8]. Shah, Vaibhav, Umang Sanghavi, 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.

[9]. Smejkal, Vladimir, and Jindrich Kodl. "Implementing trustworthy dynamic biometric signature according to the electronic signature regulations." Security Technology (ICCST), 2013 47th International Carnahan Conference on. IEEE, 2013.

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

[11]. Ribeiro, Bernardete, Noel Lopes, and Joao Goncalves. "Signature identification via efficient feature selection and GPU-based SVM classifier." Neural Networks (IJCNN), 2014 International Joint Conference on. IEEE, 2014. [12]

[12]. López-García, Mariano, et al. "Embedded System for Biometric Online Signature Verification." Industrial Informatics, IEEE Transactions on 10.1 (2014): 491-501.

[13]. Pushpalatha, K. N., A. K. Gautam, and K. B. Kumar. "Offline signature verification based on contourlet transform and textural features using HMM."Recent Advances and Innovations in Engineering (ICRAIE), 2014. IEEE, 2014.

[14]. Wibowo, Canggih Puspo, Pitak Thumwarin, and Takenobu Matsuura. "On-line signature verification based on forward and backward variances of signature. “Information and Communication Technology, Electronic and Electrical Engineering (JICTEE), 2014 4th Joint International Conference on. IEEE, 2014.

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

[16]. 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-