iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Analytical Analysis on Signature Recognition and Verification

Jasmeet Kaur[1], Dr. Reecha Sharma[2]
[1,2] UCOE Department, Punjabi University

Abstract: ***Handwritten signature verification system is one of the for most reliable, fast and cost-effective tool for user endorsement. This work examines the online written signature verification system methodologies. Signatures are acquired from devices such as pressure sensitive tablets, digitizer, etc. The aim of this paper is to review the signature feature extraction algorithms, techniques and methodologies. This gives a short description of the performance analysis parameters. The performance of algorithms is compared using varied factors which embody the False Acceptance Rate (FAR), False Reject Rate (FRR) and Equal Error Rate (EER) etc.***
Keywords: signature verification, forgery, False Acceptance Rate, False Rejection Rate, Equal Error Rate.

I. INTRODUCTION

Biometrics centered confirmation methods are enhanced methods with regards to protection than conventional verification techniques such as passwords etc. It is due to the fact that fingerprint features of every person are exclusive and cannot be lost, thieved or damaged. There are two kinds of biometrics: Behavioral Physical. Handwriting, speech etc. come under behavior biometrics. Eye design, finger marks etc. are part of physiological biometrics. The signatures are used in cheques, lawful dealings etc to find the personal identification. The legalisation of any papers occurs by placing a signature on it. This issue can be worked in two ways: On line signature verification & Off-line signature verification. In some dealings online signatures are used where the consumer includes a pen centered product. The customer has to do his signature on that product then that signature will be documented in the system/computer. Signature velocity, pen stress, pen downs & pen ups will be taken by the product & sent to the system/computer. Then it will confirm with the data source whether it is reputable or made one. On the other side offline signature is the one which can be found by deciding upon on the simple document & then checking it to the pc. Now the program will assess whether it is a authentic or made one. Off-line signature does not have any particular components whereas online signatures degree of lot of components & application to figure out reliability.

A. Types of Forgeries

Forgery indicates duplicating, changing or falsifying written matter for the objective of defrauding others.

1)Unique forgery: It is created when the signer knows the name of the sufferer and creates the signature in his own design. This forgery is definitely recognized by visual analysis. Random duplicates are established without any information of the signature's form.

2)Simulation Forgery: The forger has accessibility to a model of the authentic signature from which he methods making copies

3) Unskilled forgery: It is created when the signer copies the signature in his own design without having any previous encounter. They are produced by understanding the name of the signer but without having an example of signer's signature.

4) Skilled forgery: It is produced by looking at the original signature or by having understanding of the signature of the sufferer. Usually this type of forgery is produced by professional individuals who have encounter in duplicating the signature.

5) Tracing Forgery: The following forgery has one of the authentic trademark, which he may keep against a screen, or use as well as document or a mild box, make another piece of paper over the top, and basically track the road.

6) Cut-and-paste Forgery: A authentic signature is cut from one papers and placed on the unwarranted papers, then photocopied. If mild and quality is properly adjusted, the papers will appear authentic.

7)Electronic Forgery: The forgery basically digitizes a genuine signature by checking at a great quality, then inserts it into the unwarranted papers and printing it.

8)Free hand signature Forgery: The forger basically writes the victim's name without coming to a effort to duplicate.

False Acceptance Rate : The possibility that the program wrongly suits the feedback design to a non-matching design in the data source.

$$FAR = \frac{no.\ of\ non\ samples\ classified\ as\ samples}{total\ no.\ of\ samples\ in\ database}$$

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

False Rejection Rate: the possibility that the program is unable to identify a match between the feedback design and a related design in the data source.

$$FRR = \frac{no.\ of\ samples\ classified\ as\ non\ samples}{total\ no\ samples\ in\ database}$$

Equal Error Rate (EER): is the location on a ROC or Detection Error Trade-off curve where the FAR and FRR are equal. As the value of EER increase, the performance of the system gets decrease.

$$EER = \frac{no.of\ samples\ correctly\ classified\ in\ database}{total\ no.of\ samples\ in\ database}$$

II. SIGNATURE VERIFICATION CONCEPT

The verification and identification of off-line signature contains following actions.

A. Acquisition

The data obtain can be done in two way first way we can take the details source of signature which is available on internet. Second way tests the signature picture to change it into electronic picture.

B. Image Pre-Processing

In picture pre-processing, different function are execute on signature picture such as transformation from shade picture to gray image, eliminate disturbance, thresholding, loss, boundary detection and farming. In binary one picture is converted into grayscale picture that is the pixel of signature would be "1" and pixel of qualifications would be "o". Due to these function removal is very simple. Background delimitation and disturbance decrease is conducted in those images which are produced from some other records. Skeletonization gives a bones of 2-D binary picture which can be prepared.

C. Feature Extraction

In function removal level, we draw out some functions of signature picture. Different methods are used to draw out the features. Extracted popular functions of signature picture in this level are the information of coaching and identification level. The options can be categorized as international, collections and cover up functions. Global features provide wavelet coefficient, Fourier coefficients. Mask features provides details about guidelines of the collections of the information. The collection of set of functions is in signature verification techniques because the functions used must be appropriate for the applying.

D. Classification

When a new signature is applied, attributes are extracted and matched with those already stored in the database. If the functions are matched than it is categorized as genuine otherwise forge.

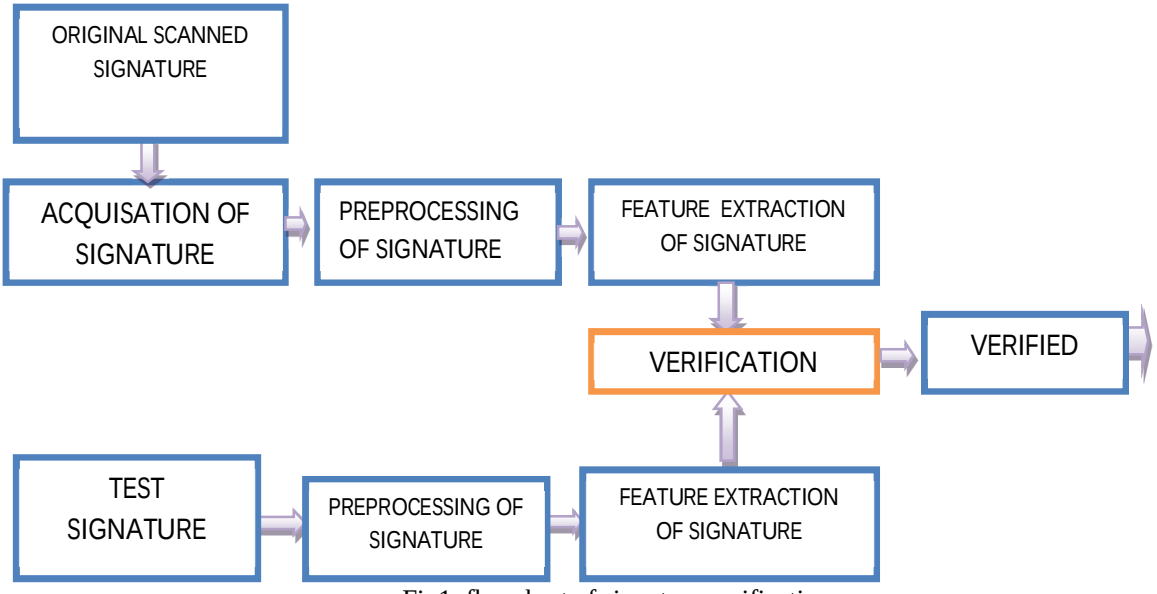


Fig1: flowchart of signature verification

©IJRASET: All Rights are Reserved

III. RELATED WORK

A.Piyush Shanker, A.N. Rajagopalan suggested a signature verification system depending on Dynamic Time warping (DTW). The technique works by extracting the vertical projection characteristic from signature images and by comparing reference and probe feature templates using flexible matching. Modifications were made to the standard DTW algorithm to account for the stability of the various parts of a signature. The standard DTW and the modified DTW methods were tested on a signature database of 100 people. The modified DTW technique, which incorporates stability of signature components, with an equal-error-rate of only 2% whereas for the standard DTW technique EER was 29%.[1]

Marcos Faundez-Zanuy, studied signature recognition techniques for on-line signature recognition which were vector quantization (VQ), nearest neighbor(NN), dynamic time warping (DTW) and hidden Markov models (HMM).Using a database of 330 users which includes 25 skilled forgeries performed by five different impostors. Experimental results showed that his proposed combination of VQ and DTW (by means of score fusion) performed significantly better than other algorithms (DTW, HMM) and achieved an equal error rate of 1.37% in case of random forgeries and 5.42% in case of skilled forgeries.

Dr. S. Adebayo Daramola and Prof. T. Samuel Ibiyemi, proposed a signature recognition technique for offline signatures using Discrete Cosine Transform (DCT) and Hidden Markov Model(HMM). The signature to be trained or recognized was vertically divided into segments at the centre of gravity using the space reference positions of the pixels. The number of segmented blocks of signature were equal to the number of states in the HMM .Experimental result showed that successful signatures recognition rates of 99.2% was possible. The result was better in comparison with previous related systems based on HMM and statistical classifiers.[2]

. J. Co etzer,B. M . Herbst and J. A. du Preez, developed a system that automatically recognizes offline signatures using discrete Radon transform (DRT) and a hidden Markov model (HMM). Using a database of 924 signatures from 22 writers which were captured offline, the system achieved an equal error rate (EER) of 18% when only skilled forgeries were considered and an EER of 4.5% in the case of only random forgeries. Using another database of 4800 signatures from 51 writers, our system achieves an EER of 12.2% for skilled forgeries. These signatures were originally captured online and then digitally converted into offline signature images.

Bao Ly Van, Sonia Garcia-Salicetti, and Bernadette Dorizzi, presented a signature verification system based on the fusion of scores issuing from a continuous HMM.They exploited the complementarity of two sorts of information, provided by the likelihood and the segmentation(Viterbi Path) of the HMM modeling a given writer. The improvement obtained with the Fusion System was of 26%using the segmentation information given by an HMM .It resulted not only in a better characterization of a writer's signature but also in a more effective detection of forgeries. relatively to the Likelihood System.[3]

Christian Gruber, Thiemo Gruber, Sebastian Krinninger, and Bernhard Sick, proposed a technique that integrates a longest common sub sequences (LCSS) detection method which measures the similarity of signature time series into a kernel function for support vector machines (SVM). A proprietary database with signatures of 153 test persons and the SVC 2004 benchmark database were used to show the properties of the new SVM-LCSS. They investigated its parameterization and compared it to SVM with other kernel functions such as dynamic time warping (DTW). Experiments showed that SVM with the LCSS kernel authenticated the persons very efficiently and with a performance which was significantly better than that of the best comparing technique, SVM with DTW kernel.[4]

Nilesh Y. Choudhary,Mrs. Rupal Patil, Dr. Umesh. Bhadade, Prof. Bhupendra M Chaudhari, proposed a scheme for off-line signature recognition & verification using back propagation neural network ,where the signature was captured and presented to the user in an image format. Signatures were verified based on features which were extracted from the signature using Invariant Central Moment and Modified Zernike moment for its invariant feature extraction.The recognition system gives the 98% success rate by the all signature pattern correctly for all that signatures which were used in training. It gives the poor performance for signature that is not in the training phase.[5]

Hao Chang , Daoming Dai , Pingshui Wang , Yong Xu Fengshan Si , Shuqin Huang, proposed a method to verify online signatures using wavelet transform. Firstly, signature data were preprocessed using normalizing and debouncing. Then wavelet transform was used for extraction of features. At last, experiments were carried out on Signature Verification Competition 2004 to verify the reliability, feasibility and performance of the approach. Equal error rate reached by 4.87% and compress ratio was achieved nearly by 5.93, which was superior to the average performance of SVC 2004. Moreover,this method saves computation time and reduces data volume.[6]

Napa Sae-Bae and Nasir Memon,proposed a simple and effective online signature verification system that was suitable for user

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653

authentication on a mobile device. Its benefits were,firstly, a histogram based feature set for representing an online signature can be derived in linear time and the system required a small and fixed-size space to store thesignature template[7]. In addition, since the feature set represents only statistics about distribution of original online signature attributes, the transformation was non-invertible. As a result, the privacy of the original biometric data was well-protected. Secondly, a user-specific classifier comprising of a user-specific quantization step size vector and its associated quantized feature vector can be trained using only enrollment samples from that user without requiring a training set from a large number of users. Several experiments performed on MCYT and SUSIG datasets demonstrate effectiveness of the proposed method in terms of verification performance as compared to existing algorithms.

IV. COMPARISION OF RECOGNITION RATES

TABLE I comparison and results

Features & Classifiers	Dataset Users/Sig	Results
Dynamic time warping	100 sign	EER=2%
V Q - Dynamic time warping	330 sign 25 skilled forgery	DCF=1.37%Random forgery DCF=5.42% Skilled forgery Accuracy=99%
DCT-HMM	500 sign	Accuracy=99.2%
DRT-HMM	924 sign 4800 sign	EER=18% EER=12.2%
SVM-EUCLID	SVC 2004	EER=13.84% Skilled forgery EER=1.11% Random forgery
SVM-DTW	SVC 2004	EER=6.06% Skilled forgery EER=3.27% Random forgery
SVM-LCSS	SVC 2004	EER=6.84% Skilled forgery EER=0.12% Random forgery
Bp-NN	672 sign	Accuracy=98%
Wavlet Transform method	SVC 2004	EER=4.87%

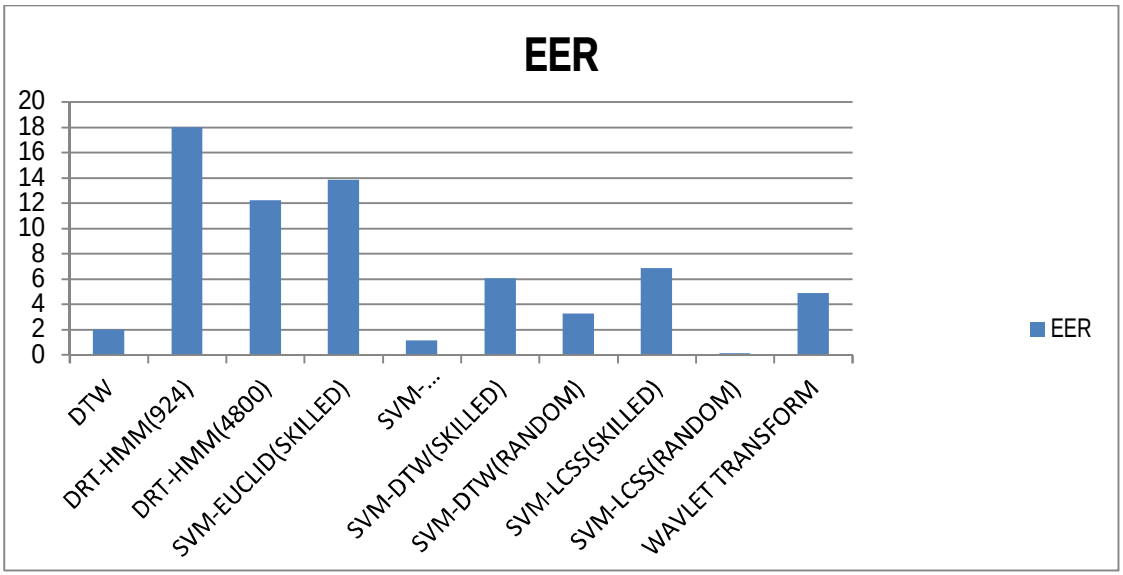


Fig2: comparison on basis of EER

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

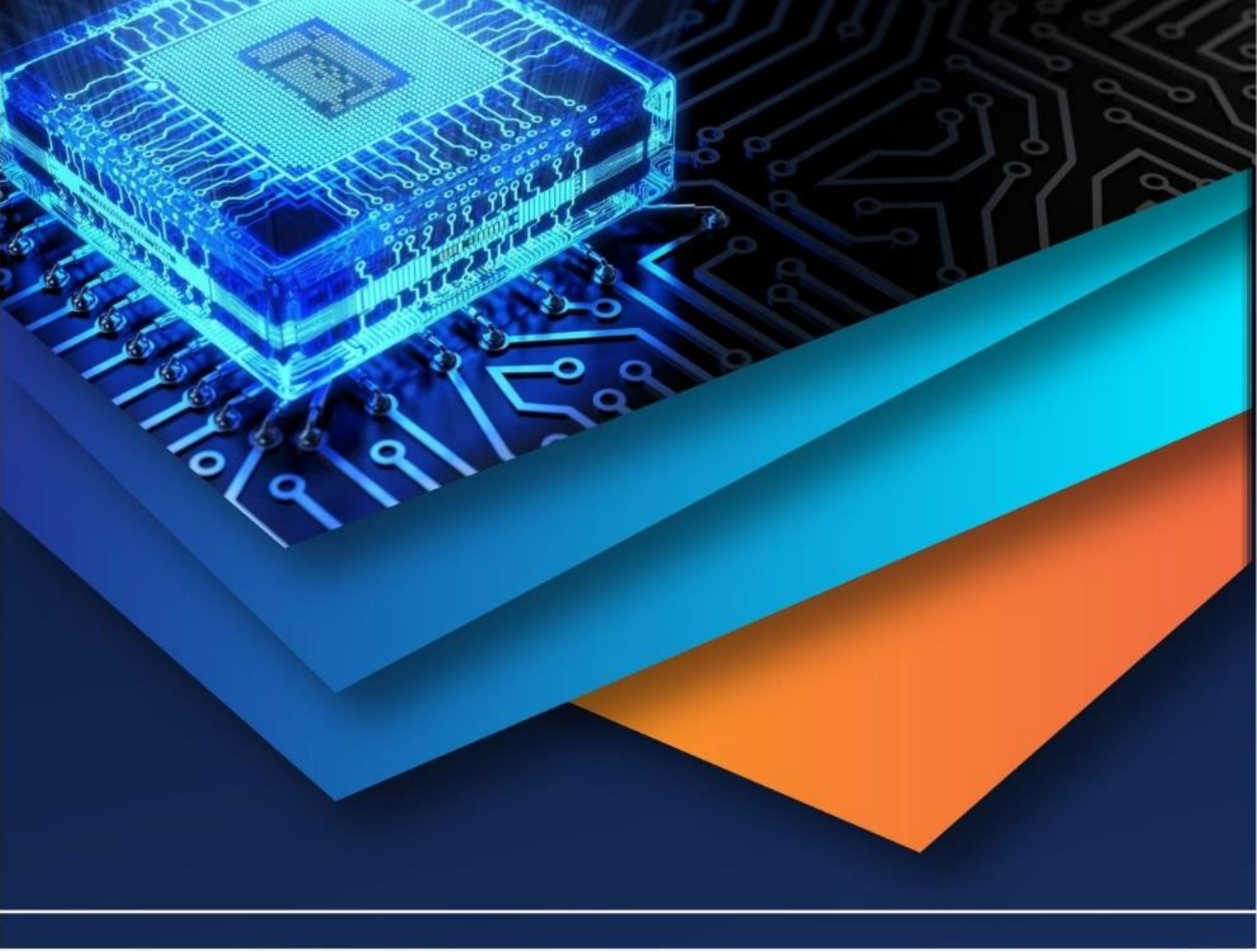
V. CONCLUSION

It is noticed that, despite the wide work conducted for off-line & online signature verification, there are still many difficulties in this research place. Signatures may be published in different 'languages' and need to carry out a thorough study on this. One problem of this is, for security reasons, it is not easy to get a signature dataset of actual signatures (such as financial documents) available to the signature verification system. Openly accessibility to signature datasets of actual records would make it possible to determine a common analysis method in order to perform relative research Scientists have used different features for signature verification. Mixture of different classifiers as well as new classifiers should be researched later on try to boost efficiency.

REFERENCES

[1] Shanker, A. Piyush, and A. N. Rajagopalan. "Off-line signature verification using DTW." Pattern recognition letters 28.12 (2007): 1407-1414.
[2] Daramola, S. Adebayo, and T. Samuel Ibiyemi. "Offline signature recognition using hidden markov model (HMM)." International journal of computer applications 10.2 (2010): 17-22.
[3] Van, Bao Ly, Sonia Garcia-Salicetti, and Bernadette Dorizzi. "On using the Viterbi path along with HMM likelihood information for online signature verification." Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on 37.5 (2007): 1237-1247
[4] Gruber, Christian, et al. "Online signature verification with support vector machines based on LCSS kernel functions." Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on 40.4 (2010): 1088-1100.
[5] Nilesh Y.Chaudhary, et al. "Signature Recognition & Verification System Using Back Propagation Neural Network." International Journal of IT, Engineering and Applied Sciences Research 2.1 (2013).
[6] Sia, Fengshan, and Shuqin Huanga. "Online Signature Verification Using Wavelet Transform of Feature Function⋆." (2012)
[7] -Bae, Napa, and Nasir Memon. "Online signature verification on mobile devices." Information Forensics and Security, IEEE Transactions on 9.6 (2014): 933-947
[8] Singh, Jyoti, and Dr Manisha Sharma. "A Survey on Offline Signature Recognition and Verification Schemes." IOSR Journal of Electronics and Communication Engineering (IOSRJECE) ISSN: 2278-2834.
[9] Dewan, Upasana, and Javed Ashraf. "Offline signature verification using neural network." International Journal Of Computational Engineering & Management (IJCEM) 15.4 (2012): 50-54
[10] Gomez-Barrero, Marta, Javier Galbally, Julian Fierrez, Javier Ortega-Garcia, and Réjean Plamondon. "Enhanced on-line signature verification based on skilled forgery detection using Sigma-LogNormal Features." In 2015 International Conference on Biometrics (ICB), pp. 501-506. IEEE, 2015.
[11] Bhattacharya, Indrajit, Prabir Ghosh, and Swarup Biswas. "Offline signature verification using pixel matching technique." Procedia Technology 10 (2013): 970-977.
[12] Impedovo, Donato, and Giuseppe Pirlo. "Automatic signature verification: the state of the art." IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 38.5 (2008): 609-635
[13]]A. Abu-Rezq and A. S. Tolba, "Cooperative self-organizing maps for signature verification," in Proc. Image Anal. Inf. Fusion (IAIF 1997),H. Pan, M. Brooks, D. McMichael, and G. Newsam, Eds., pp. 391–402.
[14] A. Abu-Rezq and A. S. Tolba, "Cooperative self-organizing maps for consistency checking and signature verification," Digit. Signal Process., vol. 9, pp. 107–119, 1999.
[15] Y. Chen and X. Ding, "On-line signature verification using direction sequence string matching," Proc. SPIE, vol. 4875, pp. 744–749, Jul. 200
[16] Y. Chen and X. Ding, "Sequence-matching-based feature extraction with applications to signature verification," Proc. SPIE, vol. 5676, pp. 76–83, Jan. 2005
[17] P. S. Deng, H.-Y. M. Liao, C. W. Ho, and H.-R. Tyan, "Wavelet-based offline handwritten signature verification," Comput. Vis. Image Underst., vol. 76, no. 3, pp. 173–190, Dec. 1999.
[18] kalera M.K., Srihari S., Xu A., Offline signature verification and identification using distance statistics, International Journal of Pattern Recognition and Artificial Intelligence, Volume 18, 7(2004) pp. 1339-1360.
[19] Herbst, N.M. and Liu, C.N., Automatic Signature Verification Based on Accelerometry, IBM Journal of Research and Development Vol 21, No. 3 pp. 245-253, May 1977
[20] Kruskal, J.B. and Liberman, M. (1999) The symmetric time-warping problem: from continuous to discrete. In Sankoff, D. and Kruskal, J. (eds), Time Warps, String Edits, and Macromolecules: The Theory and Practice of Sequence Comparison. CSLI Publications, Stanford, pp. 125-161.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)