International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 04 | April -2020 ISSN: 2582-3930

# Handwritten Signature Verification Method Using Combinational Feature Extraction

**C.M. Edwin Thurai[1], R. Jermine Reena[2]**

[1]*Assistant Professor/ECE,Bethlahem Institute Of Engineering,Karungal,Tamilnadu,India.*
[2]*Assistant Professor/ECE,, Bethlahem Institute Of Engineering,Karungal,Tamilnadu,India*

---***---

**Abstract**–Handwrittensignatures are considered as one of the most valuable biometric traits. To verify the signature the features are extracted in different ways. The featureextraction processincludes pre-processing, attribute generation,attribute truncation and quantization, and feature generation. The features of the whole signatures are extracted. In addition, the signature is segmented and the features are extracted of those segmented regions. The finalfeature vector is the combination of global and regional features. Then, the similarity measurement between the test signature and user template is done by Euclidean distance. KNN classifier is used to classify the signature to check whether it is genuine or forgery.The experimental setup is done using SG-NOTE database acquired by Samsung Galaxy Note and the MCYT-100 database captured by a WACOM pen tablet.

***Key Words***:*attribute generation, attribute truncation, quantization, Euclidean distance*.

## 1. INTRODUCTION

In order to perform signature verification, there are two possibilities(related to the classification step). One is to store different signatures of a givenperson in a data- base and in the verification phase to compare the test signatureto these signatures, called ―Reference Signatures‖ by means of a distancemeasure; in this case a dissimilarity measure is the outcome of the verificationsystem, after combining by a given function the resulting distances[9]. The other isto build a statistical model of the person‗s signature; in this case, the outcome ofthe verification system is a likely- hood measure—how likely it is that a testsignature belongs to the claimed client‗s model. The signature verification methods are online verification methods and offline verification methods[15].

In the existing work hybrid discrete wavelet transform and discrete Fourier transform were used. Fourier transform is performed to extractthe feature descriptor of the decomposed sub- bands. A dissimilarity score ofthe extracted features between the test signature and reference data is computedusing Euclidean distance. The *k*- nearestneighbour and support vector machine are applied in order to fuse multiplefeatures. The resulting score value is then normalized and compared with a threshold value in order to decide whether a given signature is genuine orforgery[4].

This paper proposes a secure and dynamic signature verification methodwhich applies to the mobile phone. The proposed method includes feature extraction processes which arepre-processing, attribute generation, attribute truncation and quantization, and feature generation. The global features and the segmented regions features are combined to get the feature vectors. KNN classifier is used in this proposed system to get the better result in signature verification.

## 2. METHODOLOGY

### 2.1. Pre-processing

Pre-processing is done to extract effective features due to thecharacteristic of signatures from mobile phones. The pre-processing steps involve elimination of redundant information, cubic spline, sizenormalization, and position normalization. Sometimes redundant information will be available in the database. It will be neglected in the first step.cubic spline is used to derive auniformly sampled signature.The size and position of signature varywhen a user writes a signature several times. So the signatures are normalized to thesame size and move the gravity centre of the signature to the original point forbetter verification performance.

### 2.2. Feature Extraction

The feature extraction process represents a major tackle in any signatureverification system. Even there is no guarantee that two genuine signatures of aperson are accurately the same (intrapersonal variations). Its difficulty alsostems from the fact that skilled forgeries follow the genuine pattern(interpersonal variations). This is unlike fingerprints or irises where fingerprintsor irises from two different persons vary widely.

Ideally interpersonal variationsshould be much more than the intrapersonal variations. Therefore it is veryimportant to identify and extract those features which minimize intrapersonalvariation and maximize interpersonal variations. There is a lot of flexibility inthe choice of features for verification of a signature. Global features, such as theoverall direction of the signature, the dimensions, and the pixel distribution, areusually not adequate to differentiate forgeries [7]. On the other hand, significantlocal features are extremely hard to locate. Great research efforts were made in order to concentrate on the local feature extraction process. Most of them aim atthe robust extraction of basic functions entities called ―strokes‖ from the originalskeleton of the signature strokes.

Thefeature extraction process ends with taking out DWT coefficients for penpositions in *x* direction, and pen positions in *y* direction, and pen movementangles. In the regional feature extractionthe elements of a signature are equally divided to k segments.

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 04 | April -2020 ISSN: 2582-3930

2.3. KNN Classifier

In KNN, K is the number of nearest neighbours. The number of neighboursis the core deciding factor. K is generally an odd number if the number ofclasses is 2. When K=1, then the algorithm is known as the nearest neighbouralgorithm.

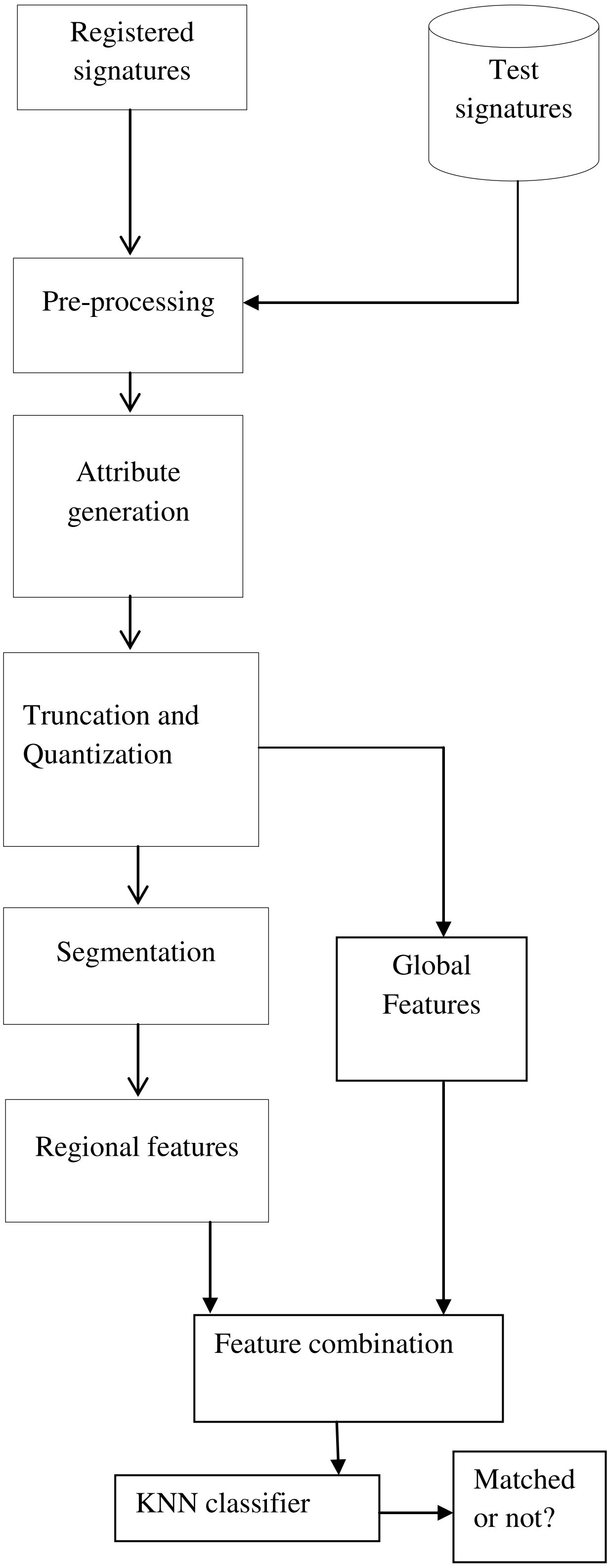


Fig -1 System Architecture

Suppose P1 is the point, for which labelneeds to predict. First, you find the one closest point to P1 and then the label of the nearest point assigned to P1[10]. For finding closest similar points, Euclidean distance is used. KNN has the followingbasic steps:

1. Calculate distance
2. Find closest neighbours
3. Vote for labels

The system architecture of the proposed method is shown in Fig -1

## 3. RESULTS AND DISCUSSION

For the signature recognition and verification system, accuracy ofthe system is basically how correctly does our system recognizes a particularsignature by giving us whom does it belongs to and whether it is forged orgenuine. The evaluation parameter used for measuring accuracy of the system isrecognition rate. We find the FAR and FRR which stand for False AcceptanceRate and False Rejection Rate. The number of falsely accepted images over thetotal images is FAR and the number of falsely rejected images over the totalimages is FRR In our experimentation, we find our accuracy to be highest with85.66% at K = 22 in our KNN classifier. The Fig -2 shows the output for which the signature is recognized.

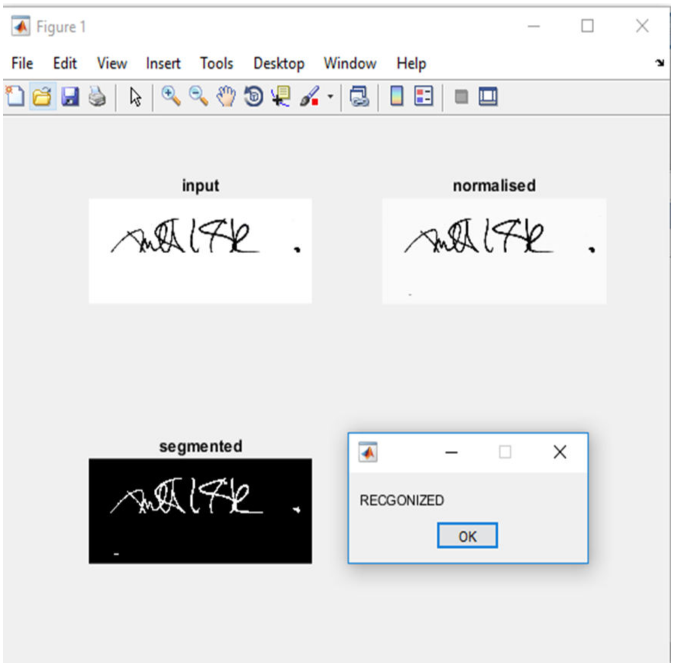


Fig -2. Signature recognized

The classifier we have used is KNN which stands for k-nearest neighbours. It is basically a classification algorithm that means it assigns a class to a testimage based on its feature values. The k-nearest neighbours'algorithm usesEuclidian distance method to find the distance between two training points. Thususing Euclidian distance we find k nearest neighbouring training points of ourtest point based on its features and the class with maximum number ofoccurrences is taken as the decision class for that test image and is assigned tothat image. If the decision class is 'orig' with same signer the image is Accepted' and otherwise Rejected'. The Fig -3 shows the output for which the signature is not recognized.

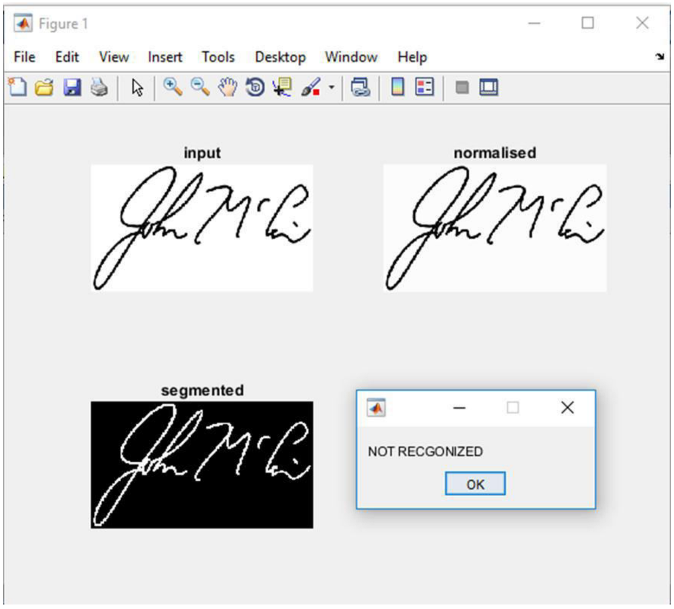


Fig -3 Signature not recognized

## 4. CONCLUSION

In this work, we proposed a secure and dynamic handwritten signatureverification system which applies to smart phones. Both the global and regionalfeatures are extracted for verification. The secure KNN is utilized to protect thetemplate and feature vector. The experiment shows that the regional featuresachieve good performance in both the two databases. It is valuable to furtherexploit the regional features in future. In addition, the skilled forgery is a morechallenging problem in signature verification. Actually, the verification with therandom forgery is a typical matching problem, while the verification with theskilled forgery is a typical two-class classification problem. Hence, an effectivecombination of two kinds of solutions may achieve an improved performance.

## ACKNOWLEDGEMENT

I would like to thank God Almighty for his blessings, strength and support to complete this work successfully. I am grateful to all of those with whom I have had the pleasure to work during this and other related projects.

## REFERENCES

1. R. Plamondon and G. Lorette, ―Automatic signature verification and writer identificationa‚ ‖the state of the art,‖ Pattern recognition, vol. 22, no.2, pp. 107–131, 1989.
2. J. Fierrez and J. Ortega-Garcia, ―On-line signature verification,‖ inHandbook of biometrics. Springer, 2008, pp. 189–209.
3. M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez,―Multi-biometric template protection based on homomorphic encryption,‖Pattern Recognition, vol. 67, pp. 149–163, 2017.
4. R. P. Krish, J. Fierrez, J. Galbally, and M. Martinez-Diaz, ―Dynamicsignature verification on smart phones,‖ in International Conference onPractical Applications of Agents and Multi-Agent Systems. Springer,2013, pp. 213–222.
5. J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho et al.,―Mcyt baseline corpus: a bimodal biometric database,‖ IEE Proceedings-Vision, Image and Signal Processing, vol. 150, no. 6, pp. 395–401, 2003.
6. W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, ―Secure knncomputation on encrypted databases,‖ in Proc. of 2009 ACM SIGMO International Conference on Management of data. ACM, 2009, pp. 139–152.
7. 7. H. Lei and V. Govindaraju, ―A comparative study on the consistency offeatures in on-line signature verification,‖ Pattern Recognition Letters,vol. 26, no. 15, pp. 2483–2489, 2005.
8. A. K. Jain, F. D. Griess, and S. D. Connell, ―On-line signatureverification,‖ Pattern recognition, vol. 35, no. 12, pp. 2963–2972, 2002.
9. A. Kholmatov and B. Yanikoglu, ―Identity authentication using improvedonline signature verification method,‖ Pattern recognition letters, vol. 26,no. 15, pp. 2400–2408, 2005.41
10. M. Faundez-Zanuy, ―On-line signature recognition based on vq-dtw,‖Pattern Recognition, vol. 40, no. 3, pp. 981–992, 2007.
11. M. I. Khalil, M. Moustafa, and H. M. Abbas, ―Enhanced dtw based onlinesignature verification,‖ in Image Processing (ICIP), 2009 16th IEEEInternational Conference on. IEEE, 2009, pp. 2713–2716.
12. N. Xiong, A. V. Vasilakos, L. T. Yang, L. Song, Y. Pan, R. Kannan, andY. Li, ―Comparative analysis of quality of service and memory usage foradaptive failure detectors in healthcare systems,‖ IEEE Journal onSelected Areas in Communications, vol. 27, no. 4, 2009.
13. X. Song, X. Xia, and F. Luan, ―Online signature verification based onstable features extracted dynamically,‖ IEEE Transactions on Systems,Man, and Cybernetics: Systems, vol. 47, no. 10, pp. 2663–2676, 2017.
14. D. Muramatsu, M. Kondo, M. Sasaki, S. Tachibana, and T. Matsumoto,―A markov chain montecarlo algorithm for bayesian dynamic signatureverification,‖ IEEE Transactions on Information Forensics and Security,vol. 1, no. 1, pp. 22–34, 2006.
15. J. Fierrez, J. Ortega-Garcia, D. Ramos, and J. Gonzalez-Rodriguez ―Hmm-based on-line signature verification: Feature extraction andsignature modeling,‖ Pattern recognition letters, vol. 28, no. 16, pp. 2325–2334, 2007.
16. A. H. Toselli, E. Vidal, V. Romero, and V. Frinken, ―Hmm word graphbased keyword spotting in handwritten document images,‖ InformationSciences, vol. 370, pp. 497–518, 2016.