Handwritten Signature Verification and Detection of Forged Signatures

Archana A Pillai[1] Ambi Rachel Alex[2] Hari.S[3]
[1]Student [2,3]Assistant Professor
[2,3]Department of Electronic & Communication Engineering
[1,2,3]Mount Zion College of Engineering Kadammanitta, Pathanamthitta, Kerala, India

Abstract— Handwritten signature verification and detection of forged signatures deals with verification of handwritten signatures and detection of forged signatures tasks. The proposed system involves the use of contourlet transform-based directional code co-occurrence matrix feature generation method. The proposed method offers a new framework for the handwritten signature verification in order to ensure the exact person or writer and detect the unauthorized signature if any person signs the forged signature more than one time. This procedure is based on writer-independent offline mode and does not require any forgery can be developed with a reduced number of reference signatures.

Key words: Contourlet transform, DFB, LP, FDM, Canberra distance

I. INTRODUCTION

The handwritten signature verification is an authentication Procedure and is required in different fields of everyday life .It is one of the most identification method widely used, inexpensive and acceptable from society. It is difficult to verify the signatures in some situations; a high similarity between two signatures does not mean that they have been written by the same person and a low similarity between two signatures does not mean that it written by different persons. The main drawback of the handwritten signature is the easiest reproduction by the professional forgers [1].Therefore it is difficult to discriminate between genuine and forged signatures.

The design of handwritten signature verification can be classified as on-line mode which allows the capturing of dynamic characteristics and off-line mode which allows generating an image and the proposed system is based on the off-line mode [12]. Off-line mode have two different approaches for signature verification; writer dependent HSV where models for genuine and forgery signatures are created for each writer. Then, the questioned signature of a writer is compared to its own model. Clearly, it requires a model for each writer to be verified and writer-independent HSV which does not require any reference model to verify its signature, a general model is generated from some writers chosen randomly. The concept of off-line handwritten signature verification using contourlet transform and co-occurrence matrix proposed by Hamadene [12] and then it is extended to a new approach for HSV using feature dissimilarity thresholding [1] and some methods proposed using bi-class support vector machine for signature verification by Guerbai [14].Also, the analysis of signature stability using local features is investigated by Malik [9].

The proposed method offers a new framework for the handwritten signature verification in order to ensure the exact person or writer and detect the unauthorized signature if any person signs the forged signature more than one time. "Handwritten signature verification and detection of forged signatures "can be done through feature generation, verification and detection .The proposed method does not require any forgery model i.e,writer-independent offline handwritten signature verification where a global model is constructed using a set of writers selected from different datasets and then it is used for unknown writers.

The remaining of the paper is organized as follows: Section 2 describes the proposed system .Section 3 describes the scheme of HSVS and steps used for HSV presented in section 2.Then, section 4 concludes the paper.

II. PROPOSED HANDWRITTEN SIGNATURE VERIFICATION AND DETECTION OF FORGED SIGNATURES

A questioned signature, sig_q is submitted to a set of reference signatures, sig_n [n=1, 2….J] where J is the number of reference signatures. Then, feature generation is performed on questioned signature and each reference signature in order to produce its respective feature vector i.e., f_q and f_n. using contourlet transform and co-occurrence matrix. After the generation of feature vector, it measure the resemblance between the questioned signature and each of the reference signature by feature dissimilarity measure (FDM).Then, a selection rule is performed which selects the representative FDM and compared to a decision threshold for accepting or rejecting the questioned signature[1]. If the questioned signature is rejected, the rejected signature is saved in the database that further compares and detects if the false signature for the next time. Hence, unauthorized signature can be easily identified.

A. Feature Generation

The feature vector of questioned signature and each of the reference signature can be generated using contourlet transform and co-occurrence matrix. The features describe the writer handwriting style through which directions are contained in signatures, the amount of each direction and their spatial distribution toward each other.

Contourlet transform has the ability to capture significant information about an object or capture smooth contour segments to provide their directional information at several resolutions and directions. The Laplacian pyramid (LP) is firstly used to capture the point discontinuities and then a directional filter bank (DFB) allow linking the point discontinuities into linear structure according to the directional sub-bands. DFB [12] has the ability to receive high frequencies of the input image which contains some information about directions. This is permitted by the Laplacian decomposition by removing low frequencies before DFB, so that the directional information can be captured efficiently. While, the co-occurrence matrix considered as a statistical feature allows describing the localization, organization and direction's occurrences. Hence, the resulting feature vector contains information

about the spatial arrangement of dominant directions contained into signature contour segments [12].

B. Feature Dissimilarity Measure

The resemblance between questioned signature and each of the reference signature can be evaluated by FDM. Canberra distance is used for computing the FDM value between the questioned signature and reference signatures.

$$s_{qn} = FDM(fq, f_n) = \sum_{t=1}^{T} \frac{|fq(t) - f_n(t)|}{|fq(t) + f_n(t)|}$$

Where s_{qn} is the FDM value and T is the size of the feature vector. Hence, a questioned signature is considered close to a reference signature when the FDM value is minimum and the minimum of the FDMs is selected as the representative one.

$$s_{min} = \text{Min}\{s_{qn}\}_{n=1}^{J}$$

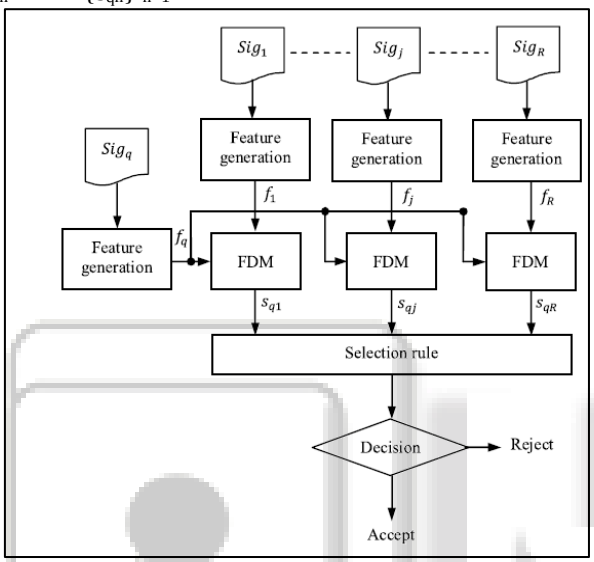

Fig. 1: Diagram for handwritten signature verification

C. Threshold selection

Let Sord = $\{s_0, \ldots, s_{L-1}\}$ where s_0 and s_{L-1} minimum and maximum values of the FDMs contained into the set S and Sord is the set which containing FDMs ordered from the stable to unstable signatures. The decision threshold, t is defined as the frontier value between stable and unstable signatures selected from the ordered set Sord.

D. Verification Step

The verification step of the questioned signature does not require any forgery model and verified independently from a specific writer's model according to the decision rule:

$Sig_q \in$ {Accepted if smin < t

Or

{Rejected otherwise

E. Detection

If the questioned signature is rejected, the rejected signature is saved in the database. Again, feature vector of rejected signature, R_{new} and the rejected signatures, R_i is generated and calculates the FDM values and then selection rule is performed .Finally, decision is taken; if it is yes, then the signature will be already there in the database. Thus unauthorized or forged signature can be detected.

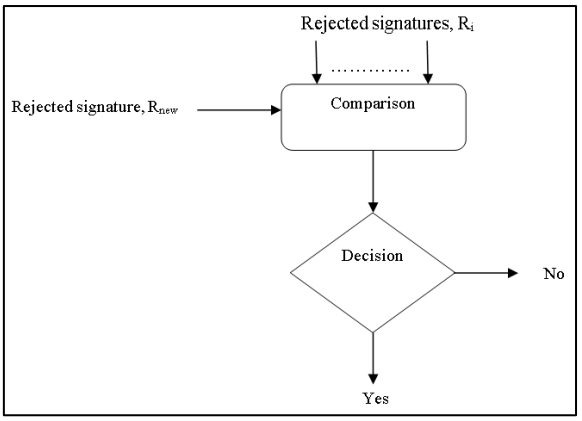

Fig. 1: Diagram for detection of forged signatures

III. SCHEME OF HSVS AND DETECTION

Fig.1 shows the scheme of handwritten signature verification and fig.2 illustrates the diagram for detection of forged signatures.

The following procedure is followed to perform handwritten signature verification and detection of forged signatures:

1) Submission of questioned signature, sig_q to a set of reference signatures, sig_n.
2) Generation of feature vector (f_q and f_n) for questioned signature and each of reference signature.
3) Measure the resemblance between questioned signature and each of reference signature using FDM.
4) Find the minimum FDM value and select the representative one.
5) Comparison of representative FDM to a decision threshold for accepting or rejecting the questioned signature.
6) Detection of forged signatures.

IV. CONCLUSION

The proposed system provides a procedure for handwritten signature verification and can be easily detect the forged or unauthorized signature. This system uses the reduced number of references and does not require any reference model for verification. The system identify the exact writer and ensures the security in different fields of everyday life.

REFERENCES

[1] A.Hamadene ,Y.Chibani, "One-class writer-independent offline signature verification using feature dissimilarity thresholding", in IEEE transactions on information forensics and security, vol. 11, no. 6, June 2016.
[2] S. N. Srihari, S. H. Cha, H. Arora, and S. Lee, "Individuality of handwriting," J. Forensic Sci., vol. 47, no. 4, pp. 1–17, Jul. 2002.
[3] D. Rivard, E. Granger, and R. Sabourin, "Multi-feature extraction and selection in writer-independent off-line signature verification," Int. Document Anal. Recognit., vol. 16, no. 1, pp. 83–103, Mar. 2013.
[4] D. Bertolini, L. S. Oliveira, E. Justino, and R. Sabourin, "Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers," Pattern Recognit., vol. 43, no. 1, pp. 387–396, Jan. 2010.

[5] S. N. Srihari, A. Xu, and M. K. Kalera, "Learning strategies and classification methods for off-line signature verification," in Proc. 9th Int.Workshop Frontiers Handwriting Recognit., Tokyo, Japan, Oct. 2004, pp. 161–166.
[6] C. Santos, E. J. R. Justino, F. Bortolozzi, and R. Sabourin, "An offline signature verification method based on the questioned document expert's approach and a neural network classifier," in Proc. 9th Int. Workshop Frontiers Handwriting Recognit., Tokyo, Japan, Oct. 2004 pp. 498–502.
[7] A. Bensefia, T. Paquet, and L. Heutte, "A writer identification and verification system," Pattern Recognit. Lett., vol. 26, no. 13, pp. 2080–2092, 2005.
[8] R. Kumar, L. Kundu, B. Chanda, and J. D. Sharma, "A writer-independent off-line signature verification system based on signature morphology," in Proc. 1st IITM, Allahabad, India, Dec. 2010, pp. 261–265.
[9] M. I. Malik, M. Liwicki, A. Dengel, S. Uchida, and V. Frinken, "Automatic signature stability analysis and verification using local features, "in Proc. 14th Int. Conf. Frontiers Handwriting Recognit., Heraklion, Greece, Sep. 2014, pp. 621–626.
[10] B. Fang and Y. Y. Tang, "Reduction of feature statistics estimation error for small training sample size in off-line signature verification," in Biometric Authentication (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2004, pp. 526–532.
[11] S. Chen and S. Srihari, "Combining one- and two-dimensional signal recognition approaches to off-line signature verification," in Proc. 13th Document Recognit. Retr., San Jose, CA, USA, Jan. 2006, pp. 1–10.
[12] A. Hamadene, Y. Chibani, and H. Nemmour, "Off-line handwritten signature verification using contourlet transform and co-occurrence matrix," in Proc. 13th Int. Conf. Frontiers Handwriting Recognit., Bari, Italy, Sep. 2012, pp. 343–347.
[13] Y. Wang, J.-P. Li, J. Lin, and L. Liu, "The contourlet transform and svm classification for face recognition," in Proc. Int. Conf. Apperceiving Comput. Intell. Anal., Chengdu, China, Dec. 2008, pp. 208–211.
[14] Yasmine Guerbai, Youcef Chibani and Nassim Abbas, "One-Class versus Bi-Class SVM Classifier for Off-line Signature Verification", IEEE 2012.
[15] A. B. Mansoor et al., "Personal identification using palm print and contourlet transform," Advances in Visual Computing (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2008, pp. 521–530.
[16] P. J. Burt and E. H. Adelson, "The Laplacian pyramid as a compact image code," IEEE Trans. Commun., vol. 31, no. 4, pp. 532–540, Apr. 1983.

