International Journal on Emerging Technologies **11**(2): 1061-1065(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

An Efficient Feature Selection Method for Offline Signature Biometrics

Mamta Garg[1,2], Ajatshatru Arora[3] and Savita Gupta[4]
[1]*Department of Computer Engineering, Govt Polytechnic College For Girls, Jalandhar 144001 (Punjab), India.*
[2]*Department of Computer Science and Engineering,*
Sant Longowal Institute of Engineering & Technology, Longowal 148106, India.
[3]*Department of Electrical and Instrumentation Engineering,*
Sant Longowal Institute of Engineering & Technology, Longowal, 148106 India.
[4]*Department of Computer Science and Engineering,*
University Institute of Engineering & Technology, Panjab University, Chandigarh 160016 India.

(Corresponding author: Mamta Garg)
(Received 14 January 2020, Revised 06 March 2020, Accepted 09 March 2020)
(Published by Research Trend, Website: www.researchtrend.net)

Abstract: Handwritten signature is considered as the most natural way of authenticating the identity of a person. It has been used for the purpose of verification and authentication for long period of time. In this paper, offline signature identification using neural network is proposed, where the signature is captured and stored in an image format. Features are extracted from pre-processed signature image by applying SIFT (Scale Invariant feature Transform) algorithm. After that GA (Genetic Algorithm) is employed on extracted features to select dominant features. The optimized features are then used to train a neural network. During identification, same feature extraction and optimization techniques are implemented on test signatures to extract features. These extracted features are then directed as input to a trained neural network which will classify it as a genuine or forged signature. Experiments are carried on signature database for 50 subjects. So this paper presents an automated and novel signature recognition system, which provides accuracy of 97.2% with low FAR (False Acceptance Rate) of 1.7%.

Keywords: Biometrics, SIFT, GA, Neural Network, FAR, Signature Recognition System.

I. INTRODUCTION

Biometric authentication deals with the automatic identification of people based on the principle of measurable physiological or behavioral characteristics. The key advantage of any biometrics system is to alleviate risks interrelated password/ token based authorization. Signature recognition biometric authentication method has gained popularity in recent years. The signature has been widely employed in administrative documents, legal documents, bank checks and commercial transactions as a means of identification. The handwritten signature perhaps has the longest history among the other possible biometrics available. Also authentication of an individual using one's signature is one of the most natural biometric techniques, since we are habituated to authenticate everything with signature. Signature based verification being non-invasive authentication procedure is highly accepted by majority of users. Although the signature of individual may vary over time and it is not as unique as iris pattern, yet signature's widespread acceptance by the general public makes it appropriate for biometric authentication systems. It exhibits significant intra-class variability since it can be affected by physical and emotional conditions. Even successive genuine signatures of the same person may vary in scale and orientation [1]. The intra-class variability within signatures must be taken into consideration while designing the signature based authentication process. The intra-class variations and intra-class similarities play a decisive role to analyze signatures as complete images.

In general, there are two types of handwritten signature verification systems: off-line and online systems. Offline signature verification and online signature verification is termed as static and dynamic signature verification respectively. In an off-line system, an image of the user's signature is scanned and stored into the computer. On the other hand, statistics of the user's signature are acquired by using specially designed tablets in an online system. In case of an off-line system, no specialized device is required to capture the signature and the presence of user is not necessary at the time of verification. For this reason, off-line signature recognition is easy and suitable in various situations such as document verification and financial transactions. The dynamic information like duration, time ordering, writing speed, number of strokes, pressure and direction of writing is lost in case off-line signature recognition systems.

The area of signature recognition is still under intensive study to find out the proper feature sets representing the unique characteristics of signature. Also research on automatic signature recognition is vital for secure and reliable financial transactions in the electronically wired information society in which we live today. The main motivation of development of handwritten signature verification/identification systems is to reduce fraud in financial transactions. The research has been motivated in recent years for obtaining effective automated solutions for signature recognition [2-7].

In this paper, SIFT algorithm is applied to extract features from the signature image. The features set

representing the biometrics is usually large in terms of dimensionality.
The features may be noisy and may contain irrelevant or unnecessary information of signature image and may cause performance degradation. Furthermore, large feature set also increases the storage cost. The main objective of feature selection approach is to improve the classification accuracy and speed. So a new optimal feature selection technique based on genetic algorithm is applied to select the most optimized features. Finally, the neural network is employed for classification, which is an efficient method for matching and verifying individuals in authentication systems. It is trained in Matlab 2016a to match the features of signature authentication system. In this paper, we present a novel approach to signature biometric systems, with the purpose of reducing the number of features used for classifying the signatures.

II. MATERIALS AND METHODS

In this paper, a novel effective approach to the feature extraction and feature selection for signature biometric is developed. First of all, the features used for classification are extracted by applying SIFT method. After that GA is applied on SIFT signature features for the purpose of optimization. The overall framework of the proposed signature biometric system is shown in Fig. 1.

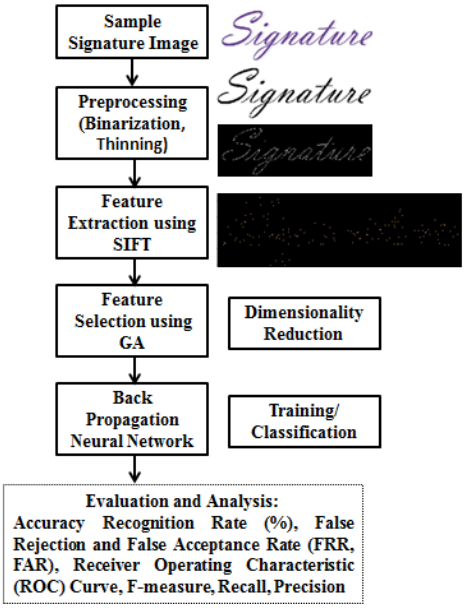

Fig. 1. Overall proposed framework of signature recognition system.

A. Image Preprocessing and Features Extraction
First of all, the scanned image of signature is preprocessed to make it suitable for extracting features. Then, significant geometric features are extracted from the preprocessed image, which are used to differentiate forged signatures from exact ones. The steps applied on both training data and testing data set in signature authentication system are briefly explained in this section.

(i) **Image Acquisition:** In this step signature from the user is acquired using digital scanner or digital camera. The digital scanner/camera scans handwritten signature and converts it to digital image. The acquired signature is stored in database as digital image for further processing.
(ii) **Image Pre-Processing:** This stage involves an array of steps used for interpretation of the image. It improves quality of image and makes it suitable for feature extraction. Each of the scanned signature passes through a sequence of following pre-processing steps.
– Color Inversion: In this step, the true color RGB image of signature is converted into grayscale intensity image by eliminating the hue and saturation information while retaining the luminance.
– Binarization: The binarization technique reduces the amount of image information (removing color and background) from grayscale signature image and coverts it into binary image. Thresholding method is applied for distinguish the signature from the background.
– Thinning: The thinning process eliminates the thickness differences of pen by making the image one pixel thick, simplifies the structural shape of signatures by obtaining the corresponding signature skeleton. The primarily use of thinning is to remove selected foreground pixels from the binary image by preserving overall structure of the image.

B. Feature Extraction by applying SIFT method
Feature extraction is employed to generate features that can be used for comparison. It is the most important process through which essential information of image is captured for interpretation. The main challenge in signature based biometric authentication system is to extract features which are robust against intra-class variability and discriminate between genuine and impostor samples at the same time. In this work, signature features are extracted by SIFT algorithm and then features are optimized by incorporating Genetic Algorithm to develop a robust signature classification system. We decided to apply SIFT algorithm to extract features from signature images because it is invariant to scaling, rotation, and illumination. The SIFT algorithm proposed by Lowe [8-9] has been successfully applied in the domain of biometrics based authentication systems including ear [10], palmprint [11], face [12], iris [13], fingerprint [14] etc. It generates descriptors representing the texture around the keypoints. The generation of SIFT feature descriptors involves the following stages.
– Scale-space extrema detection: This step identifies location and scale of salient feature points also called key-points. For this, the Difference-of-Gaussian function is applied in scale space. The scale space of an image defined by the function L(x,y,σ) is created by convolving the signature image I(x,y) with a variable scale Gaussian function G(x,y,σ) by using Equation 1, where σ is the scale of blurring and determines the smoothness of the transformed image scale and variable scale Gaussian function is calculated by using Equation 2.

$$.L(x,y,\sigma) = G(x,y,\sigma) * I(x,y) \quad (1)$$

$$G(x,y,\sigma) = \frac{1}{2\pi\sigma^2} e^{\frac{-(x^2+y^2)}{2\sigma^2}} \quad (2)$$

The difference of successive Gaussian-blurred signature images is calculated by simple image subtraction of two nearby scales separated by a constant multiplicative factor k using Equations 3 and 4. The Gaussian scale transform is applied to detect the points that are invariant to scale changes.

$$D(x,y,\sigma) = \big(G(x,y,k\sigma) - G(x,y,\sigma)\big) * I(x,y) \quad (3)$$

$$D(x,y,\sigma) = L(x,y,k\sigma) - L(x,y,\sigma) \quad (4)$$

Finally local scale-space extrema of DoG signature images is calculated by comparing each sample point to 8 neighbors in current scale as well as 9 neighbors in the above and below scales. If it has the maximum or minimum value, then is considered as best key point in that scale.

– Key-point localization: The key-points that have low contrast or are poorly localized along an edge are discarded. The final key-points selection is based on the measures of their stability. In this step, the key-points which are insensitive to noise and invariant to affine transformations are retained.

– Orientation assignment: In this step, an orientation is assigned to each key-point to create the key-point descriptor in order to reach invariance to image rotation. The gradient magnitude m(x,y) and orientation θ(x,y) for the Gaussian-smoothed signature image at scale σ are computed by using formulas as given by Equations 5 and 6.

$$m(x,y) = \sqrt{(L(x+1,y) - L(x-1,y))^2 + (L(x,y+1) - L(x,y-1))^2} \quad (5)$$

$$\theta(x,y) = tan^{-1}\frac{L(x,y+1) - L(x,y-1)}{L(x+1,y) - L(x-1,y)} \quad (6)$$

– Key-point descriptor: The highly distinctive feature vector is computed from the local image region around the key-point.

C. Genetic Algorithm

It is necessary to lessen the dimension of signature SIFT descriptors while not weakening the discrimination power. So we have employed GA to select optimized features. Genetic algorithm (GA) developed by John Holland [15] is a stochastic optimization method based on ideas originating from genetic and evolutionary theory [16] and biological genetic development principles. GA has the ability to exploit accumulated information efficiently about a large set of population [17] and has been effectively applied in the field of biometrics [18-22]. The GA operates with a population formed by a set of individuals called chromosomes. The first step of genetic algorithm is to generate the population of feasible solutions randomly. Then the evolution starts from a population of randomly generated individuals and the population in each iteration is called generation. In each generation, the fitness of every individual in the population is evaluated. The crossover rate is set to 0.8 for current experimental work. The mutation probability rate of 0.05 is considered. Roulette-wheel selection method is employed. Population size is kept 50 and number of generations are 25. The fitness function is defined as Ft=mean2(bit_value) where bit_value represents extracted SIFT features of signature image.

D. Neural Network

The final stage is the recognition of the signature which has been achieved with the help of the neural network. An ANN endeavors to emulate the computational functionality and memory capability of the human brain [23]. It learns through training like human brain. Previous researches show the effective applications of Neural Network in matching and recognition. It consists of interrelated processing units called nodes or neurons that work together to produce an output function. The features of signature are extracted by applying SIFT technique and optimized by genetic algorithm. The optimized features of signature are then used to train feed forward back propagation error neural network, which is consisted of an input layer, hidden layer and an output layer, and interconnected by modifiable weights represented by links between layers. It consists of set of inputs (x1, x2…xn) which is multiplied by multiple weights (w1, w2…wn) to provide output. The data is propagated to the output layer via the hidden layer. This is called forward pass of the back propagation algorithm. The actual output values of the output layer are compared with the desired target output values. The error between actual output and desired output values is calculated and propagated back towards hidden layer. It is used to update the connection strengths between nodes, i.e. weight matrices between input-hidden layers and hidden-output layers are updated. The weight change is done with steepest descent algorithm. The output layer provides the trained signatures, which is used for the classification.

The signature features, to be tested, are fed to the trained neural network to find the genuinely of signature. For example, if second sample of 10th person has been taken for testing then it is evident that the signature in question belonged to 10th person. If it is matched to another person instead of 10th person then the result is considered to be incorrect. In this way all the signatures in the database have been tested.

III. EXPERIMENTAL RESULTS AND DISCUSSIONS

A. Database

In our database, we collected 500 signatures from 50 persons (10 signatures each person). All the participants were females. Each individual was asked to sign non-overlapping signatures using pen on a white sheet of A4 sized paper. The signatures were collected in two sessions over a period of three months to consider intra-class variations in the signatures with time. The purpose of this exercise was to have considerable variability in the signature database, as signing characteristics depends on an individual's emotion, health, state of mind, position of pen-grip, age, writing posture, fatigue, available space, writing material, and environment factors like noise, luminance and humidity. Seven signatures were collected in the first session to train the Neural Network and remaining three signatures were collected in the second session for testing the classifier. All these sample signatures were scanned using HP ScanJet 200 Flatbed Photo Scanner and stored as genuine signatures.

B. Results

The features extracted from SIFT techniques are optimized by GA and then optimized features are applied as an input to train the feed forward neural network. Neural network is trained with 7 genuine signatures for each user and then tested with other 3 genuine signatures of the same user. Simulation was performed in Matlab R2016a to assess the performance of proposed method. We also classified the signatures by computing Euclidean Distance and results are compared with the proposed method. The performance of the system is recorded in terms of various statistical measures like False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER), and results are plotted in terms of Receiver Operating Characteristics (ROC) curves as shown in Fig. 2. Since EER measures the intrinsic strength of biometric system, it is clear from the figure that the proposed system by employing Neural Network outperforms Euclidean based signature biometric authentication system. The results exhibited that it is possible to use only a small portion of the features without affecting the classifier's recognition rate. The high value of accuracy (97.2%), recall (94.9%), precision (96.1%) and F-measure (95.4%) reveals the effectiveness of the proposed system in distinguishing between genuine and impostor signatures.

Due to lack of universal signature database, different researchers have developed their databases individually for experimental purpose, so it is difficult to compare verification/identification results.

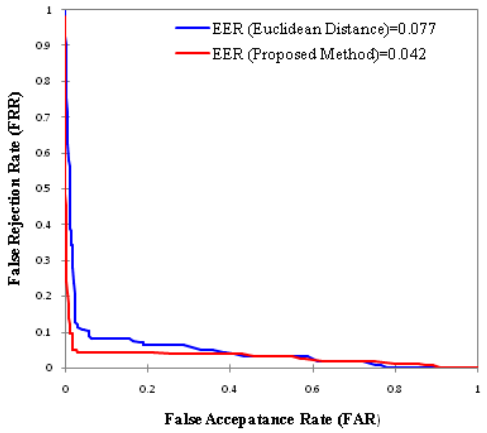

Fig. 2. ROC curves of signature recognition systems.

IV. CONCLUSIONS

We have developed a signature biometrics based authentication system by selecting minimum number of features without affecting the system accuracy. Scale Invariant Feature Transform is adopted to extract the features of the signature images. Then feature set optimized by GA is used to train the Neural Network. We have implemented the signature authentication system only on 50 subjects, however for real life applications, larger dataset can increase the robustness of the system. Although the problem of automatic signature recognition has been significantly studied, yet it offers a lot of scope for R&D community. In this study, we mainly focused on graphical features of signature, and discarded the dynamic information of digital signature. As future work, we would try to fuse static and dynamic aspects of signature to improve the classification accuracy of system. Also, we would like to extend our work by performing a feature-level fusion of signature biometrics with another complementary biometric modality like iris in order to increase the performance and security of system.

REFERENCES

[1]. A. G. Reza, H. Lim, and M. J. Alam (2011). An efficient online signature verification scheme using dynamic programming of string matching," in *Convergence and Hybrid Information Technology*, vol. 6935, G. Lee, D. Howard, and D. Ślęzak, Eds. Berlin, Heidelberg: Springer, 590-597.

[2]. B. Zhang (2011). Offline signature verification and identification by hybrid features and Support Vector Machine. *International Journal of Artificial Intelligence and Soft Computing, 2*(4), 302-320.

[3]. I. Bhattacharya, P. Ghosh, and S. Biswas (2013). Offline signature verification using pixel matching technique. *Proc. Technol., 10*, 970-977.

[4]. M. Jarad, N. Al-Najdawi, and S. Tedmori (2014). Offline handwritten signature verification system using a supervised neural network approach. In *Proc. 6th IEEE International Conference on Computer Science and Information Technology (CSIT)*, *Amman, Jordan,* 189-195.

[5]. S. Chandra, and S. Maheskar (2016). Offline signature verification based on geometric feature extraction using artificial neural network. In *Proc. 3rd IEEE International Conference on Recent Advances in Information Technology (RAIT)*, Dhanbad, India, 410-414.

[6]. D. Połap, and M. Woźniak (2016). Flexible neural network architecture for handwritten signatures recognition. *International Journal of Electronics and Telecommunicatios, 62*(2), 197-202.

[7]. T. Longjam, and D. R. Kisku (2017). A supervised manipuri offline signature verification system with global and local features. In *Proc. 7th IEEE International Symposium on Embedded Computing and System Design (ISED)*, Durgapur, India, 1-6.

[8]. D. G. Lowe (2004). Distinctive image features from scale-invariant keypoints. *Int. J. Comput. Vis., 60*, 91-110.

[9]. D. G. Lowe (1999). Object recognition from local scale-invariant features. In *Proc. 7th IEEE International Conference on Computer Vision*, Kerkyra, Greece, 1150-1157.

[10]. G. S. Badrinath, and P. Gupta (2009). Feature level fused ear biometric system. In *Proc. 7th IEEE International Conference on Advances in Pattern Recognition ICAPR'09*, Kolkata, India, 197-200.

[11]. J. Chen, and Y. S. Moon (2008). Using SIFT features in palmprint authentication. In *Proc. 19th IEEE International Conference on Pattern Recognition (IEEE) 2009*, Tampa, FL, USA, 1-4.

[12]. M. Tistarelli, A. Lagorio, & E. Grosso (2009). Face recognition by local and global analysis," in *Proc. 6th IEEE International Symposium on Image and Signal Processing and Analysis*, Salzburg, Austria, 690-694.

[13]. G. Yang, S. Pang, Y. Yin, Y. Li, and X. Li (2013). SIFT based iris recognition with normalization and enhancement. *International Journal of Machine Learning and Cybernetics*, *4*(4), 401-407.
[14]. R. Zhou, D. Zhong, and J. Han (2013). Fingerprint identification using SIFT-based minutia descriptors and improved all descriptor-pair matching. *Sensors*, *13*(3), 3142-3156.

[15]. D. E. Goldberg (1989). *Genetic algorithms in search, optimization, and machine learning,* 1st ed., Boston, MA, USA: Addison-Wesley Longman Publishing Co.
[16]. J. H. Holland (1992). *Adaptation in natural and artificial systems: an introductory analysis with applications to biology, control, and artificial intelligence*, MA, USA: MIT Press Cambridge.
[17]. B. Bhanu, S. Lee, J. and Ming (1995). Adaptive image segmentation using a genetic algorithm," IEEE *Trans. Syst. Man. Cybern.*, *25*(12), 1543-1567.
[18]. A. Cenys, D. Gibavicius, N. Goranin, and L. Marozas (2013). Genetic algorithm based palm recognition method for biometric authentication systems. *Elektronika ir Elektrotechnika*, *19*(2), 69-74.
[19]. X. Tan, and B. Bhanu (2002). Fingerprint verification using genetic algorithms. In *Proc. 6th IEEE Workshop on Applications of Computer Vision*, Orlando, FL, USA, 79-83.
[20]. A. Rozsa, A. E. Glock, and T. A.E. Boult (2015). Genetic algorithm attack on minutiae-based fingerprint authentication and protected template fingerprint systems. In *Proc. IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Boston, MA, USA, 100-108.
[21]. H. Boubenna, and D. Lee (2016). Feature selection for facial emotion recognition based on genetic algorithm. In *Proc.12th IEEE International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, Changsha, China, 511-517.
[22]. Y. Bouzouina, and Hamami (2017). Multimodal biometric: Iris and face recognition based on feature selection of iris with GA and scores level fusion with SVM. In *Proc. 2nd IEEE International Conference on Bio-engineering for Smart Technologies (BioSMART)*, Paris, France, 1-7.
[23]. R. Beale, and T. Jackson (1990). *Neural Computing-an introduction*, 1st ed., CRC Press.

How to cite this article: Garg, M., Arora, A. and Gupta, S. (2020). An Efficient Feature Selection Method for Offline Signature Biometrics. *International Journal on Emerging Technologies*, *11*(2): 1061–1065.