Journal of Theoretical and Applied Information Technology
30th April 2018. Vol.96. No 8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

OFFLINE HANDWRITTEN SIGNATURE RECOGNITION USING HISTOGRAM ORIENTATION GRADIENT AND SUPPORT VECTOR MACHINE

[1]NIDAA HASAN ABBAS, [2]KHALED N. YASEN, [3]KAMARAN HAMA ALI FARAJ, [4]LWAY FAISAL A.RAZAK, [5]FAHAD LAYTH MALALLAH

[1]Electrical Department, Faculty of Engineering, Al-Mustansiriyah University, Baghdad, Iraq.
[2]Departement of Computer Science, Cihan University Erbil, Erbil.
[3,4]Departement of Computer Science, Cihan University Sulaimani, Sulaimani, Iraq.

E-mail: [1]nidaahasan71@ummustansiriyah.edu.iq, [2]Iraq,khalid_aldabbagh@cihanuniversity.edu.iq
[3],kamaranfaraj@yahoo.com, [4]audayt@yahoo.com, [5]Fahad.layth.86@gmail.com.

ABSTRACT

Human being authentication by offline handwritten signature biometric research has been increasing, especially in the last decade. Verification process of an offline handwritten signature is not trivial task, because an individual rarely signs exactly the same signature whenever he/she signs, which is referred to as intra-user variability. The objective of this paper is proposing a feature vector of an offline handwritten signature by using an efficient algorithm as a strong feature extraction namely Histogram Orientation Gradient (HOG), in order to be passed into Support Vector Machine (SVM) classifier for the recognition operation. An experiment has been conducted to estimate the accuracy and performance of the proposed algorithm by using SIGMA database, which has more than 6,000 genuine and 2,000 forged signature samples taken from 200 individuals. The result has given accuracy as 96.8% as successful rate coming from the error type as: False Accept Rate (FAR) is 3% and False Reject Rate (FRR) is 3.35%.

Keywords: *Offline Signature, Biometrics, verification, Histogram Oriented Gradient (HOG), Support Vector Machine (SVM).*

1. INTRODUCTION

Technology development recently has contributed in digital devices to the escalating access and storage of confidential information. Therefore, the need for a more secure authentication mechanism becomes pressing and necessary.

Signature verification is one of the most accepted verification methods as well as it is deemed as behavioral biometric type. There are many applications of handwritten signatures including the banker's checks, the credit and debit cards issued by banks and various legal documents. Biometric system recognizes an individual based on a feature vector extracted from physiological or behavioral characteristic that belongs to the person [1, 2]. Biometric is one of the emerging techniques that has two main modes of a biometric system [3], firstly, the Identification Mode, which means comparing the target biometric data with all the data available in the system, or simply one that can be translated into this question: "Who are you?", or it performs a one-to-many (1:N) match. Generally, this mode consumes much time because it needs to do many comparison operations. The purpose of user identification is to search the closest matching identity. This type of biometric authentication is normally used in surveillance and forensic applications [3]. The second mode of biometric system is the Verification Mode, which is based on this question: "Are you who you claim to be?". In this mode, the target biometric data is compared with the specific reference stored in the system to authenticate its identity. In other words, it performs a one-to-one (1:1) match. Usually, this mode needs less time than the identification mode [4, 5]. Handwritten signature usually consists of the first and last name of a person and it does not contain the full name but only one part of it. This type of signature is referred to as a paraph [6]. Signature is deemed as a behavioral type of biometrics, which has a high legal value for document authentication,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

as well as being dependent on both commercial transactions and government institutions [7]. Also, it acts as a non-invasive authentication process [8]. It is considered as accepted biometrics, since most individuals have their own signatures that could be used as their own token [8]. However, the weak-point of this biometric modality is the intra-user variability because it undermines the signature recognition rate, as any individuals cannot produce a signature exactly the same as one of the previous versions. Another limitation is that handwritten signature can be forged without using specialized hardware [9], so that skilled forged signatures must be included in the conducted experiment for testing. This paper is based on an offline handwritten signature authentication which is also named static signature, this kind of verification uses scanned signature images, which are written on paper-based document, another type of signature data is referred to as online signature verification system where signature samples are captured digitally usually using digitized pen and graphical tablets. However, it is difficult to achieve high correct matching accuracy in signature verification due to the high intra-user variability, which will increase the False Reject Rate (FRR). Offline handwritten signature verification involves the following four phases: data acquisition, pre-processing, feature extraction and classification that the contribution is proving that high recognition rate of offline signature authentication will be achieved by using HOG feature extraction [10] and SVM [11] classifier. The research question in this paper tries to enhance offline handwritten signature verification by building a strong feature vector using HOG as image descriptor in order to raise the recognition rate compared with the state-of-the-art. Besides that, it explains how to choose suitable parameters of HOG descriptor to be useful in this research.

This paper is organized as follows. Section 2 is dedicated for a literature review related to offline signature verification. In Section 3, the research methodology design is presented by details. Then, the experiment of this testing is described in Section 4. In section 5, the result and discussion are presented. Finally, in Section 6, this article paper is concluded.

2. LITERATURE REVIEW

Researches of offline handwritten signature verification have been increased recently due to the development of the technology of hand-writing input devices such as Tablet and PDA. Most of the proposed verification systems, which are existing in the literature, are exploiting various methods of feature extraction and classification. In this section, a review has been done for the most updated works. One of the proposed system in 2012 [12], the verification utilized application of Associative Memory Net (AMN) for detecting forged signatures, and the cost functions are handled with detail parametric and parallel processing using OpenMP, this algorithms are trained with the genuine signature and tested with twelve very forged signatures, the accuracy of this algorithm is 92.3%. Another proposed system suggested in [13], here the database has been collected from 7 persons of total 1344 signatures that are used for experimentation, the verification operation is done by applying global and morphological operations as preprocessing, then, Daubechies wavelet transform was employed to extract a set of features, which utilize as input to a feed forward back Propagation neural network and a Radial Basis Function (RBF) network that are used for the testing. The accuracy of this method is 97.61%, however it is only 7 persons used to compute the aforementioned accuracy. In [14] another verification system has been proposed using 20 users in a database, each user has 20 genuine and 10 expert forgery signatures, Gabor wavelet coefficients with different frequencies and directions are considered as a feature extraction stage, and nearest neighbor has been used as a classifier.

Also, in [15] offline signature verification by using convolution neural networks (CNNs), which is based on the VGG16 architecture, and used ICDAR 2011 SigComp dataset to train this model, the achieved accuracy is 97% for Dutch signatures and 95% for Chinese Signatures. Also, in 2014 an Adaptive Window Positioning Techniques has been used as a feature extraction to build a feature vector which is passed to the Peasrson correlation similarity measurement for the classification as in [16], the EER of this system is 7.4%. Another proposed system for offline signatures Verification as in 2016 [17], for this verification system, signature image is first pre-processed and converted into binary image of same size with [200x200] Pixels and then different features are extracted from the image like Eccentricity, Kurtosis, Skewness and that features are used to train the neural network using back-propagation technique. Here, 6 different user signatures are taken to make database for testing, the result reported as two types error rate are as follows: False Acceptance Rate (FAR) as 5.05% and False Rejection rate (FRR) as 4.25%. In

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[18] another verification system has been proposed by using time independent signature verification using normalized weighted coefficients, result showed that by taking normalized weighted coefficients the performance parameters, are as following: FAR is 4.9% and FRR is 5.2%. Finally, in [19], two types of feature description methods, namely the Pyramid Histogram of Oriented Gradient (PHOG) and Direction Feature, were comparatively studied for signature verification, with SVM classifier resulted the following error types: FRR is 2.5% and FAR is 2% , as an accuracy is 97.8%. However, the used dataset contains signature images from only 160 individuals while our proposed algorithm using SIGMA database with 200 individuals. Accordingly, this field of research is still opened as there is no convinced result and performance with acceptable recognition rate with well-known database continuing large number of individuals to be tested.

In this paper the proposed algorithm for the offline handwritten signature recognition outperforms the state-of–the–art as overall in terms of both accuracy and number of participants for performance evolution.

3. RESEARCH METHODS

The proposed signature verification system consists of four main separate processes: pre-processing (length normalization), which is converting from online to offline signature, feature extraction and classification. Online signature samples are fed into the system for normalization so as to normalize the unknown length to the desired length online signature without affecting on the signature shape or adding distortion. More details of the signature normalization are described in [20].

The first stage is normalization, which normalizes the length of the signature to a fixed or desired length. Normalization operation to a fixed length is selected as a preprocessing operation, it is worth to mention that the SIGMA database [21] has been changed from online to offline signature images automatically by using Matlab Software, after converting from online to offline signature, the size of each signature image is [380 x 962] as image format.jpeg. Then, next stage is feature extraction operation by using HOG algorithm [10], which is deemed as a powerful feature shape descriptor of an image. Then, the output features are stored in the database as a reference model to be used in the prospective matching with anyone who wants to verify her / his signature. In the authentication process, the queried identity signature will be read by the system. The same processes that have taken place during the enrollment operation should also be applied to the queried signature sample.

In the classification process, SVM is used to compare the enrolled and authenticated signature features. Finally, decision maker based on threshold decides whether the signature must be accepted or rejected.

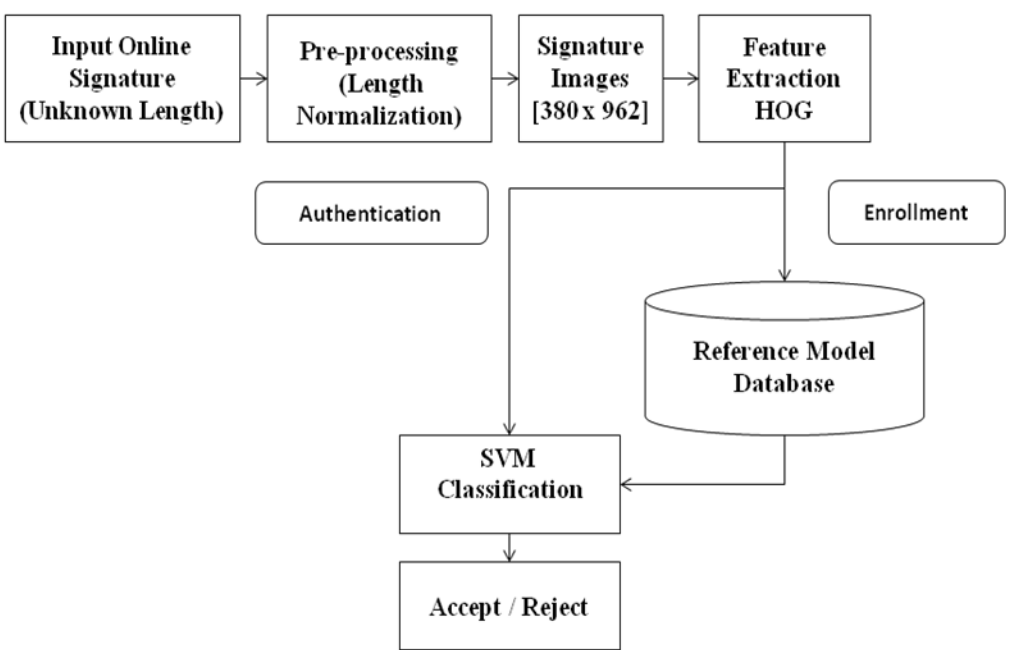

Figure 1: Diagram of the system stages.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1 PRE-PROCESSING (LENGTH NORMALIZATION)

The online signature normalization has been adapted from [20], as it works by transforming an unknown signature sample of a variety length N into the desired signature length $\overline{N}$ without distorting the signature sample.

The implementation idea is based on Up-Sampling [22] and Down-Sampling [22]. Up-Sampling is defined as follows: the output $F[n]$ of a 2 factor up sampling is obtained by interlacing the input sequence $E[n]$ with zero value. To smooth the Up-Sampler operation, a specific value is inserted instead of zero interlacing, which is estimated by performing an average neighborhood interpolation as shown in (1):

$$value = \frac{E[n] + E[n+1])}{2} \quad (1)$$

Down-Sampling is defined as follows: if $G[n]$ is the input of a 2 factor down sampling, and then the output is $H[n] = G[2n]$. Down-Sampling is required for those signatures that have signing duration N larger than the desired length $\overline{N}$, whereas Up-Sampling is required for those signatures that have signing duration N less than the desired length $\overline{N}$. Normally, Up-Sampler and Down-Sampler are applied to linear discrete-time systems. In this paper, desired length $\overline{N}$ has been chosen as 256 as the average signature length of the SIGMA Database. This type signature normalization has eliminated the drawback of the intra-user variability by providing a fix length of signature samples without any side-effects. The normalized signature samples achieved 3.4% as an average of the error rate by running the experiment to the same SIGMA database. It is worth to mention that, in this work feature extraction was PCA, in which the resulted feature vector have been trained and tested by ANN, More details are in [20].

3.2. ONLINE TO OFFLINE SIGNATURE CONVERSION

Next step is converting from online to offline signature as the main scope of this paper is doing verification for offline signature. Converting operation has been implemented using matlab-2016 for the all SIGMA database [21] by plotting the signature then storing the figure plot as an image with the same name either genuine or forge signature, it is worth to mention that the size of each signature image is [380 x 962] as image format .jpeg as illustrated in Figure 2. Ultimately, offline signature database has been built to be used for the experiment to evaluate the performance.

3.3. FEATURE EXTRACTION (HISTOGRAM ORIENTATION GRADIENT)

Histogram Orientation Gradient (HOG) is used for feature shape representation, which was introduced by Dalal and Triggs at the CVPR conference in 2005 [10].

HOG is basically used for person detector, which stands for Histograms of Oriented Gradients. In this research, HOG has been adopted to be as a feature extraction technique to recognize and authenticate the signature image.

Theoretically, the HOG descriptor technique counts occurrences of gradient orientation in localized portions of an image or region of interest (ROI). The basic implementation of the HOG descriptor, which is illustrated in Figure 3, is as follows: First, dividing the image into small connected regions (cells), and for each region compute a histogram of gradient directions or edge orientations for the pixels within the cell, then, using the gradient orientation obtained. After that, discretizing each cell into angular bins, then, each cell's pixel contributes weighted gradient to its corresponding

Figure 2: Offline signature samples as biometric.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

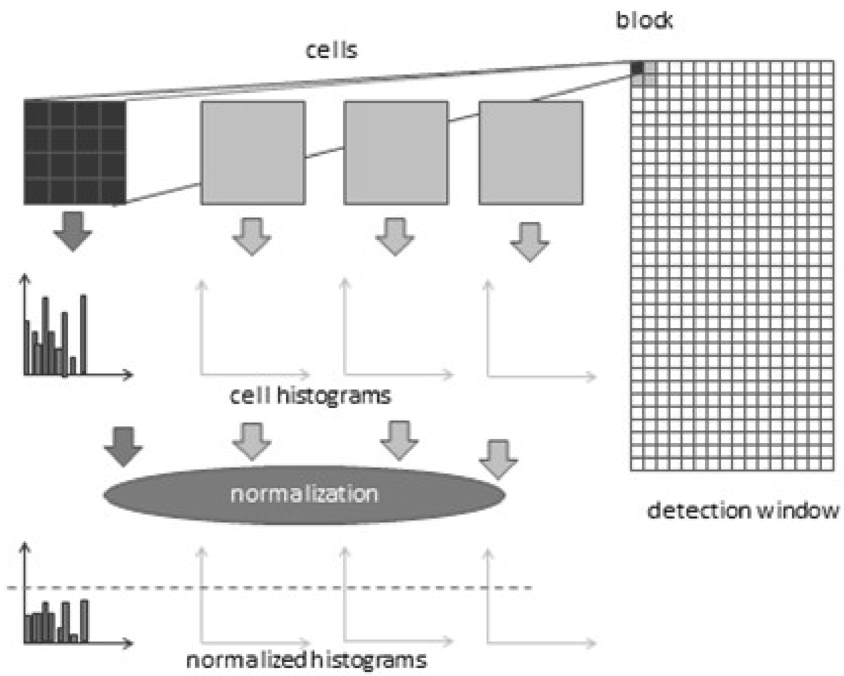

Figure 3: Demonstrates the HOG algorithm implementation.

angular bin, then, adjacenting cells are grouped into blocks in the spatial region. This forms the basis for grouping and normalization of histograms, finally, normalized group of histograms represents the block histogram and the set of these block histograms represents the descriptor.
In other words, computation of the HOG descriptor requires the following basic configuration parameters, masks to compute derivatives and gradients, geometry of splitting an image into cells and grouping cells into a block, block overlapping and normalization parameters.

In this paper, the HOG is characterized as a block size is [22x22] pixels, the cell size is 128 with 9 bin histogram per cell. Accordingly, the overall feature vector length is 216 used to represent each signature image sample. Figure 4 depicts two offline handwritten signatures with a variety of cell size that has been implemented in this research and viewed to elaborate the HOG implementation on offline signature. It is clear that, when the cell size is low, the number of plotted gradient and directions extensively exist clearer than the high cell size. Gradually, by increasing the cell size number of HOG parameter, the directions and gradient will be decreased. In Figure 4, cell size has been plotted ranging from 16 until 128 depicting the effects of HOG on the offline signature images.

3.4. CLASSIFIER (SUPPORT VECTOR MACHINE)

Support Vector Machine (SVM) is a machine learning algorithm, which is considered as a supervised learning models with associated learning algorithms that analyze data used for classification and regression analysis. SVM was developed from Statistical Learning Theory (Vapnik & Chervonenkis) [23].
It can be defined as a representation of the examples as points in space, mapped so that the examples of the separate categories divided by a clear gap that is as wide as possible. Then, new examples are mapped into that same space and predicted to a category based on which side of the gap they fall as shown in Figure 5.
In addition to performing linear classification, SVMs can efficiently perform a non-linear classification using different Kernel types.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

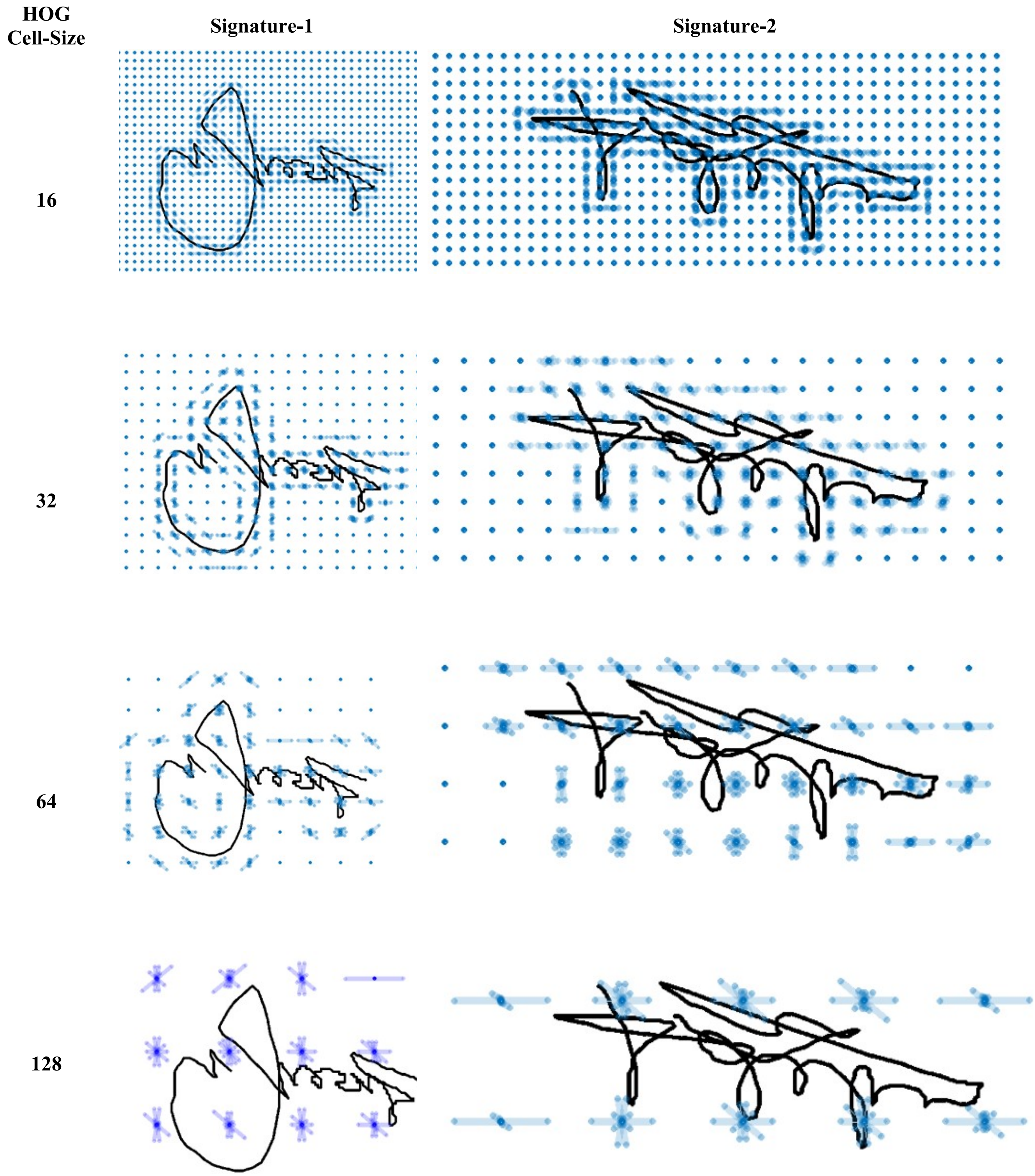

Figure 4: shows HOG implementation on offline signature with 4-set Cell size

Journal of Theoretical and Applied Information Technology
30th April 2018. Vol.96. No 8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

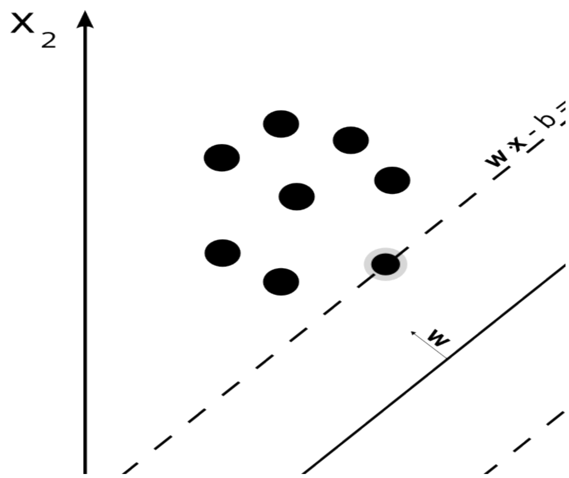

Figure 5: Illustrate SVM margin separating between two examples.

In this paper, linear kernel SVM has been exploited for the classification, as experimentally outcome the best result better than polynomial, RBF, quadratic, etc. If there is a training dataset of n points of the form, $\vec{x}_i$ is input features and $\vec{y}_i$ is the class for the input features.

$$(\vec{x}_i, y_i) \dots (\vec{x}_n, y_n)$$

Where the (y_i) are either $(+1)$ or (-1) , each indicating the class to which point $(\vec{x}_i)$ belongs. Each $(\vec{x}_i)$ is a p-dimensional real vector. In the SVM, it is required to find out the maximum margin hyperplane that divides the group of points $(\vec{x}_i)$ for which $(y_i = +1)$ from the group of points for which $(y_i = -1)$,,which is defined so that distance between the hyperplane and the nearest point $(\vec{x}_i)$ from either group is maximized. Any hyper plane can be written as the set of points $\vec{x}$ satisfying the following formula:

$$\vec{w}.\vec{x} - b = 0$$

Where $\vec{w}.\vec{x} - b = -1$ is considered as a separate of one class and $\vec{w}.\vec{x} - b = +1$ is considered as a separate of another class. Besides that, where $\vec{w}$. is the normal vector to the hyperplane. The parameter $\frac{b}{\|\vec{w}\|}$ (as shown in Figure 5) determines the offset of the hyperplane from the origin along the normal vector $\vec{w}$. According to the method, which is used here for finding the separating hyperplane type of the SVM optimization, is Sequential Minimal Optimization (SMO).

In this paper SVM has been used as a binary classification for each user type in the SIGMA database. In other words, for each user SVM must classify the user genuine signature samples to give as core +1, while the forged signature samples of the users is assigned as score -1.

Accordingly, once, there are 200 users in SIGMA database, 200 SVM training operation has been done in the experiment, in each training there will be testing classification to output +1 as genuine signature or -1 as forged signature. Certainly, the threshold used here for making the decision whether genuine or forge is 0, as the best and unbiased separation between -1 and +1 scores.

4. EXPERIMENT

The experiment rule is conducted on the offline signature template to measure the verification accuracy of the proposed offline signature verification method. The experiment is implemented according to the following steps:

1- Using signatures from the SIGMA database[21], the SVM training matrix is built. The training matrix consists of signatures from 200 individuals, for each individual, 10 genuine samples and 10 forged samples are obtained (five of them are random forged samples and the rest are skilled forged samples). Each signature sample is represented by 216 features. Accordingly, the training matrix size is $[20 \times 216]$(216 features for each sample with 20 samples for each individual). Training is run by SVM for the signatures of each individual separately.

2- The evaluation of the result produced by SVM is done by extracting the False Accept Rate (FAR) and the False Reject Rate (FRR) for each individual separately. The testing matrix is built similar to the way the training matrix was built.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3- In the training target (destination) of SVM, a sign $+1$ is assigned to the first 10 signature samples of the trained matrix, conversely, -1 is assigned to the second 10 signature samples of the training matrix to mark and train the SVM that the first 10 are genuine samples and the second 10 are forged samples.

4- The threshold that has been used is (zero).

5- FRR is computed by evaluating the resulting scores of the first 10 samples. If any sign of the first 10 samples is less than the threshold, False Rejection (FR) counter will be increased by one $(FR = FR + 1)$, since they are supposed to be as accepted (signs are larger than threshold) but they are wrongly rejected by the verifying system. On the other hand, if the results of the second 10 samples have signs more than the threshold, they are considered as False Accept (FA) and the counter will be incremented by one $(FA = FA + 1)$.

The FAR and FRR are computed as in (3) and (4) respectively:

$$\mathrm{FAR} = \frac{\mathrm{FA}}{10} \times 100\% \qquad (3)$$

$$\mathrm{FRR} = \frac{\mathrm{FR}}{10} \times 100\% \qquad (4)$$

6- The accuracy of each user is computed by using (5):

$$\mathrm{User}_{\mathrm{Accuracy}}\% = 100 - \frac{\mathrm{FAR}+\mathrm{FAR}}{2} \qquad (5)$$

7- Then, to take into consideration all individuals in the SIGMA database, an average of the 200 individuals' accuracy is computed by using (6):

$$\mathrm{AVR}_{\mathrm{Accuracy}} = \frac{1}{200}\sum_{u=1}^{200} \mathrm{User}_{\mathrm{Accuracy}}[u] \qquad (6)$$

5. RESULT AND DISCUSSION

Concerning the result of the experiment, Table 1 lists FAR, FRR and their average of the proposed recognition algorithm:

TABLE 1: THE PERFORMANCE OF THE PROPOSED ALGORITHM

FAR %	FRR %	Accuracy %
3	*3.35*	*96.8*

In order to consolidate the result of this paper, a comparison study has been done with set of benchmarks works published recently as in Table 2 compares the results of proposed scheme with some of the existing signature recognition algorithm.

As it is clear of Table 2, that FAR and FRR are less than the existing work, which has been used as a benchmark that recently published. In terms of FAR the proposed work is 3%, which is less than that in paper [17] as 5.05% and paper [18] as 4.9%. Regarding to the FRR error, the proposed work is 3,35%, which is less than the aforementioned article papers as FAR is 4.25% and 5.2% for the paper [17], [18] respectively.

It is worth to mention that, the main contribution of this paper is using HOG, which has been discovered as it is quite useful for offline biometric feature extraction by getting promising recognition rate in the future, since it has been confirmed that this research's result outperforms the state-of-the-art of offline signature recognition as shown in Table 2 comparison.

TABLE 2: THE PERFORMANCE OF THE PROPOSED ALGORITHM

Existing Techniques	*FAR (%)*	*FRR (%)*
Normalized Static Features and ANN Classification[17] / 2016	*5.05*	*4.25*
Normalized Weighted Coefficients[18] / 2016	*4.9*	*5.2*
Proposed Scheme	***3***	***3.35***

However, setting up small HOG parameters (cell size, block size, bin) will increase the length of the feature vector of the signature represented sample

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and that will cause much time consuming for the classifier and results low processing speed of the recognition. For this reason a balance maintaining of the HOG parameters selecting (not so small and not so large) will lead to the optimized and promising results in terms of both recognition accuracy and processing speed.

6. CONCLUSION

Static handwritten signature verification has been implemented using function features, which has been extracted based on Histogram Orientation Gradient (HOG) of the signature image. Then, the features of signature samples are passed to the classifier of the proposed verification system, which is SVM. The experimen thave been conducted and showed a fruitful accuracy as 96.8% as the FRR is3.35%, and FAR is 3%. In the end, the results demonstrate a significant improvement in FAR and FRR. For the future work, more improvement to the recognition rate might be done by using a stronger feature shape descriptor or using hybrid feature extraction such as combining HOG with PCA to build the presented feature vector of the signature sample.

REFERENCES

[1] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE,* vol. 91, no. 12, pp. 2021-2040, 2003.

[2] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Offline handwritten signature verification-literature review," *arXiv preprint arXiv:1507.07909*, 2015.

[3] S. M. S. Ahmad, B. M. Ali, and W. A. W. Adnan, "Technical issues and challenges of biometric applications as access control tools of information security," *international journal of innovative computing, information and control,* vol. 8, no. 11, pp. 7983-7999, 2012.

[4] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE security & privacy,* vol. 99, no. 2, pp. 33-42, 2003.

[5] F. L. Malallah, S. S. Ahmad, S. Yussof, W. W. Adnan, V. Iranmanesh, and O. Arigbabu, "A Review of Biometric Template Protection Techniques for Online Handwritten Signature Application," *International Review on Computers and Software (I. RE. CO. S.),* vol. 8, no. 12, 2013.

[6] B. Miroslav, K. Petra, and F. Tomislav, "Basic on-line handwritten signature features for personal biometric authentication." pp. 1458-1463.

[7] D. Impedovo, and G. Pirlo, "Automatic signature verification: The state of the art," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews),* vol. 38, no. 5, pp. 609-635, 2008.

[8] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri, "Cancelable templates for sequence-based biometrics with application to on-line signature recognition," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans,* vol. 40, no. 3, pp. 525-538, 2010.

[9] S. Elliott, and A. Hunt, "Dynamic signature forgery and signature strength perception assessment," *IEEE Aerospace and Electronic Systems Magazine,* vol. 23, no. 6, pp. 13-18, 2008.

[10] N. Dalal, and B. Triggs, "Histograms of oriented gradients for human detection." pp. 886-893.

[11] J. A. Suykens, and J. Vandewalle, "Least squares support vector machine classifiers," *Neural processing letters,* vol. 9, no. 3, pp. 293-300, 1999.

[12] T. Dash, T. Nayak, and S. Chattopadhyay, "Offline Handwritten Signature Verification using Associative Memory Net," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* vol. 1, no. 4, pp. pp: 370-374, 2012.

[13] P. Narkhede, and V. Ingle, "Offline Handwritten Signature Recognition using Artificial Neural Network Techniques."

[14] M. H. Sigari, M. R. Pourshahabi, and H. R. Pourreza, "Offline handwritten signature identification and verification using multi-resolution gabor wavelet," *International Journal of Biometric and Bioinformatics,* vol. 5, 2011.

[15] G. Alvarez, B. Sheffer, and M. Bryant, "Offline Signature Verification with Convolutional Neural Networks."

[16] G. Sulong, A. Y. Ebrahim, and M. Jehanzeb, "Offline handwritten signature identification using adaptive window

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

positioning techniques," *arXiv preprint arXiv:1407.2700*, 2014.

[17] M. Trikha, M. Singhal, and M. Dutta, "Signature Verification using Normalized Static Features and Neural Network Classification," *International Journal of Electrical and Computer Engineering,* vol. 6, no. 6, pp. 2665, 2016.

[18] M. Singhal, M. Trikha, and M. Dutta, "Time Independent Signature Verification using Normalized Weighted Coefficients," *International Journal of Electrical and Computer Engineering,* vol. 6, no. 6, pp. 2658, 2016.

[19] B. Zhang, "Offline signature verification and identification by hybrid features and Support Vector Machine," *International Journal of Artificial Intelligence and Soft Computing,* vol. 2, no. 4, pp. 302-320, 2011.

[20] F. L. Malallah, S. M. S. Ahmad, W. A. W. Adnan, O. A. Arigbabu, V. Iranmanesh, and S. Yussof, "Online handwritten signature recognition by length normalization using up-sampling and down-sampling," *International Journal of Cyber-Security and Digital Forensics (IJCSDF),* vol. 4, no. 1, pp. 302-313, 2015.

[21] S. M. S. Ahmad, A. Shakil, A. R. Ahmad, M. A. M. Balbed, and R. M. Anwar, "SIGMA-A Malaysian signatures' database." pp. 919-920.

[22] R. A. Gopinath, and C. S. Burrus, "On upsampling, downsampling, and rational sampling rate filter banks," *IEEE transactions on Signal Processing,* vol. 42, no. 4, pp. 812-824, 1994.

[23] V. N. Vapnik, "An overview of statistical learning theory," *IEEE transactions on neural networks,* vol. 10, no. 5, pp. 988-999, 1999.