

# Histogram of Oriented Gradient (HOG) for Off-Line Handwritten Signature Authentication

Shafaf Ibrahim, Nur Aqilah Najwa Samlan

Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Jasin, Melaka, Malaysia

shafaf2429@uitm.edu.my, qylanajwa@gmail.com

## ABSTRACT

Security is needed as it could secure the routine activities particularly when it comes to document-related works. The signature authentication system is being used widely in this era of technology to authenticate an individual's identity. Yet, several problems such as the increasing number of forge signature still occur, which induced a need for an efficient signature authentication system. The human eyes could not differentiate between the genuine and forge signature, and the traditional method to authenticate a signature in financial institutions mainly is very time-consuming. Thus, an off-line handwritten signature authentication using a technique of Histogram of Oriented Gradient (HOG) is proposed. HOG is a gradient-based feature extraction method. Initially, the offline handwritten signature images will go through the pre-processing and image enhancement processes such as binarization, thinning, noise removal, and resizing. Next, the shape feature is extracted using the HOG which produced the feature vector values. Different images will have different feature vector values. These values are then be used to measure the similarity between the genuine and tested signatures using Euclidean distance. Three threshold values are used for the performance analysis of the HOG signature authentication which are 15, 20, and 30. From the analysis conducted, it is found out that 15 and 20 are the best threshold values for HOG which returned good performance of 87.5% for Overall Accuracy (OA). It is expected that the outcome of this study may assist the user in the off-line handwritten signature authentication in the future.

**Key words:** Histogram of Gradient (HOG), offline handwritten signature, authentication, Euclidean distance

## 1. INTRODUCTION

Individual biometric authentication has become a growing trend. With the rapid development of information technology, personal authentication is becoming more necessary and even crucial in many fields [1]. In addition, it has already become a necessity in modern organizations and businesses. Among many existing biometrics used for person authentication, handwritten signature authentication is the most widely

researched one [2]. Referring to the study conducted by [3], the handwritten signature remains the most widely accepted form of confirmation and it is used to authenticate one's identity.

Signature authentication and identification is a technology that can enhance security in our day to day transaction held in society [4]. Generally, there are two types of signature authentication techniques [5] which are online and off-line. The off-line technique is known as dynamic signature authentication which works on handwritten documents. According to [6], in the off-line signature authentication technique, images of the signatures written on paper are captured using a scanner or a camera. The off-line authentication only covers the images which are obtained from a scanner or digital camera [7]. An off-line signature authentication uses some mechanism as a classifier and some sample signatures are stored in a database [8].

An off-line signature authentication system generally consists of four components such as data attainment, processing, extraction of features, identification, and authentication [9]. The authentication process must rely entirely on features which can only be extracted from the static signature picture.

Some of the off-line signature authentication applications include the authentication of bank cheques, identity cards, administrative forms, formal agreements, acknowledgment of services received and many more [3]. The basic nature of human eyes could not authenticate the signatures [10]. Human eye may have difficulty in identifying the fraudulent signatures accurately, as the individual intricacies of each signature vary each time a person signs. A study in [11] stated that, it is difficult for any expert's eye to verify the ratios between lines and angles of a genuine signature and fraud signature precisely as human eyes is prone to error. Additionally, the traditional authentication method is claimed to be very time-consuming [9]. The cheque is taken in the back room and then it is authenticated manually by a person present over there using our previous documents which are signed and stored [12].

Previously, an algorithm known as Dynamic Time Warping (DTW) is used to authenticate the signature. It is one of the

algorithms for measuring the similarity between two temporal time series sequences, which may vary in speed. However, the DTW for signature authentication forming a misalignment scores between the authenticating signature and a set of template signatures [13]. Many other problems regarding the handwritten signature due to signature forgery cases are also discussed [14]. A huge increase in forgery cases relative to signatures induced a need for efficient signature authentication system [15]. There are many types of forgeries such as simulation, tracing, cut and paste, electronic forgeries and freehand signature [16].

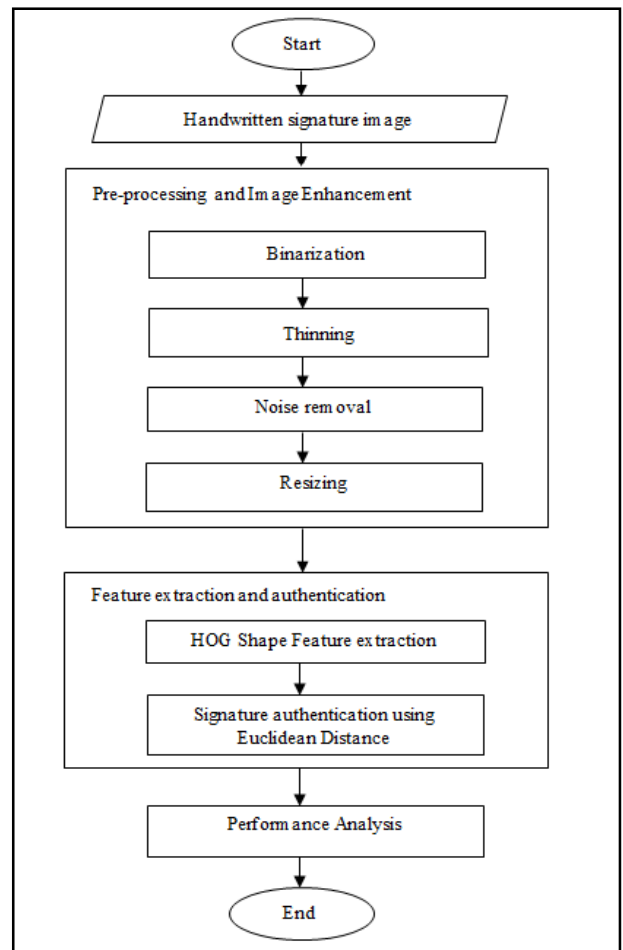
The importance of off-line signature authentication is to distinguish the genuine signature from the forgery [17]. It is a useful application in bank service and forgery detection as it provides an accurate person identification method based on the signature. Yet, although off-line signature authentication is difficult to design [7], it is still essential to authenticate one's identity as most of the financial transactions are still done on paper.

Thus, based on the problem discussed it is necessary to initiate an alternative technique to authenticate the off-line signature automatically. The Histogram of Oriented Gradients (HOG) is a very efficient feature descriptor based on gradient and does not require any language-dependent pre-process [18]. It is a directional features used to increase the accuracy of previous off-line signature authentication system. It was proven that it is one of the most effective features that represent information of local gradient directions by counting occurrences of gradient orientations in localized zones of an image [19]. As a result, HOG perform better than wavelet features.

Therefore, this paper presents a study of HOG for off-line signature authentication in avoiding signature forgeries problem. The organization of the remainder of this paper is as follows: Section 2 provides our methods, including an overview of the methodology, and the description of algorithm structure. Our results and discussions are discussed in Section 3. Finally, in Section 4, we present our conclusion.

**2. RESEARCH METHODS**

The aim of this study is to implement the HOG technique for off-line handwritten signature authentication. Figure 1 portrays the flowchart of this research.



**Figure 1:** Flowchart of proposed research

**2.1 Handwritten Signature Images**

Various handwritten signature images were collected in this phase. Fifty signatures from 10 individuals were taken as sample images. The images were collected from [20]. These signatures have different shape, width and height. The signatures are divided into two types of genuine and forge signatures. Table 1 tabulates the samples of handwritten image collected.

**Table 1:** Samples of Handwritten Images



No.	Genuine Signature	Forge Signature
1		
2		
3		
4		

**2.2 Pre-processing and Image Enhancement**

Generally, there are a few sub-processes in the pre-processing and image enhancement steps. The main objective of these stages is to make signatures standard and ready for feature extraction. There are four steps to be performed in this stage such as binarization, thinning, noise removal and resizing. These steps are explained further in the next sub-section.



**2.2.1. Binarization:** The binarization can be performed by extracting both brightness and density of an image [21]. Each image’s pixel is converted into ‘0’ or ‘1’ bit depends on value of mean of all pixel. The value will be ‘1’ if it is greater than the mean value. Otherwise, the value will be ‘0’, In other words, binarization is a process of converting coloured image to black and white. Figure 2 illustrates the sample of signature images before and after the binarization process.

**Table 2:**Sample of Handwritten Image Before and After Binarization

Before Binarization	After Binarization
	



**2.2.2. Thinning:** The thinning process helps to reduce the redundant information and maintain the main structure information of the original data [22]. In this study, the thinning process is implemented to reduce the thickness of the signature images. People may not use the same pen every time they want to sign on a paper. They may use a different pen. So, their signature’s thickness will be affected. The data collected show that one signer have many different signature’s thickness. It is due to the pen that they used. Hence, it is important to perform this step to ensure the equality of both signatures. Besides, the features could be extracted much easier afterwards. Table 3 portrays the signature images before and after thinning process.

**Table 3:** Sample of Handwritten Image Before and After Thinning

Before Thinning	After Thinning
	



**2.2.3. Noise Removal:** The noise is anything that is not prominent to the image but it can be noticed [23]. It can appear in the shape of dots and so on. When there is a noise, other image process will be difficult to be performed and it will definitely affect the prototype accuracy. Hence, to overcome the noise problem, image enhancement process is needed. The *Bwareaopen* technique is implemented in this phase. Table 4 illustrates the signature images before and after the noise removal process.

**Table 4:**Sample of Handwritten Image Before and After Noise Removal

Before Noise Removal	After Noise Removal
	

**2.2.4. Resizing:** Traditional image resizing methods usually work in pixel space and use various saliency measures. The challenge is to adjust the image shape while trying to preserve important content [24]. The resizing can be done either by decreasing or increasing the total number of pixel. In this study, it is necessary to resize the image’s size as the image’s sizes are varying. In order to resize the image, the signature image is resized to be similar size with the reference signature image which resulted to the same total number of pixel in both images. Table 5 illustrates the signature images before and after the resizing process.

**Table 5:**Sample of Handwritten Image Before and After Resizing

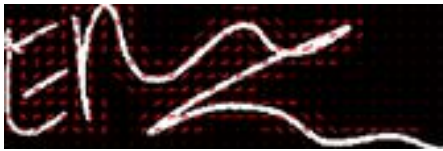
Before Resizing	After Resizing
	

**2.3 Feature Extraction and Authentication**

Feature extraction is the most vital step in image processing. The aim of feature extraction is to extract the image’s feature as ideal as possible. It is also useful in classifying and recognizing the image [25]. There are many feature extraction techniques found in literature, but HOG had been implemented as a technique to extract the off-line handwritten signature features.

HOG is a gradient based feature extraction method. It involves computing the gradient information at each pixel inside a particular grid zone [19]. It can be done either by using Cartesian or Polar grid zone. After finding the gradient orientations at each point, dominant gradient orientation must be finding in order to represent it at the first bin of histogram [26].

In gradient calculation stage, image is separated to 4x4 block size. These blocks have the area of 16x16 pixels cell size. Each cell has its own magnitude and direction information. Gradient directions are split up equal region between 0 to 180 or 0 to 360 degrees in the calculation of histograms. In this part of study, the feature extraction from the resized handwritten signature image is processed and as a result, HOG features vectors are obtained from each signature image with this algorithm. Figure 2 portrays the sample outcome of feature extraction process by using HOG technique.



**Figure 2:**Feature extraction using HOG technique

In another note, the Euclidean distance technique is employed for the authentication purpose. The Euclidean distance is one of the simple distance classifier, under template matching which is widely used in image processing. In the authentication process, the authenticated signature is evaluated by compare its features against reference signature. It is used to classify the testing signature into genuine or forgery [27]. Before the image could be authenticate, the differences between reference image’s HOG feature value and tested image’s HOG value is calculated. It can be calculated by using Euclidean distance. There are three threshold values used in testing which are 15, 20 and 30. If the Euclidean distance value is found to be below threshold value, it will authenticate the signature to be forged. Otherwise, it will authenticate as genuine. The Euclidean distance can be calculated using Eq. (1), Eq. (2) and Eq. (3).

$$Euclidean\ Distance\ (d) = \sqrt{\sum_{i=1}^n (a_i - b_i)^2} \quad (1)$$

where:

a = total number of feature vector in the reference signature image

b = total number of feature vector in the tested signature image

$$If\ d > Threshold = Forge\ Signature \quad (2)$$

$$If\ d < Threshold = Genuine\ Signature \quad (3)$$

### 2.4 Performance Analysis

The accuracy testing is conducted in analyzing the performance of HOG signature authentication. There are four types of accuracy that needs to be considered. Table 6 explains these types of accuracy.

**Table 6:**Types of Accuracy

Type of Accuracy	Explanation	Accuracy Formulae
True Positive (TP)	The accuracy of genuine signature found to be genuine	$\frac{No.\ of\ authenticate\ genuine}{Total\ no.\ of\ genuine\ image\ tested} \times 100$ (4)
False Negative (FN)	The accuracy of genuine signature found to be forge	$\frac{No.\ of\ authenticate\ forge}{Total\ no.\ of\ genuine\ image\ tested} \times 100$ (5)

True Negative (TN)	The accuracy of forge signature found to be forge	$\frac{No.\ of\ authenticate\ forge}{Total\ no.\ of\ forge\ image\ tested} \times 100\%$ (6)
False Positive (FP)	The accuracy of forge signature found to be genuine	$\frac{No.\ of\ authenticate\ genuine}{Total\ no.\ of\ forge\ image\ tested} \times 100\%$ (7)

Subsequently, according to the accuracy obtained in Table 6, the overall accuracy (OA) of the offline handwritten signature authentication is calculated using Eq. 8:

$$Overall\ Accuracy\ (OA) = \frac{TP+TN}{TP+FN+TN+FP} \times 100\% \quad (8)$$

### 3. RESULTS AND DISCUSSIONS

The performance of HOG signature authentication is tested to fifty testing signature images using three threshold values which are 15, 20 and 30. The authentication accuracy is evaluated using comparison with genuine signature image which acted as the reference image. Table 7 demonstrates the HOG authentication summary.

**Table 7:**Offline Signature

Type of Accuracy	Threshold 15	Threshold 20	Threshold 30
TP	83.33%	95%	100%
FN	16.67%	5%	0%
TN	91.67%	80%	61.67%
FP	8.33%	20%	38.33%
<b>OA</b>	<b>87.5%</b>	<b>87.5%</b>	<b>80.84%</b>

Based on the Table 7, threshold 30 returned 100% TP and 0%FN accuracy which indicates that there is no genuine signature is found to be forge. However, TN accuracy is also high which is 61.67% due to many forge signatures is found to be genuine.

On the other hand, threshold 20 produced 95% TP and 5% FN accuracy which means that there are only 5% of the genuine signatures found to be forged. 80% of forge signatures are authenticated to be forged. But, FP accuracy is still high which is 20% due to many forge signatures are found to be genuine.

Lastly, threshold 15 conveyed 83.33% genuine and 16.67% FN accuracy which signifies that, there is a lot of genuine signatures are found to be forged. But, the forge accuracy is higher than another two threshold values which is 91.67% forged signatures are authenticated accurately as forge. Whereas, fewer number of forged signatures are found to be genuine that led to 8.33% of FP accuracy.



After considering the OA, 15 and 20 are the best threshold value as both OA returned 87.5% as compared to threshold 30 which returned a slightly lower value of OA which is 80.84%. However, the performance of threshold 30 could not be underestimated as it produced 100% TP. However, higher percentage of FP is noticeable which affect the overall accuracy of threshold 30. To sum up, 15 and 20 are the best threshold values for HOG off-line handwritten signature authentication.

## 5. CONCLUSION

This paper presents a study on off-line handwritten signature authentication using a technique of Histogram of Oriented Gradient (HOG). The HOG is used to extract the shape features in analyzing the characteristics of the signatures. In another note, the Euclidean distance is used for the authentication purpose. The performance of the HOG signature authentication is tested to fifty testing signature images using three threshold values which are 15, 20 and 30. The application has been successful for a variety of testing images. The overall accuracy percentage demonstrated a strong accuracy which is 87.5% for both threshold 15 and 20. It can be inferred that the proposed off-line handwritten signature authentication using HOG is found to be successful. However, it is recommended that the latest feature extraction techniques such as deep convolutionary neural network be introduced and integrated in the future.

## ACKNOWLEDGEMENT

The research was supported by Ministry of Education Malaysia (MoE), and Universiti Teknologi MARA through the Fundamental Research Grant Scheme (FRGS) (600-IRMI/FRGS 5/3 (215/2019)).

## REFERENCES

1. C. S. Rao, K. V. S. Murthy, R. S. Shankar and V. M. Gupta. **A Novel Secure Personal Authentication System with Finger in Face Watermarking Mechanism**, in *Advances in Soft Computing and Machine Learning in Image Processing Studies in Computational Intelligence*, vol. 370, A. Hassanien and D. Oliva, Eds. Springer: Cham., 2018, pp. 319-353.
2. L. Yang, X. Jin, and Q. Jiang. **Online handwritten signature verification based on the most stable feature and partition**, *Cluster Comput* 22, pp. 1691-1701, 2019.
3. M. Arathi and A. Govardhan. **An Efficient Offline Signature Verification System**, *International Journal of Machine Learning and Computing*, vol. 4, no. 6, pp. 533-537, 2014.
4. H. Anand and D. Bhombe. **Enhanced Signature Verification and Recognition Using Matlab**, *International Journal of Innovative Research in Advanced Engineering (IJIRAE)*, vol. 1, no. 4, pp. 88-94, 2014.

5. V. Shashank, K. SachinKumar, B. Sandesh, M. D. Sunil, D. Souza, and K. R. Kusha. **Offline signature verification for the assessment of neurodegenerative diseases**, *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 5, pp. 323-324, 2019.
6. M. R. Kaur and M. P. Choudhary. **Handwritten Signature Verification Based on Surf Features Using HMM**, *International Journal of Computer Science Trends and Technology (IJCT)*, vol. 3, pp. 187-195, 2016.
7. P. R. Shahane, A. S. Choukade, and A. N. Diyewar. **Online Signature Recognition Using Matlab**, *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 3, no. VI, pp. 107-112, 2015.
8. M. S. S. Wagh and P. S. R. Gupta. **A Review on Offline Signature Verification and Recognition Using Neural Network**, *International Journal of Computer Science and Mobile Computing*, vol. 4, no. 3, pp. 725-731, 2015.
9. S. Mangale and V. Thombre. **A Survey on Efficient Image Retrieval through User Clicks and Query Semantic Signature**, *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 4, issue 5, pp. 8297-8301, 2016.
10. T. O. Oladele, K. S. Adewole, and A. O. Oyelami. **Forged Signature Detection Using Artificial Neural Network**, *African Journal of Computing & ICT*, vol. 7, no. 3, pp. 11-20, 2014.
11. W. Hussein, M. A. Salama, and O. Ibrahim. **Image Processing Based Signature Verification Technique to Reduce Fraud in Financial Institutions**, in *MATEC Web of Conferences*, vol. 76, 2016, pp. 05004.
12. C. V. Khatode and S. S. Morade. **Verification of Signatures on Bank Cheques**, *International Journal of Science, Engineering and Technology Research (IJSETR)*, vol. 4, issue 4, pp. 1098-1101, 2015.
13. J. Putz-Leszczynska. **Signature Verification: A Comprehensive Study of the Hidden Signature Method**, *International Journal of Applied Mathematics and Computer Science*, vol. 25, no. 3, pp. 659-674, 2015.
14. G. Ya, Z. Peng, C. Kim, K. Raymond, and S. Fu. **An improved online/offline identity-based signature scheme for WSNs**, *Taiwan Femto Technique*, vol. 18, pp. 1143-1151, 2016.
15. H. Patel, S. Desai, P. Desai, and A. Damani. **Review on Offline Signature Recognition and Verification Techniques**, *International Journal of Computer Applications*, vol. 179, no. 53, pp. 35-41, 2018.
16. O. A. Rosso, R. Ospina, and A. C. Frery. **Classification and Verification of Handwritten Signatures with Time Causal Information Theory Quantifiers**, in *PLoS ONE*, vol. 11, no. 12, 2016, pp. 1-19.
17. L. G. Hafemann, R. Sabourin, and L. S. Oliveira. **Offline Handwritten Signature Verification - Literature Review**, in *Proceedings of*

- the 7th International Conference on Image Processing Theory, Tools and Applications*, 2018, pp. 1–8.
18. K. Kumari and M. Shrivastava. **Factors Affecting the Accuracy of Automatic Signature Verification**, in *International Conference on Computing for Sustainable Global Development*, 2016, pp. 1805–1808.
  19. T. M. Ghanim. **Offline Signature Verification and Forgery Detection Approach**, in *2018 13th International Conference on Computer Engineering and Systems (ICCES)*, 2018, pp. 293–298.
  20. M. Liwicki M. I. Malik, L. Alewijnse, E. V. D. Heuvel, and B. Found. **ICFHR 2012 Competition on Automatic Forensic Signature Verification (4NsigComp 2012)**, in *Int. Conference on Frontiers in Writing Recognition*, 2012, pp. 823-828.
  21. N. Mehta, K. Liu, A. Y. Alibhai, I. Gendelman, P. X. Braun, A. Ishibazawa, O. Sorour, J. S. Duker, and N. K. Waheed. **Impact of Binarization Thresholding and Brightness/Contrast Adjustment Methodology on Optical Coherence Tomography Angiography Image Quantification**, *American Journal of Ophthalmology*, vol. 205, pp. 54-65, 2019.
  22. W. Miaomiao, L. Zhenglin, S. Fuyuan, and G. Lei. **An Improved Image Thinning Algorithm and Its Application in Chinese Character Image Refining**, *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China*, pp. 1870-1874, 2019.
  23. T. F. B Syedia, S. Muhammad, Y. Mussarat, and L. F. Steven. **Fundus Image Segmentation and Feature Extraction for the Detection of Glaucoma: A New Approach**, *Current Medical Imaging (2018)*, vol. 14, no. 1, pp. 77-87, 2018.
  24. M. Arar, D. Danon, D. Cohen-Or, and A. Shamir. **Image Resizing by Reconstruction from Deep Features**, *ArXiv*, 2019, abs/1904.08475.
  25. R. Goel, V. Kumar, S. Srivastava, and A. K. Sinha. **A Review of Feature Extraction Techniques for Image Analysis**, *International Journal of Advanced Research in Computer and Communication Engineering*, 6(2), pp. 55–58, 2017.
  26. M. B. Yilmaz and B. Yanikoglu. **Offline Signature Verification Using Classifier Combination of HOG and LBP Features**, in *2011 International Joint Conference on Biometrics (IJCB)*, 2011, pp. 1-7.
  27. S. N. Gunjal, B. J. Dange, and A. V. Brahmane, A. V. **Offline Signature Verification using Feature Point Extraction**, *International Journal of Computer Applications*, vol. 141, no. 14, pp. 6–12, 2016.