

Histogram Orientation Gradient For Offline Signature Verification Via Multiple Classifiers

Fadi Mohammad Alsuhiat^{1,*} and Fatma Susilawati Mohamad²

¹Department is first, then University or Company name, Insert a complete correspondence (mailing) address, Abbreviate US states, Include city and COUNTRY

²Department of Pharmacognosy, Faculty of Pharmacy, Anadolu University, 26470, Eskişehir, TURKEY

Abstract

Manuscripts should be accompanied by an abstract. The abstract should be clear, descriptive, self-explanatory and **between 100 to 250 words**. The abstract should briefly state the problem or purpose of the research, indicate the theoretical or experimental plan used, summarize the principal findings, and point out the major conclusions. Do not include references or formulae in the abstract.

Keywords: Signature Verification; HOG features extraction; KNN; SVR; SVM, DT; UTSig; CEDAR

Introduction

The signing process is one of the foremost critical forms utilized by institution to guarantee the privacy of the data and to secure it against any illegal access to or penetration of certain data. As individuals and organizations enter the digital era, there's a pressing requirement for a digital framework able of recognizing between genuine and fake signature, to ensure people's permission and determine the capabilities that are granted to them."

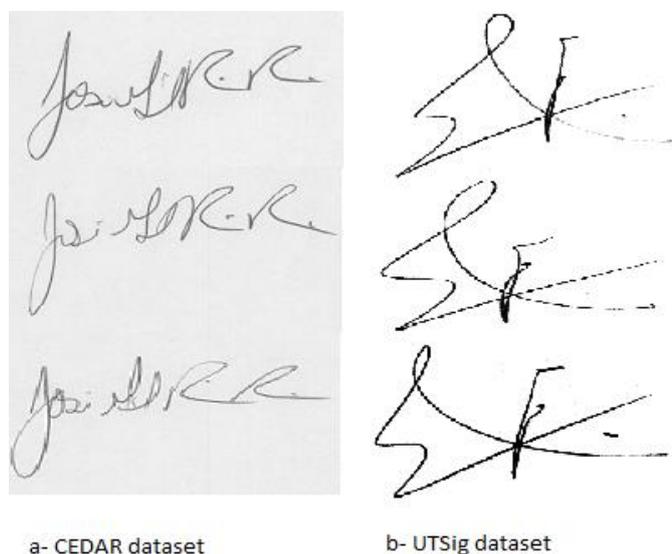
As a reference to the character, the signature is represented as an unusually composed drawing that the individual composes on any record. It is used because the person has a natural urge to sign a check, legal instrument, contract, or other documents, when someone tries to reproduce it, the problem occurs [1].

Signature verification system relies on check the individual's identity through using their handwritten signature; this system used specific elements such as (high and width) in order to identify an individual. Also, the signature verification system still the most socially and legally accepted methods for identifying an individual's [2]. In addition, Bharadwaja [3] pointed out that the signature verification system represents a basic and successful method to the distinction among a unique and fake mark.

In the digital era and with the means of growing technology the security and protection of information considered the most important topics in order to avoid phony and fraud in the data, therefore there are many methods to protect information such as facial recognition or fingerprint systems, although such systems the signature verification system is considered one of the most biometric features easy to verify people compared to other methods, where signature recognition models have two forms, online form and offline form [4].

In addition, the signature verification system has many advantages, as it is a socially acceptable method and the most secure method used in banks and credit card transactions. Also, the signature verification system is more efficient compared to other systems, because the user can change it as easy as the password, while there is no way to change the fingerprint or network patterns [5]. Figure (1) shows some various signatures done by same individual.

Figure 1. Some various signatures for the same person



A written by hand signature is an individual ability for people and incorporates a group of marks, elements, and characters drawn in a specific language, the signature is frequently utilized to permit people to perform a set of transactions, including banking operation, where the signature determine the legitimacy of the person, through making beyond any doubt that his/her signature is the genuine signature not forged [6].

According to Saikia and Sarma [7] handwritten signature is one of biometrics which used widely in personal authentication for individuals in many area such as banks and money transactions, despite handwritten signature is most common and secure way but there still some challenging's faced this system especially in phase of extracting features.

Biometric systems like handwriting signature contains two sections: first section is verification used for check the identity of user through biometric sample, while second section is identification which used for determine user among all persons stored in the system database [2].

In addition, handwritten signature consider a model of personal identification, which this model consisted three parts, first part is segmented a signature image into (vertical and horizontal) then extract the data from each individual parts, and finally compare the extracted data with the test signature samples.

On the other hand, the clustering is a method used to divide a set of data into several groups, each group being made up of identical elements, so the object of the clustering is to process the data by placing similar elements in one set and the different elements in separate sets, and the clustering method is used in multiple processes such as data extraction, pattern recognition, and image segmentation [8].

Therefore, our aim in this research is to explore the features extraction phase and the stage of classification for signature images. Therefore, we used Histogram Orientation Gradient (HOG) as features extraction algorithm, and four classifiers (SVM, SVR, KNN, and DT) have been selected and implemented on two signatures images datasets; UTSig dataset [9], and CEDAR dataset. UTSig dataset "has (115) classes containing: (27) genuine signatures; (3) opposite-hand signed samples, (36) simple forgeries and (6) skill

forgeries; we selected (2475) images as a training group to train the classification algorithms", while CEDAR dataset has consists of signatures from (55) writers. For each writer (24) original signatures and (24) skilled forgery signatures, the dataset consists of two folders; one folder contains the original signatures, while the other folder contains the skilled forgeries signatures.

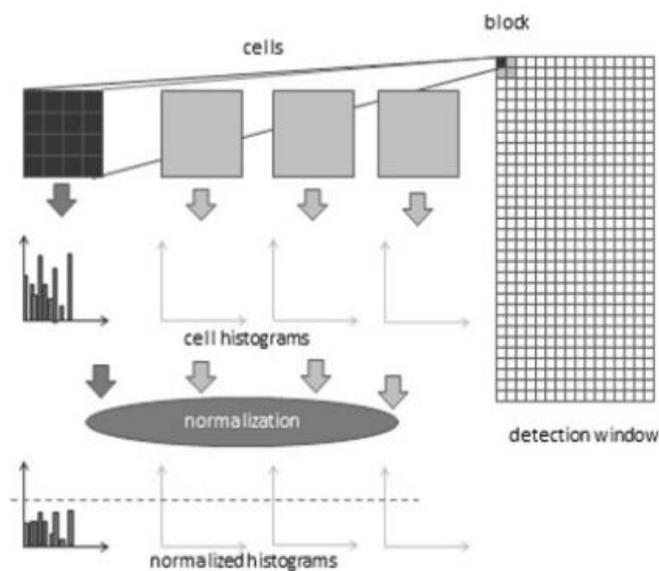
Overview of Methods

The features extraction approach and classification algorithms that are utilized for signature classification are described briefly in this part, as well as the comparison procedure. Feature normalization, feature extraction, and classification are the three phases of the suggested signature classifiers.

Features Extraction

In this research, a Hog technique was used for feature extraction phase. "Histogram Orientation Gradient (HOG) is utilized for trait shape representation, which was introduced by Dalal and Triggs [10] at the CVPR conference in 2005". 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 algorithm to identify and recognize the signature image.

Figure 2. Demonstrates the HOG algorithm implementation.



Hypothetically, the HOG descriptor method tallies events of angle introduction in localized parcels of a picture or locale of intrigued (ROI). The essential usage of the HOG descriptor, which is outlined in Fig 2, is as takes after: To begin with, partitioning the picture into little associated districts (cells) and calculate a histogram of the directions of angle and orientations edge for all pixels in each locale inside the cell, at that point, utilizing the gradient orientation gotten. After that, discretizing each cell into precise containers, at that point, each cell's pixel provides a weighted angle to the precise canister comparison; at that point, adjoining cells are gathered into pieces inside the spatial locale. This shapes the preface for histograms collecting and normalization, finally, the collected and normalized histograms speaks to the piece histogram and the group of square histograms speaks to the descriptor [11].

In this research, the HOG is characterized as block size is [4x4] pixels. Accordingly, the overall feature vector length is 34596 used to represent each signature image sample. Fig 3 depicts two offline handwritten signatures dataset with a variety of cell size that has been implemented in this research and viewed to elaborate the HOG implementation on the offline signature. According to Abbas, et al. [11] "when the cell

size is low, the number of plotted gradient and directions extensively exist clearer than the high cell-size. Gradually, exist clearer than the high cell size. Gradually, through increase the cell size number of the HOG parameter, the directions and gradient will be decreased". In Figure 3, cell size has been plotted ranging from 2 until 16 depicting the effects of HOG on the offline signature images.

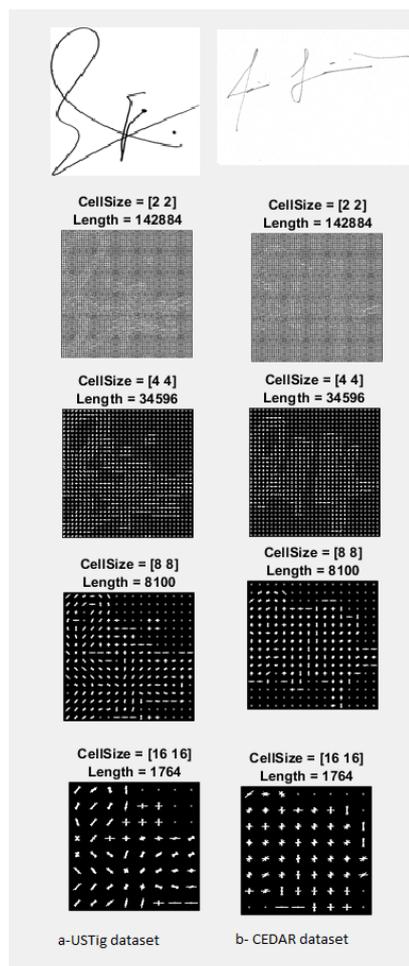
Signature Images Classification

In order to classify signature images as genuine or forged, different algorithms were used, including SVM, SVR, and KNN.

KNN: Consider a strategy for gathering elements based on the range of inner features' closest tests [12]. KNN is a common and straightforward classification method. As it combined spare distinctive vectors and markers of the learning pictures, inner gathering activities, it became a learning strategy.

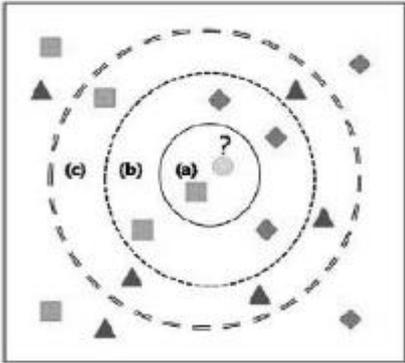
This unmarked position may be really assigned the title for its k closest neighbor's. Regularly, this thing will be categorized based on the marks of its k closest neighbor's by utilizing overwhelming portion surveying. On k=1, those parameters are categorized based on the power of the parameter closest to it. If there is a need for only two segments, then k should make an odd number. K may be an odd number when showing up multiclass arrangement. After we changed each photograph to the vector from claiming fixed-length for true numbers, we utilized the famous distance equation as a relatable point separation capacity for KNN which is Euclidean distance, in equation 1:

Figure 3. shows HOG implementation on offline signature with 4-set Cell size



$$d(x,y) = \left(\sum_{i=1}^m (x_i - y_i)^2 \right)^{1/2} \quad (1)$$

Figure 4. KNN Classification



SVM: this algorithm evaluates the signature according to a set of particular properties [13]. Through classify specific features for each signature image within the training process. In this algorithm, a signature classifier is trained by using the preparation data, in order to produce a signature prediction model using SVM algorithm, which uses characteristic vectors (x_i) as inputs, and Gaussian kernel K to configure the parameters of SVM, as shown in equation 2:

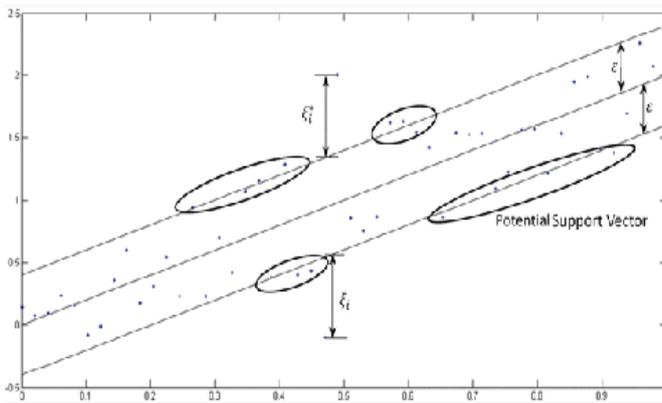
$$f(x) = \sum_{i=1}^{N_s} \alpha_i y_i K(s_i, x) + b$$

$$K(x_i, x_j) = e^{-\frac{1}{2\sigma^2} \|x_i - x_j\|^2} \quad (2)$$

SVR: SVR is characterized as an optimization problem that begins with identifying a curved-insensitive misfortune work to be minimized and locating the flattest tube that contains the majority of the preparation occurrences. SVR considers this function guessing problem to be an optimization problem in which the goal is to find the tightest tube centered around the surface while reducing the expectation mistake, or the difference between the expected and defined yields [14,15], as shown in equation 3.

Figure 5. One-dimensional linear SVR

$$f(x) = \langle w, x \rangle + b = \sum_{j=1}^M w_j x_j + b, \quad y, b \in \mathbb{R}, x, w \in \mathbb{R}^M \quad (3)$$

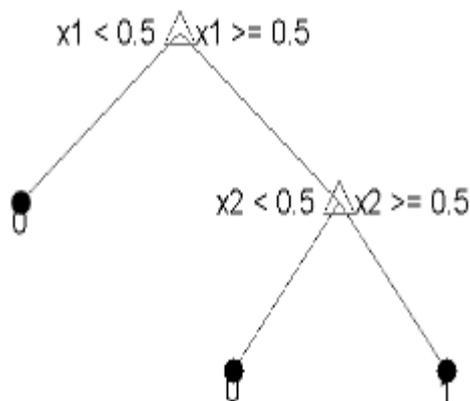


Decision Trees: A typical tree incorporates root, branches and clears out. The same structure is taken after in decision tree. It contains the root hub, branches, and leaf hubs. Testing a trait is on each inside hub, the result of the test is on department and lesson name as a result is on a leaf hub [16].

A root hub is the parent of all hubs and as the title proposes it is the highest hub in Tree. A choice tree may be a tree where each hub appears an include (trait), each connects (department) appears a choice (rule) and each leaf appears a result (categorical or proceeds esteem) [17].

As decision trees mirror the human level considering so it's so straightforward to seize the data and make some great translations. The complete thought is to form a tree-like this for the whole data and prepare a single result at each leaf, here is a simple classification tree:

Figure 6. Simple classification tree



Experimental Result

This section describe the three main parts of the implementation process of all classifiers, section (3.1) describes the dataset that used in this paper; section (3.2) indicate the setups of our experiment, while section (3.3) measure the performance for each algorithm through calculate the run-time and accuracy for each algorithm.

Database

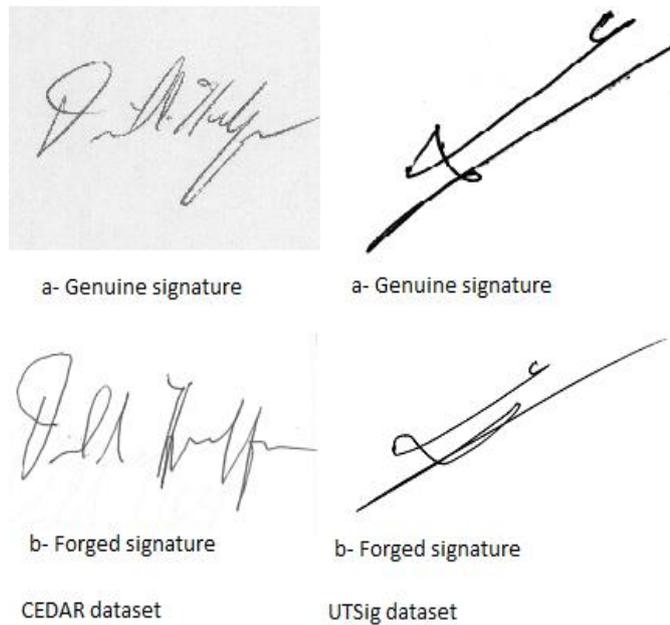
In order to implement the comparison process, we applying each algorithm two times by using two different datasets (UTSig and CEDAR). The "UTSig dataset consists of (8280) signature images for (115) persons, where each person has four classes of signature, including (27) genuine, (3) forgeries by using the opposite-hand, (36) simple forgeries, and (6) skill forgeries, as shown in Figure 6. This dataset was collected from the University of Tehran and Sharif University of Technology students, the signature images were digitized through scanned with 600 dpi resolution and stored as 8-bit Tiff files" [7, p1].

In this research for UTSig dataset, total of (3300) signatures were selected for trainset and (300) signatures were selected for testset.

CEDAR dataset consists of 55 signatures images belonging to a group of individuals from different professionals and cultural. Each individual signed 24 genuine signatures. Besides that, the forged signatures contain 24 forgery signature for each individual, where the forged signatures done by another individuals, therefore this dataset consists of (1,320) original signatures and (1, 320) forgery signatures [18].

In this paper for CEDAR dataset, total of (2200) signatures were selected for trainset and (440) signatures were selected for testset.

Figure.7 Signature images from UTSig and CEDAR datasets.



Experimental Setup

Four classifiers, SVM, SVR, KNN, and DT, were used to classify original-forgeries using features extracted from a HOG technique. In the UTSig dataset, (3300) signature images were trained for (100) people, with each person having 33 signatures (27 genuine and 6 forgeries), whereas the first model for the CEDAR dataset was trained using a set of signatures for (55) people, with each person having 40 signatures (20 genuine and 20 forgeries).

Table (1) shows the calculated run-time for each method. The result indicated that DT outperformed in both dataset (UTSig and CEDAR), than other algorithms (SVM, KNN and SVR).

Table 1 Run-Time values for each classifier

Method	Run-Time	
	UTSig dataset	CEDAR dataset
SVM	4.34	11.36
KNN	4.34	19.23
SVR	4.60	14.68
DT	3.04	2.32

Efficiency

For executing each technique on (300) signature images from the UTSig dataset and (440) signature images from the CEDAR dataset, the efficiency was measured in terms of time and accuracy values. The accuracy and time metrics for classification techniques are shown in Table II.

Table (2) shows the results of our experiment's testing, which included calculating the run-time and accuracy for each classifier. Results showed that DT outperformed (run-time) other classifier algorithms such as SVM, KNN, and SVR in both datasets (UTSig and CEDAR). Also, SVM and SVR reached accuracy better than other classifier algorithms in UTSig dataset, while SVM, SVR and DT reached accuracy better than KNN classifier in CEDAR dataset.

Table 2

Run-Time values and accuracy for each classifier

Method	Run-Time		Accuracy	
	UTSig dataset	CEDAR dataset	UTSig dataset	CEDAR dataset
SVM	1.02	1.52	92.93	99.77
KNN	1.90	46.23	65.66	69.09
SVR	0.71	1.19	92.93	99.77
DT	0.04	0.06	73.74	99.77

Conclusion and Future Work

This research conducted a comparison process among four classifier algorithms (SVM, KNN, SVR and DT) based on two signature images dataset (UTSig and CEDAR), The run-time and accuracy of each method were calculated as part of the comparison procedure. The four algorithms utilized are standard classification techniques. The comparison process based on two datasets (3300- UTSig) and (2200- CEDAR) signature images through used HOG algorithm for extract features, the result was then trained using four different classifiers: SVM, KNN, SVR, and DT. Finally, the best classifier was determined by calculating the run-time and accuracy of each algorithm. The best run time was for DT classifier in both datasets, followed by SVR classifier, SVM classifier, and finally KNN classifier, while the accuracy value for both classifier SVM and SVR was same and better than the accuracy value for KNN and DT classifiers through UTSig dataset, and SVM, SVR, and DT classifiers reached same and better accuracy value than the accuracy of KNN classifier. In the future, researchers hope to develop and test hybrid classification algorithms using the same and different datasets. They also hope that using deep learning algorithms for both phases (extract features and classification) will aid in the development of an accurate signature verification system.

REFERENCES

F. Alsuhiat, F. S. Mohamad, and M. Iqtait, "Detection and Extraction Features for Signatures Images via Different Techniques," IOP Conf. Series: Journal of Physics: Conf. Series 1179 (2019) 012087.

L. Hafemann, R. Sabourin, and L. Oliveira, "Learning features for offline handwritten signature verification using deep convolutional neural networks," Pattern Recognition, vol. 70, no.1, pp. 10-21, 2017.

A. Bharadwaja, "The Analysis of Online and Offline Signature Verification Techniques to Counter Forgery," Indian Journal of Science and Technology, vol. 8, no. 20, pp. 15-24, 2015.

M. Narayana, L. Annapurna, and K. Mounika, "Offline signature verification," International Journal of Electronics and Communication Engineering and Technology (IJECET), vol. 8, no. 2, pp.60-67, 2017.

H. Shah, P. Pawar, S. P. Khachane, S. Sharma, and S. Pithava, "Online Signature Verification and Authentication using Smart Phones," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 5, no. 6, pp. 22-34, 2017.

F. S. Mohamad, F. Alsuhiat, M. Mohamed, M. Mohamad, and A. Jamal, "Detection and Feature Extraction for Images Signatures," *International Journal of Engineering & Technology*, vol. 7, no. 3, pp. 44-48, 2018.

H. Saikia, and K. Sarma, "Approaches and Issues in Offline Signature Verification System," *International Journal of Computer Applications*, vol. 42, no. 16, pp. 51-62, 2012.

Pratima, D & Nimmakanti, N. (2011). Pattern Recognition Algorithms for Cluster Identification Problem. *International Journal of Computer Science & Informatics (IJCSI)*, 2(1+2).

Soleimani, K. Fouladi, and B. Araabi, "UTSig: A Persian offline signature dataset", *IET Biometrics.*, vol. 6, no. 1, pp. 1.8, 2016.

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

[11] N. Abbas, K. Yasen, K. H. Faraj, L. Razak, F. Malaliah, "Offline handwritten signature recognition using histogram orientation gradient and support vector machine," *Journal of Theoretical and Applied Information Technology*, vol. 96, no. 8, pp. 2075-2048, 2018.

R. Olmos, S. Tabik, and F. Herrera, "Automatic handgun detection alarm in videos using deep learning," *Neurocomputing*, vol. 275, pp. 66-72, 2018.

V. D. Nguyen, H. Van Nguyen, D. T. Tran, S. J. Lee, and J. W. Jeon, "Learning Framework for Robust Obstacle Detection, Recognition, and Tracking," *IEEE Trans Intell Transp Syst*, vol. 18, no. 6, pp. 1633-1646, 2017.

F. S. Mohamad, M. Iqtait, and F. Alsuhiat, "Age Prediction on Face Features via Multiple Classifiers", 4th International Conference on Computer and Technology Applications, 978-1-5386-6995-2/18/\$31.00 ©2018 IEEE, pp. 161-166.

M. Awad, and R. Khanna, "Efficient Learning Machines Theories, Concepts, and Applications for Engineers and System Designers," Apress, Berkeley, CA, 2015.

A. Gershman, A. Meisels, K. H. Lüke, L. Rokach, A. Schclar, A. Sturm, "A Decision Tree Based Recommender System," *InIIICS*, pp. 170-179, 2010.

S. D. Jadhav, and H. P. Channe, "Efficient recommendation system using decision tree classifier and collaborative filtering," *Int. Res. J. Eng. Technol*, vol. 3, pp. 3-8, 2016.

S. Deya, A. Dutta, I. Toledoa, S. Ghosha, J. Liados, "SigNet: Convolutional Siamese Network for Writer Independent Offline Signature Verification," *Pattern Recognition Letters*, Elsevier Ltd. All rights reserved, pp.1-7, 2017.