OFFLINE SIGNATURE VERIFICATION BASED ON USING NEURAL NETWORK CLASSIFICATION

التحقق من التوقيع OFFLINE باستخدام تصنيف الشبكات العصبية

Sameerah Faris Khlebus University of Information Technology and Communications, College of Business Informatics

ABSTRACT

The verification of handwritten signatures is one of the oldest and the most popular biometric authentication methods in our society. In addition, the evolution of technology, the different ways of comparing and analyzing signatures became more and more sophisticated. Based on the acquisition process, the field is divided into on-line and off-line parts. In on-line signature verification, the whole process of signing is captured using some kind of an acquisition device, while the off line approach relies merely on the scanned images of signatures. This research, deals some of the many open questions in the off-line field. It provides off-line signature recognition and verification system which is based on image processing, new improved method for features extraction proposed and artificial neural network are both used to attend the objective designed for this research, Two separate sequential neural networks are designed; one for signature recognition, and another for verification (i.e. for detecting forgery). A recognition network controls verification network parameters, which are produced individually for every signature. The System overall performs is enough to signature recognition and verification sing standard and popular dataset, In order to demonstrate the practical applications of the results, a complete signature verification framework has been developed, which incorporates all the previously introduced algorithms. The results provided in this it aim to present a deeper analytical insight into the behavior of the verification system than the traditional artificial intelligence-based approaches.

ملخص البحث

التحقق من التوقيعات بخط اليد هي واحدة من أقدم وأساليب المصادقة البيولوجية الأكثر شعبية في مجتمعنا. وبتطور التكنولوجيا، أصبحت طرق مختلفة للمقارنة وتحليل التوقيعات أكثر وأكثر تطورا. وبناء على عملية الاستحواذ، ينقسم هذا المجال إلى أجزاء على الخط وخارج الخط. في التحقق من صحة التوقيع على الخط، واستولت على العملية برمتها من توقيع باستخدام نوع من انواع جهاز الاستحواذ، في حين يعتمد نهج خارج الخط فقط على الصور الممسوحة ضوئيا من التوقيعات. هذا البحث يتناول بعض من كثير من الأسئلة المفتوحة في مجال خارج الخط. ويوفر خارج الخط الاعتراف التوقيع ونظام التحقق الذي يقوم على أساس معالجة الصور، طريقة جديدة محسنة لاستخراج ميزات المقترحة والشبكة العصبية الاصطناعية كلاهما يستخدم لتحقيق هدف هذا البحث، فقد تم تصميم اثنين من الشبكات العصبية منتابعة منفصلة. واحد من أجل الاعتراف التوقيع، وآخر للتحقق منه (أي للكشف عن التزوير). يتم التحكم المعلمات شبكة التحقق التي يتم إنتاجها بشكل فردي لكل التوقيع على شبكة الاعتراف النظام ينفذ عموما التوقيع والتحقق من مجموعة البيانات القياسية ، من أجل إثبات التطبيقات العملية لهذه النتائج، تم وضع إطار التحقق من صحة التوقيع الكامل، والذي يشتمل على جميع خوارزميات سبق عرضه. نتائج المنصوص عليها وكذلك يهدف إلى تقديم نظرة تحليلية أعمق في سلوك نظام التحقق من النهج القائم على الذكاء الاصطناعي التقليدية.

1. Introduction

For identification and the verification, many studies in the field of computer science have been conducted over the years by many engineers and scientists. The focus is on human biometrics. Biological measurement is the most commonly measurable such as DNA, iris, fingerprints and behavior of individuals such as Sound, signature and handwriting.

1.1 work related the Problem

A person's handwriting style is the biometric feature can be used to authentication. Research has begun in this area since 1970, for explore, various methods of different types of classification have been investigated for this matter, most them cannot be extended for other languages, as each language have its own characteristics And several types of writing, the biggest problems the encountered to find a separate language mode is the differences features of different languages [1].

The signature is behavioral biometric like handwriting, it is very useful to individual authentication; in some characteristics make it different to handwriting [2]. Example the signature styles is independent to the language of the person whose signature, many cases is just a panel made of curved lines may be mixed with writing. This can be an advantage, or a disadvantage to start looking for new methods to verify the signature, this help to focus research to algorithms that are in the independent languages classification. This means there is not a problem to different language signatures may be increase application compatibility on the issue, however, because of a property that people do not follow the exact rules in their signatures makes it difficult to find a new way to extract signature features that can be extended for other languages.

In general, the signature verification systems classify to two types categories: online systems [5]; [6]; [10]. In addition, off-line [3]; [4].

Due the dynamic of available information such as orders stroke, pressure, acceleration etc. Verification systems online be more accurate.

1.2 Statement of Problem

Because of the importance of offline signature verification on discriminating the genuine signature from the forgery and its useful application in bank service and forgery detection, it is necessary to provide an accurate person identification method based on signature. In this research, propose an off-line, language-independent signature verification method. Our feature extraction and data representation are all new in field of signature verification and have not been presented before in this domain.

Feature extraction filter is orientation of the Skelton combination by gravity center point that has been used in literatures frequently but separately for pattern based features extraction. Also, in similarity matching will uses a graph matching that can be done with graph similarity algorithms to do the classification phase.

1.3 Purpose and Objectives

- Development enhanced pattern features based on remote distance and split angular spans from signature image.
- Check offline signature features by the neural network classification tool.
- Verify the implementation of the automatic signature verification language completely independent of the accurate language to detect fraudulent and random fraud.

1.4 Structure of the proposed method

This study begins with the SigComp11-NFI signature collection and extraction feature and a neural network classification . The proposed method is then evaluated. Figure (1), depicting the structure of proposed method.

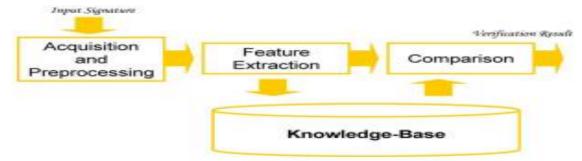


Figure (1): Structure of the proposed method

2. Research Tools

In the proposed method our offline signature verification ,The tools used are Delphi for feature extraction and preparation , and using matlab 2011 for developing whole offline signature verification using neural network classification. In data collection would be consider to use standard offline signature verification. The SigComp11-NFI signature collection dataset used in this research for evaluate the proposed method.

The SigComp11-NFI signature collection dataset contains offline signature samples. The dataset will be constituted of PNG images, scanned at 400 dpi, RGB color. Total set 362 signatures image, divided to two set Training and testing set. Training set contain 239 images and testing set 123 images, data of 10 reference writers and 26 skilled forgeries of these signatures, Figure (2) Six Sample signatures from the SigComp2011 dataset.



Figure (2): Six typical signatures of the SigComp2011 dataset. Top row the real signature and bottom row is the forgery

3. Proposed design

In this study, the offline signature verification system proposed divided into four main Phases, in Figure (3) depicts diagram proposed system.

- The Preprocessing
- The Feature extraction
- Classification and Verification

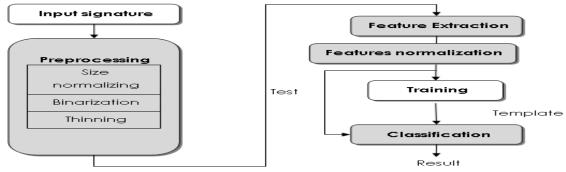


Figure (3): Diagram proposed system

In the beginning, collections of samples is collected for signature data and enter into the pretreatment phase, which includes three sub-sections. As shown in Figure (3), filters are used such as Gabor and the results will be unexpected, all signature images will be equal by to the desired size by cropping image signature from the beginning of the top left pixel to the bottom right pixel the capacitor for the image, Followed by morphology and patronization consists of spatial homogeneity. This prevents unexpected results and provides a set of standard data set data.

In next step uses a new way to extracting the feature properties, which is a combination of the center of gravity of the image with the image spin division. This step represents main part of proposed method in this research. Moreover, this issue is the fully discussed.

Output is the vector with N length; and this vector called feature vector of signature image, it's contains many features. Just after the process of feature, extraction uses the neural network classification technique.

3.1 Image Pre-processing

At this stage, the noise remove the segmentation and the thinning to provide noiseless data for the subsequent stage. The intermediate filter is used to soften the signature image with retaining small and acute details. An argument value is used for a set of the pixels for n x N dimension to replace the target processing pixel. Meanwhile, signature image threshold is also applied to convert the gray level signature image into bi-level (black & white) image using threshold value, $\theta = 128$. Safe-point Thinning Algorithm (Skelton) is used in signature image thinning.

3.1.1 Thinning Algorithm (Skelton)

In process signature images thinning is used a Safe point Thinning Algorithm (Skelton). Skelton algorithm involved two the scanning in the each execution for the each pixel. In the first scan, the edge of the entire right edge and the left edge point are marked as not a safe point for deletion later. Same process are repeated for the each point of the top edge and the bottom edge point in second scan. The deletion is performed so that there is no marking point.

The below steps are the description of the Thinning algorithm (Skelton) and as follow:

- 1) Read image from the top to bottom and from the left to right.
- 2) Save pixel value to the Variable, P.
- 3) Execute following the steps all for pixels in the row and the column.
- 4) Verify point P, if the P point is black point and isn't marked, following steps will not continue.
- 5) Verify whether edge point is p. Skelton check edge point the according to the four kinds listed as follows:

P left the edge point, when neighbor from X4 is a white point.

P right the edge point, when neighbor from X0 is a white point.

P top the edge point, when neighbor from X2 is a white point.

P bottom the edge point, when neighbor from X6 is a white point.

6) Check if the point P a safe point. Logical operations are listed to determine a safe-point as

Left safe-point,
$$S_4 = x_1 * (x_2+x_3+x_7+x_8) * (x_3+!x_4) * (x_7+!x_6) == 0$$
,

Right safe-point,
$$S_0 = x_5 * (x_6 + x_7 + x_3 + x_4) * (x_7 + !x_8) * (x_3 + !x_2) == 0$$
,

Top safe-point,
$$S_2 = x_7 * (x_8 + x_1 + x_5 + x_6) * (x_1 + !x_2) * (x_5 + !x_4) == 0$$
,

follows: Bottom safe-point,
$$S_6 = x_3 * (x_4 + x_5 + x_1 + x_2) * (x_5 + !x_6) * (x_1 + !x_8) == 0$$
.

7) Each edge-point that is not safe-point (point that failed to meet the rule of Boolean operation) will be marked and deleted. Otherwise, point P is labeled as the one.

8) The Step (2) is repeated to step (3) for all entire pixel image.

3.1.2 Feature Extraction Phase

Proposed feature extraction method can be separated to 2 parts; first we use gravity center point on signature images. In addition, the second extract N feature from the signature images.

3.1.3 Gravity Center Point

First step to extract features of input signature images is to calculate the gravity center point on signature images, to enable the presented technique to be translation invariant we are using the COG to estimate the features. The COG of the signature image (Xc, Yc) is estimated using Eq. (1). This is used as the center of the signature image.

$$(X_c, Y_c) = \left(\frac{\sum_{j=1}^m \sum_{i=1}^n iI[i,j]}{\sum_{j=1}^m \sum_{i=1}^n I[i,j]}, \frac{\sum_{j=1}^m \sum_{i=1}^n jI[i,j]}{\sum_{j=1}^m \sum_{i=1}^n I[i,j]}\right) \dots$$
(1)

Where I is a binary image of dimension m X n, X_c and Y_c are the X and Y coordinates of signature COG.

3.1.4 Signature image division

The first two features are useful for pruning the search space during the candidate signature determination stage. These features are highly descriptive for character recognition, especially for printed documents. Angular and distance span features are employed in this work because they are not sensitive to font variation and letter thickness, and are scale and rotation invariant. Rotation invariance of the angular span vector can be achieved simply by shifting vector entries by one slice to the left and right. In this work, angular and distance span vectors of the sizes 12° and 13 [7] respectively, are used. Figure (4) illustrates these vectors for an example signature from the data.



Figure (4): (A) signature image, (B) angular span, (C) distance span



Figure (5): division signature image using angular span and distance span.

3.1.5 Normalization of Input Features

The input pattern for classifier system, uses 13 slicing circles, and taking 30 segments span angular division for each signature image, so it have 414 features input.

Normalization is the uniformly applied transformation of each element of the set data so as the set has certain statistical characteristics. In this research, normalization is performed on the features extracted of angular span and distance span division functions in the range of [0, 1]. The according for several studies, the normalization of the input features showed to accelerate convergence and the recognition rate. Therefore, at this research, it is applied Min-Max technique normalization using the following formula:

$$new\ X = \frac{oldX - minVal}{maxVal - minVal} (new_{maxVal} - new_{minVal}) + new_{minVal} \dots (2)$$
 Where:
$$new\ X \text{ is value new normalized }, \\ old\ X \text{ is original value }, \\ min\ Val \text{ is smallest value for the sample }, \\ max\ Val \text{ is largest value for the sample }, \\ new_{maxVal} \text{ is largest value for the sample }, \\ new_{minVal} \text{ is smallest value for the sample,}$$

3.2 Artificial Neural Networks Classification

In this research, standard back-propagation model with sigmoid logistic activation function is used in the training and classification phases. The function is utilized in both input-to-hidden layer and hidden-to-output layer.

The input data for the model are numerical values extracted from isolated signature images using division using angular span and distance span. 362 images within 239 signature images are used in network training, and 123 images are used in testing and classification phases. The Network weights are initialized with random numbers. In addition, this work is implemented by MATHLAB 2009 using Neural Network package.

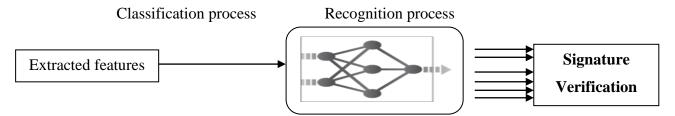


Figure (6): Design of Neural Networks in this project

The Neural network has two hidden layers named H1 and H2 it also has input and output layers. H1is composed of 414 features of 20 neurons arranged as input. It is important to know the kinds of features. Because, the connection on each neuron have had the same weights in given feature.

Other words, The Neural network in H1 uses the same weight. Each neuron has input. It takes their input from the input layer. Layer H1 has many connections share with the same weight. Layer H2 is composed of 414 features. The connection between H1 and H2 is linked between the input and H1. Each neuron in H2 combines the information coming from different feature in H1. The Connections from input layer entering H1 and H2 to neuron connections to the output layer. Figure (7) shows the structure of the Neural Network with two hidden layers

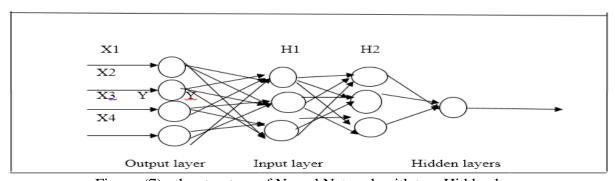


Figure (7): the structure of Neural Network with two Hidden layers

3.2.1 Target Network Output

The target vector is a 10-element vector with a one in the position of the writer it represents, and 0's everywhere else. Table (1) shows the target output in Neural Network.

| Writers | Target Network Output | | | | | | | | | |
|------------|-----------------------|---|---|---|---|---|---|---|---|---|
| Writer 001 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Writer 002 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Writer 003 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Writer 004 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| Writer 005 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| Writer 006 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| Writer 007 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| Writer 008 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| Writer 009 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| Writer 010 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

Table (1): the target output in Neural Network

3.3 Method of verification

The method used to validate system with some other styles displayed is the Equal Error Rate (EER). The EER is most popular performance indicator for authentication systems, often used in previous methods. To understand the best EER is point when the false admission rate (FAR) and the false rejection rate (FRE) equal.

FAR is a factor reveals the rate when a signature verification system accepts falsely a forgery signature. By growing up this factor, the performance of system is reducing. FRR is the same is another factor shows the rate when a signature verification system detect a genuine signature falsely as a forgery and reject it. If this factor grows up the users of the system may have many problems for authentication process and may encounter several acceptance errors.

Experiments showed for validating such these systems it is better to consider both FAR and FRR, but this task may cause some misunderstanding so it uses EER when the FAR and FRR are equal that indicates the optimum point for both of them, it is shown graphically in Figure (8).

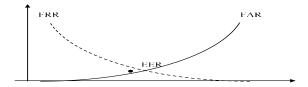


Figure (8): FAR, FRR and collision point shows EER

3.4 Preprocessing presets execution

first step the must be done on a scanned text image for make it more clear and useful of following signature identification procedures by converting the image from gray scale to black and white, eliminating blur or noise from image. Figure (9) show after and before the pretreatment of signature image.

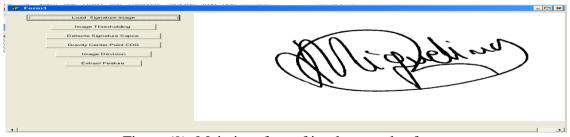


Figure (9): Main interface of implemented software



Figure (10): A and B before and the after preprocessing respectively

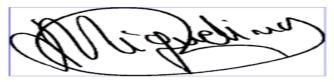


Figure (11): Offline signature image of Gravity Center is the Point COG



Figure (12): Apply a thin algorithm to same the signature image

3. 5 Divisions

After you select the components in the offline signature image, it must divide on each component from the top-bottom direction, the left- right side that moves forward from the text path.

As shown in figure (13), a magnifying image of the signature, which produces clearer look to division all around signature.

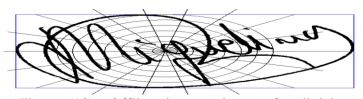


Figure (13): Offline signature image after division

3. 6 Features Extraction

This paragraph and the following article are most the important parts of all procedural stages, as they affect the effectiveness of identification and the verification process, more extraction-related characteristics lead to the better categorized signature image, resulting in better identification. Table (2) shows the first 16 features extracted from one image, a real signature, and five signatures of the events in the image after applying extracted features.

| Image name | Signature Image and simple of features extracted | | | | | | | | | |
|----------------|--|--|--|--|--|--|--|--|--|--|
| 0210015_02.bmp | Anlerhart - Waslander | | | | | | | | | |
| | Waslandel | | | | | | | | | |
| | 318 0< | | | | | | | | | |
| 0210015_01.bmp | 1318 0 0 0 0 3 2 3 3 4 0 0 0 0 0 4 7 | | | | | | | | | |

| | 319 48 2 0 44 216 9 210 0 21 63 0 0 0 3 240 | | | | | | | | |
|----------------|--|--|--|--|--|--|--|--|--|
| 0210015_02.bmp | Daslandel Waslandel | | | | | | | | |
| | 11 4 0 0 0 61 9 10 0 0 0 0 0 14 29 | | | | | | | | |
| 0210015_03.bmp | Shrterhart Waslander | | | | | | | | |
| | 17 8 0 0 0 64 108 115 22 0 0 0 0 0 0 33 | | | | | | | | |
| 0210015_04.bmp | Strkethart Was landel | | | | | | | | |
| | 25 8 0 0 0 0 0 139 42 0 0 0 1 0 0 0 26 | | | | | | | | |
| 0213015_01.bmp | In Enhant | | | | | | | | |
| | 244 0 0 0 0 8 1 9 0 0 0 0 1 17 14 22 | | | | | | | | |

Table (2): A sample of the 16 features extracted of one genuine signature, five forging the signatures image.

3.7 Normalize features

The normalization process applied for each element in the data set. The features of the proposed method are extracted in the range (0, 1). Aim of normalization is for unify the elements in the data extraction features. Figures (10), (11) and (12) illustrate simple features the 15 signature images from three deferred books.

Typical and unique features should be used in coding signature images specific to each writer in dataset, and in relation to this, a small deviation should be considered between the attributes for better differentiation rate. Figure (14), Figure (15) and Figure (16) shows the extraction of the characteristics of the signature sample of the images. Where, the X axis is number of the feature samples and the Y axis is value of feature.

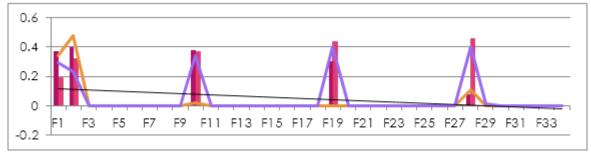


Figure (14): Sample Features the Extracted from five the images Signature return to the writer "002"

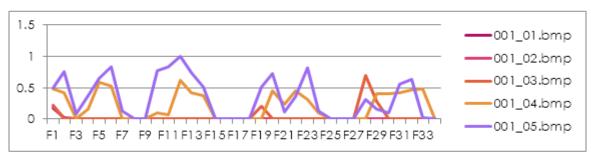


Figure (15): Sample Features the Extracted from five the images Signature return to writer "001"

Figure (14) represents the curve of extracted features after the normalization of the number writer "002" clearly show similarity between the features and the best representation of the signature image, normalization of extracted features play a very important rule in this research, caused these features can be demonstrated the proposed algorithm. Figure (15) shows (5) curves representing (35) images drawn from the (5) signature images to the number "001". In this case, it has can see respect between the values representing each picture. Figure (16) contains one curve representing a signature image written by writer number "005" and (4) of the curve represent (4) forgery signatures to the writer number "005", it's see of the great contrast of feature.

Normalized values from the extracted features fed into Artificial Neural Networks classification. The classification and verification of the offline handwriting signature.

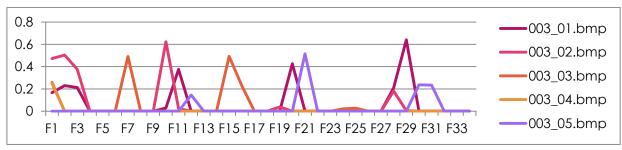


Figure (16): Sample Features the Extracted from five the images Signature return to the writer "003"

3.8 Classification of Artificial Neural Networks Design for signature verification

The design artificial neural network to the multilayer feed forward for check off-line digital signatures. Proposal ANN consists of (414) input the variables, (200) hidden neurons and (10) output variables, designed to recognize one signature at each a time. The back-processing algorithm is used for training. In first, the "input / output" database are manually created for training and ANN testing. All input vector consists of (414) the features obtained for the signing. As described earlier in the use of (24) sample to each signature. These (24) signatures divide into two sets, these each containing (12) signature. One of these sets is use in training ANN, the other set used for the testing. The database included total of (364) different the signature images used for both training and the testing. Since the characteristics of vector inputs for each image used for training purposes, a total of (240) transponders for input (datasets) in training set. The remaining 124 data sets are used for testing. ANN contained 414 binary output values, each corresponding to one signature being tested.

Under the normal operation for ANN, one output is expected to take the value of one, which indicates recognition of the signature represented by this specific output; other output values should be zero. In general, the number of outputs should be equal to the number of signatures being considered.

3.8.1 Signature Verification

The purpose in this part of the study, is to authenticate a signature, i.e., to verify that the signature is not counterfeit and that it really belongs to the person who is claimed to be the owner of the signature. The ANN used for this purpose is also a multilayer feed forward network which consists of 414 input variables, 200 hidden neurons, and 2 output variables indicating whether the signature is fake or true. Backpropagation algorithm is used for training. The training data set is obtained from 12 original (authenticated) signatures provided by the real owner and 12 fake signatures. As was done for the preparation of the training data for the ANN used in recognition, 414 invariant features per signature are used in the training set. A sample set of three signatures belonging to the same person. As explained in Figure (17).



Figure (17): Tree signatures, which belong to the true owner of the signature

3.8.2 Signature Recognition

Where used the neural network classification matlab toolbox. These tools allowed the signature images to be loaded one at a time and used in training and testing. First, the signature image is captured using a scanner. Then, through several image processing operations, it is converted to binary and normalized, and thinned, as explained earlier. Extracted spin angles an span distance features values are obtained from the thinned image, which is then used as the input vector to the ANN. After the training of the ANN for signature recognition, the system is ready to recognize a given signature.

The signature recognition system is tested using 124 signatures in tested dataset, as explained before, 124 images in database belonging to 124 different signatures are used for testing. Since 414 input values for each image were used for training purposes, under normal (correct) operation of the ANN, only one output is expected to take a value of 1 which refers to the recognition of signature represented by the specific output. The other output values must remain zero. The output layer used a logic decoder which mapped neuron outputs between 0.5-1 to a binary value of 1. If the real value of an output is less than 0.5, it's represented by a 0 value.

The ANN program recognized mostly all of the 62 signatures correctly, an 80% recognition rate, resulted in false positives (output > 0.5) while the remaining 14 are recognized correctly as not belonging to the original set (the output value was <= 0.5). Since the recognition step is always followed by the verification step, these kinds of false positives can be easily caught by verification system. In other words, the verification step serves as a safeguard against false positives as well as false negatives.

The Table (3) depicts the results for analyzing proposed system's accuracy in terms of True Negative Rate (specificity = the proportion of forgeries which are correctly identified), The True Acceptance Rate (sensitivity = the proportion of actual genuine signatures, which are correctly identified as positives).

$$Sensitivity = \frac{TP}{TP + FN}$$
$$Sensitivity = \frac{TN}{TN + FP}$$

| | Total number | forgeries | genuine | TN | TP | FN | FP | TAR sensitivity | TNR specificity |
|-------|--------------|-----------|---------|----|-----|----|----|-----------------|-----------------|
| Train | 240 | 178 | 62 | 53 | 160 | 9 | 18 | 0.946 | 0.746 |
| Test | 124 | 62 | 62 | 50 | 48 | 12 | 14 | 0.800 | 0.781 |

Table (3): The results for the proposed method for signature image verification.

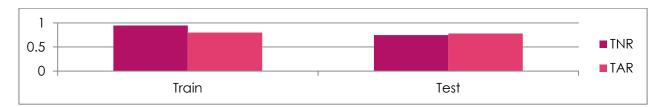


Figure (18): Bare chart show comparison between Train and test dataset.

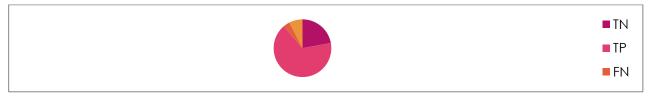


Figure (19): pie chart show comparison between TN, TP, FN, FP data analyze for train process.

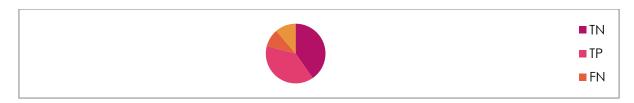


Figure (20): pie chart show comparison between TN, TP, FN, FP data analyze for test process.

For evaluate the proposed method in this research been the compared and evaluate the result gotten from this work with new published paper (Surabhi, 2013) that he used two dataset for evaluate his work, this comparison based on the systems accuracy in terms of True Negative Rate (specificity = the pron of forgeries which are correctly identified), The True Acceptance Rate (sensitivity = the proportion of actual genuine signatures, which are correctly identified as positives). The Table (4.) show comparison of the result gotten from our proposed method in this research and Surabhi result.

| work | Data | Total number | forgeries | genuine | TN | TP | FN | FP | TAR sensitivity | TNR specificity |
|---------------------|--------|--------------|-----------|---------|----|-----|----|----|-----------------|-----------------|
| research results | Train | 240 | 178 | 62 | 53 | 160 | 9 | 18 | 0.946 | 0.746 |
| research results | Test | 124 | 62 | 62 | 50 | 48 | 12 | 14 | 0.800 | 0.781 |
| (Surabhi, 2013) | Train1 | 36 | 17 | 19 | 8 | 7 | 11 | 10 | 0.389 | 0.444 |
| (Surabhi, 2013) | Test1 | 36 | 31 | 5 | 3 | 16 | 2 | 15 | 0.889 | 0.167 |
| (Surabhi, 2013) | Train2 | 36 | 14 | 22 | 13 | 9 | 9 | 5 | 0.500 | 0.722 |
| (Surabhi, 2013) | Test2 | 36 | 22 | 14 | 10 | 14 | 4 | 8 | 0.778 | 0.556 |

Table (4) comparison of the result gotten from our proposed method and Surabhi result for signature image verification.

4. Conclusions

In this study, a signature recognition and verification system an off-line based on the image processing, new improved method for features extraction have been proposed, and ANNs. New improved method for features extraction which are used as input features for ANN and be obtained from thin signature images. Two the separate sequential ANNs is used for signature recognition and another for verification. The system showed a 79% success the rate by identifying most of the rectification of all 62 signatures that were trained for. However, performance has shown poor when presented with signatures that was not trained earlier. As case it's not consider high risk, because the recognition step always follow the verification step and this kind of false positives can the easily caught by the system. Artificial neural network are designed for the multilayer feed forward to verification digital signatures, and is designed to identify one signature in each time.

Where that is also acceptable, as the person may always be given the second chance to the prove ownership of the signature.

In general, failure of recognition or verification of the signature it is due to poor image quality and the high similarity between two the signatures. The system's ability to verify and verify can increased by using the additional features in input data set.

5. Future Work

Research is consists a lot work so as the suggests following issues for future work:

- Try of the apply this technique to the deferred type the classification technique such as vector support machine, violins.
- ❖ Try of enhance the extracted feature for each section.
- ❖ Try of apply proposed technique to verify signature online.
- ❖ Try of find the plan to expand vector input feature by adding some network information and texture-related features.

REFERENCES

- [1] Alattas, E., & Meshoul, S. (2011, July). An effective feature selection method for on-line signature based authentication. In Fuzzy Systems and Knowledge Discovery (FSKD), 2011 Eighth International Conference on (Vol. 3, pp. 1431-1436). IEEE.
- [2] Kekre, H. B., & Bharadi, V. A. (2010). Gabor filter based feature vector for dynamic signature recognition. International Journal of Computer Applications, (3), 74-80.
- [3] Miroslav, B., Petra, K., & Tomislav, F. (2011, May). Basic on-line handwritten signature features for personal biometric authentication. In MIPRO, 2011 Proceedings of the 34th International Convention (pp. 1458-1463). IEEE.
- [4] Jain, C., Singh, P., & Rana, P. (2013). Offline Signature Verification System with Gaussian Mixture Models (GMM). INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY, 10(6), 1700-1705.
- [5] DR, S. K., RAJA, K., CHHOTARAY, R., & PATTANAIK, S. (2010). Off-line Signature Verification Based on Fusion of Grid and Global Features Using Neural Networks. International Journal of Engineering Science.
- [6] Pourreza, H. R. (2011, September). Offline Signature Recognition using Modular Neural Networks with Fuzzy Response Integration. In International Conference on Network and Electronics Engineering.
- [7] Sigari, M. H., Pourshahabi, M. R., & Pourreza, H. R. (2011). Offline handwritten signature identification and verification using multi-resolution gabor wavelet. International Journal of Biometric and Bioinformatics, 5.
- [8] Shirdhonkar, M. S., & Kokare, M. (2011). Off-Line Handwritten Signature Identification Using Rotated Complex Wavelet Filters. arXiv preprint arXiv:1103.3440.