Ain Shams Engineering Journal (2010) 1, 59–70

Ain Shams University

Ain Shams Engineering Journal

www.elsevier.com/locate/asej
www.sciencedirect.com

ELECTRICAL ENGINEERING

Online handwritten signature verification system based on DWT features extraction and neural network classification

Maged M.M. Fahmy *

Computer Vision, Faculty of Engineering, University of Newcastle Upon Tyne, UK

Received 12 June 2010; accepted 15 August 2010
Available online 5 November 2010

KEYWORDS

Signature recognition;
Pen position;
Pen-movement angle;
1D wavelet transform;
Multi-matcher;
Neural network

Abstract Handwritten signature is the most widely accepted biometric to identity verification. The target of research is to present online handwritten signature verification system based on discrete wavelet transform (DWT) features extraction and feed forward back propagation error neural network recognition. Steps for verifying online handwritten signature in this system start with extracting pen position data (x and y positions) of points that forming the signature. Pen-movement angles are then derived from pen position data. To reduce variations in pen-position and pen-movement angles dimensionality, data are normalized and resampled. To enhance the difference between a genuine signature and its forgery, the signature is verified in DWT domain. Low frequency sub-band signals (approximations) of pen-position parameter and pen-movement angle parameter are considered as intrapersonal features. These are used for suppressing variations between different genuine signatures and enhancing the interpersonal variations, hence are given higher scores within total recognition process. Both of pen-position and pen-movement angle features are then associated for obtaining a decision about online handwritten signature verification. A multi-matcher consists of six neural networks which use multiple representations and matching for the same input biometric signal is used to verify signature. The recognition rate for each of these neural network recognizers is discussed and a comparison of those rates is performed. Experiments are carried on signature database for five users each of 20 genuine and 20 skilled forgery signatures. Recognition success rate for genuine signatures is 95%.

* Address: 10 Ahmed Shoukri Street, San Stifano, Alexandria, Egypt.
E-mail address: dr_maged_fahmy@yahoo.com

Peer review under responsibility of Ain Shams University.
doi:10.1016/j.asej.2010.09.007

ELSEVIER Production and hosting by Elsevier

1. Introduction

There exist a number of biometrics methods at present, e.g. signatures, fingerprints, iris, etc. Fingerprints and iris verification require the installation of costly equipments and hence cannot be used at day to day places like banks, etc. There is considerable interest in authentication based on handwritten signature verification system as it is the cheapest way to authenticate a person. Banks and Government bodies recognize signatures as a legal means of authentication. Signature verification technology utilizes the distinctive aspects of the signature to verify the identity of individuals. Criminal experts cannot be employed at every place and hence there has been considerable effort towards developing computerized algorithms that could verify and authenticate the individual's identity. A handwritten signature is biologically linked to a specific individual. Modern forensic document examiners commonly compare a suspect signature with several examples of known valid signatures. They look for signs of forgery which include: Signatures written at a speed which is significantly slower than the genuine signatures; frequent change of the grasp of the writing implement; rounded line endings and beginnings; poor line quality with hesitant and shake of the line; retracing and patching; and stops in places where the writing should be free. Compared with other electronic identification methods such as fingerprints scanning and retinal vascular pattern screening, it is easier for people to migrate from using the popular pen- and paper signature to one where the online handwritten signature is captured and verified electronically. Many times the signatures are not even readable by human beings. Signature verification problem therefore is concerned with determining whether a particular signature truly belongs to a person or not. There are two approaches to signature verification, online and offline differentiated by the way data is acquired. In offline case, signature is obtained on a piece of paper and later scanned. Offline signature verification deals with a 2D static image record of the signature. It is useful in automatic signature verification found on bank checks and documents authentication. Offline verification techniques are based on limited information available only from shape and structural characteristics of the signature image. A fundamental problem in the field of offline signature recognition is the lack of a significant shape representation or shape factor. In contrast, online signature verification systems are extremely precise. It require the presence of the author during both the acquisition of the reference data and the verification process. This restrict their use to specific applications. Online handwritten signature is usually obtained on an electronic tablet and pen. Online signature verification track down path and other time-variable sequence variables using specially designed tablets or other devices during the act of signing. Automatic online signature verification is an interesting intellectual challenge with many practical applications. This technology examines the behavioral components of the signature such as: stroke order, speed, and pressure, as opposed to comparing visual images of signatures. Unlike traditional signature comparison technologies, online signature verification measures the physical activity of signing. The target of this research is to present online handwritten signature verification system based on DWT features extraction and neural network classification. This research paper is organized as the following. An overview on handwritten signature verification structure, specially online, is given in Section 1. Brief survey on current research area in this field and problem statement is presented in Section 2. The proposed system description is briefed in Section 3. The process of extracting features existing in handwritten signatures and discrete wavelet transform (DWT) is discussed in Section 4. Feature matching (classification) is discussed in Section 5. Experimental setup and obtained results are explained in Section 6. Finally, concluding remarks are in Section 7.

2. Survey on handwritten signature verification and problem statement

Most of the signature verification work done in the past years focused either on offline or online approaches. Automatic online handwritten signature verification system to prevent identity fraud by verifying the authenticity of signatures on Australian passports is presented. In this system, fuzzy modeling has been employed for developing a robust recognition [1]. Hybrid handwritten signature verification system is explained, where the online reference data is acquired through a digitizing tablet. The acquired data serves as the basis for the segmentation process of the corresponding scanned offline data [2]. A method for verifying handwritten signatures where various static (e.g., height, slant, etc.) and dynamic (e.g., velocity, pen tip pressure, etc.) signature features are extracted and used to train several network topologies is presented [3]. Handwritten signature verification system based on a Hidden Markov Model approach for representing and verifying the hand signature data is presented in [4]. Instrumented data gloves equipped with sensors for detecting finger bend, hand position, and orientation for recognizing hand signatures is used in handwritten verification [5]. A method for automatic handwritten signature verification relies on global features that summarize different aspects of signature shape and dynamics of signature production is discussed in [6]. Signature recognition algorithm relying on pixel-to-pixel relationship between signature images based on extensive statistical analysis, standard deviation, variance, and theory of cross-correlation is discussed in [7]. Online reference data acquired through a digitizing tablet is used with three different classification schemes to recognize handwritten signatures is discussed in [8]. The impact of an incremental level of skill in the forgeries against signature verification systems is explained in [9]. Criterion for an improved writer enrolment based on an entropy measure for online genuine signatures is described in [10]. Online dynamic signature verification systems using a set of 49 normalized features that tolerate inconsistencies in genuine signatures while retaining the power to discriminate against forgeries is emphasized in [11]. A statistical quantization mechanism to suppress the intra-class variation in signature features and thus discriminate the difference between genuine signature and its forgery is emphasized in [12]. An algorithm for online handwriting signature verification using two levels verification method by extracting wavelet features and using neural network recognition is proposed in [13]. Dynamic handwritten signature verification using the wavelet transform with verification by the back propagation neural network (NN) is explained in [14]. Other online signature verification system based on extracting local information time functions of various dynamic properties of the signatures. Discrete 1D wavelet transform is performed on these features [15]. The use of discrete wavelet transform (DWT) in extracting features from handwritten signatures that achieved higher verification rate than that of a time domain verification system is reported in [16,17].

Using DWT as a mean of signature features extractor is surveyed in many research work [13–17]. Almost all of these were carried on with genuine signatures and mostly not tested with real skilled forged signatures. These did not also find a satisfactory solution for eliminating forgeries.

The target of this research is to present online handwritten signature verification system. This system is based on extracting sub-bands that represent intrapersonal features of signature from DWT representations of that signature. DWT features vectors (coefficients) of user genuine signatures that are mostly similar are selected as candidates for signature authentication features. Among those, vectors that are uncorrelated to their corresponding from forged signatures are selected to enhance difference (variations) between genuine and forged signatures. A multi-matcher consists of six back propagation neural networks is then used as classifier tool in this research. The proposed system is tested using a database of genuine signatures as well as a database of its skilled forgery signatures.

3. Proposed system description

The proposed online handwritten signature recognition system consists mainly of three phases: Signal modeling, feature extraction, and feature matching. The x and y positions of signature points are extracted and each is represented as 1D time domain signal. Pen moving angles are derived from pen position data points. It is then used as the third time domain signal. These signals are then normalized and resampled. This is to overcome the problem of different sizing and different number of points exists in every signature even for the same user. Discrete wavelet transform is used to extract features from these signals. Sub-band decomposition is used to extract intrapersonal features from the DWT features to enhance signature individuality. The extracted feature vectors are used to train back propagation neural networks bank that are used within multi matcher as a classifier. In the testing phase, signals which were captured from a signature of unknown person are subjected to feature extraction. The resulting features are inputted to the bank of the trained neural networks of multi matcher. The resultant outputs are allowing the unknown signature to be identified if it is a genuine handwritten signature or not. To summarize, two algorithms are of critical importance to handwritten identification system. The first is feature extraction process (obtained from discriminatory information). The second is classification process (using the features to determine the correct signal, which corresponds to the correct handwritten signature). The proposed handwritten signature verification system is shown in Fig. 1.

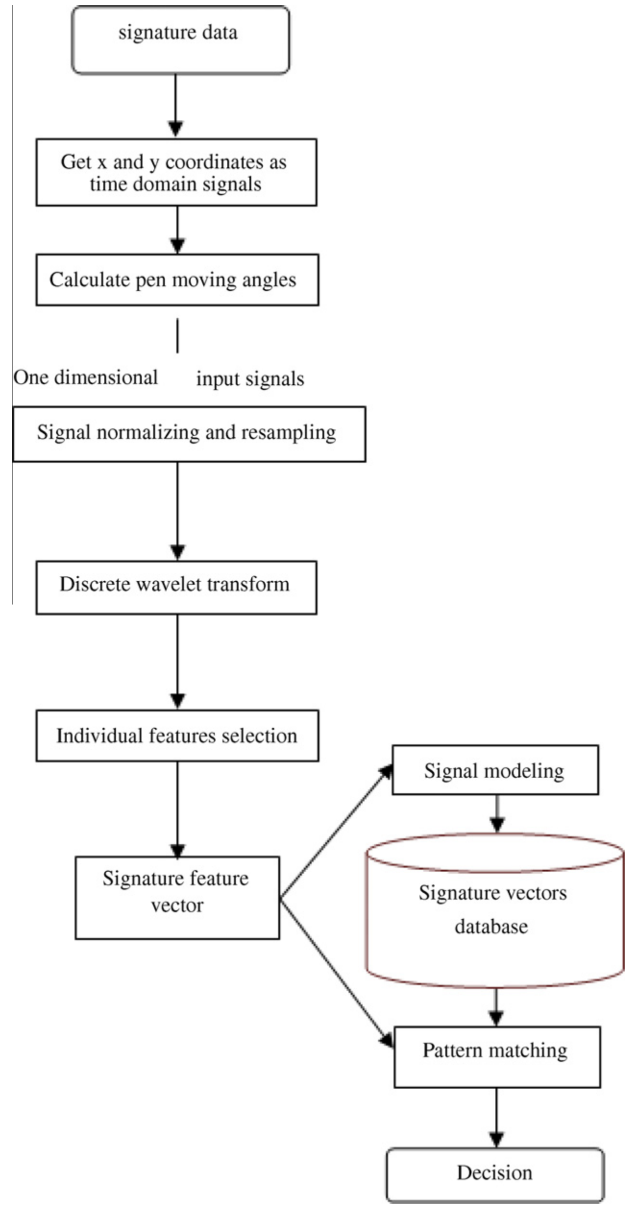


Figure 1 Online handwritten signature verification system based on extracting DWT features and neural network classification.

4. Features extraction process of handwritten signatures

The feature extraction process represents a major tackle in any signature verification system. Even there is no guarantee that two genuine signatures of a person are accurately the same (intrapersonal variations). Its difficulty also stems from the fact that skilled forgeries follow the genuine pattern (interpersonal variations). This is unlike fingerprints or irises where fingerprints or irises from two different persons vary widely. Ideally interpersonal variations should be much more than the intrapersonal variations. Therefore it is very important to identify and extract those features which minimize intrapersonal variation and maximize interpersonal variations. There is a lot of flexibility in the choice of features for verification of a signature. Global features, such as the overall direction of the signature, the dimensions, and the pixel distribution, are usually not adequate to differentiate forgeries. On the other hand, significant local features are extremely hard to locate. Great research efforts were made in order to concentrate on the local feature extraction process. Most of them aim at the robust extraction of basic functions entities called "strokes" from the original skeleton of the signature strokes. The feature extraction process in this research starts with pen position data. Two factors are considered: pen positions in x direction and pen position in y direction. Pen movement angles are derived from pen position data as a third factor. The number of points in a captured handwritten signature varies with respect to its size and speed of writing even for the same individual. To overcome different sizes of signature, data points that represents x position and y position are normalized. It is difficult to train a neural network for such large variations in number of points represent a signature. Hence, it is desirable to resample the signature contour to obtain fixed number of points. As a consequence, each of the three factors should be normalized and resampled. The feature extraction process then ends with taking out DWT coefficients for pen positions in x direction, and pen positions in y direction, and pen movement angles. Each step carried on for the system proposed in this research is described in the following subsections.

4.1. Pen-position data

The online signature is digitized with the electronic pen tablet. Only pen-position parameter is considered in this research since it is provided even in using PDA for handwriting signature. Pen-position parameter consists of discrete time-varying signals of x and y co-ordinates, which are $x(n)$ and $y(n)$, respectively. $n = 0, 1, \ldots, N$ is the time index and N is number of signature points. As the online signature is a dynamic biometric, each writing time is different from the others. This results in the different number of sampled data even in genuine signatures.

4.2. Pen movement angle

Each individual has a unique way of running his/her signature and so pen-movement angle parameter could help to identify the signature characteristics. The pen movement angle parameter is derived from the pen-position parameter. It is calculated for each two successive points obtained from pen-position parameter. Therefore, calculating pen moving angles requires no additional sensor and it is realized even when signing using the PDA. The pen-movement angle parameter is defined as $\theta(n)$ in Eqs. (1)–(4):

$$\begin{aligned}
\theta(n) = {} & \tan^{-1}\ \Delta y(n)/\Delta x(n), \quad \Delta x(n) > 0, && (1)\\
& \tan^{-1}\ \mathrm{sgn}(\Delta y(n)) \cdot \pi/2, \quad \Delta x(n) = 0, && (2)\\
& \tan^{-1}\ \Delta y(n)/\Delta x(n) + \pi, \quad \Delta x(n) < 0, \quad \Delta y(n) \geqslant 0, && (3)\\
& \tan^{-1}\ \Delta y(n)/\Delta x(n) - \pi, \quad \Delta x(n) < 0, \quad \Delta y(n) < 0, && (4)
\end{aligned}$$

where $n = 1, 2, 3, \ldots, N-1$, and

$$\Delta x(n) = x(n+1) - x(n), \tag{5}$$

$$\Delta y(n) = y(n+1) - y(n). \tag{6}$$

The pen-movement angle parameter essentially has 2D characteristics. As a result, it is expected to bring more obvious individual feature than the pen-position parameter which is actually in 1D. It is also confirmed that the pen-movement angle parameter has large intrapersonal variation in signatures of one individual. For utilizing the pen-movement angle parameter as well as pen position parameters in verification, some reduction method of this parameter variation is required. This could be achieved using data normalization and resampling.

4.3. Data normalization and resampling

Online signature is a dynamic biometric and hence each writing time is different from the others. This results in the different number of sampled data even in genuine signatures. In addition, different writing place and different size of signature cause disparity in pen position factor and hence pen moving angles factor. To reduce such disparities, these factors are normalized using the following equations:

$$x(m) = \alpha_x(x(n) - x_{\min})/(x_{\max} - x_{\min}), \tag{7}$$

$$y(m) = \alpha_y(y(n) - y_{\min})/(y_{\max} - y_{\min}), \tag{8}$$

$$\theta(m) = \alpha_\theta(\theta(n) - \theta_{\min})/(\theta_{\max} - \theta_{\min}), \tag{9}$$

where $x(m)$, $y(m)$, and $\theta(m)$ are normalized time index of $x(n)$, $y(n)$, and $\theta(n)$. $x_{\max}$, $y_{\max}$, and θ_{max} are maximum values of $x(n)$, $y(n)$, and $\theta(n)$, respectively. $x_{\min}$, $y_{\min}$, and $\theta_{\min}$ are minimum values of $x(n)$, $y(n)$, and $\theta(n)$, respectively. α_x, α_y, and α_θ are scaling factors for eluding underflow calculation in subband decomposition described later. Normalized x position, y position, and pen movement angle features signals of a genuine signature, represented as signals in time domain, are shown in Fig. 2.

The pen position data and pen movement angles are then resampled to get output vectors of fixed length. This means the sampling rate of each vector is to be changed so as to get always vectors of fixed length that best representing the original x, y, or θ points. Resampling data signals applies an anti aliasing finite impulse response filter (FIR) to the data and changes the sampling rate of the signal by decimation or interpolation. Although one can resample the data at a higher rate, the resampled values occurring between measured samples do not represent measured information about the signal. Resampling should perform the decimation without aliasing effects. A factor of T should be included to normalize the data spectrum and preserve the energy density after decimation. Because the total signal energy is preserved by this operation and this energy must now be squeezed into a smaller frequency range, the amplitude of the spectrum at each frequency increases. Thus, the energy density of the decimated signal is not constant. The new sampling rate is actually derived from the average of the genuine signature data rates of a user. Sampled x position, y position, and θ of signals are shown in Figs. 2 and 3. The original genuine signature and the same signature after normalizing and resampling are shown in Fig. 4.

4.4. Handwritten signature 1D-DWT feature extraction

In this research, three factors are representing handwritten signature, x position, y position, and derived pen moving angle. Each of these vectors is considered as a stationary raw signal

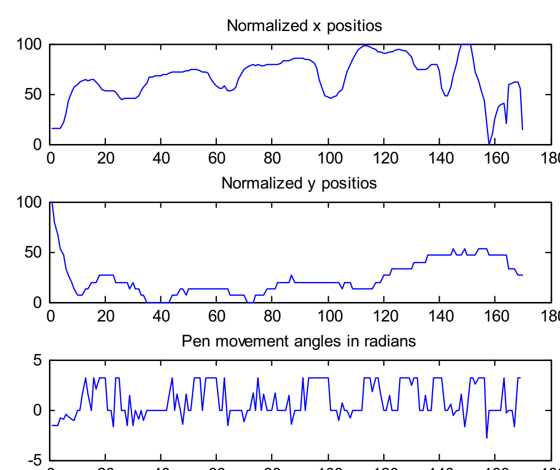


Figure 2 Normalized x position, y position, and pen movement angle features.

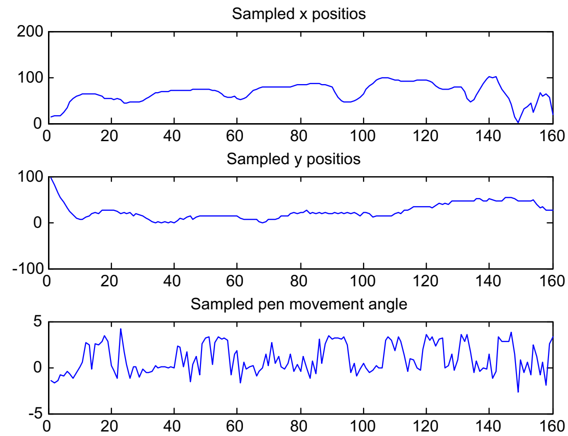


Figure 3 Sampled x position, y position, and θ.

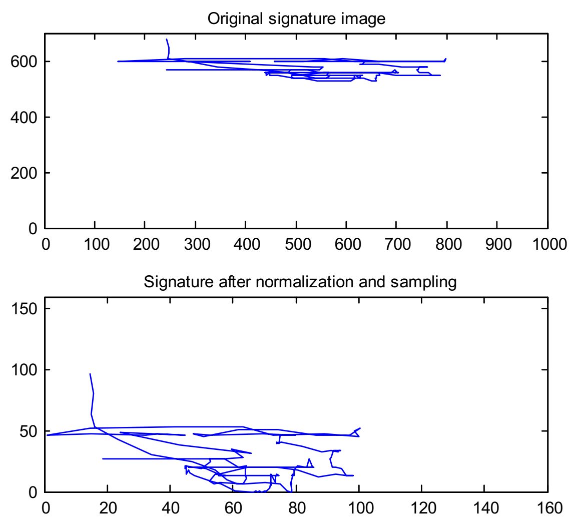


Figure 4 Example of a genuine signature after normalization and sampling.

in time domain. The reason is that the included information within these factors is advanced in time domain as long as the pen is moving by the user to form his signature. It is required to acquire relevant information along the whole signature. The discrete wavelet transform (DWT) provides sufficient information both for analysis and synthesis of the original signal with a significant reduction in the computation time. A wavelet is small (wave-like) waveform of limited duration with average zero value. In discrete signals, frequency is expressed in terms of radians. The following is a description of how the DWT is actually computed. The DWT analyzes the signal at different frequency bands with different resolutions by decomposing the signal into a coarse approximation and detail information. DWT employs two sets of functions called scaling functions and wavelet functions. These are associated with low pass and high pass filters, respectively. The decomposition of the signal into different frequency bands is simply obtained by successive high pass and low pass filtering of the time domain signal. The original signal $x[n]$ is first passed through a half band high pass filter $g[n]$ and a low pass filter $h[n]$. After the filtering, half of the samples can be eliminated according to the Nyquist's rule, since the signal now has a highest frequency of $\pi/2$ radians instead of π. The signal can therefore be sub-sampled by 2, simply by discarding every other sample. This constitutes one level of decomposition and can mathematically be expressed as follows:

$$y_{\text{high}}[k] = \sum_{n} x[n] \cdot g[2k - n], \tag{10}$$

$$y_{\text{low}}[k] = \sum_{n} x[n] \cdot h[2k - n], \tag{11}$$

where $y_{\text{high}}[k]$ and $y_{\text{low}}[k]$ are the outputs of the high pass and low pass filters, respectively, after sub-sampling by 2. The above procedure, which is also known as the sub-band coding, can be repeated for further decomposition. Thus, filtering and sub-sampling at every level will result in half the number of samples (and hence half the time resolution) and half the frequency band spanned (and hence doubles the frequency resolution). Fig. 5 illustrates this procedure, where $x[n]$ is the original signal to be decomposed, and $h[n]$ and $g[n]$ are lowpass and highpass filters, respectively.

This process continues until two samples are left. In this research and for each of the three time domain signals of x position, y position, and pen movement angle, there would be eight levels of decomposition, each having half the number of samples of the previous level. The DWT of the original signal is then obtained by concatenating all coefficients starting from the last level of decomposition. The DWT will then have the same number of coefficients as the original signal. Note that due to successive sub-sampling by 2, the signal length must be a power of 2, or at least a multiple of power of 2, in order this scheme to be efficient. The length of the signal determines the number of levels that the signal can be decomposed to. For example, if the signal length is 256, eight levels of decomposition are possible. The frequencies that are most prominent in the original signature signals will appear as high amplitudes in that region of the DWT signal that includes those particular frequencies. The frequency bands that are not very prominent in the original signature signals will have very low amplitudes. That part of the DWT signal can be discarded without any major loss of information hence allowing data reduction. Wavelet transform could have infinite set of basis. These basis functions are localized in time as well as frequency. There are different types of wavelet families like Morlet, Haar, Daubechies, etc. Daubechies wavelets are optimal in the sense that they have a minimum support for a given number of vanishing moments. Let vectors X and Y correspond to the x and y co-ordinates of the points of a resampled and normalized signature. The wavelet feature of the signature is extracted by applying DWT to the vectors X and Y separately. The approximation and detailed coefficients of DWT of X and Y are considered as the wavelet features for signature verification. Daubechies wavelet of the order 8 is used for DWT coefficients computation in this

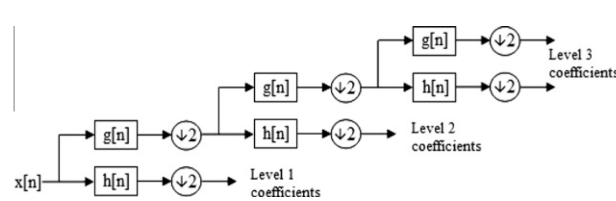


Figure 5 DWT computation process.

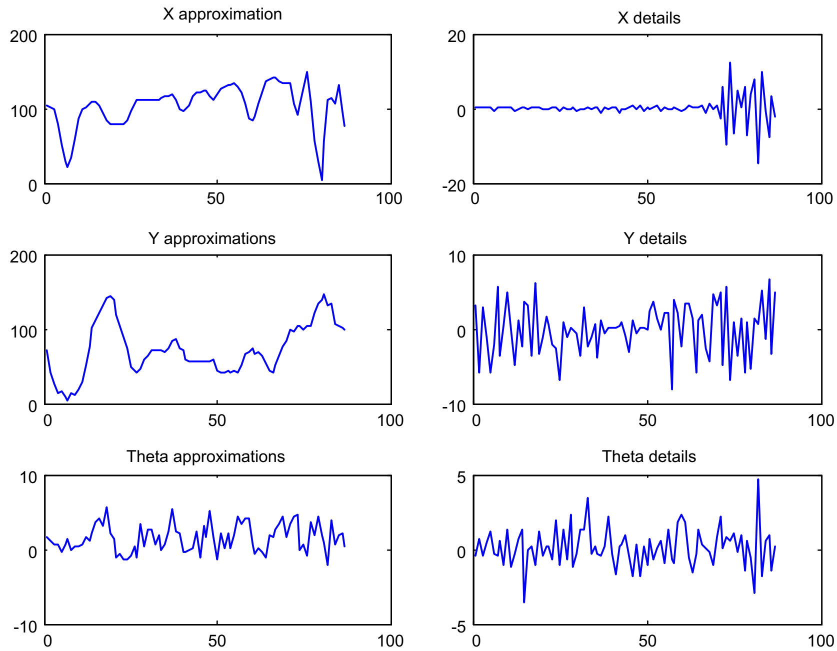


Figure 6 DWT coefficients for three features of the signature shown in Fig. 3.

research. DWT coefficients for three features of the signature (shown in Fig. 3) are shown in Fig. 6.

5. Classification using artificial neural networks

Classification is a process which has two phases: signal modeling and pattern matching. The combination of a handwritten signature feature signals and a matching technique is called handwritten signature classifier. The classification step in online handwritten signature identification systems is in fact a feature matching process between the features of a new handwritten signature and the features saved in the database. For successful classification, each handwritten signature is modeled using a set of data samples in the training mode, from which a set of feature vectors is generated and saved in a database. Common classifiers in signal identification include Gaussian Mixture Models (GMMs), Hidden Markov Models (HMMs), Vector Quantization (VQ) and Neural Networks (NNs) which is used in this research.

Neural networks are widely used for feature matching. The multi-layer feed-forward neural network is used for verification process. Major advantage of using it is its simplicity and adaptation to online implementation. It consists mainly of an input layer, hidden layer(s), and an output layer. Each layer consists of a number of neurons. Each neuron is connected to all neurons in the next layer through weights. To determine weight values, one must have set of examples of how outputs must relate to inputs. The task of determining weights from these examples is called training or learning. Multilayer feed forward neural network with only one hidden layer and sufficient number of neurons acts as universal approximate of nonlinear mappings. Addition of extra hidden layer can enhance the perceptive ability of neural network model at the cost of added computational complexity. It is difficult to determine exact number of hidden neurons required to realize desired accuracy. Frequently, number of neurons in hidden layer is determined by trial and error.

Error back-propagation learning algorithm consists mainly of two passes through the different layers of the network. In the forward pass, an input vector is applied to the sensory neurons of the network, and its effect propagates through the network layer by layer. Finally, a set of outputs produced as the actual response of the network. During the forward pass the synaptic weights of the networks are all fixed. In the backward pass the synaptic weights are all adjusted in accordance with an error correction rule. The actual response of the network is subtracted from a target response to produce an error signal. This error signal is then propagated backward through the network. Neural networks are useful when the underlying statistics of the task are not well understood. The simplest implementation of back propagation learning updates the network weights and biases in the direction in which the performance function decreases most rapidly, the negative of the gradient.

Bayesian regularization back propagation is a training function used in this research. It updates the weight and bias values according to Levenberg–Marquardt optimization. It minimizes a combination of squared errors and weights, and then determines the correct combination so as to produce a network that generalizes well. It minimizes performance function during training towards zero.

The learning and generalization capability of network is judged on the basis of certain performance measures such as MSE, SSE, NMSE, correlation coefficients, and rate of correct classification which is the most important criteria. The learning process inherent in neural networks (NN) is applied to the process of verifying handwritten signatures that are electronically captured.

6. Experimental setup and results

The handwritten signature information is extracted as time functions of various dynamic properties of the signatures. Features are extracted from the training data essentially striping away all unnecessary information leaving only the characteristic information with which handwritten signature models can be constructed. Only data for x position and y position are used in this research. Pen moving angles are then calculated from these data. The three time domain signals of x position, y position, and pen moving position are then normalized and resampled. Points (160) were chosen as resampling rate per signature. The discrete 1D wavelet transform (DWT) is performed on these features. When features of some unknown captured handwritten signature is extracted, pattern matching techniques are used to map the features from the input handwritten signature to a model corresponding to a known handwritten signature. Two experiments were carried on in this research. The first one implements the recognition of handwritten signature using total features extracted for each handwritten signature. The second one is to recognize handwritten signature using only distinguished DWT features of captured handwritten signature data. The two experiments are carried on the same handwritten signature database. A performance evaluation is done for each. A comparison of the performance of two experiments is then done. The proposed online handwritten signature verification system includes a database of signature templates storing verified signature (genuine) information. The set of measurements stored in a captured signature are compared against the known set of handwritten signature measurements to verify the identity of the signatory. Multi-matcher system which uses multiple representation and matching algorithms for the same input biometric signal is used to verify signature. The system is finally tested with skilled forged handwritten signatures. Following is a description of the used handwritten signature database.

6.1. Handwritten signature database

The signature database used in this research is the one used in First International Signature Verification Competition (SVC2004) [18]. Handwritten signatures were captured electronically after signing using PDA. Set of measurements representing points for each signature is saved in a text file. Out of these, only $x(n)$, $y(n)$ are used and then, pen moving angle $\theta(n)$ relating to the handwritten signature is determined. All data are stored in a signature file. The data set used in this research contains signature data collected from five users. Two databases were used in order to assess the system behavior. The first one is an offline database made of 20 genuine signatures for each of those five users. Second database includes 20 skilled forgeries created by different 20 volunteers for each of those five users. Each genuine/forgery signature is stored in a separate text file and also there is an image file for each of these signatures. In each signature text file, the signature is simply represented as a sequence of points. Examples of handwritten signature images of a user constructed from both x points and y points used in this research is shown in Fig. 7. One can notice high intrapersonal variations appear from these signatures. One can also notice low interpersonal variations appear from some of these signatures. Examples of handwritten skilled forgery signature images for these genuine signatures are shown in Fig. 8.

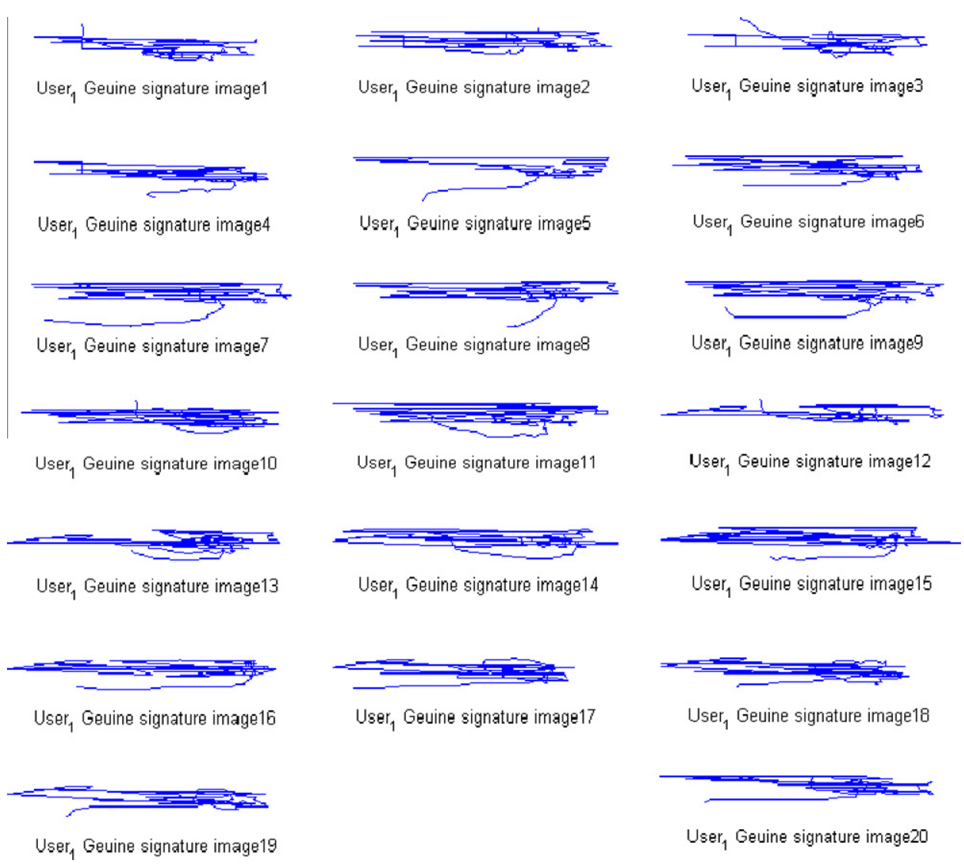


Figure 7 Examples of user 1 genuine signatures.

Figure 8 Examples of skilled forgery signatures for user 1.

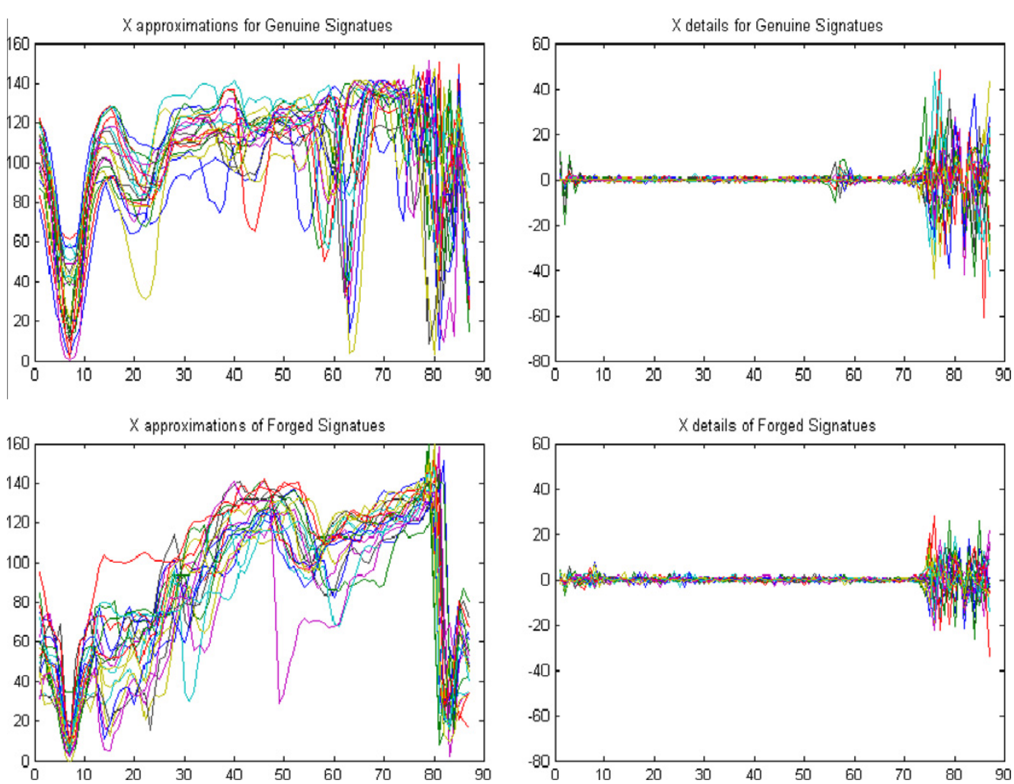


Figure 9 DWT features for x position parameter for genuine 20 signatures of user 1.

DWT feature coefficients are extracted for x position, y position parameters, and pen moving angles. Figs. 9–11 show the extracted DWT feature coefficients for both genuine signatures in Fig. 7 and forgery ones in Fig. 8. From these figures, one can notice a degree of similarity between most of the extracted coefficients for both genuine signatures and forgery signatures. Also, one can notice a degree of dissimilarity between the extracted coefficients for genuine signatures and forgery

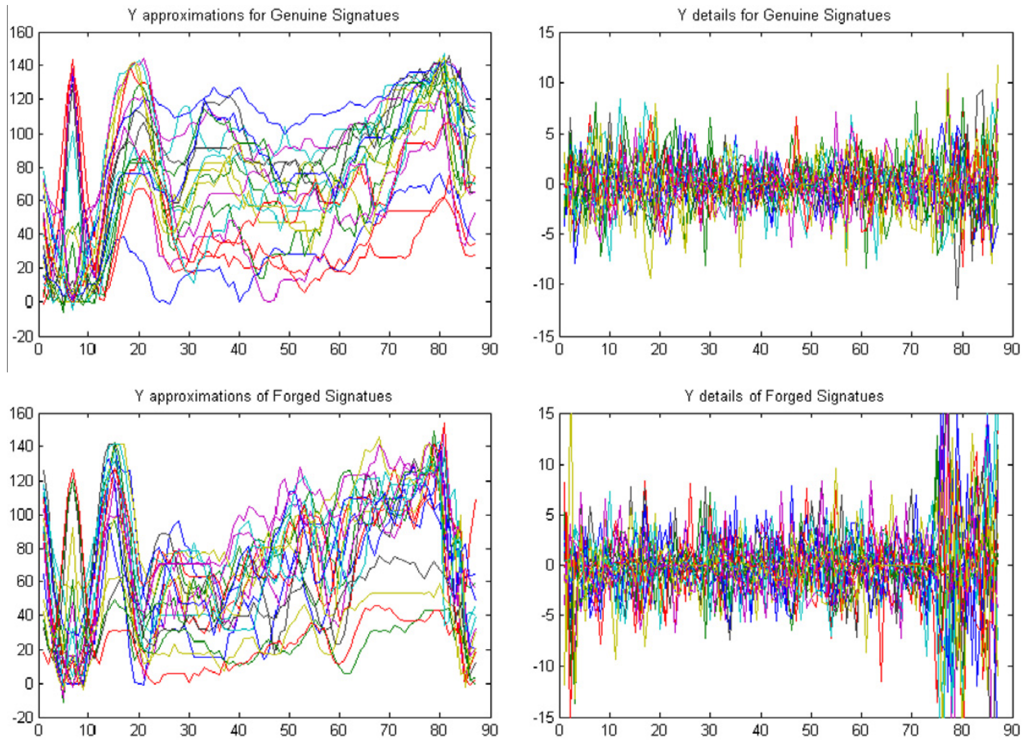


Figure 10 DWT features for y position parameter for genuine 20 signatures of user 1.

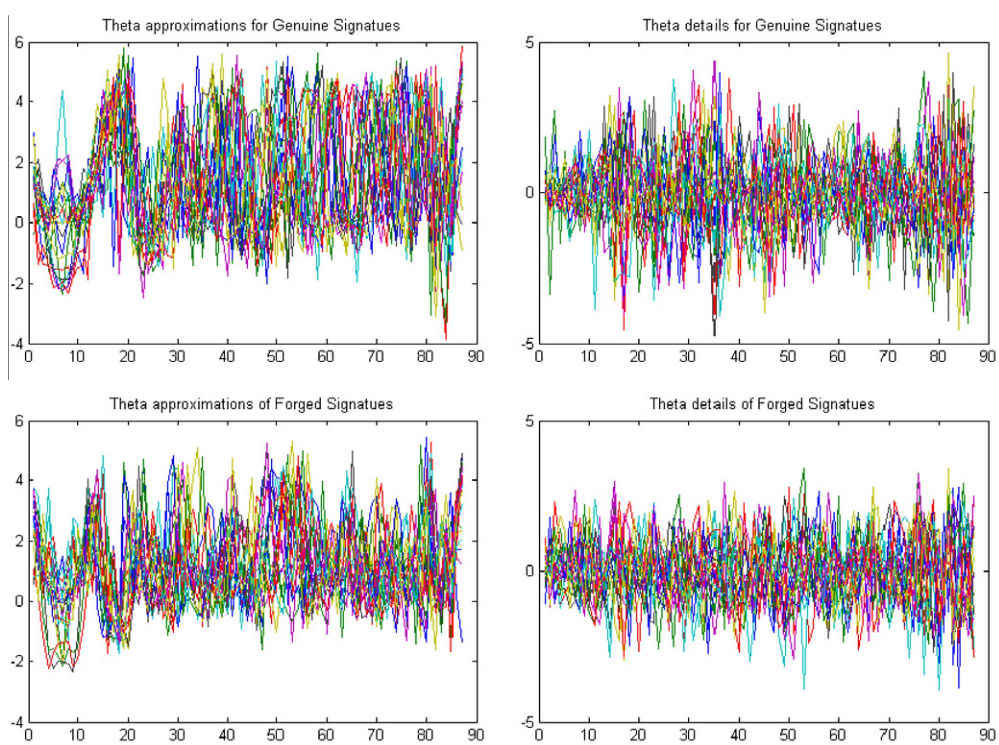


Figure 11 DWT features for moving angle parameter for genuine 20 signatures of user 1.

signatures for other coefficients. Signature forensic (expert) distinguish between forged handwritten signature and genuine one by looking for features that always happens in genuine ones but not in others (forged). The idea is to extract the distinguished features exists on approximations of x position, y position, and pen moving angle (θ) from group of genuine signatures and using them as a prove of within_class of the signature which means belonged_to_class factor to this signature. Then the distinguished extracted features from DWT details for each of each of three signature parameters could then assist in verifying if the signature is a genuine one and not forged. These specially collected, or extracted, feature vectors are those who exist always in genuine signatures, i.e. correlated to each other, and absolutely not occurring or uncorrelated to their correspondence in forged ones.

6.2. Neural network structure and design parameters

A bank of six neural networks is used as multi-matcher that uses multiple representations for the same input biometric signal (signature) to verify (Fig. 12). Each of the neural network adopted in this bank consists of an input layer having 87 inputs corresponds to DWT coefficients of x, y co-ordinates, and moving angle (θ) parameter; one hidden layer of neurons (70 neurons); and an output layer having 5 neurons. One of these output neurons is high (level 1) that represent the class which this signature belonged to among five genuine signatures classes.

In the learning or testing phase, wavelets features of training signatures are applied to neurons of input layer of neural network. The resultant output of each of the neural networks in this matcher is then multiplied by 'scaled score' value associated to that neural network. The total decision output of this multi matcher is then the sum of these 'scaled score' outputs of these neural networks. If this output exceeds a predetermined threshold, the signature is accepted as recognized. The total decision output of this multi matcher depends highly on the scaled score of the neural network output. The researcher suggests that the value of this 'scaled score' is to be the recognition rate that results when testing this neural network with genuine signatures that it was not trained to recognize. The training performance using Bayesian regularization of this multi matcher is shown in Fig. 13.

6.3. Obtained results and analysis

Programs for implementing the feature extraction and neural network verification phases in this proposed handwritten signature verification system are written using MATLAB. The verification scheme is achieved by observing the scored output for all six neural networks corresponding to inputs of approximations and details for each of the three parameters representing the signature. Each neural network is trained with 10 genuine signatures for each user and then tested with other 10 genuine signatures of the same user. Then the network is tested with 20 skilled forged signatures for each user.

Two experiments have been done. The first one when using all the DWT features extracted for each of the three parameters. The performance table is shown in Table 1. The second one when using only 25 DWT coefficients (selected intrapersonal features). These were chosen (to represent 'individuality') from DWT features for each of the three parameters that represents genuine signature. The performance table is shown in Table 2.

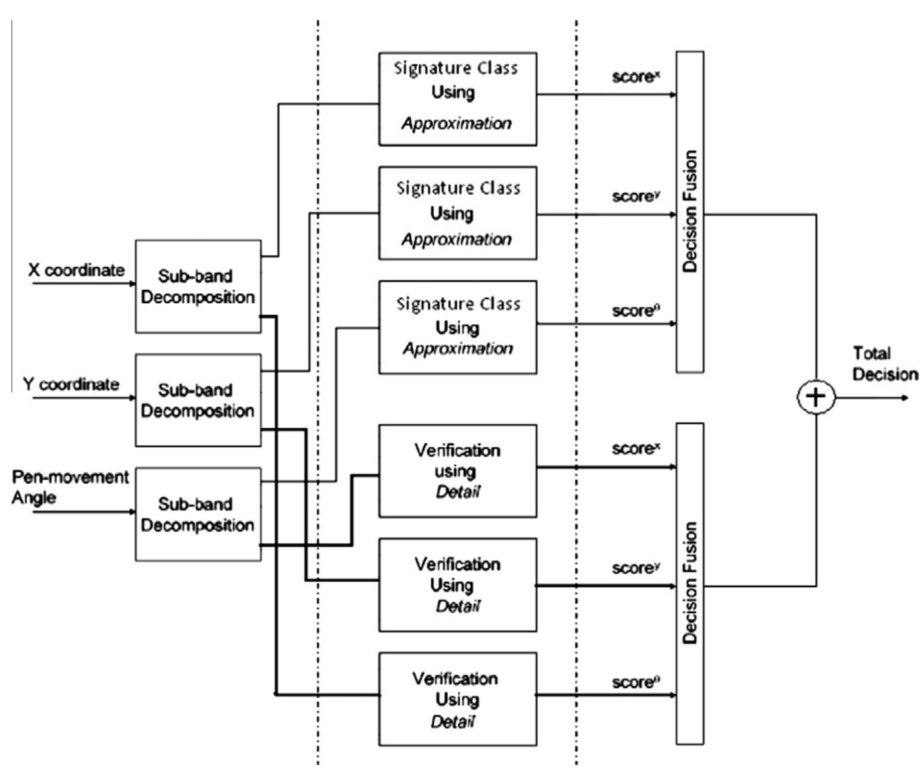


Figure 12 Proposed multi matcher verification for online handwritten signature.

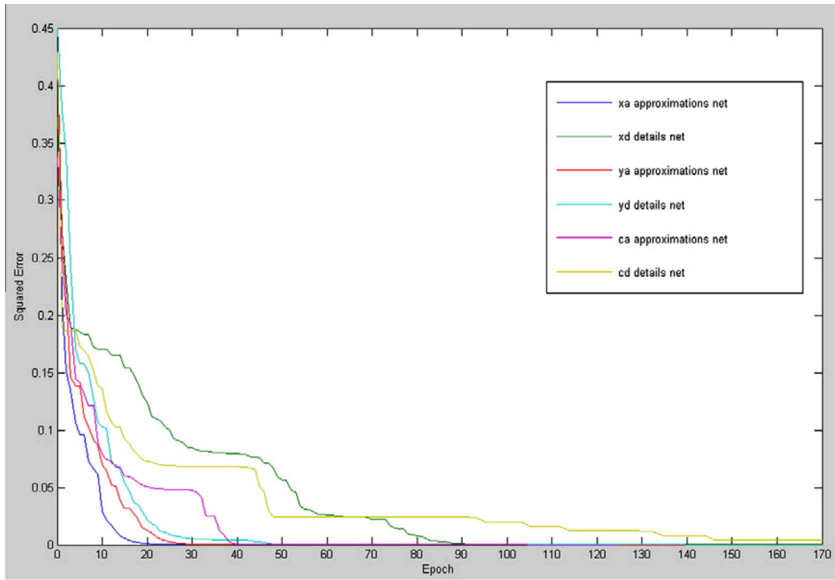


Figure 13 Training performance for six neural networks of multi matcher.

Table 1 The performance of first experiment when using all (87) the DWT features extracted for each of the three parameters x, y, and θ. 'a' means approximations and 'd' means details.

Selected features	Classification genuine trained (%)	Classification genuine not trained (%)	Classification of forgery as genuine (%)
x_a	100	90.0	24.0
x_d	100	46.0	24.0
y_a	100	90.0	27.0
y_d	100	34.0	27.0
θ_a	100	82.0	22.0
θ_d	100	30.0	27.0

Table 2 The performance of second experiment when using only (25 of less mean) individuality DWT features extracted for each of the three parameters x, y, and θ. 'a' means approximations and 'd' means details.

Selected features	Classification genuine trained (%)	Classification genuine not trained (%)	Classification of forgery as genuine (%)
x_a	100	94.0	11.0
x_d	100	79.0	9.0
y_a	100	95.0	14.0
y_d	100	74.0	8.0
θ_a	100	86.0	12.0
θ_d	100	78.0	8.0

For the first experiment, the results show that success rate was up to 90% when using all wavelet approximation features extracted thereby, suggesting that DWT feature extraction serves as a powerful tool for signature verification process (Table 1).

For the second experiment, it is observed that using only intrapersonal selected DWT features from approximation features results in remarkable improvement in the accuracy up to 95% (Table 2). It has been observed that using 'DWT approximations' as features for the recognition process give high recognition rates in both of the two experiments. While using DWT details results in poor recognition rates although it was improved in the second experiment.

7. Conclusion and recommendation for future work

Online handwritten signature verification system based on extracting sub-bands that represent intrapersonal features of signature from DWT representations of that signature is presented in this paper. Both extracted pen position and derived pen-movement angle parameters of handwritten signature data were decomposed into sub-band signals by DWT. Low frequency (approximations) and high frequency (details) sub-band signals were extracted for these parameters. Low frequency sub-band signals (approximation) are found consistent as features to enhance the difference between a genuine signature and its forgery. This is at least when using it in the recognition process with the signature database used in this research. The signature database consists of 20 genuine signatures for each of five users as well as 20 skilled forgeries for each user. A multi matcher (recognizer) consisting of six neural networks is used to recognize online handwritten signature. The inputs to this multi matcher are approximations and details of DWT coefficients for each of the three used parameters of a signature. The results show that success rate of the recognizer is 100% when tested with signatures it has been trained to recognize. When using all the extracted DWT approximation features, the success rate of the recognizer is up to 90% when tested with untrained genuine signatures. The rate of recognizing forgery signature as a genuine one is 24%. When only selected DWT features (that enhance interpersonal and suppress intrapersonal variations) are used in training and recognition processes, it results in improving the accuracy. Success rate of the recognizer is up to 95% when tested with untrained genuine signatures. Also, the rate of recognizing forgery signature as a genuine one is down to 8%. System performance could be improved if genuine signatures are more correlated and intrapersonal variations among it is low. Zero misclassification is required in such applications even if it is in the expense of high recognition rate. Other required target is that the recognition probability of forgery signature as if it is a genuine one is zero. Future work targets at further improving resultant system accuracy by fine tuning the selection of individual features (coefficients) that enhance the variation between genuine and forgery signatures. Also, improving the performance by selecting correlated genuine signatures as the training samples. Moreover, looking for better methods for selecting coefficients that represent intrapersonal features and hence could improve system performance. Furthermore, to compare performance of this system to performance of other systems when using same online handwritten signatures databases.

References

[1] Madasu Vamsi K, Lovell Brian C, Kubik Kurt. Automatic handwritten signature verification system for australian passports. In: Science, engineering and technology summit on counter-terrorism technology, Canberra, 14 July, 2005. p. 53–66.

[2] Zimmer Alessandro, Ling Lee Luan. A hybrid on/off line handwritten signature verification system. In: Seventh international conference on document analysis and recognition (ICDAR'03), vol. 1; 2003. p. 424.

[3] Trevathan Jarrod, Read Wayne, McCabe Alan. Neural network-based handwritten signature verification. J Comput 2008;3(8): 9–22.

[4] McCabe A, Trevathan J. Markov model-based handwritten signature verification. In: International conference on embedded and ubiquitous computing (IEEE/IFIP); 2008.

[5] Tolba AS. GloveSignature: a virtual-reality-based system for dynamic signature verification. Digital Signal Process 1999;9(4): 241–66.

[6] Güler İnan, Meghdadi Majid. A different approach to off-line handwritten signature verification using the optimal dynamic time warping algorithm. Digital Signal Process 2008;18(6):940–50.

[7] Bandyopadhyay SK, Bhattacharyya D, Das P. Handwritten signature recognition using departure of images from independence. In: 3rd IEEE conference on industrial electronics and applications (ICIEA 2008), Singapore, 2008.

[8] Zimmer Alessandro, Ling Lee Luan. Offline signature verification system based on the online data. EURASIP J Adv Signal Process 2008;2008:Article No. 112.

[9] Fernandez FA, Fierrez J, Gilperez A, Galbally J, Ortega-Garcia J. Spainrobustness of signature verification systems to imitators with increasing skills. In: 10th international conference on document analysis and recognition, 2009.

[10] Garcia-Salicetti S, Houmani N, Dorizzi B. A novel criterion for writer enrolment based on a time-normalized signature sample entropy measure. EURASIP J Adv Signal Process 2009;2009:Article No. 9.

[11] Lee Luan L, Berger Toby, Aviczer Erez. Reliable on-line human signature verification systems. IEEE Trans Pattern Anal Mach Intell 1996;18(6):643–7. doi:10.1109/34.506415.

[12] Ong Thian Song, Khoh WH, Teoh A. Dynamic handwritten signature verification based on statistical quantization mechanism. In: International conference on computer engineering and technology (ICCET'08), Singapore, 2009, vol. 2; 2009. p. 312–6.

[13] Nakanishi I, Sakamoto H, Nishiguchi N, Itoh Y, Fukui Y. Multi-matcher on-line signature verification system in DWT domain. IEICE Trans Fundam 2006;E89-A(1):178–85.

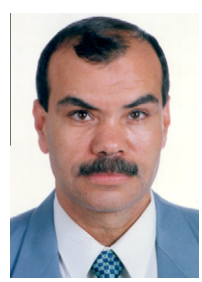
[14] Lejtman Dariusz Z, George Susan E. On-line handwritten signature verification using wavelets and back-propagation neural networks. In: Sixth international conference on document analysis and recognition (ICDAR'01); 2001. p. 0992

[15] Nanni Loris, Lumini Alessandra. A novel local on-line signature verification system. Elsevier; 2007.

[16] Nakanishi I, Nishiguchi N, Itoh Y, Fukui Y. On-line signature verification based on subband decomposition by DWT and adaptive signal processing. IEICE Trans Fundam 2004;J87-A(6):805–15.

[17] Enqi Zhan, Jinxu Guo, Jianbin Zheng, Chan Ma, Linjuan Wang. On-line handwritten signature verification based on two levels back propagation neural network. In: International symposium on intelligent ubiquitous computing and education (IUCE), China, 2009.

[18] First International Signature Verification Competition (SVC2004). <http://www.cse.ust.hk/svc2004/download>.



Dr. Maged worked as Researcher in Informatics Research Institute, Mubarak City for Scientific Research and Technological Application, Alexandria, Egypt. During the same time he was acting as Assistant Professor at Faculty of Science, Computer Division, Alexandria University. He got B.Sc. in Electronic Engineering, M.Sc. in Computer Security from Alexandria University in 1986. He got Ph.D. Engineering in Computer Vision from University of Newcastle (UK) in 1995. His fields of interest is in Programming Languages, Artificial Intelligence, Computer Vision, Fuzzy Logics, and Computer Networks.