Freeman Chain Code (FCC) Representation in Signature Fraud Detection Based On Nearest Neighbour and Artificial Neural Network (ANN) Classifiers

Aini Najwa Azmi *aininajwa.azmi@gmail.com*
Deparment of Computer Science,
Faculty of Computing,
Universiti Teknologi Malaysia,
Skudai, 81310, Malaysia

Dewi Nasien *dewinasien@utm.my*
Deparment of Computer Science,
Faculty of Computing,
Universiti Teknologi Malaysia,
Skudai, 81310, Malaysia

Abstract

This paper presents a signature verification system that used Freeman Chain Code (FCC) as directional feature and data representation. There are 47 features were extracted from the signature images from six global features. Before extracting the features, the raw images were undergoing pre-processing stages which were binarization, noise removal by using media filter, cropping and thinning to produce Thinned Binary Image (TBI). Euclidean distance is measured and matched between nearest neighbours to find the result. MCYT-SignatureOff-75 database was used. Based on our experiment, the lowest FRR achieved is 6.67% and lowest FAR is 12.44% with only 1.12 second computational time from nearest neighbour classifier. The results are compared with Artificial Neural Network (ANN) classifier.

Keywords: Offline Signature Verification System (SVS), Pre-processing, Thinned Binary Image (TBI), Feature Extraction, Freeman Chain Code (FCC), Nearest Neighbour, Artificial Neural Network (ANN).

1. INTRODUCTION

Biometrics authentication is subject to the identification and verification of humans by their characteristics or traits. Biometrics is widely utilise in computer science as a form of access control and identification. It is also used to recognize individuals in groups that are under surveillance. SVS is a system that identifies and verifies a handwritten signature to detect either it is genuine or forgeries. Usually, it can be done by comparing one-to-one process. Similar in personal identification, the system compares the signature information with all the images stored in the database [1]. It is very important in forensic, security and resource access control such as banking, money scam, marriage approval and user access devices. In the field of human identification, signature is one of the cheapest biometric beside DNA, fingerprint, palm print, face, vein pattern, retina and iris. These physiological traits are almost unchanged throughout of a person's life. Unlike signature, it may change with mood, environment and age. A person who does not sign in a consistent manner may have difficulty in identifying and verifying his/her signature. The database should be changed or updated in a few specified periods to make sure the authentication system is working properly. In addition, a good database must have a series of signatures from a person that are almost similar between each other for better verification. In the series, many characteristic must remain constant to determine the confidence level.

There are three groups in signature forgeries. The first one is simple forgery that the forger makes no attempt to simulate or trace a genuine signature means that the forger does not know at all how the signature looks like. The second one is random possible. The problem that we want to solve is regarding to skilled forgeries compare to simple and random forgeries [2]. Handwritten is different compare to signature. Signature must be treated as an image because people may use symbol, letter or group of letters in their signatures. This means that we cannot always identify the name of the writer when looking into the signature.

Signature Verification System (SVS) can be classified to static (offline) and dynamic (online). In an offline system, users write their signature on a paper and digitize by using a scanner or a camera. The SVS recognizes the signature by analyzing its shape or static features. In the other hand, an on-line system needs a user to write their signature in a digitizing tablet, that needs the signature in real time form. Another possibility is the acquisition by smart phone, tablet or stylus-operated PDAs. An on-line system can record dynamic features of the signature that make it difficult to forge. An on-line system is appropriate to use in real-time applications, such as financial transactions, document authenticity and office automation [1].

Generally, a SVS can be classified to four major components called as can see in Figure 1:

i. Data acquisition
ii. Pre-processing
iii. Feature extraction
iv. Verification

1.1 Data Acquisition

Data acquisition is the process of sampling signals that measure real physical conditions and converting the resulting samples into digital values that can be manipulated by a computer. A data acquisition system is converting analogue waveforms into digital values for processing. MCYT-SignatureOff-75 database will be used in the entire phases include pre-processing, feature extraction and classification. There are 75 users in this database. One user has 15 genuine signatures and 15 forgery signatures [3].

1.2 Pre-processing

Pre-processing is the process to prepare a clean signature image as an input to feature extraction. There are a lot of techniques had been done in previous works discussed in next section. As the original images contain a lot of noises and redundancy pixel, cropping, skew adjustment and thinning had been done. In an off-line handwritten Signature Authentication System (SAS), static signatures which normally scanned from a flatbed scanner contain a lot of redundant pixels that need to be removed. Besides that, size adjustments were applied to the signature images, aiming to become the authentication process more robust [4].

1.3 Feature Extraction

Feature extraction is a process that involves simplifying the amount of resources required to describe a large set of data accurately. When performing analysis of complex data one of the major problems occurs from the number of variables involved. Analysis with a large number of variables generally requires a large amount of memory and computation time or a classification function which over fits the training sample and generalizes poorly to new samples. Feature extraction is a general form for methods of generating combinations of the variables to get around these problems while still describing the data with sufficient accuracy.

1.4 Verification

Verification or classification may refer to categorization and recognization which are processes in which ideas and objects are differentiated, and understood. Classification and clustering are examples of the more general problem of pattern recognition, which is the task of some sort of output value to a given input value. Other examples are regression, which assigns a real-valued output to each input; sequence labeling, which assigns a class to each member of a sequence of values.

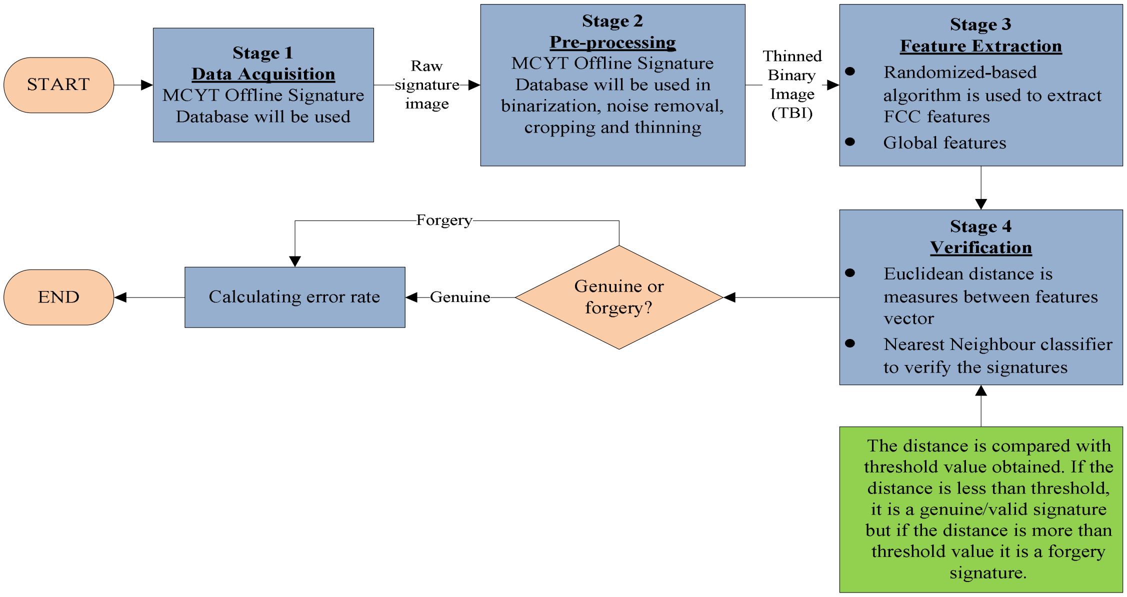
START
Stage 1
Data Acquisition
MCYT Offline Signature Database will be used
Raw signature image
Stage 2
Pre-processing
MCYT Offline Signature Database will be used in binarization, noise removal, cropping and thinning
Thinned Binary Image (TBI)
Stage 3
Feature Extraction
Randomized-based algorithm is used to extract FCC features
Global features
Stage 4
Verification
Euclidean distance is measures between features vector
Nearest Neighbour classifier to verify the signatures
The distance is compared with threshold value obtained. If the distance is less than threshold, it is a genuine/valid signature but if the distance is more than threshold value it is a forgery signature.
Genuine or forgery?
Forgery
Genuine
Calculating error rate
END

FIGURE 1: Four major components in a SVS.

2. LITERATURE REVIEW

2.1 Data Acquisition and Pre-processing

Data acquisitions for on-line and off-line systems are totally different. Signature samples will be divided to two sets which are genuine and forgery sets. In on-line system, signatures can be captured using a variety of input devices such as specially designed pens, hand gloves, special tablets, personal digital assistant (PDA) and tracking-camera [1,5]. The tablet can gather the signature position coordinates, including of X coordinates, Y coordinates, total signing duration, number of pen-ups, number of strokes and the pressure value of the pen. Some features extracted from these signatures can be used as expressing one's handwriting habit and individuality, such as pen pressure, velocity in X and Y direction [1]. All of these are called as dynamic information that we can consider as features in the next stage. In the other hand, in an off-line system, signatures are optically captured by using a scanner and the completed signatures are available as images [6]. As a scanned signature contains a lot of noise thus it must be pre-processed to produce a clean image as preparation prior feature extraction.

In an off-line system, static signatures which normally scanned from a flatbed scanner contain a lot of redundant pixels that need to be removed. Besides, size adjustments were applied to the signature images, aiming to become the authentication process more robust [4]. Some algorithm that commonly used in removing or reducing noise such as by using median filter and thinning by using morphological operation [2,7,8]. Noise removal method that based on counting filter was proposed by [9]. Besides, they also binarized and resized the image with the signature fitted to the frame or know as edges cutting [10].

Binarization means the images are converted to binary images such that signature become white and background become black. A histogram-based threshold technique was applied for binarization and the image will be stored in TIFF format [11,12] In addition, Otsu's method was used to binarize and enhance the quality of a signature image [13]. The Robert edge detection was applied on a signature image to convert it into edges and Gaussian filter was used to remove noise [2]. Color inversion, filtering and binarization were applied to the signatures images [9,15]. The true color image RGB was converted to the grayscale intensity image by eliminating the hue and saturation information while retaining the luminance and a low pass FIR was used to remove the image high frequency components. Center of mass normalizing and smoothing by using Gaussian filter was applied in [16]. Center of mass normalizing was used to calculate image coordinates easier. Zhang-Suen Skeletonization Algorithm was applied in [9] to extract a region-based shape feature representing the general form of an object. Segmentation was done in [17, 18, 19] when the signature image was segmented to ten concentric circles instead of rectangle frame that commonly used in literature. In this case, the signature was fitted to the circular frame. By segmenting the signature image to ten concentric circles, the calculations of the feature became easy. In addition, Hamming Distance was used to stabilize the static signature image [20]. Table 1 shows summary of pre-processing methods in previous work of offline systems.

Authors	**Year**	**Pre-processing Methods Used**
Ubul *et. al* [4]	2012	Resizing
Cheng-Yaw *et. al* [8] Tomar and Singh [7] Ravi *et. al* [2]	2008 2011 2012	
Cheng-Yaw *et. al* [8]	2008 2011 2012	Noise reduction by median filter and thinning by morphological operation
Oz [9]	2005	Noise reduction by counting filter
Karouni *et. al* [16] Tomar and Singh [7]	2008 2011	Noise reduction by Gaussian filter
Ghandali & Moghaddam [10]	2008	Binarization
Porwik [11]	2007	Binarization using threshold technique
Pal *et. al* [13]	2012	Binarization using Otsu's method
Tomar and Singh [7]	2011	Robert's edge detection
Cheng-Yaw *et. al* [8] Pourshahabi *et. al* [15]	2008 2009	Colour inversion
Karouni *et. al* [16]	2008	Removing high frequency components by using low pass FIR
Karouni *et. al* [16]	2008	Center mass normalization
Cheng-Yaw *et. al* [8]	2008	Zhang-Suen Skeletonization Algorithm
Lei & Huichuan [17] Ning [19] Biswas *et. al* [18]	2009 2009 2010	Segmentation
Impedovo & Pirlo [20]	2011	Hamming Distance

TABLE 1: Summary of pre-processing methods in previous works of offline systems.

2.2 Feature Extraction

Two signatures wrote from a person are hard to compare. Some possibilities may occur such as variations in length, additions and deletions of portions of them, and changes in velocity due to pauses or hesitations of the writer [21]. Figure 2 and 3show two signatures that wrote by a person. We can see the difference between the two images but of course they have a lot of similarities that can be extracted as features that will be discussed in detail in the this section.

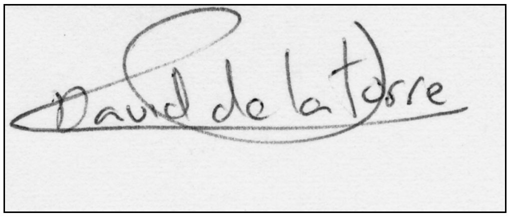

FIGURE 2: Sample signature image from person A.

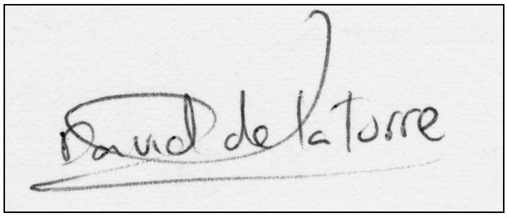

FIGURE 3: Another sample from person A.

In an off-line system, Discrete Wavelet Transform (DWT) was proposed to use in image reduction phase in order to extract the features [10, 22, 23]. DWT decomposed a signature image to sub-image based on different frequency bands. The reduced images were fused in high frequency sub image and generated a pattern matrix that will be the feature vector of a signature image. Ratios of the pixels of strokes of every section to the pixels of strokes of signature were calculated to produce the feature vector.

Different features such as direction features, gradient features, under-sampled bitmaps and modified chain-code extracted from both background and foreground components are employed for this purpose [12]. They proposed a new technique in under-sampled bitmaps that used both foreground and background pixels. A binarized signature image will be divided to 100 non-overlapping blocks and the chain code frequency for four directions was used instead of eight directions. A Robert's filter was applied on the image to obtain the gradient image after the image was binarized, normalized and resized.

Zernike moment and histogram of gradient were the two features that used by [13,14]. The Zernike moment feature obtained by solving several complex-valued polynomials. According to their passed work in [12] Robert's filter was still used to obtain the gradient image. In addition, they calculate histograms image. The intrinsic features of handwriting signature were described [24]. The features included calculation of height/width ratio, principal axis orientation, elongation, handwritten slope, amount of connected components, hole and cavity attributes and point density of different areas.

Contourlet transform was used as feature extraction in [15, 25, 26] and was an efficient tool for capturing smooth contours. Contourlet transform has five significant features which are multiresolution, localization, critical sampling, directionality and anisotropy. Contourlet transform is applied on each block of the image separately and feature vector was created for that block. By putting the 4 created feature vectors together, final feature vector was obtained. Genetic algorithm was used to find the number of optimal regions that optimally separate the spectral classes. This algorithm took into account multivariate relationships between the components of the spectral signatures [27]. The second one was an L_1-norm Support Vector Machine (SVM) that produces sparse solutions.

The pre-processed signature was considered and spatial domain features were extracted leads to global [13]. The features included height and width of signature, diagonal distance and center of gravity. Several NN-based classification models including support vector machines (SVM) with linear, polynomial, and RBF kernels and multilayer perceptron (MLP), radial basis function (RBF) network were developed for signature extraction and device identification. These models were trained and tested using spike train data gathered from the Fourier analysis of the input current waveform in the presence of multiple devices [24]. There were two approaches used in [7] for feature extraction which were energy density method and chain code method. Aspect ratio was used as a global feature and energy density was used as local feature. Chain-code is based on the direction of the connecting pixels. Each pixel was observed for next connected pixel and their direction changes mapped by giving a numerical value to every 8-direction chain code. Statistical features such as aspect ratio, slant angle, variance, skewness, kurtosis, horizontal and vertical shift, entropy, join entropy and mutual information were extracted in [28].

A system that based on wavelet feature was proposed by [29]. Wavelet features consists horizontal and vertical projection that produced when the DWT was applied to the image. A system that based on Statistical Analysis, Theory of Estimation and Mean Variance was proposed [30]. A new Data Hiding and Extraction algorithms for data protection that detection, more verification, convincing for ownership and are more efficient for recipient and more secure was proposed in [31]. After pre-processed, the signature image was projected into feature space by using Discrete Radon Transform (DRT). As DRT yields feature space of high dimensionality, Principle Components Analysis (PCA) is introduced to compress the DRT feature without losing the significant attributes [8]. After that, PCA feature was statistically discritized into binary representation. Proportion and distribution of pixels, tilt, pressure, and centroid were applied in [32]. The proportion referred to the ratio between the height and width of the image, the distribution of pixels was made through a grid which subdivided the image and it was counted how many pixels are expressed in the current sub image. The handwritten signature in [33] was represented in time domain representation. The representation was in discrete time sequence which all the elements were in complex numbers. Feature extraction was done by mean of the Hotelling's discriminant analysis [34]. The Hotelling's approach allowed removing such features which has the smallest discriminant power. Practically, discriminant analysis is useful to decide, whether selected pair "feature–method" is important for the classification process – if not, the other pair "feature–method" is tested. The Feature-Method-Selection (FMS) was proposed when they found that there were some insufficient criteria found in the literature they had done. Geometric features were used in [16] in their feature extraction. The geometric features included area, center of gravity, eccentricity, kurtosis and skewness. The combination of variance into Dynamic Time Warping algorithm to calculate the intra-class distance (between real signatures) and inter-class distance (between real-forged signatures) was used in [35].

Three methods were used in [17] There were edge detection, Wavelet Transform and Hough Transform. Moment invariants were properties of connected regions in binary images that were invariant to translation, rotation and scaling. This method was applied in [9]. Levenshtein method in a signature recognition process was proposed in [36]. Proportion factor, center of gravity and Hough Transform were used [11] for their feature extraction. The features used in [37] were width, height, tri-Surface, six-fold surface, best fit, geometric parameters, Polar and Cartesian Direction Feature (MDF), K-Means, Histogram of frequencies, Discrete Cosine Transform and Wavelet Transform. Multi-dimensional modified grid information features were extracted according to the character of Uyghur signatures [4]. A combination of multiple distance-based classification techniques, namely individually optimized re-sampling, weighted Euclidean distance, fractional distance and weighted fractional distance was used in [38] . In order to process large amount of data, a hierarchical partitioning of data by utilizing two database reduction techniques which were feature selection and clustering and by finding the classifier that was appropriate for each signature model was proposed by [19,39]. Recently, pixel matching technique was used to verify the signature of the user with the signature that kept inside database [31] There was also a multiple feature extraction used in [40] that increased diversity of information produced in signature images. Table 2 below shows summary of feature extraction methods in previous works of offline systems.

Authors	Year	Feature Extraction Method Used
Pottier & Burel [24]	1994	Intrinsic features (height/width ratio, principal axis orientation, elongation, handwritten slope, amount of connected components, hole and cavity attributes and point density of different area)
Deng *et. al* [22] Ghandali & Moqhaddam[10] Fahmi [23] Angadi & Gour [29]	2003 2008 2010 2013	Discrete Wavelet Transform (DWT)
Pal *et. al [12]* Tomar & Singh [7]	2011 2011	Modified chain-code
Pal *et. al* [13] Pal *et. al* [14]	2012 2012	Zernike moment and histogram of gradient
Pourshahabi *et. al* [15] Soleymanpour *et. al* [25] Abushariah *et. al* [26]	2009 2010 2012	Contourlet transform
Pranckeviciene *et. al* [27]	2005	Genetic Algorithm (GA)
Akram *et. al* [28]	2012	Statistical features (aspect ratio, slant angle, variance, skewness, kurtosis, horizontal and vertical shift, entropy, join entropy and mutual information)
Bandyopadhyay *et. al* [30]	2008	Statistical Analysis, Theory of Estimation and Mean Variance
Cheng-Yaw *et. al* [8]	2008	Principle Components Analysis (PCA)
De Medeiros Napoles *et. al* [32]	2011	Global features (proportion and distribution of pixels, tilt, pressure, and centroid)
Doroz & Porwik [34]	2011	Hotelling's discriminant analysis
Karouni *et. al* [16]	2011	Feature-Method-Selection (FMS)
Palys *et. al* [37]	2013	Cartesian Direction Feature (MDF),
Oz	2005	Moment invariants
Melin [36]	2012	Levenshtein method
Ubul *et. al* [4]	2012	Multi-dimensional modified grid information features
Bhattacharya *et. al* [31]	2013	Pixel matching technique

TABLE 2: Summary of feature extraction methods in previous works of offline systems

2.3 Classifications

Neural network was one of the famous classifier that employed in previous works [20]. A modular neural network (MNN) with fuzzy integration for the problem of signature recognition was proposed by [36]. Two separate sequential neural networks were designed by [9] one for signature recognition and another for verification to detect forgery. Also a time delay neural network was used by [41]. A neural network of radial basis function optimized by Differential Evolution Algorithm with features that best discriminates between a genuine signature of a simulated forgery was proposed by [32]. A multi layer feed forward network employing a back propagation was introduced by [7,16,28]. Several NN-based classification models including multilayer perceptron (MLP) [26,42] radial basis function (RBF) network, and support vector machines (SVM) with linear, polynomial, and RBF kernels were developed for signature extraction and device identification [29]. The proposed 2-layer perceptron neural networks were compared with other classifiers as pseudo-inverse, k-Nearest Neighbours (k-NN) and K-Means [24]. K-Nearest Neighbours (k-NN) [34,43] was developed by inserting HMM based features [18] Euclidian Distance was used by [4, 10, 15, 21, 38 ,44] in their verification stage. Support Vector Machine (SVM) [13, 14, 25, 27, 45, 46] and Nearest Neighbour (NN) were used as classifier in [12]. The Support Vector Machine (SVM), with biometric watermarking to precisely extract the signature code from the host [8]. They abbreviated the proposed method as Support Vector Machine-Biometric Watermarking) SVM-BW. The performance of SVM-BW was validated against simulated frequency and geometric attacks. An autoregressive Hidden Markov Model (AR-HMM) was employed in [47]. The correlation technique was used to match between genuine signatures [2]. A proposed Hidden Markov Model (HMM) by [48] was evaluated the robustness of their system against changes with time using long term and large scale signature database. Adaptation of the Levenshtein method in a signature recognition process is proposed by [37]. A suitable classifier was determined to a different cluster of hierarchical partitioning [38]. Neural Networks, Support Vector Machines, Bayesian classifiers or Decision Trees were known to perform well in a signature recognition system. Clustering techniques making no assumptions about the structure of the data are also widely used in this area. Global classifier was used in [49] to work on assumption that there exist forgery features that differentiate between genuine and forgery signatures. Table 3 shows summary of classification methods in previous works of offline systems.

Authors	**Year**	**Classifications Methods Used**
Pottier and Burel [24] Oz [9] Tomar & Singh [7] Karouni *et. al* [16] Jayadevan *et. al* [41] De Medeiros Napoles *et. al* [32] Akram *et. al* [28]	1994 2005 2011 2011 2012 2012 2012	Neural Network (NN)
Melin [36]	2012	Modular Neural Network (MNN)
Heinen & Osorio [42] Abushariah *et. al* [26]	2006 2012	Multi-Layer Perceptron (MLP-NN)
Srinivasan *et. al* [50]	2006	Radial Basis Function (RBF) Network
Pranckeviciene *et. al* [27] Srinivasan *et. al* [50] Cheng-Yaw *et. al* [8] Soleymanpour *et. al* [25] Batista *et. al* [46] Ribeiro *et. al* [45] Pal *et. al* [12] Pal *et. al* [13]	2005 2006 2008 2010 2010 2011 2011 2012	Support Vector Machine (SVM) Support Vector Machine (SVM)
Pottier and Burel [24] Shashi Kumar *et. al* [42] Doroz & Porwik [34] Pal *et. al* [12]	1994 2010 2011 2011	k-Nearest Neighbours (k-NN)
Ghandali & Moqhaddam [10] Pourshahabi *et. al [15]*	2008 2009	Euclidian Distance

Mendaza-Ormaza *et. al* [44] Munich & Perona [21] Ubul *et. al* [4] Moolla *et. al* [38]	2011 2011 2012 2012	
Paulik & Mohankrishnan [47]	1993	Hidden Markov Model (HMM)
Palys *et. al* [37]	2013	Levenshtein method
Moolla *et. al* [38]	2012	Bayesian Network
Putz-Leszczynska & Pacut [49]	2013	Global classifier

TABLE 3: Summary of classifications used in previous works of offline systems.

3. RESEARCH METHODOLOGY

3.1 The Research Framework

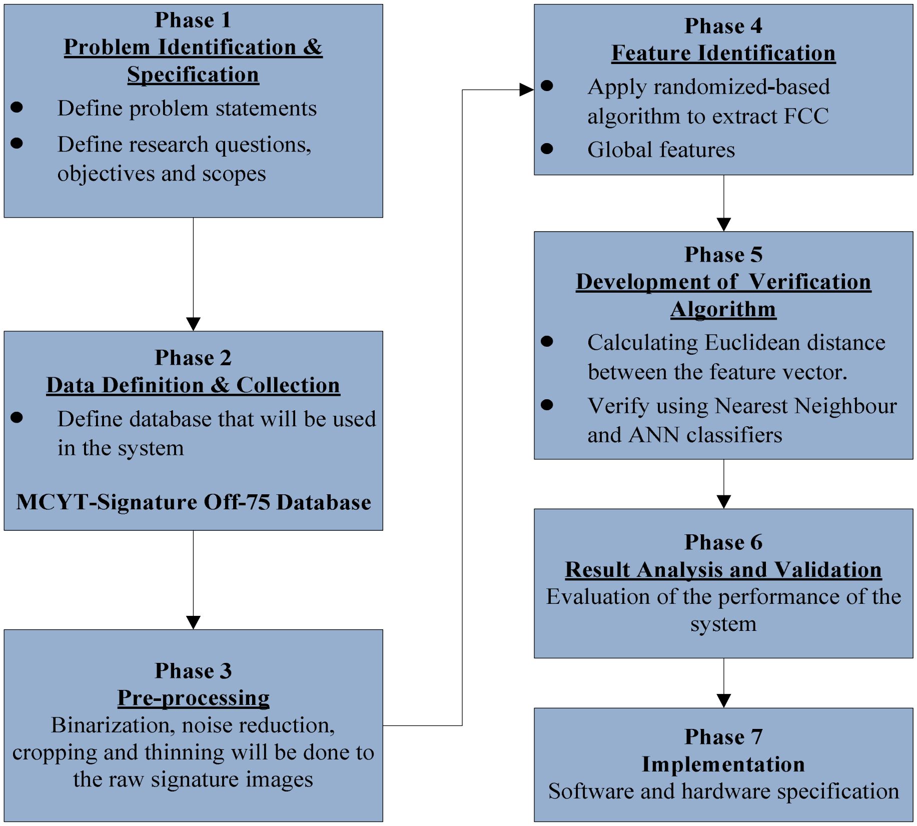
Phase 1
Problem Identification & Specification
Define problem statements
Define research questions, objectives and scopes
Phase 2
Data Definition & Collection
Define database that will be used in the system
MCYT-Signature Off-75 Database
Phase 3
Pre-processing
Binarization, noise reduction, cropping and thinning will be done to the raw signature images
Phase 4
Feature Identification
Apply randomized-based algorithm to extract FCC
Global features
Phase 5
Development of Verification Algorithm
Calculating Euclidean distance between the feature vector.
Verify using Nearest Neighbour and ANN classifiers
Phase 6
Result Analysis and Validation
Evaluation of the performance of the system
Phase 7
Implementation
Software and hardware specification

Figure 4: The research framework.

Research framework is describing the whole activity in this research. The research framework is shown in Figure 4. It shows the processes involved in each phase briefly. The research framework has seven phases, which are:

i. Problem Identification and Specification.
ii. Data Definition and Collection.
iii. Pre-Processing and Freeman Chain Code (FCC) Extraction.
iv. Development of Feature Extraction
v. Development of Verification Algorithm.
vi. Result Analysis and Validation.
vii. Implementation

3.2 The Problem of Identification and Specification

In Phase 1, the procedure started with literature review on issues related signature authentication systems. The trend of the methods for each phase can be seen that can give a clear idea on what will be done in this research. In pre- processing, several techniques will be used to prepare the signature images prior feature extraction phase. In feature extraction and selection, a randomized-based algorithm [51] will be applied to generate the chain code and followed by feature selection to be generated. Next, is the problem and description of ANN and HMM as classifiers to classify signature images. Finally the problems in verification process are to find the lowest error rate for the system.

Next, once the literature review of signature authentication system is studied, the problem statement of the research is conducted so that the objective can be achieved to answer the problem statements. The process of problem identification of the research is done by referring to the previous literatures in published papers and journals. In order to constraint the work, scope must be defined according to the decided objectives.

After the problem statements are identified, objectives and scopes of the research must be clearly defined to avoid duplication of work that has been previously made by researchers. Finally, issues on implementation specification namely software and tools for the experimentation, and hardware required for the purpose is specified. After the problem identification and specification is completed, the next step is data definition and collection

3.3 Data Definition and Collections

Data definition is a process of defining the type of data used, deciding the sources of database, checking the validity of the database, and categorizing the database for testing and validation. In the other hand, data collection means having the input data extracted or built from the original source and gathered into a compilation of huge numbers of input. Therefore, data collection is gathering relevant information in order to develop, testing, validating and analysing the algorithms.

In this research, an off-line signature database which is known as MCYT-SignatureOff-75 has been used. This database contains 75 users and originally from Universidad Autónoma de Madrid, Spain. In the case of the MCYT_Signature subcorpus, 15 client signatures and 15 highly skilled forgeries with natural dynamics are obtained for each individual [3] that equals to total of 30 signatures per user. The MCYT-SignatureOff-75 database will be used in the entire phases of this research.

3.4 Data Acquisition and Pre-processing

In pre-processing phase, binarization was done to every signature images. After that, median filter was applied to remove image noises. Next, cropping is done to the original signature images. Cropping refers to the removal of the outer parts of an image to improve framing, accentuate subject matter. This is important in aspect ratio calculation in feature extraction phase.

Cropping also must be done before skew adjustment. Finally, thinning algorithm is used to remove redundancies by eliminating specific foreground pixels. In converting raw binary image to Thinned Binary Image (TBI), thinning function in Image Processing Toolbox of MATLAB software is used respectively [51]. The proposed thinning algorithm for MCYT database is parallel thinning algorithm. Manipulation from the raw binary image to TBI is using 'bwmorph' function in the Image Processing Toolbox in MATLAB. The result of TBI will be copied automatically in a directory that is determined earlier into text format (.txt file) and for easier usage. Figure 3.4 is showing the sample signature image after every technique in feature extraction phase. Figure 3.5 shows the flow of output image of every technique used in pre-processing phase.
The signature images received are all in equal size which is 850x360 pixels. In this phase, resizing is not required. Since the database is not big, the size is acceptable in the pre-processing, feature extraction and verification phase.

Chain code representation gives the code of the boundary of signature image, the codes that is representing the direction of where is the location of the next pixel and correspond to the neighbourhood in the image. The FCC algorithm of a signature image must use binary image as input. Binary image is a image with only two gray values for each pixel, such as 0 is for background and 1 is for foreground. . An 8-direction FCC is used for descriptions of object borders in image field because of simplicity of the data representation and fast computational time. This research uses 8-neighbourhood in FCC generation of signature images as shown in Figure 5.

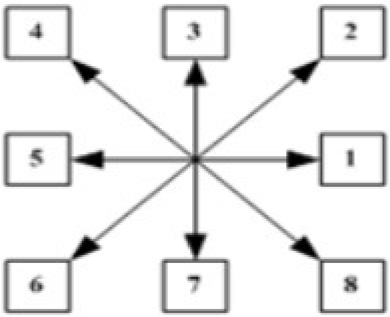

FIGURE 5: 8-Neighbourhood FCC Direction [51].

Freeman Chain Code (FCC) will be generated using randomized-based algorithm that generated the shortest computation time [51]. The randomized-based algorithm is an algorithm that makes random route choices. The advantage of randomized algorithm is the one that comes with a very high probability of correct computed results. Randomized-based algorithm is one of Heuristic technique. Heuristic technique is an optimization problem that is focused on space and time needed. Time is referred to the computational time of the program running while space is referred to the amount of computer memory needed during the program execution. A certain amount of time and space are needed to solve the computation of complexity theory [51].

The desire output is the FCC generation which is in forms of FCC length and computation time needed during generating the FCC. The first node to start the chain code tracing is randomly select. There are two possibilities, either by "node method" or "end node method". The former is to find any node based on its position at each "corner" whereas left upper, right upper, left lower and right lower. The selection of the shortest route length from the list of FCC is by selecting the chain code string with the minimum route length. If there are many minimums of route length found, the string is chose by the first time it found in the list [51].The only difference in this research is only largest contiguous pixel block of a signature image is considered in extracting the chain code because the problem will be occurred during execution since the signature image is not always in one word.

3.5 Feature Identification and Selection

Assembly of a feature vector is the target of feature identification as input for the verification phase. Sixty-nine features contained in a single vector is a combination of 2 feature parts: global features and features from character image FCC (8 FCC directional frequencies * FCC divisions).

There were three FCC directions will be tested which are 4, 8 and 16. The global features are:

(i) Signature Width (1 feature count). The signature image is scanned from left to right and measure the distance between two points in horizontal projection.

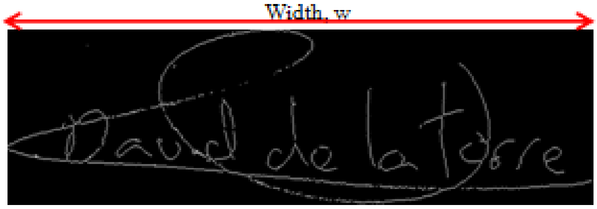

FIGURE 6: The value of width can be obtained by scanning from left to right of the image.

(ii) Signature Height (1 feature count). The signature image is scanned from top to bottom and measure the distance between two points in vertical projection.

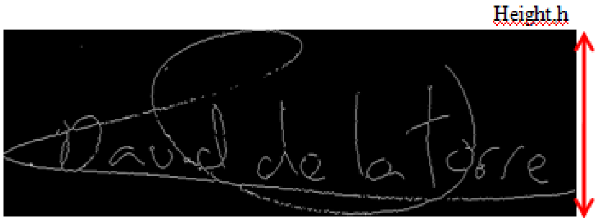

FIGURE 7: The value of height can be obtained by scanning from top to bottom of the image.

(iii) Aspect Ratio (1 feature count). It is the ratio of signature width to height. The calculation is shown in equation 1. Figure 3.5 shows a signature image with dimension.

$$Aspect\ Ratio = \frac{\text{Signature Width,w}}{\text{Signature Height,h}} \qquad (1)$$

(iv) Diagonal Distance (2 features count): The distance is measured from left to right diagonal distance of a cropped signature image which is top right to the bottom low and top left to the bottom right. Blue line is the diagonal line, ld. Refer Figure 8.

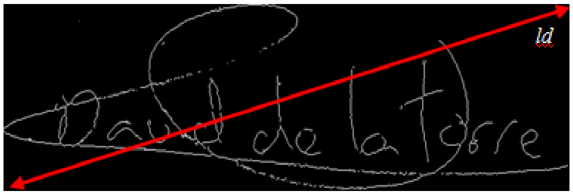

FIGURE 8: After the image was cropped, the values of left and right diagonal can be obtained.

(v) Centres of mass of all foreground pixels in an image (2 features count): is calculated for signature image by adding all x and y locations of foreground pixels and dividing it by number of pixel counted.

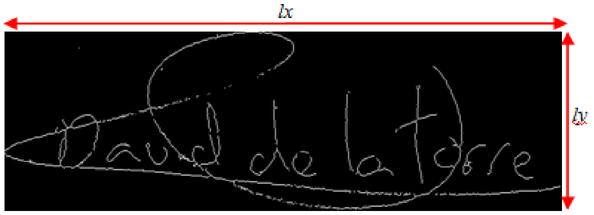

FIGURE 9: A signature image after pre-processing process.

Based on Figure 9, the equation to find the centres of mass for x and y locations:

$$x_{centre\ of\ mass} = \sum_{x=0}^{x=lx} x\, f(x) \quad (2)$$

$$y_{centre\ of\ mass} = \sum_{y=0}^{y=ly} y\, f(y) \quad (3)$$

(vi) Counting pixel value total shift per horizontal/vertical line. There are calculated by slicing the image horizontally into four parts and by summing shifts from black to white or white to black image. For vertical shifts, image is to be sliced vertically. This information is another unique property of signature because the chances of two signatures having exactly same shift numbers are very low.

$$Feature\ count = 4\ \text{lines}\ (2\ \text{directions}) = 8 \quad (4)$$

Feature vector formed from the MCYT signature database will be compiled to verification phase. Total of 32 features from FCC and 15 features from global features will be combined as one feature vector and verification input later.

3.6 Development of Verification Algorithm

Verification is the process of testing whether a claimed signature is the same writer (class) or not as the set of signatures trained in the system for that class. In our case, we have trained 12 genuine signatures and test 3 genuine and all 15 forgery signatures. Verification involved loading the template MATLAB file enrolled in the system and comparing its stored parameters. Nearest Neighbour (NN) classifier performs matching score calculation based on Euclidean distance [52]. Euclidean distance is one of the most favourite method for measuring the distance between vectors. The function has the following prototype:

results = nn_classification PhD(train, train_ids, test, test_ids, n, dist, match_kind);
Here train and test denote the training and testing feature vector matrices which are train_ids and test_ids. They stand for corresponding label vectors n represents the number of feature used in the calculations of Euclidean distance, dist ('euc') denoted the matching distance to use and match_kind ('all' (default)) represented a string identifier controlling the matching procedure. When a similarity matrix needs to be constructed, where all feature vectors from the training-feature-vector-matrix train are matched against all feature vectors in the test-feature-vector-matrix test. The similarity matrix generated by this option is stored in the results structure under results.matchdist. The structure can then be stored, where performance graphs and metrics are computed from the entire similarity matrix. The corresponding verification error rates are computed by pooling FRR data from the valid similarity matrix and FAR data from the forgery similarity matrix.

In identification process, the lowest distance between feature vector of input image and stored feature vectors is computed by using Euclidean distance and its related signature class is specified. In verification process for each signature class, a reference point is considered, if the distance between feature vector of input image and this reference point is less than a specific threshold, input image is a valid signature otherwise it is a forgery signature. A threshold value can be considered as a vector containing mean of corresponding elements of feature vectors of each class

3.7 Result Analysis and Validation

The performance quality is measured by FAR (False Acceptance Rate) and FRR (False Rejection Rate). FAR is the rate of accepting forgery signature as genuine signature wrongly. FRR is the rate of rejecting genuine signature as forgery one wrongly. FAR and FRR are related to each other inversely. By setting and changing a threshold, when FAR is increasing, FRR is decreasing. Equation 5 and 6 show the formulas of FAR and FRR.

$$FAR = \frac{Number\ of\ Falsely\ Accepted\ Images}{Total\ number\ of\ person\ in\ the\ database} \qquad (5)$$

$$FRR = \frac{Number\ of\ Falsely\ Rejected\ Images}{Total\ number\ of\ person\ in\ the\ database} \qquad (6)$$

In pre-processing stage, it provided "input base directory", that is sample image path for noise removal and thinning. "File extension" is used to search for other image extension. Current database sample uses file.bmp so this parameter can be ignored. The script searches recursively (all files and subdirectory) starting from its current location.

In feature extraction stage, it provided "input base directory", that is the signature image path. Output feature directory is set for output location. It is usually the same as pre-processing part in order to ensure all features to be located in same place.. Freeman Chain Code (FCC) extraction is done in this part.

In verification stage, it provided "input feature directory" which is one directory level up from intended location. The intended location name is put at "sample user number". This configuration is due to database having 75 folders with numbers labeling the sample. It also provided "output directory" to save trained parameters with its input/output data and result. The training is based on specific folder, not recursively as in previous two phases. Since there are 15 samples for both valid and forgery classes the data can be divided based on "data division" value. There are 12 valid signatures will be trained while the rest 3 valid signatures and all 15 forgery signatures will be tested.

3.8 Implementations

This section explains the equipment required in the implementation of the proposed framework. The requirements to develop the integrated system are classified into two parts: hardware and software. The hardware specification used in this research was a Asus Model s400c laptop with Intel ® Core ™ i5-3317U CPU @ 1.7 GHz, 4 Core(s) processor, 8GB RAM memory, 500 GB hard disk and Windows 8 64-bit operating system. MATLAB R2008a (version 7.6.0) is used as platform to write the code for pre-processing, FCC and feature extraction for nearest neighbour.

4. EXPERIMENTAL RESULT AND DISCUSSIONS

In this section, the result and some comparisons from previous work are highlighted. Table 4 and Table 5 show the results from both classifiers. Result from Nearest Neighbour classifier shows better result and faster computational time compare to result from ANN. In the other hand, Table 6 below shows comparison between our work and previous works.

Chain Code Division	4	8	16
FRR (%)	6.67	6.67	10.67
FAR (%)	12.44	12.44	12.00
Computational Time (s)	1.12	3.03	3.42

TABLE 4: Results from Nearest Neighbour based on Euclidean Distance.

Chain Code Division	4	8	16
FRR (%)	16.67	16.00	15.10
FAR (%)	20.22	21.60	20.90
Computational Time (s)	7.80	11.35	12.00

TABLE 5: Results from ANN.

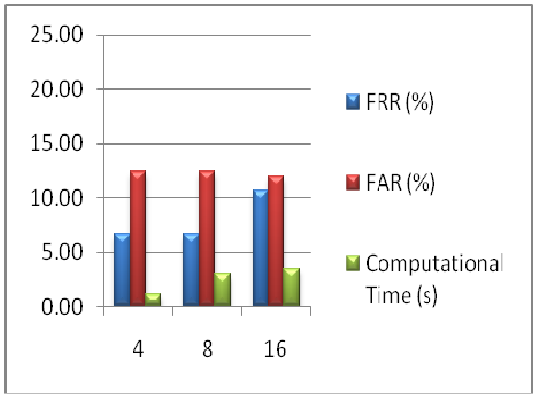

FIGURE 10: Trend chart results computed from Nearest Neighbour.

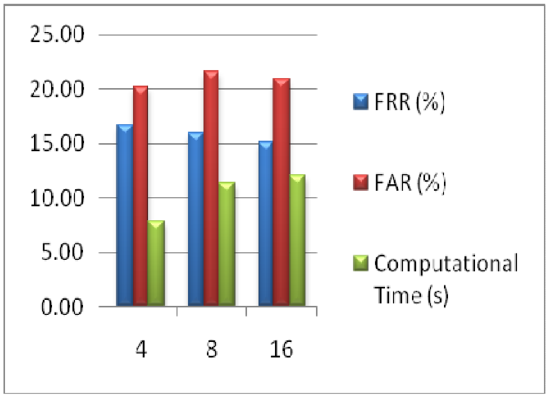

FIGURE 11: Trend chart results computed from ANN.

Authors	**Pre-processing**	**Feature Extraction**	**Classification**	**Performance**	**Dataset**
Our proposed system	Binarization, noise removal, cropping and thinning	FCC and global features	Euclidean Distance and Nearest Neighbour	FAR: 12.44% FRR:6.67%	MCYT
Pourshahabi	Colour inversion	Contourlet Transform	Euclidean Distance	FAR: 22.72% FRR:23.18%	Self-collected
Ghandali & Moghaddam (2008)	Binarization	Discrete Wavelet Transform (DWT)	Euclidean Distance	FAR: 8.5% FRR:11.1%	Self-collected
Moolla *et. al*, 2012	Binarization and thinning	Modified direction feature edge detection,	Modular neural network (MNN)	TSR: 89.2%	GPDS

		wavelet transform and Hough transform			
Ubul *et. al*, 2012	Noise reduction, binarization and normalization	Multi-dimensional modified grid information features	Euclidean Distance, K-Nearest Neighbor (KNN) and Bayesian Euclidean Distance	Accuracy: 86.45%	Self-collected

TABLE 6: Comparison between our work and previous works.

The database we used has 75 signers. As mentioned before, each signer has 15 valid signatures and 15 forgery signatures and total of signatures is 2250 images. In verification stage, the signatures will be divided to training and testing phases. Twelve images from each signer will be trained, three valid signatures and all fifteen forgery signatures will be tested. There are 180 valid signature from 75 signers will be trained and the rest are tested to yield the desire results.

Based on our systems, the lowest FRR achieved is 6.67% and lowest FAR is 12.44% with only 1.1178 second computational time from nearest neighbour classifier. Our results are satisfactory yet better than some previous works. Comparing with work from Moolla *et. al* [38], they are also used Euclidean distance with min FRR and FAR for skilled forgeries is 15.32% each. They investigated the use of a combination of multiple distance-based classification techniques, namely individually optimized re-sampling, weighted Euclidean distance, fractional distance and weighted fractional distance. In feature extraction stage, they are used directional features and modified directional features. Furthermore, Ghandali and Moghaddam [10] work was identifying and verifying handwritten signatures that were based on image registration Discrete Wavelete Transform (DWT) and image fusion. The classifier is based on Euclidean distance to obtain FAR 8.5% and FRR 11.1%. While in [4], they obtained 86.45% in Euclidean Distance (ED) classifier with extracted features that based on grid feature. Lastly, the work from [15] reported that they applied a special type of Contourlet transform on signature image and also related Contourlet coefficients are computed and feature vector is created. Euclidean distance is used as classifier. The results obtained for English signatures are FAR 22.72% and FRR 23.18%.

The algorithms and methods used in this system especially in feature extraction stage are simple and utilized less memory. There is no involving of complicated mathematic formula and easy to understand. This is the reason why the computational time became very short. A short computational time is important in this time for any security system when people are all in rush. Furthermore, in the context of number of features, our features are only 47. Compared to some previous works like in [4], the number of features was 120 which will need a lot of time and memory in classification stage. An optimum number of features is really important to make sure the system is working in an optimum efficiency. Based on our experiment, larger chain code division which leads to bigger number of features do not improved the error rate yet the computational time become longer that we need to avoid.

5. CONCLUSIONS AND FUTURE WORKS

This paper presents a signature verification system that used (FCC) as directional feature and data representation. There are 47 features were extracted from the signature images from six global features. Before extracting the features, the raw images were undergoing pre-processing stage which were binarization, noise removal by using media filter, cropping and thinning to produced Thinned Binary Image (TBI). Euclidean distance is measured and matched between nearest neighbours to find the result. MCYT-SignatureOff-75 database was used. Based on our systems, the lowest FRR achieved is 6.67% and lowest FAR is 12.44% with only 1.1178 second computational time.

In the future, we are planning to calculate the value of Equal Error Rate (EER) from the system. Besides, we are going to seek and explore new methods or algorithms for feature extraction to improve the results. Furthermore, we are planning to build a hybrid classifier to test the effect on error rate and accuracy of the system.

Acknowledgement This work is supported by the Universiti Teknologi Malaysia and Ministry of Education Malaysia with Research Grant (FRGS – 4F264). The authors would like to thanks Research Management Centre (RMC), Universiti Teknologi Malaysia (UTM) for the support in R & D, and Soft Computing Research Group (SCRG) for the inspiration in making this study success. The authors would also like to thank the anonymous reviewers who have contributed enormously to this work.

6. REFERENCES

[1] Al-Mayyan, Waheeda, Own, Hala S., & Zedan, Hussein. (2011). Rough set approach to online signature identification. *Digital Signal Processing, 21*(3), 477-485. doi: http://dx.doi.org/10.1016/j.dsp.2011.01.007.

[2] Ravi, J., Hosamani, S., & Raja, K. B. (2012, 26-28 July 2012). *Off-line Signature Identification Based on DWT and Spatial Domain Features.* Paper presented at the Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on Computing Communication & Networking Technologies.

[3] Ortega-Garcia, J., et al. (2003).: MCYT baseline corpus: A bimodal biometric database. IEEE Proceedings Vision, Image and Signal Processing 150(6).

[4] Ubul, K., Adler, A., Abliz, G., Yasheng, M., & Hamdulla, A. (2012, 2-5 July 2012). *Off-line Uyghur signature recognition based on modified grid information features.* Paper presented at the Information Science, Signal Processing and their Applications (ISSPA), 2012 11th International Conference on Information Science, Signal Processing and their Applications.

[5] Zhang, Zhaoxiang, Wang, Kaiyue, & Wang, Yunhong. (2011). A Survey of On-line Signature Verification. In Z. Sun, J. Lai, X. Chen & T. Tan (Eds.), *Biometric Recognition* (Vol. 7098, pp. 141-149): Springer Berlin Heidelberg.

[6] Zhan, Enqi, Guo, Jinxu, Zheng, Jianbin, Ma, Chan, & Wang, Linjuan. (2009, 15-16 May 2009). *On-line Handwritten Signature Verification Based on Two Levels Back Propagation Neural Network.* Paper presented at the Intelligent Ubiquitous Computing and Education, 2009 International Symposium on Intelligent Ubiquitous Computing and Education.

[7] Tomar, Minal, & Singh, Pratibha. (2011). An Intelligent Network for Offline Signature Verification Using Chain Code. In N. Meghanathan, B. Kaushik & D. Nagamalai (Eds.), *Advanced Computing* (Vol. 133, pp. 10-22): Springer Berlin Heidelberg.

[8] Cheng-Yaw, Low, Beng-Jin Teoh, A., & Connie, Tee. (2008, 3-5 June 2008). *Support Vector Machines (SVM)-based biometric watermarking for offline handwritten signature.* Paper presented at the Industrial Electronics and Applications, 2008. ICIEA 2008. 3rd IEEE Conference on Industrial Electronics and Applications.

[9] Oz, Cemil. (2005). Signature Recognition and Verification with Artificial Neural Network Using Moment Invariant Method. In J. Wang, X.-F. Liao & Z. Yi (Eds.), *Advances in Neural Networks – ISNN 2005* (Vol. 3497, pp. 195-202): Springer Berlin Heidelberg.

[10] Ghandali, S., & Moghaddam, M. E. (2008, 16-19 Dec. 2008). *A Method for Off-line Persian Signature Identification and Verification Using DWT and Image Fusion.* Paper presented at

the Signal Processing and Information Technology, 2008. ISSPIT 2008. IEEE International Symposium on Signal Processing and Information Technology.

[11] Porwik, P. (2007, 28-30 June 2007). *The Compact Three Stages Method of the Signature Recognition.* Paper presented at the Computer Information Systems and Industrial Management Applications, 2007. CISIM '07. 6th International Conference on Computer Information Systems and Industrial Management Applications.

[12] Pal, S., Alireza, A., Pal, U., & Blumenstein, M. (2011, 6-8 Dec. 2011). *Off-line Signature Identification Using Background and Foreground Information.* Paper presented at the Digital Image Computing Techniques and Applications (DICTA), 2011 International Conference on Digital Image Computing Techniques and Applications.

[13] Pal, S., Alireza, A., Pal, U., & Blumenstein, M. (2012, 4-7 Dec. 2012). *Multi-script off-line signature identification.* Paper presented at the Hybrid Intelligent Systems (HIS), 2012 12th International Conference on Hybrid Intelligent Systems.

[14] Pal, S., Pal, U., & Blumenstein, M. (2012, 10-15 June 2012). *Off-line English and Chinese signature identification using foreground and background features.* Paper presented at the Neural Networks (IJCNN), The 2012 International Joint Conference on Neural Networks.

[15] Pourshahabi, M. R., Sigari, M. H., & Pourreza, H. R. (2009, 4-7 Dec. 2009). *Offline Handwritten Signature Identification and Verification Using Contourlet Transform.* Paper presented at the Soft Computing and Pattern Recognition, 2009. SOCPAR '09. International Conference of Soft Computing and Pattern Recognition.

[16] Karouni, Ali, Daya, Bassam, & Bahlak, Samia. (2011). Offline signature recognition using neural networks approach. *Procedia Computer Science, 3*(0), 155-161. doi: http://dx.doi.org/10.1016/j.procs.2010.12.027.

[17] Lei, Liu, & Huichuan, Duan. (2009, 14-16 Aug. 2009). *The Research of handwritten signatures.* Paper presented at the IT in Medicine & Education, 2009. ITIME '09. IEEE International Symposium on IT in Medicine & Education.

[18] Biswas, Samit, Bhattacharyya, Debnath, Kim, Tai-hoon, & Bandyopadhyay, SamirKumar. (2010). Extraction of Features from Signature Image and Signature Verification Using Clustering Techniques. In T.-h. Kim, A. Stoica & R.-S. Chang (Eds.), *Security-Enriched Urban Computing and Smart Grid* (Vol. 78, pp. 493-503): Springer Berlin Heidelberg.

[19] Ning, Wang. (2009, 24-26 Nov. 2009). *Signature Identification Based on Pixel Distribution Probability and Mean Similarity Measure with Concentric Circle Segmentation.* Paper presented at the Computer Sciences and Convergence Information Technology, 2009. ICCIT '09. Fourth International Conference on Computer Sciences and Convergence Information Technology.

[20] Impedovo, Donato, & Pirlo, Giuseppe. (2011). Stability Analysis of Static Signatures for Automatic Signature Verification. In G. Maino & G. Foresti (Eds.), *Image Analysis and Processing – ICIAP 2011* (Vol. 6979, pp. 241-247): Springer Berlin Heidelberg.

[21] Munich, M. E., & Perona, P. (2003). Visual identification by signature tracking. *Pattern Analysis and Machine Intelligence, IEEE Transactions on, 25*(2), 200-217. doi: 10.1109/TPAMI.2003.1177152.

[22] Deng, P. S., Li-Jing, Jaw, Jau-Hwang, Wang, & Cheng-Tan, Tung. (2003, 14-16 Oct. 2003). *Trace copy forgery detection for handwritten signature verification.* Paper presented at the Security Technology, 2003. Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on Security Technology.

[23] Fahmy, Maged M. M. (2010). Online handwritten signature verification system based on DWT features extraction and neural network classification. *Ain Shams Engineering Journal, 1*(1), 59-70. doi: http://dx.doi.org/10.1016/j.asej.2010.09.007.

[24] Pottier, I., & Burel, G. (1994, 27 Jun-2 Jul 1994). *Identification and authentification of handwritten signatures with a connectionist approach.* Paper presented at the Neural Networks, 1994. IEEE World Congress on Computational Intelligence., 1994 IEEE International Conference on Neural Networks.

[25] Soleymanpour, E., Rajae, B., & Pourreza, H. R. (2010, 27-28 Oct. 2010). *Offline handwritten signature identification and verification using contourlet transform and Support Vector Machine.* Paper presented at the Machine Vision and Image Processing (MVIP), 2010 6th Iranian.

[26] Abushariah, A. A. M., Gunawan, T. S., Chebil, J., & Abushariah, M. A. M. (2012, 3-5 July 2012). *Automatic person identification system using handwritten signatures.* Paper presented at the Computer and Communication Engineering (ICCCE), 2012 International Conference on Computer and Communication Engineering.

[27] Pranckeviciene, Erinija, Somorjai, Ray, Baumgartner, Richard, & Jeon, Moon-Gu. (2005). Identification of signatures in biomedical spectra using domain knowledge. *Artificial Intelligence in Medicine, 35*(3), 215-226. doi: http://dx.doi.org/10.1016/j.artmed.2004.12.002.

[28] Akram, M., Qasim, R., & Amin, M. A. (2012, 18-19 May 2012). *A comparative study of signature recognition problem using statistical features and artificial neural networks.* Paper presented at the Informatics, Electronics & Vision (ICIEV), 2012 International Conference on Informatics, Electronics & Vision.

[29] Angadi, S. A., & Gour, Smita. (2013). LVQ-Neural Network Based Signature Recognition System Using Wavelet Features. In M. S & S. S. Kumar (Eds.), *Proceedings of the Fourth International Conference on Signal and Image Processing 2012 (ICSIP 2012)* (Vol. 222, pp. 1-13): Springer India.

[30] Bandyopadhyay, S. K., Bhattacharyya, D., Das, P., & Debnath, D. (2008, 24-26 April 2008). *Handwritten Signature Authentication Using Statistical Estimation.* Paper presented at the Multimedia and Ubiquitous Engineering, 2008. MUE 2008. International Conference on Multimedia and Ubiquitous Engineering.

[31] Bhattacharya, Indrajit, Ghosh, Prabir, & Biswas, Swarup. (2013). Offline Signature Verification Using Pixel Matching Technique. *Procedia Technology, 10*(0), 970-977. doi: http://dx.doi.org/10.1016/j.protcy.2013.12.445.

[32] De Medeiros Napoles, S. H. L., & Zanchettin, C. (2012, 10-15 June 2012). *Offline handwritten signature verification through network radial basis functions optimized by Differential Evolution.* Paper presented at the Neural Networks (IJCNN), The 2012 International Joint Conference on Neural Networks.

[33] Dhar, K., & Kunz, A. (1988, 5-7 Oct 1988). *Digital technique to analyze handwritten signatures.* Paper presented at the Security Technology, 1988. Crime Countermeasures, Proceedings. Institute of Electrical and Electronics Engineers 1988 International Carnahan Conference on Security Technology.

[34] Doroz, Rafal, & Porwik, Piotr. (2011). Handwritten Signature Recognition with Adaptive Selection of Behavioral Features. In N. Chaki & A. Cortesi (Eds.), *Computer Information Systems – Analysis and Technologies* (Vol. 245, pp. 128-136): Springer Berlin Heidelberg.

[35] Doroz, Rafal, & Wrobel, Krzysztof. (2012). Dynamic Signature Recognition Based on Modified Windows Technique. In A. Cortesi, N. Chaki, K. Saeed & S. Wierzchoń (Eds.), *Computer Information Systems and Industrial Management* (Vol. 7564, pp. 158-167): Springer Berlin Heidelberg.

[36] Melin, Patricia. (2012). Signature Recognition with a Hybrid Approach Combining Modular Neural Networks and Fuzzy Logic for Response Integration *Modular Neural Networks and Type-2 Fuzzy Systems for Pattern Recognition* (Vol. 389, pp. 77-92): Springer Berlin Heidelberg.

[37] Palys, Malgorzata, Doroz, Rafal, & Porwik, Piotr. (2013). Statistical Analysis in Signature Recognition System Based on Levenshtein Distance. In R. Burduk, K. Jackowski, M. Kurzynski, M. Wozniak & A. Zolnierek (Eds.), *Proceedings of the 8th International Conference on Computer Recognition Systems CORES 2013* (Vol. 226, pp. 217-226): Springer International Publishing.

[38] Moolla, Y., Viriri, S., Nelwamondo, F. V., & Tapamo, J. R. (2012, 12-15 Aug. 2012). *Handwritten signature verification using weighted fractional distance classification.* Paper presented at the Signal Processing, Communication and Computing (ICSPCC), 2012 IEEE International Conference on Signal Processing, Communication and Computing.

[39] Potolea, Rodica, Bărbănţan, Ioana, & Lemnaru, Camelia. (2011). A Hierarchical Approach for the Offline Handwritten Signature Recognition. In J. Filipe & J. Cordeiro (Eds.), *Enterprise Information Systems* (Vol. 73, pp. 264-279): Springer Berlin Heidelberg.

[40] Rivard, Dominique, Granger, Eric, & Sabourin, Robert. (2013). Multi-feature extraction and selection in writer-independent off-line signature verification. *International Journal on Document Analysis and Recognition (IJDAR), 16*(1), 83-103. doi: 10.1007/s10032-011-0180-6.

[41] Jayadevan, R., Kolhe, S. R., Patil, P. M., & Pal, U. (2012). Automatic processing of handwritten bank cheque images: a survey. *International Journal on Document Analysis and Recognition (IJDAR), 15*(4), 267-296. doi: 10.1007/s10032-011-0170-8.

[42] Heinen, M. R., & Osorio, F. S. (2006, 0-0 0). *Handwritten Signature Authentication using Artificial Neural Networks.* Paper presented at the Neural Networks, 2006. IJCNN '06. International Joint Conference on Neural Networks.

[43] Shashi Kumar, D. R., Ravi Kumar, R., Raja, K. B., Chhotaray, R. K., & Pattanaik, Sabyasachi. (2010). Combined Off-Line Signature Verification Using Neural Networks. In V. Das & R. Vijaykumar (Eds.), *Information and Communication Technologies* (Vol. 101, pp. 580-583): Springer Berlin Heidelberg.

[44] Mendaza-Ormaza, A., Miguel-Hurtado, O., Blanco-Gonzalo, R., & Diez-Jimeno, F. (2011, 18-21 Oct. 2011). *Analysis of handwritten signature performances using mobile devices.* Paper presented at the Security Technology (ICCST), 2011 IEEE International Carnahan Conference on Security Technology.

[45] Ribeiro, Bernardete, Gonçalves, Ivo, Santos, Sérgio, & Kovacec, Alexander. (2011). Deep Learning Networks for Off-Line Handwritten Signature Recognition. In C. San Martin & S.-W. Kim (Eds.), *Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications* (Vol. 7042, pp. 523-532): Springer Berlin Heidelberg.

[46] Batista, Luana, Granger, Eric, & Sabourin, Robert. (2010). A Multi-Classifier System for Off-Line Signature Verification Based on Dissimilarity Representation. In N. Gayar, J. Kittler & F. Roli (Eds.), *Multiple Classifier Systems* (Vol. 5997, pp. 264-273): Springer Berlin Heidelberg.

[47] Paulik, M. J., & Mohankrishnan, N. (1993, 16-18 Aug 1993). *A 1-D, sequence decomposition based, autoregressive hidden Markov model for dynamic signature identification and verification.* Paper presented at the Circuits and Systems, 1993, Proceedings of the 36th Midwest Symposium on Circuits and Systems.

[48] Wada, N., & Hangai, S. (2007, 7-8 June 2007). *HMM Based Signature Identification System Robust to Changes of Signatures with Time.* Paper presented at the Automatic Identification Advanced Technologies, 2007 IEEE Workshop on Automatic Identification Advanced Technologies.

[49] Putz-Leszczynska, Joanna, & Pacut, Andrzej. (2013). Universal Forgery Features Idea: A Solution for User–Adjusted Threshold in Signature Verification. In N. Nguyen (Ed.), *Transactions on Computational Collective Intelligence IX* (Vol. 7770, pp. 152-172): Springer Berlin Heidelberg.

[50] Srinivasan, D., Ng, W. S., & Liew, A. C. (2006). Neural-network-based signature recognition for harmonic source identification. *Power Delivery, IEEE Transactions on, 21*(1), 398-405. doi: 10.1109/TPWRD.2005.852370.

[51] Nasien, Dewi (2012). Feature Extraction and Selection Algorithm for Chain Code Representation of Handwritten Character. Ph. D Thesis. Universiti Teknologi Malaysia, Malaysia.

[52] Štruc V., Pavešic, N.: The Complete Gabor-Fisher Classifier for Robust Face Recognition, EURASIP Advances in Signal Processing, vol. 2010, 26 pages, doi:10.1155/2010/847680, 2010.