Multimed Tools Appl (2017) 76:15341–15355
DOI 10.1007/s11042-016-3831-2

Biometric signature verification system based on freeman chain code and k-nearest neighbor

Aini Najwa Azmi[1] · **Dewi Nasien**[1] · **Fakhrul Syakirin Omar**[1]

Received: 11 November 2015 / Revised: 5 June 2016 / Accepted: 2 August 2016 /
Published online: 19 September 2016

Abstract Signature is one of human biometrics that may change due to some factors, for example age, mood and environment, which means two signatures from a person cannot perfectly matching each other. A Signature Verification System (SVS) is a solution for such situation. The system can be decomposed into three stages: data acquisition and preprocessing, feature extraction and verification. This paper presents techniques for SVS that uses Freeman chain code (FCC) as data representation. Before extracting the features, the raw images will undergo preprocessing stage; binarization, noise removal, cropping and thinning. In the first part of feature extraction stage, the FCC was extracted by using boundary-based style on the largest contiguous part of the signature images. The extracted FCC was divided into four, eight or sixteen equal parts. In the second part of feature extraction, six global features were calculated against split image to test the feature efficiency. Finally, verification utilized Euclidean distance to measured and matched in k-Nearest Neighbors. MCYT bimodal database was used in every stage in the system. Based on the experimental results, the lowest error rate for FRR and FAR were 6.67 % and 12.44 % with AER 9.85 % which is better in term of performance compared to other works using that same database.

Keywords Offline signature verification system · Preprocessing · Feature extraction · Freeman chain code · Euclidean distance

✉ Aini Najwa Azmi
ainajwa.azmi@gmail.com

✉ Dewi Nasien
dewinasien@utm.my

✉ Fakhrul Syakirin Omar
fsyakirin2@live.utm.my

[1] Department of Computer Science, Faculty of Computing, Universiti Teknologi Malaysia, Skudai, 81310 Johor Bahru, Johor, Malaysia

1 Introduction

Biometrics verification is a subject on the identification and verification of humans by their characteristics or traits. Biometrics is widely utilized in computer science as a form of access control and identification. Signature Verification System (SVS) is a system that identifies and verifies a handwritten signature whether it is genuine or forgeries. Similar to other human biometrics, the system compares the signature information with all the images stored in the database [2]. Usually, it can be done by comparing one-to-one process that includes data acquisition and preprocessing, feature extraction and verification. 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 besides DNA, fingerprint, palm print, face, vein pattern, retina and iris. These physiological traits are almost unchanged throughout a person's life, unlike signature that 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 verification 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. A series of signatures means a same person will sign several times and the signature will be kept as reference. In the series, many characteristic must remain constant to determine the confidence level, measured in accuracy.

SVS can be classified to static (offline) and dynamic (online). In an offline system, user writes their signature on a paper and is digitized using a scanner or a camera. The SVS recognizes the signature by analyzing its shape or static features. On the other hand, an online system needs a user to write their signature on a digitizing tablet, that records the signature in real time form. Another possibility is the acquisition via smart phone, tablet or stylus-operated PDAs. An online system can record dynamic features of the signature that make it difficult to forge. An online system is appropriate to use in real-time applications, such as financial transactions, document authenticity and office automation [2]. This paper is focusing on offline system only.

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; the forger does not even know how the signature looks like. The second one is random forgery that the forger uses his/her own signature as a forgery signature. The last one is skilled forgery that the forger practices and tries to copy or duplicate the genuine signature as close as possible. The problem that is addressed in this paper is regarding the latter. Handwritten is different as compared to signature, where a signature must be treated as an image because people may use symbol, letter or group of letters in their signatures, which implies that the name of the writer is not evident when looking at the signature.

As it is clear that signature is not a rigid biometric of a human being and easy to be forged, every process in every stage play important role to build a robust system. Generally, SVS can be decomposed into three major stages: data acquisition and preprocessing, feature extraction and verification. 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, for example in varying color, gray level, or binary format [7]. MCYT Bimodal Offline Signature database will be used in the entire stages. There are 75 users in this database, each having 15 genuine signatures and 15 forgery signatures [17].

In preprocessing, the image will be in binary values. Noise removal will be applied to the signature images before cropping. Finally, thinning algorithm is used to remove all redundancy by eliminating excess foreground pixels. In converting raw binary image to thinned binary image (TBI), thinning function in Image Processing Toolbox in MATLAB software is used. As the first important stage, image and data preprocessing performs the purpose of extracting regions of interest, enhancing and cleaning up the images, so that they can be directly and efficiently processed by the feature extraction component in the next stage [7].

In image processing, feature extraction is a special form of dimensionality reduction. When the input data to an algorithm is too large to be processed and it is suspected to be redundant, it will be transformed into a simplified representation set of feature vector by carefully choosing relevant information from the input data. In order to perform this important task, Freeman chain code (FCC) will be used, constructed using boundary based style.

Lastly, k-NN will be used as classifier, chosen because this classifier is performing excellently in pattern recognition system [1, 19]. The first one, k-NN, has been proven to perform well in previous researches and the generalization is in the given distance measure. Almost all verifiers depend, in one way or the other, on a given distance measure. K-NN is advantageous in that it reflects the human decision making because it is only based on the distance measure designed by the researcher [26]. K-NN also does not involve a lot of parameters like other verifiers. The performance quality is measured by error rates such as FAR (False Acceptance Rate) and FRR (False Rejection Rate), and AER (Average Error Rate).

2 Literature review

In this section, we listed and analyzed related works in data acquisition and preprocessing, feature extraction and verification from various offline systems.

2.1 Data acquisition and preprocessing

Data acquisition for online and offline systems are totally different. In online system, signatures can be captured using a variety of input devices like specially designed pens, hand gloves, special tablets, personal digital assistant (PDA) and tracking-camera [2, 28]. The tablet can gather the pen X and Y coordinate sequences, total signing duration, number of pen-ups, strokes count and the pressure value of the pen. These 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 [2], called dynamic information that can be considered as features for next stage. In the other hand, in an offline system, signatures are optically captured by using a scanner and the completed signatures are available as images [9]. As a scanned signature contains a lot of noise, it must be preprocessed to produce a clean image as preparation prior to feature extraction.

Pre-processing is an important task in SVS especially for an offline system. The purpose of this task is to prepare a standard image for the feature extraction stage [18]. Since signature images for an offline system are always scanned using a flatbed scanner, the images contain a

lot of noise such as "salt-and-pepper" noise [5]. As can be seen in Table 2.1, there are more pre-processing methods found for offline systems in previous research. The most popular method used is filtering and noise removal. The Gaussian filter is always used for noise removal. Since the Gaussian function is symmetric, smoothing is performed equally in all directions, and the edges in an image will not bias towards a particular direction [13]. Furthermore, thinning and skeletonization are used to minimize or reduce the computational time required by the verifier. Thinning and skeletonization are the processes to remove the thickness of a signature image to one-pixel thick [13]. In addition, segmentation of the outer traces is done because the signature boundary normally corresponds to flourish, which has high intra-user variability, whereas normalization of the image size is aimed to make the proportions of different realizations of an individual equal [3]. On the other hand, images in an online system contains less or zero noise, so less effort is needed for the pre-processing of the online system.

2.2 Feature extraction

The feature extraction techniques used in the offline signature verification systems discussed above have some limitations that make it difficult for them to detect skilled forgeries effectively. Therefore, many of the previous techniques were only meant to detect simple and random forgeries [24]. Each of us exhibits specific physiological and behavioural characteristics. These characteristics can be used to identify an individual based on the feature vectors extracted from the biometric data using a pattern-recognition system [20]. When the acquired biometric data is sent to the feature extraction module and processed, a set of salient features are extracted and computed into vectors [12]. In a fingerprint image, these features can be the position and orientation of minutiae points which forms the local ridge and valley singularities of the image [12]. One of the techniques used is the feature fusion where feature vectors of different biometric indicators with similar measurement scale are concatenated into a high-dimensional resultant feature. The new feature vector is postulated to carry more discriminative power for the biometric identification process [12].

A powerful feature extraction module must also be equipped with feature reduction techniques where the module is capable of extracting the most salient features from a large set of features. Researchers have proposed different techniques to identify the salient features of human signature. In a heuristic-based analysis introduced by [15], the human signature is represented as the simulation of a series of elements. The grey-level comparison technique had been proposed to solve problems in the static signature verification approach involving tracing forgeries [23]. The slope histogram has also been used to represent signature samples [10]. The constant properties of curvature, total length, and slant angle of signatures observed in different samples could help isolate forged signatures.

On the other hand, the dynamic signature verification approach makes use of the largely available signals generated by the movement of the pen tip [14]. These signals are functions of time, carrying information such as x-y coordinates, speed, and pressure. The extensive possible solutions from this approach have encouraged researchers to design data processing technique solely for the acquisition stage [14]. In 1989, Baron and Plamondon analyzed the acceleration signal of hand-pen movements acquired from an accelerometer pen [6, 27]. A segmentation technique that locally compares a segmented part of the signature to reference signatures, leaving the optimal set of segmentation points was proposed by [8]. The elimination of global comparisons reduces processing time and allows the extraction of local features that are essential for signature verification.

Signature authenticity is crucial in any legal, financial, and professional practices. Ongoing research to improve the techniques and approaches in signature verification is essential in order to overcome and solve problems involving signature forgeries.

2.3 Verification

Verification is a crucial stage in every verification system. Common verification techniques used in both offline and online systems are Artificial Neural Network (ANN), k-Nearest Neighbour (k-NN), Support Vector Machine (SVM), and Hidden Markov Model (HMM). The reasons ANN is always used in the verification stage are that it can be trained to recognize signatures and its characteristics are such that it could be used to classify signatures as genuine or forged as a function of time through a retraining process based on recent signatures. But there is a primary disadvantage where a large number of samples are needed to ensure that the network does actually learn ([14]. Most researchers used large, standard database of signatures to ensure sufficient information for the learning stage of verification. The advancement of signature verification approaches since 1989 has promoted the application of neural networks into identity verification systems [11]. One essential capacity of neural networks is the training ability to learn. Not only can the system learn to recognize signatures and perform class separation, the system can also, through retraining process, classify signatures based on the authenticity as a function of time [14]. There are successfully trained neural networks that can identify pressure, horizontal speed, and vertical speed as a function of time.

However, in order to properly learn, the neural networks require a large number of samples for the training process. Samples of forged signatures must be introduced during the training phase. These samples are not easily available, thus making the classification of forgers much harder to define. This problem attributes to the major concern of developers. In attempting to solve this problem, some researchers proposed the use of networks designated for one class of signers while other suggested the use of random or computer-generated forgeries of the genuine signatures.

Another machine learning technique that may be similar to neural networks is the K-NN model. Despite the simplicity of the model, it employs the strategy of using the distance measure designed by the researcher, thus closely mimicking the human decision making [26]. Moreover, unlike other verifiers, the K-NN does not require a large number of parameters. However, neural networks does have the capacity to become a more powerful tool since the technique allows learning of complex nonlinear input-output relationships, application of sequential training procedures, and has data adaptation ability [25].

3 Research methodology

Figure 1 shows the research framework of this paper. In Stage 1, problem background is analyzed where three problems were identified. The first one is related to entire SVS. As signature is a type of biometric that may change with mood, environment and age, some solutions for this problem are defined. A good signature database must be updated in a few specific times so that the database is relevant to be used from time to time. Besides, a person must sign in a consistent manner to construct a series of signatures that are almost similar between each other. The second problem relates to FCC generation that failed to extract from

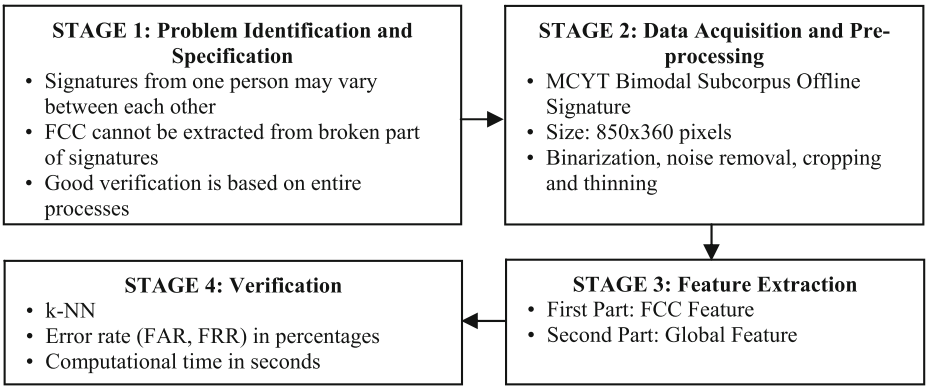

Fig. 1 The research framework

broken parts of signature. Thus, only the largest contiguous part of the signature is chosen to extract the FCC. The third problem related to verification in order to achieve a good result. Earlier processes, namely preprocessing and feature extraction, must work efficiently to achieve the desired results from k-NN.

In Stage 2, an offline signature database which is known as MCYT Bimodal Subcorpus Offline Signature [17] has been selected for use. There are 75 individual, each having 15 genuine and 15 highly skilled forgery signature samples, totaling to 2250 signatures for entire database. This database will be used in the entire stage of this paper. In preprocessing, 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 outer parts of an image to improve framing, accentuating the subject matter. This is important in aspect ratio calculation in feature extraction stage. Finally, thinning algorithm is used to remove redundancies by eliminating redundant foreground pixels. In process of converting raw binary image to TBI, thinning function in Image Processing Toolbox in MATLAB software is used [16]. The signature images received are all in equal size, 850 × 360 pixels. In this stage, resizing is not required since the size is not big; the size is acceptable in the preprocessing, feature extraction and verification stage.

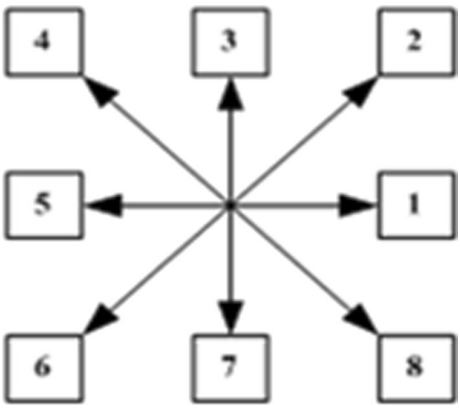

Fig. 2 8-Neighbourhood FCC Direction

```
1. Initialize data
2. Locating starting node (scan image from left to right and top to
   bottom to find the first node)
3. Follow outermost border of the image
4. Stop until the tracer reaches the starting node again
```

Fig. 3 Pseudo-code of applied boundary-basedon Freeman Chain Code (FCC)

In Stage 3, there are two parts of feature extraction involved in this research. The first part is regarding to FCC feature. Chain code representation describes the outline for signature image by recording the direction of where is the location of the next pixel and corresponds to the neighborhood in the image. 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, as shown in Fig. 2. In order to extract FCC, a boundary-based style is used to minimize chain code length and it is only applied on largest contiguous part of the signature due to inability of FCC to be extracted from broken parts of signature.

Figure 3 shows the pseudo-code of FCC extraction in boundary-based style. This thesis proposed three types of chain code divisions. They are divided to four, eight and sixteen division for training and testing in verification stage later. For every chain code division, appearance frequency is calculated to become the directional feature. The number of features is counted with formulas in Eq. 1, 2 and 3:

$$\text{Feature count} = 4 \text{ division} * 8 \text{ directional code frequency} = 32 \tag{1}$$

$$\text{Feature count} = 8 \text{ division} * 8 \text{ directional code frequency} = 64 \tag{2}$$

$$\text{Feature count} = 16 \text{ division} * 8 \text{ directional code frequency} = 128 \tag{3}$$

On the other hand, the global features are listed below and the feature count is for unsplit image.

1) *Signature Width*: The signature image is scanned from left to right and the distance between two points in horizontal projection is measured. This will produce one feature.
2) *Signature Height*: The signature image is scanned from top to bottom and the distance between two points in vertical projection is measured. This will produce one feature.

3) *Aspect Ratio*: Ratio of signature width to height. The calculation is shown in Eq. 4. This will produce one feature.

$$\text{Aspect Ratio} = \frac{\text{Signature Width}-w}{\text{Signature Height}-h} \tag{4}$$

4) *Diagonal Distance*: 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. This will produce two features.

5) *Centres of mass of all foreground pixels in an image*: is calculated for signature image by adding all x and y locations of foreground pixels and dividing it by number of pixel counted. This will produce two features. Eqs. 5 and 6 are equations to find the centres of mass for x and y locations:

$$x_{\text{centre of mass}} = \sum_{x=0}^{x=lx} x\, f(x) \tag{5}$$

$$y_{\text{centre of mass}} = \sum_{y=0}^{y=ly} y\, f(y) \tag{6}$$

6) *Counting pixel value total shift per horizontal/vertical line*: They 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 is counted as Eq. 7.

$$\text{Feature count} = 4\ \text{lines}*(2\ \text{directions}) = 8 \tag{7}$$

Besides of applying the global features to the normal TBI, the features are calculated to split TBI too. Based on Figs. 4 and 5, the image is split horizontally and vertically in order to test the efficiency of global feature. There are three sets of global feature produced which contain 15 features (original image), 60 features (one time split) and 240 features (two time splits).

As summary, after combining two parts of feature extractions, there are 9 possible sets of feature vector with combination of three set from part one and three set from part two. Table 1 shows the feature vector calculation.

Finally in Stage 4, verification is the process of testing whether a signature is the same writer or not. In our case, we have trained 12 signatures from each genuine and forgery classes and tested 3 signatures also from each class. k-NN classifier performs matching score calculation based on Euclidean distance, one of the most favorite methods for measuring the distance between vectors. The performance quality is measured by FAR and FRR and AER. By setting and changing threshold value, when FAR is increasing, FRR is decreasing. Eq. 8 and 9 shows the formulas for FAR and FRR. See Eqs. 8 until 10 for the formulas.

$$FAR = \frac{\text{Number of Falsely Accepted Images}}{\text{Total number of person in the database}} \tag{8}$$

$$FRR = \frac{\text{Number of Falsely Rejected Images}}{\text{Total number of person in the database}} \tag{9}$$

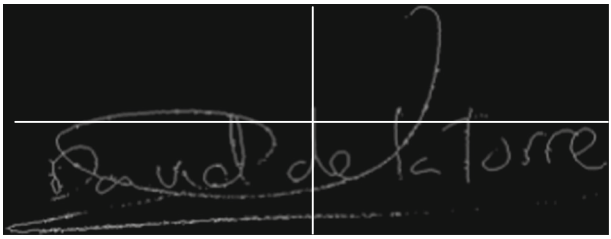

Fig. 4 Split signature image (one time split)

$$AER = \frac{FAR + FRR}{2} \tag{10}$$

4 Experimental results

In verification 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 genuine signature, otherwise it is a forgery signature. A threshold value can be considered as a vector containing mean of corresponding elements of feature vectors in each class. The result of k-NN is as shown in Table 2. For higher chain code division, the computational time consumed is higher due to increasing number of features. The lowest FRR, 6.67 %, is obtained from four chain code division for unsplit image, while the lowest FAR is from sixteen chain code division which is 12 %. But, the overall result from chain code division four is the best compared to two others with lowest computational time.

The experimental results of the present study are satisfactory, and in some cases better, when compared to the previous works that are listed in Table 3. The link between this study and those previous works is the database utilized, which is the MCYT Bimodal Offline Signature database.

An approach based on relative orientations of geometric centroids of split portions of signatures was proposed [21]. The centroid orientation features of offline signatures were used to form an interval-valued symbolic feature vector for representing the signatures. They

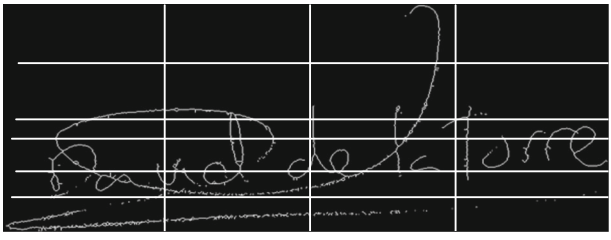

Fig. 5 Split signature image (two times split)

Table 1 Feature vector calculation

CC Division	4 * 8 directional code frequency = 32 features		
Image Splitting (Times)	None (15 features)	1 (60 features)	2 (240 features)
Number of features	47	92	272
CC Division	8 * 8 directional code frequency = 64 features		
Image Splitting (Times)	None (15 features)	1 (60 features)	2 (240 features)
Number of features	79	124	304
CC Division	16 * 8 directional code frequency = 128 features		
Image Splitting (Times)	None (15 features)	1 (60 features)	2 (240 features)
Number of features	143	188	368

also investigated the feasibility of the proposed representation scheme for signature verification.

Using the same signature database, Prakash and Guru extended their work by using k-NN and obtained the FRR of 14.85 % and FAR of 19.82 % [22]. This time, they proposed signature verification based on the score level fusion of distance and orientation features of centroids of the signatures. They also presented a method that employed symbolic representation of offline signatures using bi-interval-valued feature vector.

A different method for verifying handwritten signatures using Mahalanobis distance was presented by [3]. They presented two automatic measures for predicting the performance in the offline signature verification. The area of the signature slants of different directions and the intra-variability of the set of signatures were measured.

Table 2 Result of k-NN

CC Division	4		
Image Splitting (Times)	None	1	2
FRR (%)	6.67	9.78	17.56
FAR (%)	12.44	16.89	13.11
AER (%)	9.56	13.36	15.36
CC Division	**8**		
Image Splitting (Times)	None	1	2
FRR (%)	6.67	9.78	18.22
FAR (%)	12.44	17.11	12.89
AER (%)	9.56	13.45	15.56
CC Division	**16**		
Image Splitting (Times)	None	1	2
FRR (%)	10.67	9.78	17.78
FAR (%)	12.00	16.89	13.11
AER (%)	11.36	13.36	15.45

Table 3 Comparison between proposed work and previous works

Authors	Preprocessing	Feature Extraction	Classification	Performance	Dataset
[21]	Binarization	Symbolic representation	k- Nearest Neighbour	FAR:14.66 % FRR:25.11 % AER: 19.89 %	MCYT
[22]	Binarization	Distance and orientation feature	k- Nearest Neighbor	FAR:19.82 % FRR:14.85 % AER: 17.36 %	MCYT
[3]	Binarization, segmentation, and normalization	Slant direction measurement	Mahalanobis Distance	FAR: 38.40 % FRR:38.13 % AER: 38.27 %	MCYT
[4]	Binarization, segmentation, and normalization	Local Image Analysis	HMM	FAR: 22.04 % FRR: 22.93 % AER: 22.46 %	MCYT
Proposed system	Binarization, noise removal, cropping and thinning	FCC and global features	Euclidean distance and Nearest Neighbor	FAR: 12.44 % FRR:6.67 % AER: 9.56 %	MCYT

From the proposed variability measure, they found that with more signatures in the enrolment set, less variability is desirable.

Furthermore, proposed another work based on two machine experts was proposed by [4]. One was based on global image analysis and statistical distance measures, and the second one was based on local image analysis and Hidden Markov Models. They evaluated the impact of signature legibility and signature type on the recognition rates of an offline SVS. The best results were repeatedly obtained for legible cases, whereas the non-legible cases resulted in no significant improvement or even poorer performance.

5 Conclusion and discussion

This paper presents a SVS that uses FCC as directional feature and data representation. Among nine sets of feature vector, the best results came from 47 features, where 32 features were extracted from the FCC and 15 feature features from global features. Before extracting the features, the raw images went through preprocessing stage which includes binarization, noise removal, cropping and thinning to produce TBI. Euclidean distance is measured and matched between nearest neighbors to find the result. MCYT Bimodal Sub-corpus database was used. Based on our systems, lowest FRR achieved was 6.67 %, lowest FAR was 12.44 % and AER was 9.56 %.

The algorithms and methods used in this system, especially in feature extraction stage, are simple and utilizes less memory. There is no involvement of complicated mathematical formula and easy to understand. This is the reason why the computational time can be very short. A short computational time is important in this time for any security system when people are all in rush. An optimum number of features are really important to make sure the system is working in an optimum efficiency. Based on our experiment, while the increasing of chain code division will produce bigger number of features, there is no improvement for the error rate. Even worse, the computational time becomes longer.

There are a lot of methods or techniques in developing an SVS have been done by researchers nowadays. Pre-processing is one of the important stages that need to be studied. In this paper, there are four pre-processing techniques are involved which are binarization, noise removal, cropping and thinning. In the future, the slant and the skew of the signatures can be corrected. In extracting the FCC, only boundary-based style is used to generate the chain code. Some of old and new meta-heuristic techniques can be experimented in order to search the best and shortest route using other FCC extraction styles. Examples of meta-heuristic techniques are Firefly Algorithm, Cuckoo Search, Harmony Search and Hybridization of Meta-heuristics. Besides, there are so many new techniques of feature extraction can be experimented. The examples are Gabor Filter, Scale Invariant Feature Transform (SIFT), Principal Component Analysis (PCA), Kernel Principle Component Analysis

(KPCA) and Partial Least Square. Finally, in verification stage, a hybrid verifier can be experimented in the future work.

Acknowledgments The authors are grateful to the Research Management Centre of Universiti Teknologi Malaysia (UTM), Ministry of Higher Education Malaysia for the Fundamental Research Grant Scheme (FRGS) vote number 4F264, Research University Grant (RUG) vote number 10 J73 and The World Academy of Sciences-Committee on Scientific and Technological (TWAS-COMSTECH) vote number 4B197, which have facilitated the success of this project.

References

1. Akram M, Qasim R, Amin MA (2012) A comparative study of signature recognition problem using statistical features and artificial neural networks. In: International Conference on Informatics, Electronics & Vision. Dhaka, Bangladesh, pp. 925–929
2. Al-Mayyan W, Own HS, Zedan H (2011) Rough set approach to online signature identification. J. Digital Signal Processing 21(3):477–485
3. Alonso-Fernandez, F., Fairhurst, M.C., Fierrez, J., Ortega-Garcia, J., (2007a) *Automatic Measures for Predicting Performance in Offline Signature*. Proceedings of the 2007 15th International Conference On Image Processing. September 16–19, 2007. Texas, USA. 1–369.
4. Alonso-Fernandez, F., Fairhurst, M. C., Fierrez, J., and Ortega-Garcia, J. (2007b). *Impact of Signature Legibility and Signature Type in Off-Line Signature Verification*. Proceedings of IEEE Biometrics Symposium. September 11–13. Baltimore. 1–6.
5. Baltzakis H, Papamarkos N (2001) A new signature verification technique based on a two-stage neural network classifier. *Engineering applications of Artificial intelligence 14*(1):95–103
6. Baron R, Plamondon R (1989) Acceleration measurement with an instrumented pen for signature verification and handwriting analysis. *Instrumentation and Measurement, IEEE Transactions on 38*(6):1132–1138
7. Cheriet M, Kharma N, Liu CL, Suen C (2007) Character recognition systems: a guide for students and practitioners. John Wiley & Sons, Canada
8. Dimauro, G., Impedovo, S., and Pirlo, G. (1993). A signature verification system based on a dynamical segmentation technique, in *Proceeding 3rd International Workshop on Frontiers in Handwriting Recognition, Buffalo*, May 1993, pp. 262–271.
9. Enqi Z, Jinxu, G Jianbin Z, Chan M, Linjuan W (2009) Online handwritten signature verification based on two levels back propagation neural network. In: proceeding international symposium on intelligent ubiquitous computing and Education, pp. 202–205, Chengdu, China
10. Goodman D, Wilkinson J (1990) Patterns of research and innovation in the modern agro-food system. *Technological Change and the Rural Environment*:127–146
11. I. Graham, "Neural network technique in client authentication", in Proc Conf on Computers in the City 88, Nov 1988, pp. 207–228.
12. Jain AK, Ross A, Prabhakar S (2004) An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology* 14(1):4–20
13. Kanawade MV, Katariya SS (2013) Review of Offline Signature Verification and Recognition System. *International Journal of Emerging Technology and Advanced Engineering 3*(7):659–662
14. Leclerc F, Plamondon R (1994) Automatic signature verification: The state of the art—1989–1993. *International Journal of Pattern Recognition and Artificial Intelligence* 8(03):643–660

15. Lee S, Pan JC (1992) Offline tracing and representation of signatures. *Systems, Man and Cybernetics, IEEE Transactions on 22*(4):755–771
16. Nasien D (2012) Feature Extraction and Selection Algorithm for Chain Code Representation of Handwritten Character. Universiti Teknologi Malaysia, Malaysia, Ph. D Thesis
17. Ortega-Garcia J et al. (2003) MCYT baseline corpus: a bimodal biometric database. IEEE proceedings vision, image and. Signal Process 150(6):395–401
18. Ozgunduz, E., Senturk, T., & Karsligil, M. E. (2005, September). *Off-line signature verification and recognition by support vector machine*. In Signal Processing Conference, 2005 13th European (pp. 1–4). IEEE
19. Pal S, Alireza A, Pal U, Blumenstein M (2011) Offline signature identification using background and foreground information. In: International Conference on Digital Image Computing Techniques and Applications. Adelaide, Australia, pp. 672–677
20. Prabhakar S, Pankanti S, Jain AK (2003) Biometric Recognition: Security and Privacy Concerns. *Journal of Security Privacy* 1(2):33–42
21. Prakash, H. N., and Guru, D. S. (2009). Relative Orientations of Geometric Centroids for Off-Line Signature Verification. *Proceedings of the 2009 I.E. 7th International Conference Advances in Pattern Recognition*. February 4–6. Kolkata. 201–204.
22. Prakash HN, Guru DS (2010) Offline signature verification: an approach based on score level fusion. Journal of Computer Applications 1(1):52–58
23. Sabourin, R. and Plamondon, R. (1990). Progress in the field of automatic handwritten signature verification systems using grey-level images, in Proceeding of International Workshop on Frontiers in Handwriting Recognition, Montreal, Apr. 1990.
24. Samuel D, Samuel I (2010) Novel feature extraction technique for off-line signature verification system. *International Journal of Engineering Science and Technology* 2(7):3137–3143
25. Singh A, Kumar S, Singh TP (2013) Analysis of Hopfield associative memory with combination of MC adaptation rule and an evolutionary algorithm. *International*. Journal of Computer Applications 78(11):37–42
26. Song, Y., Huang, J., Zhou, D., Zha, H., and Giles, C. L. (2007).IKNN: Informative K-Nearest Neighbor Pattern Classification. In *Knowledge Discovery in Databases: PKDD 2007*. 248–264. London: Springer Berlin Heidelberg.
27. Taguchi, G., Elsayed, E. A., & Hsiang, T. C. (1989). Quality engineering in production systems. McGraw-Hill, New York, p 173
28. Zhang Z, Wang K, Wang Y (2011) A survey of online signature verification. In: Biometric Recognition, 6th Chinese Conference, CCBR 2011, Beijing, China, Springer Berlin Heidelberg, pp 141–149

Aini Najwa Azmi is a Master's student in Department of Computer Science, Faculty of Computing, Universiti Teknologi Malaysia, Malaysia. She is graduated in Master of Science (Computer Science in July 2016). She is a member of Soft Computing Research Group (SCRG). Her research interests are pattern recognition, soft computing and image processing. She was born in Penang Malaysia. She graduated her bachelor degree in Electrical Engineering majoring in Microelectronics in 2009 from Universiti Teknologi Malaysia

Dewi Nasien is a Senior Lecturer at Faculty of Computing, Universiti Teknologi Malaysia, Malaysia since on July 2012 until now. She is a member of Soft Computing Research Group (SCRG). Her research interests are pattern recognition, soft computing, forensic anthropology and image processing. She was born in Pekanbaru, Riau, Indonesia. She received her BSc degree in Information Technology from Universitas Islam Negeri Sultan Syarif Kasim, Indonesia on July 2005. Then she received MSc and PhD degrees in Computer Science from Universiti Teknologi Malaysia, Malaysia on August 2008 and May 2011

Fakhrul Syakirin Omar is graduated from Faculty of Electrical Engineering majoring in Microelectronics in Universiti Teknologi Malaysia year 2009. He is a researcher in Soft Computing Research Group (SCRG) in Faculty of Computing of Universiti Teknologi Malaysia. His research interests are pattern recognition, soft computing, forensic anthropology and image processing. He is a great programmer and algorithm developer in various computer languages. He was born in Pengkalan Chepa, Kelantan, Malaysia