Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 7 (2012) pp. 71-78

Camera-Based Signature Verification System through Discrete Radon Transform (DRT) and Principle Component Analysis (PCA)

Ooi Shih-Yin, Tee Wilkin and Hiew Bee-Yan

Faculty of Information Science and Technology, Multimedia University,
Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia
{syooi, tee.wilkin08, byhiew}@mmu.edu.my

***Abstract*: This paper presents a low cost camera-based signature verification system by using discrete Radon transform (DRT) and principle component analysis (PCA). The system is tested on independent database, and reported with false acceptance rate (FAR) of 7% for random forgery; and 27% for skilled forgery.**

Keywords: camera-based signature verification system, discrete Radon transform, principle component analysis, layered biometrics, false acceptance rate (FAR), false rejection rate (FRR).

I. Introduction

Biometric system is an advanced method to induce security and mainly for personal authentication. Among all of the biometric authentication systems, handwritten signature appears as the most socially accepted model for personal verification. A lot of works have been done in the field of automatic signature verification system for both dynamic signature verification and offline (static) signature verification, comprising numerous methods and approaches.

A signature is a handwritten depiction of someone's name, nickname or some other identifying mark that a person writes on documents as a proof of identity and will. Unlike other biological biometric features, human handwritten signature patterns (behavioral biometric features) inherit great intra-variance due to the age, geographic location, posture, illness, emotional state and other reasons.

Signature verification system normally focuses on detection of one or more categories of forged signatures. There are few popular groups of forgery, for instance, random forgery and skilled forgery. Skilled forgery is produced by the professional forger that has unrestricted practice to the writer's actual signatures. While a random forgery is any random scribble, a genuine signature or a high quality forgery for other writer. Skilled forgery detection emerged as the most challenging task even for expert document examiners.

This paper proposed a low cost camera-based signature verification system which combined the time of signing (dynamic information) and the image of signature (static information) with the aim of decreasing the intra-variances of handwritten signature patterns and increasing the system accuracy.

II. Literature Review

There are many signature verification system researches have been done since 1980. The state of the art before year 1989 [1], from year 1989 to 1993 [2], and from year 1993 to 2000 [3] of the similar study were extensively published by R. Plamondon et al. We also conducted the similar research study recently, reported the development of signature verification system from year 2000 to 2010 [4].

Personal authentication is a crucial issue. Dynamic signature verification has been extensively studied due to its legal and social acceptance. Most of the relevant signature verification systems are using portable devices to collect signature dynamic information, such as the Tablet PCs and gyro pen. Tablet PC is a stable and reliable signature capturing device. It captures both the dynamic (speed, pressure, centripetal and tangential acceleration) and static (2-D image) features of a handwritten signature.

A. K. Jain et al. [5] utilized a digitizing tablet to capture the dynamic and spatial information of writing. The digitizing tablet used was the IBM CrossPad from A.T. Cross Company. IBM CrossPad has a sampling rate of 100-150 samples per second and it is able to record the x-coordinates and y-coordinates of the points in the signature. By using a database of 1232 signatures from 102 individuals, they reported a FRR of 2.8% and a FAR of 1.6%.

F. Alonso-Fernandez et al. [6] developed a prototype of securing access and securing document application using Tablet PC system. Two different commercial Tablet PC systems (Hewlett- Packard TC 1100 with Intel Pentium Mobile 1.1 *Ghz* processor and Toshiba Portege M200 with Intel Centrino 1.6 *Ghz* processor) were evaluated. The information of interest for signature verification systems such as sampling and pressure statistics were also been tested and evaluated. The experiments were tested against both random and skilled forgeries by using a new database contented with over 3000 signatures. According to their report [7], the Toshiba Tablet performed better with the equal error rate (EER) of 3.20% to 2.76% for random forgeries and EER of 8.27% to 8.05% for skilled forgeries.

F. Alonso-Fernandez et al. [8] also presented a high versatile and scalable prototype for Web-based secure access using signature verification. The proposed architecture was a signature verification server that able to manage the verification process requested by the user terminal Tablet PC through the HTTP protocol. Both the web server and the signature verification server can be installed in a standard PC with Tablet PC within a local area network (LAN) environment.

Recently, the research group who inspired us on this research - D. Muramatsu et al. [9] proposed a camera-based online signature verification system. Web camera was used as data acquisition device and a sequential Monte Carlo (SMC) method was used to track a pen tip. Three items were being considered in the experiment, the position of the web camera, the method of obtaining pen trajectories and the limited amount of data that can be obtained. The online signature data were collected as time-series data of the tracked pen tip position. The distances between two sets of time-series data of the extracted features were calculated by using dynamic time warping (DTW). Lastly, the fusion model was trained with AdaBoost to combine the distances and then compute a final score. The experiments were performed by using a private database of 260 genuine signatures collected from 13 students and 780 forgeries signature collected from 2 forgers. The proposed system reported EER of 4.0%.

Furthermore, they proposed a scheme to detect signature images and re-estimate the pen tip position associated with the blurred images [10]. The pen tracking algorithm computed with SMC method and a sequential marginal likelihood was used in blurred image detection. By using private database that consisting of 390 genuine signatures and 1560 forged signatures, they reported a better EER of 3.2% instead of 3.8% (only SMC method without sequential marginal likelihood).

Besides, they also proposed a visual-based online signature verification system that used only a low-cost camera without any aid of electronic tablet [11]. The pen tip tracking was again computed by using the SMC method. By using another private database of 390 genuine signatures and 1560 skilled forged signatures, the proposed verification system reported EER of 4.1%.

Lately, S. A. Daramolo et al. [12] proposed a robust automatic online signature verification system with the aid of Wacom graphic tablet. The tablet is able to capture 100 samples per second along with the pressure value at a resolution of 0.005cm. This proposed system was tested by using 800 genuine signatures from 200 users, 400 skilled forgeries from 200 forgers and 400 random signatures, reporting FRR of 0.5% for skilled forgery and FAR of 0.25% for genuine signatures.

From the review, we can see that most of those high performance systems are very product-dependent, and most of the tablets and gyro pens involved are very expensive. Therefore, we see the potential of developing a dynamic handwritten signature verification system by adopting a low cost camera or web-camera.

III. Overview of Work

Our system flow chart is depicted in Figure 1. Generally, a handwritten signature verification system includes preprocessing, feature extraction and encoding as well as matching. All of these methodologies will be further discussed in the following sections.

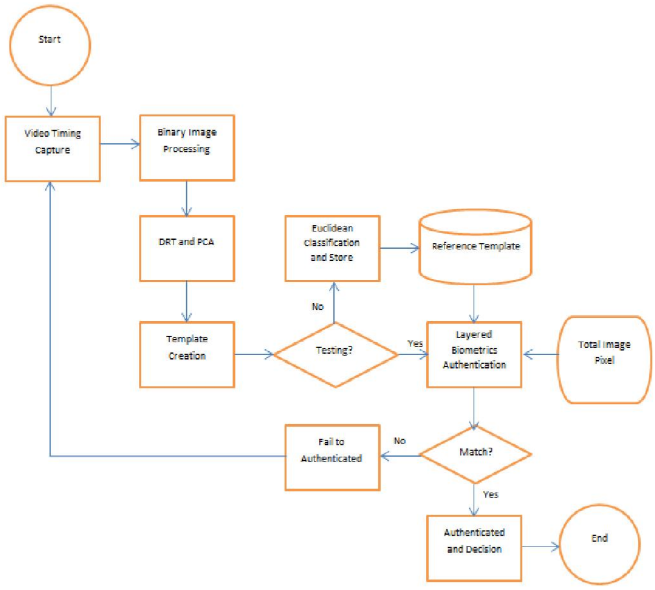

Figure 1. Flow chart of our proposed system

IV. Data Preprocessing

Any camera or web-camera with enough resolution can be used as an image acquisition device. However, the capturing hardware may introduce certain noises to a signature image. Another source of noise may be speckled paper background on which the signature is signed on. These noises on signature image may thwart the feature extraction process. We do not figure the real noise distribution, but we use the median filter to smooth the image of a signature. The using of median filtering is similar as an averaging filter like mean filter, in that each output pixel is set to an average of the pixel values in the neighborhood of the corresponding input pixel. The median is a more robust average than the mean and so a single very unrepresentative pixel in a neighborhood will not affect the median value significantly. Besides, the median filter does not create new unrealistic pixel values when the filter straddles an edge due to the fact that median value must actually be the value of one of the pixels in the neighborhood. Thus, the median filter is much better at preserving sharp edges than the mean filter.

After the smoothing, image is binarized through a simple thresholding scheme. A binary image can be considered as a special kind of intensity image, containing only black (1) and white (0). Binarization tends to minimize the database storage because it uses far less memory. It is normally not more than 1 bit/pixel, and this can be reduced as such images are very amenable to compression. On another hand, it also encouraging simpler algorithms than those applied to grey-level images.

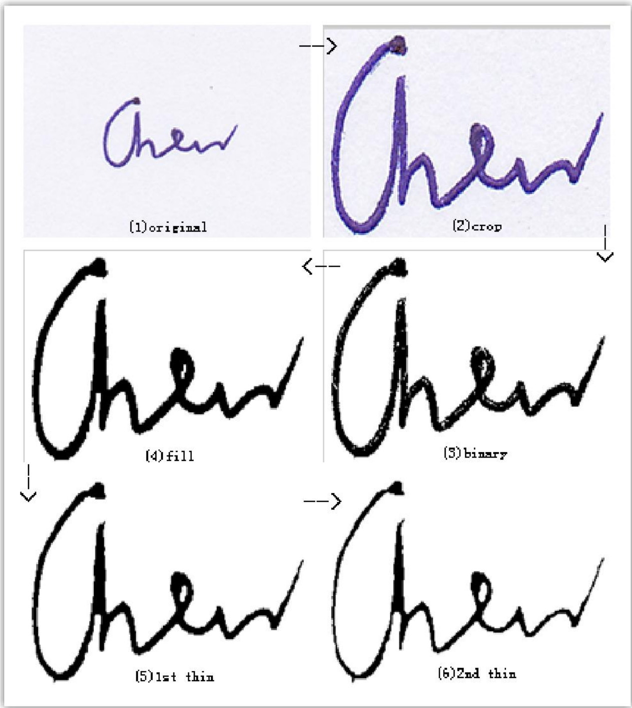

Figure 2. Preprocessing of a handwritten signature image

V. Feature Extraction

A. Discrete Radon transform (DRT)

DRT [13] is chosen to transform the signature images into a feature space. It is able to transform two dimensional images with lines into a domain of possible line parameters, where each line in the image will give a peak positioned at the corresponding line parameters. DRT has several advantages. Each signature is a static image and contains no dynamic information, thus by calculating projections at different angles, simulated time evolution is created from one feature vector to the next, where the angle represent the dynamic variable. DRT represents a projection (shadow) of the signature at different angle. A set of transform values is produced after the transformation. The DRT of an image can be calculated as follows.

Assume that each signature image consists of N pixels in total, and that the intensity of the ith pixel is denoted by I_i, $i = 1,\ldots,N$. The DRT is calculated using β non-overlapping beams per angle and Θ angles in total. The cumulative intensity of the pixels that lie within the jth beam is denoted by R_j , $j = 1,\ldots, \beta\Theta$. This is called the jth beam sum. In its discrete form, the Radon transform can therefore be expressed as the following:

$$R_j = \sum_{i=1}^{N} w_{ij} I_i, \; j = 1,2,\ldots,\beta\Theta, \quad (1)$$

where w_{ij} indicates the contribution of the ith pixel to the jth beam sum. The value of w_{ij} is determined by two-dimensional interpolation. Each projection therefore contains the beam sums that are calculated at a given angle. The accuracy of the DRT will be determined by the number of angles (Θ), the number of beams per angle (β), and the interpolation method used to calculate w_{ij}.

Our system works on DRT at Θ angles. These angles are equally distributed between 0° and 180° as depicted in Figure 3 and Figure 4.

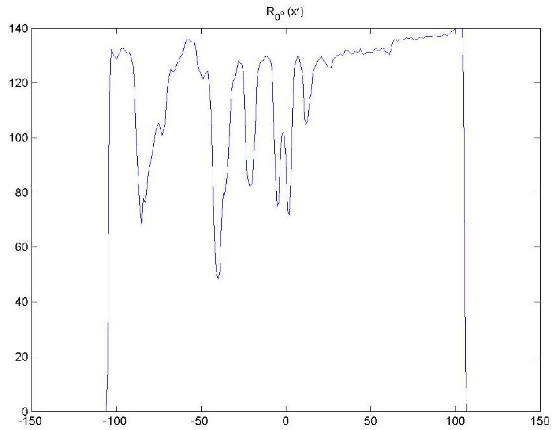

Figure 3. Radon transform for a signature image at 0°

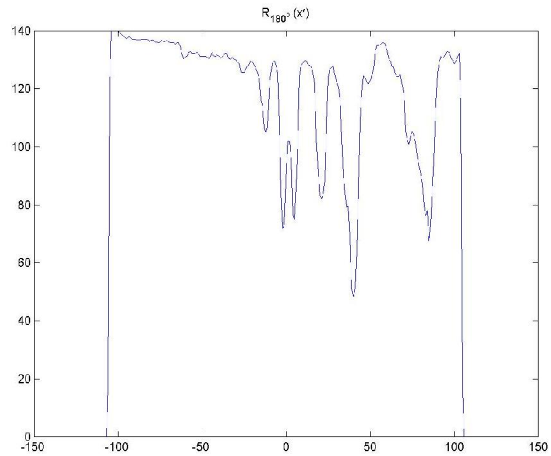

Figure 4. Radon transform for a signature image at 180°

B. Principle component analysis (PCA)

PCA has been widely used for dimensionality reduction in computer vision [14], [15], [16]. It finds a set of orthogonal basis vectors which describe the major variations among the training images and with minimum reconstruction means square error. The successful implementation of PCA in various recognition tasks popularized the idea of matching images in the compressed subspaces.

Since the number of transformed values after DRT is too huge, PCA is utilized here for feature data compression. In the PCA method, the average of K DRT features with M dimension is defined as R_{avg}. Each DRT feature, R_j differs from R_{avg} by the vector $\varphi_j = R_j - R_{avg}$. A covariance matrix as following equation is constructed.

$$C=\sum_{j=1}^{K}\varphi_j\varphi_j^T \quad (2)$$

Then, eigenvectors, v_k and eigenvalues, λ_k with symmetric matrix C are calculated. v_k determines the linear combination of K difference images with φ to form the EigenSignature,

$$U_l=\sum_{k=1}^{K} v_{lk}\varphi_k \qquad l=1,\ldots,K\,. \quad (3)$$

Then, $P(<K)$ EigenSignatures are chosen to correspond to the P highest eigenvalues, which imply that the P features are selected. An input DRT feature, R_k is transformed and projected into the EigenSignature space by the operation, $\rho_k = U_k(R_k - R_{avg})$, where $k = 1,\ldots,P$.

VI. Verification System Setup

A. Video time capturing

A camera is placed to the left side of the writing hand if the person is a right-handed person and vice versa. The period time of sign will be collected as a dynamic data from the video.

During the enrolment phase, a user will write down his or her name and produces several signatures. The writing process will be captured and recorded. The best position of the camera for acquiring the signature data is just above the writing surface, the opposite site of the writer hand and most importantly does not blocking by the writer hand. The example of this suggested position is shown in Figure 5. The mean of timing of the particular person signing will be calculated and stored with the person name.

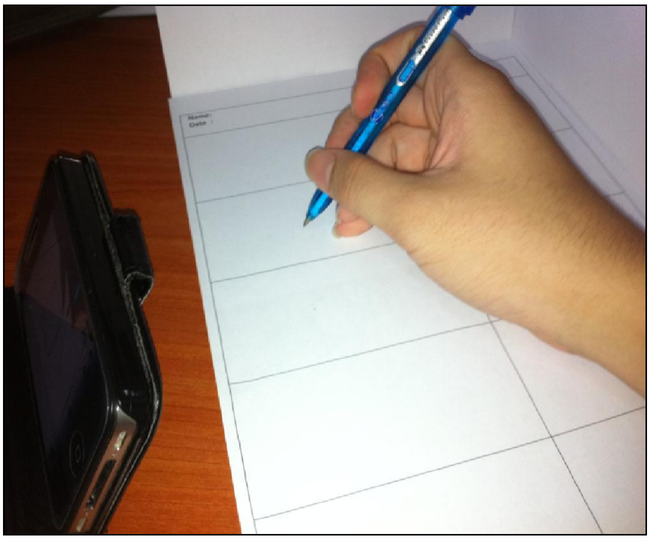

Figure 5. The position of camera

The video is trimmed and the front and end unused part are cropped. Open source software like Window Live Movie Maker and any video converter is used to do this. The video is then converted to AVI format which is readable by MatLab. After that, the information of the video is computed using Matlab 'mmreader' and 'get' functions. The algorithm is then able to calculate the duration of the signing time (dynamic information of a particular handwritten signature).

B. Database

Due to the non-repetitive nature of variation of the signatures, the signatures produced will have certain variations among same writers. Thus, the data preparation was mainly divided into two stages. In the first stage, five sample signatures are registered per writer at a single contact session. In the second stage, another set of five genuine signatures were supplied by the same writer during the contact sessions 1 day after the initial session. Thus, by recording the specific date, we can observe the variations among the same signature for a single session and different sessions. For the forgery part, the skilled forgeries are obtained from 3 expert forgers. We provided them with several samples of each signatory's genuine signature and they are allowed ample opportunity to practice on it.

The pen or pencil used by each writer is not prescribed but signatures are written within a pre-drawn 5 x 2 grid on A4 paper as depicted in Figure 6. The individual images are extracted and labeled with both the writer names and the signature class number.

The experiment schemes are designed as follow: four samples of each person are sequentially selected for Eigen basis construction and the remaining six samples are used for testing, the PCA length is set to 100. We will evaluated the system based on false acceptance rate (FAR), false rejection rate (FRR), and average error rate (AER).

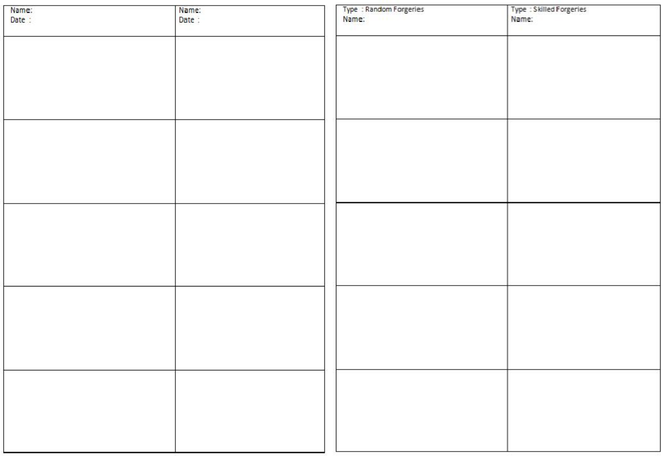

Figure 6. The template to collect handwritten signatures

C. Feature matching

There is a need to compare two signatures based on their feature vectors. With the feature matching and classification process, the identity of an individual can be verified. Euclidean distance is being used in this experiment.

Euclidean distance (L_2-norm) or Euclidean metric is the most common distance metric. In our case, the feature vectors after the interpolation (through DRT) are of the same length, thus the best way to compare them would be the use of Euclidean distance. Euclidean distance gives a measure of similarity of feature values between two compared templates. The matching equation is shown below.

$$d_{L_2} = \sqrt{\sum_{j=1}^{m} \left| X_j - Y_j \right|^2} \qquad (4)$$

where X_j and Y_j are two templates' feature values of m dimensions to be compared. Lower value of the measure gives a closer vector and vice versa. Determination will be made based on the computed dissimilarity score whether accept user as a legitimate client or reject user as an imposter. User is assumed as a legitimate client as long as his or her calculated dissimilarity score is less than the predefined threshold value.

VII. Verification System Prototype

In order to start the verification, we will train the database by choosing the correct training database. The user is asked to key in his/her password before supply the handwritten signatures. The password is encrypted before store in database. By doing this, the system security can be increased. After the training is done, we can start to test the system. The test image and video will be select; the fusion scores will be calculated and compared to the defined threshold. If the score is less than threshold, we assume the user is legitimate writer, else, we will assume him/her as imposter. Screen shots (Figure 7 – Figure 12) are shown to depict how our system works.

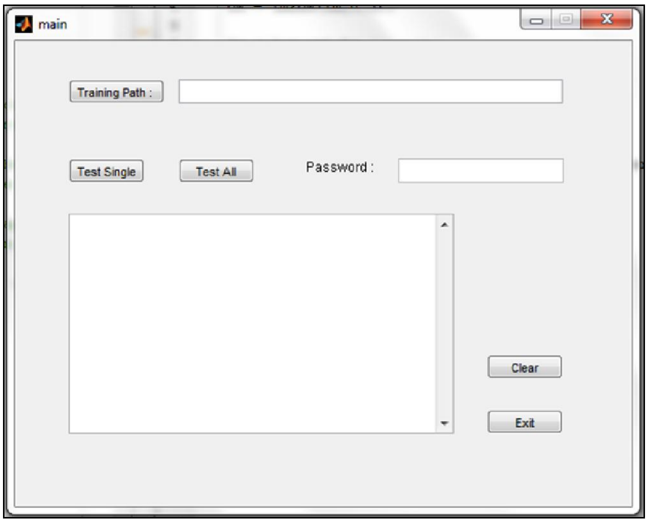

Figure 7. Main page of the prototype

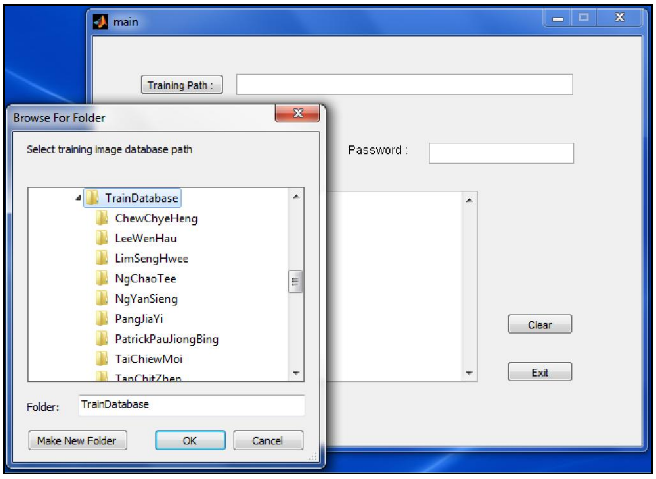

Figure 8. Select the appropriate training database folder

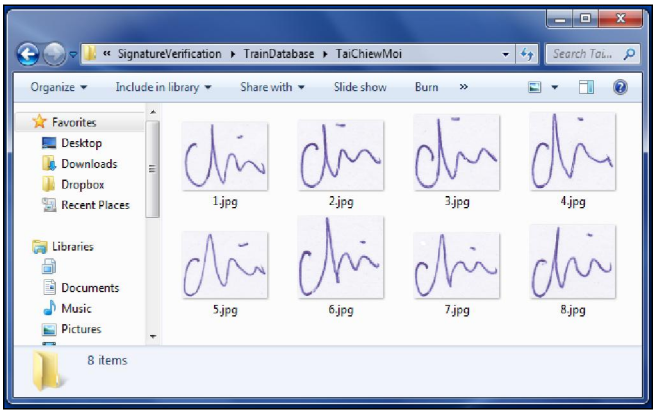

Figure 9. Example of training database folder

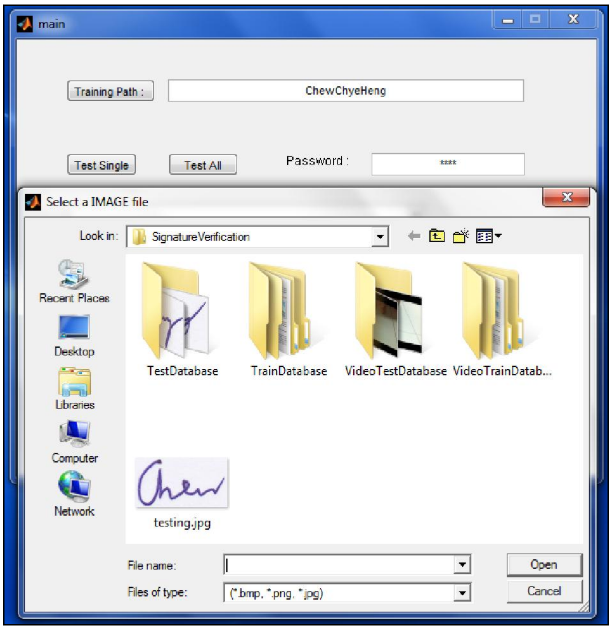

Figure 10. Choose test image

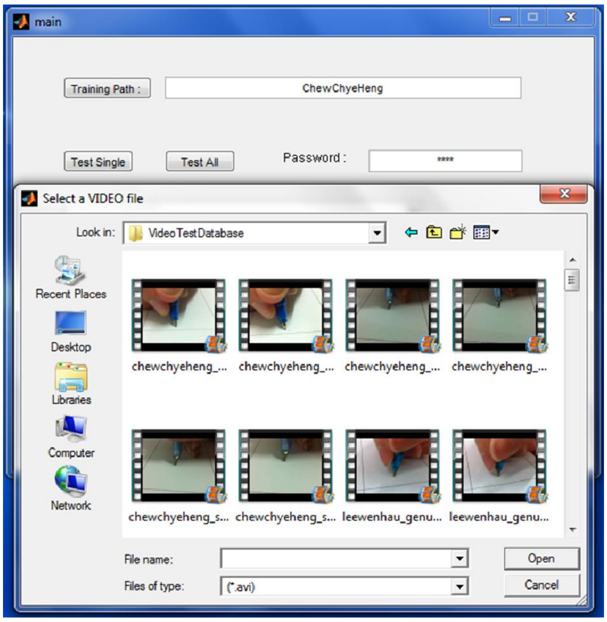

Figure 11. Choose test video

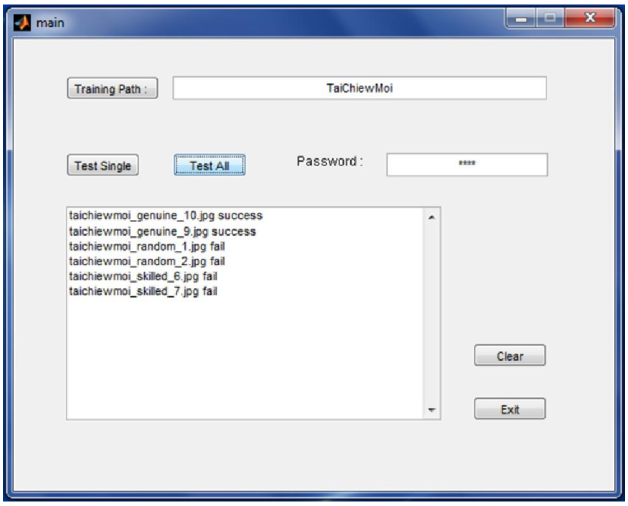

Figure 12. Example of verification output

VIII. Experimental Results

There are three thresholds in the system, which are Euclidean distance difference, duration of signing and total pixel of the signature image. We have brute-force testing our system with different sets of possible threshold combination in order to find the optimal one.

Table 1. Result of total error occurs with different threshold combination sets.

Total error occur with different threshold																
EUC/TIM/PIX	3/100/300	3/300/300	3/300/500	5/100/300	5/300/300	5/300/500	10/100/300	10/300/300	10/300/500	15/100/300	15/300/300	15/300/500	20/100/300	20/300/300	20/300/500	
ChewChyeHeng	0	0	0	0	0	0	2	2	2	2	2	2	2	2	2	18
LeeWenHau	1	2	2	1	2	2	1	1	1	1	1	1	1	1	1	19
LimSengHwee	4	4	4	4	4	4	4	4	4	3	3	3	1	1	1	48
NgChaoTee	1	0	0	1	0	0	1	0	0	2	1	1	2	1	2	12
NgYanSieng	1	2	2	1	2	2	1	2	2	1	1	1	1	1	1	21
PangJiaYi	1	2	2	1	2	2	1	2	2	2	3	3	2	3	2	30
PatrickPauJiongBing	2	2	2	2	2	2	0	0	2	1	1	1	1	1	1	20
TaiChiewMoi	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	2
TanChitZhen	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	30
TeePohJun	1	2	2	0	1	1	1	1	1	1	1	1	1	1	1	16
TeeWilkin	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	30
YeeJiaHao	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	3
YongTeenZhen	4	4	4	2	2	2	2	2	2	2	2	2	2	2	2	36
	19	23	23	16	19	19	17	18	20	19	19	19	18	18	18	

Table 1 shows the result of using different threshold for the system. We can see that by using a 5 Euclidean threshold, 100 millisecond of timing ranging and 300 pixel of signature image pixel ranging produced the optimal result for this system. It only has 16 errors by testing on 78 signatures (26 genuine, 26 random and 26 skilled signature) from 13 signatory.

Table 2. The optimum threshold combination set.

Total Error For Different Signature Type (5/100/300)			
Name\Type Of Signature	Genuine	Random	Skilled
ChewChyeHeng	0	0	0
LeeWenHau	1	0	0
LimSengHwee	0	2	2
NgChaoTee	1	0	0
NgYanSieng	1	0	0
PangJiaYi	0	0	1
PatrickPauJiongBing	0	0	2
TaiChiewMoi	0	0	0
TanChitZhen	0	0	2
TeePohJun	0	0	0
TeeWilkin	2	0	0
YeeJiaHao	0	0	0
YongTeenZhen	2	0	0
	7	2	7

By referring to *Table 2*, we can see that there are 7 errors, 2 errors and 7 errors respectively for 26 signatures of each genuine, random and skilled forgery signatures. From the result above, our verification reported a FRR of 27%, and FAR of 7% and 27% for random and skilled forgeries respectively, yielding AER of 21%.

IX. Conclusions

This paper proposed camera-based signature verification through DRT, and PCA without any aid of tablets or gyro pens. The acceptable accuracy is feasible to filter the forgery from the genuine signature, especially for skilled forgery. The results are encouraging and thus should motivating the research. We also will increase the database size in the near future.

Acknowledgment

Our thanks and appreciations to those referred work listed in literature.

References

[1] R. Plamondon, G. Lorette. "Automatic Signature Verification and Writer Identification: The State of the Art", *Pattern Recognition*, 22 (2), pp. 107-131, 1989.

[2] R. Plamondon, F. Leclerc. "Automatic Signature Verification: The State of the Art", *International Journal of Pattern Recognition and Artificial Intelligence (IJPRAI)*, pp. 643-660, 1994.

[3] R. Plamondon, S. Srihari. "Online and Offline Handwriting Recognition: A Comprehensive Survey", *Pattern Analysis and Machine Intelligence, IEEE Transactions*, pp. 63-64, 2000.

[4] W. Tee, S.Y. Ooi. "State of the Art: Signature Verification System". In *Proceedings of the 7th International Conference on Information Assurance and Security (IAS2011)*, pp. 110-115, 2011.

[5] A.K. Jain, F.D. Griess, S.D. Connel. "Online Signature Verification System", *Pattern Recognition*, 35 (12), pp. 2963-2972, 2002.

[6] F. Alonso-Fernandez, J. Fierrez-Aguilar, F. del-Valle, J. Ortega-Garcia. "On-line Signature Verification Using Tablet PC". In *Proceedings of the 4th International Symposium (ISPA)*, pp. 245-250, 2004.

[7] F. Alonso-Fernandez, J. Fierrez-Aguilar, J. Ortega-Garcia. "Sensor Interoperability and Fusion in Signature Verification: A Case Study Using Tablet PC", *Biometric Recognition Systems*, pp. 180-187, 2005.

[8] F. Alonso-Fernandez, J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez. "Secure Access System Using Signature Verification over Tablet PC". *Aerospace and Electronic Systems Magazine*, IEEE, pp. 3-8, 2005.

[9] D. Muramatsu, K. Yasuda, T. Matsumoto. "Biometric Person Authentication Method Using Camera-Based Online Signature Acquisition". In *Proceedings of the 10th International Conference of Document Analysis and Recognition (ICDAR)*, pp. 46-50, 2009.

[10] D. Muramatsu, K. Yasuda, T. Matsumoto, S. Shirato. "Camera-Based Online Signature Verification with Sequential Marginal Likelihood Change Detector". In *Proceedings of CAIP*, pp. 229-236, 2009.

[11] D. Muramatsu, K. Yasuda, T. Matsumoto, S. Shirato. "Visual-Based Online Signature Verification Using Features Extracted from Video", *Network and Computer Applications*, pp. 333-341, 2009.

[12] S.A. Daramolo, T.S. Ibiyemi. "Efficient Online Signature Verification System", *International Journal of Engineering & Technology*, 2010.

[13] J. Coetzer, B.M. Herbst, J.A. du Preez. "Offline Signature Verification Using the Discrete Radon Transform and A Hidden Markov Model", *EURASIP Journal on Applied Signal Processing*, 4, pp.559-571, 2004.

[14] G. Lu, D. Zhang, K. Wang. "Palmprint Recognition Using Eigenpalms Features", *Pattern Recognition Letters*, 24 (9-10), pp.1473-1477, 2003.

[15] M.A. Turk, A.P. Pentland. "Eigenfaces for Recognition", *Journal of Cognitive NeuroScience*, 3 (1), pp.71-86, 1991.

[16] X. Wang, K.P. Kuldip. "Feature Extraction and Dimensionality Reduction Algorithms and Their Applications in Vowel Recognition", *Pattern Recognition*, 36 (10), pp.2429-2439, 2003.

Author Biographies

Ooi Shih-Yin received her Bachelor of Information Technology (Hons) and Master of Science (Information Technology) from Multimedia University, Malaysia in 2004 and 2006 respectively. Shih-Yin joined the Faculty of Information Science and Technology in Multimedia University, Malaysia where she is the currently the Program Coordinator of B. IT (Hons) Security Technology. She has authored few indexing journals and conference papers, and served as paper reviewer in the field of biometrics, image processing, machine intelligence, computer vision, and data mining.

Tee Wilkin born at Melaka 17 August 1990, graduated from Mohd Dato Taha, Negeri Sembilan during secondary school. He was graduated from Multimedia University, Melaka Campus, Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia in Bachelor of Information Technology (Hons) Security Technology.

Hiew Bee-Yan from Malaysia received her Bachelor of Information Technology (Hons) from University of Malaya, Malaysia in 2004. In 2008, she obtained her Master of Science (Information Technology) from Multimedia University Malaysia. She is presently a lecturer of Faculty of Information Science and Technology, Multimedia University, Malaysia. Her research interests include computer vision and image processing.