American Journal of Applied Sciences 6 (2): 233-240, 2009
ISSN 1546-9239

A Novel Approach to Dynamic Signature Verification Using Sensor-Based Data glove

[1]Shohel Sayeed, [2]Nidal S. Kamel and [3]Rosli Besar
[1]Faculty of Information Science and Technology, Multimedia University,
Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia
[2] Department of Electrical and Electronic Engineering, Universiti Teknologi PETRONAS,
Bandar Seri Iskandar, 31750 Tronoh, Perak, Malaysia
[3]Faculty of Engineering and Technology, Multimedia University,
Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia

Abstract: Data glove is a new dimension in the field of virtual reality environments, initially designed to satisfy the stringent requirements of modern motion capture and animation professionals. In this study we try to shift the implementation of data glove from motion animation towards signature verification problem, making use of the offered multiple degrees of freedom for each finger and for the hand as well. We used an SVD-based technique to extract the feature values of different sensors' locating on corresponding fingers in the signing process and evaluated the results for writer authentication. The technique is tested with large number of authentic and forgery signatures using data gloves with 14, 5 and 4 sensor and shows a significant level of accuracy with 2.46~5.0% of EER.

Key words: Data glove, signature verification, singular value decomposition, euclidean distance

INTRODUCTION

In early days, human beings were commonly identified by their names. As the human population increased, method of identifying a person became more sophisticated. People needed to be associated with more information such as family's background, nationality, gender, age and blood group to label each and every human being as the unique person in the world. The problem of personal identification is multiplied when computer comes into the communication channel of two parties. For this reason, more reliable authentication scheme is needed to build up the required trust of communication link. Password, PINs and token are examples of traditional authentication technology. However, these methods have major drawbacks as passwords and PINs tend to be forgotten or shared out whereas token can be easily lost or stolen.

Alternatively, biometry offers potential for automatic personal verification and differently from other biometric means it is not based on the possession of anything or the knowledge of some information.

People recognition by means of biometrics[1-3] can be split into two main categories: a) Passive or Physiological biometrics such as face recognition, fingerprint, iris or retina, hand geometry, off-line hand signature and DNA (Deoxyribonucleic Acid) analysis. b) Active or Behavioral biometrics such as voice recognition, hand signature and typing behavior. Signature recognition belongs to this last category and according to market share reports[4] it is the second most important within this group, just behind speech recognition and over keystroke, gait, gesture, etc.

SIGNATURE RECOGNITION

Signature recognition can be split into two categories: Off-line or Static and On-line or Dynamic. In off-line mode, users write their signature on paper, digitize it through an optical scanner or a camera and the biometric system recognizes the signature analyzing its shape. In on-line mode, users write their signature in a digitizing tablet such as the device[5], which acquires the signature in real time. Another possibility is the acquisition by means of stylus-operated PDAs.

There are three types of forgeries can be established for a signature verification system, depending on testing conditions and environment[6]:

- Simple forgery where the forger makes no attempt to simulate or trace a genuine signature.
- Random forgery where the forger uses his/her own signature as a forgery.
- Skilled forgery where the forger tries and practices

Corresponding Author: Shohel Sayeed, Faculty of Information Science and Technology, Multimedia University, Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia Tel: +606-2523296 Fax: +606-2318840

imitating as closely as possible the static and dynamic information of the signature to be forged.

Dynamic signature verification taking into account the highest security levels, which can be achieved by dynamic systems, most of the efforts of the international scientific community are addressed toward this group. This research will be mainly devoted to dynamic signature verification[7-8].

In dynamic signature verification system involves (i) data acquisition (ii) feature extraction (iii) matching and (iv) decision.

Data acquisition: For dynamic signature verification system digitizing tablet or pen tablet or smart pen is used to acquire the signature data.

Feature extraction: Static or dynamic features are extracted for verification process. Static features are extracted from the whole process of signing, such as maximum, minimum and average of writing speed, curvature measurements, etc. On the contrary, the dynamic features are the evolution of a given parameter as function of time f(t). Examples are position x(t), y(t), velocity v(t), acceleration a(t), pressure p(t), tangential acceleration $t_a(t)$, curvature radius r(t), normal acceleration $n_a(t)$, etc. These features are also named functions.

Matching: Consists of measuring the similarity between the claimed identity model and the input features. When using dynamic features, some kind of length normalization must be done, because different repetitions of a signature from a given person will last differently.

Decision: Once a similarity score is obtained, the decision implies the computation of a decision threshold. If the similarity is greater than a threshold, the decision is accepted as genuine; otherwise it is rejected as forgery.

PROPOSED METHOD FOR DYNAMIC SIGNATURE VERIFICATION

In the early days, some researchers have worked on simple or random forgeries while others have dealt with the signature verification of skilled forgeries. Present research deals with the signature verification of skilled forgeries using sensor-based data glove.

The model for the proposed dynamic signature verification system is shown in Fig. 1. The proposed system is divided into two phases such as enrollment phase and verification phase. In the enrollment phase, the users are first enrolled by providing a limited number of samples (reference signatures). In this phase, SVD is performed on the signer data matrix and the r-principal subspace is extracted and saved in the database (template database) as reference signature model. In the verification phase, user input the signature using data glove. The r-principal subspace is calculated. When a user claims be a particular individual, his/her principal subspace is then matched to the reference signature model in the template database through the similarity factor. Finally, the similarity factor is compared with the decision threshold for accepted or rejected as genuine or forgery, respectively.

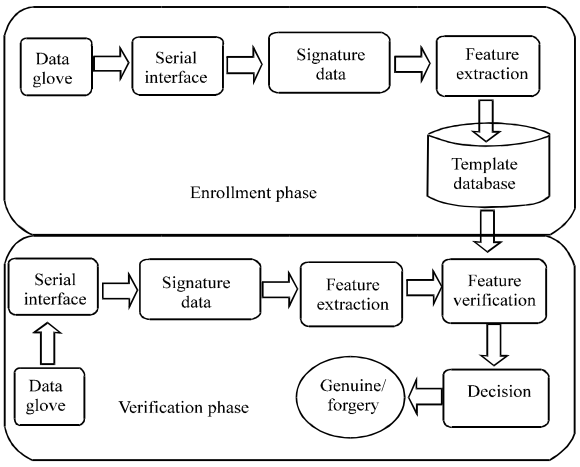


Fig. 1: Sensor-based Dynamic Signature Verification System

Hand Skeleton Model: Human hand is highly articulated. To model the articulation of fingers, the kinematical structure of hand should be modeled. In this research, the skeleton of a hand can be abstracted as stick figure with each finger as a kinematical chain with base frame at the palm and each fingertip as the end-effecter. Such a hand kinematical model is shown in Fig. 2 with the names of each joint. This kinematical model has 27 Degrees of Freedom (DoF)[9]. Each of the four fingers has four DoF.

The distal interphalangeal (DIP) joint and proximal interphalangeal (PIP) joint each has one DoF and the metacarpophalangeal (MCP) joint has two DoF due to flexion and abduction.The thumb has a different structure from the other four fingers and has five degrees of freedom, one for the interphalangeal (IP) joint and two for each of the thumb MCP joint and trapeziometacarpal (TM) joint both due to flexion and abduction. The fingers together have 21 DoF. The

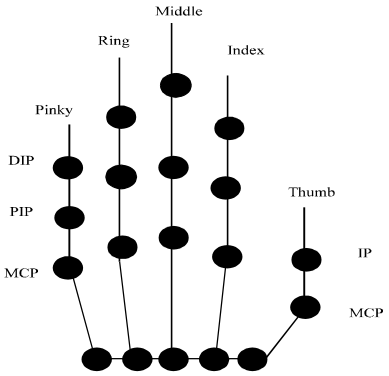


Fig. 2: Kinematical structure and joint notations

remaining 6 degrees of freedom are from the rotational and translational motion of the palm with 3 DoF each. These 6 parameters are ignored since we will only focus on the estimation of the local finger motions rather than the global motion. Articulated local hand motion, i.e. finger motion, can be represented by a set of joint angles θ, or the hand state. In order to capture the hand motion, glove-based devices have been developed to directly measure the joint angles and spatial positions by attaching a number of sensors to hand joints. Data Glove is such a device. In this study, we employ a right-handed Data glove. The glove has two sensors for the thumb (a MCP and a IP), two sensors for each of the fingers Pinky, Ring, Middle and Index (a MCP and a PIP), respectively and four more abduction sensors for the abduction/adduction angle these five fingers. There are total of fourteen sensor readings of the finger joint angles; therefore we are able to characterize the local finger motion by 14 parameters. The glove can be calibrated to accurately measure the angle within 5 degrees.

From Fig. 3, we can clearly observe some correlations in the joint angle measurements. Therefore, together with the data collected from static states and the finger motions, we then perform SVD to reduce the dimension of the model and thus reduce the search space while preserving the components with the highest energy.

Data Glove: Data glove is a new dimension in the field of signature verification and forgery detection[10-11]. The glove signature is a virtual-reality- based environment to support the signing process. Most input devices offer one, two, or three degrees of freedom, the data glove is unique in that it offers multiple degrees of freedom for each finger and for the hand as well. This permits a user to communicate to the computer a far richer picture of his or her intentions than most other input devices. The

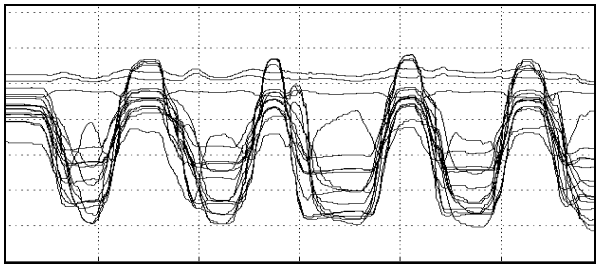


Fig. 3: Joint angle measurements from the motion of making and opening a fist

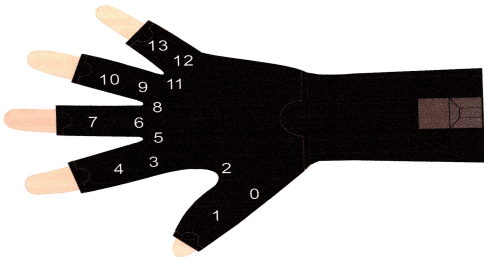


Fig. 4: Sensor mappings for 5DT data glove 14 ultra

dynamic features of the data glove provide information on:

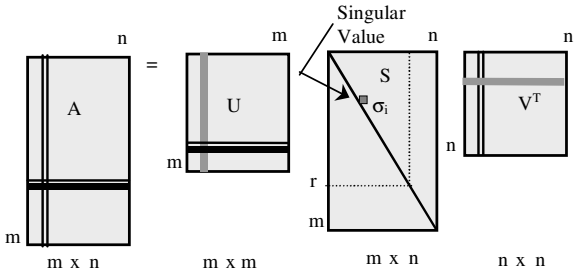
- Patterns distinctive to an individuals' signature and
- hand size.
- Time elapsed during the signing process.
- Hand trajectory dependent rolling.

In this research, we used a 5DT Data Glove 14 Ultra model hand glove shown in Fig. 4 with 14 fully enclosed fiber optic bend sensors spread two per finger as well as abduction between fingers[12]. The Data Glove interfaces with the computer via a cable to the Platform Independent USB Port. This glove is made up of flexible material like lycra to fit to many hand sizes. The data captured using this glove is of 8-bit flexure resolution and at the sampling rate of minimum 75 Hz.

SVD for Dynamic Signature Verification: Consider a data glove of m sensors each generates n samples per signature, producing an output data matrix, A(m×n). Usually n>>m, where m denotes the number of measured channels while n denotes the number of measurements. In this research, we try to ponder the implementation of SVD and the principal components of data matrix A towards signature verification system.

Theorem 1: For any real m×n matrix A, there exist a real factorization:

$$A = \underset{m\times m}{U} \cdot \underset{m\times n}{S} \cdot \underset{n\times n}{V^T} \quad (1)$$



in which the matrices U and V are real orthonormal and matrix S is real pseudo-diagonal with nonnegative diagonal elements. The diagonal entries σi of S are called the singular values of the matrix A. It is assumed that they are sorted in non-increasing order of magnitude. The set of singular values $\{\sigma_i\}$ is called the singular spectrum of matrix A. The columns u_i and v_i of U and V are called respectively the left and right singular vectors of matrix A. The space S_U^r = span $[u_1, u_2,\ldots, u_r]$ is called the r-th left principal subspace. In a similar way, the r-th right singular subspace is defined.

Conceptual relations between SVD and oriented energy: We are now in the position to establish the link between the singular value decomposition and the concept of oriented energy distribution.

Define the unit ball UB in R^m as $UB = \{q \varepsilon R^m \mid \|q\|_2 = 1\}$

Theorem 2: Consider a sequence of m-vectors $\{a_k\}$, k = 1, 2, …, n and the associated m×n matrix A with SVD as defined in Eq. (1) with n ≥ m. Then:

$$E_{u_i}[A] = \sigma_i^2 \quad (2)$$

$$\forall_q \varepsilon UB : \text{if } q = \sum_{i=1}^{m} \gamma_i . u_i \text{ then}$$

$$E_q[A] = \sum_{i=1}^{m} \gamma_i^2 . \sigma_i^2 \quad (3)$$

Proof: Trivial from theorem 1.

With the aid of theorem 2, one can easily obtain, using the SVD, the directions and spaces of extremal energy, as follows:

Corollary 1: Under the assumptions of theorem 2:

$$\max_{Q^r \subset R^m} E_{Q^r}[A] = E_{S_U^r}[A] = \sum_{i=1}^{r} \sigma_i^2 \quad (4)$$

$$\max_{Q^r \subset R^m} E_{Q^r}[A] = E_{(S_U^{r-m})^\perp}[A] = \sum_{i=m-r+1}^{r} \sigma_i^2 \quad (5)$$

where max and min denote operators, maximizing or minimizing over all r-dimensional subspaces Q^r of the ambient range space R^m. S_U^r is the r-dimensional principal subspace of matrix A while $(S_U^{m-r})^\perp$ denotes the r-dimensional orthogonal complement of S_U^{m-r}.

The above properties of SVD are very desirable in dynamic signature verification, when signature data are taken using data glove.

Now, having identified each signature through its r-th principal subspace S_U^r, the authenticity of the tried signature can be obtained by calculating the Euclidean distance between its principal subspace and the genuine reference. The Euclidian distance for every genuine or forged signature $X_i \in \{x_1, x_2, \ldots, x_k\}$ with the reference signature $Y_i \in \{y_1, y_2, \ldots, y_k\}$ is calculated by given equation:

$$\text{Distance}(X_i, Y_i) = \left(\sum_{i-1}^{k} \left| X_i - Y_i \right|^2 \right)^{1/2} \quad (6)$$

Summary of our Dynamic Signature Verification Technique using distance measurement:

- From the data glove output form data matrix A (m×n)
- Compute the SVD of matrix A $A = \underset{m\times m}{U} - \underset{m\times n}{S} - \underset{n\times n}{V^T}$
- From matrix **U** extract the first *r* left singular vectors and form the principal subspace S_U^r
- Find the Euclidean distance between its principal subspace and the genuine reference

EXPERIMENTAL RESULTS AND DISCUSSION

To verify the efficiency of the proposed technique in handwritten signature verification, the 5DT Data Glove 14 Ultra is used. This glove is using 4, 5 and 14 sensors to measure finger flexure (two sensors per finger) as well as the abduction between fingers. The system interfaces with computer via cable to USB port or via Bluetooth technology (up to 20 m distance). The SVD-signature verification algorithm is written in MATLAB 7.0 and run on a machine powered by Intel Core 2 Dual processor.

The data is collected from only genuine and skilled forgers and shown in Table 1 and 2.

Table 1: Description of database for glove-based signatures

No. of writers	40
No. of genuine samples per writer	25
No. of forgeries (imposter) per writer	10

Table 2: Distribution of database for performance evaluation

Reference signatures	Signatures for testing	
Genuine	Genuine	Forgery
40×10	40×15	40×10×10

Table 3: Similarity factor for genuine and imposter using 14, 5 and 4 sensor based signature data sets

Signature type	Genuine			Imposter		
similarity factor (%)	14-sensor	5-sensor	4-sensor	14-sensor	5-sensor	4-sensor
(91-100)%	28.5	54.5	70.5	0	0.2	3.1
(86-90)%	45.5	14.5	7.5	0	1.1	5.6
(81-85)%	15.0	14.5	6.0	0	2.4	8.2
(76-80)%	7.5	7.5	3.5	0.35	8.6	6.0
(71-75)%	0.35	7.0	4.0	2.90	12.7	13.9
(66-70)%	0	2.0	5.0	9.70	17.9	17.1
(61-65)%	0	0	3.5	17.70	22.2	18.6
(51-60)%	0	0	0	48.05	33.1	16.5
<50%	0	0	0	21.30	1.8	11.0

As Table 1 and 2 indicate, the signature data samples are collected from two types of writers: genuine and imposter. The genuine data set is divided into the reference and test sets. The reference or template set comprises the first 10 genuine signatures and the test sets consist of the remaining samples (i.e., 40×15= 600 genuine) and 40×10×10 = 4000 skilled forgery. Forgers (40 persons) are given the signature images of the genuine (10 persons) and allowed to familiarize and practice the target signatures (10 forgery trails by each of the forger) with unlimited trials for forging.

The SVD-based technique is run with the data in Table 2 and the similarity factor is calculated in percent and given in Table 3. It is clear from Table 3 that with genuine samples the SVD-signature verification technique, for a data glove of 14 sensors is producing 100% samples with similarity factor >76% and approximately zero samples for similarity factor lower than 76%. This simply means that, for the worst case of repetition of a signature by the same writer, the SVD-based signature verification technique manages to recognize the similarity with other genuine one by at least 76% and for average quality of repeated samples the similarity factor is about 96.5%. On the contrary, out of the 4000 forgery samples the suggested technique produces 0% number of trials with similarity factor greater than 70%, making it nearly impossible for any skilful forger to exceed this threshold. Table 3 also shows that when the similarity factor >76%, data sets

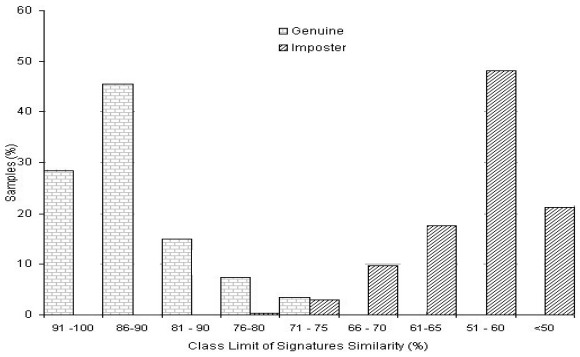


Fig. 5: Similarity measure between the reference signature and imposter trials using 14-sensor based signature data sets

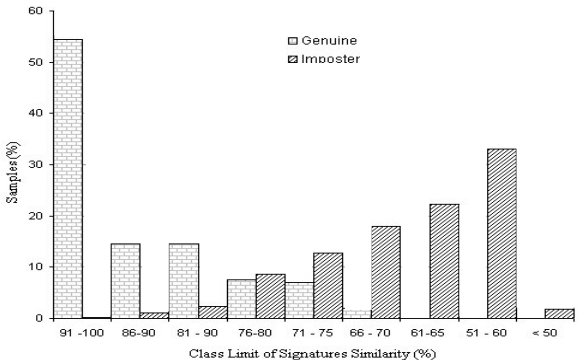


Fig. 6: Similarity measure between the reference signature and imposter trials using 5-sensor based signature data

using 5 and 4 sensor for genuine group of writer produces similarity factor 91 and 87.5% samples respectively. In contrast, skilful forger able to produce 12.3 and 22.9% samples when the similarity factor >76% using data sets of 5 and 4 sensor, respectively.

To visualize the contribution of the similarity factors between the reference signature and imposter trials using 14, 5 and 4-sensor based data sets are shown in Fig. 5-7, respectively.

In a nutshell, it can be said that the suggested SVD-based signature verification technique using 14-sensor based data glove is showing quit powerful performance in recognizing the similarities between genuine signatures with lower bound of 76% and upper bound of approximately 97% which is reported in Table 4. This performance creates gap between the two cases (genuine-genuine and genuine-imposter) large enough to easily and safely distinguish between authentic and forgery trials with approximately zero error using data glove.

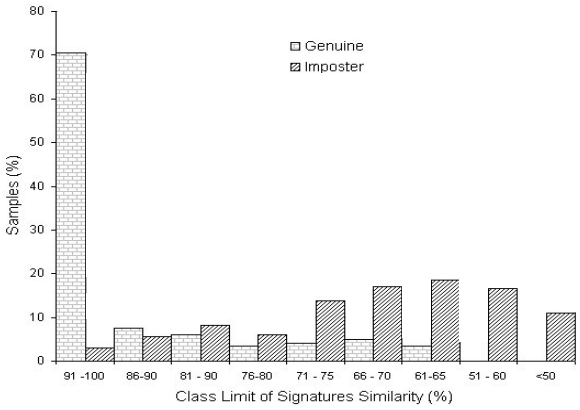


Fig. 7: Similarity measure between the reference signature and imposter trials using 4-sensor based signature data sets

Table 4: EER obtained from 14, 5 and 4 sensor-based signature data sets

Data type	14 sensor- based	5 sensor- based	4 sensor- based
ERR	2.46%	3.6%	5.0%
Threshold	0.024	0.028	0.026

Furthermore, the performance of a signature verification system is evaluated according to the error representation of a two-class pattern recognition problem, that is, with Type I and Type II error rates. The Type I error rate (False Rejection Rate (FRR)), measures the number of genuine signatures classified as forgeries as a function of the classification threshold. The Type II error rate (False Acceptance Rate (FAR)), evaluates the number of false signatures classified as genuine ones as a function of the classification threshold. To evaluate the performance of our signature verification system, we adopt the Equal Error Rate (EER) at which the percentage of FAR equal the percentage of FRR. This EER provides an estimation of the statistical performance of the algorithm. It can be adopted as a unique measure for characterizing the security level of a biometric system. The FAR and FRR are calculated for the normalized threshold values ranging from 0 to 1. FAR and FRR are calculated by

$$FAR = \frac{\text{Total number of accepted forgeries}}{\text{Total number of tested forgeries}} \times 100 \qquad (7)$$

$$FRR = \frac{\text{Total number of genuine rejected}}{\text{Total number of tested genuines}} \times 100 \qquad (8)$$

The performance of our proposed technique using 14, 5 and 4 sensor based signature data sets are illustrated in Figures 8, 9 and 10, respectively.

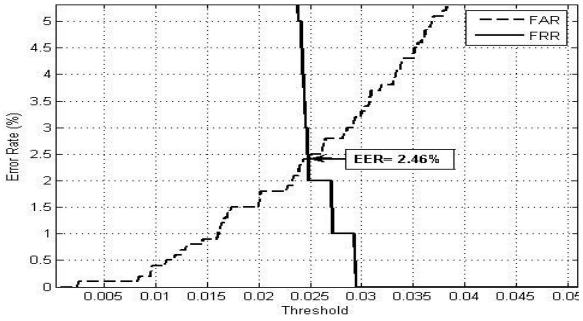


Fig. 8: FRR and FAR as a function of the classification threshold using 14-sensor based signature data sets

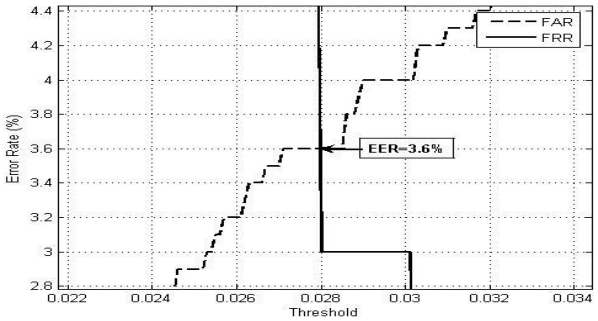


Fig. 9: FRR and FAR as a function of the classification threshold using 5-sensor based signature data sets

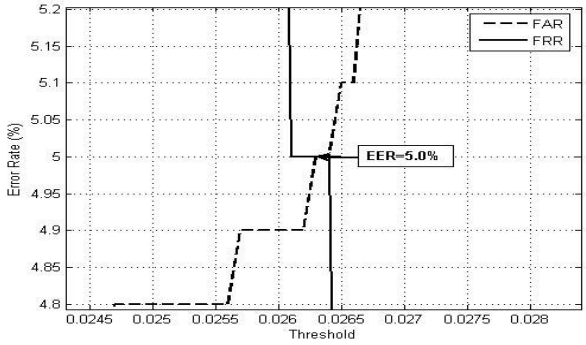


Fig. 10: FRR and FAR as a function of the classification threshold using 4-sensor based signature data

From the experimental results obtained by our proposed dynamic signature verification technique, we noticed that the system produced 2.46% of EER using 14 sensor based signature data sets and 5.0% of EER using 4 sensor based signature data sets, which is reported in Table 5.

Table 5: Dynamic Signature Verification and Error Rates

	Error Rates (%)		
Technique	FAR	FRR	EER
Hamilton *et al.*[19]	7.0%	6.0%	-
Lee *et al.*[20]	5.0%	20.0%	-
Han *et al.*[21]	4.0%	7.2%	-
Mingming *et al.*[22]	-	-	5.0%
Muramatsu *et al.*[23]	-	-	2.6%
Nakanishi *et al.*[24]	-	-	3.3%
Shinatro *et al.*[25]	-	-	4.1%
Nakanishi *et el.*[26]	-	-	4.2%
Fierrez-Aguilae *et al.*[27]	-	-	5% - 7%
Fierrez-Aguilar *et al.*[28]	-	-	7.2%
Shohel *et al.* (proposed)	-	-	2.46%~5%

From our findings, so far no other technique on on-line signature verification is available for data glove. Hence, it is unfair to compare with techniques based on different input data devices. However, based on the performance of the most recently proposed techniques for on-line signature verification in terms of their FAR and FRR or EER achieved values is shown in Table 4. The purpose of this comparison is to show the effectiveness of the proposed system as an emerging solution to the on-line signature verification problem.

Moreover, a promising result appears clearly on Table 5 that the proposed technique yields slightly lower EER value than the other on-line signature verification technique. However, we are sure that the achieved EER value can be further reduced if a data glove especially designed for signature verification is used.

Eventually, our proposed technique achieved accuracy with 2.46, 3.6 and 5.0% of EERs using 14, 5 and 4 sensor based data glove, which is comparable with other dynamic signature verification techniques and it is promising for future applications of dynamic signature verification techniques.

In addition to the aforementioned verification techniques, the First International Signature Verification Competition (SVC2004) has tested 13 systems from industry and academia and found that the best equal error rate for class of skilled forgeries is 2.84%[29].

CONCLUSION

In this research, we have presented a new approach to dynamic signature verification problem with data glove as input device to the on-line signature verification system. The technique is based on the singular value decomposition in finding r-singular vectors sensing the maximum energy of the tried signature and thus account for most of variation in original data so that the effective dimensionality of the data can be reduced. The Euclidean distance between the r-principal subspaces of the different signatures is used as indicator to the authenticity of the tried signature and refereed to as similarity factor. The experimental result shows that our proposed dynamic signature verification technique appears to be promising with 2.46~5.0% of EER.

This research paper is an initial attempt to demonstrate the data glove as an effective high bandwidth data entry device for dynamic signature verification.

In future, the structure of the data glove can be further simplified by interfacing with the computer wirelessly by means of Bluetooth technology as well as increase the database size and decrease the number of sensors.

REFERENCES

1. Nanavati, S., M. Thieme and R. Nanavati, 2002. Biometrics. Identity Verification in a Networked World. Wiley, New York.
2. Jain, A., R. Bolle and S. Pankanti, 1999. Biometrics. Personal Identification in a Networked Society. Kluwer Academic Publishers, Dordrecht.
3. Zhang, D.D., 2000. Automated Biometrics. Technologies and systems. Kluwer Academic Publishers. Dordrecht.
4. http://www.biometricgroup.com.
5. http://www.cadix.com.
6. Plamondon, R. and G. Lorette, 1989. Automatic Signature Verification and Writer Identi.cation-the State of the Art. Pattern Recognition, 1 (2): 107-131.
7. Jain, A.K., F.D. Griess and S.D. Connell, 2002. On-line signature verification. Pattern Recognition, 35: 2963-2972.
8. Lei, H. and V. Govindaraju, 2005. A comparative study on the consistency of features in on-line signature verification. Pattern Recognition Lett., 26: 2483-2489.
9. Chang, C. and W. Tsai, 2000. Model-based analysis of hand gestures from single images without using marked gloves or attaching marks on hands. Proceeding of the 4th Asian Conference on Computer Vision (ACCV2000), pp: 923-930.
10. Sayeed, S., R. Besar and N.S. Kamel, 2006. Dynamic signature verification using sensor based data glove. Proceeding of 8th Intl. Conference on Signal Processing, pp: 2387-2390.

11. Sayeed, S., N.S. Kamel and R. Besar, 2007. Biometric personal authentication based on handwritten signature. Proceeding of the 3rd Intl. Colloquium on Signal Processing and its Applications, pp: 34-39.
12. http://www.5dt.com/products/pdataglove14.html.
13. Golub, G.H. and C.F. Van Loan, 1996. Matrix computations. 3rd Edn., Johns Hopkins University Press. Baltimore, MD.
14. Golub, G.H. and H.Y. Zha, 1995. The canonical correlations of matrix pairs and their numerical computation, in Linear Algebra for Signal Processing. Springer-Verlag, New York, pp: 27-49.
15. Bjorck, A. and G.H. Golub, 1973. Numerical methods for computing angles between linear subspaces. Math. Comp., 27: 579-594.
16. Chatelin, F., 1993. Eigenvalues of Matrices. John Wiley and Sons, Chichester, UK.
17. Gohberg, I.C. and M.G. Krein, 1969. Introduction to the theory of linear nonselfadjoint operators. Transl. Math. Monogr. 18, AMS, Providence, RI.
18. Drmac, Z., 2000. On principal angles between subspaces of Euclidean space. SIAM J. Matrix Anal. Appl., 22 : 173-194.
19. Hamilton, D.J., J. Whelan, A. McLaren and I. MacIntyre, 1995. Low Cost Dynamic Signature Verification System. In: European Covention on Security and Detention, London, UK, pp: 202-206.
20. Lee, L., T. Berger and E. Aviczer, 1996. Reliable online human signature verification system. IEEE Trans. Pattern Anal. Mach. Intel., pp: 643-647.
21. Han, Chang, Hsu and Jeng, 1999. An online signature verification system using multi-template matching approaches. Proceedings of the IEEE International Carnahan Conference on Security Technology, Madrid, Spain.
22. Mingming, M. and W. Wijesoma, 2000. Automatic online signature verification based on multiple models. In CIFER.'01: Computational Engineering in Financial Engineering Conference, pp: 30-33.
23. Muramatsu, D. and T. Matsumoto, 2003. An HMM on-line verifier incorporating signature trajectories. Proceeding of 17th Int. Conference on document analysis and recognition (ICDAR).
24. Nakanishi, I., H. Sakamoto, Y. Itoh and Y. Fukui, 2005. Multi-matcher on-line signature verification system in DWT domain, ICASSP' 2005.
25. Shintaro, K., M. Daigo and M. Takashi, 2006. On-line signature verification based on user generic fusion model with marcov chain monte carlo method. Proceedings of the International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS2006), Yonago Convention Center, Tottori, Japan.
26. Nakanishi, I., H. Hara, H. Sakamoto, Y. Itoh and Y. Fuki,2006. Parameter fusion in DWT domain on-line signature verification. Proc. of the Int. Sym. On Intelligent Signal Processing and Communication Systems (ISPACS), Japan.
27. Fierrez-Aguilar, J., L. Nanni, J. Lopez-Penalba, J. Ortega-Garcia and D. Maltoni, 2005. An online signature verification system based on fusion of local and global information. Proc. of the 5th IAPR International Conference on Audio and Video Based Biometric Person Authentication, AVBPA, Springer LNCS-3546, New York, USA, pp: 523-532.
28. Fierrez-Aguilar, J., J. Ortega-Garcia and J. Gonzalez-Rodriguez, 2005. Target dependent score normalization techniques and their application to signature verification. IEEE Trans. Syst. Man Cybernetics-Part C: Application and Rev., 35 (3).
29. Yeung, D., H. Chang, Y. Xiong, S. George, R. Kashi, T. Matsumoto and G. Rigoll, 2004. SVC2004: First International Signature Verification Competition. ICBA 2004, LNCS, Springer-Verlag, Berlin Heidelberg, 3072: 16-22.