International Journal of Fuzzy Logic and Intelligent Systems, vol. 4, no. 3, December 2004 pp. 271-276

A study on the Dynamic Signature Verification System

*Jin-Whan Kim, *Hyuk-Gyu Cho and **Eui-Young Cha

* School of Computer and Information Engineering Youngsan University

** Dept. of Computer Science Pusan National University

Abstract

This paper is a research on the dynamic signature verification of error rate which are false rejection rate and false acceptance rate, the size of signature verification engine, the size of the characteristic vectors of a signature, the ability to distinguish similar signatures, the processing speed and so on. Also, we present our efficient user interface and performance results.

Key Words : Dynamic Signature Verification, Evaluation, Characteristic Vector, User Interface

I. Introduction

Dynamic signature verification technology is to verify the signer by calculating his writing manner, speed, angle, and the number of strokes, order, the down/up movement of pen when the signer input his signature with an electronic pen for his authentication.

Verifying yourself to a machine is the first step of most automated transaction. The desire for increasing convenience and security motivates the development of biometric techniques in order to replace keys, passwords, and smart cards. Signature verification presents four advantages unlike over other physiological biometric techniques from the point of view of adoption in the market place. First, it is a socially accepted identification method already in use in bank and credit card transaction; second, most of the new generation of portable computer, personal digital assistants (PDAs) and especially smart phone use handwriting as the main input channel; third, a signature may be changed by the user, similarly to a password, while it is not possible to change fingerprints, iris or retina patterns; fourth, group users can share signature key with very simple pattern of signature unlike physiological biometric technology. That is, physiological biometric technology cannot be shared for group users.

All biometric techniques have false accepts generated by the imperfections of the classification method or by errors in the acquisition device. However, dynamic signature verification using behavioral biometric technique, compared with physiological biometric techniques such as fingerprint, face, iris or retina, have additional advantage that a forger with not-enough information about the true signature could not deceive the verification algorithm because multi-dimensional feature information of dynamic signature, that is, speed of stroke, size of signature, pressure, variable shape, pen down/up information and so on decrease the risk of accepting skilled forgeries since they are not available to the forger.

Manuscript received Aug. 23, 2004; Revised Oct. 19, 2004.

The rest of this paper is organized as follows: Section 2 describes the dynamic signature verification system; Section 3 describes suggested evaluating factors for the performance analysis of the system; Section 4 describes experimental results of our system and conclusions follow it in section 5.

The contributions of this paper are the following:

First, It is new enhanced graphical user interface for dynamic signature verification using a tablet or touch screen LCD;

Second, We suggest objective criteria for the performance analysis of the dynamic signature verification system;

Third, Our system shows an excellent performance results in terms of the suggested criteria of the dynamic signature verification;

(http://www.mmigroup.net/en/mmi_products_signq.php)

2. Dynamic Signature Verification System

Figure 1 shows the diagram of a typical dynamic signature verification system (DSVS). DSVS, like all other biometric verification systems, involves two processing modes: registering and verifying. In the registering mode include three phases: training, testing and saving. In the training, the user provides signature samples that are used to construct a template (or prototype feature vector) representing some distinctive characteristic of his signature. In the testing, the user provides a new signature to judge authenticity of the presented sample and choose his own threshold security level for him.

The performance of a verification system is generally evaluated with Type I and Type II error rates. The Type I error rates, or False Rejection Rate (FAR), measures the number of genuine signatures classified as forgeries as a function of the classification threshold. The Type II error rate, or False Acceptance Rate (FAR), evaluates the number of false signatures classified as real ones as a function of the classification threshold. The equal error rate (EER) as Figure 2, that is the error rate at which the percentage of false accepts equals the percentage of false rejects, provides an estimate of the statistical performance of the algorithm, i.e., it provides an estimate of its generalization error.

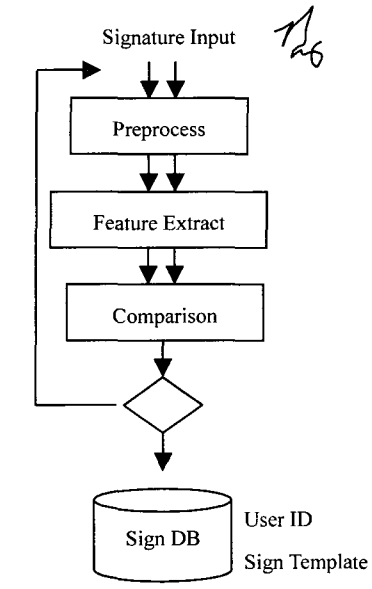


Figure 1. Dynamic Signature Verification System

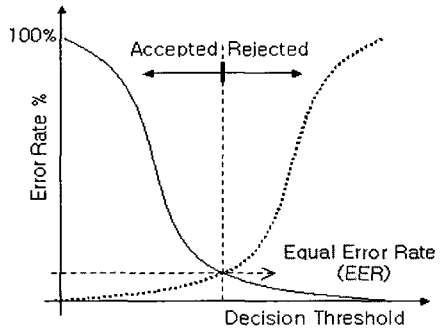


Figure 2. Graph of Equal Error Rate

3. Proposed Evaluating Factors for Performance Analysis of the DSVS

The dynamic signature verification system (DSVS) is a technology to distinguish a true signature and a forgery signature using the informationabout the form and dynamic information (the order of writing, information about time and pressure) by inputting a signature, which is written real-time with an inputting equipment such as a tablet or a digitizer, an electronic pen, or a mouse, to the system.

At present, various dynamic signature verification systems were developed and spread domestically and internationally, but it is a pity that there is no standard or guideline to evaluate and verify this technology objectively. This study attempts to examine factors that can evaluate it more objectively.

Signatures are changing according to nation, age, time, habit, and psychological and physical status, and it should absorbthese changes well. It should be remembered that every security technology needs users' efforts basically, and users' absent-mindedness and carelessness can make any security technology powerless. We will suggest evaluating factors for the excellent dynamic signature verification system.

1) Convenience (Easy User Interface Design)

Security and convenience are contrary concepts, but it is desirable to design to promote convenience to use in the process of registering signatures. The interface suggesting proper security level according to user's degree of skill in signature will be very important. By the consistence of security level suggested here, the performance of error rate in signature engine will be measured in some degrees.

2) Error Rate

Above all, the technology that can reduce false acceptance rate (FAR) and false rejection rate (FRR) to the minimum is important, but there are some difficulties in the way evaluating error rate objectively in reality. For this, signature database (true signature and forgery signature) that is objectively approved in public should be prepared.

3) Accuracy

(Discriminating power of similar patterns such as figure, speed, pressure, etc.)

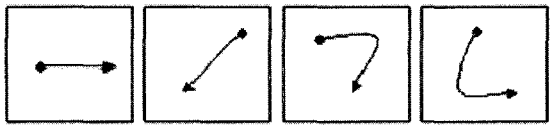


Figure 3. Very simple signature patterns

As shown in Figure 3,4,5 and 6, comparison algorithm has to calculate precisely minute changes of two patterns according to the complexity or simplicity of the signature's patterns.

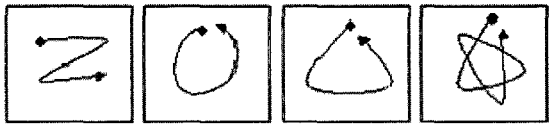


Figure 4. Fairly simple signature patterns

Figure 5. Simple signature patterns.

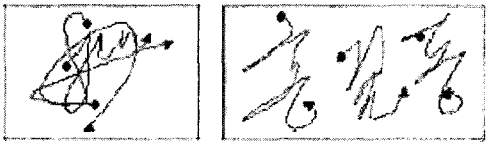


Figure 6. Common signature patterns

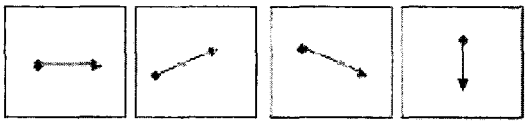


Figure 7. Discriminating power concerning the direction of elements

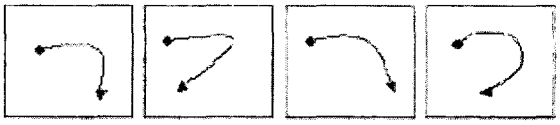


Figure 8. Discriminating power concerning minute differences between figures

As in Figure 7 and 8, the algorithm for determining the discriminating power about direction of elements and minute difference of figures has to be applied.

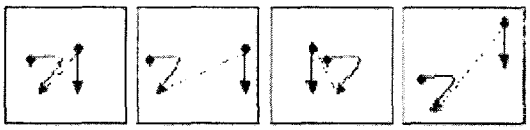


Figure 9. Discriminating power concerning the direction of pen up elements and minute difference of length

As in Figure 9, the change of the pen up element (information from the point holding up the pen to the point pressing the pen while signing) is one of the most important characteristic information for the signature verification, so it mustn't be ignored.

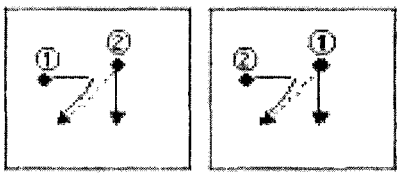


Figure 10. Discriminating power when the orders of stroke are different

As in Figure 10, if the order of strokes is different, the dynamic signature verification system, which puts a high value on order information even though the apparent figure is almost the same, should have the discriminating power.

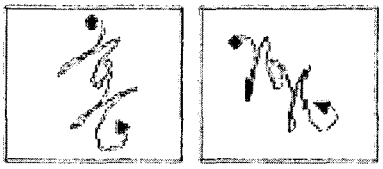


Figure 11. Discriminating power when slants are different

As in Figure 11, as for the information concerning the slant of the whole signature that can result from a change of the signature location, it would be desirable to use it as characteristic information of the signature in the case that security is prior to convenience.

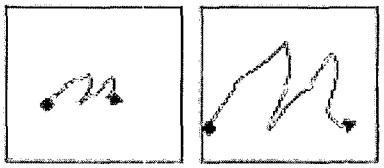


Figure 12. Discriminating power when the size of signature is different

As in Figure 12, when the entire size of two signatures are different, it would be better to ignore them to reduce the false rejection rate. However, in the case that security is prior to convenience, it would be desirable not to normalize the size of the signature but to use it as characteristic information.

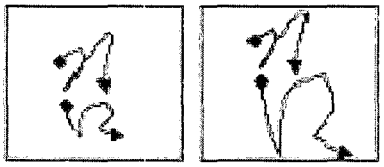


Figure 13. Discriminating power when the sizes of some parts in a signature are different

Figure 14. Discriminating power when the figures of some parts in a signature are different

As in Figure 13 and 14, not the change of the entire size of two signatures, but the change of size, figure, or speed in particular parts has to be used as important characteristic information of the signature. An elaborate comparison algorithm that can calculate minute differences to a numerical value has to be applied.

4) Size of Signature Engine

When considering the possibility of being broadly used in small-sized mobile equipment such as cellular phone, smart phone and PDA, the smaller the size of signature engine, the better.

5) Size of Signature Database (Characteristic Vectors)

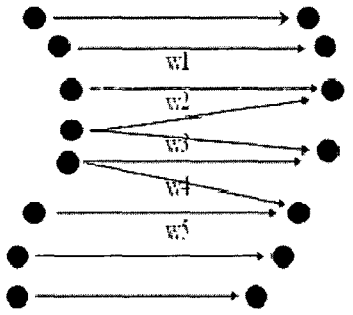
The size of characteristic vectors of a signature not only influences the speed of verification process but also needs memory with big capacity when operating the signature verification server, so the size of a signature's characteristic vectors has to be also considered.

6) Speed of Verification Process

In order to be broadly used for users' verification on the Internet, the speed of verification process has to be fast so that it can make high efficiency of business and give fewer loads to the verification server system. In this way, the signature verification server system could be established with less cost.

7) The Kind of Characteristic Information of Used Signature and Endowment of Proper Weight

Characteristic information of signature	Weight
Speed	W1
Shape	W2
Order of Strokes	W3
Number of Strokes	W4
Entire elapsed time for signature	W5
...	...



[Signature A] [Signature B]

Figure 15. Weight of characteristic information

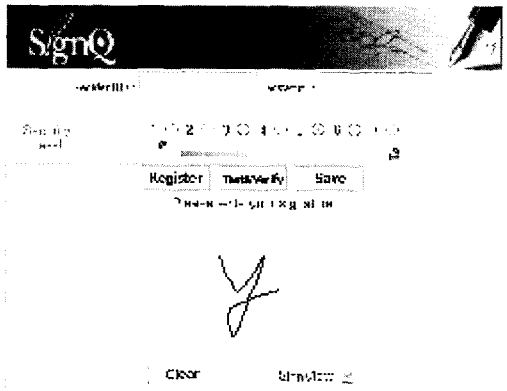
It is more important than anything that good characteristic information for dynamic signature verification reduce the change range of true signature, make big discrimination from forgery signature, and calculate the degree of similarity between two signatures by combining characteristic information well and endowing proper weight when using plural characteristic information.

This thesis is a study on the factors that can evaluate dynamic signature verification technology, which stands out as a key security technology for the next generation, more objectively. It is expected that this will be used as a basic material to understand the same technology and evaluate performance and as a reference when a signature verification system with prominent function is developed or examined.

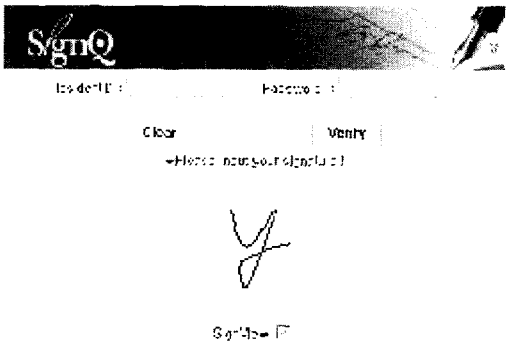
4. Performance Results

The characteristics of our system are as follows;

1) Dynamic Time Warping (DTW) well known for excellent pattern matching algorithm has been modified and applied to this system. Reliability for checking the similarities between signatures is high and a newly developed fast algorithm in processing time is adopted in the system. To make access easier, we considered efficient user interface design.
2) Size of feature vector for the signature is very small. It needs 20byte-250byte of memory capacity to register feature information of a signature in average.
3) Processing time must be fast for the verification. In general DTW system, it is good to check similarity between patterns, but it has defect to make processing time because of computing complexity of data to be processed. But in our system, we make compressed data and the data structure well designed which is not affected by time so that the verification is processed within 0.01 second at IBM compatible PC (CPU: 650MHz, Main Memory 64MB).
4) Security must be excellent. By recommendation of the feedback system, the signer can choose the security level of seven classes according to skillfulness of the signer.
5) The size of signature engine is small. Our engine's size is 32KB for Win9x/ME/2000, 6KB for WinCE, 6KB for JAVA virtual machine. So, our system can be used in small handy device.
6) This system can be applied to a wide range of security systems with low cost because of strong independence of input device such as electronic pen, mouse, digitizer and so on.
7) Like changing PIN number and password, user can change his signature, as he want.
8) Using dynamic information makes nearly hacking impossible.
9) Error rate is low and robust for weather, temperature, physical condition, outside noise and so on.
10) Especially in case of using PDA, Web pad, Tablet PC, Panel PC, smart-phone etc., signature security system is economical and simple because you install just our software program without purchasing any input devices.
11) Error rate (rejection rate for true signer and acceptance rate for forgery signature) is very low. (Nearly 0 for random forger)
12) Easy user interface



(Interface window for the signature register)



(Interface window for the signature verification)

5. Conclusions

We have suggested objective criteria for performance analysis and the performance results of our dynamic signature verification system. The experimental results show very accurate degree of similarity for two similar signatures, fast processing time, small signature template (feature vector) size, etc.

The importance of security is emphasized more and more at present, this system is applicable to the security of a computer, important document, the access restriction of network server, on-line shopping, credit card, military secret, national administrative security, internet banking, cyber trading, admittance to building, personal approval and so on. Government owes people to protect from an unsafe transaction in Internet. Also we have to pay attention to adopting the verification approval system teenagers to protect from the numerous immoral adult sites. This dynamic signature verification technology has been realized as one of the highly valued, useful and efficient technology for the security all over the world.

References

[1] M.C Fairhurst, "Signature Verification Revisited: Promoting Practical Exploitation of Biometric Technology," *Electronics and Comm. Eng. J.*, pp.273-280, 1997

[2] T. Hastie, E. kishon. M. Clark, and J. Fan, "A Model for signature verification," *proc. IEEE Conf. Systems, Man and Cybernetics*, pp.191-196, 1991

[3] K. Huang and H. Yan, "On-Line Signature Verification Based On Dynamic Segmentation and Global and Local Matching," *Optical Eng.*, vol.34, no.12, pp.3480-3487, 1995.

[4] F. Leclerc and R. Plamondon, "Automatic Signature Verification," *Int'l J. Pattern Recognition and Artificial Intelligence*, vol.8 no.3 pp.643-660, 1994.

[5] G. Lorette and R. P amondon, "Dynamic Approaches to Handwritten Signature Verification," *Computer Processing of Handwriting*, pp.21-47, 1990.

[6] R. Martens and L. Claesen, "On-Line Signature Verification by Dynamic Time-Warping," *Proc. 13th Int'l Conf. Pattern Recognition*, pp.38-42, 1996.

[7] M.E. Munich and P. Perona, "Visual Input for Pen-Based Computers," *PhD thesis*, Calif. Inst. Of Technology, Pasadena, Jan. 2000.
http://www.vision.caltech.edu/mariomu/thesis/thesis.ps.gz

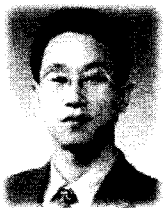
[8] B. Wirtz, "Stroke-Based Time Warping for Signature Verification," *Proc. Int'l. Document Analysis and Recognition*, pp.179-182, 1995.

[9] M.E. Munich and P. Perona, "Visual Identification by Signature Tracking," *IEEE Trans. Pattern Analysis and machine Intelligence*, vol.25, no.2, pp.200-217, Feb. 2003.

[10] R. Plamondon, and G.Lorette, "Automatic Signature Verification and Writer Identification - The state of the Art Pattern Recognition," Vol.22, No.2, pp.107-131, 1989.

[11] Mitsu YOSHIMURA, Yutaka KATO, Shin-ichi MATSUDA and Isao YACHIMURA, "On-line Signature Verification Incorporating the Direction of Pen Movement," *IEICE TRANSACTION*, VOL. E 74, NO.7, JULY, 1991.

[12] John R. Parks and Hampshire, "METHODS AND APPARATUS FOR SIGNATURE VERIFICATION," *US Patent* number 5109426, Apr.28, 1992.



Jin-Whan Kim received a BS degree in computer and statistics from Pusan National University in 1989, and MS and PhD'scourse in computer and science form Yonsei University in 1992 and Pusan National University in 2002, respectively. He is currently working as a professor in Youngsan University and as a CEO in MMiGroup Co., Ltd. His research areas are dynamic signature verification, on-line character recognition, voice processing, multi-modal biometric system and wired/wireless Internet security.

Phone : +82-55-380-9331
E-Mail : kjw@ysu.ac.kr

Hyuk-Gyu Cho received a BS degree in computer and statistics from Pusan National University in 1988, and MS and PhD'scourse in computer and science form Pusan National University in 1990 and 1992, respectively. He is currently working as a professor in Youngsan University and as a CTO in MMiGroup Co., Ltd. His research areas are information retrieval, natural language processing and text processing of bioinformatic data.

Phone : +82-55-380-9289
E-Mail : hgcho3@ysu.ac.kr

Eui-Young Cha Chareceived a BS degree in electronic engineering from Kyungpook National University in 1979, and MS and PhD in computer engineering from Seoul National University in 1982 and 1998, respectively. He is currently working as a professor of computer science department in Pusan National University. His research areas are image processing, computer vision, neural network and wavelet.

Phone : +82-51-510-2878
E-Mail : eycha@harmony.cs.pusan.ac.kr