A Study on an Advanced Evaluation Method for Dynamic Signature Verification System

Jin-Whan Kim, Jae-Hyun Cho and Kwang-Baek Kim, *Member, KIMICS*

Abstract— **This paper is a research on an evaluating method for the dynamic signature verification system. It is described about various factors such as error 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 of signature verification and so on. This study identifies factors to consider in evaluating signature verification systems comprehensively and objectively without an officially approved signature database, examines the meaning of each of the factors, and proposes criteria for evaluating and analyzing the factors.**

Index Terms— **Dynamic Signature Verification, Evaluation, User Interface Design**

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 [1]-[4].

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 [5],[6]. 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.

The rest of this paper is organized as follows: Section 2 describes the dynamic signature verification system; Section 3 describes suggested evaluation method for the DSVS; Section 4 describes conclusions.

II. DYNAMIC SIGNATURE VERIFICATION SYSTEMS

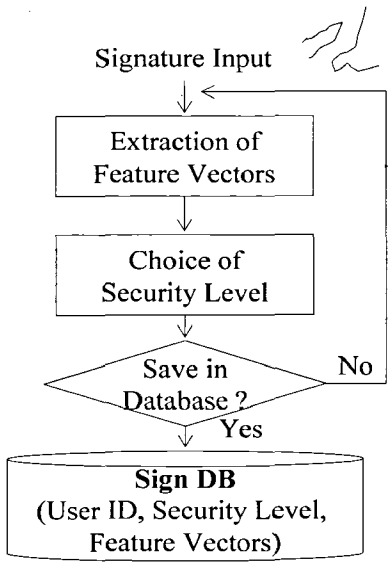
Figure 1 shows the diagram of a typical dynamic signature verification system (DSVS). DSVS, like all other biometric verification systems, involves two processing modes: registering and verifying. In the registering mode include three phases: training, testing and saving. In the training, the user provides 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.

Manuscript received February 11, 2010; revised March 1, 2010; accepted March 15, 2010.

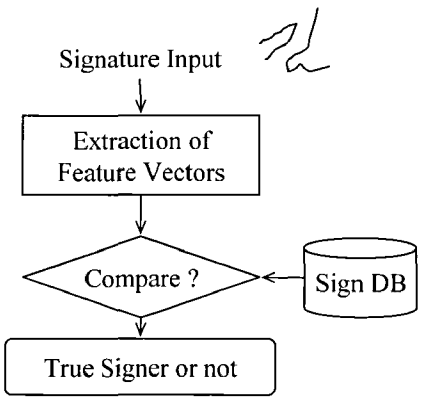
Jin-whan Kim is with the Dept. of Computer Engineering, Youngsan University, Yangsan 626-790, Korea (Tel: +82-55-380-9331, Fax: +82-55-380-9249, Email: kjw@ysu.ac.kr)

Jae-hyun Cho is with the Dept. of Computer Engineering, Catholic University of Pusan, Busan, 607-757, Korea (Tel: +82-51-510-0642, Fax: +82-51-510-0658, Email: jhcho@cup.ac.kr)

Kwang-Baek Kim is with the Division of Computer and Information Engineering, Silla University, Busan, 617-736, Korea (Tel: +82-51-999-5052, Fax: +82-51-999-5657, Email: gbkim@silla.ac.kr)



(a) Registration Processing



(b) Verification Processing

Fig. 1. Dynamic Signature Verification System

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.

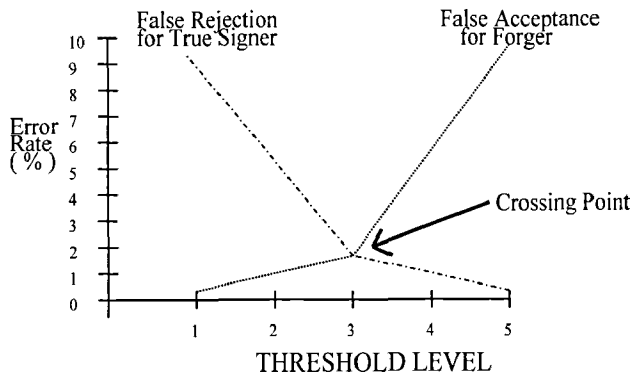


Fig. 2. Graph of Equal Error Rate

III. PROPOSED METHOD FOR THE EVALUATION OF THE DSVS

It is very important to evaluate biometric system for the user convenience and system reliability [7].

The dynamic signature verification system (DSVS) is a technology to distinguish a true signature and a forgery signature using the information about 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 absorb these 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. Figure 3 shows the user interface for enrollment of the signature. In this case, it is useful in a little wide screen.

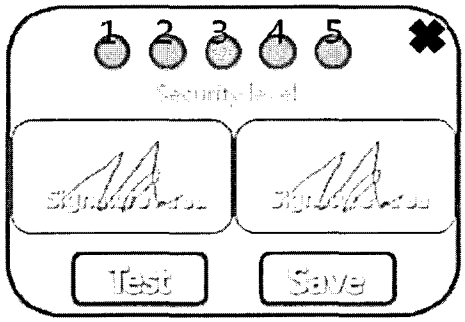


Fig. 3. User interface for enrollment of the signature

Figure 4 shows another user interface for enrollment of the signature. In this case, it is useful in a small screen like the PDA, SignPad, Smart-phone etc.

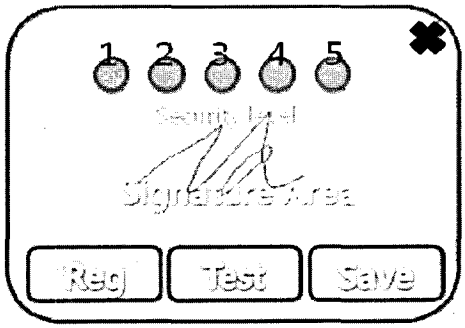


Fig. 4. User interface for enrollment of the signature

Figure 5 shows the user interface for verification of the signature. This is a general interface design.

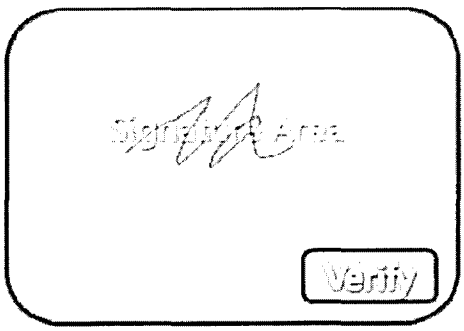


Fig. 5. User interface for verification of the signature

Figure 6 shows the user interface for verification of the signature. This is an interface design using password(PIN) and signature.

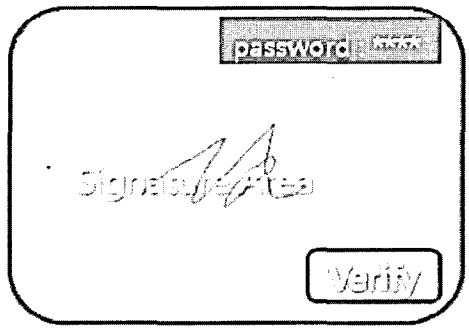


Fig. 6. User interface for verification of the signature : password(PIN)

Figure 7 shows the user interface for verification of the signature. This is an interface design using PKI (Public Key Infrastructure) password and signature. In Korea, PKI password is being widely used for Internet public/private financial transaction.

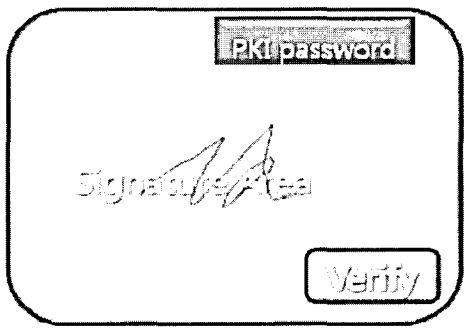


Fig. 7. User interface for verification of the signature : PKI password

Figure 8 shows the user interface for verification of the signature. This is an interface design using other biometrics technologies and signature. Nowadays, multi-modal biometrics system is being tried in wide area for high convenience and security.

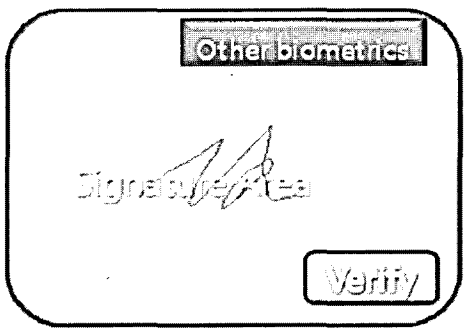


Fig. 8. User interface for verification of the signature : other biometrics

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

It needs the discriminating power of similar patterns such as figure, speed, pressure, size, gradient, stroke order, stroke position, stroke direction etc. Various algorithms including DTW(Dynamic Time Warping) and HMM(Hidden Markov Model) are being used [8]-[13].

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 Vector)

The size of characteristic vector of 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 signature characteristic vector 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

Table 1 shows the various characteristic information and corresponding weight values (W1, W2, ...).

TABLE 1.
WEIGHT OF CHARACTERISTIC INFORMATION

Characteristic information of signature	*Weight*
Speed	W1
Shape	W2
Pressure	W3
Order of stroke	W4
Number of stoke	W5
Entire time of signature	W6
Position of stroke	W7
Size of signature	W8
...	...

It is more important than anything that good characteristic information for dynamic signature verification reduces 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 performances and as a reference when a signature verification system with prominent function is developed or examined.

8. Adaptation for the various signatures

Some people use simple signatures including one or two strokes, but others use complex signatures including ten strokes or over. In any case, It must be processed consistently. Figure 9 shows the various signatures. The DSVS should provides consistent matching and a value of similarity.

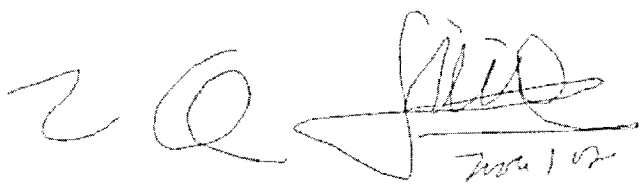


Fig. 9. Various signatures

9. Adaptation for the various environments

There are so many computing environments such that various hardware of general PC, PDA, smart-phone, cell-phone, special embedded system and various operating system of Windows, Linux, UNIX, Windows mobile, Embedded Linux, Android etc.

10. Adaptation for the various pen devices

Nowadays, many pen devices are developed throughout the world. There are simple pens such that touch pad, sign pad and pen mouse, but complex pens such that various pen digitizers tablet monitors using magnetic field and supersonic waves.

IV. CONCLUSIONS

We have suggested objective criteria (convenience, error rate, accuracy, size of signature engine, size of signature database, speed of verification process, characteristic information and weight, adaptation for the various signatures, environments and devices etc.) for

performance evaluation of the dynamic signature verification system (DSVS).

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

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

[3] Huang, K., and Yan, H.: On-Line Signature Verification Based On Dynamic Segmentation and Global and Local Matching. *Optical Eng.*, Vol.34. No.12. (1995) 3480-3487

[4] Leclerc, F., and Plamondon, R.: Automatic Signature Verification. *International Journal of Pattern Recognition and Artificial Intelligence.* Vol.8. No.3. (1994) 643-660

[5] A. Jain, L. Hong, and S. Pankanti, "Biometric Identification," *Communications of the ACM*, Vol.43, No.2, pp.91-98, Feb. 2000.

[6] J.L. Wayman, "Fundamentals of Biometric Authentication Technologies," *National Biometric Test Center Collected Works*, Ver.1.3, pp.1-19, Aug. 2000.

[7] P.J. Phillips, A. Martin, C.L. Wilson, and M. Przybocki, "An Introduction to Evaluating Biometric Systems," *Computer*, Vol.33, No.2, pp.56-63, Feb. 2000.

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

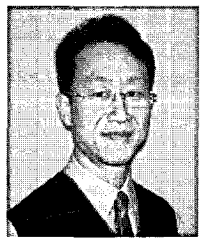
[9] Wirtz, B.: Stroke-Based Time Warping for Signature Verification. *Proc. Int'l. Document Analysis and Recognition.* (1995) 179-182

[10] Hansheng Lei, Srinivas Palla, Venu Govindaraju, "ER2: An Intuitive Similarity Measure for On-Line Signature Verification", *Ninth International Workshop on Frontiers in Handwriting Recognition (IWFHR'04)*, pp.191-195, October 2004.

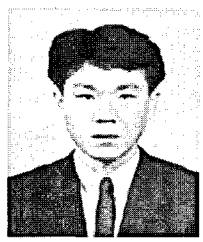
[11] Sascha Schimke, Claus Vielhauer, Jana Dittmann, "Using Adapted Levenshtein Distance for On-Line Signature Authentication", *Pattern Recognition, 17th International Conference on (ICPR'04)* Volume 2, pp.931-934, August 2004.

[12] Mohammad M. Shafiei, Hamid R. Rabiee, "A New On-Line Signature Verification Algorithm Using Variable Length Segmentation and Hidden Markov Models", *Seventh International Conference on Document Analysis and Recognition* Volume I, pp.443, August 2003.

[13] H. S. Yoon, J. Y. Lee, H. S. Yang, "An On-Line Signature Verification System Using Hidden Markov Model in Polar Space", *Eighth International Workshop on Frontiers in Handwriting Recognition (IWFHR'02)*, pp.329, August 2002.



Jin-Whan Kim received a B.S. degree in computer and statistics from Pusan National University in 1989, and M.S. and Ph.D. in computer and science from Yonsei University, Seoul, Korea, in 1992 and Pusan National University, Pusan, Korea, in 2006, respectively. He is an associate professor in Youngsan University and a CEO in MMIGroup Co., Ltd. His research areas are dynamic signature verification, on-line character recognition, voice processing, multi-modal biometric system, ubiquitous computing and wired/wireless internet security.



Jae-Hyun Cho received B.S. degree in Computer Science from Pusan National University, Busan, Korea, in 1986 and M.S. degree in Computer Science from Soongsil University, Seoul, Korea, in 1989, and Ph.D. degree in Computer Science from Pusan National University, Busan, Korea, in 1998. Since 2001, he has been a professor in Dept. of Computer Engineering at Catholic Univ. of Pusan, Korea. His research interests include Neural Networks, Image Processing and Human Visual System.

Kwang-Baek Kim received his M. S. and the Ph.D. degrees in Department of Computer Science from Pusan National University, Busan, Korea, in 1993 and 1999, respectively. From 1997 to present, he is an associate professor, Division of Computer and Information Engineering, and Silla University in Korea. He is currently an associate editor for Journal of Korea Multimedia Society and The Open Artificial Intelligence Journal(USA). His research interests include Fuzzy Neural Network and Application, Bioinformatics, Image Processing.