A New Enhanced Dynamic Signature Verification System Using Smart-phone

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

*School of Computer & Information Engineering, Youngsan University,

**School of Computer & Information Engineering, Youngsan University,

***Dept. of Computer Science, Pusan National University

*Yangsan City Gyeongsangnam-do Korea, ***Pusan City Korea

* kjw@ysu.ac.kr, ** hgcho3@ysu.ac.kr , *** eycha@harmony.cs.pusan.ac.kr

Abstract -- We propose a new enhanced graphical user interface and algorithm for dynamic signature verification using Smart-phone. Also, we suggest objective criteria for evaluating the performance of a dynamic signature verification system, which determine the authentication of signatures by comparing and analyzing various dynamic data such as shape of the signature, writing speed, slant of shape, and the order and the number of strokes for personal signatures using an electronic pen, expecting the system to be understood and utilized widely in the industrial field.

I. INTRODUCTION

Authentication security becomes a more important problem with the increasing use of the computer network and wired/wireless Internet. The biometrics technology using physical and behavior characteristics of a person is hot issue nowadays. Many different types of the biometrics technologies of a person such as fingerprint, face, iris, vein, DNA, brain wave, palm, voice, dynamic signature, etc. had been studied widely but remains unsuccessful because they do not meet the social demands. However, recently many of these technologies have been actively revived and researchers have developed new products on various commercial fields. The 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 the pen when the signer input his signature with an electronic pen for his authentication. Then the signature verification system collects various feature information mentioned above and compares it with the original one and simultaneously analyzes to decide whether the signature is a forgery or not. The prospect of the signature verification technology is very promising and its use will be wide spread in terms of economy, security, practicality, stability and convenience.

Expanded use of computer for business in most of areas makes computer related crimes unavoidable. To reduce such crimes, we have researched handwriting signature security for the wireless Internet and Smart-phone market.

Fig.1 Smart-phone

In this paper, we describe how this signature security system works when the signer signs his signature with an electronic pen of a Smart-phone. Using not only signature shape but also the various information from signer's writing speed, angles, strokes, etc., this system decides whether the signature is a forgery or not.

This technology can be applied to various security fields for electronic transactions, Internet banking system, home trading system, computer file, server and network against computer crimes as well as a door-pass of the authenticated person.

II. DYNAMIC (ON-LINE) SIGNATURE VERIFICATION SYSTEM

The signature verification system is to decide whether the signature is TRUE or FALSE. There are two ways for the system. One is to sign your signature on a paper then input it

into the system by using a digital camera or a scanner. In this case, we call off-line signature verification. The other is to sign your dynamic signature by using input devices such as an electronic pen or a digitizer and then the system obtains the dynamic information of the signature when the signer signs. In this case, we call dynamic (on-line) signature verification.

On-line signature is more distinctive than off-line system in judging a true signature or a forgery signature because the latter uses only static information while the former uses dynamic information of writing order, consuming time, pressure on the pen.

Another disadvantages in the off-line signature is that it takes time and cost to do image processing. Consequently, the on-line system is preferred in terms of error rate, speed, cost and so on.

To describe the on-line system, we can classify the system into several processes. To compare a true signature with a forgery signature, variation range of each signature have to be reduced and feature points are subtracted. To verify an authentic one, the feature information will be registered. To calculate the degree of similarity, a comparing process will be done. To verify a true signature or not, a decision process will be needed.

The characteristics of our on-line signature verification system is as follows:

(1) Error rate (rejection rate for true signer and acceptance rate for forgery signature) is very low

(2) Dynamic Time Warping (DTW) well known for excellent pattern matching algorithm has been modified and applied to this system.

$$G(i,j) = \min \begin{vmatrix} G(i-j-1) * d + w \\ G(i-1, j-1) * d \\ G(i-1, j) * d + w \end{vmatrix}$$

d : difference between two features

w : weight value for not diagonal comparison ($i \neq j$)

G(i, j) : accumulated value for similarity between two signatures

Reliability for checking the similarities of the signatures is high and a newly developed fast algorithm in processing time is adopted in the system. To make access easier, we considered an efficient user interface design in Fig. 3 and Fig. 4.

(3) Database for the signature is very small. It needs 20byte-500byte of memory capacity to register feature information of a signer.

(4) Processing time must be fast for the verification. In the general DTW system, it is good to check similarity between patterns, but it has defect to make processing time because of the computational 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.

(5) Security must be excellent. By the recommendation of the feedback system, the signer can choose the security level of seven classes according to skillfulness of the signer.

(6) The size of the signature engine is small. The size of our engine is 6KB for WinCE and JAVA. So, our system can be used in small handy device like a smart-phone.

(7) Like changing PIN number and password, signer can change his signature if he wants.

(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) The signature security system using a smart-phone is economical and simple because you can just install signature verification software without purchasing any signature input devices.

(11) The signer's training and efforts are needed for the higher security level of the signature system.

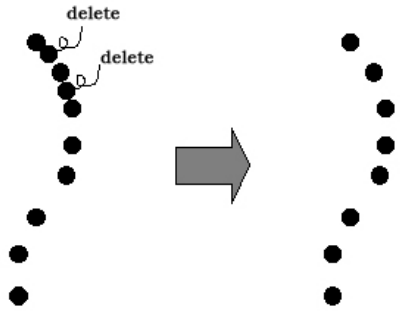
1. The preprocess

The signing varies as the age, time, habit as well as psychological and physical condition. This preprocessing is the part to reduce the variation occurring during signing the signature. It consists of a noise reducing process, re-sampling process, normalizing process and so on.

-Noise reducing process is to reduce or remove the noise produced from the surface slip on the input device or hand trembling during signing the signature.

-Re-sampling process is to speed up the processing time in the comparing process by reducing the number of coordinate points in case there are too many input coordinates as you see in Fig. 1.

-Normalizing process is to handle the variance of the size and slope of signature.



Signature before the preprocessing | Signature after the preprocessing

Fig. 2. Signature before and after the preprocessing

2. Feature extraction process

We introduce useful feature points in on-line signature verification system. Finding out the best method to calculate the degree of similarity is very important, and the previous approach for that is to select and arrange distinctive points. For the best signature verification, it is important to reduce the range of variation of true signature and extend distinctiveness between true and forgery signature. Assigning the adequate weight for the every feature is another important point.

The useful feature points are below:

- Speed, velocity, acceleration, pressure information
- Shape of coordinates, direction and slope between two points
- Number of pen down/up points
- Information of pen down/up movement
- Total time taken in signing
- Pen down/up time between strokes
- Number of strokes
- Total number of coordinates

Our system uses mainly directions and absolute distances (Fig. 3) between two points for the pen down/up strokes.

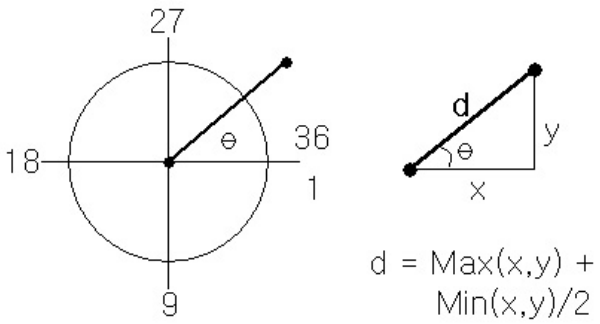


Fig. 3. Signature features of direction and distance

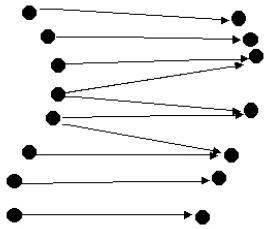
3. Comparison process

In the comparison process, we compare an input signature with the registered signatures to calculate the degree of similarity. The degree of similarity is the key to decide if the signature is a forgery or not. Dynamic programming, Hidden Markov Modeling, Neural Network are main methods to calculate the degree of similarity. In this paper we use the revised dynamic programming method.

The direction and distance between the two points are used as main distinctive elements by assigning them the appropriate weight acquired from experiments. Because these two features have important information including speed, shape and so on.

Also considering pen-up components, the number of strokes and relationships between the strokes are used to calculate the degree of similarity. Fig. 4. Below are the distinctive points of Pattern A corresponding to Pattern B.

-Pattern A= A1, A2, A3 .....An (n feature points)
-Pattern B= B1,B2, B3.....Bm (m feature points)



Signature Pattern A Signature Pattern B

Fig. 4. Comparison of the feature points of signatures

4. Signature registration process

Registration process is the stage to store signatures of the signer into the signature database. Fig. 5 shows the user interface to register signature. Signer signs his signature and then click 'Register' button. The Signer signs same signature one more time and click 'Test&Verify' button to see the degree of similarity

If the degree of similarity were a little high then the signatures would be approved as skilled signer and the signer can move to next stage for final test and checking his security level. After the signer test with his signing and security level several times, finally the signer registers his signature into the signature database.

The signer can choose the security level according to his needs (secret: 1, important: 2 average: 5 low: 7) and tests many times. If the signer satisfies, he can press the 'Save' button to store his signature's feature information and the value of the security level into database.

One important thing is the number of standard signatures to register. If you must register too many standard signatures it occurs inconveniences in the registration process and more memories are required. If less number of signatures is registered, it will be convenient in registration and smaller amount of memories are required. In our system we use one signature as the standard signature.

We reduced inconveniences in registration process and require only 60-500 bytes of memory capacity per person. The result of inspection is satisfactory.

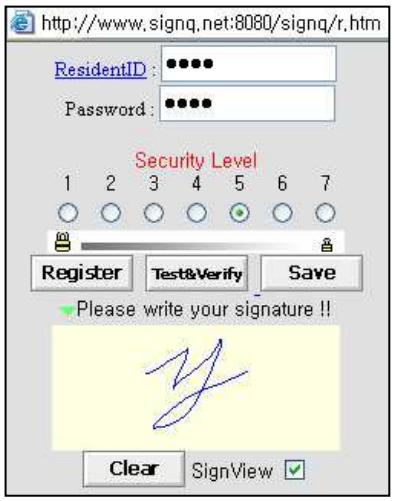


Fig. 5. Signature registration window

5. Signature verification process

Using the degree of similarity between the registered standard signature and the input signature obtained from the comparison process and the security level chosen by the signer, The final decision is made if the signature is a forgery or not.

Fig. 6 shows user interface to get the verification result if the signer is the right person. In this process if the signer is proved to be the right person, the certain authority will be given. If the signer does not want his signature to appear on the screen, he can control with 'SignView' button.

Fig. 6. Signature verification window

6. Evaluation of accuracy

As shown in Fig. 7, 8, 9 and 10, comparison algorithm has to calculate precisely minute changes of two patterns according to the complexity or simplicity of the signature's patterns,.

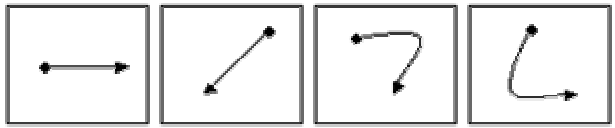


Fig. 7. Very simple signature patterns

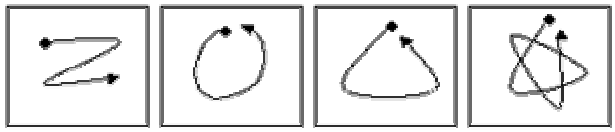


Fig. 8. A little simple signature patterns

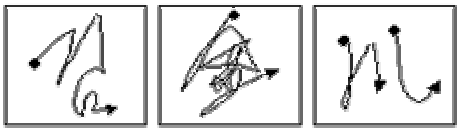


Fig. 9. Simple signature patterns

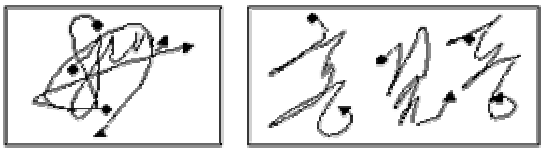


Fig. 10. Common signature patterns

As in Fig. 11 and 12, the algorithm to determine the discriminating power about direction of elements and minute difference of figures has to be applied.

Fig. 11. Discriminating power about direction of elements

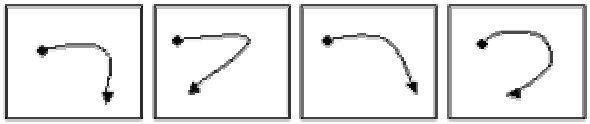


Fig. 12. Discriminating power about minute difference of figures

As in Fig. 13, 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 shouldn't be ignored.

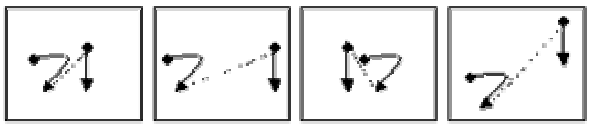


Fig. 13. Discriminating power about direction of pen up elements and minute difference of length

As in Fig. 14, if the order of stokes is different, the dynamic signature verification system, which puts high value on order information even through the apparent figure is almost same, should have the discriminating power.

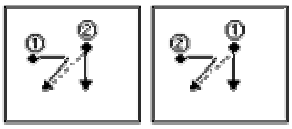


Fig. 14. Discriminating power when the orders of stroke are different

As in Fig. 15, as for the information about the slant of the whole signature that can be resulted from the change of the signature location, it would be desirable to use it as a characteristic information of the signature in the case that security is prior to convenience.

Fig. 15. Discriminating power when slants are different

As in Fig. 16, when the entire sizes of two signatures are different, it would be better to ignore them for convenience (to reduce false reject 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 a characteristic information.

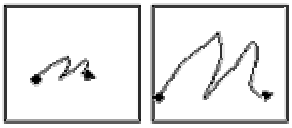


Fig. 16. Discriminating power when the size of signature is different

As in Fig. 17 and 18, not the change of entire sizes 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 numerical value has to be applied.

Fig. 17. Discriminating power when the sizes of some parts in signature are different

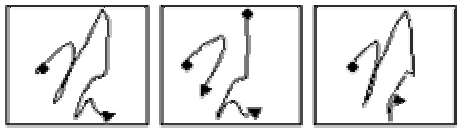


Fig. 18. Discriminating power when the figures of some parts in signature are different

III. APPLICATION FIELDS

This technology is applicable to various areas for the enhanced user authentication security than existing method such as the PIN, password, simple key and card for entrance. Mobile electronic payments for various goods of shopping mall, cartoon, movie, ticket, music etc. and transactions are increased.

The various application fields are as follows:

Internet (Wired / Wireless / Mobile)
-VPN (Virtual Private Network)
-Internet Banking
-Internet HTS (Home Trading System)
-Virtual University LOGIN
-EC (Electronic Commerce)
-Client/Server
-Electronic Approval
Electronic Money Transaction
-ATM (Automated Teller Machine)
-Electronic Money
-Credit Card Reader
Computer (PC, PDA, WebPad, Tablet PC, Panel PC)
-Data, Program, File Access.
-LOGIN
Business
-Safer Security
-Admittance for Building Entrance
Health Care
-Electronic Prescription
Combination with other security technology for more reliable, flexible security system
-Password, Signature, Voice, Fingerprint, Iris, Palm, Vein, DNA, Brain Wave, etc.

IV. CONCLUSIONS

On-line (dynamic) signature verification system tells true signature from forgery ones. While the signer input his signature with an input device such as an electronic pen, our system analyzes and extracts feature information from the

dynamic signature data and verifies whether the signature is a forgery or not by analyzing the dynamic information of the signer such as writing speed, writing order, elapsed time and pen up/down etc.

In previous techniques, the signature appears on the monitor when the signer signs to verify. In our system, the signature to be verified does not appear on the monitor. Thus the possibility of the danger to be stolen is reduced.

In the registration process of previous technique, the signer can sign his signature to register without any restriction. In our system, the signer signs his signature one time in advance to check the signatures (the angle, shape, number of strokes, writing order, speed, etc.) each other. Then the system decides if the signature will be permitted for the registration according to the degree of similarity.

The system was designed to induce the signer himself to sign his signature consistently so that the system becomes more efficient and the degree of security is enhanced. As a result, the imitation is nearly impossible.

The importance of security is emphasized more and more at present, our 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.

Finally, we provide online test of our dynamic signature engine "SignQ". You can test our various version such as WinCE, Windows 9x/NT/2000/XP, JAVA, ActiveX at http://www.mmigroup.net/en/mmi_products_signq.php.

REFERENCES

[1]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.

[2]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.

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

[4]M. Parizeau and R. Plamondon, " A Comparative Analysis of Regional Correlation, Dynamic Time Warping, and Skeletal Tree Matching for Signature Verification," IEEE Trans. on PAMI, vol. 12, no. 7, pp.710-717, Jul. 1990

[6]R. Plamondon and M. Parizeau, "Signature Verification from position, velocity and acceleration signals: A comparative study," Proc. 9th Int. Conf. Patt. Rec. pp.260-265, 1988

[7]R. F. Farag and Y. T. Chien, "On-line signature verification," Proc. Conf. on On-line Interactive Comput. pp.403, Brunel University, London, 1972