MULTIBIOMETRICS AUTHENTICATION IN POS APPLICATION

Chunlei Yang[1], Guiyun Tian[2] and Steve Ward[2]
[1] LeuchTek GmbH, Hans-Henny-Jahnn-Weg 17, D-22085 Hamburg, Germany
[2] University of Huddersfield, Queensgate, Huddersfield HD1 3DH, UK

ABSTRACT

In traditional Point of Sales (POS) device, the legitimate user is mainly authenticated by PIN (Personal Identification Number). PIN method has drawbacks like easy to be forgotten. Fingerprint technology, as the most viable biometrics in the special and restricted hardware environment of POS device, has been used to increase user convenience. However, due to inherent problems, fingerprint alone can hardly replace PIN in many high secure applications. Although keystroke pattern as one kind of biometrics is in research for years, no real satisfied results have been got due to its inherent great variability. In this paper, we proposed an innovative method by adapting and increase keystroke pattern technology to POS device and applications. Together with fingerprint system, the adapted keystroke pattern recognition system constitute a multibiometric system, which helps achieve an increase in performance, and provide anti-spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously. Since this approach is a combination of partially feature-based and partially knowledge-based, it can be a more deployable alternative to strengthen existing PIN and pure biometric authentication methods. Experimental results support that this approach can be better trade-off of the security and user convenience.

Keywords Biometrics, Point-Of-Sales, Keystroke pattern, Security

1 INTRODUCTION

In most of current POS (Point-of-Sales) devices, the legitimate user is mainly authenticated by two factors: payment card as token-based security factor, and PIN (Personal Identification Number) as knowledge-based security factor. After the smart or magnetic card is inserted into a POS device, for user verification purpose, a correct PIN is required to input from the keypad.

The well-know problem of PIN authenticated method has drawbacks like easy to be forgotten. Biometrics technology, as feature-based authentication method, has advantages of "not being lost or forgotten, unique", it can dramatically increase user convenience. Therefore it is increasingly used in security field. Figure 1 illustrates two samples of POS devices with/without fingerprint sensor.

Compared with other biometrics like face, iris and hand geometry recognitions, fingerprint has the feature of convenience, proven, miniaturization and inexpensive, thus it has the best potential for mass-market application like in POS devices [1] to replace PIN in some authentication applications. However, fingerprint solely can hardly replace PIN in many high secure applications. Fingerprint has its own limitations. For example, the National Institute of Standards and Technology (NIST) reported that it is not possible to obtain a good quality fingerprint from approximately two percent of the population. In the fact, as analyzed in paper [2], fingerprint system solely is not quite trustable and exists many security risks.

One solution to strengthen the security of biometric system is to build multibiometrics system. Multibiometric system refers to the fusion of multiple biometric indicators, e.g. detecting face, voice, signature together to identify a person. Multibiometric systems provide anti-spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously. Multibiometric systems have been also approved to be able to help achieve an increase in performance that may not be possible using a single biometric indicator [3].

How to build a multibiometric system based on the limited available resources of POS device? Prior researches in computer security have supported, each user has his/her unique keystroke behavior, or called keystroke pattern. Keystroke pattern is a biometric that identifies an individual based on their unique typing rhythm. Unfortunately the existing research results on keystroke pattern are not suitable

for payment terminal applications because of its inherent great variability. More details of keystroke pattern will be discussed later in Section 2.

This paper proposes a novel method of adapting the keystroke pattern to POS applications. This approach is a hybrid of knowledge- and feature-based authentication. It increases the security but also user convenience. By working together with fingerprint, a keystroke pattern recognition system can be built based on limited resource to become a more promised method to strengthen PIN.

The rest of this paper is organized as following: Section 2 is literature survey of strokes biometrics. How to adapt keystroke pattern into POS is studied. Section 3 presents the preliminary experimental system and test results. Conclusion and future worked are summarized in Section 5.

2 ADAPT KEYSTROKE PATTERN INTO POS APPLICATIONS

In this section, first we conduct a quick literature survey of keystroke pattern for the verification applications. Latter a proposal of improvement and adaptation to payment terminal is presented.

2.1 keystroke Pattern

Keystroke pattern, is an approach as behaviour biometrics used to verify the identity of an individual by examining his/her keystrokes on a keyboard or keypad. The premise behind this protection layer is that each individual exhibits a distinctive pattern and cadence of typing. As early as 1980, researchers have been studying the use of habitual patterns in a users typing behaviour for identification. Gaines et al. investigated the possibility of using keystroke timings for authentication [4]. Later more studies have been done. Keystroke pattern is known with a few different names: keyboard dynamics, keystroke analysis, typing biometrics and typing rhythms [5, 8-11].

Most studies have used durations between keystrokes (latencies) as features for user verification, but some have also used keystroke durations (the time a key is held down). Used classification methods include traditional statistic techniques, Bayesian classifiers, neural networks and fuzzy systems. Bleha et al. [5] tried using a detecting the keystroke pattern of users' "username" for user verification and reached FRR 8.1% and FAR 2.8%. Obaidat and B. Sadoun [6] made a comprehensive study of different classification methods that can be used with keystroke pattern. It was noted that keystrore durations gave better results than latencies between keystrokes, but using both measurements together gave the best results. Best results was achieved by neural methods of Fuzzy ARTMAP (a generalization of adaptive resonance theory networks (ART) with fuzzy set theory operations), RBFN (Radial Basis Function Network) and LVQ (Learning Vector Quantization).

Unlike other biometric systems which may be expensive to implement, the attractive advantage of keystroke pattern is that it requires almost no extra hardware expense—the only hardware required is the keyboard. Nevertheless, user authentication through keystroke characteristics remains a difficult task. The reason is quite understandable: physiological features such as face, retinal and fingerprint patterns are strongly stable over time, unlike behavioural features such as writing and keystroke pattern [7].

Some conclusion can be made based on previous works. Keystroke authentication requires typing in a relatively long segment of text to get distinct features. For the people works daily before computer, and for well-known, regularly typed strings, better recognition results can be gotten. Thus currently the main application of keystroke pattern is proposed as an auxiliary authentication technique in computer network security, rather than as the normal method for user authentication.

2.2 Adapt the keystroke pattern to POS application

As illustrated in Figure 2, a high level security system needs base on "three-factors": token-factor (e.g. a card), knowledge-factor (e.g. PIN) and features-factor (e.g. fingerprint, keystroke pattern). There is no possible to replace one by another entirely. Theoretically, even a perfect biometrics system can also not completely replace the knowledge-base authentication method, e.g. PIN.

POS device and its applications have specialties. First, different from computer keyboard, the keypad of POS device only has numerical keys (0-9) and very few command keys (Enter, Clear, Cancel). As a matter of fact, the layout and position of the numerical keys are strictly specified by standards (Refer to Figure 1). Secondly, the number of key strokes is highly limited, typically 4-6 keystrokes, which means

only very few features are available for keystroke pattern analysis. Thirdly, it even has higher security requirements because it directly deals with money. Due to the reasons given above, to apply authentication based on a natural (unintentional) keystroke pattern will be unfeasible in the POS applications. However it will be relatively easier if users want to intentionally build his/her special typing patterns. Such deliberated typing patterns can be more consistent and distinguishable, thanks to the features of POS applications, namely a simple and fixed layout and limited number of keystrokes.

We proposed a system as illustrated in figure 3. It consisted of fingerprint and keystroke pattern systems. Each system generates a match similarity score for final decision. In the keystroke pattern system, users were asked to deliberately build a special pattern according to his/her preference, e.g. stop on a special key for a long time. This special typing pattern will be recorded for latter auxiliary authentication.

The deliberately built typing patterns actually are no long purely belong to the traditional defined biometrics, which refer to natural features or behaviors. User must intentionally to memorize some special behaviour. Therefore, it is already a combination of feature-based security factor and knowledge-based security factor. Thanks to this hybrid feature, it offers the possibility to better replace the PIN method which is knowledge-base methods.

To make better trade-off between security and user convenience, the new authentication procedure can be outlined as below:
1).During enrolment mode, a prompt (message) which helps to memorize the keystrokes and pattern can be defined by user themselves.
The prompt could have direct or indirect connections with the real keystrokes. Rather than defining a PIN as an arbitrary sequence, this new method allows users to input and define their authentication method in a more natural and memorable way.

2).The prompt will be shown on the display, only after the fingerprint matching score is above preset threshold. Referring to the prompt, user inputs some keystrokes.
For instance, after the fingerprint matching score exceeds 25, a prompte is showed on the terminal display, e.g. "1234", the user can tying in with predefined typing pattern. Key "1"(hold 50ms)-(release for 80ms)-"2"(hold 60ms)-(release for 150ms)-"3"(hold 65ms)-(release for 80ms).
Furthermore, to increase the security level again, user can input keys other than prompt messages (but corresponding to the enrolment template). That means, although the prompt is "1234", user can input "5678" according to his knowledge of his template.

3).The keystrokes and pattern will be analysed to matching the template, and generate a matching score. That means, even the impostor knows the keystrokes should be „1234", due to the wrong typing pattern , the impostor still have difficulties to access.

4).The system carries out a fusion analysis based on the keystrokes score as well as fingerprint score to make a decision.

5).The template has self-learning function. After successful accesses, the template will be modified slightly to adapt some natural changes of users typing pattern. After five failed tries, system will be locked.

This procedure is similar to traditional PIN input thus it can be quite acceptable. Whatever, to remember some simple behaviours is easier than to memorize a real PIN, especially with the assistance of prompt message. Additionally, in case the keystroke pattern is disclosed, it can be updated (which normal biometrics lack this feature).

2.3 Classification and verification

Both keystrokes latencies and duration are acquired to build N-dimensional feature vectors for keystroke pattern analysis. Let R = $[r_1; r_2; : : : ; r_N]$ and U= $[u_1; u_2; : : : ; u_N]$, R represents the reference vectors (template) and U represents unknown feature vectors. Then the following classifiers were used for recognition.

- Euclidean distance measure
"Similarity" is based on the Euclidean distance between the pattern vectors. Euclidean distance between the two N-dimensional vectors U and R, is defined as:

$$D(R,U) = \left[\sum_{i=1}^{N} (r_i - u_i)^2 \right]^{\frac{1}{2}} \quad (1)$$

$i = 1, 2, 3 \ldots N$, where N = number of pattern vectors.

- Probability and weighted probability
Let U and R be N-dimensional pattern vectors as defined previously. Furthermore, let each component of the pattern vectors be the quadruple (μ_i, σ_i, o_i, x_i), representing the mean, standard deviation, number of occurrences, and data value for the *i*th feature. The score can be calculated [3] between a reference profile R and unknown profile U as:

$$Score(R,U) = \sum_{i=1}^{N} \frac{1}{O_{u_i}} \left[\sum_{i=1}^{o_{u_i}} \Pr ob\left(\frac{X_{ij}^{(u)} - u_{ri}}{\sigma_{r_i}}\right) \right] \quad (2)$$

O_{ui} – number of occurrences of u_i
$X_{ij}^{(u)}$ – value of j^{th} occurrence of u_i
μ_i – mean of the *i*th of u_i

Since paper [7] indicated that keystroke durations gave better distinct features than latencies between keystrokes. Thus we gave higher weights on keystroke duration than that of keystroke latencies. In our experiment we assign the preliminary weight of keystroke duration $W_{du} = 0.6$ and the weight of keystroke latency $W_{la} = 0.4$. The score was calculated as (3) where $i = 1 \ldots \frac{N}{2}$.

$$Score(R,U) = \sum_{i=1}^{2i-1} \frac{W_{du}}{O_{u_i}} \left[\sum_{i=1}^{o_{u_i}} \Pr ob\left(\frac{X_{ij}^{(u)} - u_{ri}}{\sigma_{r_i}}\right) \right] + \sum_{i=1}^{2i} \frac{W_{la}}{O_{u_i}} \left[\sum_{i=1}^{o_{u_i}} \Pr ob\left(\frac{X_{ij}^{(u)} - u_{ri}}{\sigma_{r_i}}\right) \right] \quad (3)$$

3 PRELIMINARY EXPERIMENTAL RESULTS

After a prototype system was built, 15 people were invited to join preliminary keystroke pattern tests. They were divided into two groups: group A (5 members) and group B (10 members). Group A was regarded as genuine user and group B was regarded as impostor.

In our experiment, we only tested the extreme cases: assume impostor had already known which keys and the consequence need to be stroked, but the impostor didn't know the user typing pattern. Meanwhile, the prompt message was identical for all users (instead of the user can define the prompt by themselves). A progress bar, which is controlled by 100ms timer, is shown on display as reference to help user manage the duration and latency time. An example is given in figure 4.

During enrolment, group A members were asked to design individual tying patters but should not tell others. After 10 times keystrokes, a typing pattern template was build. Testing data was recorded in 15 deferent sessions separated by at least 3 days. Each participant in each session inputs 3 times keystrokes as in Table 1. In group A, are used to attach others. Thus totally more than 4075 data were recorded.

Our experiments base on the hypothesis that the impostors know the PIN. Although the results in table 1 are not very encouraging, if the keystroke pattern is used as additional authentication method to PIN and fingerprint authentications, actually the system security can be improved a lot.

4 CONCLUSIONS UND FUTURE WORKS

We proposed a novel multimodal biometric system, which integrates fingerprint and keystroke pattern recognitions to strengthen the PIN authentication. The new method bases on deliberately built keystroke pattern has hybrid knowledge-based and feature-based characteristics, thus it can better replace traditional PIN method and increased user convenience as well. Preliminary experimental results demonstrate that the verification established by such an integrated system is more reliable.

To improve the performance, we work on bringing fuzzy logic into our application. Fuzzy logic offers a mathematical theory and logical notation to manipulate the uncertainties found in natural language and natural processes. Because the keystroke pattern belongs to behavior pattern and has uncertainties, we believe that fuzzy logic can better satisfy the requirements.

REFERENCES

[1] George Walner. A biometric solution is ideal at the point of sale, Biometric Technology Today, Volume 10, Issue 3, 31 March 2002, pp. 7-8.
[2] Chunlei Yang, Guiyun Tian and Steve Ward. *Biometric based smart card for security.* In Proceedings of 2nd International Conference on E-Business and Telecommunication Networks (ICETE 2005), Reading, UK, October 2005. pp. 49-56.
[3] Fabian Monrose and Aviel D. Rubin. *Keystroke dynamics as a biometric for authentication.* Future Generation Computer Systems 16 (2000) pp.351–359.
[4] R. Gaines, W. Lisowski, S. Press, N. Shapiro. *Authentication by keystroke timing: some prelimary results.* Rand Rep. R-2560-NSF, Rand Corporation, 1980.
[5] Bleha, S., Slivinsky, C., Hussien, B. *Computer-access security systems using keystroke dynamics*. IEEE Transactions on Pattern Analysis and Machine Intelligence 12 (1990) pp. 1217–1222.
[6] Obaidat, M.S., Sadoun, B. *Verification of computer users using keystroke dynamics.* IEEE Transactions on Systems, Man and Cybernetics 27 (1997) pp. 261–269.
[7] Francesco Bergad Ano, Daniele Gunetti and Claudia Picardi. *User Authentication through Keystroke Dynamics.* ACM Transactions on Information and System Security (TISSEC). Volume 5, Issue 4 2002. ISSN:1094-9224. pp.367 – 397.
[8] Anil K. Jain, Sarat C. Dass and Karthik Nandakumar. *Can soft biometric traits assist user recognition?* Proceedings of SPIE Defense and Security Symposium, Orlando, April 2004.
[10] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman and A. K. Jain, *FVC2004: Third Fingerprint Verification Competition,* Proc. International Conference on Biometric Authentication (ICBA), Hong Kong, July 2004. pp. 1-7.
[11] R. Joyce and G. Gupta. *Identity Authentication Based on keystroke Latencies.* Communications of ACM, Vol. 33, No. 2, pp. 168-176, February 1990.

Figure 1: Example of POS device from Ingenico (a) without fingerprint sensor (b) with fingerprint sensor

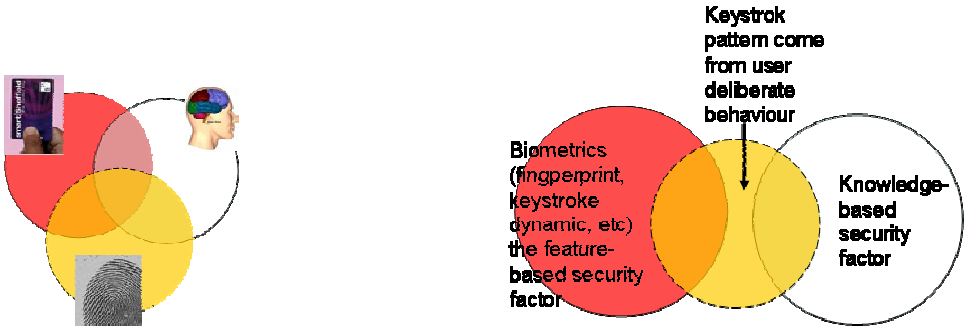

Figure 2: (a) Three factors constitute the highest level of security system: token, knowledge and feature. (b) Deliberate keystroke represents a combination of feature based and knowledge-based factors

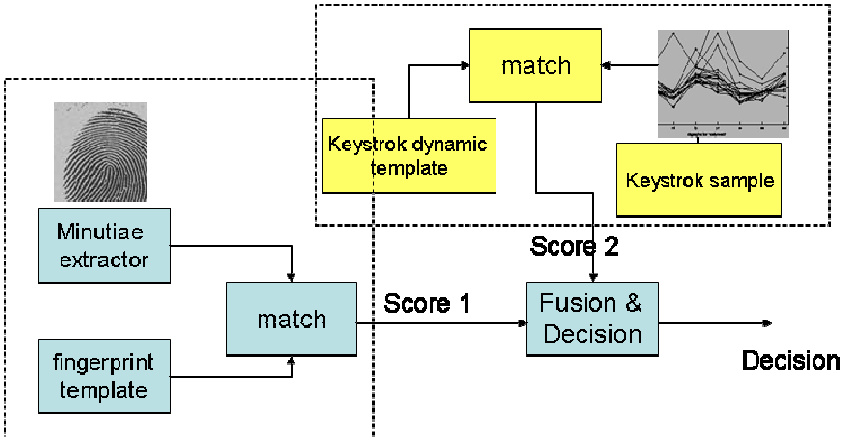

Figure 3: System structure diagram

Figure 4: Example of prompt, timer bar and real keystrokes

Total attempts	Keystrokes	Feature Dimension	FAR	FFR
675	222	7	3.8%	7.5%
675	123	7	3.4%	8.2%
675	649	7	3.9%	8.7%
675	55555	11	3.6%	9.5%
675	12345	11	3.2%	8.2%
675	67853	11	2.9%	7.9%

Table 1: tested keystroke and result