A NOTE ON BIOMETRICS-BASED AUTHENTICATION WITH PORTABLE DEVICE

Shinsuke Ohtsuka[†], Satoshi Kawamoto[‡], Shigeru Takano[‡], Kensuke Baba[‡] and Hiroto Yasuura[†]
Graduate School/Faculty of Information Science and Electrical Engineering, Kyushu University
Motooka 744, Nishi-ku, Fukuoka, 819-0395, Japan

Keywords: Biometrics, authentication, mobile system, spoofing.

Abstract: Individual authentication technologies are essential for electronic systems as social infrastructures. Especially, biometrics-based authentication has been receiving increasing attention and is expected to be implemented on systems with portable devices such as mobile phones for realizing more useful services. The most important problem in biometrics-based authentication is to prevent a leakage of biological information. This paper focuses on the leakage which enables a spoofing and consider two cases, a leakage from data stored in a server for verification of biological information and a leakage by a cheating detection. This paper proposes a solution by applying a function to biological information and shows the properties required for the function to solve the problem. Moreover, this paper proposes an idea of biometrics-based authentication system with portable devices which is provided a function to capture biological information.

1 INTRODUCTION

Personal authentication has been one of the most important and fundamental techniques in our life as personal identification has become more common because of the requirement of certification of ATM cards, management of entering and leaving room or buildings, airport security system, and so on. Especially, as one of the techniques for identifying a person, biometrics-based authentication has attracted attention among many researchers in cryptography and computer security. This technique identifies a person by analysis of his/her physical characteristics which are called "biometric information" and is generally considered to be able to develop robust system against counterfeit attack thanks to their uniqueness and permanence. Furthermore, by introducing biometric authentication to a system based on mobile terminal devices and the internet, more useful and effective services can be rendered to the users for mobile communications.

One of the most important problem in biometric authentication is to prevent the leakage of biometric information. To solve this problem, we have to pay attention to privacy concerns. Moreover, we need to be concerned that it is possible to create a counterfeit of a part of a living body (Matsumoto et al., 2002). In a certain authentication, a "prover" is the entity which is to prove that s/he is a particular user and a "verifier" is the entity which is to verify the proof. Here we assume that secure communications including destination certifications are available by proper cryptographic technologies. And then, we do not consider the leakage of biometric information in daily life which is not concerned with procedure for personal authentication. And yet, under the above assumptions, it is conceivable that we can easily produce the leakage of biological information by guessing from verifier's information or biometric observation by fake verifier.

We propose the following method for solving the above problems. First, about the leakage of biometric information by guessing from verifier's information, we can solve it by applying the idea of "cancellable biometrics (Ratha et al., 2001)". Now, we assume the case that the prover registers biometric information, which is observed in advance, as a "template" to the verifier. The main idea of cancelable biometrics is to apply a transformation, which is difficult to reconstruct the original information, to the observed bio-

Ohtsuka S., Kawamoto S., TakanoâĂą S., BabaâĂą K. and YasuuraâĂă H. (2008).
A NOTE ON BIOMETRICS-BASED AUTHENTICATION WITH PORTABLE DEVICE.
In *Proceedings of the International Conference on Security and Cryptography*, pages 99-102
DOI: 10.5220/0001927300990102

metric information so that the template can be cancelled. In short, by the transformation, the original biometric information remains secure even if there is a leakage of the template by security attacks. However, by pretending to be the verifier and observing the living body directly, one can obtain the original biometric information before the transformation is applied. This problem can be solved by using a mobile terminal with an ability for the biometric observation. If the mobile terminal is managed by a prover and the malware threat can be prevented, by applying an irreversible transformation to the observed biometric information on this terminal, one cannot reconstruct the original information by using every output of the terminal.

Firstly, in this paper, we propose a model of biometric-based authentication for the purpose of clarifying the above problems. In our proposed model, to consider the possibility of an unjust observation of biometric information, "scanner" is expressly formulated as an entity collecting biometric information by analyzing human body. To prevent the leakage of biometric information from the verifier's information, we have some requirements for the transformation which is applied to the biometric information. These requirements are corresponding to the property of the transformation to realize cancelable biometrics in the paper (Ratha et al., 2001). By applying such a transformation to the biometric information under the management of the prover, the effect is useful clearly for an unjust biometric observation.

This paper shows clearly that our approach can prevent the leakage of biometric information by using cancelable biometrics. Then, applying our method to a biometric-based authentication based on mobile terminal, we also illustrate to have the effect to prevent another possible type of leakage. Finally, we discuss the implementation about our method and present the problems of the biometric-based authentication using mobile terminal.

2 MODELING BIOMETRICS-BASED AUTHENTICATION

In this section, a model of biometrics-based authentication is introduced to bring out the problem we tackle in this paper. Σ and N denote the alphabet and the set of nonnegative integers, respectively.

2.1 A Model

In this paper, we consider identification of a user as authentication. Each of the users who can be a target of authentication is denoted by $u_1, u_2, \ldots \in U$. In a trial of authentication, a *prover* is the entity which is to prove that the prover is a particular user and a *verifier* is the entity which is to verify the proof. We consider a model with a single verifier in the rest of this paper. The atomic procedure of authentication is that the prover submits a string w to the verifier, and the verifier decides who the prover is in U.

A key feature of our model is that biological information as digital sequences is distinguished from the living body of a target user, which enables us to examine leakage of biological information from a cheating scanner which detects biological information. The following argument does not depend on a kind of the part of a living body for biometrics-based authentication, therefore we regard a *living body* as the user who has it. A piece of *biological information* is a string over Σ and the set of the pieces of biological information of $u_i \in U$ is $B_i \subset \Sigma^*$. For $R \subseteq N$, a *scanner* is a function $f : U \times R \to \Sigma^*$ which outputs a piece of biological information from a living body and a variable. Intuitively, this is modeling the situation that several kinds of biological information (in a sense of digital sequences) can be detected from a single living body. Then, the protocol of authentication is the following.

Protocol 1. (1) *The prover puts* $u \in U$ *on the scanner;*
(2) *the scanner computes* $f(u,r)$ *for an* $r \in R$*;*
(3) *the scanner sends* $f(u,r)$ *as* w *to the verifier;*
(4) *the verifier regards the prover as* $u_i \in U$ *if and only if* $w \in B_i$.

In the previous protocol we are considering identification with no "ID", that is, the verifier does not know who the prover is (or insists) at the step (4). In the case where the prover sends his ID first, u from the step (1) to (3) are replaced to u_i.

Now, we ignore a decline of an accuracy of authentication which is caused by the obscurity of biological information.

Assumption 1. *For any* $1 \leq i, j \leq |U|$, $B_i = \{ f(u_i, r) \mid r \in R \}$ *and* $B_i \cap B_j = \emptyset$ *if* $i \neq j$.

In practical systems of biometrics-based authentication, biological information as purely scanned data is usually large, and hence it is not practical that the verifier holds the B_i to examine whether $w \in B_i$. The straightforward method to solve this problem is considering a function g which is defined by an idea of a distance on strings and a threshold c with respect to a string t_i. t_i is called a *template* of u_i. Now, we ignore a decline of an accuracy of authentication which

is caused by definition of a template and a distance on strings.

Assumption 2. *There exist* $g : \Sigma^* \times \Sigma^* \to N$ *and* $c \in N$ *such that* $\{b \mid g(t_i, b) \leq c, b \in \Sigma^*\} = B_i$ *for any* $1 \leq i \leq |U|$.

2.2 Problems

The problem we consider is a spoofing which is caused by leaked biological information. In fact, in some practical systems, it is possible to make a fake or artificial living-body from a piece of biological information (Matsumoto et al., 2002). Therefore, we assume the following in terms of the model introduced in the previous subsection.

Assumption 3. *For any* $1 \leq i \leq |U|$, *a single* $b \in B_i$ *enable to make u such that* $f(u,r) \in B_i$ *for* $r \in R$.

Some cases of leakage of biological information caused by man-made factor (such as, carelessness of a verifier or a cheating verifier) are out of the scope of cryptographic technologies. On the assumption of the secure path by suitable cryptographic technologies, we focus on the following cases of the leakage:

- leakage of a template at the verifier,
- leakage of a piece of biological information at the scanner.

In usual systems, a template is obtained by a reasonable feature-extraction based on biology from scanned biological information or is exactly the information. In this situation, biological information can be estimated from a leaked template and it enables a spoofing as the user of the template.

On our model, the naive method to decide a template is expressed by the condition that any element in B_i can be t_i. Moreover, a straightforward feature-extraction enables an estimation of the definition of the distance, that is, we should assume g to be open. Therefore, the essential point of the former case of the leakage is that an element of B_i can be estimated from t_i by Assumption 2 even if B_i cannot be obtained exactly. The latter case is exactly the leakage of $b \in B_i$. Thus, by Assumption 3 these cases enable the spoofing.

3 SOLUTIONS

To solve the problems in the previous section, we propose solutions by modifying biological information. The modification is expressed on the proposed model as a function from a string to a string with some properties. Moreover, we consider the entity which should apply the function to biological information.

3.1 Leakage of Template at Verifier

The problem of a spoofing by a leakage of a template from the verifier is expressed on the proposed model as that an element of B_i can be estimated from t_i. In conclusion, this problem is solved by applying a generalized idea of "cancelable biometrics (Ratha et al., 2001)", although the original idea is proposed to enable changing a template rather than to prevent a spoofing by a template. In fact, the results of this subsection are obtained by interpreting the argument in (Ratha et al., 2001) into our model.

We consider to prevent a spoofing using t_i by applying a function $\phi : \Sigma^* \to \Sigma^*$ to biological information. Let $t_i = \phi(b)$ for a $b \in B_i$. The prover (who has a living body) u_i submits $\phi(b')$ for $b' \in B_i$ as w to the verifier. Then, on Assumption 1 and 2, the condition for realizing identification is described as the following property of ϕ.

Condition 1. *There exists* g' *such that, for any* $p, q \in \Sigma^*$, $g'(\phi(p), \phi(q)) \leq c$ *if and only if* $g(p,q) \leq c$.

If we consider to add a step for applying ϕ into Protocol 1, the possibility is only between the step (2) and (3). Therefore, we assume that the scanner has a suitable function for it, that is, the scanner is redefined to be another function $f \circ \phi$ and whether $f(u,r) \in B_i$ is examined by $\phi(f(u,r))$ on the previous condition.

Protocol 2. (1) *The prover puts* $u \in U$ *on the scanner;*
(2) *the scanner computes* $\phi(f(u,r))$ *for an* $r \in R$;
(3) *the scanner sends* $\phi(f(u,r))$ *as w to the verifier;*
(4) *the verifier regards the prover as* $u_i \in U$ *if and only if* $\phi^{-1}(w) \in B_i$.

Now, we do not assume any confidentiality of g' for preventing the spoofing. Then, a spoofing using t_i can be prevented if ϕ has the following property.

Condition 2. *For any* $p \in \Sigma^*$, *it is difficult to find q such that* $p = \phi(q)$ *for p.*

On the previous condition, the verifier does not always have the result of $\phi^{-1}(w)$ at the step (4) in Protocol 2. Formally, we have to refer the idea of "computational indistinguishability (Goldreich, 2001)" for the definition of the word "difficult". However, in some practical systems the properties of Condition 1 and 2 are not required strictly. The former guarantees the property of a kind of "collision-free" and the latter is the property of "one-way". On Condition 1, if a simple idea of distance is used as g', then an attack based on "hill-climbing" successes. Namely, in a search of q such that $p = \phi(q)$ for a given $p \in \Sigma^*$, it is possible to have an r such that $g(q,r) < g(q,r')$ by considering whether $g'(\phi(q), \phi(r)) < g'(\phi(q), \phi(r'))$ recursively. This situation contradicts to Condition 2 in a strict sense. One of the solutions for this problem

is to use a complex function as g'. To find a suitable ϕ with g' is one of the difficulties for realizing a practical system based on the idea of cancelable biometrics.

3.2 Leakage of Biological Information at Scanner

As mentioned in Subsection 2.2, the same problem as the case of a leakage of a template is caused by a leakage of a piece of biological information at the scanner. Applying a function which has the properties of Condition 1 and 2 can prevent a spoofing using a template. However, if we consider a leakage of a piece of biological information at the scanner, we can not have the effect of this solution in systems of a naive implementation of this idea. We have to analyze the protocol from the viewpoint of the entity which should apply the function to biological information.

In practical systems with biometrics-based authentication such as a door access control system or an ATM, the scanner is usually managed by the prover as a part of the system. The prover cannot avoid a risk of the leakage of his biological information as long as he has to put his living body on a scanner which is not trustworthy.

A simple solution is that the prover manages the scanner and the function. In this case, the prover outputs only the result of $\phi(f(u,r))$ and hence $f(u,r)$ cannot be obtained from it by Condition 2. Therefore, a system based on this idea can prevent a leakage of $b \in B_i$ which enables a spoofing as u_i. A difficulty of this solution is how to implement a system with this idea. It is natural to consider a PDA or a mobile phone as the scanner which is managed by the prover since the devices have suitable functions for the computation of the functions, the scan of biological information, and the communication with other entity. Thus, it is useful in preventing spoofing in biometrics-based authentication systems to implement the functions to scan some kinds of living bodies on portable devices besides a camera and a microphone.

The assumption that the prover manages f and ϕ yields another problem by "duplicated packet" or a kind of "replay attack". Namely, in the step (3) in Protocol 2, the private scanner can send an old $\phi(f(u,r))$ as w. A simple solution for this problem is that the verifier adds w which was accepted once into a negative list for the examination of $w \in B_i$. The essential solution is to recognize information which is intrinsic to living bodies, which is realized by using a special part of biological information such as information of a reflex action or applying the idea of "zero-knowledge (Goldreich, 2001)" into the detection at a scanner. To realize a function to recognize living bodies is one of the most important problems for biometrics-based authentication. Besides to find a part of a living body which contains information to enable the recognition of living body, it is also useful to apply the idea of "challenge and response (Delfs and Kneble, 2002)" into scanners on portable devices, for example, a camera with a special kind of flash. Note that this realizes authentication by the verifier of the prover instead of his portable device.

4 CONCLUSIONS AND FUTURE WORK

We introduced a model of biometrics-based authentication and made the problem of spoofing by using leaked biological information clear. We proposed a solution to apply a function to biological information and showed the properties required for the function to solve the problem. Moreover, we proposed an idea of biometrics-based authentication system with a mobile device which has a function to detect biological information.

By the analysis of an implementation of the system, we can extract the following results: biometrics-based authentication which is secure against a spoofing can be realized by applying the idea of cancelable biometrics into a system with portable devices; and therefore, it is meaningful to implement functions to capture biological information on portable devices.

ACKNOWLEDGEMENTS

This work has been supported by the Grant-in-Aid for Scientific Research (A) No. 19200004 of the Ministry of Education, Culture, Sports, Science and Technology (MEXT) from 2007 to 2009.

REFERENCES

Delfs, H. and Kneble, H. (2002). *Introduction to Cryptography - Principles and Applications*. Springer.

Goldreich, O. (2001). *Foundation of Cryptography - Basic Tools*. Cambridge University Press.

Matsumoto, T., Matsumoto, H., Yamada, K., and Hoshino, S. (2002). Impact of artificial "gummy" fingers on fingerprint systems. In *Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques IV*, volume 4677, pages 275–289.

Ratha, N. K., Connell, J. H., and Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication system. *IBM System Journal*, 40(3).