

A Framework for Alternative PIN Service Based on Cancellable Biometrics

Byoung-Jin Han, Yong-Nyuo Shin, In-Kyung Jeun and Hyun-Chul Jung

Korea Information Security Agency (KISA)
138-950, Seoul, Korea
{bjhan, ynshin, ikjeun, hcjung}@kisa.or.kr

Abstract. The i-PIN service, an alternative Residence Registration Number (i.e., a kind of PIN) service, and cancellable biometrics have many things in common. We point this out and design a framework for an alternative PIN service based on cancellable biometrics. In this paper, we match the PIN and the biometric template based on their uniqueness and permanence, and we also match the alternative PIN and the distorted template on their characteristic of being cancellable. We propose a framework for an alternative PIN service based on cancellable biometrics. This cancellable property is a promising solution for the privacy problems which stem from the uniqueness and permanence of biometrics and PIN. The proposed framework offers distinct advantages compared with other biometric authentication methods. First, employing the cancellable property encourages the participation of individuals who would otherwise avoid using biometric systems out of concern for their privacy. Second, we provide not only a method of authentication, but also an alternative PIN, which creates opportunities for the expansion of its scope of application.

1 Introduction

The radical growth of Information and Communication Technology (ICT) has helped to enhance the quality of human life. However, it has also accelerated illegal copying, information leakage, and deletion, thereby making privacy a matter of grave concern. The need for effective information security in order to solve these problems has been emphasized. The most fundamental technologies of the information security are access control and encryption/decryption.

Identification and authentication is at the front-end of access control. For identification, the Personal Identification Number (PIN) is most widely used. In Korea, a Resident Registration Number (RRN, also called a Personal Number) is used as a PIN, whereas in the U.S.A. the user's social security number is used. Especially in Korea, the RRN is an essential requirement for registering as a member on most websites. Because the RRN distinguishes a person and is permanently assigned to an individual, it raises a serious problem in that the RRN and the name of the user may be flowed out on the Internet and misused by malicious persons. As such, the Korean MIC (Ministry of Information and

Communication) operates an alternative RRN service named i-PIN (Internet Personal Identification Number), which provides an identification service for websites and delivers an i-PIN number as an alternative RRN instead of the RRN itself. The i-PIN number can be cancelled and regenerated by re-enrollment [1, 2].



Fig. 1. The i-PIN service in Korea

On the other hand, Authentication distinguish between the authorized users and not, then let the authorized users to allow accessing information and to provide differentiated service. The traditional simple authentication method depends on what he knows such as ID, password, and secret information, or on what he has such as key, card, badge, or biometrics. However, these items of information can be embezzled by stealing or leakage, and modified or forged by attackers with relative ease, and sometimes they are simply forgotten. Biometrics has three major characteristics — universality, uniqueness, and permanence [3, 4]. Because of the last two characteristics, the outflow of a biometrics template can cause a serious privacy problem. Cancellable biometrics has been introduced to solve that problem. With this privacy-protecting technology, a distortion transform is applied to a biometric template: only those distorted templates are stored. If a distorted template is compromised, it can be cancelled by choosing another distortion transform [5, 6].

As is clearly apparent, the i-PIN service - an alternative RRN (PIN) service - and cancellable biometrics have many things in common. We point this out and design a framework for an alternative PIN service based on cancellable biometrics. We match the PIN and the biometric template on their uniqueness

and permanence, and also match the alternative PIN and the distorted template on their characteristic of being cancellable.

The rest of this paper is organized as follows: In Section 2, we briefly review the background knowledge; In Section 3, we present our proposed framework; In Section 4, we analyze the security of the proposed framework; and in Section 5 we present the conclusion.

2 Backgrounds

2.1 i-PIN service overview

In Korea, the RRN is widely used for the purpose of verifying a user's real name, because the interview verification method is difficult to apply. RRN offers uniqueness and permanence, and can uniquely distinguish a person from other users, without ever having to be changed during that user's lifetime. However, a large amount of privacy information such as RRN, name, and address has flowed out several times via online and/or offline channels in recent times. Impersonation of a person using leaked RRN causes serious breaches of privacy and raises various security problems. To solve this issue, the MIC in Korea operates an alternative RRN service named i-PIN, which consists of an identification service for websites and delivers an i-PIN number as an alternative RRN instead of the RRN itself. However, the i-PIN number is not assigned permanently, and thus can be cancelled and regenerated [1].

The i-PIN service consists of three parties — the user, website, and trusted verifier. Figure 2 shows the procedure for issuing i-PIN. After issuance, the procedure for using i-PIN is the same as removing the dotted red box from Figure 2. All the user input data and the i-PIN verification information are exchanged via a secure channel.

2.2 Biometric system

Biometric systems recognize individuals based on their biological and behavioral characteristics. The favorite biological characteristics are fingerprints, face, iris, hand geometry, veins in the hands, retina, DNA, and palm prints. These characteristics are considered to satisfy the following desirable properties [4].

- **Universality:** Every individual should have the characteristic;
- **Uniqueness:** Each individual should have a different characteristic;
- **Permanence:** The characteristics should not show any variation that may be caused by the ageing process.

For convenience' sake, the following terms and definitions apply.

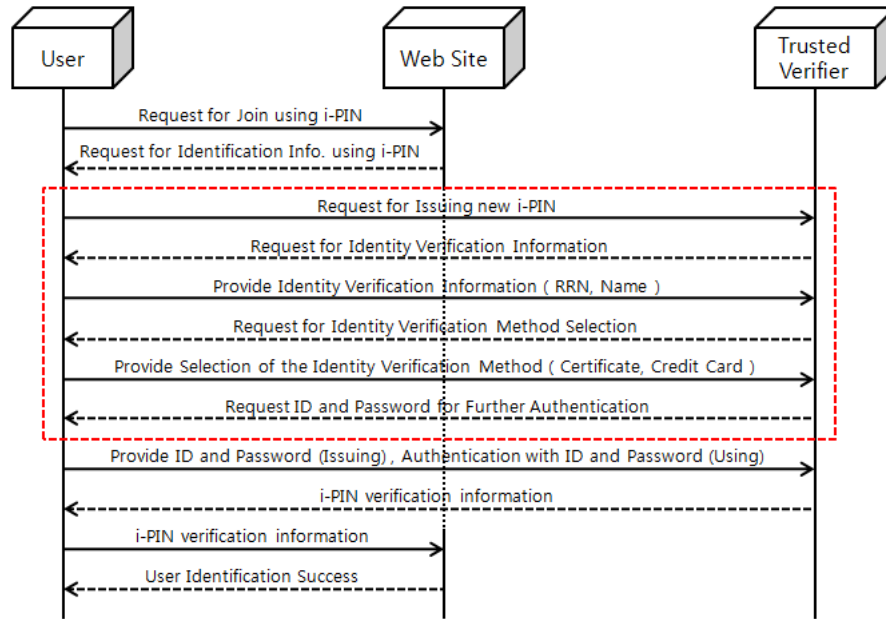


Fig. 2. The i-PIN issuing procedure

- **Biometric Template:** A set of stored biometric features that are directly comparable to the biometric features of a recognition biometric sample;
- **Biometric Sample:** Analog or digital representation of biometric characteristics prior to the feature extraction process, obtained from a biometric capturing device and a biometric capturing subsystem;
- **Biometric Reference:** One or more stored biometric samples, biometric templates or biometric models attributed to a subject and used for comparison.

Biometric verification and identification are powerful techniques against reputation and have been widely used in various security systems. For the authentication and/or identification of an individual, a biometric system processes a probe sample and one or multiple stored biometric reference(s). The biometric reference could be a biometric sample or a set of biometric features. However, such biological biometric characteristics are intrinsically immutable, so when they are stolen or leaked, a permanent compromise may result.

Cancellable Biometrics A strong security and privacy concern for biometric systems relates to cancellable biometrics. Cancellable means the renewability and revocability of biometric references. Because individuals have a limited number of irises and fingers, identity theft makes the corresponding biometric references

unsuitable for future use. Due to its quality of permanence, a biometric reference that has been compromised once remains compromised forever [5, 7].

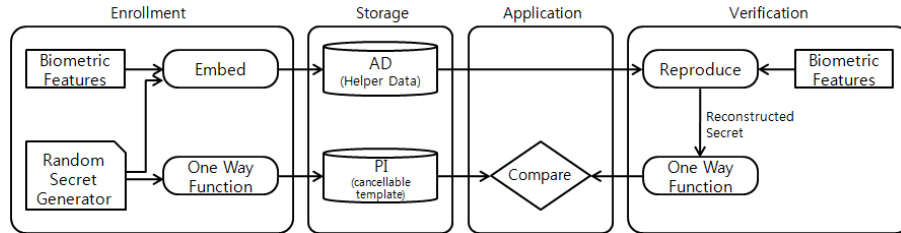


Fig. 3. High level description of cancellable biometrics

The risk of biometric references being compromised can be mitigated by developing methods that allow cancellable biometric references. If various different biometric references can be extracted from the same biometric sample, then the biometric reference can be cancelled and renewed in the event that it becomes compromised.

In the cancellable biometric system we employed, the biometric reference consists of two data elements: a pseudo identity (PI) and the corresponding auxiliary data (AD). Both data elements are generated during enrolment and should be stored, because both are required for verification.

Key Binding The biometric-cryptosystem is a combination of biometrics and cryptography. In a cryptosystem, its security is determined by the security of the key. A user’s identity must be authenticated whenever he or she wants to use the key. Because cryptographic keys are long and random, they are difficult to memorize. As a result, the cryptographic keys can also be stored somewhere (for example, on a computer or on a smart card) and released by using some alternative authentication (e.g., password) mechanism. As such, there is a need for a secure and convenient method of generating a digital key from each user’s biometric data [3].

The methods of combining the key and biometrics determine the applicable models. Generally speaking, there are two models in the biometric-cryptosystem: the biometric key binding/generation model and the biometric key release model. In this paper, we focus on the biometric key binding model.

In the biometric key binding model, a given cryptographic key is bound with the biometric template, which should be stored in a safe way. The system will restore/regenerate the same key with the safe template and a genuine query sample. ‘Safe template’ implies that the template will not leak any information about the original biometric template and the given key.

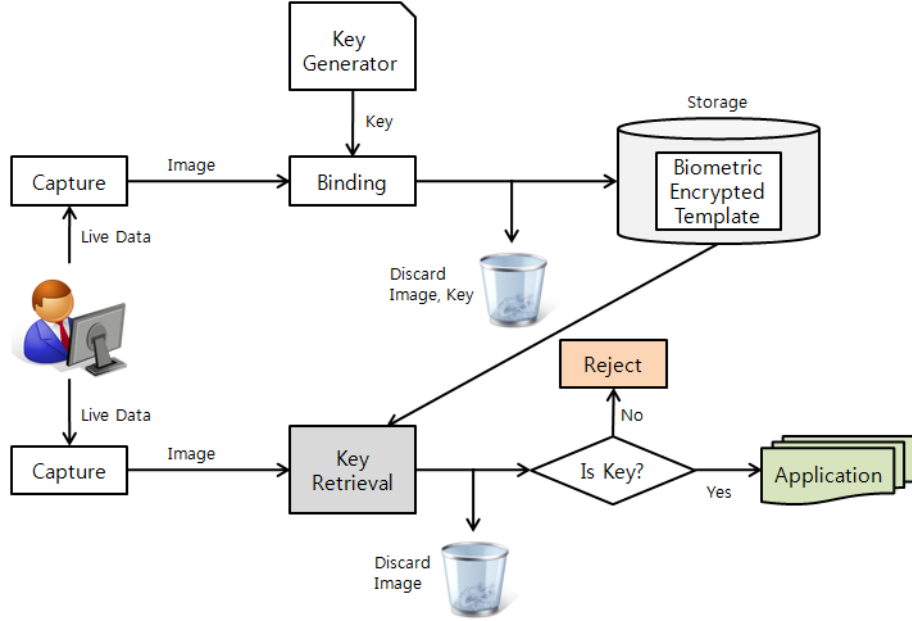


Fig. 4. High level description of key binding

3 A Framework for Alternative PIN Service Based on Cancellable Biometrics

We propose a framework for an alternative PIN service based on cancellable biometrics. As mentioned earlier, the alternative PIN service and cancellable biometrics have many things in common. Thus, we design a framework that matches the PIN and the original biometric template and that also matches the alternative PIN and the distorted template (PI) for their characteristic of being cancellable. The proposed framework provides a means of privacy-enhanced secure authentication. The following assumptions are defined for clarity and for convenience's sake.

- A1. In the proposed framework, the ID, alternative PIN, and the individual's biometric characteristics are unique.
- A2. The types of physical attack for biometrics (e.g. forged fingerprint) are out of scope.

The design of the proposed framework is divided into two parts: enrollment and verification. First, the enrollment part is presented below. To issue a new alternative PIN, an individual enrolls in the system with his or her biometric data and ID. Figure 5 describes the enrollment procedure.

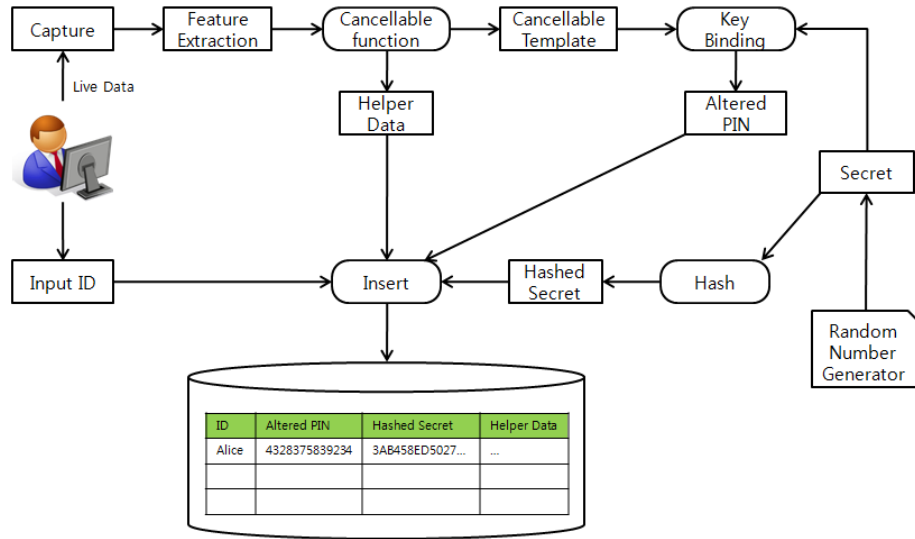


Fig. 5. Enrollment procedure of proposed framework

— Enrollment Procedure:

- E1.* An Individual provides his or her ID and biometric samples to the system;
- E2.* The captured biometric samples undergo feature extraction;
- E3.* Generating a cancellable template and helper data through the cancellable biometric function;
- E4.* Random number generator provides a new random secret;
- E5.* The key binding function generates an alternative PIN using the cancellable template and the random secret;
- E6.* The hash function transforms a secret into a hashed secret;
- E7.* All derived data: the alternative PIN, helper data, and hashed secret are loaded into the DB with the ID.

As you can see, this framework is designed for 1:1 matching. It means that the framework will work on a authentication process, not on a identification process. The biometric samples are provided with ID for the enrollment stage and also for the verification stage.

Next comes the verification part, which is presented below. To verify the alternative PIN for a third party, an individual undergoes the verification procedure. Figure 6 describes the verification procedure.

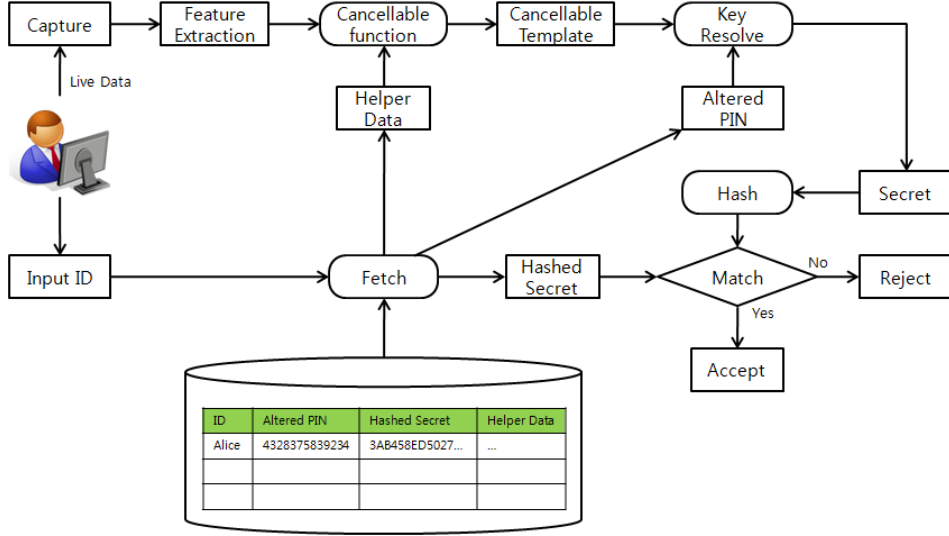


Fig. 6. Verification procedure of proposed framework

— Verification Procedure:

- V1. An Individual provides his or her ID and biometric samples to the system;
- V2. The alternative PIN, helper data, and hashed secret are fetched using the inputted ID;
- V3. The biometric template is generated from the captured biometric sample through feature extraction;
- V4. The biometric template and helper data are used as inputs to generate a cancellable template in the cancellable biometric function;
- V5. The secret is regenerated by the key resolve function using the cancellable template and the alternative PIN;
- V6. The stored hashed secret and output of the hash function is compared with the regenerated secret;
- V7. If those two values are the same, verification has been successful.

The enrollment and verification procedure are presented above. Since we propose a framework, we do not mention a specific mechanism for the cancellable biometrics, key binding/resolve, and hash function. The proposed framework maintains four major types of data: First, the ID is used as an index of record. Second, the alternative PIN is a cancellable identifier for an individual and is

provided to a third party. It does not contain any information about the original biometric template. Third, the hashed secret is the output of the hash function for random secret input. It is used to determine whether verification has been successful or not by comparison. Lastly, the helper data is the output of the cancellable biometric function in the enrollment procedure. It is used to generate a cancellable template from the feature-extracted biometric template. If an individual wants to cancel and renew the cancellable template, the helper data will be changed.

4 Discussion

The security of the proposed framework only depends on the security of the original biometric template. If the ID, alternative PIN, hashed secret, and helper data are disposed of, the security of the proposed framework will not be damaged. Because we employ cancellable biometrics, the original biometric template is threatened by physical attack.

The proposed framework was not designed to cooperate with the real PIN service. To cooperate with the real PIN service, we consider more complicated issues such as separating the real PIN DB from our DB, and merging real PIN verification with our enrollment procedure. This would be a suitable topic for further study.

5 Conclusions

In this paper, we proposed a framework for an alternative PIN service based on cancellable biometrics. The property of being cancellable is a promising solution for the privacy problem stemming from the uniqueness and permanence of biometrics and the PIN. The proposed framework emphasizes the property of being cancellable to safeguard privacy. We employ cancellable biometrics and key-binding technology to generate an alternative PIN and to verify it. The alternative PIN does not leak any information about the original biometric template and random secret.

The proposed framework has distinct advantages when compared with other biometric authentications. First, employing the cancellable property encourages the participation of individuals who would otherwise avoid using biometric systems out of concern for their privacy. Second, we provide not only authentication, but also an alternative PIN, which creates opportunities for the expansion of its scope of application.

For further study, we consider the cooperating out proposed framework with the real PIN service, as this could pave the way to the widespread use of cancellable biometrics.

References

1. Ministry of Information and Communication (MIC) , “Privacy Protection and i-PIN”, 2007.

2. Korea Information Security Agency (KISA), "Introduction to i-PIN", http://www.kisa.or.kr/kisa/ipin/jsp/ipin_0000.jsp, accessed on May 2009.
3. A. Cavoukian and A. Stoianov, "Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security and Privacy", Information and Privacy Commissioner/Ontario, Mar. 2007.
4. N. Pavesic, T. Savic and S. Ribaric, "Multimodal Biometric Authentication System Based on Hand Features", *From Data and Information Analysis to Knowledge Engineering*, Springer Berlin Heidelberg, pp. 630-637, 2006.
5. N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometric-based authentication systems", *IBM SYSTEMS JOURNAL*, Vol 40, No 3, pp. 614-634, 2001
6. M. Savvides, B. b. K. Bijaya Kumar and P. K. Khosla, "Cancellable biometric filters for face recognition", *Proceedings of the 17th International Conference on Pattern Recognition (ICPR'04)*, Vol 3, pp. 922-925, 2004.
7. Q. Li, Y. Sutcu, and N. Memon, "Secure sketch for biometric templates", *Advances in Cryptology - ASIACRYPT 2006*, LNCS 4284, pp 99-113, Nov. 2006.