Design and Analysis of a Highly User-Friendly, Secure, Privacy-Preserving, and Revocable Authentication Method

Article *in* IEEE Transactions on Computers · April 2014

DOI: 10.1109/TC.2013.25

CITATIONS
16

READS
140

4 authors, including:

Xukai Zou
Indiana University-Purdue University Indianapolis
83 PUBLICATIONS **1,128** CITATIONS

SEE PROFILE

Yingzi Du
Indiana University-Purdue University Indianapolis
101 PUBLICATIONS **1,652** CITATIONS

SEE PROFILE

Design and Analysis of a Highly User-Friendly, Secure, Privacy-Preserving, and Revocable Authentication Method

Yan Sui, *Student Member, IEEE* , Xukai Zou, *Member, IEEE* ,
Eliza Y. Du, *Senior Member, IEEE* , and Feng Li, *Member, IEEE*

Abstract—A large portion of system breaches are caused by authentication failure, either during the login process or in the post-authentication session; these failures are themselves related to the limitations associated with existing authentication methods. Current authentication methods, whether proxy based or biometrics based, are not user-centric and/or endanger users' (biometric) security and privacy. In this paper, we propose a biometrics based user-centric authentication approach. This method involves introducing a reference subject (RS), securely fusing the user's biometrics with the RS, generating a BioCapsule (BC) from the fused biometrics, and employing BCs for authentication. Such an approach is user friendly, identity bearing yet privacy-preserving, resilient, and revocable once a BC is compromised. It also supports "one-click sign-on" across systems by fusing the user's biometrics with a distinct RS on each system. Moreover, active and non-intrusive authentication can be automatically performed during post-authentication sessions. We formally prove that the secure fusion based approach is secure against various attacks. Extensive experiments and detailed comparison with existing approaches show that its performance (i.e., authentication accuracy) is comparable to existing typical biometric approaches and the new BC based approach also possesses many desirable features such as diversity and revocability.

Index Terms—Authentication, privacy-preserving, cancelable biometrics (CB), biometric cryptosystem (BCS), BioCapsule (BC), secure fusion

1 Introduction

User-proxy based authentication is well developed and widely used, it is also both effective and efficient in user authentication [17], [19], [23], [40]. However, the growth in user-credential theft in proxy based authentication and increased security requirements have prompted investigation of alternative authentication [29], [55]. A central theme of authentication is to authenticate users using characteristics intrinsically linked with human users rather than some external factors [29]. A promising direction emerging from this effort is biometrics [30]. Currently, the further adoption of biometrics is limited by the security of users' biometric templates extracted in the biometric authentication process: they are irreplaceable once compromised, and original biometric data can be reconstructed from the biometric templates [10], [58]. A biometric template is derived from a user's biometric data and contains the user's private information, thus its compromise may divulge sensitive information (e.g., gender, possible disease). Intensive research has been conducted to address the security and revocability of biometrics, as well as user privacy; concepts such as biometric cryptosystem (BCS) [32], [33], [43], [51], [52], [53], [68] and cancelable biometrics (CB) [4], [5], [12], [45], [48], [50], [64] have emerged from this research.

According to Rathgeb and Uhl [55], there are limitations associated with both BCS and CB. Compared to conventional biometric systems, BCS displays a noticeable decrease in performance [55], [63]; this is due to the hardness of alignments of biometrics and a higher degree of quantization at feature level. Also for the BCS, the system performance and key entropy are highly related, and a direct relation between the maximum length of keys and the error rates has been identified by Buhan et al. [9] which is defined as $k \leq -\log_2 FAR$, where FAR is the false acceptance rate (FAR). For a generic cryptographic purpose (e.g., with a 128-bit key) maintaining a $FAR \leq 2^{-k}$ is very difficult.

For the CB, provable security (e.g., irreversibility and cross-matching resistance (CMR) is rarely done, and for some approaches it is extremely a sophisticated work [55]. Similar to BCS, in the case of hardness of alignments of biometrics and the complexity of transformation, performance decrease is also observed. However, some such approaches have reported an increase in performance, especially when introducing a user-specific external factor (e.g., PIN/token). According to Rathgeb and Uhl [55], this performance gain is based on impractical assumptions during evaluation, and the user-specific transformation parameters must then be

- *Y. Sui and X. Zou are with the Department of Computer and Information Science, Indiana University-Purdue University Indianapolis, 723 W. Michigan St. SL280, Indianapolis, IN 46202. E-mail: {ysui, xkzou}@cs.iupui.edu.*
- *E.Y. Du is with the Department of Electrical and Computer Engineering, Indiana University-Purdue University Indianapolis, 723 W. Michigan St. SL160, Indianapolis, IN 46202. E-mail: yidu@iupui.edu.*
- *F. Li is with the Department of Computer and Information Technology, Indiana University-Purdue University Indianapolis, 799 W. Michigan Street, ET 301D, Indianapolis, IN 46202. E-mail: fengli@iupui.edu.*

Manuscript received 6 Apr. 2012; revised 9 Oct. 2012; accepted 14 Jan. 2013; date of publication 15 Feb. 2013; date of current version 5 Mar. 2014.
Recommended for acceptance by C. Nita-Rotaru.
For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TC.2013.25

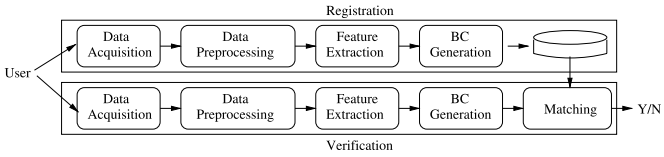


Fig. 1. The new BC based authentication model.

assumed compromised for such evaluation. According to Jain et al. [29], an ideal secured biometric system possesses various properties: security, privacy-preservation, cross-matching resistance, etc. And existing BCS and CB approaches cannot fully address one or more of these properties [55]. In this research, we propose a BioCapsule (BC) and use the BC for user authentication (and identification as well) to address these issues in a comprehensive manner.

We have previously proposed the BC concept in [61]. The BC generation in [61] is based on the difference of the user's biometric feature and that of a proposed reference subject (RS). There are, however, some limitations related to this difference based BC design. First, generation is at the feature level, thus scope is limited. Second, the formal security proof is difficult to obtain and it generally assumes that the RS is a physical entity and physically protected. In this paper, we present a unique BC generation method based on "secure fusion" of the user biometrics and the RS biometrics. The fusion process applies to different stages of biometric processing such as signal, feature or template level. The fusion based BC construction is more usable and flexible, while also secure, resilient to different attacks, and tolerant to the disclosure of both the RS and BC.

The rest of the paper is organized as follows. Section 2 introduces the newly proposed mechanism: key extraction and secure fusion, and the integration of the secure fusion with biometric processes. The analysis of the security of the proposed approach is also included in this section. Section 3 presents experimental results and property analysis. Section 4 further analyzes the BC approach by comparing it with existing methods in two particular aspects: security and performance. Related works are briefly reviewed in Section 5. We conclude the paper and highlight some challenging research issues in Section 6.

2 New Biometric Authentication

The proposed authentication system contains two stages as shown in Fig. 1: registration and verification. For registration, user biometrics is sampled and fused with the RS biometrics; from the fused biometrics a user's BC is generated and stored (in the system database). Upon a verification request, user biometrics is re-sampled and fused with the RS biometrics. Again from the fused biometrics a user BC is derived which is further compared to the stored BC (of an individual). If the two BCs are close enough according to some distance metric, the user is authenticated as the individual.

Selection and setting of RS in the system. The RS can be a physical one or a logical one. A physical RS is some object from which RS biometrics can be sampled on-the-fly, and a logical RS can be a biometric image. RS is a system-wide object and managed by the authentication system, not by a user, which frees users' burden on carrying or memorizing

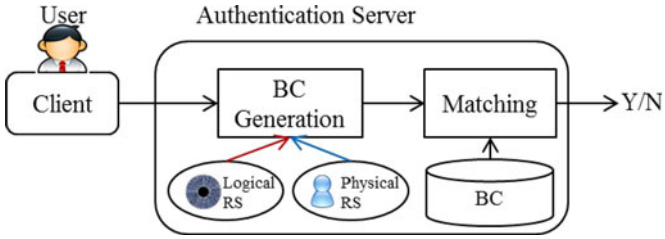


Fig. 2. Diagram of the system.

something. Typically, RS is configured with the authentication server; since the compromised RS will not jeopardize the biometric security and users' privacy, the RS can also be located on client sites. For example, a RS can be configured on client computers at security check points which scan the RS and passenger biometrics and send then the computed BC to the authentication server for authentication. A diagram of a system with the RS at the authentication server is shown in Fig. 2. The user's biometrics is captured via (built-in) camera of the authentication client and sent to the authentication server. Through some preprocessing (omitted in the figure), the user biometrics is fused with the RS biometrics which is either sampled against a physical object on-the-fly or a logical one stored in the server. The server matches the generated BC against the BC stored in the BC database for an authentication decision ("Y/N").

Where to locate and how to configure the RS in a system depends on the system's configuration, security, and application requirements, such as whether a secure transmission channel exists between the authentication server and the user client, and whether the computer used as the authentication server is powerful enough to sample and compute BC without becoming a performance bottleneck. In most critical environments such as military systems and nuclear power stations, a physically protected RS should be used, since a physical RS will prevent attackers from trying to compromise RS remotely. The RS can be considered as a (system-wide) salting mechanism. This mechanism needs the extracted key and features from the RS for salting. A random secret key may be directly used as the RS. It is not clear whether a random secret key has the characteristics of a biometric image such that the secret key and features can be extracted and then fused with the user biometrics. And it is worthy of further efforts to investigate if using a random secret key (as a logical RS) for salting can give us the same security strength and matching performance as does a biometric RS.

Design criteria for the BC. To design an effective fusion and BC construction mechanism, there are following considerations: 1) What impact does the fused biometrics have on the matching performance? Are the users still representable by the fused biometrics? If the user biometrics is surpassed by the RS biometrics, the fused biometrics will be less discriminative thus will deteriorate matching performance. 2) Are the user biometrics and the fused biometrics correlated, or are the fused biometrics using different RSs correlated? If there is a strong correlation, there would be a vulnerability of cross-matching thus infringing user privacy.

Our primary design criteria for the BC follow the requirements of biometric protection [29] and the design

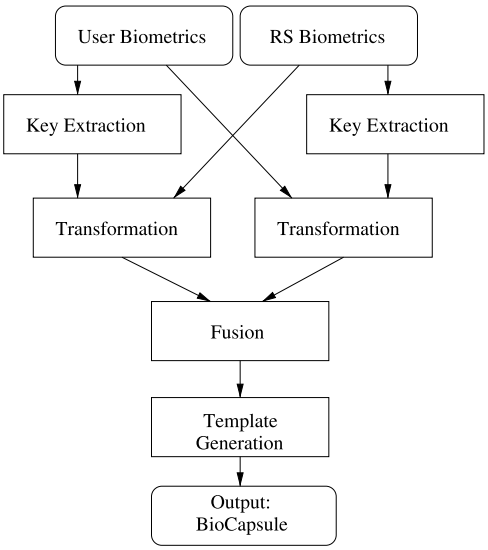


Fig. 3. The BC generation model.

rationale for such BC generation includes the following: 1) The user and the RS are treated equally and the BC bears no hints that the user is weighted more than the RS; 2) Introduce user-intrinsic key extraction for generating a user-specific RS, thus reducing the risk resulting from sharing the common secret (i.e., RS) by all users; 3) Extract keys such that key stability and distinguishability can be balanced; 4) Make it difficult to get the user's biometrics (or the RS's) by reversing a user's BC along with the RS's biometrics (or the user's).

Our designed BC generation model is shown in Fig. 3. From user (RS) biometrics, user (RS) key is extracted and used for RS (user) biometrics transformation. Transformed user biometrics and RS biometrics are fused, and from fused biometrics a BC is generated.

Evaluation metrics and property definition. Based on an information-theory metric (i.e., biometric system entropy (BSE) [62]), search space complexity and probability, we define the following properties for the system.

System security refers to the required effort to be accepted by a biometric system as a certain individual without having access to the biometrics of this individual, which is also known as the brute force attack.

Definition 1. *A biometric system is claimed to provide δ_1 security if the search space to be accepted by the system as a certain individual is δ_1.*

Biometric privacy refers to the required effort to obtain the biometric information of an individual.

Definition 2. *A biometric system is δ_2 privacy preserving if the search space to obtain the biometric information of an individual is δ_2 when the system stored information (e.g., BC, RS) is known.*

One critical property of biometric systems is diversity and cross-matching resistance. It is likely that the user utilizes the same biometrics across systems, thus it should be possible to build different versions of biometric credentials based on the same biometrics. One concern here is that these credentials may be strongly correlated, leading an adversary to try and match the different versions of biometric credentials. Based on Simoens et al.'s indistinguishability game [60], we define the cross-matching resistance as follows.

Definition 3. *A biometric credential generation mechanism is claimed to be δ_3 cross-matching resistant when the cross-matching resistance factor between C and C' is equal to δ_3, $\delta_3 = 1 - 2|\phi - \frac{1}{2}|$ if $Pr(D(C, C') < \sigma) = \phi$, where C and C' are different sets of biometric credentials based on the same biometrics, D is a distance metric between $c \in C$ and $c' \in C'$, and σ is a threshold of accepting a matching. We write $CMR(C, C') = \delta_3$.*

The compromised biometric credential needs to be revoked and replaced by a new one to prevent the attacker from injecting the compromised one directly into the system if the attacker is extremely powerful. Also the periodic update of biometric credentials is a useful practice which will enhance the security of the system and protect a user's privacy. The revocability is closely related to the diversity and cross-matching resistance of the system; based on the same biometrics a new credential can be generated, and the compromised biometric credential cannot be matched against the new one.

Definition 4. *A biometrics system is claimed to be δ_4 revocable if $CMR(C_{old}, C_{new}) = \delta_4$, where C_{old} and C_{new} are old and new biometric credential sets based on the same biometrics.*

The performance (e.g., false acceptance rate (FAR), false rejection rate (FRR), equal error rate (EER)) of a biometric system is based on the distinguishability of the biometric credentials (e.g., BCs). To evaluate the distinguishability, we use biometric system entropy [62], which is defined as the average decrease in uncertainty about the identity of a person due to the biometric system.

Definition 5. *A biometric system is claimed to provide δ_5 distinguishability if the $BSE(C) = \delta_5$, where BSE is the biometric system entropy, C is the biometric credential set of the system.*

Usability is the ease of use [1]. In this paper, usability refers to the necessity to require external factors (e.g., password, token) from users for authentication. A possible metric for usability is the information entropy of external factor, e.g., 128 bits of a user-specific password. From this aspect, a system which does not require external user-provided factors has best usability.

Definition 6. *A biometric system is claimed to provide good usability if it does not require users' efforts to provide external factors for authentication.*

In the following, we present the new mechanisms based on iris biometrics and form a concrete construction of iris-based authentication. The main components of this mechanism are: key extraction, secure fusion and integration of the proposed mechanisms with existing biometric processes, as described below.

2.1 Key Extraction

To create a personalized RS, a user-intrinsic key is extracted from the user's biometrics and used as the transformation parameters to the RS. We propose a light-weight key extraction considering the following criterion:

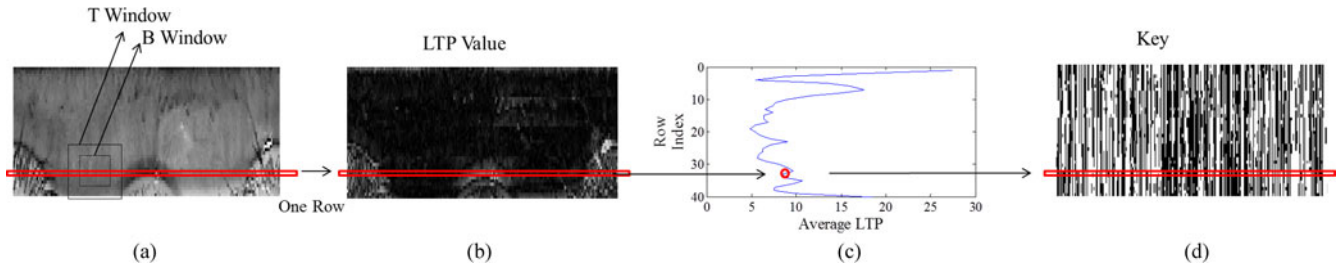


Fig. 4. A key extraction process.

1. To facilitate usability, the key is directly generated from the user biometrics, thus avoiding the need for a user to memorize a password or carry a token to provide transformation parameters. Also, this key is directly generated from user biometrics and is user-intrinsic, making its compromise significantly more difficult when compared to factors artificially bound to a user.
2. Since the keys are not used for authentication, the BC approach does not require 100 percent stable and user-distinct keys (as do some BCSs).
3. The conflict between key stability and distinguishability should be optimally balanced, since it will create further impact on the fusion of biometrics. Intuitively, completed stability will reduce distinguishability. Moreover, noisy features of different samplings of biometrics create constraints on stability, unless more helper data is used. On the other hand, complete distinguishability necessitates the use of complicated fuzzy handling techniques such as error correction codes.

Scheme-1. *The proposed key extraction scheme Ext^K comprises the following procedures as shown in Fig. 4:*

- *Extract iris signature: 1) Obtain processed iris (described as a $m-by-n$ matrix) as Fig. 4a. 2) Compute the grayscale-invariant local texture pattern (LTP) [22] (Fig. 4b). The LTP computation starts with the definition of two windows: T window ($X-by-Y$) and B window which is the center of ($x-by-y$) in window T. The LTP for each pixel at coordinates (i,j) inside B is the pixel value I_{ij} subtracted by the mean A_T of the pixel value of window T such as $LTP_{ij}=|I_{ij}-A_T|, (i,j)\in B$. I_{ij} is the grayscale value of the pixel at (i,j) in B, and A_T is the mean grayscale value inside T. There is $A_T=\frac{1}{N}\sum_{(x,y)\in T} I_{xy}$, with N the total number of pixels contained within T. 3) Generate a temporary signature (Fig. 4c) $\tilde{s}\in \mathbb{R}^m$ by averaging the LTP values of rows.*
- *Compute the mean V of the temporary signature. Given a system mean parameter M, obtain the iris signature by $s=(\tilde{s}-V)+M$, with V obtained by $V=\frac{1}{m}\sum \tilde{s}$.*
- *Encode the iris signature s to a key (Fig. 4d). Encoding is an essential part of the key extraction. Each iris signature component s_i $(1\le i\le m)$ is an average of a row of LTP values, thus theoretically $0.0\le s_i\le 255.0$ (due to the pixel value range of grayscale image). However, the (iris) biometric pattern would not have dramatic contrast on local areas (indicated by the results of [22]). Practically, the iris signature component could possibly range from 0.0 to 18.0 (a tighter boundary used by our experiments). To encode such a s_i, we create an encoding book which is a mapping $Map:\{0.0-18.0\}\rightarrow\{-1,1\}^n$ considering the 10th decimal part of s_i. This encoding book is created in system initialization and stored in the system as the system parameters. A $m\times n$-length key is obtained by applying Map on s.*

The key extraction is applied on the preprocessed images. During the preprocessing [20], the iris image segmentation and polar transformation steps help mitigate the scaling and distortion problems of biometric images. During the key extraction, LTP average computation is a rotation-invariant process [22]. So image scaling, rotation, and distortion are mitigated in the key extraction, and relatively stable keys can be produced. Moreover, the method of encoding will have an impact on the key stability and distinguishability. For example, encoding a signature component by considering more bits of the decimal fraction (e.g., hundredth decimal) increases the distinguishability, while considering less bits (e.g., by rounding the signature) increases the stability.

2.2 Secure Fusion of User and Reference Subject

Our goal of fusion aims to increase the security of the biometrics. Through the fusion, the RS biometrics hides the user biometrics, thus providing biometric security and preserving privacy. Our fusion equally treats the user and the RS and the BC bears no hints that the user is weighted more than the RS. Our security proof, later in this section, also consolidates the contribution of designing equal treatment of the user and the RS.

Scheme-2. *On biometric inputs F^u, F^r, K^u and K^r where $F^u, F^r\in\{F_i\}^n$ $(f^L\le F_i\le f^U)$ and $K^u, K^r\in\{K_i\}^n$ $(K_i=1, -1)$, through "secure fusion" the fused biometrics $F^{u,r}$ (or $\{F_i^{u,r}\}^n$) is obtained by*

$$F_i^{u,r}=\left(F_i^u\cdot K_i^r+F_i^r\cdot K_i^u(f^U-f^L)\right)+f^L, \qquad (1)$$

within F_i^u is one component of the user biometrics, F_i^r is one component of the RS biometrics, K_i^u is one key bit of the user key and K_i^r is one key bit of the RS key. It is obvious that $F^{u,r}\in\{F_i\}^n$ $(f^L\le F_i\le f^U)$.

An actual fusion process is illustrated in Fig. 5. One ICE [2] image and one RS image (i.e., Fig. 8a) are used to illustrate the fusion process. From these two images, user key and RS key are extracted using **Scheme-1**, and the user feature set and RS feature set are extracted using 1D Log-Gabor [39] (results are shown in Fig. 5a). In a closer view, 10 user (RS) features/10 bits of the user (RS) key in the

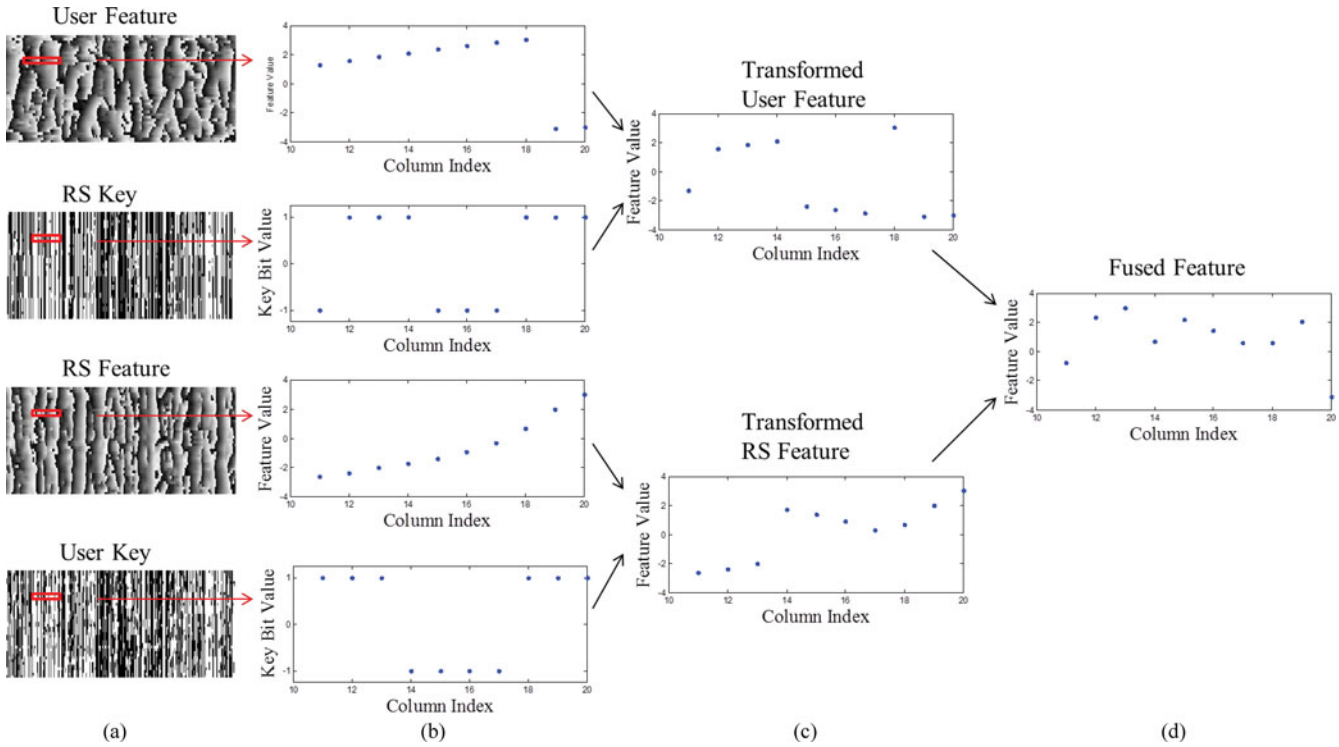


Fig. 5. A secure fusion process: illustrated by an ICE image and an RS image (showed in Fig. 8). For clarity, we use a portion of the entire feature and key (red box in (a)) to present the following fusion procedure in (b), (c) and (d).

dashed box of Fig. 5a are shown in Fig. 5b. The definition of F_i depends on the biometrics and the feature extraction approach. For 1D Log-Gabor, each feature's space is from $-\pi$ to π. Each key bit is either 1 or -1. One transformed user/RS feature is obtained by multiplying the user/RS feature with 1 bit of the RS/user key (results are shown in Fig. 5c). The fused features are obtained through Eq. (1) (results are shown in Fig. 5d).

2.3 Integration of Secure Fusion with Existing Biometric Processes

The proposed fusion mechanism is a general procedure, which can be integrated with existing biometric processes to generate BCs. And to show how the fusion fits into the biometric system, Fig. 6 presents a model of the integration of "secure fusion" with existing biometric processes at feature level. The model uses traditional preprocessing, feature extraction and template generation approaches without modification; it applies the "secure fusion" before the template generation and after the feature extraction. This property not only makes the proposed fusion more deployable but also keeps the same domain of inputs and outputs, thus theoretically enabling the fusion at other levels (e.g., signal, template).

Next, we illustrate the concrete integration of "secure fusion" with 2D Gabor [20]. Through the integration of "secure fusion" with existing biometric procedures, a complete BC generation process is given as follows:

Scheme-3. *Given user biometric data D^u and RS biometric data D^r, a $feature - BCE$ ("BioCapsule Extractor") scheme is composed of the following procedures:*

- *Extract the user key K^u and the RS key K^r from D^u and D^r using* **Scheme-1**.

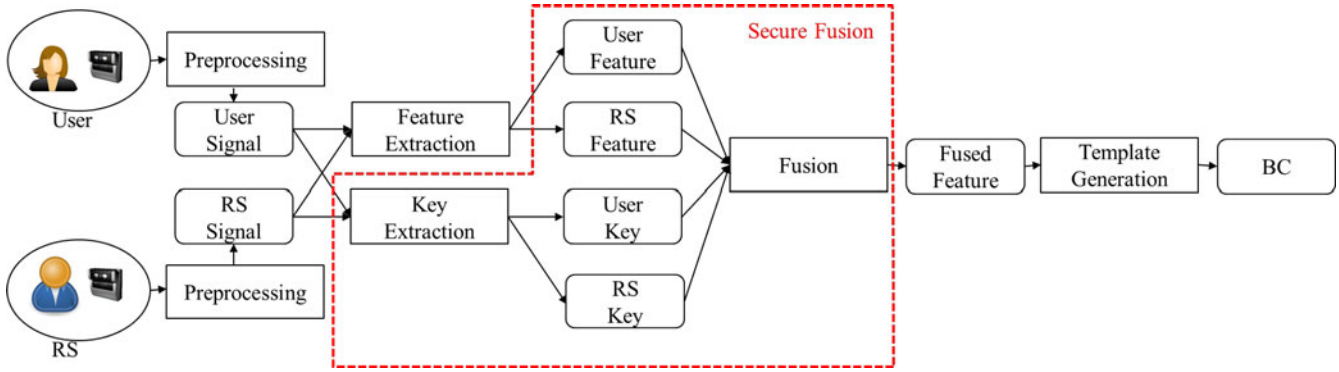


Fig. 6. Integration of the secure fusion (red box) with existing biometrics processes at feature level.

- *Extract features using 2D Gabor from biometric data by feature extraction procedure Ext^F and obtain user biometric feature $F^u = Ext^F(D^u)$ and RS biometric feature $F^r = Ext^F(D^r)$.*
- *Fuse the user feature and the RS feature using K^u and K^r by the procedure defined in* **Scheme-2**. *Obtain $F^{u,r}$.*
- *Quantize the fused feature $F^{u,r}$ into a BioCapsule BC^u.*

Scheme-3 integrates the proposed mechanism "secure fusion" with the existing biometric process and presents a complete BC generation process. In the following, we will analyze the security of the BC approach.

2.4 Security Analysis

The system logically stores BCs and RS (if a logical RS is used). In this section, we prove the security of the users' biometrics (i.e., privacy-preservation) of the BC approach considering BCs and/or RS are compromised.

1) Security against a lost BC:

Theorem 1. *Deriving the user biometrics (or the RS) from a compromised user's BC is equivalent to solving an undetermined equation.*

Proof. From the compromised BC, the attacker approximately obtains the $F^{u,r}$ (a range of the fused biometrics). Then, the attack is reduced to solving the following equation: $F^{u,r} = F^u \cdot K^r + F^r \cdot K^u$, with F^u, K^u, F^r, K^r unknown, in which F^u, K^u are the user biometrics and the user key, and F^r, K^r are the RS biometrics and the RS key. This equation is undetermined, and no single solution can be found. Thus, the BC approach defeats the attack of recovering the user biometrics (or the RS) from a compromised BC. □

2) Security against loss of both a BC and the RS:

Theorem 2. *The security of the user biometrics against a compromised BC and RS can be equivalently measured by the strength of the key used for "secure fusion".*

Proof. The proof begins at the relations among user LTP values, user biometric feature F^u and user key K^u (similar for RS LTPs, F^r and K^r). The key extraction in **Scheme-1** involves LTPs and K^u, and it averages the LTP values row by row and encodes the results into K^u. Given the fact that from the average of a set of data it is difficult to reconstruct the original data, there is no direct relation that can be built for each LTP value and each key bit. Also, the LTP values are different from the feature F^u (as in **Scheme-3**). Thus, we infer that F^u (or each F_i^u) is independent from K^u (or K_i^u) (similar for F^r and K^r).

From the compromised RS, using **Scheme-1** K^r can be extracted, and using the assumed public feature extraction F^r can be extracted. From the compromised BC, the attacker approximately obtains the $F^{u,r}$ (a range of the fused biometrics). For a feature-BCE, the problem reduces to solving the equation, $F^{u,r} = F^u \cdot K^r + F^r \cdot K^u$, with F^u and K^u unknown. This equation can be expanded to an equation system if we consider the entire feature consisting of n component

$$\begin{cases} F_1^{u,r} = F_1^u \cdot K_1^r + F_1^r \cdot K_1^u \\ \cdots \\ F_n^{u,r} = F_n^u \cdot K_n^r + F_n^r \cdot K_n^u, \end{cases}$$

with F_i^u and K_i^u $(1 \le i \le n)$ unknown. Since F_i^u and K_i^u are independent, we can treat them as two variables. This equation system is undetermined and no single solution can be found. Observing the equation system, F^u can be obtained by: 1) guessing $K_1^u, \ldots, K_n^u$; 2) computing $F_i^u = (F_i^{u,r} - F_i^r \cdot K_i^u) \cdot (K_i^r)^{-1}$; then 3) checking if $Ext^K(F_1^u, \ldots, F_n^u) = \{K_i^u\}^n$. The search space is the key space (e.g., our experiments using $O(180^{32}) \approx O(2^{224})$) which is computationally hard. Thus, the new BC approach is able to prevent user biometrics from being recovered even though both RS and BC are disclosed/compromised. □

This proof is also applicable to an attack wherein an insider gets his own BC and biometrics, and tries to derive the RS. Due to the equal treatment of the user biometrics and RS, RS security can be assured following similar arguments.

3) Security against external collusion attack:

Theorem 3. *Deriving the RS from BCs of various users, even under the situation which is most favorable to the attacker, is equivalent to solving an undetermined system of equations.*

Proof. From the BCs (from $u_1, \ldots, u_v$), the attacker approximately obtains the $F^{u,r}$s (ranges of fused biometrics (feature)). Then, the attack is reduced to solving the following equation system:

$$\begin{cases} F^{u_1} \cdot K^{r_1} + F^{r_1} \cdot K^{u_1} = F^{u_1,r_1} \\ \cdots \\ F^{u_v} \cdot K^{r_v} + F^{r_v} \cdot K^{u_v} = F^{u_v,r_v}. \end{cases} \tag{2}$$

Without loss of generality, in the worst case let us assume that those BCs are generated from the same RS and the same key encoding, thus $F^{r_1} = F^{r_2} = \cdots = F^{r_v} = F^r$ and $K^{r_1} = K^{r_2} = \cdots = K^{r_v} = K^r$. The equation system becomes

$$\begin{cases} F^{u_1} \cdot K^r + F^r \cdot K^{u_1} = F^{u_1,r} \\ \cdots \\ F^{u_v} \cdot K^r + F^r \cdot K^{u_v} = F^{u_v,r}, \end{cases} \tag{3}$$

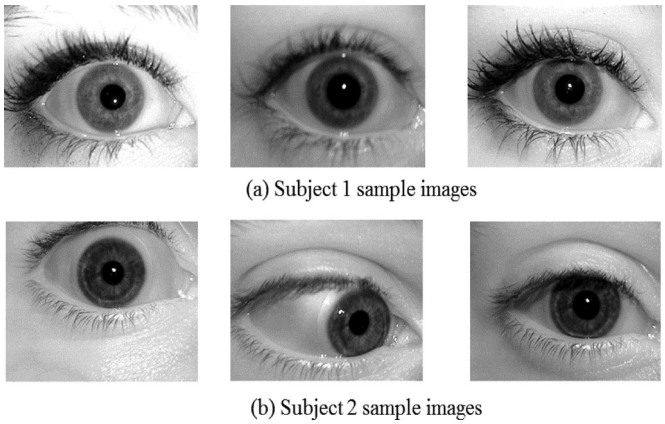
with K^r, F^r, K^{u_i} and F^{u_i} $(1 \le i \le v)$ unknown. The system of equations is undetermined and a unique solution is not available. Thus, the BC approach is able to defeat the attack of recovering the RS from a set of BCs, that is it is resilient to the external collusion attack. □

4) Security against internal collusion attack:

Theorem 4. *Deriving the RS from various users' biometrics and corresponding BCs, even under the situation which is most favorable to the attacker, is equivalent to solving an interval linear system of equations, which is NP-hard [35].*

Proof. From those BCs (from $u_1, \ldots, u_v$), ranges of $F^{u,r}$s can be obtained. Without loss of generality, in the worst case let us assume that those $F^{u,r}$s are generated from the same RS (if a logical RS is used) and same key encoding. Thus, the problem is reduced to solving the following equation system with F^r and K^r unknown:

$$\begin{cases} F^{u_1} \cdot K^r + F^r \cdot K^{u_1} = F^{u_1,r} \\ \cdots \\ F^{u_v} \cdot K^r + F^r \cdot K^{u_v} = F.^{u_v,r} \end{cases} \tag{4}$$



(a) Subject 1 sample images

(b) Subject 2 sample images

Fig. 7. Sample images of two subjects from NIST/ICE.

This is an interval linear system, and solving such a system is NP-hard [35], where the NP-hardness of solving the problem is due to the computational complexity of the problem itself. The running time to solve the problem grows exponentially with the number of unknowns [35]. In our case, the number of unknowns is 12,000 (i.e., 12,000 features of RS). Such NP-hardness makes it practically infeasible to derive the RS, thus the system is resilient to the internal collusion attack. □

The above two attacks are against the RS. However, even if the RS is determinable, determining the RS helps no further if the attacker acquires another user's BC and tries to derive this user's biometrics. Following Theorem 2, user biometrics is secure against a lost RS and the user's BC.

5) Security against internal Cross-RS attack:

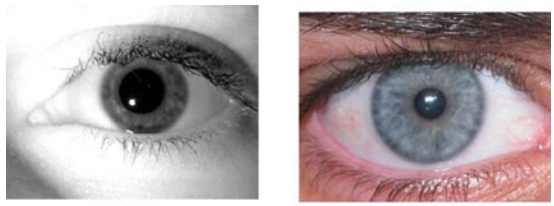
Theorem 5. *The attacker collects a group of users' biometrics and multiple copies of BCs using various RSs of those users and another user's BCs for those RSs, and tries to obtain the user's biometrics. Under the situation which is most favorable to the attacker, the attack is equivalent to solving an interval linear system of equations, which is NP-hard [35], and thereafter an undetermined system.*

Proof. From those BCs (from $u_1, \ldots, u_v$) using various RSs (illustrated in the following using two RSs, e.g., RS_1 and RS_2), a range of the fused biometrics can be obtained. Attackers can get an equation system from BCs using RS_1, and also an equation system from BCs using RS_2. From Theorem 4, this internal attack for a single RS is hard. Thus, obtaining RS_1 and RS_2 necessitates solving interval linear systems, which are computationally hard.

If we assume the worst, RS_1 and RS_2, and thus F^{r_1}, K^{r_1} (RS_1's biometrics and RS_1's key) and F^{r_2}, K^{r_2} (RS_2's biometrics and RS_2's key) are all obtained. The attacker then obtains another user u_i's BCs $BC_1^{u_i} = F^{u_i,r_1}$ for RS_1 and $BC_2^{u_i} = F^{u_i,r_2}$ for RS_2, and tries to get F^{u_i} by solving the following:

$$\begin{cases} F^{u_i} \cdot K^{r_1} + F^{r_1} \cdot K_1^{u_i} = F^{u_i,r_1} \\ F^{u_i} \cdot K^{r_2} + F^{r_2} \cdot K_2^{u_i} = F^{u_i,r_2} \end{cases} \quad (5)$$

with F^{u_i}, $K_1^{u_i}$ and $K_2^{u_i}$ unknown. First, this equation is an interval linear system. Second, the two systems can take different key encoding Maps such that $K_1^{u_i} \neq K_2^{u_i}$, in which case it is then an undetermined system. Solving such a system is hard, thus the BC approach is resilient to the internal cross-RS attack. □



(a) RS 1 (b) RS 2

Fig. 8. Reference subjects' biometrics.

From the above proofs, it is evident that the BC based approach is resilient against various attacks including colluding and cross-matching attacks. Therefore, the security of the users' biometrics can be guaranteed and user privacy can be preserved.

3 Experimental Results and Performance Analysis

In order to evaluate the performance of the proposed BC approach, we have conducted extensive experiments on (various components of) the BC approach.

3.1 Experiment Setting

The performance of the proposed technique was tested on the ICE database which is provided by National Institute of Standards and Technology (NIST) for the Iris Challenge Evaluation (ICE) 2005 [2], [47]. The ICE database contains 1,426 images from the right eye from 132 subjects, and 1,527 images from the left eye from 132 subjects. These images were collected with the LG EOU 2200 and intentionally represent a broader range of quality than the camera would normally acquire. This includes iris images that did not pass the quality control software embedded in the LG EOU 2200. And they were all used in our experiments. The ICE 2005 is commonly used by academic institutions, research laboratories and companies and is a benchmark database used for system evaluation. Sample images from ICE 2005 database are provided in Fig. 7.

We chose an iris image from the UBIRIS [49] and one iris image from ICE as our RS iris image as shown in Fig. 8. If the RS is a logical one (e.g., an image stored in the system), it will display no image distortion. If the RS is a physical one, there will be some degree of image distortion on the obtained RS image for each sampling. To produce multiple distorted RS images for simulation, as suggested by Jung et al. [34] we introduced random white Gaussian noise with signal-to-noise ratio (SNR) 40 into a logical RS image considering that the International Organization for Standardization (ISO) suggests the SNR of an iris camera should be better than 40 db. Due to the fact that the physical RS was not a live person that demonstrates pupil focusing, defocusing, head tilting and so on, we did not introduce defocus blurring in the sampled RS images. For the approach evaluation, using the physical RS setting we provide the receiver operating characteristic (ROC) as well as the probability distribution of inter-class and intra-class matching (Note: if we assume a stable RS, we get similar matching results, which are thus omitted).

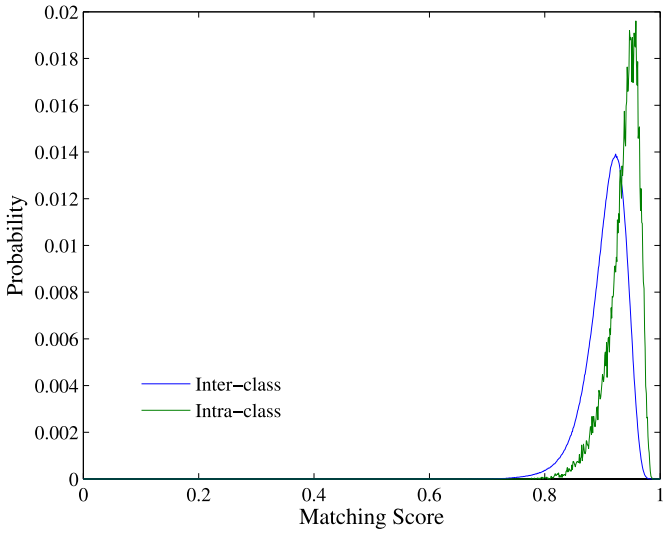


Fig. 9. Key stableness and distinguishability (extracted key intra-class and inter-class distribution).

3.2 Key Stableness and Distinguishability

Key stableness and distinguishability were investigated; this experiment consisted of matching the extracted keys against each other. For example, in the ICE database with 2,953 images, $2,953 \times 2,952$ matches are performed. The curves in Fig. 9 show the matching score distribution of matchings of intra-class (genuine) and inter-class (impostor). The more "sharp" and "right-shifted" intra-class curve indicates more stableness of extracted keys. The more "distanced" curves indicate better distinguishability. The proposed key extraction approach presents good stability and moderate key distinguishability. In the following experiment, we evaluate how the extracted keys affect the fusion, and thus the matching performance of the extracted BC.

3.3 Identity-Bearing of the BC

This experiment tested the identity-bearing of the BC. To establish this, we constructed a BC for each image from the ICE database using the RS_1 (i.e., Fig. 8a). For the BC generation, 1D Log-Gabor was used for feature extraction. To make a comparison, we also implemented 1D Log-Gabor IrisCode [39]. The experimental results are shown in Fig. 10. In particular, Fig. 10a compares the ROC, and Fig. 10b compares the intra-class and inter-class distribution. These curves are quite overlapped, which indicates that the BC mechanism maintains the identity-bearing of the original IrisCode quite well. From this experiment, we observe that when the keys are not as stable, their application in the fusion makes the "matching" of biometrics less similar. However, inter-class and intra-class matchings follow the same trend as indicated by the left shifting from IrisCode curves to BC curves (e.g., Fig. 7b). As the inter-class and intra-class distributions are both left-shifted, the BC keeps the distribution as distinguishable as the original biometrics, while properly maintaining the system performance.

3.4 Applicability of the BC to Existing Biometric Modules

This experiment tested the applicability of the BC to existing biometric modules. We implemented the BC approach

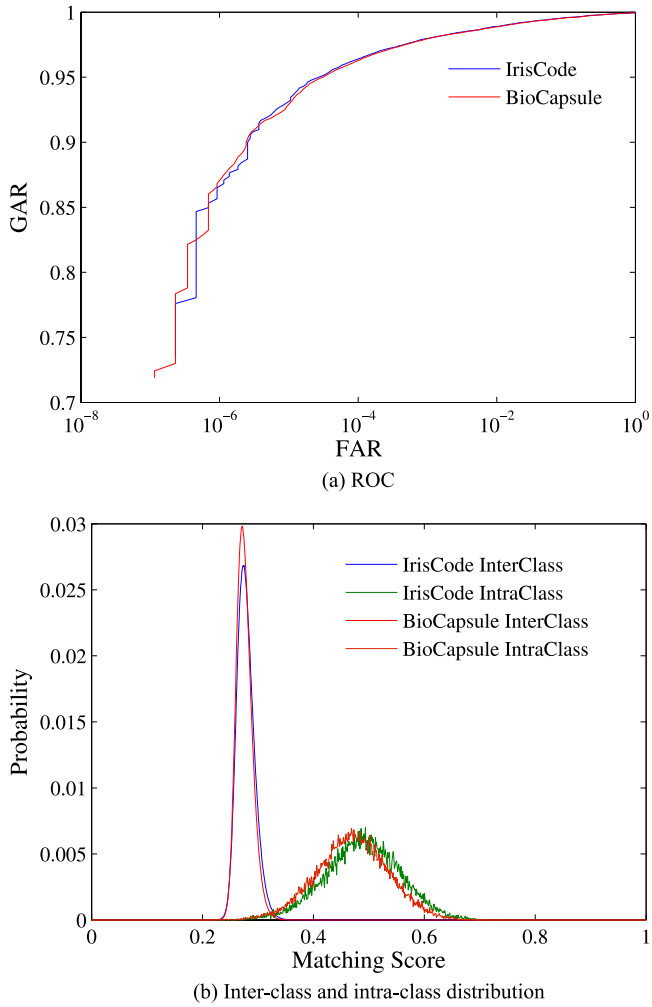


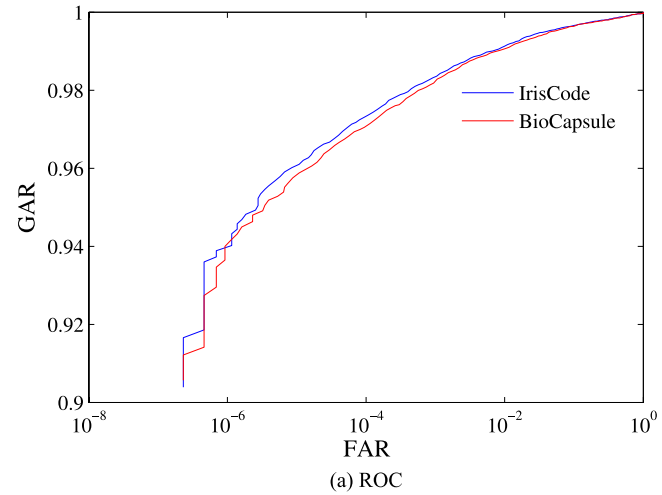
Fig. 10. IrisCode and BC performance comparison on the ICE database using 1D Log-Gabor.

using RS_1 (i.e., Fig. 8a), and either 1D Log-Gabor or 2D Gabor were used for the feature extraction. To make a comparison, we also implemented 1D Log-Gabor IrisCode [39] and 2D Gabor IrisCode [20]. As the experimental results show in both Fig. 10 (1D Log-Gabor results) and Fig. 11 (2D Gabor results), the ROC, inter-class and intra-class distribution curves of the IrisCode and the BC are quite overlapping. These observations indicate that BC is generally applicable to existing biometric modules, e.g., 1D Log Gabor, 2D Gabor, and possibly others.

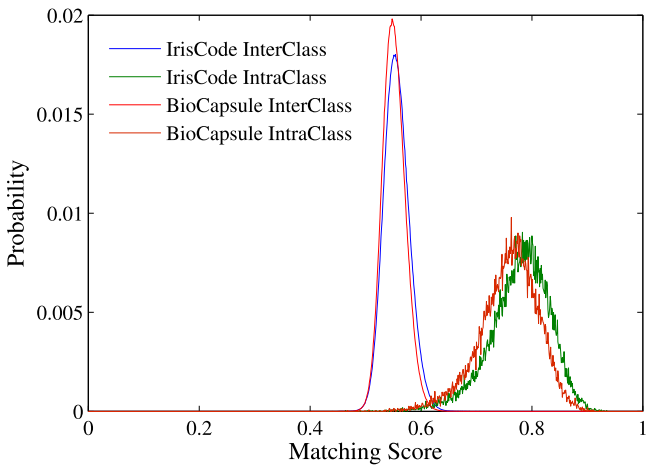
3.5 Effect of Image Quality on the BC Performance

This experiment tested the effects of image quality on BC performance. We applied the BC approach on the entire image set and quality image set (partial of entire set).[1] Table 1 summarizes the performance (e.g., FAR, FRR, EER) of two popular approaches: 1D Log-Gabor IrisCode, 2D Gabor IrisCode, and the proposed BC approach using different feature extractions on the ICE database. From the

1. Excluding the upper four and lower four rows of the image which are always occluded by eyelids and eyelashes, images without more than 35 percent occlusion on remaining rows are considered quality images.



(a) ROC



(b) Inter-class and intra-class distribution

Fig. 11. IrisCode and BC performance comparison on the ICE database using 2D Gabor.

table, it can be observed that both IrisCode approaches and the BC approach perform better on quality images. Also the BC approach shows comparable performance to the IrisCode, thus maintaining the performance of the traditional biometrics regardless of the image quality.

3.6 Revocability

To satisfy the property of revocability, BCs using different RSs, generated from a single user subject, have to appear random to themselves (like BCs of different subjects). To establish this, we constructed BCs using RS_1 (i.e., Fig. 8a) and BCs using RS_2 (i.e., Fig. 8b). The two sets of BCs are cross-matched.

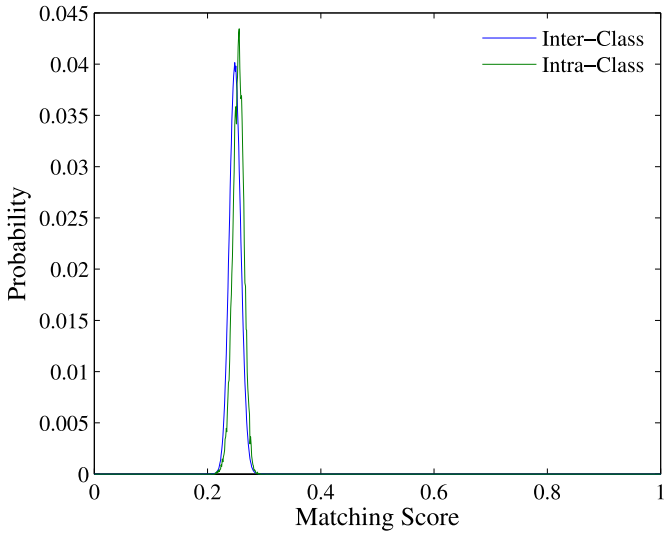


Fig. 12. Inter-class and intra-class distribution between BCs using RS_1 and BCs using RS_2 ($RS_1 \neq RS_2$).

Fig. 12 shows quite overlapped intra-class (genuine) and inter-class (impostor) distributions. The mixed distributions indicate that it is hard to determine whether or not two BCs (i.e., one from RS_1, and the other from RS_2) are from the same user. In this sense, we argue that the old BC cannot be used to identify or authenticate a user by comparing it to the new BC, and thus is revoked.

3.7 Cross-Matching Resistance of the BC

The purpose of this experiment is to test cross-matching resistance of the BC. We consider two cases: 1) system 1 uses the BC technique, and system 2 uses the IrisCode technique; and 2) system 1 and system 2 both use the BC technique, but with different RSs. To be cross-matching resistant, biometric credentials from different systems, generated for a single user subject, have to appear random to themselves (like BCs of different subjects). Further, the matchings have to appear random (inter-class and intra-class distributions are mixed). Fig. 13 shows the genuine and impostor distribution of matching IrisCodes to BCs. The more mixed distribution indicates indistinguishability from IrisCode to BC, which also indicates good capability of defeating cross-matching attack. The cross-matching resistance of the BCs using different RSs is equivalent to the revocation in Section 3.6, which is well established.

TABLE 1
Experiments Summary

DATABASE	Approach	EER	FRR(FAR = 10^{-3})	FRR(FAR = 10^{-4})	FRR(FAR = 10^{-5})
ICE (entire database)	1D Log-Gabor IrisCode	0.0108	0.0204	0.0365	0.0695
	BC using 1D Log-Gabor	0.0111	0.0203	0.0376	0.0700
ICE (2245 quality images)	1D Log-Gabor IrisCode	0.0028	0.0035	0.0063	0.0105
	BC using 1D Log-Gabor	0.0029	0.0037	0.0067	0.0111
ICE (entire database)	2D Gabor IrisCode	0.0090	0.0164	0.0264	0.0390
	BC using 2D Gabor	0.0094	0.0181	0.0295	0.0412
ICE (2245 quality images)	2D Gabor IrisCode	0.0028	0.0033	0.0051	0.0084
	BC using 2D Gabor	0.0029	0.0036	0.0059	0.0096

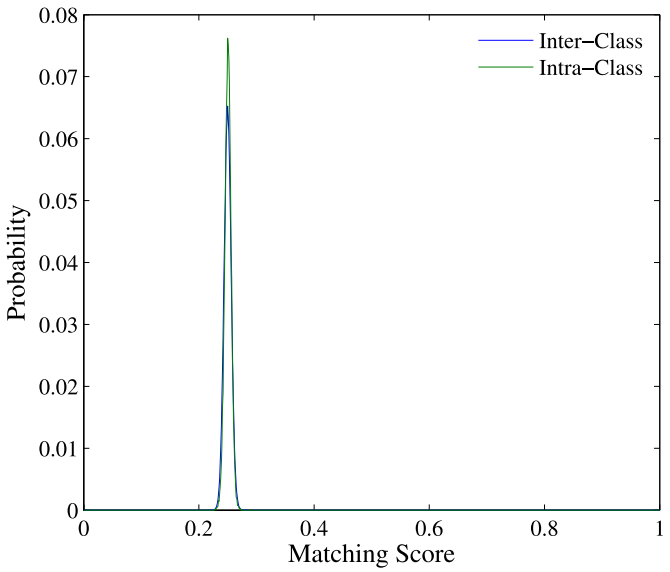


Fig. 13. Inter-class and intra-class distribution between matchings of 1D Log-Gabor IrisCodes and BCs.

3.8 Property Analysis

We analyze the properties of the concrete iris based BC authentication system according to the definitions proposed in Section 2 as follows:

Security. We consider the BC system that accepts an attacker U as a certain individual I when the attacker provides a BC^U and $Hamming(BC^U, BC^I)/Length(BC) \leq 0.35$. In the experiments, the BC is of 12,000*2 bits (Note: each fused feature is quantized and encoded into 2 bits.). The search space is approximately $\frac{2^{24000}}{\sum_{i=0}^{24000*0.35} \binom{24000}{i}} \approx 2^{1582}$ according to the bound given by Gallier [25]. Thus, the security of the BC system is around 1,582 bits.

Privacy-preservation. The hardness of obtaining user biometrics from BC (with/without RS) has been analyzed in Section 2.4. It has been shown that the user biometric privacy is preserved under different situations.

Cross-matching resistance. Various biometric credentials are considered: BCs (using RS_1), $BC^{'}$s (using RS_2) and IrisCodes. A very practical way proposed by Buhan et al. is to measure the cross-matching resistance given the threshold σ when FAR equals to FRR [8]. Under this consideration, according to our experimental results we obtain $CMR(BC, BC^{'}) = 0.8106$, $CMR(BC, IrisCode) = 0.9881$ and $CMR(IrisCode, IrisCode) = 0.046$.[2] The results indicate that the BC mechanism improves the cross-matching resistance of traditional biometric systems.

Revocability. Using the BC approach, BCs are generated using RS_1 and $BC^{'}$s are generated using RS_2. If the system is replacing RS_1 with RS_2, we obtain $CMR(BC, BC^{'}) = 0.8106$, which indicates that the BC approach provides good revocability.

Performance. We obtain the biometric system entropy of the BC system and conventional IrisCode system, i.e., $BSE(BC) = 5.93$ and $BSE(IrisCode) = 4.89$. This result shows that BC provides better distinguishability when compared to the IrisCode.

Usability. The proposed system does not require any external factors from users, thus providing good usability.

3.9 Time Performance of the BC System

The proposed BC follows the standard steps utilized by existing biometric systems, i.e., preprocessing, feature extraction, and matching. The additional steps are RS preprocessing, RS feature extraction, RS key extraction, user key extraction and the fusion. The preprocessing of an edge-detection based approach of the RS can take around 0.3 s; the user (RS) key extraction takes around 0.082 s. The feature extraction takes around 0.0051 s, and the fusion process can take around 0.0026 s. (Note: results are obtained through experiments implemented using Matlab 2010 on a laptop with Dual-Core CPU 2.10 GHz and 4 GB RAM. The program is not optimized for the running time. If C/C++ is used, the speed can be further improved.) Thus, the total time for all additional steps is around 0.47 s.

Through the experiments and analysis in this section, we have proven that the BC based approach is quite usable, revocable, cross-matching resistant, and applicable to 2D Gabor and 1D Log-Gabor approaches. It is also noteworthy that the "lost-key" scenario is not considered in experiments. Since in the BC model the user-intrinsic key is directly derived from the user biometrics, they should not be considered as the "additional" factor of the system.

4 Comparison with Existing Works

This section compares the BC scheme with typical BCS and CB approaches in terms of both security and accuracy. Here, we mainly consider the potential attacks against BCS and CB identified by Rathgeb and Uhl [55]. Table 2 summarizes different security/attack parameters and the security capability of typical BCS and CB approaches as well as that of the BC mechanism.

1) *Substitution attack*: This is a typical attack on biometric salting when an attacker obtains secret transform parameters or secret keys [55]. In such an attack, the attacker alters the contents of a stored biometric credential [59]. Performing such an attack is difficult in our system if a physical RS is used and RS biometrics is sampled on-the-fly for each authentication request, since this system does not store RS logically and it is more robust against remote attacking attempts to RS. Without the RS, forging a BC is difficult.

2) *Blended substitution attack*: This is a typical attack on fuzzy vault in which a user's template and the attacker's template can be merged into one single template for authentication [55]. The mixing of user's BC and the attacker's BC generates a gabble result since the BC itself is a mixing of the user biometrics and the RS biometrics.

3) *Brute force attack*: Some BCS approaches suffer from brute force attacks when the generated keys are short [55]. According to our property analysis in Section 3.8, BC provides quite large search space, and the brute force attack against BC is difficult.

4) *Attacks on error correction code*: Improper utilization of error correction codes could make some fuzzy commitment

2. For comparison purpose, the CMR is obtained when the IrisCode set is partitioned into two subsets and assumed to be the IrisCode sets for two different systems.

TABLE 2
Key Approaches Security Summaries

Potential Attack	Fuzzy Commitment	Shielding function	Fuzzy Vault	Key Generation	Non-invertible transform	Biometric salting	ours
Substitution	R	NK	NK	NK	S (lost token)	SP	R
Blended Substitution	NK	NK	S	NK	NK	NK	R
Brute force	SP	NK	SP	SP	NK	NK	RP
Attacks on error correction code	SP	NA	NA	NA	NA	NA	NA
Attacks on chaff points	NA	NA	SP	NA	NA	NA	NA
False acceptance attacks	NK	NK	NK	S	NK	S (stolen token)	RP
Record Multiplicity Collusion (same secret)	SP	SP	SP	SP	SP	NK	RP
Cross matching attack (different secret)	SP	S	SP	NK	NK	NK	RP
Internal collusion attack	NK	NK	NK	NK	NK	NK	RP
"Lost-token (secret)"	SP	NK	SP	NK	S	S	RP

SP: Suffer Possible; NK: Not Known; RP: Resistant Proved: NA: Not Applicable; S: Suffer; R: Resistant

schemes security and privacy vulnerable according to existing studies [36], [54], [55], however such attack is not applicable to the BC mechanism.

5) *Attacks on chaff points*: The security of a fuzzy vault relies highly on the methodology of generating chaff points [13], [55], but such an attack is not applicable to the BC mechanism.

6) *False acceptance attacks*: The performance of some BCS and CB, as compared to conventional biometric systems, is decreased [55]. In particular, some biometric salting in the event of a lost token suffers from this attack [55]. Our experimental results demonstrate that the BC approach does not display significant degradation on system performance, thus the BC approach is less vulnerable to it.

7) *Attack via record multiplicity (Collusion attack)*: Some constructions of fuzzy vault and fuzzy commitment suffer from this attack in the case that an attacker possesses multiple invocations of the same secret [6]. In the BC mechanism, we consider that attackers get copies of BCs using the same secret (i.e., RS). Such collusion attack, as we analyzed in Theorem 3, is hard.

8) *Cross matching (linkability) attack*: It is demonstrated that any quantization approach suffers from this cross matching attack [8], [55], thus infringing user privacy. Our security proof and experimental results justify that the cross matching in the BC mechanism is difficult.

9) *Internal collusion attack*: Insiders collect their BCs generated using the same system secret (RS) and try to obtain the secret [55]. Considering the fact that such an attack requires the attackers (insiders of the system) to share their biometrics (and they may reluctantly do so [55]), this type of attack could be rare. Regardless, such an attack, as analyzed in Theorem 4, is hard.

10) *"Lost-token"*: Some approaches exhibit high vulnerability when attackers are in possession of secret tokens [38], [55]. However, our security analysis demonstrates that even though the system secret (RS) is compromised, attackers cannot use it to further derive another user's biometrics.

Through the above comparisons and analysis, it is evident that the BC approach is able to defeat various attacks which challenge existing approaches. Regarding to authentication performance, as is known in biometric practice image distortion and low-quality make it hard to achieve zero FAR with concurrent zero FRR. By adjusting the threshold of accepting or rejecting the user authentication, the systems actually balance the FAR and the FRR. In the following, we will compare the BC approach to existing typical approaches by providing the FRRs (with corresponding FARs) and other factors related to system performance.

Table 3 summarizes key approaches to BCS and CB, as well as the BC approach. For comparison, we implemented the BC approach on both the ICE2005 and CASIAv1.0 [11] databases. As a typical fuzzy commitment approach, Hao et al.'s scheme [27] presents an impressive FRR result. However, according to Bringer et al. [7], the 700 images in their experiment are ideal, and the approach does not perform as well as the same parameters on the ICE database while also giving too large a rate of FRR (e.g., 10 percent of FRR with 0.80 percent of FAR). And its 44 bits operation security is not adequate in current cryptographic applications. Another fuzzy commitment scheme proposed by Rathgeb and Uhl [52] obtains a 4.92 percent FRR for CASIAv3 database using training. The BC approach does not use training, and on the entire ICE set gives a 0.94 percent EER, and 4.12 percent FRR when FAR is set to 10^{-5}, on ICE quality image set (Note: quality image is not equivalent to ideal image) gives a 0.29 percent EER, 0.96 percent FRR when FAR is 10^{-5}, and 1.58 percent FRR when FAR is set to 0. According to Bringer et al. [7] there is a theoretical limit

TABLE 3
Key Approaches Performance Comparisons

Authors	Category	Performance(%)	Remarks
Hao *et al.* [27]	Fuzzy commitment	0.47 FRR/0 FAR	ideal images; 44 bit security
Rathgeb *et al.* [52]	Fuzzy commitment	4.92 FRR	training; CASIAv3
Wu *et al.* [66]	Fuzzy vault	5.56 FRR/0 FAR	training; partial images from CASIAv1.0
Rathgeb *et al.* [53]	Quantization	4.91 FRR	5 enroll samples; CASIAv3
Hammerle *et al.* [26]	Cancelable	1.3 EER	CASIAv3
Ouda *et al.* [46]	Cancelable	2.31 EER	CASIAv3; partial images; training
Ours	Hybrid	0.94 EER (entire ICE) 0.61 EER (entire CASIAv1.0) 1.58 FRR/0 FAR (quality ICE)	no training, no requirements on multiple samples, test on both non-ideal and ideal, quality and entire data set

for the systems using classic error correction codes on achievable optimal FRR for ICE, which is FRR 2.49 percent for key length 42, 4.87 percent for key length 80 and 9.1 percent for key length 128 if an optimal error correction code is available. The security strength of these systems is equal to the length of the key. And the security of our system depends on BC, whose security strength is much longer than 128 bits as analyzed in Section 3.8. Furthermore, the key is used directly for matching and authentication, thus the goal is to obtain longer and 100-percent stable keys from multiple biometrics. In contrast, the keys in our BC system are not used for matching but for transformation and fusion of a users biometrics and the RS biometrics. The roles of keys in two mechanisms are not the same, thus, the performance comparison between systems using classical error correction codes and ours in terms of key length does not give much sensible information. However, if we could literally compare the security strength of the systems using classic error correction codes and the BC system in terms of key length, we can analyze as follows. The BC scheme extracts keys based on total 12,000 biometric features of each preprocessed image and the key length is 12,000 (in bits). The key strength (as analyzed earlier) is 224 (in bits). Thus, the keys in BC longer than 128 will have better security strength; furthermore, the performance of our BC scheme in terms of FRR is better.

A fuzzy vault approach for iris was presented by Wu et al. [66]. It uses CASIAv1.0 and chooses three good quality images out of seven for each subject, uses two images for each subject for training, and the other one for test, and obtains 5.56 percent FRR. Rathgeb and Uhl [53] proposed a quantization approach to generate keys, and obtained 4.91 percent FRR for CASIAv3. It considered that every subject would provide five enroll samples to obtain the quantization parameters. The proposed BC mechanism does not need training and does not require multiple enrollment samples.

Hammerle-Uhl et al. [26] and Ouda et al. [46] developed cancelable biometrics for iris, and they used CASIAv3 database and obtained 1.3 and 2.31 percent EER respectively when applying the approach on entire CASIAv3 and partial images (with training). For some experiments, we were not able to obtain some details, e.g., how they select good quality images, how they train, etc. We used the entire CASIAv1.0 database, and our EER result is 0.61 percent. If we use quality images according to our criteria, we can obtain 0 EER.

The security and authentication accuracy of the BC approach is comparable to and outperforms some BCS and CS approaches through the comparison. The comparison also establishes a good position for the BC mechanism; it is different from current multi-model approaches [57] (e.g., combining iris and face) and hybrid methods (e.g., [41] using user biometrics and additional PIN, [42] integrating fuzzy vault with fuzzy commitment). The proposed BC approach involves a key extraction from user biometrics and also a transformation of user biometrics through fusion. As it uses one factor (i.e., user's single biometrics) without additional PIN/password, we suggest it is a new category.

5 Related Work

Emerging techniques for user authentication involve traditional biometric authentication, cognitive authentication, BCS, CB and the hybrid approach.

Traditional biometrics binds users to their biological traits, either physiological traits (e.g., iris [20], palmprint [18], sclera [69]) or behavior traits (e.g., mouse dynamics [3], gait [67]). As indicated previously, a limitation of traditional biometrics is security, user privacy risk and irreplaceability.

Cognitive biometrics [24], [56] can be used to improve the revocability property. Cognitive biometrics represents a new approach which generates a "thought signature" of people using biological signals that characterize the brain's response to certain stimuli, giving a high degree of uniqueness to the individual. Revocability is provided by training a new thinking process and generating a new "thought signature" to replace the compromised one. However, catching brain signals requires special equipment. Also, the thinking process may change over time.

Biometric cryptosystems can be used for user authentication by matching the exactness of the outputted keys. The majority of BCSs require some biometric-dependent public information (known as helper data), which is not supposed to reveal much information about the biometrics; with the helper data, the cryptographic key is retrieved or extracted from the query biometrics. The helper data are either obtained by binding a chosen key to biometrics or derived only from biometrics. BCSs use different techniques to deal with biometric variance; for example, some schemes apply error correction codes [32], [33], while some others apply quantization [65]. The introduction of helper data, in some circumstances (e.g., when multiple copy of helper data extracted from the single biometrics are obtained) may create vulnerabilities [28], [37], [60]. However, without using helper data it is believed that extracting a sufficiently long and revocable key is not feasible because of the information entropy limitation of most biometric characteristics [55]. Utilizing error-correction codes and cryptography, a concept secure sketch is generalized which allows error correction of a noisy input. Secure sketches can be used as primitives to build fuzzy extractors which extract a uniformly random string [21]. Secure sketches and fuzzy extractors, as primitive formalisms, have been used in concrete BCSs. Quantization has also been used frequently in BCSs [51], [53]. In the BCS using quantization techniques, several enrollment samples are trained to derive appropriate intervals for feature quantization. As in [53], the authors apply a context-based reliable component selection and construct intervals for the most reliable features of each subject. Such approaches require multiple samples from each subject to reliably extract helper data.

Cancelable biometrics applies a transformation on traditional biometrics and matches the biometrics in a transformed domain for authentication. Cancelable biometrics was first introduced by Ratha et al. in [50]. Pillai et al. presented a CB approach using random projections which embed biometrics from a higher dimensional space to a lower dimensional space [48]; however, it is shown that the system is less secure if an attacker obtains both the random projection parameters and the transformed

patterns. Biotoken was proposed by [4] to transform original biometric feature via scaling and translation into a transformed version; the transformed feature is then split into a stable part termed integer and unstable part. There are several questions associated with this approach, namely, how to design the function which separates biometric features into stable and unstable parts, and how to apply the approach to other biometrics. Ouda et al. [45] proposed a tokenless cancelable biometrics. This approach extracts consistent bits from original iris codes by training a set of images from each subject. The consistent bits are mapped to another set of bits (system selected) to constitute the protected BioCode. This approach requires an enrolling user to provide enough training images to satisfy the "consistence". The discriminative capability of the "consistent" sequence determines the performance; the length of a "consistent" sequence is critical to the security, which is not shown in the paper.

Some hybrid approaches using both BCS or CB are proposed. The biohashing scheme [16], [31] operates as a key-binding scheme but combined user-specific tokenized random numbers to generate a set of binary bit strings. Given the binary string, it is not feasible to recover biometric data. Several works note that the improved performance of biohashing could be achieved with subject-specific tokenized random numbers [14], [15], however if the token is stolen, the system accuracy deteriorates. Nandakumar et al. proposed a hardened fuzzy vault using a user-specific secret key or password [44]. Introducing user-specific information, however, has an impact on the usability of the biometric system. It was also pointed out that such a "stolen-key scenario" must be considered for system evaluation, otherwise biometrics is trivial since the system could rely on the key without any complications [38]. Introducing the additional factor, which is not intrinsically bound to the user, logically creates more vulnerabilities. It could suffer from the same issues of traditional proxy-based systems in that information can be stolen, lost or forgotten. The user-specific key is an additional factor correlated to each individual, which has the chance to reveal user-privacy. Further introducing a so-called user-specific key makes the identification under non-cooperative identification troublesome.

6 Conclusion

In this paper, we proposed a user-friendly, secure, privacy-preserving and revocable secure-fusion based biometric authentication method. The proposed approach involves key extraction: the extracted key is used in a "secure fusion" for mixing the user's biometrics and a reference subject's biometrics, and the fused biometrics is fed into an existing biometric system to generate a BioCapsule for authentication. The proposed BC mechanism has many desired features: 1) security analysis shows that the approach is secure and able to defeat various attacks, thus the security of the user biometrics is guaranteed and the user privacy is preserved; 2) experimental results prove the revocability of the proposed approach; 3) both security analysis and experimental results justify the cross-matching resistance of the proposed approach; 4) comparisons with existing approaches and the experimental results show comparable performance to traditional approaches and other BCS and CB systems; 5) the BC mechanism is generally applicable to typical biometric modules verified through experiments, thus, it can be fed into newly designed biometric systems to continuously enhance the authentication accuracy in the long run; 6) the cross-matching resistance enables the interoperability of the BC system, and it supports "one-click sign-on" across multiple systems by using a distinct RS; and 7) the system does not require user training, and is both easy to use and transparent to end-users since they are not required to remember a password or carry a token. These features make the proposed BC mechanism a user-centric authentication approach. We will continue to extend our study to other biometrics (e.g., face) and investigate the integration of the fusion at different biometric processing levels. We are also interested in extending the application of the proposed BC mechanism in a broader context, for instance, active and non-intrusive authentication.

Acknowledgments

The authors would like to thank the anonymous reviewers and editors for the time and effort they have invested in reviewing our manuscript and for providing constructive comments. Also the authors thank the NIST for the ICE 2005 [2], University of Beira Interior for UBIRIS [49], and the Chinese Academy of Sciences' Institute of Automation for the CASIAv1.0 [11]. This work was partially supported by IU CACR grant.

References

[1] http://en.wikipedia.org/wiki/Usability, 2013.
[2] http://iris.nist/gov/ice/, 2013.
[3] A. Ahmed and I. Traore, "A New Biometric Technology Based on Mouse Dynamics," *IEEE Trans. Dependable and Secure Computing*, vol. 4, no. 3, pp. 165-179, July/Sept. 2007.
[4] T. Boult, "Robust Distance Measures for Face-Recognition Supporting Revocable Biometric Tokens," *Proc. Seventh Int'l Conf. Automatic Face and Gesture Recognition*, pp. 560-566, Apr. 2006.
[5] T. Boult, W. Scheirer, and R. Woodworth, "Revocable Fingerprint Biotokens: Accuracy and Security Analysis," *Proc. IEEE Conf. Computer Vision and Pattern Recognition*, pp. 1-8, June 2007.
[6] X. Boyen, "Reusable Cryptographic Fuzzy Extractors," *Proc. 11th ACM Conf. Computer and Comm. Security (CCS '04)*, pp. 82-91, 2004.
[7] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zemor, "Theoretical and Practical Boundaries of Binary Secure Sketches," *IEEE Trans. Information Forensics and Security*, vol. 3, no. 4, pp. 673-683, Dec. 2008.
[8] I. Buhan, J. Breebaart, J. Guajardo, K. de Groot, E. Kelkboom, and T. Akkermans, "A Quantitative Analysis of Indistinguishability for a Continuous Domain Biometric Cryptosystem," *Proc. 4th Int'l Workshop, and Second Int'l Conf. Data Privacy Management and Autonomous Spontaneous Security*, pp. 78-92, 2010.
[9] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis, "Constructing Practical Fuzzy Extractors Using QIM," Technical Report TR-CTIT-07-52 2007.
[10] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint Image Reconstruction from Standard Templates," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 29, no. 9, pp. 1489-1503, Sept. 2007.
[11] CASIA-IrisV1. http://biometrics.idealtest.org/, 2013.
[12] A. Cavoukian and A. Stoianov, "Biometric Encryption," *Encyclopedia of Biometrics*. Springer, 2009.
[13] E. Chang, R. Shen, and F. Teo, "Finding the Original Point set Hidden Among Chaff," *Proc. ACM Symp. Information, Computer and Comm Security (ASIACCS '06)*, pp. 182-188, 2006.

[14] K. Cheung, A. Kong, D. Zhang, M. Kamel, and J. You, "Revealing the Secret of Facehashing," *Proc. Int'l Conf. Advances in Biometrics*, pp. 106-112, 2006.

[15] K. Cheung, A. Kong, D. Zhang, M. Kamel, J. You, and H. Lam, "An Analysis on Accuracy of Cancellable Biometrics Based on Biohashing," *Proc. Ninth Int'l Conf. Knowledge-Based Intelligent Information and Eng. Systems (KES '05)*, pp. 1168-1172, 2005.

[16] C. Chin, A. Jin, and D. Ling, "High Security Iris Verification System Based on Random Secret Integration," *Computer Vision and Image Understanding*, vol. 102, no. 2, pp. 169-177, May 2006.

[17] A. Ciaramella, P. D'Arco, A. De Santis, C. Galdi, and R. Tagliaferri, "Neural Network Techniques for Proactive Password Checking," *IEEE Trans. Dependable and Secure Computing*, vol. 3, no. 4, pp. 327-339, Oct./Dec. 2006.

[18] J. Dai, J. Feng, and J. Zhou, "Robust and Efficient Ridge-Based Palmprint Matching," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 34, no. 8, pp. 1618-1632, Aug. 2012.

[19] P. D'Arco and A. De Santis, "On Ultralightweight RFID Authentication Protocols," *IEEE Trans. Dependable and Secure Computing*, vol. 8, no. 4, pp. 548-563, July/Aug. 2011.

[20] J. Daugman, "How Iris Recognition Works," *IEEE Trans. Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21-30, Jan. 2004.

[21] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," *Proc. Advances in Cryptology (Eurocrypt)*, vol. 3027, pp. 523-540, 2004.

[22] Y. Du, R. Ives, D. Etter, and T. Welch, "Use of One-Dimensional Iris Signatures to Rank Iris Pattern Similarities," *Optical Eng.*, vol. 45, no. 3, 2006.

[23] G. Duggan, H. Johnson, and B. Grawemeyer, "Rational Security: Modelling Everyday Password Use," *Int'l J. Human-Computer Studies*, vol. 70, no. 6, pp. 415-431, 2012.

[24] L. Faria, V. Sa, and S. de Magalhaes, "Multimodal Cognitive Biometrics," *Proc. Sixth Iberian Conf. Information Systems and Technologies (CISTI)*, pp. 1-6, June 2011.

[25] J. Gallier, *Discrete Mathematics (Universitext Series)*. Springer, 2011.

[26] J. Hammerle Uhl, E. Pschernig, and A. Uhl, "Cancelable Iris Biometrics Using Block Re-Mapping and Image Warping," *Proc. 12th Int'l Conf. Information Security*, pp. 135-142, 2009.

[27] F. Hao, R. Anderson, and J. Daugman, "Combining Crypto with Biometrics Effectively," *IEEE Trans. Computers*, vol. 55, no. 9, pp. 1081-1088, Sept. 2006.

[28] T. Ignatenko and F.M.J. Willems, "Information Leakage in Fuzzy Commitment Schemes," *IEEE Trans. Information Forensics and Security*, vol. 5, no. 2, pp. 337-348, June. 2010.

[29] A. Jain, K. Nandakumar, and A. Nagar, "Biometric Template Security," *EURASIP J. Advances in Signal Processing*, vol. 2008, no. 113, pp. 1-17, 2008.

[30] A. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Trans. Circuits and Systems for Video Technology*, vol. 1, no. 1, pp. 4-20, Jan. 2004.

[31] A. Jin, D Ling, and A. Goh, "Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenized Random Number," *Elsevier Pattern Recognition*, vol. 37, pp. 2245-2255, 2004.

[32] A. Juels and M. Sudan, "A Fuzzy Vault Scheme," *Designs, Codes and Cryptography*, vol. 38, pp. 237-257, 2006.

[33] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme," *Proc. Sixth ACM Conf. Computer and Comm. Security (CCS '99)*, pp. 28-36, 1999.

[34] H. Jung, K. Park, and J. Kim, "Depth of Capture Volume Extension by Constrained Least Square-Based Image Restoration, Quantitative Evaluation," *Optical Engineering*, vol. 49, no. 4, pp. 047004-047004-13, 2010.

[35] P. Kahl, "Solving Narrow-Interval Linear Equation Systems Is NP-Hard," (January 1, 1996). ETD Collection for University of Texas, El Paso. Paper AAIEP04846.

[36] D. Karakoyunlu and B. Sunar, "Differential Template Attacks on PUF Enabled Cryptographic Devices," *Proc. IEEE Int'l Workshop Information Forensics and Security (WIFS)*, pp. 1-6, Dec. 2010.

[37] E. Kelkboom, J. Breebaart, T. Kevenaar, I. Buhan, and R. Veldhuis, "Preventing the Decodability Attack Based Cross-Matching in a Fuzzy Commitment Scheme," *IEEE Trans. Information Forensics and Security*, vol. 6, no. 1, pp. 107-121, Mar. 2011.

[38] A. Kong, K. Cheung, D. Zhang, M. Kamel, and J. You, "An Analysis of Biohashing and Its Variants," *Pattern Recognition*, vol. 39, no. 7, pp. 1359-1368, July 2006.

[39] L. Masek, "Recognition of Human Iris Patterns for Biometric Identification," technical report, Univ. of Western Australia, 2003.

[40] H.G. Miller and J.L. Fisher, "Requiring Strong Credentials: What's Taking So Long?" *IT Professional*, vol. 12, no. 1, pp. 57-60, Jan./Feb. 2010.

[41] F. Monrose, M. Reiter, and S. Wetzel, "Password Hardening Based on Keystroke Dynamics," *Proc. Sixth ACM Conf. Computer and Comm. Security (CCS '99)*, pp. 73-82, 1999.

[42] A. Nagar, K. Nandakumar, and A. Jain, "A Hybrid Biometric Cryptosystem for Securing Fingerprint Minutiae Templates," *Pattern Recognition Letters*, vol. 31, no. 8, pp. 733-741, June 2010.

[43] K. Nandakumar, A. Jain, and S. Pankanti, "Fingerprint-Based Fuzzy Vault: Implementation and Performance," *IEEE Trans. Information Forensics and Security*, vol. 2, no. 4, pp. 744-757, Dec. 2005.

[44] K. Nandakumar, A. Nagar, and A. Jain, "Hardening Fingerprint Fuzzy Vault Using Password," *Proc. Second Int'l Conf. Biometrics*, pp. 927-937, Aug. 2007.

[45] O. Ouda, N. Tsumura, and T. Nakaguchi, "BioEncoding: A Reliable Tokenless Cancelable Biometrics Scheme for Protecting Iriscodes," *IEICE Trans. Information and Systems*, vol. E93-D, no. 7, pp. 1878-1888, July 2010.

[46] O. Ouda, N. Tsumura, and T. Nakaguchi, "Tokenless Cancelable Biometrics Scheme for Protecting Iris Codes," *Proc. 20th Int'l Conf. Pattern Recognition (ICPR)*, pp. 882-885, Aug. 2010.

[47] P. Phillips, K. Bowyer, P. Flynn, X. Liu, and W. Scruggs, "The Iris Challenge Evaluation 2005," *Proc. Second IEEE Int'l Conf. Biometrics: Theory, Applications and Systems (BTAS '08)*, pp. 1-8, Oct. 2008.

[48] J. Pillai, V. Patel, R. Chellappa, and N. Ratha, "Secure and Robust Iris Recognition Using Random Projections and Sparse Representations," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 33, no. 9, pp. 1877-1893, Sept. 2011.

[49] H. Proena and L.A. Alexandre, "Ubiris: A Noisy Iris Image Database," *Proc. 13th Int'l Conf. Image Analysis and Processing*, pp. 970-977, 2005.

[50] N. Ratha, J. Connell, and R. Bolle, "Enhancing Security and Privacy in Biometrics-Based Authentication Systems," *IBM Systems J.*, vol. 40, pp. 614-634, 2001.

[51] C. Rathgeb and A. Uhl, "An Iris-Based Interval-Mapping Scheme for Biometric Key Generation," *Proc. Sixth Int'l Symp. Image and Signal Processing and Analysis*, pp. 511-516, Sept. 2009.

[52] C. Rathgeb and A. Uhl, "Adaptive Fuzzy Commitment Scheme Based on Iris-Code Error Analysis," *Proc. Second European Workshop Visual Information Processing (EUVIP)*, pp. 41-44, July 2010.

[53] C. Rathgeb and A. Uhl, "Privacy Preserving Key Generation for Iris Biometrics," *Proc. 11th IFIP TC 6/TC 11 Int'l Conf. Comm. and Multimedia Security*, pp. 191-200, 2010.

[54] C. Rathgeb and A. Uhl, "Statistical Attack against Iris-Biometric Fuzzy Commitment Schemes," *Proc. IEEE Conf. Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 23-30, June 2011.

[55] C. Rathgeb and A. Uhl, "A Survey on Biometric Cryptosystems and Cancelable Biometrics," *EURASIP J. Information Security*, vol. 2011, no. 3, pp. 1-25, 2011.

[56] K. Revett and S. Tenreiro de Magalhes, "Cognitive Biometrics: Challenges for the Future," *Proc. Sixth Int'l Conf. Global Security, Safety, and Sustainability*, pp. 79-86, 2010.

[57] A. Ross, K. Nandakumar, and A. Jain, "Introduction to Multibiometrics," *Handbook of Biometrics*, pp. 271-292, Springer, 2008.

[58] A. Ross, J. Shah, and A. Jain, "From Template to Image: Reconstructing Fingerprints from Minutiae Points," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 544-560, Apr. 2007.

[59] W. Scheirer and T. Boult, "Cracking Fuzzy Vaults and Biometric Encryption," *Proc. Biometrics Symp.*, pp. 1-6, Sept. 2007.

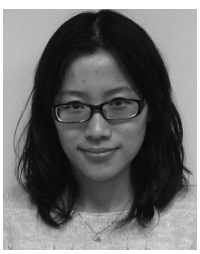
[60] K. Simoens, P. Tuyls, and B. Preneel, "Privacy Weaknesses in Biometric Sketches," *Proc. 30th IEEE Symp. Security and Privacy*, pp. 188-203, May 2009.

[61] Y. Sui, X. Zou, and E. Du, "Biometrics-Based Authentication: A New Approach," *Proc. 20th Int'l Conf. Computer Comm. and Networks (ICCCN)*, pp. 1-6, Aug. 2011.

[62] K. Takahashi and T. Murakami, "A Metric of Information Gained Through Biometric Systems," *Proc. 20th Int'l Conf. Pattern Recognition (ICPR '10)*, pp. 1184-1187, 2010.

[63] U. Uludag, S. Pankanti, S. Prabhakar, and A. Jain, "Biometric Cryptosystems: Issues and Challenges," *Proc. IEEE*, vol. 92, no. 6, pp. 948-960, June 2004.

[64] E. Verbitskiy, P. Tuyls, C. Obi, B. Schoenmakers, and B. Skoric, "Key Extraction from General Nondiscrete Signals," *IEEE Trans. Information Forensics and Security*, vol. 5, no. 2, pp. 269-279, June 2010.
[65] C. Vielhauer, R. Steinmetz, and A. Mayerhoefer, "Biometric Hash Based on Statistical Features of Online Signatures," *Proc. 16th Int'l Conf. Pattern Recognition (ICPR '02)*, vol. 1, pp. 123-126, 2002.
[66] X. Wu, N. Qi, K. Wang, and D. Zhang, "A Novel Cryptosystem Based on Iris Key Generation," *Proc. Fourth Int'l Conf. Natural Computation*, vol. 4, pp. 53-56, Oct. 2008.
[67] J. Zhang, J. Pu, C. Chen, and R. Fleischer, "Low-Resolution Gait Recognition," *IEEE Trans. Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 40, no. 4, pp. 986-996, Aug. 2010.
[68] L. Zhang, Z. Sun, T. Tan, and S. Hu, "Robust Biometric Key Extraction Based on Iris Cryptosystem," *Proc. Third Int'l Conf. Advances in Biometrics (ICB '09)*, pp. 1060-1069, 2009.
[69] Z. Zhou, E. Du, N. Thomas, and E. Delp, "A New Human Identification Method: Sclera Recognition," *IEEE Trans. Systems, Man, and Cybernetics, Part A: Systems and Humans*, vol. 42, no. 3, pp. 571-583, May 2012.



Yan Sui received the MS degree in computer science from Indiana University-Purdue University Indianapolis in 2009. She is currently working toward the PhD degree with the Department of Computer and Information Science of Indiana University-Purdue University Indianapolis. Her research interest includes network security, and biometric security and privacy. She received the university fellowship in 2007 and the Gersting Award as the outstanding graduate student of School of Science in 2009.

Xukai Zou received the PhD degree in computer science from the University of Nebraska-Lincoln. His current research focus is applied cryptography, network security, biometrics, authentication and communication networks. He is a faculty member with the Department of Computer and Information Sciences at Indiana University-Purdue University Indianapolis. His research has been supported by US National Science Foundation (NSF), the Department of Veterans Affairs and Industry such as Cisco and Northrop Grumman.

Eliza Y. Du received the the BS and MS degrees in electrical engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1996 and 1999, respectively, and the PhD degree in electrical engineering from the University of Maryland, Baltimore County, Baltimore, in 2003. She is currently an associate professor with the Department of Electrical and Computer Engineering at Indiana University-Purdue University Indianapolis (IUPUI), Indianapolis. From September 2003 to July 2005, she was an assistant research professor with the Electrical Engineering Department at the United States Naval Academy. Her research interests include image processing, pattern recognition, and biometrics. Her research has been funded by the Office of Naval Research, National Institute of Justice, Department of Defense, National Science Foundation, Canada Border Services Agency, Indiana Department of Transportation, and several industry and IUPUI internal grants. She received an Office of Naval Research (ONR) Young Investigator award in 2007, the Indiana University Trustee Teaching Award in 2009, the Supervisor of the Year Award at IUPUI in 2009, and the Best Paper Award with her students in IEEE Workshop on Computational Intelligence in Biometrics: Theory, Algorithms, and Applications in 2009. She is a member of the honor societies Tau Beta Pi and Phi Kappa Phi.

Feng Li received the PhD degree in computer science from Florida Atlantic University in August 2009. His PhD advisor was Dr. Jie Wu. He joined the Department of Computer, Information, and Leadership Technology at Indiana University-Purdue University Indianapolis (IUPUI) as an assistant professor in August 2009. His research interests include the areas of wireless networks and mobile computing, security, and trust management. He has published more than 30 papers in conferences and journals.