Graduate School ETD Form 9
(Revised 12/07)

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Yan Sui

Entitled
Design and Evaluation of a Secure, Privacy-Preserving
and Cancelable Biometric Authentication: Bio-Capsule

For the degree of Doctor of Philosophy

Is approved by the final examining committee:

Xukai Zou
Chair

Feng Li

Elisa Bertino

Ninghui Li

Eliza Du

To the best of my knowledge and as understood by the student in the *Research Integrity and Copyright Disclaimer (Graduate School Form 20)*, this thesis/dissertation adheres to the provisions of Purdue University's "Policy on Integrity in Research" and the use of copyrighted material.

Approved by Major Professor(s): Xukai Zou

Approved by: Sunil Prabhakar / William J Gorman 07/03/2013
Head of the Graduate Program Date

DESIGN AND EVALUATION OF A SECURE, PRIVACY-PRESERVING AND CANCELABLE BIOMETRIC AUTHENTICATION: BIO-CAPSULE

A Dissertation

Submitted to the Faculty

of

Purdue University

by

Yan Sui

In Partial Fulfillment of the

Requirements for the Degree

of

Doctor of Philosophy

August 2013

Purdue University

West Lafayette, Indiana

ACKNOWLEDGMENTS

This dissertation would not be done without the help and support of many people.

I would like to express my gratitude to my advisors Prof. Xukai Zou and Prof. Elisa Bertino for their great support and help as I worked on graduate courses and the dissertation. Their supervision helped expedite my research and new discoveries.

I would also like to thank my committee members Prof. Ninghui Li, Prof. Eliza Du, and Prof. Feng Li for their time and guidance. I am also thankful to many department staff, including, but not limited to, Dr. Gorman, Sandra, Nicole, Scott, all people and students from my department, for their patience and help as they came along with me during this process.

Finally, I would like to thank my families for their love and support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SYMBOLS

u:	a user to be authenticated.
RS:	a Reference Subject.
D^u:	biometric data or patterns of user u.
F^u:	biometric feature of user u.
T^u:	biometric template of user u.
K^u:	biometric key of user u.
BC^u:	Biometric Capsule (or Bio-Capsule or BC) of user u.
Ext^K:	key extraction procedure.
Ext^F:	feature extraction procedure.
$Fuse$:	fusion procedure.
I:	grayscale value of a pixel.
s:	iris signature.

ABBREVIATIONS

BC:	Biometric Capsule (BioCapsule).
BCS:	Biometric CryptoSystem.
CB:	Cancelable Biometrics.
RS:	Reference Subject.
ECG:	ElectroCardioGram.
EEG:	ElectroEncephaloGram.
EDR:	ElectroDermal Response.
RFID:	RadioFrequency IDentification.
CMR:	Cross-Matching Resistance factor.
FAR:	False Acceptance Rate.
FRR:	False Rejection Rate.
EER:	Equal Error Rate.
BSE:	Biometric System Entropy.
LTP:	Local Texture Pattern.
BCE:	BioCapsule Extractor.
SNR:	Signal-to-Noise Ratio.
ROC:	Receiver Operating Characteristic.
FSCU:	Frame to Safe Continue Use.
FCR:	Frame to Correct Reject.
SC:	Security Characteristic.
USC:	Usability-Security Characteristic Curve.

ABSTRACT

Sui, Yan Ph.D., Purdue University, August, 2013. Design and Evaluation of a Secure, Privacy-Preserving and Cancelable Biometric Authentication: Bio-Capsule. Major Professors: Professor Xukai Zou and Professor Elisa Bertino.

A large portion of system breaches are caused by authentication failure either during the system login process or even in the post-authentication session, which is further related to the limitations associated with existing authentication approaches. Current authentication methods, whether proxy based or biometrics based, are hardly user-centric; and they either put burdens on users or endanger users' (biometric) security and privacy. In this research, we propose a biometrics based user-centric authentication approach. The main idea is to introduce a reference subject (RS) (for each system), securely fuse the user's biometrics with the RS, generate a BioCapsule (BC) (from the fused biometrics), and employ 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 multiple 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 the user's post-authentication on-line session. In this research, we also formally prove that the proposed secure fusion based BC approach is secure against various attacks and compare the new approach with existing biometrics based approaches. Extensive experiments show that the performance (i.e., authentication accuracy) of the new BC approach is comparable to existing typical biometric authentication approaches, and the new BC approach also possesses other desirable features such as diversity and revocability.

1 INTRODUCTION

User-proxy based authentication (e.g., password, security token) has been well developed and widely used, it is also both effective and efficient in user authentication [1, 2]. However, the growth in user-credential theft in proxy based authentication and the increased security requirements have prompted investigation of alternative authentication [3, 4]. A central theme of authentication is to authenticate users against characteristics intrinsically linked with human users rather than some external factors [3]. A promising direction emerging from this effort is biometrics [5], which binds users to their biological traits.

Biometrics is a technology which uses physiological or behavioral characteristics to identify or verify a person. Typical characteristics used for authentication include fingerprint, face, and iris. A conventional biometric authentication system consists of two phases: enrollment and verification as shown in Figure 1.1. During the enrollment phase, biometric features are extracted from a user's biometric data and a template is created and stored. During the verification phase, the same feature extraction algorithm is applied to query biometric data, and the resulting query features are used to construct a query template. The query template is matched against the stored template(s) for authentication. Compared to password/smartcard-based authentication approaches, biometrics-based solutions have many desired features such as *being resistant to losses* incurred by theft of passwords and smartcards, as well as *user-friendliness*. Biometrics is "what you are" and using biometrics for authentication frees users from carrying smartcards, storing PINs, or remembering passwords. Biometrics cannot be easily lost or forgotten. Biometrics bears a user's identity and it is not easy to be forged.

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 signals can be reconstructed from the biometric templates [6, 7].

Recently, Galbally *et al.* has demonstrated a successful reconstruction of the iris image from an iris template (e.g., binary iriscode) such that synthetic iris images are very realistic and there is a high chance that they can break into an iris recognition system [8]. Given a compromised template (e.g., iriscode) B of a user, the proposed approach reconstructed a normalized iris image I_R who associates with iriscode B_R, and the attack is successful when $Similarity(B, B_R) \geq \sigma$, where σ is the matching threshold of the iris recognition system. The approach applies the genetic algorithm which is a heuristic search tool to optimize the $Similarity(B, B_R)$. The proposed approach uses the 1D Log-Gabor approach for the development stage to reconstruct the iris images in BioSecure database using their iriscodes and uses these reconstructed images to test the vulnerabilities of a commercialized iris recognition system – VeriEye. It is also shown that the success rate is around 86% for a low security point (i.e., FAR = 0.1%) and around 75% for a very high security point (i.e., FAR=0.0001%). This recent work demonstrates that attacks are possible if the stored templates (i.e., iriscode) are obtained by the attacker. To avoid the stored templates being compromised, template encryption and many other template protection techniques are needed. However, it is worthy of further efforts to investigate if the existing and also the proposed approaches can effectively defeat such probabilistic reconstruction attack. As observed in this work, iriscodes obtained from one system (1D Log-Gabor system) can help to attack on a different system (VeriEye). Using different RSs in distinct systems could make such attack more difficult. Yet, it is challenging to give a formal analysis how difficult it is to perform such an attack on the existing template protection and proposed BC techniques.

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 of the human user (e.g., gender, possible disease).

According to [3], an ideal secured biometric system possesses the following properties:

- Security and Privacy: it is computationally hard to obtain the original biometrics from the stored data, e.g., the secured template, the helper data, and the system is

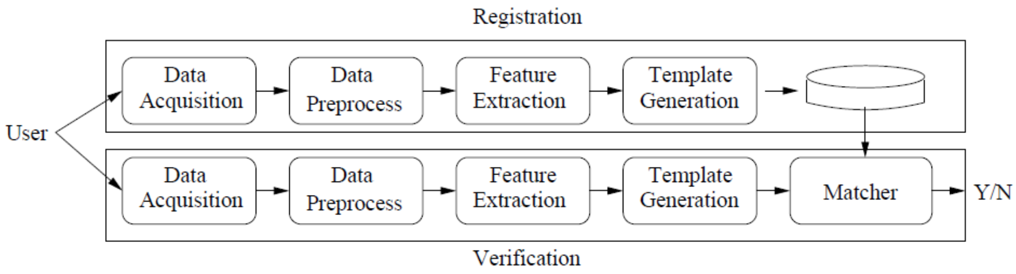


Figure 1.1.: Conventional biometric authentication

able to defeat various attacks. The usage of biometrics does not reveal user privacy information.

- Revocability (Cancelability): it is feasible to reissue a new template based on the same biometrics, thus a compromised template is revocable.
- Diversity and Cross-matching Resistance: based on the same biometrics, different versions of secured biometric templates can be generated, while the secured templates do not allow cross-matching among databases.
- Performance: the distinguishability of the original biometrics is properly maintained, thus the system performance is not degraded.

Intensive research has been conducted to address the security and revocability of biometrics as well as the user privacy, and concepts like biometric cryptosystem (BCS) [9–16] and cancelable biometrics (CB) [17–21] have emerged from this research. Biometric cryptosystem was originally developed for securing a cryptographic key using biometrics or directly generating a cryptographic key from biometrics [22, 23], and it was further used to enhance the security of an existing secret [24, 25]. BCS can be used for authentication by matching the exactness of outputted keys. Cancelable biometrics applies a transformation function to the biometrics and matches the biometrics in the transformed domain [17]. The usage of the transformation provides both cancelability and privacy-preservation, and the irreversibility of the transformation provides security.

Typical authentication approaches do not distinguish the initial log-in user from the current user during an open session of the system as long as the session remains active. Thus, attackers can target at a post-authentication session, which may cause system breaches.

Active authentication seeks to address this problem by developing ways to continuously sample credentials from a user to validate user's identity. An effective active authentication needs to be non-intrusive and cost-effective, that is, the active authentication should be transparent to users and cause no (much) inconvenience for the users to accomplish their usage of the system [26].

A promising direction is biometrics. Biometrics can be collected in a non-intrusive way, thus users are not asked for active cooperation. Without distracting the users, biometrics authentication can be incorporated into the system. Also biometrics binds users to their intrinsically biological traits and can not be easily separated from users compared to other artificially-bound credentials, e.g., passwords, tokens. In a sense, biometrics can provide more safety. However, there are several challenges for utilizing biometrics in active authentication. Firstly, biometrics collection is a fuzzy process, thus the system can face a situation that at a given time, poor quality biometrics or no biometrics observations are obtained, e.g., face image collection when the user walked away from cameras, typing keystrokes when the user is listening to music. Secondly, the goal of active authentication is akin to detect the absence of the log-in user or the presence of an intruder efficiently (i.e., security), as well as maintain the legal usage of the system (i.e., usability). These two factors can be contradicting, and finding a good trade-off between them can be critical. Finally, the biometrics based active authentication requires innovative and attack-resilient solutions. Active authentication system repeatedly sends biometric credentials to the authentication server, thus besides the potential attacks of conventional one-time authentication system, e.g., replay attacks, etc., the attacker can accumulate more information about the user and perform other attacks, e.g., spoofing user biometrics through data accumulation. Biometrics is user-specific, and compromise of biometrics may reveal user private information (e.g., gender, possible disease) thus infringe user privacy.

Existing active authentication systems mostly focus on tackling the first two issues, while rarely consider system security and user privacy issues which have been identified in conventional one-time authentication [27, 28].

1.1 Current Status of Biometric Authentication

According to a recent survey [4], there are limitations associated with both BCS and CB. Compared to conventional biometric systems, a noticeable decrease [4,29] of the BCS performance is observed because of the hardness of alignments of biometrics and 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 [30] which is defined as $k \leq -\log_2 FAR$. For a generic cryptographic purpose (e.g., with a 128-bit key) maintaining an $FAR \leq 2^{-k}$ can be too rigorous and difficult to achieve in the BCS. Also the BCS uses helper data which contains information about biometrics and is a factor to affect the security and privacy leakage [31]. For the CB, the provable security (e.g., irreversibility and unlinkability) is hardly done, and for some approaches it is also a sophisticated work [4]. Also, in the case of hardness of alignments of biometrics and the complexity of transformation, performance decrease is also observed. However, some approaches can report an increase in performance, especially by introducing an additional factor, e.g., user-specific PIN/token, for transformation. According to [4], this performance gain can be caused by unpractical assumptions during evaluation, and the user-specific transformation parameters have to be assumed compromised for such evaluation. From [4], existing BCS and CB approaches have complications in addressing one or more above five properties.

1.2 Main Contribution of the Dissertation

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 proposed the BC concept in [32]. The BC generation method in [32] is based on the difference of the user's biometric feature and that of a proposed construct: reference subject (RS). However, there are some limitations related to such a difference based BC design. First, such a generation is at the feature level, thus its scope is limited. Secondly, the formal security proof is difficult to obtain and it generally assumes that the RS is a physical entity and physically protected.

In this dissertation, we present a brand new BC generation method based on "secure fusion" of the user biometrics and the RS biometrics. The fusion process applies to different levels of biometric processing such as signal, feature or template. Moreover, a (user-intrinsic) cryptographic key is extracted from the user's biometric feature and is used during the process of secure fusion. Thus, the new fusion based BC construction is more usable and flexible, and it is proven to be secure, resilient to different attacks, and tolerant to the disclosure of both the RS and BC (thus, the RS in this new method can be a physical or logical entity). The proposed BC approach can be applied in continuous authentication model to fulfill a secure and privacy-preserving continuous authentication.

1.3 Organization of the Dissertation

The rest of the dissertation is organized as follows. Related works are briefly reviewed in Chapter 2. Chapter 3 presents the newly proposed biometrics-based authentication approach. Section 3.2 introduces the model of the new BC based authentication. Section 3.3, Section 3.4 and Section 3.5 present the key components of the new BC based authentication: key extraction, secure fusion and the integration of secure fusion with existing biometric processes. Formal proof of security and privacy-preservation analysis is presented in Section 3.6. Chapter 4 presents experimental results of the proposed BC authentication. Chapter 5 presents the proposed BC-based continuous authentication approach. Chapter 6 presents experimental results of the proposed BC based continuous authentication. Chapter 7 further analyzes the BC approach by comparing it with existing ones from two aspects: security and performance, also it compares the BC based continuous authentication with current continuous authentication approaches. Chapter 8 draws our conclusions and presents our future work.

2 RELATED WORK

Emerging techniques for user authentication involve proxy-based authentication, traditional biometric authentication, cognitive authentication, BCS, CB and the hybrid approach. In the following, we discuss them one by one.

Proxy-based authentication uses either passwords, or identification cards and tokens [2, 33]. The primary limitation of proxy-based authentication is that a user's credentials are artificially bound to a user. Passwords and PINs can be forgotten or stolen, and the identification cards and tokens can be lost and also stolen. Once those are acquired by the attacker, the attacker has total access to the user's resources. Also, there is no protection against repudiation by user's credentials. User's credentials can be shared with a colleague, and there is no way for the system to distinguish the actual user from the illegitimate one. Traditional proxy-based authentication has become inadequate in this way. Moreover, memorizing/carrying (multiple) PINs/tokens is difficult for individuals and reuse of a PIN/token across systems can result in cross-system breaches [34].

Traditional biometrics provides an alternative for proxy-based authentication. Biometrics binds users to their biological traits, either physiological traits, e.g., iris [35], palmprint [36], sclera [37], or behavior traits, e.g., mouse dynamics [38], gait [39]. As indicated previously, a limitation of traditional biometrics is security, user privacy risk and irreplaceability.

Cognitive biometrics [40–42] can be used to improve the revocability property. Cognitive biometrics represents a new approach to generate 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, thus it lowers the usability of the cognitive biometrics. 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, e.g., some schemes apply error correction codes [9, 13], and some others apply quantization [43]. The introduction of helper data, in some circumstances, e.g., multiple copy of helper data extracted from the single biometrics, may create vulnerabilities [44]. 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 [4]. BCSs reveal a noticeable decrease in recognition performance according to [29] because of the hardness of alignments of biometrics and higher degree of quantization at feature level [4]. Utilizing error correction codes and cryptography, secure sketches, an idea generalized by Dodis *et al.* [45], allows error correction of a noisy input. Secure sketches can be used as primitives to build fuzzy extractors which extract a uniformly random string. Secure sketches and fuzzy extractors, as primitive formalisms, have been used in concrete BCSs. The fuzzy vault scheme [9, 10] can be used as a secure sketch for set difference. The fuzzy vault schemes use chaff points to hide the genuine points (a description of user biometrics); the usage of chaff points makes the system vulnerable to some attacks [46]. The fuzzy commitment scheme [13] and its concrete implementations [11, 12] can be used as a fuzzy extractor for hamming distance. Systems based on the fuzzy commitment scheme can suffer from certain vulnerabilities [31], i.e., decodability attack [47]. Quantization has also been used frequently in BCSs [14, 15]. In general biometrics, several enrollment samples are trained to derive appropriate intervals for feature quantization. As in [15], the authors apply a context-based reliable component selection and construct intervals for the most reliable features of each subject. However, such approaches require multiple samples from each subject to reliably extract helper data. In some circumstances, obtaining those multiple samples could be difficult.

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 [17]. Pillai *et al.* [18] use random projections which embed biometrics from a higher dimensional space to a lower dimensional space. However, it is shown that the system is less secure if an attacker obtaining both the random projection parameters and the transformed patterns. Biotoken was proposed by [19, 20] to transform original biometric feature via scaling and translation into a transformed version. The transformed feature is split into a stable part termed integer and unstable part. There are several questions associated with this approach, e.g., 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.* [21] 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 provided in the paper.

Some hybrid approaches using both BCS or CB and proxy are proposed. The biohashing scheme [48,49] 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 [50, 51], 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 [52]. Introducing user-specific information, however, has an impact on the user-friendliness/convenience 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 [53]. Introducing the additional factor which is not intrinsically bound to the user, logically creates more vulnerabilities. It could also suffer from the same issues of traditional knowledge-based and token-based systems as those information can be stolen, lost or forgotten. The user-specific key is an additional factor correlated to each individual, which has a chance to reveal user-privacy. Further introducing a so-called user-specific key makes the identification under non-cooperative identification troublesome.

Ross *et al.* [54] explore the possibility of using visual cryptography for biometric privacy. In this approach, a biometric data are decomposed into pieces such that each piece can be stored in one server, and the original biometric data can be recovered when all pieces are available. The approach provides user privacy since pieces of information do not reveal original data. The approach is a new trial of using cryptography for biometric privacy, the cooperation between the different servers is essential however.

Different from above approaches, Othman and Ross [55] generate virtual identities by mixing two different fingerprints at the image level obtained from two different fingers to conceal the original identities. The security and cancelability need further studied such as the impact on the original fingerprints if mixed fingerprint compromised, and the possibility to generate new mixed fingerprint if original fingerprints compromised.

Above we reviewed the different approaches on secure biometric system, which are mainly used for one-time authentication. Active authentication has been dealt with indirectly in various areas including free-text detection of keystrokes dynamics biometrics [56, 57], and mouse dynamics biometrics recognition [38, 58]. There is certain research going on to directly deal with active authentication also [59, 60].

Biometrics based active authentication has been studied in the application of protecting PCs and workstations. Niinuma *et al.* proposed using soft biometrics (i.e., user face color, clothing color) and hard biometrics (i.e., face eigenfeatures) for active authentication [59]. There are four different modes of this active authentication: 1) a password-based initial authentication which registers user's face color, clothing color and the eigenface; 2) a continuous authentication using face color and clothing color; 3) enrollment template update if illumination change is detected; and 4) a re-login authentication using eigenface. The system registered a user template at password log-in, thus if the password is stolen the system will always think the impostor is the legitimate user. Also the system uses soft biometrics only to judge if the log-in user is present, while soft biometrics can be less robust compared to hard biometrics, since users can dress similar clothes (e.g., uniforms) and have similar face color.

Physiological biometrics has been used a lot in active authentication [60–67]. Sim *et al.* proposed to use face and fingerprint for authentication [61]. They use holistic score fusion to integrate face and fingerprint observations over time. However, the system requires training. Niinuma *et al.* proposed an active authentication using physiological biometrics without pre-registration [62]. The system registers user face and body at the password log-in and uses decaying weighted function to integrate the similarity score of face and body between the registered template and the template derived from the sampled biometrics for continuous authentication. A major issue is that the system will not be secure if the password is compromised.

There are efforts using behavior biometrics (e.g., keystrokes, mouse movement) for active authentication [68–70]. Monrose *et al.* proposed to use keystroke dynamics for active authentication. They collected timing information (e.g., duration and latency) through training and found those keys and key combinations that are used often by the user and typed in a stable way. There are many challenges in using keystrokes for active authentication. Firstly, users are using their devices on free text, thus finding stable “features” is critical. Secondly, the way users use their devices can be highly dynamic and easily affected by their mood, health situations, etc. Finally, training can be a burden to users.

Human cognitive biometrics is intrinsically in a continuous way, thus it could be used for active user authentication. Cognitive biometrics is defined as methods and technologies for the recognition of humans based on the measurements of signals generated directly or indirectly from their thought processes, and commonly seen biosignals include electrocardiogram (ECG), electroencephalogram (EEG) and electrodermal response (EDR). There is a framework proposed by [71] which uses ECG for continuous authentication in a specific context (i.e., health-care system). There is a need of special equipment to capture the biosignals or specific measurements to quantify the cognitive biometrics, which can become a limitation of general usage of cognitive biometrics based active authentication.

There are also efforts on the ownership factors used for active authentication. Radio-frequency identification (RFID) has been explored in a corporate environment [72]. The system uses a knowledge- or biometrics-based authentication scheme to gain initial entry to a system, while RFID is used subsequently to continuously verify the presence of a valid user. However, the RFID can be lost or stolen, and there are more privacy concerns using the RFID, e.g., tracking employee, tracking people location, identifying groupness of multiple RFIDs.

Besides the corporate environment in [72], the active authentication can be applied in more scenarios, e.g. location-aware application [73], combining with intrusion detection [74, 75], ubiquitous environments [71].

3 BIOMETRICS BASED AUTHENTICATION

This chapter presents the proposed biometrics based authentication approach.

3.1 Assumptions and Threat Model

A biometric authentication system contains two stages as presented in Chapter 1: registration and verification. Initially, the system samples and pre-processes the user biometrics. From the preprocessed biometrics, biometric features are extracted and a biometric credential (i.e., biometric template) is generated for registration. During any future verification, the user is sampled again and through the same processes a query biometric credential (i.e., query template) is generated and matched against the registered one.

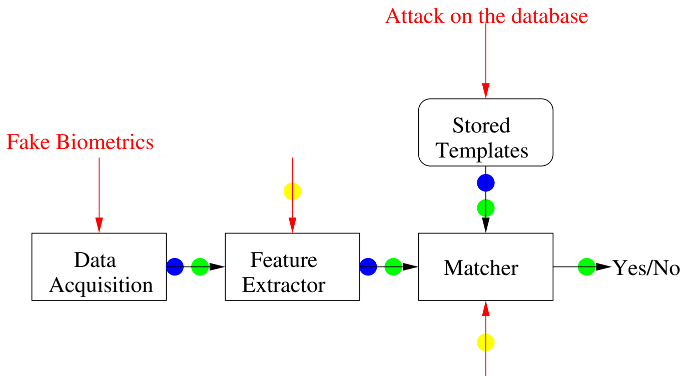


Figure 3.1.: Biometric system attack model.

For such a typical biometric authentication system, a few possible attacks have been identified as shown in Figure 3.1 [3]. It is possible that user biometrics is obtained by the attacker from other sources, and a spoofed biometrics is generated and presented to the data acquisition module. Defeating such an attack requires the capability of the biometric authentication system to distinguish the biometrics sampled from a live person from that of a spoofed one. There have been some research observed to do this liveness detection [76–78]. Concerning the communication channels between two biometric modules, the attacker can perform an injection attack. In Figure 3.1 (Figure 3.1 shows simplified model of biometric system, here we omit preprocessing and template generation modules), we have labeled such possible attack points using green dots. The attacker can perform injection attack as following: 1) inject synthesized biometric data or data obtained from a legitimate user into the channel between data acquisition module and feature extraction module; 2) inject biometric feature into the channel between feature extraction module and matching module; 3) inject matching decision outputted by the matching module. These attacks are due to the lack of secure channels between biometric modules. To defeat such an attack, cryptography techniques can be explored to build a secure channel. Another possible attack on biometric system is data interception. The attacker can explore the weakness of the system to get information about user biometrics. Similarly, in Figure 3.1 we use blue dots to label the possible attack points of this data interception attack. Also the attacker can compromise some biometric modules, such as the matcher (labeled as yellow dot). One of the most serious attack on the biometric system is the attack against the biometric system database. The system database stores biometric credentials (e.g., template). These credentials (of conventional biometric systems) are irreplaceable once compromised. And from the compromised biometric credentials, the synthesized biometric data/feature can be reconstructed which are then injected into the biometric system. Moreover, the compromised templates can be directly injected into the channel between the template generation module and matching module. In addition, the compromised template from one biometric system (e.g., banking database) can be cross-matched to another biometric system (e.g., health care system) to obtain user information thus infringes user privacy. In this dissertation, we assume that the system has liveness detection mechanisms, secure channels, and intact biometric modules. One major work of the dissertation is to proposed a secure, privacy-preserving, and cancelable biometric system which can defeat the attack against on information stored in biometric system database. In Figure 3.2, we label the attacks that are concerned in the BC authentication system.

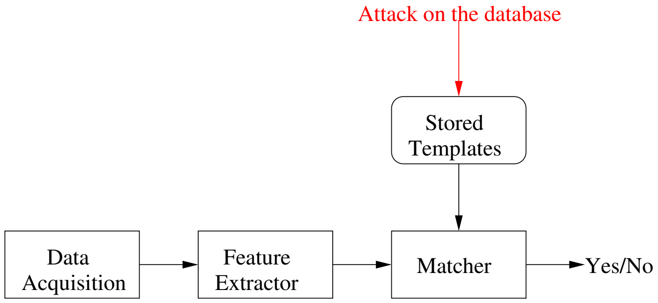


Figure 3.2.: BC system attack model.

3.2 Biometrics Based Authentication – New Model

The proposed authentication system also contains two stages as shown in Figure 3.3: registration and verification. Initially, the system samples the RS[1]. For registration, the user biometrics is fused with the RS biometrics, and from the fused biometrics the user's BC is generated. During any future verification, the user biometrics is sampled again and his biometrics is fused with the RS's (re-sampled if using a physical RS) again and the derived BC is compared with the stored BC.

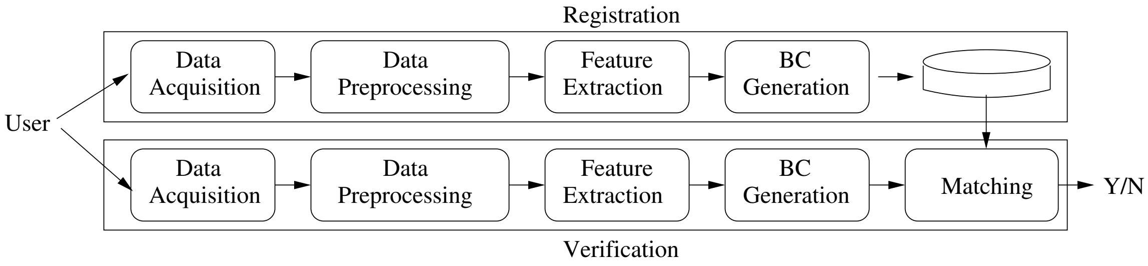


Figure 3.3.: The new BC based authentication model.

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-wise object and managed by the authentication system, not by a user, which frees users' burden on carrying or memorizing 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

[1] The RS can be a physical object or an image. Although a physical RS can increase an attacker's difficulty in stealing the RS, the scheme does not require this physical configuration due to the scheme's resiliency to RS disclosure.

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 Figure 3.4. 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").

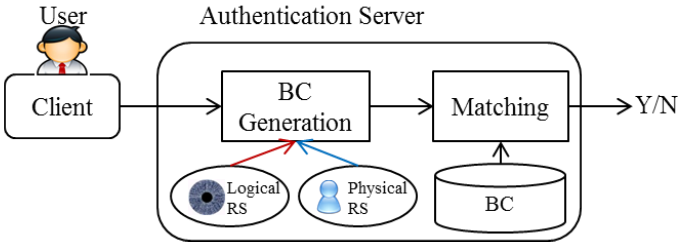


Figure 3.4.: Diagram of the system.

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-wise) 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. Designing a fusion process and generating a BC is a great challenge. To design an effective fusion and BC construction mechanism, we have the following considerations:

- 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 deteriorating matching performance.
- Are the user biometrics and the fused biometrics correlated; or are the fused biometrics using different RSs correlated? If there is a strong correlation between the user biometrics and fused biometrics, or among the fused biometrics using different RSs, 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 [3], that is security and revocability (against BC compromise, also to protect user privacy), diversity (to defeat cross-matching attack and protect user privacy), distinguishability (for authentication accuracy), as well as usability (for user convenience and acceptance of the BC). Our design rationale for such BC generation includes the following:

- the user and the RS are treated equally and the BC bears no hints that the user is weighted more than the RS;
- 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;
- keys are extracted in such a way that can balance between key stability and distinguishability;
- it is 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 Figure 3.5. From user (RS) biometrics, user (RS) key is extracted and used for RS (user) biometrics transformation. Transformed

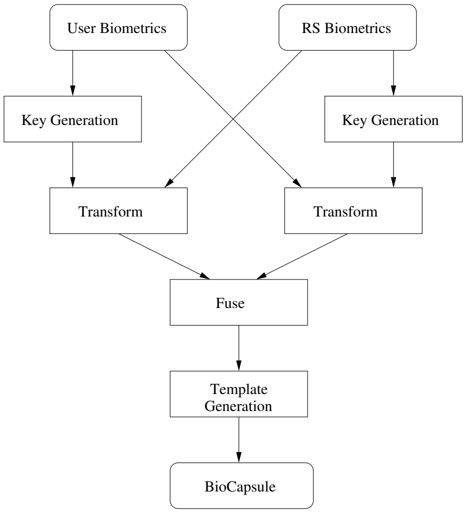


Figure 3.5.: The BC generation model.

user biometrics and RS biometrics are fused, and from fused biometrics a BioCapsule is generated.

Evaluation metrics and property definition. To formally analyze the proposed approach and other approaches, we propose the following measurements for a biometric system. Based on an information theory metric (i.e., biometric system entropy [79]), 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 [44], 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 (CMR) 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 (BSE) [79], 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 [80]. Bonneau *et al.* [81] presented a frame work to evaluate the authentication approaches. And usability is an important part of it. Usability here refers to the necessity to require external factors (e.g., password, token) from users for authentication (as the Memorywise-Effortless and Nothing-to-Carry in [81]). 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 mechanism 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.

3.3 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 several light-weight key extraction approaches considering the following criterion:

- To make it ease to use, 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, thus compromising this key is more difficult when compared to factors artificially bound to a user.
- Since the generated keys are not used for authentication, the BC approach does not require 100% user-distinct keys.
- 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, and thus, authentication accuracy. Moreover, noisy features of different samplings of biometrics create constraints on stability, unless more helper data is used. On the other hand, completed distinguisha-

bility necessitates the need of using complicated fuzzy handling techniques such as error correction codes.

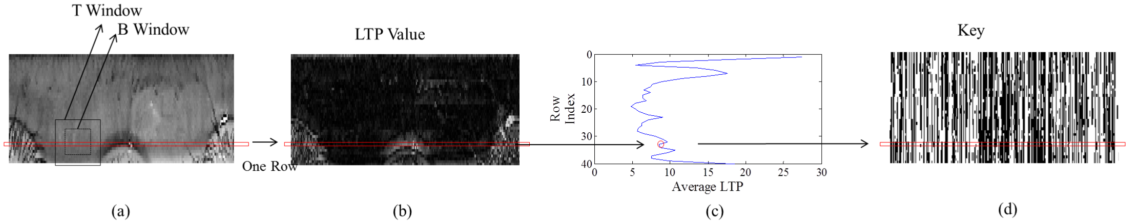


Figure 3.6.: A key extraction process.

The following key extraction schemes all satisfy the above design criterion, while it performs differently when different scheme is integrated into the whole system. We will conduct experiments on it.

3.3.1 Key extraction scheme 1

The first key extraction scheme is based on grayscale-invariant local texture pattern (LTP) [82].

Key extraction scheme 1. *The proposed key extraction scheme Ext^K comprises the following procedures as shown in Figure 3.6:*

- *Extract iris signature:*
  - *1) preprocess the obtained iris data and get processed data (described as a $m-by-n$ matrix) as Figure 3.6 (a).*
  - *2) compute the grayscale-invariant local texture pattern (LTP) [82] (Figure 3.6 (b)). 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, which is given as*

$$LTP_{ij} = |I_{ij} - A_T|, (i, j) \in B \tag{3.1}$$

In Eq. 3.1, I_{ij} is the grayscale value of the pixel at (i, j) in B, and A_T is the mean grayscale value inside T, which is given as

$$A_T = \frac{1}{N} \sum_{(x,y) \in T} I_{xy}, \tag{3.2}$$

with N the total number of pixels contained within T.

  - *3) generate a temporary signature (Figure 3.6 (c)) $\tilde{s} \in \mathbb{R}^m$ 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*

$$s = (\tilde{s} - V) + M, \tag{3.3}$$

  with V obtained by

$$V = \frac{1}{m} \sum \tilde{s}. \tag{3.4}$$

- *Encode the iris signature s to a key (Figure 3.6 (d)). Encoding is an essential part of the key extraction. Each iris signature component s_i $(1 \leq i \leq m)$ is an average of a row of LTP values, thus theoretically $0.0 \leq s_i \leq 255.0$ (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 [82]). 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 tenth 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 method of encoding will have an impact on the stability and distinguishability of the extracted keys. 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., rounding the signature to integer, increases the stability. Also the key in the system is encoded into a $\{-1, 1\}$ string instead of a $\{0, 1\}$ string, since applying a $\{0,1\}$ key in the BC generation actually will rule out part of the biometric features, which will degrade the system performance. We have also conducted experiments to see the best encoding strategy of the key, e.g., encoding the key into $\{-2,2\}$ string, etc. And it turns out that $\{-1,1\}$ key outperforms others which it is believed that $\{-1,1\}$ key actually helps maintain the distinguishability of original biometric features. And other key encodings actually amplify the instableness of the biometrics thus decreasing the performance.

3.3.2 Key extraction scheme 2

Key extraction scheme 2. *The proposed key extraction scheme Ext^K comprises the following procedures:*

- *Extract iris signature:*
  - *1) preprocess the obtained iris data and get processed data (described as a $m-by-n$ matrix) as Figure 3.6 (a).*
  - *2) compute the grayscale-invariant local texture pattern (LTP) [82] (Figure 3.6 (b)). 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, which is given as*

    $$LTP_{ij} = |I_{ij} - A_T|, (i,j) \in B \tag{3.5}$$

    In Eq. 3.5, I_{ij} is the grayscale value of the pixel at (i,j) in B, and A_T is the mean grayscale value inside T, which is given as

    $$A_T = \frac{1}{N} \sum_{(x,y)\in T} I_{xy}, \tag{3.6}$$

    with N the total number of pixels contained within T.
  - *3) generate a temporary signature (Figure 3.6 (c)) $\tilde{s} \in \mathbb{R}^m$ by averaging the LTP values of rows.*

- *4) add one component into the temporary signature which is the average of $\tilde{s}$, thus the iris signature $s = [\tilde{s}, mean(\tilde{s})]$.*

- *Encode the iris signature s to a key (Figure 3.6 (d)). Encoding is an essential part of the key extraction. Each iris signature component s_i $(1 \leq i \leq m)$ is an average of a row of LTP values, thus theoretically $0.0 \leq s_i \leq 255.0$ (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 [82]). 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 tenth 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.*

3.3.3 Key extraction scheme 3

Key extraction scheme 3. *The proposed key extraction scheme Ext^K comprises the following procedures:*

- *preprocess the obtained iris data and get processed data (described as a $m - by - n$ matrix) as Figure 3.6 (a).*
- *this key extraction scheme also 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 key bit k for each pixel at coordinates (i, j) inside B is defined as following:*

$$k_{ij} = (I_{ij} <= A_T), (i, j) \in B \tag{3.7}$$

In Eq. 3.7, I_{ij} is the grayscale value of the pixel at (i, j) in B, and A_T is the mean grayscale value inside T, which is given as

$$A_T = \frac{1}{N} \sum_{(x,y) \in T} I_{xy}, \tag{3.8}$$

with N the total number of pixels contained within T.

3.4 Secure Biometrics Fusion

Our goal of fusion aims to increase the security of the biometrics. By fusing the user biometrics and the RS biometrics, the RS biometrics hides the user biometrics, thus providing 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.

3.4.1 Fusion scheme 1

Fusion scheme 1. *On biometric inputs F^u, F^r, K^u and K^r where $F^u, F^r \in \{F_i\}^n$ ($f^L \leq F_i \leq f^U$) 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*

$$F_i^{u,r} = (F_i^u \cdot K_i^r + F_i^r \cdot K_i^u \mod (f^U - f^L)) - f^L, \tag{3.9}$$

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 $F^{u,r} \in \{F_i\}^n$ ($f^L \leq F_i \leq f^U$).

An actual fusion process is illustrated in Figure 3.7. One ICE [83] image and one RS image (i.e., Figure 4.2(a)) 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 [84] (results are shown in Figure 3.7(a)). In a closer view, 10 user (RS) features/10 bits of the user (RS) key in the dashed box of Figure 3.7(a)) are shown in Figure 3.7(b). 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

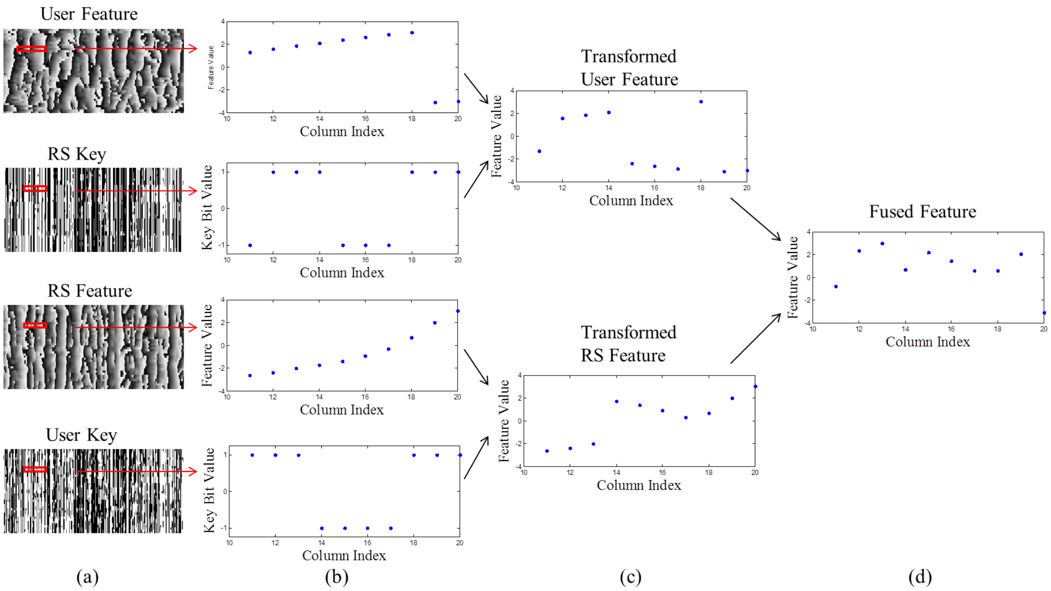


Figure 3.7.: A secure fusion process: illustrated by an ICE image and the RS.

feature with one bit of the RS/user key (results are shown in Figure 3.7(c)). The fused features are obtained through Eq. 3.13 (results are shown in Figure 3.7(d)).

3.4.2 Fusion scheme 2

Fusion scheme 2. *On biometric inputs F^u, F^r, K^u and K^r where $F^u, F^r \in \{F_i\}^n$ ($f^L \leq F_i \leq f^U$) 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*

$$F_i^{u,r} = (F_i^u \cdot (\log F_i^r) \cdot K_i^r + F_i^r \cdot (\log F_i^u) \cdot K_i^u \mod (f^U - f^L)) - f^L, \tag{3.10}$$

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 $F^{u,r} \in \{F_i\}^n$ ($f^L \leq F_i \leq f^U$).

3.4.3 Fusion scheme 3

Fusion scheme 3. *On biometric inputs F^u, F^r, K^u and K^r where $F^u, F^r \in \{F_i\}^n$ ($f^L \leq F_i \leq f^U$) 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*

$$F_i^{u,r} = ((\log F_i^u) \cdot K_i^r + (\log F_i^r) \cdot K_i^u \mod (f^U - f^L)) - f^L, \tag{3.11}$$

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 $F^{u,r} \in \{F_i\}^n$ ($f^L \leq F_i \leq f^U$).

3.4.4 Other fusion schemes

Before we came up with the proposed fusion model, there are many fusion schemes that we tried. To help get the insight of the proposed fusion model, we also list the other fusion schemes in this section.

Fusion scheme 4. *On biometric inputs F^u, F^r, and K^u where $F^u, F^r \in \{F_i\}^n$ ($f^L \leq F_i \leq f^U$) and $K^u \in \{K_i\}^n$ ($K_i = 1, -1$), through "secure fusion" the fused biometrics $F^{u,r}(or\ \{F_i^{u,r}\}^n)$ is obtained by*

$$F_i^{u,r} = ((F_i^u + F_i^r) \cdot K_i^u + F_i^r \mod (f^U - f^L)) - f^L, \tag{3.12}$$

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

Fusion scheme 5. *On biometric inputs F^u, F^r, and K^u where $F^u, F^r \in \{F_i\}^n$ ($f^L \leq F_i \leq f^U$) and $K^u \in \{K_i\}^n$ ($K_i = 1, -1$), through "secure fusion" the fused biometrics $F^{u,r}(or\ \{F_i^{u,r}\}^n)$ is obtained by*

$$F_i^{u,r} = ((F_i^u + F_i^r) \cdot K_i^u + F_i^u \mod (f^U - f^L)) - f^L, \tag{3.13}$$

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

These fusion schemes do not fit the proposed fusion model such that the user and the RS are not treated equally, which may result in security problems. If the user knows his BC, it is quite likely that F^r is disclosed.

3.5 Integration with Biometrics Modules

The proposed fusion mechanism is a general procedure, which can be integrated with existing biometric processes to generate BCs. The fusion uses traditional preprocessing, feature extraction and template generation approaches without modification. Such a property makes the proposed fusion more deployable. Moreover, such a fusion keeps the same domain of inputs and outputs, thus theoretically enabling at various levels (e.g., signal, feature, template). Next, we illustrate the concrete integration of "secure fusion" with 2D Gabor [85]. Through the integration of "secure fusion" with existing biometric procedures, a complete BC generation process is give as follows:

Fusion at signal-level. Figure 3.8 shows a model of the integration of "secure fusion" with existing biometric processes at signal-level. It applies the "secure fusion" directly after the signal preprocessing.

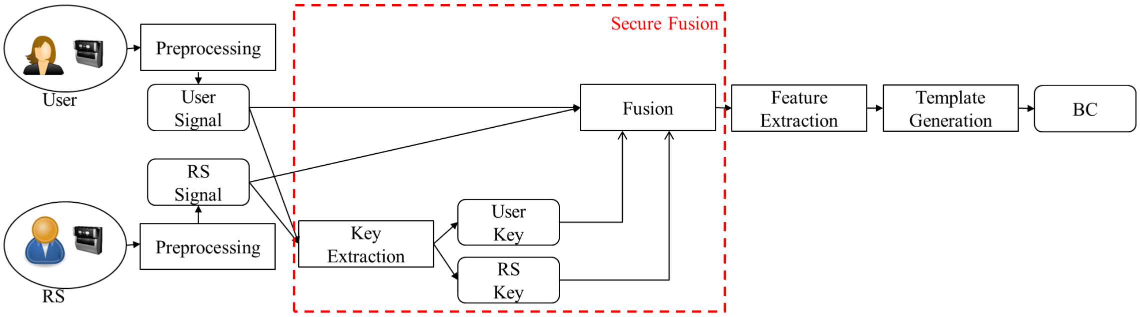


Figure 3.8.: Integration of the secure fusion (red box) with existing biometrics processes at signal-level.

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

- *Extract the user key K^u and the RS key K^r from D^u and D^r using* **Scheme-1**.
- *Fuse user data (signal) and reference subject data (signal) by computing $D^{A(u)}e^{Fuse(D^{\Phi(u)},D^{\Phi(r)})}$, thus obtaining fused signal $D^{u,r}$.*
- *Extract features using 2D Gabor from fused biometric data by feature extraction procedure Ext^F and obtain fused biometric feature $F^{u,r} = Ext^F(D^{u,r})$.*
- *Quantize the fused feature $F^{u,r}$ into a BioCapsule BC^u.*

Fusion at feature-level. Figure 3.9 shows a model of the integration of "secure fusion" with existing biometric processes at feature-level. It applies the "secure fusion" before the template generation and after the feature extraction.

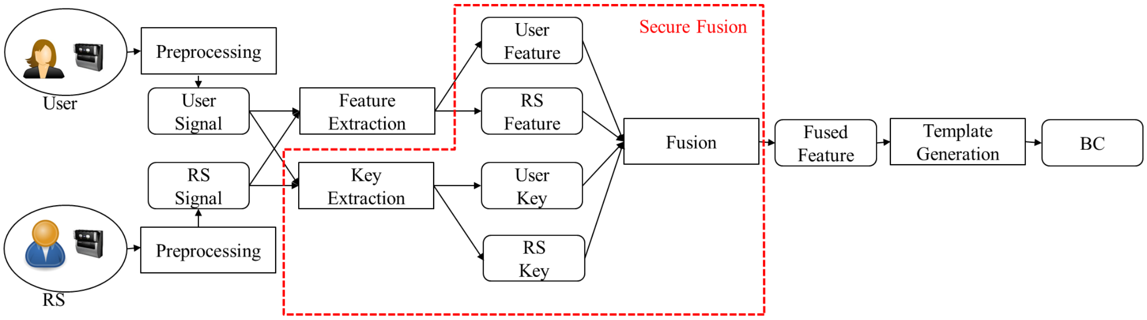


Figure 3.9.: Integration of the secure fusion (red box) with existing biometrics processes at feature-level.

Scheme-4. *Given user biometric data D^u and RS biometric data D^r, a $feature - BCE$ ("BioCapsule Extractor") scheme comprises following procedures:*

- *Extract the user key K^u and the RS key K^r from D^u and D^r using* **Scheme-1**.
- *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 procedure $Fuse$ defined in* **Scheme-2**. *Obtain $F^{u,r}$.*
- *Quantize the fused feature $F^{u,r}$ into a BioCapsule BC^u.*

Fusion at template-level. Figure 3.10 shows a model of the integration of "secure fusion" with existing biometric processes at template-level. It applies the "secure fusion" after the template generation.

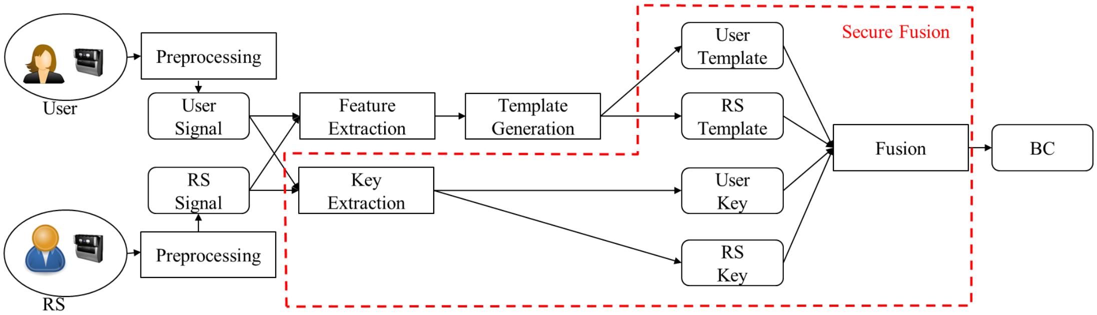


Figure 3.10.: Integration of the secure fusion (red box) with existing biometrics processes at template-level.

Scheme-5. *Given user biometric data D^u and RS biometric data D^r, a $template-BCE$ ("BioCapsule Extractor") scheme comprises following procedures:*

- *Extract the user key K^u and the RS key K^r from D^u and D^r using* **Scheme-1**.
- *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 $F^r = Ext^F(D^r)$.*
- *Quantize the features into templates T^u and T^r.*
- *Fuse the user template and the RS template using K^u and K^r by procedure $Fuse$ defined in* **Scheme-2**. *Obtain $T^{u,r}$, which is used as the BC^u.*

We have presented the proposed mechanism "secure fusion" with the existing biometric process and a complete BC generation process in this section. In the following, we will analyze the security of the BC approach.

3.6 Security and Privacy-Preservation Analysis

The following security and privacy-preservation analysis is based on key extraction scheme 1 and fusion scheme 1. Basically the system using key extraction scheme 1 (2, or

3) and fusion scheme 1 (2, or 3) follows the similar arguments. The BC approach does not store user biometrics or keys, but discards them after BCs are computed. Thus, if a physical RS is used, the risk of compromising/stealing the RS is greatly reduced. The system stores the BC for each enrolling user, thus we consider security of the approach assuming that stored BCs are obtained by attackers, then from compromised BCs, attackers try to obtain users' original biometrics. Next we prove the security of the BC approach under different attack models.

- Security against a lost BC:

  Claim 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:

  $$F^{u,r} = F^u \cdot K^r + F^r \cdot K^u \tag{3.14}$$

  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, thus no single solution can be found. Thus, the BC approach is able to defeat the attack of recovering the user biometrics (or the RS) from a compromised BC. □

- Security against loss of both a BC and the RS:

  Claim 2. *The security of the user biometrics against a compromised BC and the 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 a fact that from the average of a set of data it is hard to reconstruct the original data, there is no direct relationship 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^u_i corresponding to a pixel) is independent from K^u (or K^u_i) (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,

$$F^{u,r} = F^u \cdot K^r + F^r \cdot K^u \tag{3.15}$$

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

$$\begin{cases} F^{u,r}_1 = F^u_1 \cdot K^r_1 + F^r_1 \cdot K^u_1 \\ \cdots \\ F^{u,r}_n = F^u_n \cdot K^r_n + F^r_n \cdot K^u_n \end{cases} \tag{3.16}$$

with F^u_i and K^u_i $(1 \leq i \leq n)$ unknown. Since F^u_i and K^u_i are independent, we can treat them as two variables, thus this equation system is undetermined and no single solution can be found. Observing the equation system, F^u can be obtained by: 1) guessing $K^u_1, \cdots, K^u_n$; 2) computing $F^u_i = (F^{u,r}_i - F^r_i \cdot K^u_i) \cdot K^{r-1}_i$; then 3) checking if $Ext^K(F^u_1, \cdots, F^u_n) = \{K^u_i\}$. 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. Because of the equal treatment of the user biometrics and the RS's, the RS security can be assured following the similar arguments above.

- Security against external collusion attack:

  Claim 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 $u_1, \cdots, u_v$), 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

$$\begin{cases} F^{u_1} \cdot K^{r_1} + F^{r_1} \cdot K^{u_1} = F^{u_1,r_1} \\ F^{u_2} \cdot K^{r_2} + F^{r_2} \cdot K^{u_2} = F^{u_2,r_2} \\ \cdots \\ F^{u_v} \cdot K^{r_v} + F^{r_v} \cdot K^{u_v} = F^{u_v,r_v}. \end{cases} \tag{3.17}$$

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

$$\begin{cases} F^{u_1} \cdot K^{r} + F^{r} \cdot K^{u_1} = F^{u_1,r} \\ F^{u_2} \cdot K^{r} + F^{r} \cdot K^{u_2} = F^{u_2,r} \\ \cdots \\ F^{u_v} \cdot K^{r} + F^{r} \cdot K^{u_v} = F^{u_v,r}, \end{cases} \tag{3.18}$$

with $K^r, F^{u_1}, \cdots, F^{u_v}$ unknown. The system of equations is undetermined and a unique solution is not available. On closer inspection, much research attempts to look for $sparse$ solutions of such a system. However, this sparse solution to a general undetermined system of equations is NP-hard. Also, it is an interval linear equation system, solving an interval linear equation system is also NP-hard [86]. 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. □

Even though the RS is derivable, determining the RS helps no further if the attacker acquires another user's BC and tries to obtain the user biometrics. Following Theorem 2, the user biometrics (feature) is secure against a lost RS and a BC.

- Security against internal collusion attack:

Claim 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 [86].*
Proof. From those BCs (from $u_1, \cdots, u_v$), 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 same RS and same key encoding. Thus, the problem is reduced to solving the following equation system with F^r and K^r unknown.

$$\begin{cases} F^{u_1} \cdot K^r + F^r \cdot K^{u_1} = F^{u_1,r} \\ F^{u_2} \cdot K^r + F^r \cdot K^{u_2} = F^{u_2,r} \\ \cdots \\ F^{u_v} \cdot K^r + F^r \cdot K^{u_v} = F^{u_v,r} \end{cases} \tag{3.19}$$

This is an interval linear system, and solving such a system is NP-hard [86], 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 [86]. 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. □
Even F^r is determinable, determining the F^r helps no further if the attacker acquires another user's BC and tries to derive this user biometrics. Following Theorem 2, user biometrics (feature) is secure against a lost RS and the user's BC.

- Security against internal cross-RS attack:

Claim 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 [86], and therefore an undetermined system.*
Proof. From those BCs (from $u_1, \cdots, u_v$) 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

$$\begin{cases} F^{u_i} \cdot K^{r_1} + F^{r_1} \cdot K_1^{u_i} = F^{u_i,r_1} \\ F^{u_i} \cdot K^{r_2} + F^{r_2} \cdot K_2^{u_i} = F^{u_i,r_2} \end{cases} \tag{3.20}$$

with F^{u_i}, $K_1^{u_i}$ and $K_2^{u_i}$ unknown. First, this equation could be 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. □

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.

4 EXPERIMENTS, ANALYSIS AND DISCUSSIONS

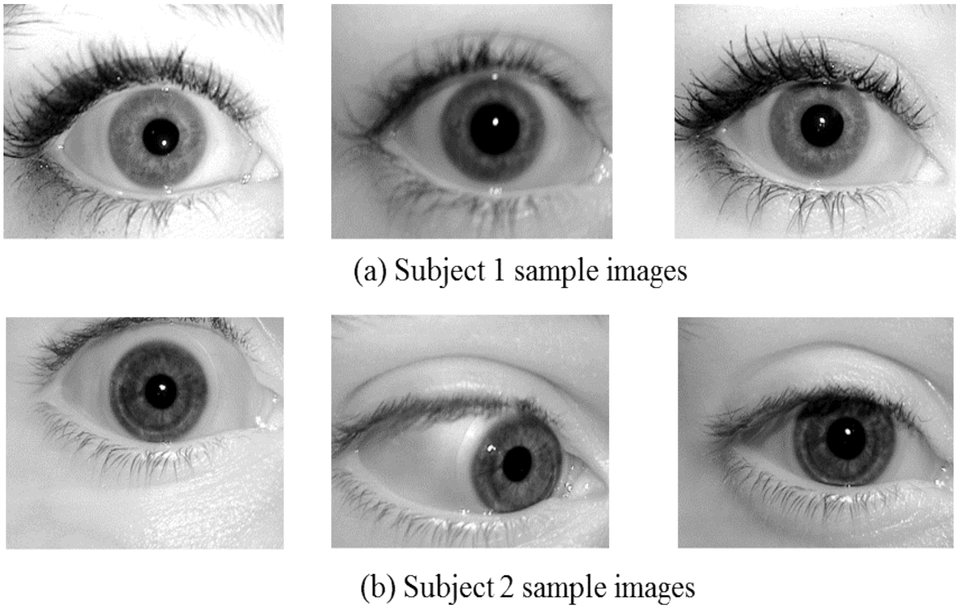
In order to evaluate the performance (i.e., authentication accuracy) of the proposed BC approach, we have conducted extensive experiments on (various components of) the BC approach. This section presents our experimental results.

4.1 Experiments

4.1.1 Experiment settings

In the case of experiments, the performance of the proposed technique was tested on both the ICE database and CASIAv1.0 database. The ICE database is provided by National Institute of Standards and Technology (NIST) for the Iris Challenge Evaluation (ICE) 2005 and it contains 1,426 images from the right eye from 132 subjects, and 1,527 images from the left eye from 132 subjects. The CASIAv1.0 database is provided by Chinese Academy of Science, and it contains 756 iris images from 108 eyes. 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 Figure 4.1.

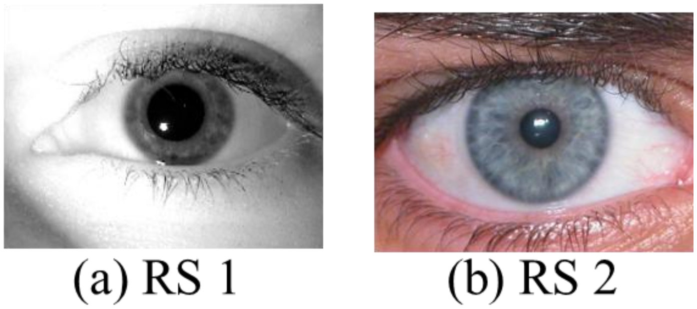
We chose an iris image from the UBIRIS [87] and one iris image from ICE as our RS iris image as shown in Figure 4.2. If the RS is a logical one (e.g., an image stored in the system), it will display no image distortion. If the RS is a physical one, there will be



(a) Subject 1 sample images

(b) Subject 2 sample images

Figure 4.1.: Sample images of two subjects from NIST/ICE.



(a) RS 1

(b) RS 2

Figure 4.2.: Reference subjects' biometrics.

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.* [88] 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 40db. Due to the fact that the physical RS was not a live person that demonstrates pupil focusing, defocussing, 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).

Here we reviewed the biometric modules that are used in our experiments. The iris segmentation locates the iris region. We used the circle based edge detection to find the pupillary and limbic boundary. And we transferred the extracted iris to the polar coordinates and generated the mask map (for matching).

Two feature extraction approaches are used in our experiments: 2D Gabor filter and 1D Log-Gabor filter. 2D Gabor filter is proposed by Daugman (Eq. 4.1), which is wildly used in commercial iris recognition system [85]. From the segmented polar image, phase information is extracted and encoded to be the iris feature (template).

$$h\{Re, Im\} = sgn\{Re, Im\} \int_{\rho}\int_{\phi} I(\rho,\phi) e^{-i\omega(\theta_0-\phi)} e^{-\frac{i(\gamma_0-\rho)^2}{\alpha^2}} e^{-\frac{i(\theta_0-\phi)^2}{\beta^2}} \rho \, d\rho \, d\phi, \tag{4.1}$$

where $h\{Re, Im\}$ is the complex value obtained by applying the 2D Gabor on the biometric image I,the wavelet sizes of the 2D Gabor Wavelet on the radial and angular axes are α and β, and ω is used for the wavelet frequency.

1D Log-Gabor is developed by Masek *et al.*, which acts as a bandpass filter for feature extraction [84]:

$$G(\omega) = e^{\frac{-\log((\omega/\omega_0)^2)}{2\log(\sigma)^2}}, \tag{4.2}$$

where σ is used to control the filter bandwidth and ω_0 is the filter's center frequency.

Hamming distance (HD) is used for pattern matching.

$$HD = \frac{\sum\sum((T_A \otimes T_B) \cap M_A \cap M_B)}{\sum\sum(M_A \cap M_B))}, \tag{4.3}$$

where M_A and M_B are masks for two images which marked the iris areas, and T_A and T_B are the biometric credentials (e.g., IrisCode, BC).

4.1.2 Key extraction

In this experiment, the key stableness and distinguishability were investigated. The experiment consisted of matching the extracted keys against each other. For example, in the ICE database with 1,426 images, $1,426 \times 1,426$ matches are performed. The curves in Figure 4.3 shows the similarity (measured by hamming distance) distribution of matchings of intra-class (genuine) and inter-class (impostor) using two key extraction approaches. The more "sharp" and "right-shifted" intra-class curve indicates more stableness of extracted keys. The more "distanced" curves indicate better distinguishability. key extraction scheme 1 (Figure 4.3(a)) shows better key stability compared to key extraction scheme 3 (Figure 4.3(c)), while the scheme 3 shows better key distinguishability.

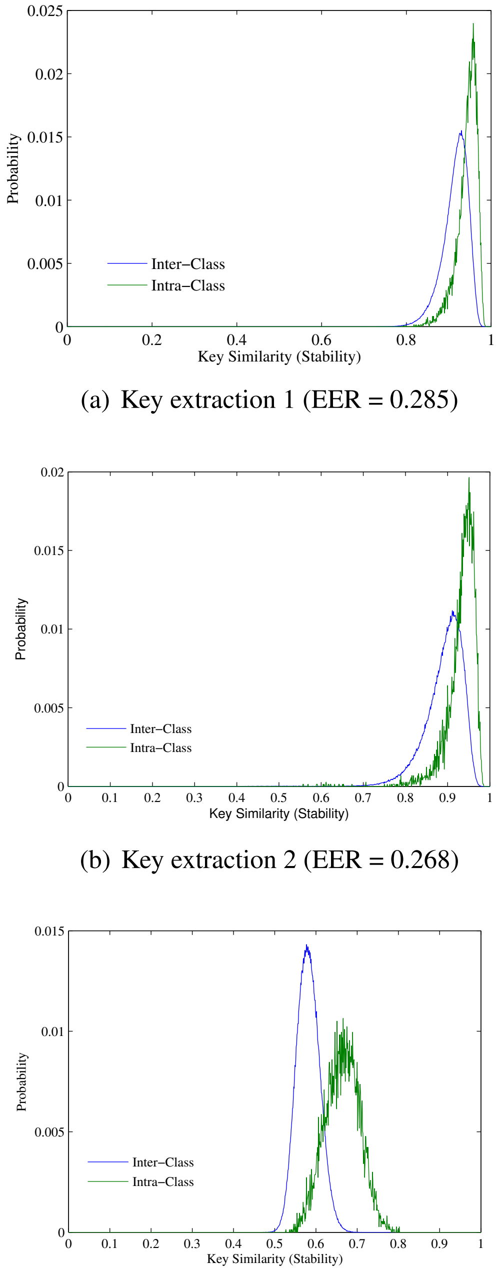
We are interested in what the effect of the stability and distinguishability of the extracted keys on the BC performance. Intuitively, more stable and distinguished keys will keep the original biometrics distinguishability better. We evaluated how the extracted keys affect the matching performance of the extracted BC. Figure 4.4 shows the ROCs using the above key extraction approaches (note: secure fusion scheme 1 is used.).

From Figure 4.4, it is obvious that BC approaches using scheme 1 and scheme 2 show higher accuracy. From intuitive the good stability of extracted keys help maintain the distinguishability of original biometrics. From a closer view of experimental results shown in Table 4.1, BCs using key extraction scheme 1 shows slightly better performance compares to that using scheme 2, which can be due to the better stability of scheme 1.

Table 4.1: Experiments summary of BCs using different key extraction schemes.

Key Extraction	EER
Scheme 1	0.0078
Scheme 2	0.0082
Scheme 3	0.03

We have also conducted experiments on the encodings of the keys. The keys in our system are encoded into 1 and -1 strings. However, it is possible that keys are encoded into $\{2, -2\}^n, \{3, -3\}^n$, etc. However, through our experimental results, encoding keys into $\{1, -1\}^n$ is the best strategy. It maintains the biometric system performance well.



(a) Key extraction 1 (EER = 0.285)

(b) Key extraction 2 (EER = 0.268)

(c) Key extraction 3 (EER = 0.130)

Figure 4.3.: Extracted key (ICE) intra-class and inter-class distribution.

Other encoding approaches to some extent degrade the system performance (i.e., accuracy), which can be explained as the biometrics variances are amplified.

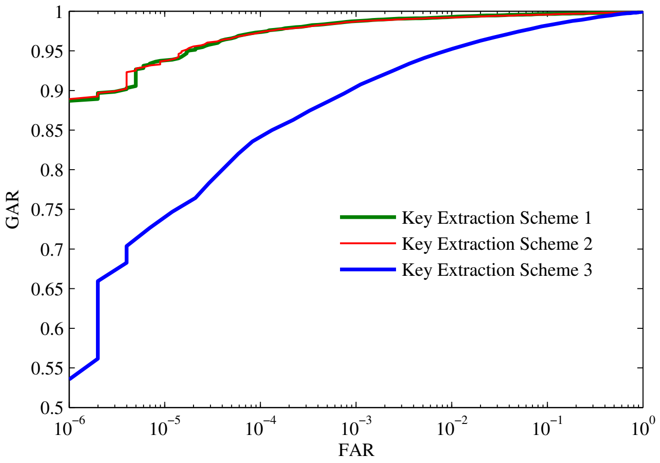


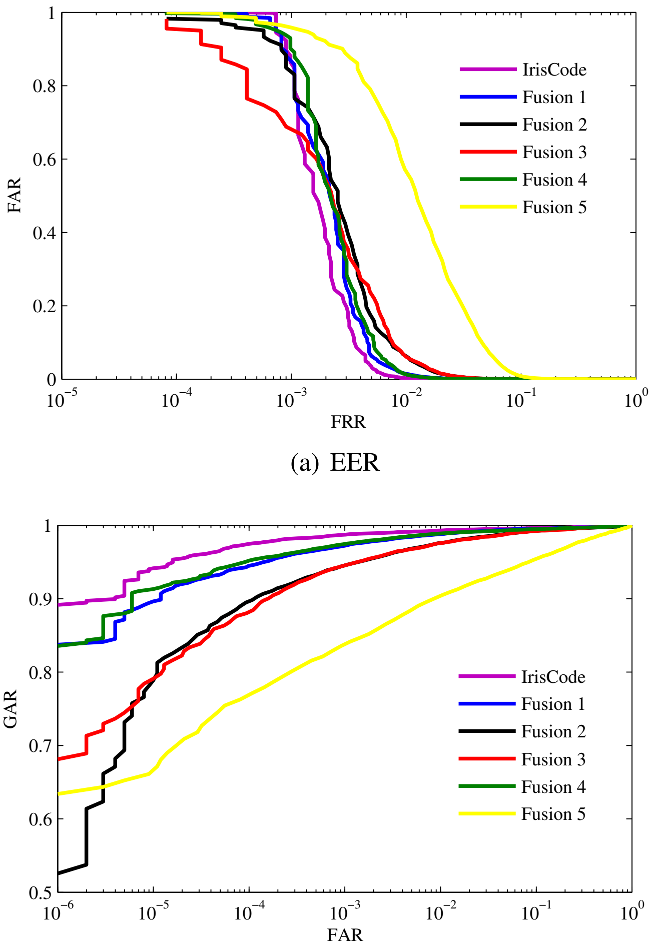
Figure 4.4.: ROCs on ICE (right set) using 1D Log-Gabor and: 1) key extraction scheme 1, 2) key extraction scheme 2, and 3) key extraction scheme 3.

4.1.3 Secure fusion

We have proposed five different secure fusion schemes. In this section we analyze these five schemes from the performance aspect. To conduct this experiment, we use ICE database right-eye set with 1,426 images. We use each fusion scheme and key extraction scheme 1 to extract BCs. The BC generation uses a stable RS. And the secure fusion happens at the signal-level. Next, we compare the performance of the BCs generated from different fusion schemes. Figure 4.5 shows the comparison results, particularly Figure 4.5(a) (and Table 4.2) and Figure 4.5(b) show the EER and ROC comparisons respectively. From the result, it is observed that BCs using fusion 1 and fusion 4 provide best matching performance.

Table 4.2: Performance summary of BCs using different secure fusion schemes.

Schemes	EER
IrisCode	0.0077
BCs using fusion 1	0.0112
BCs using fusion 2	0.0181
BCs using fusion 3	0.0192
BCs using fusion 4	0.0111
BCs using fusion 5	0.0569



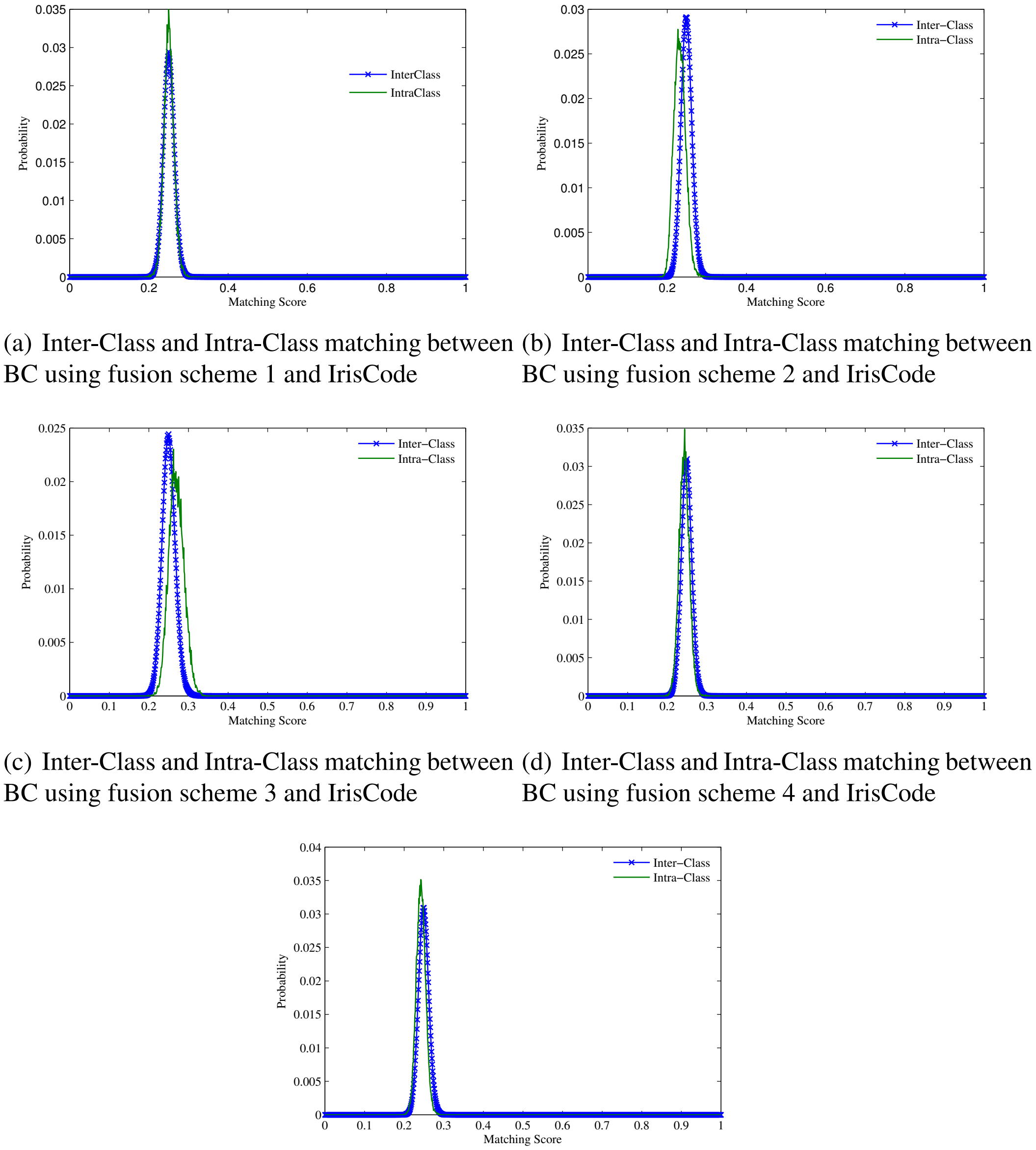
(a) EER

(b) ROC

Figure 4.5.: Performance of IrisCode and BCs using five fusion schemes.

We also tested the unlinkability (cross-matching resistance) of the BCs using different fusion schemes. We consider two systems: system 1 uses the one BC technique, and system 2 uses the IrisCode technique. Figure 4.6 shows the comparison results on inter-class and intra-class distribution of matching between BC using various fusion schemes and IrisCode. It is shown in Figure 4.6 that the inter-class and intra-class distribution of matching between BC using fusion scheme 1 and IrisCode (as shown in Figure 4.6(a)) is more mixing compared to other four.

Table 4.3 summarizes the unlinkability performance of BCs using different fusion schemes based on the metrics CMR (note: higher CMR indicates better unlinkability). From



(a) Inter-Class and Intra-Class matching between BC using fusion scheme 1 and IrisCode

(b) Inter-Class and Intra-Class matching between BC using fusion scheme 2 and IrisCode

(c) Inter-Class and Intra-Class matching between BC using fusion scheme 3 and IrisCode

(d) Inter-Class and Intra-Class matching between BC using fusion scheme 4 and IrisCode

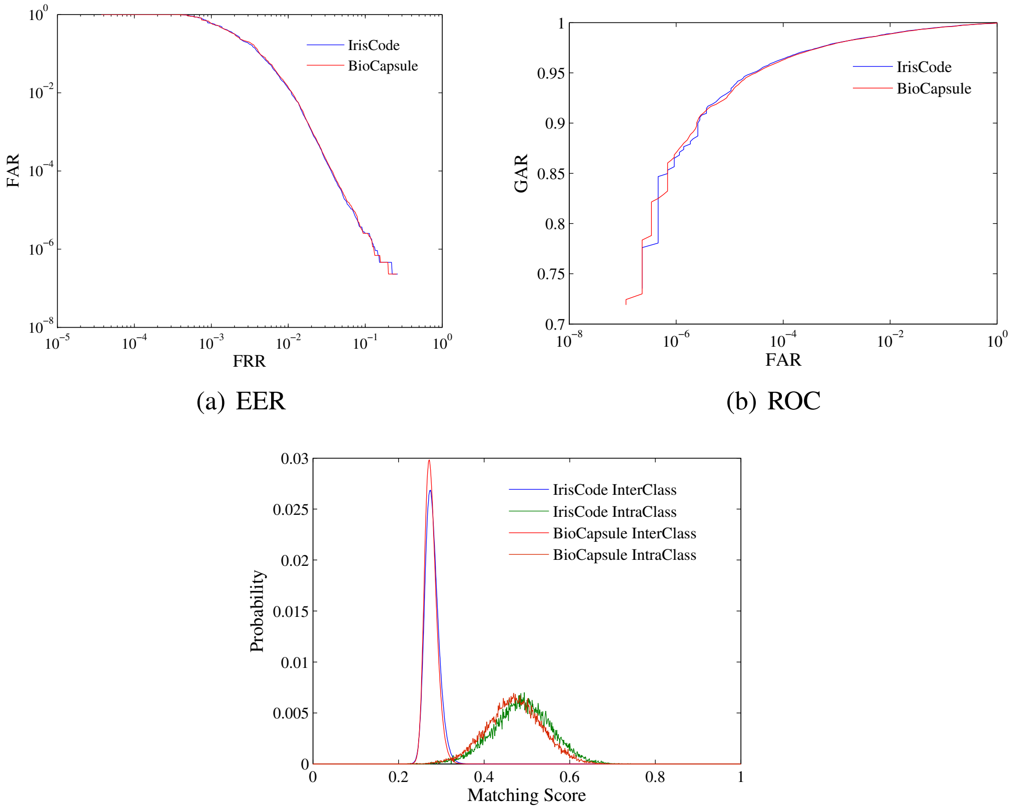
(e) Inter-Class and Intra-Class matching between BC using fusion scheme 5 and IrisCode

Figure 4.6.: Unlinkability of BCs using five fusion schemes.

CMR results, we can draw the same conclusion that BCs using fusion scheme 1 provides the best unlinkability performance.

Table 4.3: Unlinkability summary of BCs using different secure fusion schemes.

Schemes	CMR (between BC and IrisCode)
BCs using fusion 1	0.9750
BCs using fusion 2	0.5256
BCs using fusion 3	0.6115
BCs using fusion 4	0.7833
BCs using fusion 5	0.7507



(a) EER

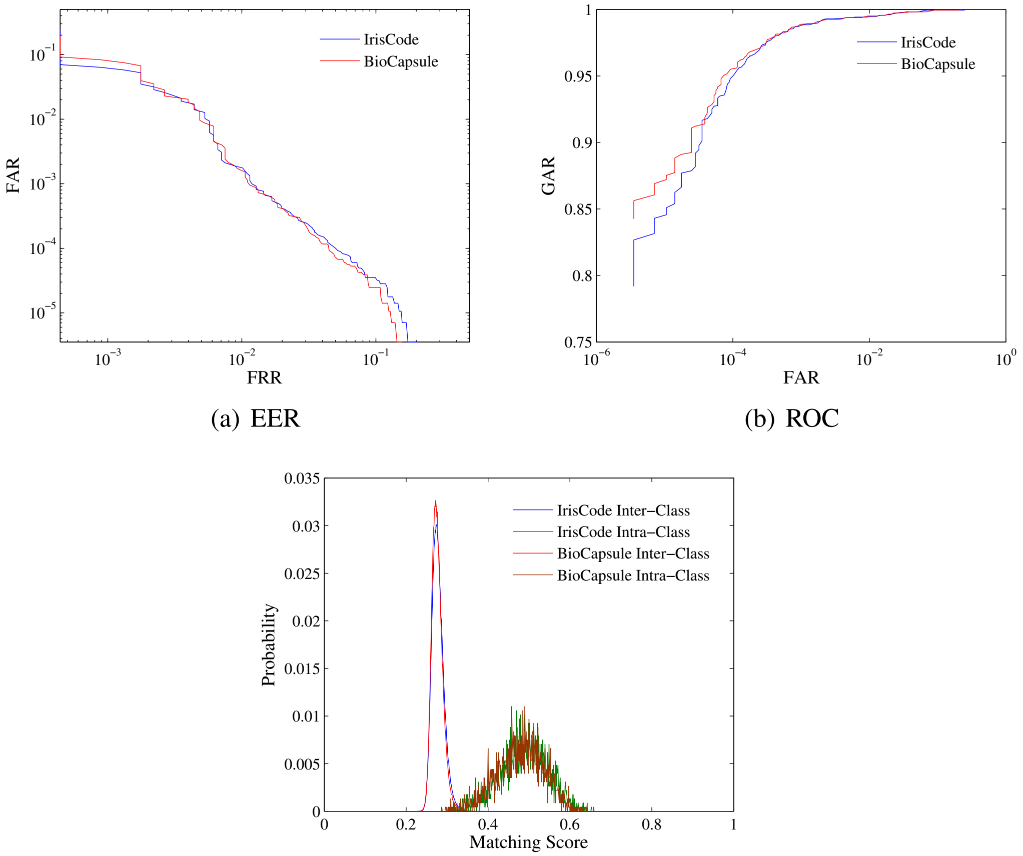
(b) ROC

(c) Inter-class and intra-class distribution

Figure 4.7.: IrisCode and BC performance on the ICE database using 1D Log-Gabor.

4.1.4 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., Figure 4.2(a)). For the BC generation, 1D Log-Gabor was used for feature extraction. To make a comparison, we also implemented 1D Log-Gabor IrisCode [84]. The experimental results are shown in Figure 4.7. Especially, Figure 4.7(b) compares the ROC, and Figure 4.7(c) compares



(a) EER

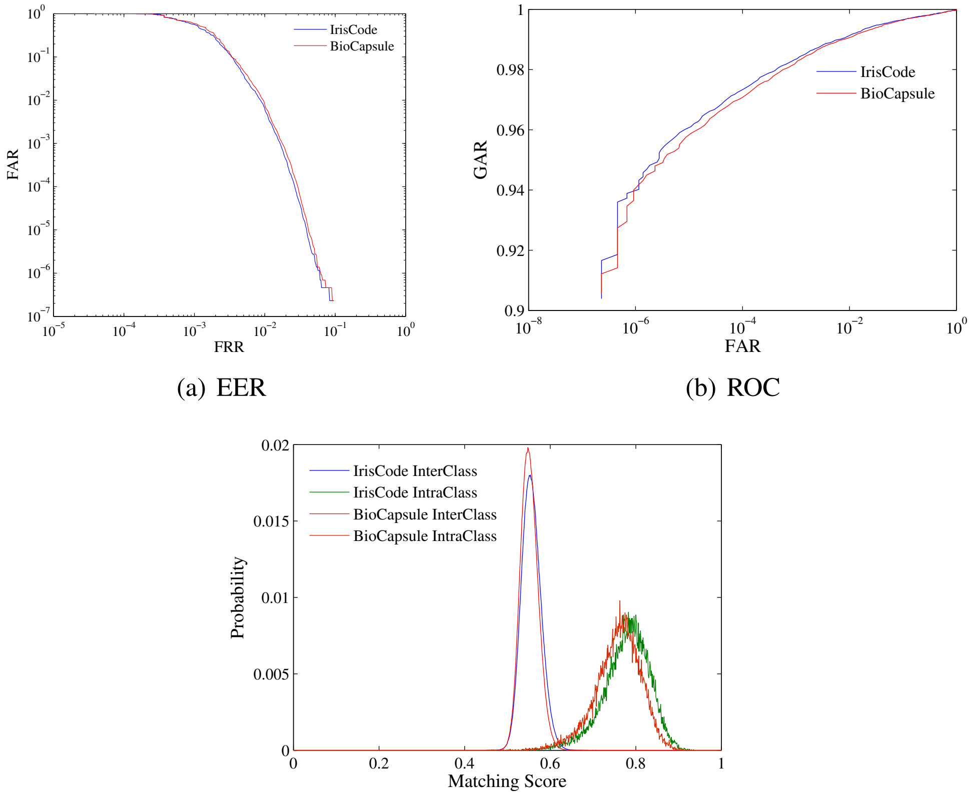
(b) ROC

(c) Inter-class and intra-class distribution

Figure 4.8.: IrisCode and BC performance on the CASIA database using 1D Log-Gabor.

the intra-class and inter-class distinguishability. Those 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., Figure 4.9(c)). 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.



(a) EER

(b) ROC

(c) Inter-class and intra-class distribution

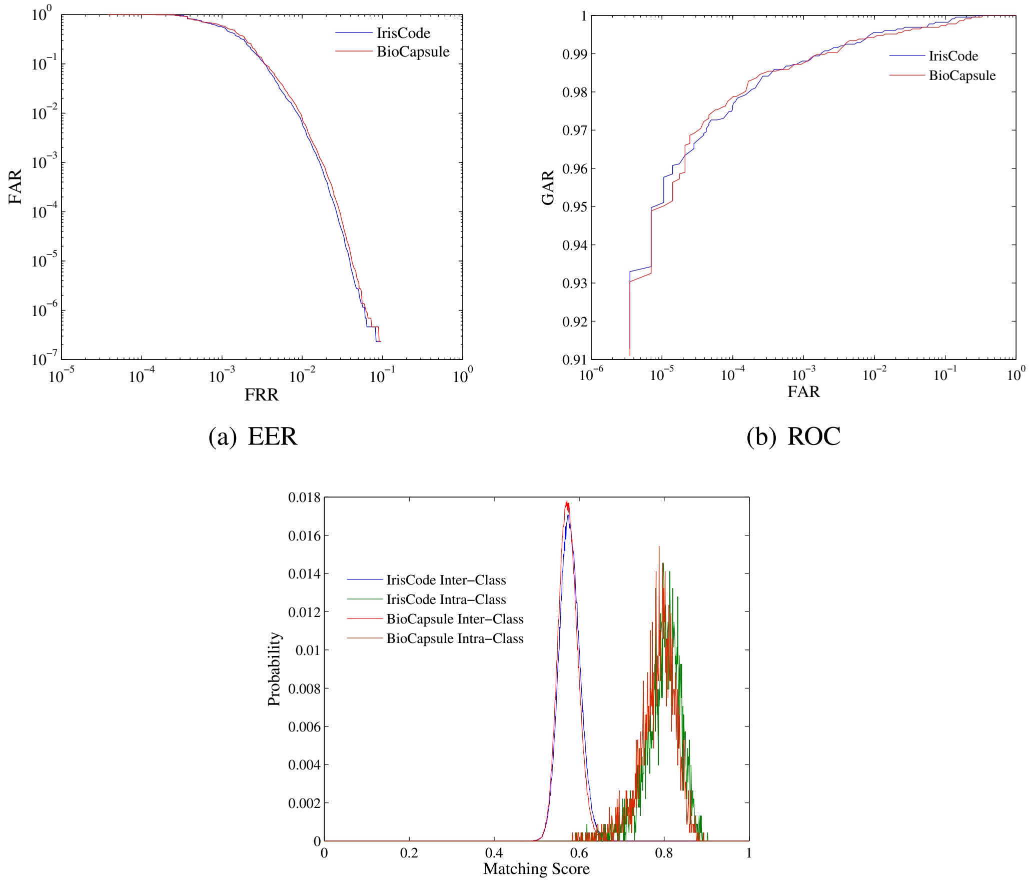
Figure 4.9.: IrisCode and BC performance on the ICE database using 2D Gabor.

Table 4.4: Experiments summary of applying BCs on different levels.

Level	EER	FRR(FAR = 10^{-3})	FRR(FAR = 10^{-5})	FRR(FAR = 0)
signal	0.0253	0.0042	0.0253	0.0304
feature	0.0145	0.0015	0.0061	0.0099
template	0.0150	0.0018	0.0069	0.0108

4.1.5 Applicability of the BC at different levels

This experiment tested the applicability of the BC at different levels. In this experiment, we used the quality right image set. We implemented the BC approach using RS 1 (i.e., Figure 4.2(a)), and 1D Log-Gabor was used for the feature extraction. As the experimental results show results of applying the BC at different levels in Figure 4.11 and Table 4.4, the performance of the signal-level BC is slightly worse compared to the feature-level BC, this indicates that fusion in a higher level (signal-level) outputs most mix-up of user information

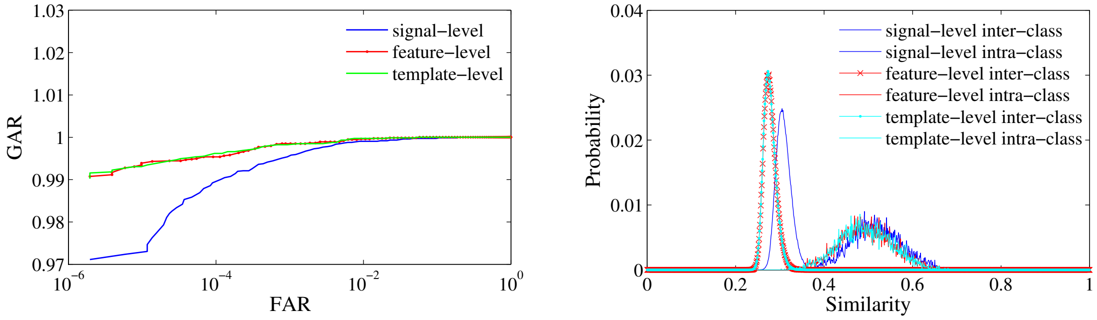


(a) EER

(b) ROC

(c) Inter-class and intra-class distribution

Figure 4.10.: IrisCode and BC performance on the CASIA database using 2D Gabor.



(a) ROC

(b) Inter and intra-class distribution

Figure 4.11.: Performance of BC at different levels on the ICE database.

and reference subject information. Performance of the template-level BC are quite close to but slightly worse than the feature-level BC, this is due to the impact of the template generation. The template generation quantizes features, and the quantization actually loses accurate information about features. Thus, fusion on the template-level actually works on a less accurate level. Also the EER and ROC of feature-level BC are mostly close to the EER and ROC of IrisCode. This is reasonable since user information and reference information are fused at a most “accurate” level, in which noise are removed, and pre-quantization also preserves more information. The performance of BC on different levels are quite close, which indicates that BC is generally applicable to various levels of biometric processes.

4.1.6 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 using RS 1 (i.e., Figure 4.2(a)), 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 [84] and 2D Gabor IrisCode [85]. As the experimental results show in both Figure 4.7 (1D Log-Gabor results) and Figure 4.9 (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.

4.1.7 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 4.5 summarizes the performance of 1D Log-Gabor IrisCode, 2D Gabor IrisCode and the BC approach using different feature extractions on the the ICE database. From the 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 the image quality.

[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% occlusion on remaining rows are considered quality images.

We also observe that the proposed BC outperforms conventional biometric authentication in some experimental settings, which happens (Figure 4.12) when the matching score of two images are close to the selected threshold. The intra-class variability of on-the-fly collected RS samples and the extracted keys could make two iris biometrics matching in the BC while in conventional system they do not.

Table 4.5: Performance summary of BCs.

DATABASE	Approach	EER	FRR(FAR = 10^{-3})	FRR(FAR = 10^{-4})	FRR(FAR = 10^{-5})
ICE	1D Log-Gabor IrisCode	0.0108	0.0204	0.0365	0.0695
(entire database)	BC using 1D Log-Gabor	0.0108	0.0206	0.0374	0.0700
ICE	1D Log-Gabor IrisCode	0.0028	0.0035	0.0063	0.0105
(2245 quality images)	BC using 1D Log-Gabor	0.0030	0.0037	0.0064	0.0109
CASIA	1D Log-Gabor Iris Code	0.0060	0.0119	0.0503	0.1490
(entire database)	1D Log-Gabor + BC	0.0062	0.0114	0.0445	0.1248
CASIA	1D Log-Gabor Iris Code	0	0	0	0
(164 quality images)	1D Log-Gabor + BC	0	0	0	0
ICE	2D Gabor IrisCode	0.0090	0.0164	0.0264	0.0390
(entire database)	BC using 2D Gabor	0.0097	0.0177	0.0291	0.0421
ICE	2D Gabor IrisCode	0.0028	0.0033	0.0051	0.0084
(2245 quality images)	BC using 2D Gabor	0.0029	0.0037	0.0059	0.0096
CASIA	2D Gabor Iris Code	0.0067	0.0119	0.0238	0.0423
(entire database)	2D Gabor + BC	0.0061	0.0123	0.0212	0.0498
CASIA	2D Gabor Iris Code	$7.6 * 10^{-5}$	0	0.0036	0.0036
(164 quality images)	2D Gabor + BC	0	0	0	0

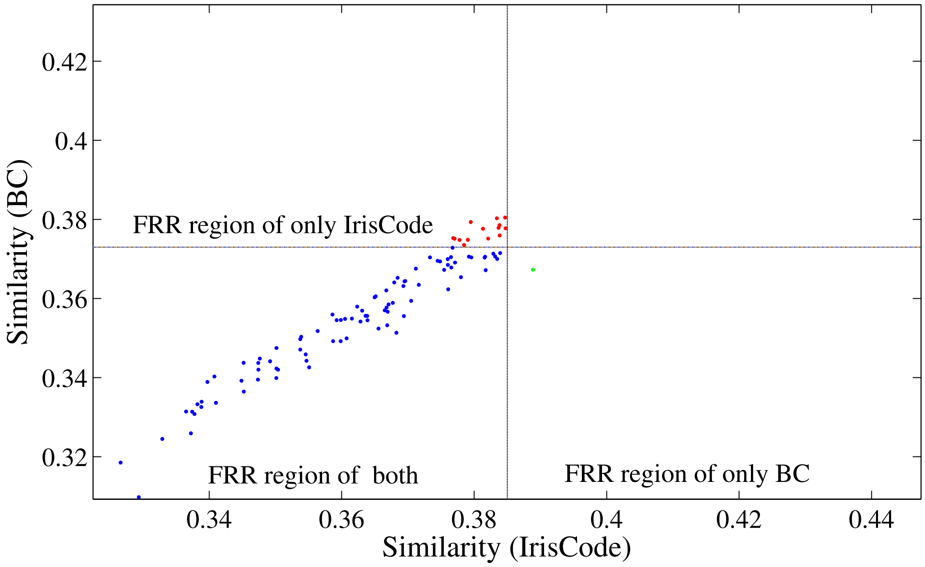


Figure 4.12.: Matching of IrisCode and BC (using 1D Log-Gabor) at FAR 10^{-4}.

4.1.8 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 R_1 (i.e., Figure 4.2(a)) and BCs using R_2 (i.e., Figure 4.2(b)). The two sets of BCs are cross-matched.

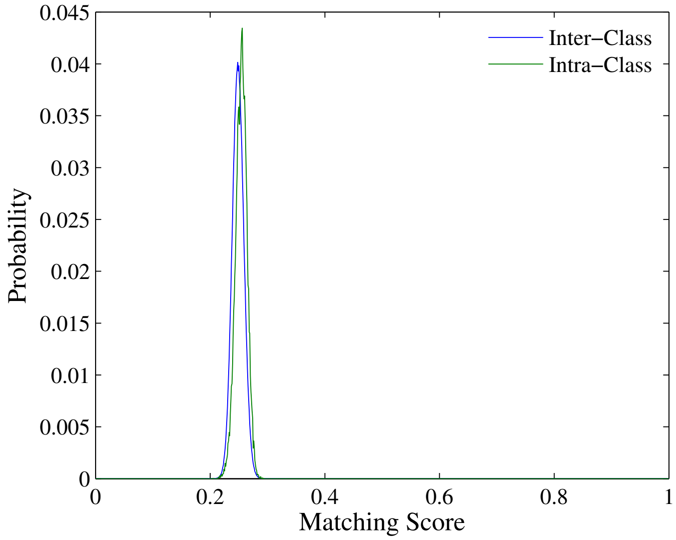


Figure 4.13.: Matching between BCs using R_1 and BCs using R_2 ($R_1 \neq R_2$).

Figure 4.13 shows the intra-class (genuine) and inter-class (impostor) distributions which are quite mix-up. The mixed distributions indicate that it is hard to determine whether or not two BCs (i.e., one from R_1, and the other from R_2) are from the same user. In this sense, we argue that the old BC can not be used to identify or authenticate a user by comparing it to the new BC, and thus is revoked.

4.1.9 Unlinkability and cross-matching resistance of the BC

The purpose of this experiment is to test unlinkability (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 unlinkable, BCs 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 matchings are mixed).

Figure 4.14 shows the genuine and impostor distribution of matching IrisCodes to BCs. The mixed distributions indicate good capability of defeating cross-matching attacks.

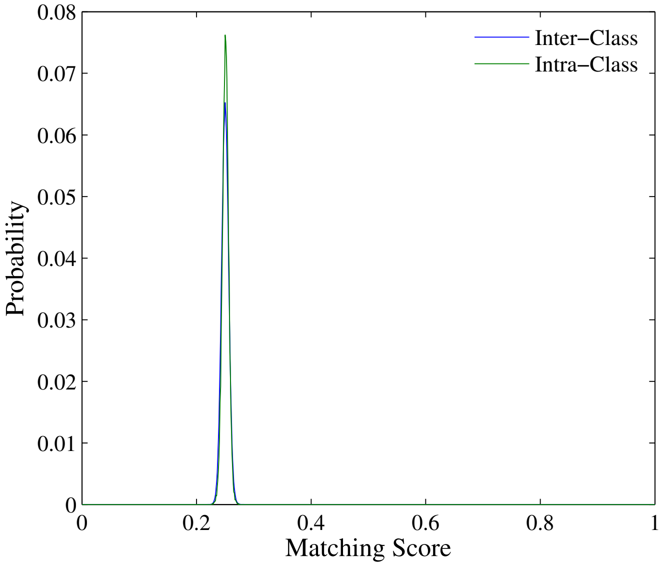


Figure 4.14.: 1D Log-Gabor IrisCodes match to BCs.

The unlinkability of the BCs using different RSs is equivalent to the revocation in subsection 4.1.8 which is well established.

Through the experiments in this section, we have proved that the BC based approach is quite usable, revocable, and cross-matching resistant. It is general applicable to 2D Gabor and 1D Log-Gabor approaches and possibly others. Moreover, the performance of the system is maintained. It is also noteworthy that ”lost-key” scenario is not considered in experiments which is raised by some BCS and CB approaches using additional factors like user-specific password or PIN. 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.

4.1.10 Performance variations using a physical/logical RS

In Section 3 **Selection and setting of RS in the system**, we have proposed that 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. Here, we measure the performance variations when a physical/logical RS is used in the authentication system. (Note: as above experiment settings, we introduced SNR = 40 to simulate the physical RS. And the results are obtained on whole database.) Figure 4.15 shows the comparisons of EER, ROC and inter and intra-class distribution of these two cases. It is obvious from Figure 4.15 that the performance makes no much difference, which is a good sign such that the key extraction and secure fusion mechanisms can tolerate this RS variances very well.

On a closer view of the results (Table 4.6), BCs using logical RS perform slightly better than BCs using physical RS.

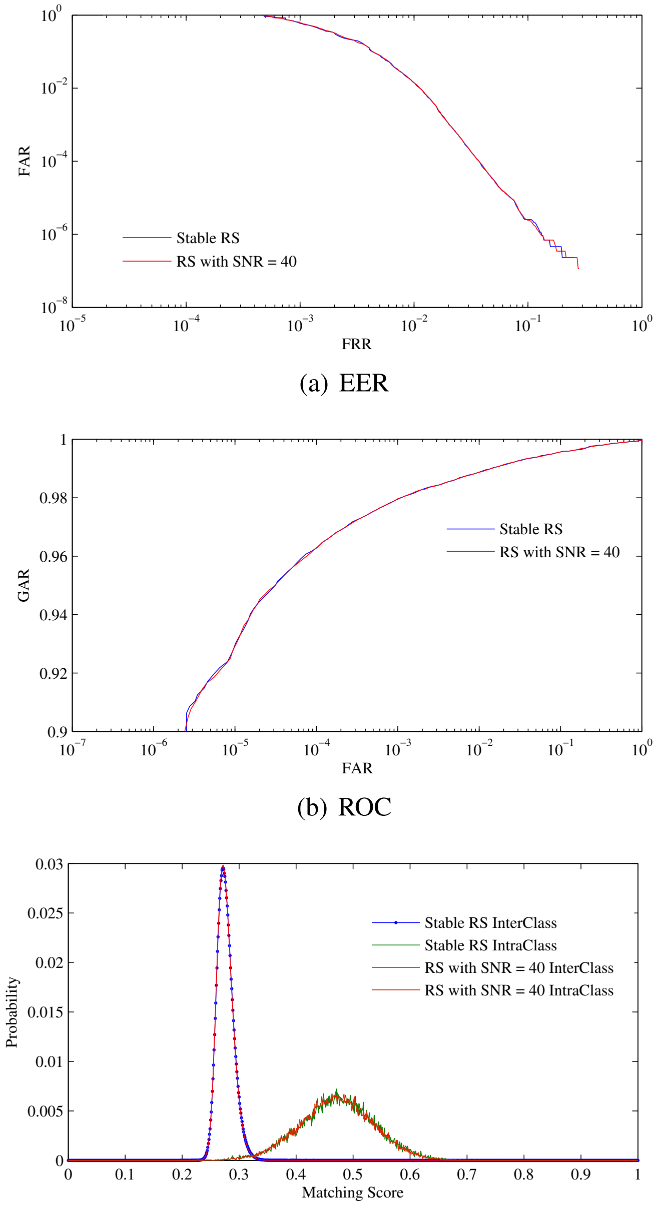
Table 4.6: Experiments summary of BCs using physical/logical RS.

RSs	EER	FRR(FAR = 10^{-3})	FRR(FAR = 10^{-4})	FRR(FAR = 10^{-5})
Stable RS	0.0108	0.0206	0.0374	0.0698
RS with SNR = 40	0.011	0.0203	0.0376	0.0699

4.1.11 Performance of the BC using user-specific RS

As many CB and BCS systems using user-specific information, our BC system allows each user to have a user-specific RS. To test on this case, we randomly generate a RS for each user. The experiment results are shown in Figure 4.16. (Note: the results are obtained on whole database. And the system-wise RS is assumed stable thus it is a logical RS.)

It is quite interesting from Figure 4.16(c) that the intra-class distributions of using system-wise and user-specific RS are quite similar. From this result, we can claim that the introducing of system-wise RS does not change the original characteristics (distribution) of biometrics. However, the introducing of user-specific RS makes inter-class matching harder, thus the performance is increased. Table 4.7 shows a closer view on the compar-



(a) EER

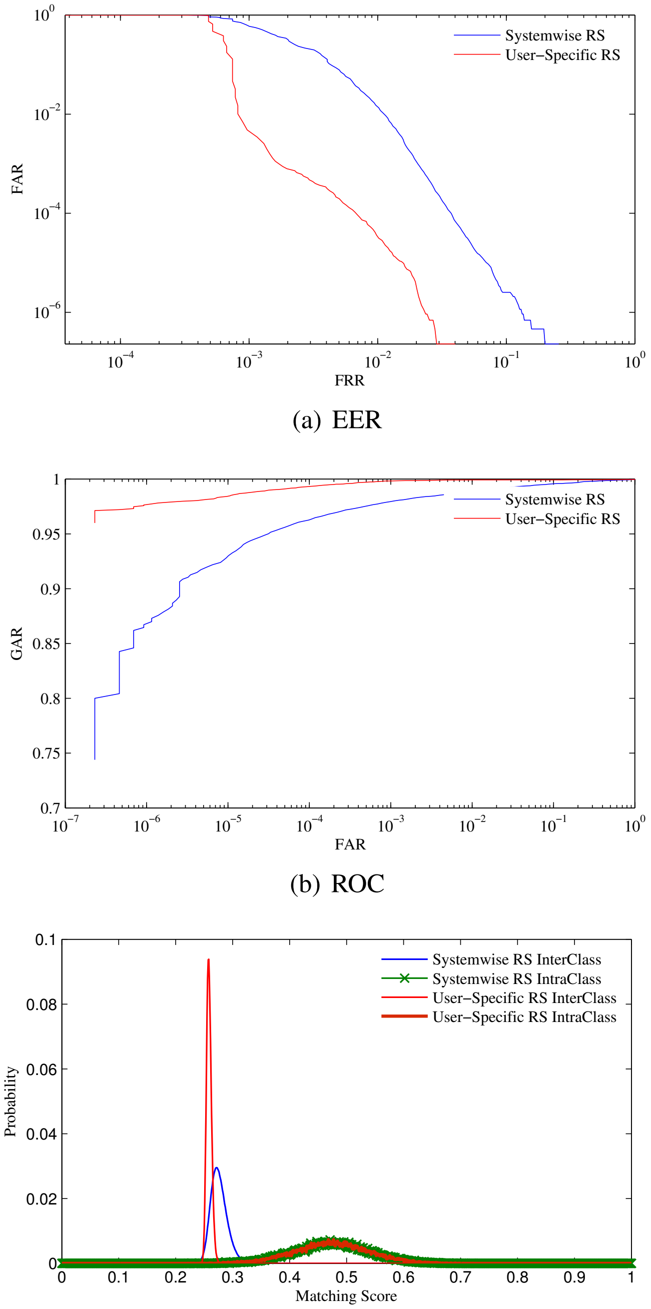
(b) ROC

(c) Inter and intra-class distribution

Figure 4.15.: Performance of BC using a physical/logical RS.

Table 4.7: Performance of BCs using system-wise/user-specific RS.

Level	EER	FRR(FAR = 10^{-3})	FRR(FAR = 10^{-4})	FRR(FAR = 10^{-5})
System-wise RS	0.0108	0.0206	0.0374	0.0698
User-Specific RS	0.0015	0.0017	0.0067	0.0159



(a) EER

(b) ROC

(c) Inter and intra-class distribution

Figure 4.16.: Performance of BC using a system-wise(stable)/user-specific RS.

isons of performance of BC using system-wise and user-specific RS. It is obvious that BCs using user-specific RS performs much better compared to that using system-wise RS. This is similar to the CB systems that use user-specific information.

4.2 Analysis and Discussions

4.2.1 Security: entropy of the BC

In the ideal case, the security of the BC is the bit string length of the BC. However, in practice, due to the distribution of the biometric data, the entropy of the BC cannot reach the maximum, i.e., the length of the BC. Therefore, we compute the true entropy of the BC which is a measure of the BC security. There are two approaches to compute the entropy of the BC: entropy summation and degrees of freedom [89].

Assume different bits in the BC are independent to each other, the entropy of the BC is the summation of the entropy of the each bit:

$$\sum H(b_i) = -(p_r \log_2(p_r) + (1-p_r)\log_2(1-p_r)), \tag{4.4}$$

where p_r is the probability of $b_i = 1$.

However, we can expect that the bits in the BC are not always independent to each other as IrisCode does [85]. Assume the distances between binary templates follow the binomial distribution (which is justified through experiments), the degree of the freedom is useful in the situation that the bits of binary templates are correlated, and it is obtained by [85]:

$$N = p(1-p)/\sigma^2, \tag{4.5}$$

where p is the average normalized hamming distance, σ^2 is the variance of the normalized hamming distances between different binary templates.

Guessing BC (if some other's BC is known)

According to [90], there are correlations that exist in every iris due to the radial structure of furrows and etc. And the information entropy of a BC, due to the correlations, can hardly be comparable to the length of the BC. Table 4.8 summarizes the degree of freedom using different approaches proposed in the dissertation. It is shown that the information entropy of the BC is comparable to that of the traditional IrisCode. And the information entropy of the 1D Log-Gabor feature based BC and the 1D Log-Gabor template based BC reach up to 1000 bits, which shows adequate security given nowadays computation power. Also, according to [90], from the BC, if the attacker has no or little knowledge about how a person's iris bits are correlated (which is always the case with current state of knowledge), the BC is much more secure than expected (i.e., around 1000 bits).

Table 4.8: BC: degree of freedom.

DATABASE	Approach	Degree of Freedom
ICE (right)	1D Log-Gabor IrisCode	882
	1D BC(Signal)	749
	1D BC (Feature)	1002
	1D BC(Template)	1004

Security if a BC and RS both lost (guessing Key from attacker's own key)

According to above analysis, the security of the system if both BC and RS are lost, is equal to the key strength. The degree of freedom of the key extraction approach 1 is 76 bits, and that of the key extraction approach 3 is 269 bits. We say this security is based on the assumption that the attacker has the knowledge of the distributions of all users' keys. However, as the analysis of BC's degree of freedom, if attacker has no or little knowledge about how a person's key bits are correlated, the key is much more secure than expected (i.e., around 224 bits in key extraction approach 1 as we analyzed earlier).

4.2.2 Property analysis

We analyze the properties of the concrete iris based BC authentication system according to the definitions proposed in Section 3.2 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 12000*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 [91]. Thus, the security of the BC system is around 1,582 bits.

Privacy-preservation. The hardness of obtaining user biometrics from BC has been analyzed in Subsection 3.6. 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 [92]. 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 scheme provides the following usability: user of the scheme does not need to remember any information; and user of the scheme does not need to carry any physical object.

4.2.3 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

[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.

experiments implemented using MatLab 2010 on a laptop with Dual-Core CPU 2.10 GHz and 4GB 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.

4.2.4 Revocability improvement

The above proposed authentication approach uses a single RS for all user. Intuitively, the revocation of a RS requires all users to re-register against a new reference subject which is clearly not a good revocability solution. In this section, we propose a revocability improvement solution. In case that the system RS R_1 needs to be revoked, the system selects a new RS R_2. For the future authentication, the BC is generated through two steps of fusions. The first fusion happens between the sampled biometrics and R_1, while the second fusion happens between the fusion result from previous fusion and R_2. Before that, the system will update the existing database (i.e., the storing BCs) to a new set of BCs which are the fusion between the old BCs and R_2. The usability of this solution depends on the performances of the updated BCs, which is shown in Figure 4.17. Actually, compared to the original BCs, the performance of this updated BC set shows some degradation. However, we can gradually update a secondary BC set, which is generated from sample biometrics (from an authentication request) and a RS R_3.

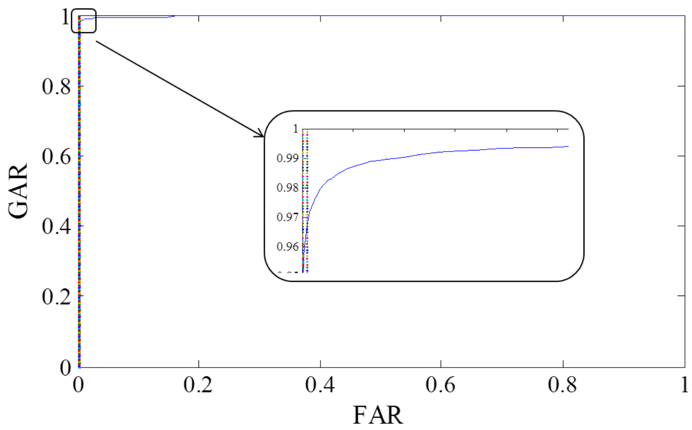


Figure 4.17.: Performance of the updated BC set.

4.2.5 Application of BC on user identification

Identification and authentication are too different processes. We say authentication is a process to verify the claimed identify of a user using some credentials (e.g., password, certificate, biometrics), while the identification is a process to establish user's identify. Identification can be naturally broke into a sequence of authentications [4]. Figure 4.18 shows the work mode of a typical biometric identification of conventional biometric systems. Here, a template which is called query template is generated from the sampled biometrics. And the matcher matches the query template against a set of templates coming from system database for identification.

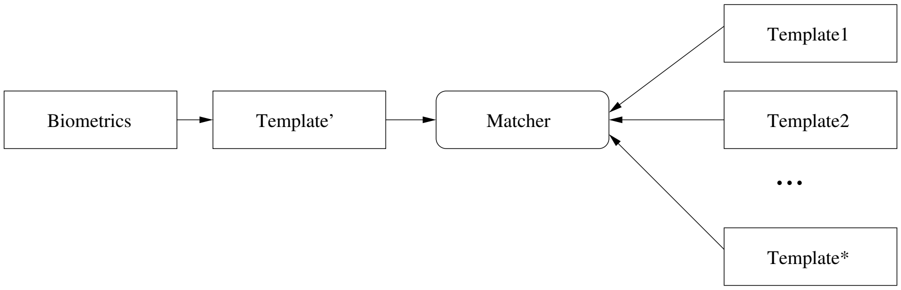


Figure 4.18.: Identification process of conventional biometrics systems.

Let us see what will happen if the biometric identification is proceeded in a biometric system using system-storing helper data. Examples of such a system include fuzzy commitment system, fuzzy vault, etc. In such a system (Figure 4.19), from the sample biometrics the credential generator uses the helper data (for each identity) to extract the query credential (e.g., hash of codeword in fuzzy commitment system), and the query credential is matched to the credential associated with the helper data. Compared to the conventional biometrics system, identification in such system is more heavy.

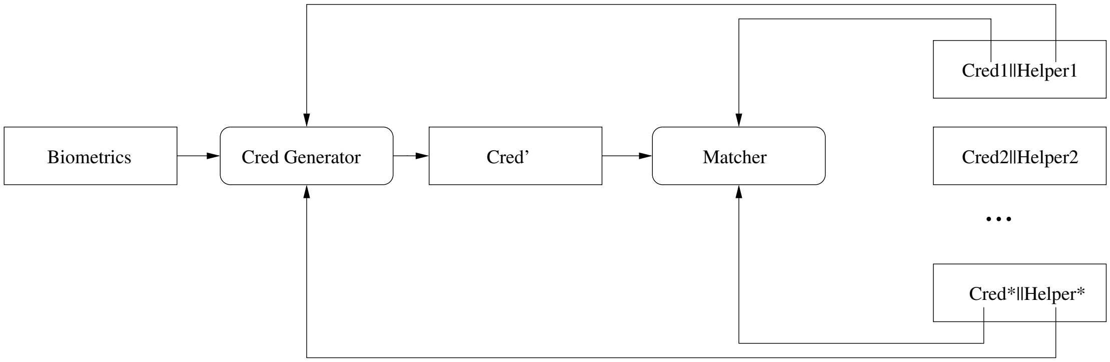


Figure 4.19.: Identification process of biometrics systems using helper data.

Figure 4.20 shows the word mode of identification in BC system. In the BC system, the BC generator extracts query BC from the sampled biometrics and the RS. Thereafter, the query BC is matched against a set of BCs stored in the system database. Here we observe that the work mode of BC system in this scenario is quite similar to that of the conventional biometrics systems. The only addition is the BC generation, which compared to the systems in Figure 4.19 is much more efficient.

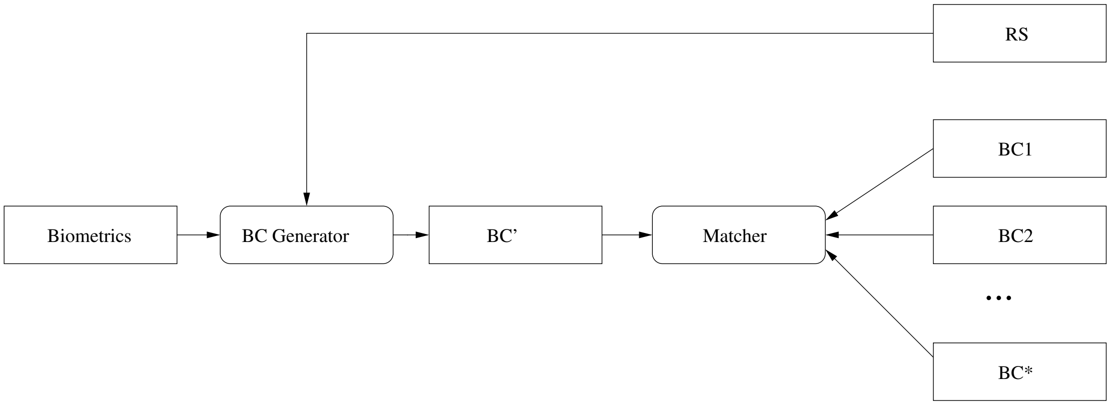


Figure 4.20.: Identification process of BC system.

There is another system that requires user to provide user-specific information (e.g., PIN) for authentication. The work mode of such a system is similar to ours, however it requires user cooperation which in many scenarios (e.g., surveillance) is not practical. Yet the proposed BC system can be applied to identification without this kind of user cooperation.

5 BIOMETRICS BASED ACTIVE AUTHENTICATION

This chapter presents the proposed biometrics based active authentication approach.

5.1 Threat Model

A biometric authentication system contains two stages as presented in Chapter 3: registration and verification. Initially, the system samples and pre-processes the user biometrics. From the preprocessed biometrics, biometric features are extracted and a biometric credential (i.e., biometric template) is generated for registration. During any future verification, the user is sampled again and through the same processes a query biometric credential (i.e., query template) is generated and matched against the registered one. A biometric active authentication system can periodically repeat the verification stage and make authentication decision [93].

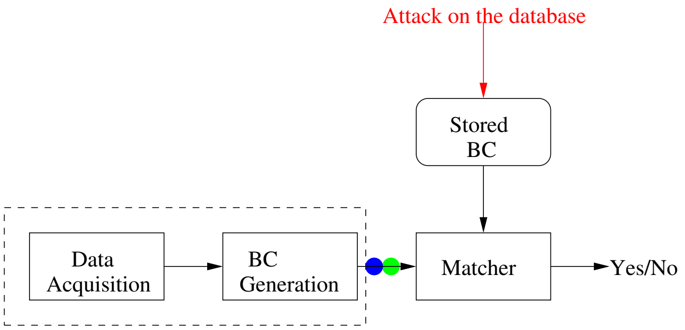


Figure 5.1.: Active authentication system attack model.

In Figure 5.1, we identify the attack model for the active authentication system. Different from the attacks on conventional biometric authentication systems [28], the attacker can accumulate a larger amount of evidences towards user biometrics by using certain vul-

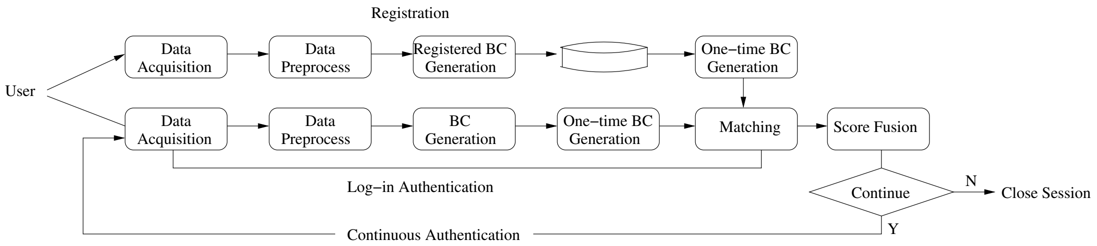


Figure 5.2.: Proposed active authentication system.

nerabilities. Here are listing several attacks which are assumed more feasible to launch and hard to detect and can breach system security or infringe user privacy:

- Intercept a query biometric information: the attacker can intercept the biometric credentials (e.g., biometric template) sent from the authentication client and derive user biometrics.
- Intercept and accumulate data: different from one-time authentication, the attacker can accumulate a larger amount of evidences (e.g., biometric credentials) towards user biometrics by exploiting certain vulnerability of the system, and from the accumulated data may be able to make educated guess of user biometrics.
- Replay old biometric data and get authenticated: the attacker replays an old biometric data he/she observed and tries to get authenticated.
- Forge biometric credentials and get authenticated: the attacker tries to generate biometric credentials, inserts it into the communication channel of the system and gets authenticated.
- Attacks on system database: similar to the attacks in conventional biometric authentication, the biometric information stored in the system database can be a target for the attacker.

Given this model, we propose biometrics based active authentication system as follows.

5.2 Biometrics Based Active Authentication Model

In the proposed model, the user client will compute the authentication credentials and transmit them to the server for authentication and we are not assuming there is a secure channel between the user client and the server, the authentication credentials are vulnerable to various attacks, e.g., replay attack, man-in-the-middle attack, etc. For this reason, the authentication mechanism needs to be secured.

In our previous work [32, 94], we proposed a secure and privacy-preserving biometric credential BioCapsule (BC) which is used instead of conventional biometric template for user authentication. The BC is a “secure fusion” of user biometrics and reference subject (RS) biometrics using some intrinsic keys directly extracted from user biometrics and RS biometrics. And user biometrics is secure in case of a lost BC and the RS.

For this client-server active authentication model, we propose that the user client and the server share a common reference subject (RS). Due to the security feature of the BC, BC transmitted from client to the server will not reveal information about user biometrics. Considering that an attacker can replay (or forge) a BC for continuous authentication even though the attacker cannot obtain user biometrics from the BC and that the attacker can accumulate information to make educated guess of user biometrics even though such an attack is not known yet, we propose the one-way hash chain to utilize temporary RSs and generate changing BCs (i.e., one-time BCs). Because of the changing of BCs, outdated BCs will not be matchable to the new BC. And due to the utilization of the one-way hash chain, outdated BCs will not help to forge BCs for future verification.

It is expected that during the active authentication the legitimate user can fail to continuously provide quality biometric observations. However, the system must be able to compute a confidence score that the current user is same as the log-in one at any given time point even without biometric observations. For this purpose, we use fusion approach. The fusion approach integrates the evidences along the time axis. The fusion is designed according the criteria: 1) at a given point if no biometrics is observed, the fusion gives a reduced confidence; and 2) older observations (i.e., older evidences) provides less certainty about the user, thus contribute less in the fusion.

The proposed biometrics based active authentication system consists of several stages (Figure 5.2): user registration, log-in authentication and continuous authentication.

- User registration (Figure 5.3): the system samples user biometrics, and fuses user biometrics with a long-term RS biometrics RS^L by “secure fusion” [94]. From the fused biometrics a “registered BC” BC^R is extracted and stored in the system database. The long-term RS RS^L is stored both in the server and the authentication client.

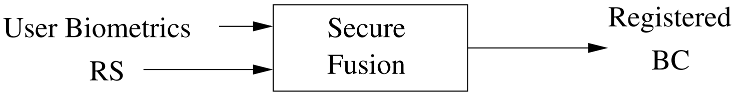


Figure 5.3.: User registration.

- Log-in authentication: the system samples user biometrics and fuses the user biometrics with the RS^L through “secure fusion”. From the fused biometrics, a query BC BC^Q is generated and sent to the server. The server will match BC^Q with the registered BC^R, and the similarity score of the two BCs is matched against a pre-defined threshold for authentication. Upon a successful log-in authentication, the server sends the client a seed RS RS^S. The client and the server can generate independently from the shared seed RS RS^S a list of short-term RSs (i.e., $RS_i = hash(RS_j)$) using a one-way hash chain and reverse order of the list, the set of short-term RSs is represented using $RS_1, RS_2, \cdots, RS_n$ such that it is infeasible to derive RS_j from RS_i $(j > i)$ (Note: the user can also pre-loaded with a set of short-term RSs. However, more storage is required.).

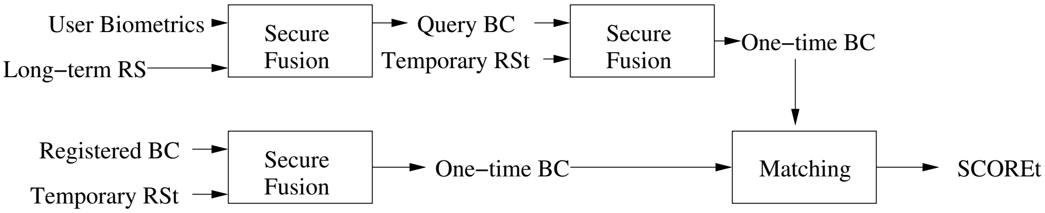


Figure 5.4.: One-time BC generation and matching.

- Continuous authentication: after a successful log-in authentication, the system enters into the continuous authentication stage. Periodically the system samples user biometrics. At the jth sampling, at the client side a one-time BC (i.e., BC_j^Q) is generated using RS_j and sent to the server. The server matches BC_j^Q and the corresponding one-time BC $BC_j^{'}$ generated using BC^R and the same RS_j. A score $SCORE_j$ recording the similarity between BC_j^Q and $BC_j^{'}$ is obtained (Figure 5.4). Considering the $SCORE$s (i.e., $SCORE_i, \cdots, SCORE_j$) obtained during a time window W, the server fuses those scores and computes a confidence score that records the belief that the current user (present at the jth sampling) is the same as the log-in user (as shown in Figure 5.5). W can be as large as containing all previous $SCORE$s since successful log-in authentication, or as small as containing only latest $SCORE$. The confidence score is compared to a pre-defined threshold θ for "Y/N" decision of locking the current session. The selection of W and θ is related to the security (e.g., how quickly the intrusion can be detected) and usability (i.e., how legal user can use the system), which will be justified through experiments later (Note: in another word, according to security and usability requirements, choices of W and θ can be made.) .

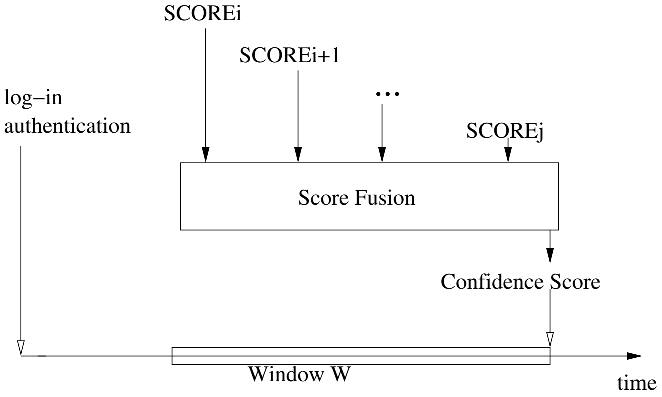


Figure 5.5.: Score fusion for continuous authentication.

Different fusion mechanisms which meet the criteria mentioned above can be used for computing the confidence score. Two are used here: Time-Decaying score fusion and Dempster-Shafer score fusion (Note: we will compare the performance of various fusion mechanisms in the following section.). At a given time j, from a time window W a set of similarity scores $SCORE_i, \cdots, SCORE_j$ is obtained along the time axis (i.e., $SCORE_i$ is an older observation, $SCORE_j$ is the current (latest) observation). Each score, denoted using $SCORE_*$, is a quantization of similarity between the current user and the log-in user, and can be used as an indication of the confidence that the current user is same as the log-in user. The Time-Decaying fusion based confidence score $CONF_j$ (at time j) is obtained by:

$$CONF_k^{decay} = w * CONF_{k-1}^{decay} * e^{-r\Delta t} + (1-w) * SCORE_k, \tag{5.1}$$

$k = 2, \cdots, j$, where w is a weight, Δt is the difference between current time and the time when $CONF_{k-1}^{decay}$ is computed, and r is the decay rate. By adjusting w and r an older observation can be made contribute less in the fusion.

The Dempster-Shafer score fusion is derived from Dempster-Shafer theory [95], which allows to combine evidences from different sources and arrive at a degree of belief that takes into account all the available evidences. The Dempster-Shafer fusion based confidence score is obtained by [96]:

$$CONF_k^{DS} = \frac{(CONF_{k-1}^{DS} * SCORE_k)^p}{((CONF_{k-1}^{DS} * SCORE_k)^p + ((NonCONF_{k-1}^{DS}) * (NonSCORE_k))^p)}, \tag{5.2}$$

$k = 2, \cdots, j$, where p is the parameter to weight the evidence. We say $SCORE_k$ and $NonSCORE_k$ is the belief and disbelief that the user (at time k) is same as the log-in user, and

$$\begin{aligned} NonCONF_*^{DS} &= 1 - CONF_*^{DS}, \\ NonSCORE_* &= 1 - SCORE_* \end{aligned}$$

Eq. 5.2 is a generalization of Dempster-Shafer theory, and it is suitable to fuse information from the same source (i.e., in our case, a set of SCOREs from the same client). According to [97], choosing a p setting $p > 0.5$ will weight more on the newly coming observations, while choosing a setting $p < 0.5$ will give less weight when new observations are fused.

It is possible that at a given time no biometric observation is obtained, at this situation the confidence score needs to be reduced but not directly drop to zero. Dropping direct to zero will generate lots of false rejection thus deteriorate system usability. The Time-Decay fusion (Eq. 5.1) can meet the criteria though decaying. For Dempster-Shafer fusion, assigning $SCORE = 0$ will make confidence score directly drop to zero according to

Eq. 5.2 and violates this criteria. For this reason we assume that there is a "virtual user" and assign $SCORE$ (and $NonSCORE$) a small value to indicate that the "virtual" user is same to the log-in user with small belief (and disbelief). In the following, we use $SCORE_{no}$ and $NonSCORE_{no}$ to specify belief and disbelief when no biometric observation is obtained at a sampling time, and it is not necessary that $SCORE_{no} + NonSCORE_{no} = 1$.

As mentioned above, the system sets a threshold θ. At a given time point, if the confidence score is above θ, the continuous authentication phase is continued. While if the confidence score drops below θ, the session is automatically logged out.

5.3 Security Analysis

In the following we analyze how the proposed system can defeat against potential attacks.

- Intercept a query biometric credential: obtaining user biometrics from a lost BC_i^Q needs to decompose two steps of "secure fusions". The first fusion fuses user biometrics with a long-term RS, and the second one fuses the query BC (i.e., the fusion result from the first fusion) and a short-term RS. According to our analysis, user biometrics is secure against a lost BC (and the RS) [94], that is, decomposing one "secure fusion" is difficult. Thus such an attack is not feasible.
- Intercept and accumulate data: If the system does not have the second fusion and uses only query BC for continuous authentication, even though the fusion is secure, it is possible that the attacker accumulates a large number of the query BCs and make educated guess of user biometrics (although it is not known how to do the guessing). The system introduces the second fusion, through which one-time BCs are generated using changing short-term RSs. Thus for each intercepting one-time BC, a new unknown (i.e., the corresponding short-term RS) is introduced to confuse the attacker. With/without knowing the short-term RSs, the secure fusion makes the deriving of the query BC from one-time BCs difficult. Thus accumulation of one-time BCs will not help to recover query BC and then derive user biometrics.

- Replay old credentials and get authenticated: due to the usage of short-term RSs in the second “secure fusion”, each one-time BC is generated from a different short-term RS. Thus the old one-time BC cannot match to new one-time BCs toward different short-term RSs. Replaying attack is not feasible.
- “Forge biometric credentials and get authenticated” can happen if the attacker can: (i) forge one-time BC without any knowledge; (ii) forge one-time BC BC_j^Q $(j > i)$ if an older observation BC_i^Q is obtained; and (iii) forge one-time BC BC_j^Q $(j > i)$ if an older observation BC_i^Q and its corresponding RS_i are both obtained. It is evident that among those three attacks, attack (iii) is the easiest one. Such an attack, however, in our approach is hard. Firstly, similar to the attack as analyzed in [94], given a one-time BC (e.g., BC_i) and its corresponding RS (e.g., RS_i) obtaining another fusion component (i.e., the query BC BC^Q towards the long-term RS) is hard. Secondly, given RS_i obtaining RS_j $(j > i)$ is hard due to the usage of the one-way hash chain. Without the two components BC^Q and RS_j, forging BC_j^Q is difficult.

Above analysis indicates that the proposed system can defeat various attacks raised in our security model.

6 EXPERIMENTS AND ANALYSIS

In this chapter, we will quantitatively analyze the performance (i.e., security, usability) of the proposed system.

6.1 Experiment Setting and Evaluation Metrics

Some commonly used biometrics are iris, face, fingerprints, etc. Among these techniques, iris is tested to be one of the most reliable ones [85]. In this section we use iris as a case to test the performance of the proposed system. A typical iris recognition system includes the following major steps: image acquisition, iris segmentation, feature extraction, template generation and matching. The proposed system uses one-time BC instead of template for matching. The process of one-time iris BC generation is shown in Figure 6.1, which includes the iris image acquisition, iris segmentation, long-term BC generation [94], one-time BC generation.

The iris segmentation locates the iris region. We used the circle-based edge detection to find the pupillary and limbic boundary. And we transferred the extracted iris to the polar coordinates and generated the mask map (for matching). For BC generation, we used the BC proposed in [94] in which 1D Log-Gabor is used as a bandpass filter for feature extraction [84]:

$$G(\omega) = e^{\frac{-\log((\omega/\omega_0)^2)}{2\log(\sigma)^2}}, \tag{6.1}$$

where σ is controlling the filter bandwidth and ω_0 is the filter's center frequency and derived from filter wavelength. The similarity of the one-time BC from client (i.e., user) and another one computed by the authentication server is calculated. These similarity scores which are collected along time dimension are fused by either Time-Decay fusion

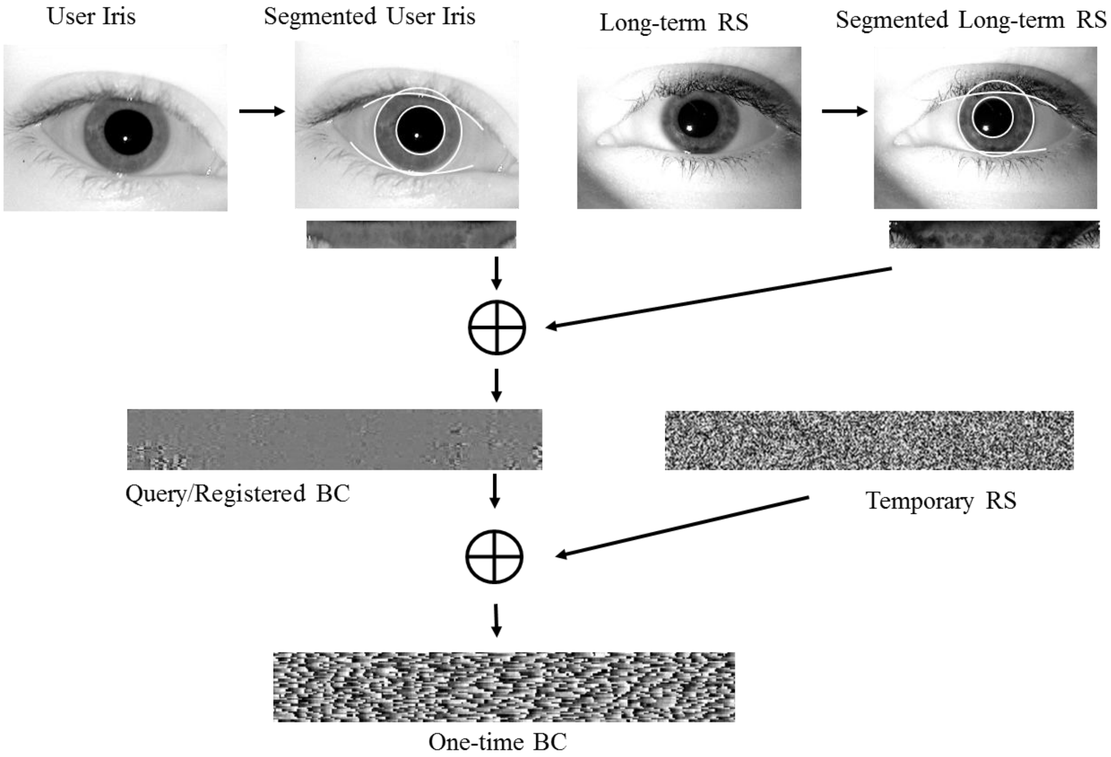


Figure 6.1.: One-time iris BC generation.

or Dempster-Shafer fusion. Experiment results will show the advantages of different fusions under different situations.

A challenge for continuous authentication system is that without active cooperation it is possible that there could be no quality biometric observations: the user either fails to provide biometrics or provides poor quality biometrics, e.g., occluded images. In the following, we call frames containing no quality biometric observations *invalid frames*. And it is reasonable to assume that there is a preprocessing step using certain mechanism (as proposed in [35]) to measure the quality of the iris frames and filter out invalid frames.

Database. The performance of the proposed technique was simulated based on the ICE database [83] which is provided by National Institute of Standards and Technology for the Iris Challenge Evaluation (ICE) 2005. We performed experiments based on the right eye set for system evaluation. We chose one iris image from ICE as our long-term RS (Figure 4.2 (a)) and one iris image from UBIRIS [87] as the RS seed (Figure 4.2 (b)) to generate a set of short-term RSs.

Evaluation Metrics. Typical metrics for one-time authentication are FAR (false acceptance rate) and FRR (false rejection rate). However, these metrics do not consider *time* information for continuous authentication. For continuous authentication, Sim *et al.* proposed metrics, e.g.,"Time to Correct Reject", "probability of Time to Correct Reject", ect., based on timing information [61]. Here, we observe that time consists of two factors: frame number and sample frequency. Assume for a time period T, N frames (either valid or invalid) are sampled for biometrics. Obviously, the sample rate is N/T, and each frame if authenticated can grant access for a time period T/N. To ease the analysis, we use the frame as basis for new performance metrics. Also we use the following metrics for evaluation of security of the system.

- EER and ROC for Log-in. The proposed system uses one-time BC for log-in authentication. Thus same as conventional one-time authentication system, we use EER and ROC to measure the log-in authentication accuracy.
- Usability. Analogous to GAR (genuine acceptance rate), the usability is defined to be the fraction of the total time that a legitimate user is granted access by the system. For instance, a legitimate user tried to get authenticated for a time period during which N frames are sampled. And the user can get access for n out of N frames. The usability will be n/N.
- Frame to Safe Continue Use (FSCU). For continuous authentication, it is possible that during a time period a legitimate user fails or an impostor is careful not to present any biometric observations (i.e., continuous invalid frames are provided). In this case, the system gradually reduces the confidence score and after certain time when the confidence score drops below a threshold, rejects the user. For higher security requirements, the FSCU should be set smaller, however a smaller FSCU may give lower usability, vice versa.
- Frame to Correct Reject (FCR). "Time to Correct Reject" is proposed in [61] which considers the intruder's presence not harmful as long as he/she takes no actions (e.g., copy files). Different from this, we define FCR be the number of observed valid frames between the system starts to observe intruder's presence until the system logs

out the intruder. A small FCR indicates that the system can detect the presence of intruders more quickly, while a small FCR can also reduce system usability.

- Security Characteristic (SC). Security is defined to be

$$1/\log(FCR+1)\log(FSCU+1). \tag{6.2}$$

  An intruder may be careful not to present any biometric observations to the system. In this case, the intruder can illegally use the system for a time period during which a number (i.e., equal to FSCU) of frames are sampled. The higher the FCR, the lower security is obtained. Also FCR contributes to the security characteristic of the system. The bigger the SC is, more secure the system obtains. Given the most secure case that (FSCU = 1) whenever an invalid frame is sampled by the system, the user is rejected and that (FCR = 1) intruders are always rejected within one valid frame, the ideal security the system provided. And at this situation, $SC = 1/\log(1+1)\log(1+1) = 2.0814$. As FSCU and FCR increase, less security the system provides.

- Usability-Security Characteristic Curve (USC). The USC is a plot of Usability versus SC. Similar to conventional one-time authentication, the system will make authentication decision based on a threshold θ. If the confidence score is bigger than θ, the user is accepted, vice versa. For a θ, a Usability and corresponding SC are obtained. By changing the θ, the USC curve is obtained. USC is helpful for selecting a θ given various Usability and SC requirements.

6.2 Analysis of Log-in Authentication

The log-in authentication uses the BC. Thus we constructed a BC using the long-term RS (as shown in Figure 4.2 (a)) for each image from the right set of the ICE database and cross-matched them. The EER (i.e., equal error rate when FAR equals to FRR) of the system is 1.16%, and the authentication accuracy is around 98.84%. These results indicate that the BC is good for identity-bearing and the iris based BC can be used as identity credentials for log-in authentication.

6.3 Analysis of One-time BC Performance

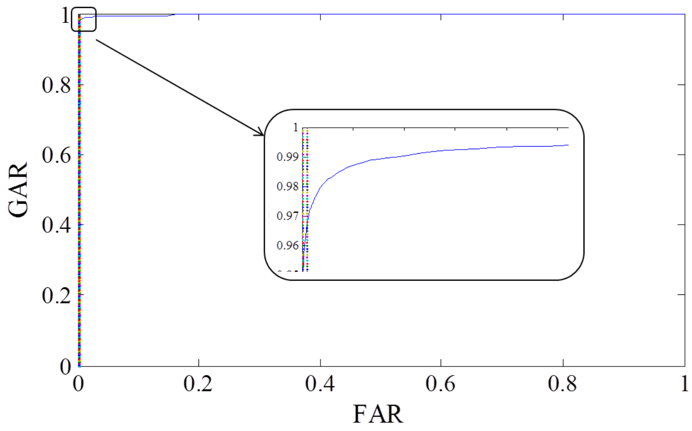


Figure 6.2.: Performance of the One-time BCs.

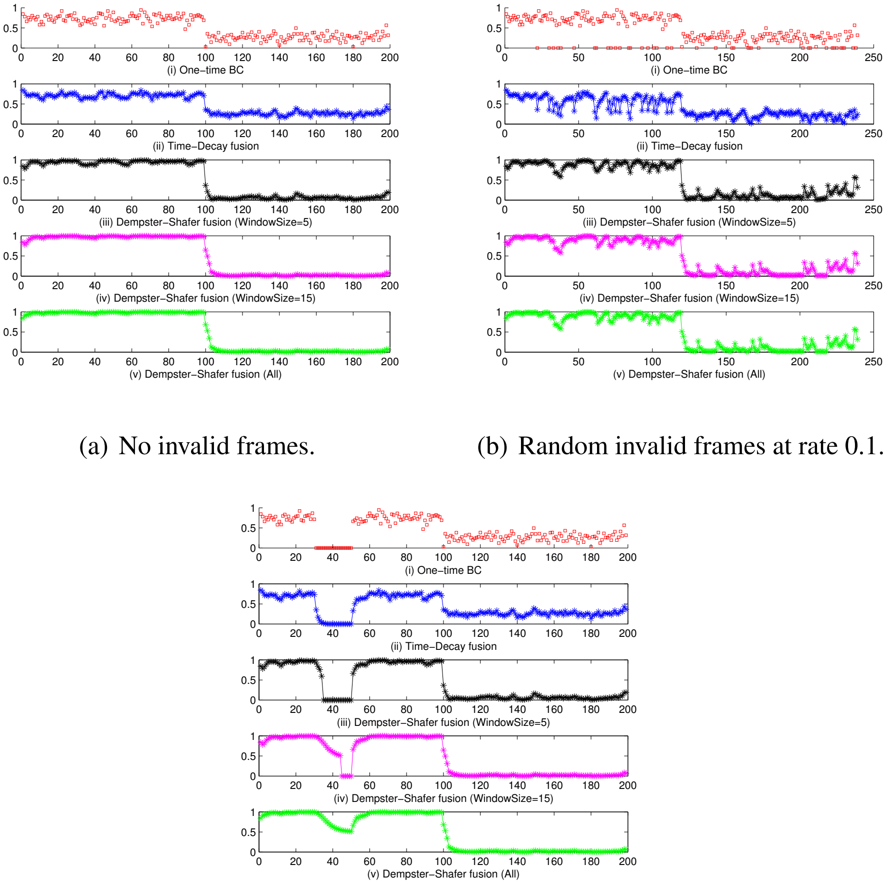
The continuous authentication stage uses one-time BCs to generate confidence score. And identity-bearing of one-time BCs is important for computing good confidence scores. To test the identity-bearing of one-time BC, we constructed a one-time BC using the long-term RS (as shown in Figure 4.2 (a)) and short-term RS (as shown in Figure 4.2 (b)) for each image from the right set of the ICE database, and cross-matched them. The ROC curve for one-time BC matching is shown in Figure 6.2. The EER (i.e., equal error rate when FAR equals to FRR) of the system is 1.20%, and the authentication accuracy is around 98.80%. Moreover, instead of using the same short-term RS (as the experiment setting), each user's one-time BC generation actually is using a different short-term RS (since each user has different RS seed), which will gives better one-time BC performance.

6.4 Analysis of Fusion Methods for Continuous Authentication

To simulate the experiment setting of continuous sampling of biometrics, we used right ICE set as the basis to generate synthetic data. For each user from ICE we selected one iris image and randomly introduced noise into this image to generate a set of synthetic iris images. There are 124 users from ICE, and for each user 100 synthetic iris images are generated. The inter-class and intra-class similarity of BCs derived from those synthetic images have the similar distribution compared to that of the ICE. We divided 124 users into two sets: one contains 50 legitimate users, and the other contains 74 illegitimate users. To evaluate the performance of the continuous authentication, we created 50×74 sessions. And each session is opened by a legitimate user and taken over by an illegitimate user. Three cases are considered in the experiments: 1) ideally all the biometric data are acquired at fix sampling time; 2) at a certain rate (e.g., 0.1) users fail to provide biometric data and invalid frames are randomly distributed; and 3) legitimate users fail to provide biometric data for a time period. Other scenarios can be trivial, for instance, the intruder intentionally does not provide biometrics, which is same to the situation that the legitimate user does the same thing. Figure 6.3 shows the confidence scores of different fusion approaches for one randomly selected session. For Time-Decay fusion, decay rate $r = 0.2$ and weight $w = 0.5$ are used. For Dempster-Shafer fusion, $SCORE_{no} = NonSCORE_{no} = 0.2$ and $p = 0.8$ are used.

Case 1). To construct this session, 100 frames of a legitimate user which are followed by 100 frames of an intruder are injected into the fusion approaches one by one. Figure 6.3(a) shows the confidence scores for the ideal situation. Figure 6.3(a)-(i) shows the similarity scores $SCORE$s of matching of one-time BCs. Figure 6.3(a)-(ii) shows the confidence scores of Time-Decay fusion. Figure 6.3(a)-(iii) to Figure 6.3(a)-(v) show the confidence scores of Dempster-Shafer fusion with different window size. The one-time BC and Time-Decay fusion shows the most fluctuation.

Case 2). To construct this session, 100 frames of a legitimate user which are followed by 100 frames of an intruder are injected into the fusion approaches one by one. And at a certain rate (i.e., 0.1) invalid frames are randomly injected into the session. Given rate = 0.1, that is, the legitimate user provides 110 frames with 10 of them are invalid (because of “lacks of quality biometric observations issue) and the same for the intruder. Figure 6.3(b) shows the results. Without fusion approaches, using only one-time BC, the system can

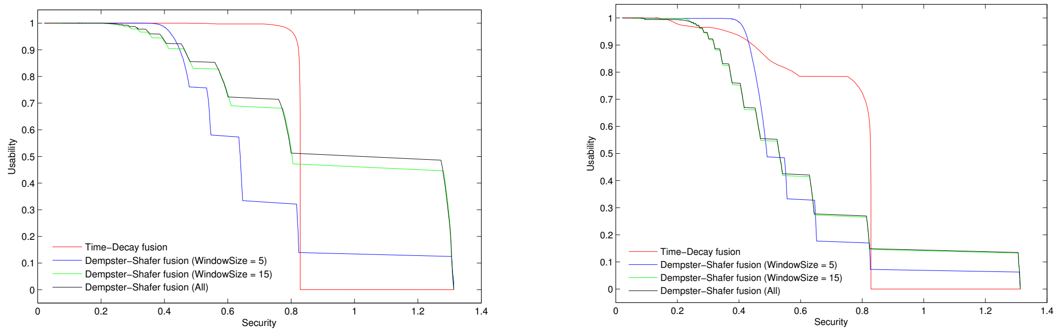


(a) No invalid frames.

(b) Random invalid frames at rate 0.1.

(c) Continuous invalid frames.

Figure 6.3.: Confidence scores of a legitimate + impostor session.



(a) Ideal situation.

(b) Invalid frame rate = 0.1.

Figure 6.4.: Usability-Security Characteristic Curve (USC).

reject all those frames, thus a higher false rejection can be predicted. Using the fusion, the confidence scores will not show dramatic decrease even though no biometric observations are provided at given time points. Compared to Dempster-Shafer fusion, the Time-Decay fusion shows more fluctuation.

Case 3). To construct this session, 100 frames of a legitimate user which are followed by 100 frames of an intruder are injected into the fusion approaches one by one. And then at a given time, a number of invalid frames (i.e., 20) are injected into the genuine session continuously. As time elapses, the Time-Decay fusion presents a quicker decrease of the confidence score (Figure 6.3(c)-(ii)), while the Dempster-Shafer fusion presents a smoother decrease at first (Figure 6.3(c)-(iii) to Figure 6.3(c)-(v)). It is worth mentioning that by changing the decay rate r of Time-Decay and $SCORE_{no}(NonSCORE_{no})$ and p for Dempster-Shafer the decrease can be adjusted. And it shows that the Dempster-Shafer (All) turns to give a smooth curve and not decrease any more when more invalid frames are injected (as shown in Figure 6.3(c)-(v)). However, considering a given window size W, after $W-1$ invalid frames are injected, the confidence score dramatically decreases to zero when the Wth frame is injected (as shown in Figure 6.3(c)-(iii) and Figure 6.3(c)-(iv)).

And in all these three cases, compared to the Time-Decay fusion the Dempster-Shafer fusion computes confidence scores which show more distinctiveness between the genuine session and the impostor session.

The goal of the continuous authentication is to provide system security (e.g., detect the intrusion as soon as possible) while maintain a certain usability for the legitimate user. Figure 6.4 is a plot of *Usability* versus the *Security* of the different fusion approaches for various threshold θ. The results were coming from the average of 50×74 sessions. Intuitively, for the lower security, the system can allow a longer time period that the user provides no biometric observations or slower that the intruder is detected, which indicates higher usability. Figure 6.4(a) gives the USCs of various fusion approaches under ideal situation, that is, all frames are valid. Under this situation, when security is lower (e.g., < 0.4) the usability of Time-Decay fusion and Dempster-Shafer fusion (WindowSize=5) are better, which is close to 1. When security is higher (e.g., > 0.9), the Dempster-Shafer fusion provides better usability compared to the Time-Decay fusion. And the bigger the WindowSize of the Dempster-Shafer fusion, the higher the usability is. The ideal situation is hard to achieve, thus we also simulated the situation that at a given rate (i.e., 0.1) the user fails to provide quality biometric observations. The results are shown in Figure 6.4(b). Under this situation, with lower security requirement (e.g., < 0.45), the usability of Dempster-Shafer fusion (WindowSize=5) provides highest usability, while with higher security requirement (e.g., > 0.9), the usability of Dempster-Shafer fusion provides also higher usability compared to the Time-Decay fusion. And for medium security, the Time-Decay fusion outperforms others.

Table 6.1 and Table 6.2 summarize the FCR given usability = 0.9, usability = 0.95 and usability = 0.99. The tables show that the Dempster-Shafer (WindowSize =5) can detect intrusion more quickly given certain usability. Generally higher security is obtained at the expense of less usability. The results in Figure 6.4, Table 6.1 and Table 6.2 can help determine the trade-off between usability and security.

Table 6.1: Summary of FCR (ideal).

Approach	FCR (Usability=0.9)	FCR (Usability = 0.95)	FCR (Usability=0.99)
Time-Decay	1-3	1-4	1-5
Dempster-Shafer (WindowSize =5)	1-4	1-5	1-5
Dempster-Shafer (WindowSize =15)	1-5	1-6	1-13
Dempster-Shafer (All)	1-5	1-6	1-13

Table 6.2: Summary of FCR (Non-ideal).

Approach	FCR (Usability=0.9)	FCR (Usability = 0.95)	FCR (Usability=0.99)
Time-Decay	1-19	1-22	1-95
Dempster-Shafer (WindowSize =5)	1-5	1-6	1-7
Dempster-Shafer (WindowSize =15)	1-13	1-14	1-14
Dempster-Shafer (All)	1-3	1-14	1-14

Sample Rate. For continuous authentication, it is important to decide the sample rate: how frequent it is to sample the biometrics. The sample rate is closely related to the security and system performance. It is evident that more frequent sampling will provide higher security also higher processing overhead. For instance, the preprocessing including the segmentation of iris images can take time ranging from 0.2 to 0.4s, and the one-time BC generation can take time ranging from 0.1 to 0.2s (Note: results are obtained through experiments implemented using MatLab 2010 on a laptop with Dual-Core CPU 2.10 GHz and 4GB RAM.). Generally the sampling rate cannot exceed the processing rate (i.e., BC generation rate, and commonly they are in the same pace), that is, around 2 BCs per second. However, it is also possible that the system samples the user biometrics more frequently and according to the quality of the biometrics within a time window selects the best quality image and generate one-time BC towards to this image.

7 COMPARISON WITH EXISTING WORKS

7.1 Comparison of BC with Typical BCS and CB

This section compares the BC scheme with typical existing BCS and CB approaches in terms of both security and accuracy. From the security aspect, spoofing and replay attacks are not considered, and there are other technologies (e.g. liveness detection) to defeat such attacks. Here, we mainly consider the potential attacks against BCS and CB identified by [4]. These attacks include but not limited to attacks on error correction codes of fuzzy commitment, attacks via record multiplicity on shielding function, and so on. Table 7.1 summarizes different security/attack parameters mentioned by [4] and the security capability of typical BCS and CB approaches as well as the BC mechanism.

Table 7.1: Key approaches security summary.

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

For the BC mechanism, there are following analysis:

- **Substitution attack**: this is a typical attack on biometric salting when attacker obtains secret transform parameters or secret keys [4]. In such an attack, the attacker alters the contents of a biometric record with or without knowing the biometric data [46]. 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.

- **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 [4]. 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.
- **Brute force attack**: Some BCS approaches suffer from brute force attacks when the generated keys are short [4]. According to our property analysis in Subsection 4.2.2, BC provides quite large search space, and the brute force attack against BC is difficult.
- **Attacks on error correction code**: improper utilization of error correction codes in fuzzy commitment schemes could be security and privacy vulnerable according to existing studies [4, 98–100], however such attack is not applicable to the BC mechanism.
- **Attacks on chaff points**: the security of a fuzzy vault highly relies on the methodology of generating chaff points [4, 101], but such an attack is not applicable to the BC mechanism.
- **False acceptance attacks**: the performance of some BCS and CB, as compared to conventional biometric systems, is decreased [4]. In particular, some biometric salting in the event of a lost token, suffers from this false acceptance attack [4]. Our experimental results show that the BC approach does not have much degradation on system performance, thus the BC approach is less vulnerable to it.
- **Attack via record multiplicity (Collusion attack)**: the vulnerability of the secure sketches and fuzzy extractors in the case that an impostor is in possession of multiple invocations of the same secret was noted by many researches [102]. Fuzzy vault and fuzzy commitment, as two concrete implementations using fuzzy extractors, suffer from this collusion attack. Moreover, if the attacker has the knowledge of the secret, the template can be recovered [46]. 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 above, is reduced to solving an undetermined equation system. There are no determined solution to such a system. Even if the attacker knows the secret, such an attack, in our system, is reduced to solving an interval linear equation system; solving an interval linear equation system is NP-hard [86].

- **Cross-matching (linkability) attack**: it is demonstrated that any quantization approach suffers from this cross-matching attack [4, 92], thus infringes user privacy. Our security proof and experimental results justify that the cross-matching in the BC mechanism is hardly feasible.
- **Internal collusion attack**: insiders collect their BCs generated using the same system secret (RS) and try to obtain the secret [4]. Considering the fact that such an attack requires the attackers (insiders of the system) to share their biometrics (and they may reluctantly do so [4]), this type of attack could be rare. Regardless, such an attack is reduced to solving an interval linear equation system; solving an interval linear equation system is NP-hard [86].
- **"Lost-token"**: some approaches exhibit high vulnerabilities when attackers are in possession of secret tokens [4, 53]. 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. In the following, we will compare the BC approach to existing typical approaches in terms of EER (equal error rate), FAR (false acceptance rate), FRR (false rejection rate) and other factors related to system performance.

Table 7.2: Key approaches performance summary.

Authors	Category	Performance(%)	Remarks
Hao *et al.* [90]	Fuzzy commitment	0.47 FRR/0 FAR	ideal images; 44 bit security
Rathgeb *et al.* [12]	Fuzzy commitment	4.92 FRR	training; CASIAv3
Wu *et al.* [103]	Fuzzy vault	5.56 FRR/0 FAR	training; partial images from CASIAv1.0
Rathgeb *et al.* [15]	Quantization	4.91 FRR	5 enroll samples; CASIAv3
Hammerle *et al.* [104]	Cancelable	1.3 EER	CASIAv3
Ouda *et al.* [105]	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

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 7.2 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 [106] databases. As a typical fuzzy commitment approach, Hao *et al.*'s scheme [90] presents an impressive FRR result. However, according to Bringer *et al.* [107], 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% of FRR with 0.80% of FAR). And its 44 bits operation security is not adequate in current cryptographic applications. Another fuzzy commitment scheme proposed by Rathgeb *et al.* [12] obtains a 4.92% FRR for CASIAv3 database using training. The BC approach does not use training, and on the entire ICE set gives a 0.94% EER, and 4.12% 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% EER, 0.96% FRR when FAR is 10^{-5}, and 1.58% FRR when FAR is set to 0. According to Bringer *et al.* [107] there is a theoretical limit for the systems using classic error correction codes on achievable optimal FRR for ICE, which is FRR 2.49% for key length 42, 4.87% for key length 80 and 9.1% 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 Subsection 4.2.2. 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 user's 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.* [103]. It uses CASIAv1.0 and chooses 3 good quality images out of 7 for each subject, uses 2 images for each subject for training, and the other one for test, and obtains 5.56% FRR. Reddy [108] proposed a hardened fuzzy vault scheme applied on CASIAv1.0 and obtained 9.6 FRR. Rathgeb [15] proposed a quantization approach to generate keys, and obtained 4.91% FRR for CASIAv3. It considered that every subject would provide 5 enroll samples to obtain the quantization parameters, for some situations acquiring multiple samples could be not practical. The proposed BC mechanism does not need training and does not require multiple enrollment samples.

Hammerle [104] and Odua [105] developed cancelable biometrics for iris, and they used CASIAv3 database and obtained 1.3% and 2.31% 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, which has the same image quality as CASIAv3, and our EER result is 0.61%. 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 [109] (e.g., combining iris and face) and hybrid methods (e.g., [25] using user biometrics and additional PIN, [110] 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.

7.2 Comparison of BC Based Active Authentication with Existing Works

Table 7.3: Active authentication summary.

Approach	Technique	Pre-registration	Training	Cost	Security and Privacy	Performance Metrics
Sim [61]	face, fingerprint	Yes	Yes	Mouse (fingerprint)	N	Time to correct reject Usability, etc
Niinuma [59]	Soft face, clothing	No	Yes	common camera	N	FAR/FRR
Monrose [68]	keystroke	Yes	Yes	standard keyboard	N	stokes to reject
Niinuma [62]	face, body	No	Yes	common camera	N	FAR/FRR, no results reported
Altinok [60]	face, voice, fingerprint	Yes	Yes	camera, recorder sensor for fingerprint	N	FAR/FRR
Chowdhury [71]	cognitive	Yes	N/A	health-care sensors	N	N/A
Kurkovsky [72]	RFID	Yes	No	RFID equipments	N	N/A
Ours	Iris	Yes	No	NIR camera	Y	SC, Usability frame to reject

Table 7.3 is giving a summary on typical active authentication approaches. According to the technique used, we category existing approaches into biometrics-based active authentication (what you are) and possession-based active authentication (what you have). The choice of techniques is related to its cost. Biometrics based active authentication can also be fine-tuned into physiological biometrics based active authentication, behavioral biometrics based active authentication, or cognitive biometrics based active authentication. It is worthy to mention that not every biometrics is suitable for active authentication. It has to be either continuous in its manner, e.g. typing, mouse movement, brain activity, or can be efficiently measured continuously, e.g. fingerprint (with special mouse), face or eye scan. Similarly, it is true for the possession-based active authentication. Existing physiological biometrics based active authentication usually uses face, fingerprint [111], while behavior biometrics based active authentication uses keystrokes, mouse movement [38, 56].

We can also categorize the techniques into pre-registration required or pre-registration free active authentication. The pre-registration required active authentication asks for information about user credentials (mainly biometrics) ahead for the continuous authentication, while the pre-registration free active authentication registers user credentials at the initial log-in stage. For pre-registration free active authentication a common attack is log-in credential lost attack. Such system usually uses passwords or other credentials artificially bound to a user. If the credential is lost, the system cannot detect the intruder. Training is an important consideration for such systems also. The cost of the active authentication systems also varies, and some of the systems require specific requirements, e.g., mouse, RFID reader. Right now, there is hardly a common set of metrics for active authentication, thus from this aspect it is hard to make comparisons. We also list the metrics for system performance evaluation in various systems. And an important factor is the system security and user privacy. Current approaches mainly focus on system performance, yet we also consider the security of the system and privacy of users.

The proposed system can work various biometrics for active authentication providing both system security and user privacy. The iris biometrics is used as a case study here. Iris works with near infrared light, so an NIR camera is required. The proposed approach does not need training. And we proposed useful metrics considering timing information: SC, etc. Our experimental results show security and usability trade-off.

8 CONCLUSIONS AND FUTURE WORK

We will continue to study the proposed BC authentication system. Our future work includes but not limits to:

- Investigate the interoperability of the BC mechanism: the architecture (Figure 8.1) consists of: multiple servers, each with a different reference subject. A user can enroll at one server and be verified at a server rather than the server the user enrolled. The verification will be conducted via multiple servers by BC composition.

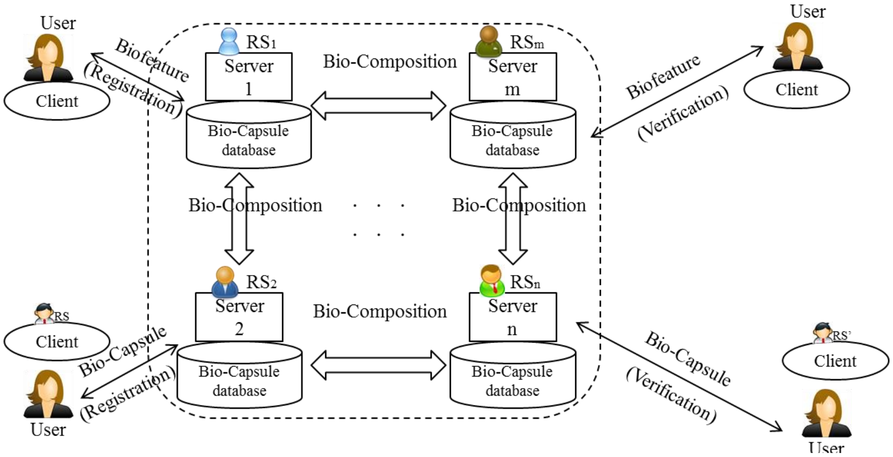


Figure 8.1.: The interoperability of the BC mechanism.

- Extend the system to other biometrics, e.g., face, fingerprints.

In this research, 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 unlinkability experiment proves the interoperatability of the BC system, and it supports “one-click sign on” across multiple systems by using a distinct RS on each system without infringing user privacy; 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. In addition, the BC can be naturally applied in continuous authentication to achieve a secure and privacy-preserving biometrics based active authentication system. We use fusion approaches to tackle the “lacks of quality biometric observation” issue. We also identify potential attacks for biometrics based active authentication and propose an effective mechanism to defeat them. Upon utilizing the biometrics, the system preserves user biometric privacy. Our simulation results show the effectiveness of the active authentication system and also provide a good evidence for selecting trade-off between security and usability. These features make the proposed BC mechanism a user-centric authentication approach.

LIST OF REFERENCES

LIST OF REFERENCES

[1] A. Ciaramella, P. D'Arco, A. De Santis, C. Galdi, and R. Tagliaferri. Neural network techniques for proactive password checking. *IEEE Transactions on Dependable and Secure Computing*, 3(4):327–339, October–December 2006.

[2] P. D'Arco, and A. De Santis. On ultralightweight RFID authentication protocols. *IEEE Transactions on Dependable and Secure Computing*, 8(4):548–563, July–August 2011.

[3] A. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP Journal on Advances in Signal Processing*, 2008(113):1–17, 2008.

[4] C. Rathgeb, and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, 2011(1):3, 2011.

[5] A. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. *IEEE Transaction on Circuits and Systems for Video Technology*, 14(1):4–20, 2004.

[6] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni. Fingerprint image reconstruction from standard templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(9):1489–1503, September 2007.

[7] A. Ross, J. Shah, and A. Jain. From template to image: Reconstructing fingerprints from minutiae points. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):544 –560, April 2007.

[8] J. Galballya, A. Rossb, M. Gomez-Barreroa, J. Fierreza, and J. Ortega-Garciaa. From the iriscode to the iris: A new vulnerability of iris recognition systems. *Black Hat USA 2012*, 2012.

[9] A. Juels, and M. Sudan. A fuzzy vault scheme. *Designs, Codes and Cryptography*, 38(2):237–257, 2006.

[10] K. Nandakumar, A. Jain, and S. Pankanti. Fingerprint-based fuzzy vault: Implementation and performance. *IEEE Transactions on Information Forensics and Security*, 2(4):744–757, December 2007.

[11] L. Zhang, Z. Sun, T. Tan, and S. Hu. Robust biometric key extraction based on iris cryptosystem. In *Proceedings of the 3rd International Conference on Advances in Biometrics*, pages 1060–1069, 2009.

[12] C. Rathgeb, and A. Uhl. Adaptive fuzzy commitment scheme based on iris-code error analysis. In *2nd European Workshop on Visual Information Processing*, pages 41–44, July 2010.

[13] A. Juels, and M. Wattenberg. A fuzzy commitment scheme. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pages 28–36, 1999.

[14] C. Rathgeb, and A. Uhl. An iris-based interval-mapping scheme for biometric key generation. In *Proceedings of 6th International Symposium on Image and Signal Processing and Analysis*, pages 511–516, September 2009.

[15] C. Rathgeb, and A. Uhl. Privacy preserving key generation for iris biometrics. In *Proceedings of the 11th International conference on Communications and Multimedia Security*, pages 191–200, 2010.

[16] Y. Sui, K. Yang, Y. Du, S. Orr, and X. Zou. A novel key management scheme using biometrics. In *Proceedings of Mobile Multimedia/Image Processing, Security, and Applications 2010 conference*, page 77080C, 2010.

[17] N. Ratha, J. Connell, and R. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634, 2001.

[18] J. Pillai, V. Patel, R. Chellappa, and N. Ratha. Secure and robust iris recognition using random projections and sparse representations. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 33(9):1877–1893, September 2011.

[19] T. Boult. Robust distance measures for face-recognition supporting revocable biometric tokens. In *7th International Conference on Automatic Face and Gesture Recognition*, pages 560–566, April 2006.

[20] T. Boult, W. Scheirer, and R. Woodworth. Revocable fingerprint biotokens: Accuracy and security analysis. In *IEEE Conference on Computer Vision and Pattern Recognition*, pages 1–8, June 2007.

[21] O. Ouda, N. Tsumura, and T. Nakaguchi. BioEncoding: A reliable tokenless cancelable biometrics scheme for protecting IrisCodes. *IEICE Transactions on Information and Systems*, E93-D(7):1878–1888, July 2010.

[22] A. Cavoukian, and A. Stoianov. Biometric encryption. *Encyclopedia of Biometrics Springer*, 2009.

[23] E. Verbitskiy, P. Tuyls, C. Obi, B. Schoenmakers, and B. Skoric. Key extraction from general nondiscrete signals. *IEEE Transactions on Information Forensics and Security*, 5(2):269–279, June 2010.

[24] F. Monrose, M. Reiter, Q. Li, and S. Wetzel. Cryptographic key generation from voice. In *2001 IEEE Symposium on Security and Privacy*, pages 202–213, 2001.

[25] F. Monrose, M. Reiter, and S. Wetzel. Password hardening based on keystroke dynamics. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pages 73–82, 1999.

[26] I. Traore, and A. Ahmed. *Continuous Authentication Using Biometrics: Data, Models, and Metrics*. IGI Publishing, Hershey, PA, USA, 1st edition, 2011.

[27] Y. Sutcu, Q. Li, and N. Memon. Protecting biometric templates with sketch: Theory and practice. *IEEE Transactions on Information Forensics and Security*, 2(3):503–512, 2007.

[28] A.K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP Journal on Advances in Signal Processing*, 2008(113):1–17, January 2008.

[29] U. Uludag, S. Pankanti, S. Prabhakar, and A. Jain. Biometric cryptosystems: Issues and challenges. *Proceedings of the IEEE*, 92(6):948–960, June 2004.

[30] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis. Constructing practical fuzzy extractors using QIM. In *Technical Report TR-CTIT-07-52*, CTIT technical report series. University of Twente, CTIT, 2007.

[31] T. Ignatenko, and F.M.J. Willems. Information leakage in fuzzy commitment schemes. *IEEE Transactions on Information Forensics and Security*, 5(2):337–348, June 2010.

[32] Y. Sui, X. Zou, and E. Du. Biometrics-based authentication: A new approach. In *2011 Proceedings of 20th International Conference on Computer Communications and Networks*, August 2011.

[33] H.G. Miller, and J.L. Fisher. Requiring strong credentials: What's taking so long? *IT Professional*, 12(1):57–60, January–February 2010.

[34] G. Duggan, H. Johnson, and B. Grawemeyer. Rational security: Modelling everyday password use. *International Journal of Human-Computer Studies*, 70(6):415–431, 2012.

[35] Z. Zhou, E. Du, and C. Belcher. Transforming traditional iris recognition systems to work in nonideal situations. *IEEE Transactions on Industrial Electronics*, 56(8):3203–3213, August 2009.

[36] J. Dai, J. Feng, and J. Zhou. Robust and efficient ridge-based palmprint matching. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 34(8):1618–1632, 2011.

[37] Z. Zhou, E. Du, N. Thomas, and E. Delp. A new human identification method: Sclera recognition. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 42(3):571–583, 2012.

[38] A. Ahmed, and I. Traore. A new biometric technology based on mouse dynamics. *IEEE Transactions on Dependable and Secure Computing*, 4(3):165–179, July–September 2007.

[39] J. Zhang, J. Pu, C. Chen, and R. Fleischer. Low-resolution gait recognition. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 40(4):986 – 996, August 2010.

[40] L. Faria, V. Sa, and S. de Magalhaes. Multimodal cognitive biometrics. In *6th Iberian Conference on Information Systems and Technologies*, pages 1–6, June 2011.

[41] K. Revett, and S. de Magalhes. Cognitive biometrics: Challenges for the future. In *Global Security, Safety, and Sustainability, Communications in Computer and Information Science*, pages 79–86. 2010.

[42] K. Revett, F. Deravi, and K. Sirlantzis. Biosignals for user authentication – Towards cognitive biometrics? In *2010 International Conference on Emerging Security Technologies*, pages 71–76, September 2010.

[43] C. Vielhauer, R. Steinmetz, and A. Mayerhoefer. Biometric hash based on statistical features of online signatures. In *Proceedings of the 16th International Conference on Pattern Recognition*, pages 123–126, 2002.

[44] K. Simoens, P. Tuyls, and B. Preneel. Privacy weaknesses in biometric sketches. In *30th IEEE Symposium on Security and Privacy, 2009*, pages 188–203, May 2009.

[45] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM Journal on Computing*, 38(1):97–139, 2008.

[46] W. Scheirer, and T. Boult. Cracking fuzzy vaults and biometric encryption. In *Biometrics Symposium*, pages 1–6, September 2007.

[47] E. Kelkboom, J. Breebaart, T. Kevenaar, I. Buhan, and R. Veldhuis. Preventing the decodability attack based cross-matching in a fuzzy commitment scheme. *IEEE Transactions on Information Forensics and Security*, 6(1):107–121, March 2011.

[48] A. Jin, D. Ling, and A. Goh. Biohashing: Two factor authentication featuring fingerprint data and tokenized random number. *Elsevier Pattern Recognition*, 37(11):2245–2255, 2004.

[49] C. Chin, A. Jin, and D. Ling. High security iris verification system based on random secret integration. *Computer Vision and Image Understanding*, 102(2):169–177, May 2006.

[50] K. Cheung, A. Kong, D. Zhang, M. Kamel, J. You, and H. Lam. An analysis on accuracy of cancelable biometrics based on biohashing. In *Proceedings of the 9th International Conference on Knowledge-Based Intelligent Information and Engineering Systems*, pages 1168–1172, 2005.

[51] K. Cheung, A. Kong, D. Zhang, M. Kamel, and J. You. Revealing the secret of facehashing. In *Proceedings of the 2006 International Conference on Advances in Biometrics*, pages 106–112, 2006.

[52] K. Nandakumar, A. Nagar, and A. Jain. Hardening fingerprint fuzzy vault using password. In *Proceeding of 2nd International Conference on Biometrics*, pages 927–937, August 2007.

[53] A. Kong, K. Cheung, D. Zhang, M. Kamel, and J. You. An analysis of biohashing and its variants. *Pattern Recognition*, 39(7):1359–1368, July 2006.

[54] A. Ross, and A. Othman. Visual cryptography for biometric privacy. *IEEE Transactions on Information Forensics and Security*, 6(1):70 –81, March 2011.

[55] A. Othman, and A. Ross. Mixing fingerprints for generating virtual identities. In *2011 IEEE International Workshop on Information Forensics and Security*, pages 1–6, December 2011.

[56] D. Gunetti, and C. Picardi. Keystroke analysis of free text. *ACM Transactions on Information and System Security*, 8(3):312–347, August 2005.

[57] P. Dowland, H. Singh, and S. Furnell. A preliminary investigation of user authentication using continuous keystroke analysis. In *Proceedings of the 8th IFIP Annual Working Conference on Information Security Management and Small System Security*, 2001.

[58] M. Pusara, and C. Brodley. User re-authentication via mouse movements. In *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, pages 1–8, 2004.

[59] K. Niinuma, U. Park, and A.K. Jain. Soft biometric traits for continuous user authentication. *IEEE Transactions on Information Forensics and Security*, 5(4):771 –780, December 2010.

[60] A. Alphan, and T. Matthew. Temporal integration for continuous multimodal biometrics. In *Multimodal User Authentication*, pages 11–12, 2003.

[61] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar. Continuous verification using multimodal biometrics. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):687 –700, April 2007.

[62] K. Niinuma, and A.K. Jain. Continuous user authentication using temporal information. In *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, page 76670L, April 2010.

[63] Q. Xiao, and Xue D. A facial presence monitoring system for information security. In *IEEE Workshop on Computational Intelligence in Biometrics: Theory, Algorithms, and Applications.*, pages 69–76, April 2009.

[64] A. Azzini, S. Marrara, R. Sassi, and F. Scotti. A fuzzy approach to multimodal biometric continuous authentication. *Fuzzy Optimization and Decision Making*, 7(3):243–256, September 2008.

[65] I. G. Damousis, D. Tzovaras, and E. Bekiaris. Unobtrusive multimodal biometric authentication: the humabio project concept. *EURASIP Journal on Advances in Signal Processing*, 2008(110):1–11, January 2008.

[66] A. Azzini, and S. Marrara. Impostor users discovery using a multimodal biometric continuous authentication fuzzy system. In *Proceedings of the 12th International Conference on Knowledge-Based Intelligent Information and Engineering Systems*, pages 371–378, 2008.

[67] H. Kang, and M. Ju. Multi-modal feature integration for secure authentication. In *Proceedings of the 2006 International Conference on Intelligent Computing*, pages 1191–1200, 2006.

[68] F. Monrose, and A. Rubin. Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems - Special Issue on Security on the Web*, 16(4):351–359, February 2000.

[69] I. Brosso, A. La Neve, G. Bressan, and W. Vicente Ruggiero. A continuous authentication system based on user behavior analysis. In *International Conference on Availability, Reliability and Security*, pages 380–385, February 2010.

[70] A. Ahmed, and I. Traore. Dynamic sample size detection in continuous authentication using sequential sampling. In *Proceedings of the 27th Annual Computer Security Applications Conference*, pages 169–176, 2011.

[71] M.A. Chowdhury, J. Light, and W. McIver. A framework for continuous authentication in ubiquitous environments. In *2010 6th International Conference on Wireless Communication and Sensor Networks*, pages 1–6, December 2010.

[72] S. Kurkovsky, E. Syta, and B. Casano. Continuous RFID-enabled authentication and its privacy implications. In *2010 IEEE International Symposium on Technology and Society*, pages 103–110, June 2010.

[73] S. Kurkovsky, and E. Syta. Approaches and issues in location-aware continuous authentication. In *Proceedings of the 2010 13th IEEE International Conference on Computational Science and Engineering*, pages 279–283, 2010.

[74] S. Bu, F. Yu, X. Liu, and H. Tang. Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks. *IEEE Transactions on Wireless Communications*, 10(9):3064–3073, September 2011.

[75] J. Liu, F. Yu, C. Lung, and H. Tang. Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks. *IEEE Transactions on Wireless Communications*, 8(2):806–815, February 2009.

[76] S.T.V. Parthasaradhi, R. Derakhshani, L.A. Hornak, and S.A.C. Schuckers. Time-series detection of perspiration as a liveness test in fingerprint devices. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, 35(3):335–343, August 2005.

[77] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni. Fake finger detection by skin distortion analysis. *IEEE Transactions on Information Forensics and Security*, 1(3):360–373, September 2006.

[78] E. C. Lee, K. R. Park, and J. Kim. Fake iris detection by using purkinje image. In *Proceedings of the 2006 International Conference on Advances in Biometrics*, pages 397–403, 2006.

[79] K. Takahashi, and T. Murakami. A metric of information gained through biometric systems. In *Proceedings of the 2010 20th International Conference on Pattern Recognition*, pages 1184–1187, 2010.

[80] http://en.wikipedia.org/wiki/usability.

[81] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, pages 553–567, 2012.

[82] Y. Du, R. Ives, D. Etter, and T. Welch. Use of one-dimensional iris signatures to rank iris pattern similarities. *Optical Engineering*, 45(3):037201, 2006.

[83] http://iris.nist/gov/ice/.

[84] L. Masek. Recognition of human iris patterns for biometric identification. Technical report, University of Western Australia, 2003.

[85] J. Daugman. How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):21–30, January 2004.

[86] P. Kahl. Solving narrow-interval linear equation systems is NP-hard. Digitalcommons@UTEP – University of Texas at El Paso. `http://digitalcommons.utep.edu/cgi/oai2.cgi`, 1996.

[87] H. Proena, and L. A. Alexandre. University of beira interior UBIRIS: A noisy iris image database. In *13th International Conference on Image Analysis and Processing*, pages 970–977, 2005.

[88] H. Jung, K. Park, and J. Kim. Depth of capture volume extension by constrained least square-based image restoration, quantitative evaluation. citeseerx - scientific literature digital library and search engine. `http://citeseerx.ist.psu.edu/oai2`, 2010.

[89] Y. C. Feng, P. C. Yuen, and A. K. Jain. A hybrid approach for generating secure and discriminating face template. *IEEE Transactions on Information Forensics and Security*, 5(1):103–117, March 2010.

[90] F. Hao, R. Anderson, and J. Daugman. Combining crypto with biometrics effectively. *IEEE Transactions on Computers*, 55(9):1081–1088, 2006.

[91] J. Gallier. *Discrete Mathematics*. Universitext Series. Springer, 2011.

[92] 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. In *Proceedings of the 4th International Workshop, DPM2009 and 2nd International Workshop, SETOP 2009 on Data Privacy Management and Autonomous Spontaneous Security*, pages 78–92. 2010.

[93] Y. Sui, X. Zou, F. Li, and E. Du. Active user authentication for mobile devices. In *7th International Conference on Wireless Algorithms, Systems, and Applications*, pages 540–548, 2012.

[94] Y. Sui, X. Zou, Y. Du, and F. Li. Design and analysis of a highly user-friendly, secure, privacy-preserving, and revocable authentication method. *IEEE Transactions on Computers*, (PrePrints), 2013.

[95] Shafer G. A mathematical theory of evidence. *Princeton University Press*, 1976.

[96] N.D. Kalka, J. Zuo, N.A. Schmid, and B. Cukic. Image quality assessment for iris biometric. In *Proceedings of SPIE 6202, Biometric Technology for Human Identification III*, page 62020D, 2006.

[97] R.R. Murphy. Dempster-Shafer theory for sensor fusion in autonomous mobile robots. *IEEE Transactions on Robotics and Automation*, 14(2):197–206, April 1998.

[98] D. Karakoyunlu, and B. Sunar. Differential template attacks on PUF enabled cryptographic devices. In *IEEE International Workshop on Information Forensics and Security*, pages 1–6, December 2010.

[99] A. Adler. Vulnerabilities in biometric encryption systems. In *Proceedings of the 5th International Conference on Audio- and Video-Based Biometric Person Authentication*, pages 1100–1109, 2005.

[100] C. Rathgeb, and A. Uhl. Statistical attack against iris-biometric fuzzy commitment schemes. In *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, pages 23–30, June 2011.

[101] E. Chang, R. Shen, and F. Teo. Finding the original point set hidden among chaff. In *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security*, pages 182–188, 2006.

[102] X. Boyen. Reusable cryptographic fuzzy extractors. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*, pages 82–91, 2004.

[103] X. Wu, N. Qi, K. Wang, and D. Zhang. A novel cryptosystem based on iris key generation. In *4th International Conference on Natural Computation*, pages 53–56, October 2008.

[104] J. Hammerle-Uhl, E. Pschernig, and A. Uhl. Cancelable iris biometrics using block re-mapping and image warping. In *Proceedings of the 12th International Conference on Information Security*, pages 135–142, 2009.

[105] O. Ouda, N. Tsumura, and T. Nakaguchi. Tokenless cancelable biometrics scheme for protecting iris codes. In *20th International Conference on Pattern Recognition*, pages 882–885, August 2010.

[106] CASIA-IrisV1. http://biometrics.idealtest.org/.

[107] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zemor. Theoretical and practical boundaries of binary secure sketches. *IEEE Transactions on Information Forensics and Security*, 3(4):673–683, December 2008.

[108] E. Reddy, and I. Babu. Performance of iris based hard fuzzy vault. In *IEEE 8th International Conference on Computer and Information Technology Workshops*, pages 248–253, July 2008.

[109] A. Ross, K. Nandakumar, and A. Jain. Introduction to multibiometrics. In *Handbook of Biometrics*, pages 271–292. Springer US, 2008.

[110] A. Nagar, K. Nandakumar, and A. Jain. A hybrid biometric cryptosystem for securing fingerprint minutiae templates. *Pattern Recognition Letter*, 31(8):733–741, June 2010.

[111] O. Hamdy, and I. Traore. Cognitive-based biometrics system for static user authentication. In *4th International Conference on Internet Monitoring and Protection*, pages 90–97, May 2009.

VITA

VITA

Yan Sui obtained her bachelor's degree in computer science from Harbin Institute of Technology, China in 2007, and master's degree in computer science from Indiana University – Purdue University Indianapolis in 2009. After that she entered the Ph.D program of Purdue West Lafayette. Her research interests include cyber security, security on mobile devices, and biometric security and privacy.

Publications:

- Y. Sui, X. Zou, Y. Du, and F. Li. Design and Analysis of a highly user-friendly, secure, privacy-preserving, and revocable authentication method. *IEEE Transaction on Computers*, (PrePrints), 2013.

- P. Adusumilli, Y. Sui, X. Zou, B. Ramamurthy, and F. Li. A Key distribution scheme for distributed group with authentication capability. *International Journal of Performability Engineering, Dependability of Wireless Systems and Networks* (in press).

- Y. Sui, X. Zou, and E.Y. Du. Cancellable biometrics (book chapter), Biometrics: From Fiction to Practice, Pan Stanford Publishing, 2012.

- Y. Sui, X. Zou, F. Li and E. Y. Du. Active user authentication for mobile devices. In *7th International Conference on Wireless Algorithms, Systems, and Applications*, pages 540–548, 2012.

- Y. Sui, X. Zou, Y. Du and F. Li. Secure and privacy-preserving biometrics based active authentication. In *2012 IEEE International Conference on Systems, Man, and Cybernetics*, pages 1291–1296, 2012.

- Y. Sui, X. Zou, and E. Du. Biometrics-based authentication: A new approach. In *2011 Proceedings of 20th International Conference on Computer Communications and Networks*, July–August, 2011.

- X. Zou, F. Maino, E. Bertino, Y. Sui, K. Wang, and F. Li. A new approach to weighted multi-secret sharing. In *2011 Proceedings of 20th International Conference on Computer Communications and Networks*, July–August, 2011.

- X. Zou, M. Qi, F. Li, Y. Sui, and K. Wang. A new scheme for anonymous secure group communication. In *44th Hawaii International Conference on System Sciences*, January 2011.

- Y. Sui, K. Yang, Y. Du, S. Orr, and X. Zou. A novel key management scheme using biometrics. In *Proceedings of Mobile Multimedia/Image Processing, Security, and Applications 2010 conference*, 7708(77080C), 2010..

- K. Yang, Y. Sui, Z. Zhou, Y. Du, and X. Zou. A new approach for cancelable iris recognition. In *Proceedings of Mobile Multimedia/Image Processing, Security, and Applications 2010 conference*, 7708(77080C), 2010.

- W. Zhao, Y. Liang, Q. Yu, and Y. Sui. H-WSNMS: A web-based heterogeneous wireless sensor networks management system architecture. In *International Conference on Network-Based Information Systems*, pages 155–162, 2009.

- K. Wang, X. Zou, and Y. Sui. A multiple secret sharing scheme based on matrix projection. In *33rd Annual IEEE International Computer Software and Applications Conference*, pages 400–405, 2009.

- Y. Sui, F. Maino, Y. Guo, K. Wang, and X. Zou. An efficient time-bound access control scheme for dynamic access hierarchy. In *2009 5th International Conference on Mobile Ad-hoc and Sensor Networks*, pages 279–286, 2009.

- K. Wang, Y. Sui, X. Zou, A. Durresi, and S. Fang. Pervasive and trustworthy healthcare. In *22nd International Conference on Advanced Information Networking and Applications – Workshops*, pages 750–755, 2008.