Biometrics-based Authentication: a New Approach

Yan Sui[*], Xukai Zou[*] and Yingzi Du[†‡]
[*]Department of Computer and Information Science
Indiana University Purdue University Indianapolis, Indiana 46202, USA
Email: {ysui, xkzou}@cs.iupui.edu
[†]Department of Electronic and Computer Engineering
Indiana University Purdue University Indianapolis, Indiana 46202, USA
Email: yidu@iupui.edu

***Abstract*—Authentication is a fundamental issue to any trust-oriented computing system and also a critical part in many security protocols. Performing authentication is notoriously difficult. Biometrics has been widely used and adopted as a promising authentication method due to its advantages over some existing methods, particularly, its resistance to losses incurred by theft of passwords and smart cards. However, biometrics introduces its own challenges, such as being irreplaceable once compromised. Moreover, the use of biometrics introduces privacy concern.**

In this paper, we propose a simple yet effective biometrics-based authentication solution. The proposed approach introduces new constructs - Reference Subject and Biometric Capsule, and stores the "difference" (called Biometric Capsule) between the user and the Reference Subject for authentication without revealing a user's original biometric information. This approach supports replaceability and protect users' privacy. Moreover, the proposed approach creates more advantages: (a) *being user-friendly* **without any additional burden on users and possessing** *one-for-all* **power; (b)** *being generic* **enough to be applied to various biometrics (e.g., fingerprint, face, iris) or combinations of them; and (c)** *being adaptive* **in terms of security and privacy to fit different authentication models, application requirements, available resources, and trusted or non-fully-trusted environments. The experimental results on iris validate its performance and prove it a practical mechanism.**

***Index Terms*—biometrics, authentication, replaceability, privacy, Reference Subject, Biometric Capsule, biometric template.**

I. Introduction

Authentication is a critical part of any trustworthy computing system; it ensures that only individuals with verified identities can log on the system or access system resources. In addition, authentication also serves as the first step for many other security purposes, such as key management and secure group communication [3]. Passwords or smartcards have been the most widely used authentication methods due to easy implementation and replacement; however, memorizing a password or carrying a smartcard, or managing multiple passwords/smartcards for different systems (one for each system), is a significant overhead to users. In addition, they are artificially associated with users and cannot truly identify individuals. More seriously, they can be lost or stolen, resulting in impersonation and other security breaches. As a result, biometrics is becoming a promising authentication/identification method because it binds an individual with his identity and overcomes the main shortcomings inherent in the use of passwords and smartcards.

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 (Fig 1). During the enrollment phase, a biometric feature set is extracted from 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 feature set is used to construct a query template. The query template is matched against the stored template(s) for authentication.

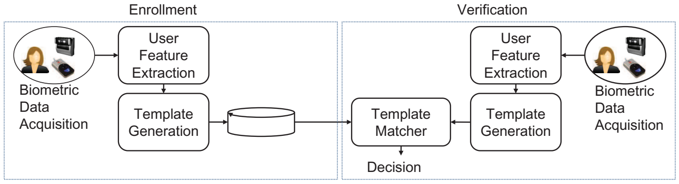


Fig. 1: Conventional biometric authentication

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 bears a user's identity and it is hard to be forged. Unfortunately, biometrics brings its own complications:

- Security concern: conventional biometric authentication system record *biometric templates* in a Central Authentication Entity's (CA's) database. The stored templates, which correlate to users' biometric data, become potential targets to be attacked. Some literature [6], [7] has identified the vulnerabilities caused by the compromise of stored templates.
- Privacy concern: Biometrics identifies individuals. To the best of our knowledge, conventional biometric authentication system is primarily built upon a fully-trusted model; that is, the central authentication entity (CA) is trusted to take full control of users' biometric information and is assumed to not misuse the information. This assumption of trustworthiness about the CA is not sufficient in the

[‡] Corresponding author.

current malicious environments, since handing over one's biometric information to other parties or loss/compromise of one's biometric template will cause serious user privacy concern.

- Irreplaceability: biometric data is permanently bound to a user, and it is almost impossible to generate a new set of biometric features for a legitimate user. Thus compromised biometrics is not replaceable.

Many approaches [9], [5] addressing the security and privacy issues of biometrics have been proposed in the literature. These approaches avoid storage of plain biometric templates by recording them in a "distorted" way.

In this research we propose a privacy-preserving yet replaceable biometrics-based authentication approach. In the proposed approach, neither plain nor distorted biometric templates are stored in CA's database, instead the system stores *decorated* data (what we called *Biometric Capsule*, denoted as *Bio-Capsule* or BC) derived from biometric information of an enrolling user and a *Reference Subject* (RS). From the BC, a user's original information is revealed only to a bare minimum. Moreover, the proposed approach can be applied in different environments: a fully-trust environment in which the CA is allowed to know users' biometric information, a distributed-trust environment in which any party cannot gain full information about a user, as well as a non-trust environment in which user's true biometric information is hidden from the CA. This approach can be adopted to various biometrics, e.g., iris, face, fingerprint, or any combination of them. In summary, aside from the desirable features provided by conventional biometric authentication approaches, the proposed approach has several other attractive features: 1) it is able to defend not only against some attacks from outsiders but also against possible misbehavior or compromise of the CA; 2) user privacy is preserved, and compromised BC can hardly reveal user's true biometric information; 3) unsubscription cost from the system is minimized; 4) it can be applied to various biometrics, e.g. iris, face; even other authentication approaches such as password/smartcard-based ones.

The rest of the paper is organized as follows. Related works are briefly reviewed in Section II. Section III introduces the proposed approach. The approach applied in non-trusted environment is briefly presented in Section IV. Section V applies the approach to practical iris data and presents experimental results. We conclude the paper and highlight some challenging research issues in Section VI.

II. Related Works

Providing secure and replaceable biometrics-based authentication solution by directly applying traditional cryptographic methods to biometrics requires extracting non-changing patterns from biometric data, which is often challenging [6]. Instead some research applies a transformation function to extracted patterns and uses the transformed patterns for authentication. Lee [9] proposed a fuzzy vault system which incorporates fuzzy logic and error correction with local iris features to tolerate the within-class variance. Still, the design of a robust hashing algorithm to better tolerate the within-class variance of biometric templates, while discriminating between-class distance, is very challenging. In [13], Ratha proposed the "cancelable biometrics" method which transforms the original biometric data and creates alternatives for matching. The transformation parameters are determined by external added randomness, such as a user PIN or token. The transformed patterns can be changed (or revoked/reissued) by changing the user PIN or token; as a result, this method achieves "cancelability". They also proposed three types of non-invertible transformation (Cartesian transformation, polar transformations and function transformation) to map the original biometric data to another space and store the transformed template in a database [12]. Takahashi [18], [19] generated a scrambling filter which is applied to the original image to produce a scrambled template to enroll into the database. Similar work was done in [15], for the enrollment stage where Savvides used a random convolution kernel and a randomly generated frequency shuffler to scramble the original images, and synthesize transformed images as an encrypted MACE (minimum average correlation energy) filter as the form in a frequency domain. In [4], Govindaraju proposed a biometric convolution method which transforms the primary biometrics to a new set of features using the one-way mapping function derived from a secondary or tertiary biometrics. Maiorana [11] introduced a set of non-invertible transformations applied to biometrics whose template can be represented by a set of sequences to generate multiple transformed versions of the template.

Some research applies biometric patterns to cryptosystems to generate cryptographic keys and perform authentication as well. Hao [5] proposed a two-factor scheme using coding theory. Other popular approaches are the fuzzy vault scheme proposed by Juels [8], and its implementations. Dodis [1] proposed two primitives: fuzzy extractor which extracts nearly uniformly random keys from biometric input, and secure sketch which produces public helper information without revealing much about the biometric input. Sutcu [16] discussed the practical issues in secure sketch construction and showed the subtleties in evaluating security of practical systems. The application of secure sketch in the design of multi-factor (e.g., biometrics and password) and multi-biometrics (e.g., face and fingerprint) were also investigated [16], [17].

III. Proposed Approach

Before we continue the introduction of the proposed approach, some notations used in the paper are listed as follows:
u: a user to be authenticated.
RS: a Reference Subject.
u_D: biometric data or patterns of user u.
u_F: biometric feature set of user u.
u_{BC}: Biometric Capsule (or Bio-Capsule or BC) of user u.
u_{ID}: user u's identity, e.g., name, id.

A. Principle

The conventional biometric authentication collects biometric data from an enrolling user and extracts a biometric feature set from the biometric data; from the feature set a template is generated (as shown in Fig 1). Different from conventional biometric authentication approaches, during the enrollment phase, the proposed approach selects *a reference feature set* (or extract *a reference feature set* from a Reference Subject) and computes the *difference* between the user's feature set and the reference feature set, then from the *difference* generates a *Bio-Capsule* to uniquely represent the enrolling user (as shown in Fig 2). In the verification phase, a query biometric feature set from a user and the same reference feature set are used to generate a query Bio-Capsule which is compared against the registered Bio-Capsule. If the registered Bio-Capsule and the query Bio-Capsule are within a certain distance, the user is successfully authenticated (Fig 2).

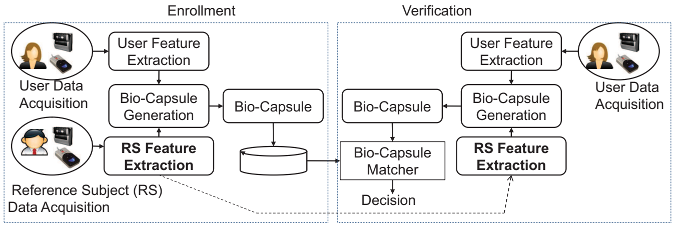


Fig. 2: Proposed Reference Subject feature-based authentication

Assume user feature $f = (f_1, \cdots, f_m)$ and reference feature $g = (g_1, \cdots, g_m)$ are given. To generate a Bio-Capsule for a user, we design the following three possible measurements for computing feature difference.

- Absolute-Value-Comparison (AVC): this is to compare two features f, g by direct value comparison.

$$c(f(i), g(i)) = \begin{cases} 0 & \text{if } |f(i) - g(i)| \le Th \\ -1 & \text{if } f(i) < g(i) - Th \\ 1 & \text{if } f(i) > g(i) + Th \end{cases} \quad (1)$$

  where Th is a pre-selected threshold, $1 \le i \le m$.
- Relative-Value-Comparison (RVC): the difference is formulated by

$$\begin{aligned} & c(f(i), g(i)) = a, \\ \text{if } & \frac{2a-1}{2} Th < \frac{f(i) - g(i)}{avg(f(i), g(i))} \le \frac{2a+1}{2} Th, \end{aligned} \quad (2)$$

  where $a \in \{-N, \cdots, -1, 0, 1, \cdots, N\}$, $1 \le i \le m$, and avg is the average.
- Relative-Entropy-Comparison (REC): a measure of the difference between two probability distributions f and g,

$$c(f, g) = \sum_i f(i) \log \frac{f(i)}{g(i)}. \quad (3)$$

Given two Bio-Capsules $\vec{p} = (p_1, p_2, \cdots, p_n)$ and $\vec{q} = (q_1, q_2, \cdots, q_n)$, to measure the distance between them we can use different metrics:

- Euclidean Distance (ED):

$$ED(\vec{p}, \vec{q}) = \sqrt{\sum_{i=1}^{n} (p_i - q_i)^2} \quad (4)$$

- Manhattan Distance (MD):

$$MD(\vec{p}, \vec{q}) = ||\vec{p} - \vec{q}|| = \sum_{i=1}^{n} |p_i - q_i| \quad (5)$$

- Chebyshev Distance (CD):

$$CD(\vec{p}, \vec{q}) = max_i |p_i - q_i| \quad (6)$$

Thus, the proposed approach computes the difference (measured by AVC, RVC or REC) of user biometric feature set and reference feature set, then uses the difference to construct the Bio-Capsule. If the distance (measured by ED, MD or CD) of enrolling Bio-Capsule and query Bio-Capsule is within preselected threshold, the user is authenticated.

B. Justification

To justify the proposed approach, we compare the proposed approach with conventional biometric authentication methods. In conventional biometric authentication, user u provides his biometric data u_D, from which feature set u_F is extracted. For authentication, from query biometric data $u_D^{'}$ feature set $u_F^{'}$ is extracted. If Eq. 7 is true, the user is authenticated.

$$DIS(u_F, u_F^{'}) < thresh \quad (7)$$

In comparison, the proposed approach computes the distance of enrolling Bio-Capsule $u_{BC} = BC(u_F, RS_F)$ and query Bio-Capsule $u_{BC}^{'} = BC(u_F^{'}, RS_F)$.

$$DIS(u_{BC}, u_{BC}^{'}) = DIS(BC(u_F, RS_F), BC(u_F^{'}, RS_F)) < thresh^{'} \quad (8)$$

As mentioned, BC may take different metrics: AVC, RVC, etc. and DIS may take ED, MD, etc. If each feature set F consists of n features as $F = (F(1), F(2), \cdots, F(n))$ and each feature $F(i)$ has m components as $F(i) = (f(i,1), \cdots, f(i,m))$. We illustrate two cases as follows.

- Case 1: BC is measured by AVC, and DIS is measured using ED. Then

$$\begin{aligned} DIS(u_F, u_F^{'}) &= \frac{\sum_{j=1}^{n} ED(u_F(j), u_F^{'}(j))}{n} \\ &= \frac{\sum_{j=1}^{n} \sqrt{\sum_{i=1}^{m} (u_f(j,i) - u_f^{'}(j,i))^2}}{n} \end{aligned} \quad (9)$$

  From Eq. 1, $BC(f,g) \approx \frac{f-g}{Th}$, where Th is the selected threshold. Then

$$\begin{aligned} DIS(u_{BC}, u_{BC}^{'}) &= \frac{\sum_{j=1}^{n} ED(u_{BC}(j), u_{BC}^{'}(j))}{n} \\ &= \frac{\sum_{j=1}^{n} ED(\frac{u_f(j,i) - RS_f(j,i)}{Th}, \frac{u_f^{'}(j,i) - RS_f(j,i)}{Th})}{n} \\ &= DIS(u_F, u_F^{'})/Th \end{aligned} \quad (10)$$

- Case 2: C is measured by RVC, and DIS is measured using MD. Then

$$\begin{aligned} DIS(u_F, u_F^{'}) &= \frac{\sum_{j=1}^{n} MD(u_F(j), u_F^{'}(j))}{n} \\ &= \frac{\sum_{j=1}^{n} \sum_{i=1}^{m} |u_f(j,i) - u_f^{'}(j,i)|}{n} \end{aligned} \quad (11)$$

And from Eq 2, $C(f,g) \approx \frac{f-g}{g \times Th}$. The distance of u's enrolling Bio-Capsule and query Bio-Capsule turns

$$
\begin{aligned}
DIS(u_{BC}, u'_{BC}) &= \frac{\sum_{j=1}^{n} MD(u_{BC}(j), u'_{BC}(j))}{n} \qquad (12) \\
&= \frac{\sum_{j=1}^{n} \sum_{i=1}^{m} |BC(u_f(j,i), RS_f(j,i)) - BC(u'_f(j,i), RS_f(j,i))|}{n} \\
&\approx \frac{\sum_{j=1}^{n} \sum_{i=1}^{m} |\frac{u_f(j,i) - u'_f(j,i)}{RS_f(j,i) \times Th}|}{n}
\end{aligned}
$$

In these two cases (and others omitted), $DIS(u_{BC}, u'_{BC})$ could be considered as a projection of $DIS(u_F, u'_F)$. This projection preserves the discrimination among users, thus the Bio-Capsule u_{BC} can be used instead of the template u_F for authentication, which has also been justified by the experimental results.

C. Security Analysis

As mentioned in [16], the security of biometrics-based system should consider measurements in terms of information entropy loss as well as FAR and FRR. In this paper, we consider the security of the proposed approach from those two aspects. This subsection investigates several criteria based on Shannon information [14] and consider security measure in terms of entropy loss, the FAR and FRR results will be presented in Section V.

One important design objective of the proposed approach is that from u_{BC} attackers can not easily get information about u_F. Furthermore, from u_{BC} and RS_F, attackers or the CA can not gain full information about u_F. In this case, we will model the CA as honest-but-curious, that is, the CA honestly uses the RS_F and follows the protocol, but will try to get more information about u_F. Given a Shannon entropy or self-information $H(u_F)$ of a user u's feature u_F and a conditional entropy $H(u_F|u_{CLS})$ of user u's feature u_F on his user class u_{CLS}, there is a definition of mutual information as:

$$I(u_F; u_{CLS}) = H(u_F) - H(u_F|u_{CLS}) \qquad (13)$$

The higher $I(u_F; u_{CLS})$ implies greater relevance of u_F to u_{CLS}.

The conditional information loss of u_F on a class u_{CLS} is defined as indicative of how much information u_F gives about u_{CLS}:

$$ILoss(u_F|u_{CLS}) = 1 - 2^{-I(u_F; u_{CLS})} \qquad (14)$$

Intuitively, it can be seen that: 1) a more relevant feature reveals more about a class; and 2) a less relevant feature indicates less about a class.

It is considered as a challenging open problem to find quantitative means to measure the success probability of smart attacks against biometric data and also to determine the exact information loss of the biometric data [16]. Thus, we prove the enhanced security of proposed approach by comparing to conventional biometric authentication as follows.

In conventional biometric authentication, for higher authentication accuracy, it is necessary that each user's feature set uniquely represents the user, thus user u's feature set u_F is more relevant to his own class u_{CLS} than other users' classes. However, a more relevant feature set implies high information loss, which compromises security. This trade-off of accuracy and security is a problem for many biometrics-based authentication approaches. However, the proposed approach uses u_{BC} for authentication, and the conditional information loss of a user's Bio-Capsule u_{BC} on a class u_{CLS} is:

$$ILoss(u_{BC}|u_{CLS}) = 1 - 2^{-I(u_{BC}; u_{CLS})} \qquad (15)$$

u_{BC} comes from user's feature u_F and the Reference Subject's feature RS_F, thus u_{BC} is much less relevant to u_{CLS} than u_F does. From the information theory point of view, $I(u_{BC}; u_{CLS}) \ll I(u_F; u_{CLS})$ results in a smaller information loss and provides better security, which also justifies the assertion that from u_{BC} the attackers can not easily get information about u_F.

Let us define conditional mutual information between a Bio-Capsule u_{BC} and the reference feature set RS_F conditioned on a class u_{CLS} as

$$I(u_{BC}; RS_F|U_{CLS}) = H(u_{BC}|u_{CLS}) - H(u_{BC}|u_{CLS}, RS_F) \qquad (16)$$

which is an estimation of the quantity of information shared between u_{BC} and RS_F when u_{CLS} is known: it implies how attackers or the CA can learn about user biometric information when u_{BC} and RS_F are known. Also let us define the information loss of u_{BC} given RS_F and u_{CLS} as

$$ILoss(u_{BC}|(RS_F, u_{CLS})) = 1 - 2^{-I(u_{BC}; RS_F|u_{CLS})} \qquad (17)$$

This shows that better security and privacy is equivalent to minimizing $ILoss$. In an environment in which a user's information is fully exposed to the CA, $ILoss$ is maximum, as denoted as $ILoss_0$. In the proposed approach, since $I(u_{BC}; RS_F|CLS) < I(u_F|CLS)$, $ILoss$ is less than $ILoss_0$. In other words, compared to the conventional biometric authentication, the proposed approach secures user's biometric information and preserves user's privacy much better.

IV. Enhanced capability of the new approach in a Non-Trust Model

One of the primary advantages of the proposed approach is that it fits for different security requirements and application environments. From Fig. 1 and Fig. 2, it is clear that the new approach can be directly used in the conventional biometric authentication model in which the CA is allowed to completely know and fully control users' biometric information. Furthermore, utilization of BC allows the deployment of the proposed approach in not-fully trusted environments. In this section, we briefly present one system design which demonstrates such an advantage.

A. Model and Objectives

In the non-trust model, there are two entities: a non-trusted CA and users. By *non-trust*, the CA is stipulated as some party who is kept away from users' true biometric data. Here users are individuals to be authenticated.

The design objectives in this model are as follows:

- Service: users can register to the system, be authenticated by the CA, and unsubscribe from the system at any time.

- Security and privacy: no information is learned by any non-legitimate or un-intended party; compromised information will not infringe upon users' biometric data. In particular, the CA does not know users' original biometric data.

B. Secure Multiple Party Computation (SMPC)

Secure Multiple Party Computation (SMPC) is described as a problem in which people are jointly conducting computation tasks based on the private inputs they each supply; however each person wants to keep his inputs from being known by others. SMPC has been intensively studied and some good approaches have been proposed [10], [20]. SMPC, especially, Secure Two-Party Computation (STPC) will be utilized in this model. As a result, a user's real biometric information will not be revealed to the CA but the CA can compute the user's BC for storage during enrollment and the BC for authentication during verification.

C. Non-trusted Model Design

The system design in this model includes three components: enrollment, verification (as shown in Fig 3), and revocation .

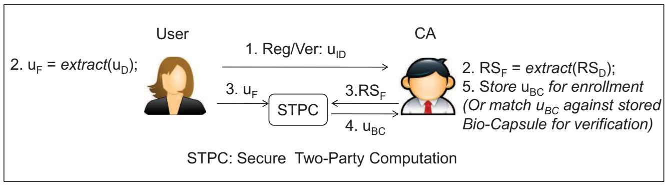

User
CA
1. Reg/Ver: u_{ID}
2. u_F = *extract*(u_D);
3. u_F
STPC
3.RS_F
4. u_{BC}
2. RS_F = *extract*(RS_D);
5. *Store* u_{BC} *for enrollment*
(Or match u_{BC} *against stored Bio-Capsule for verification)*
STPC: Secure Two-Party Computation

Fig. 3: System design in a non-trust model

1) Enrollment:

- *Step 1*: user u starts enrollment by sending CA an enrollment request containing his identity:

  $u \rightarrow CA$: $Reg : u_{ID}$.
- *Step 2*: user u and CA acquire biometric data u_D and RS_D and extract the feature sets u_F and RS_F respectively.
- *Step 3 and 4*: user u and CA conduct a STPC on feature sets to compute $u_{BC} = c(u_F, RS_F)$.
- *Step 5*: upon receipt of u_{BC}, the CA stores it as the Bio-Capsule for u.

2) Verification:

- *Step 1*: u initiates a verification process by sending the CA a verification request containing his identity:

  $u \rightarrow CA$: $Ver : u_{ID}$.
- *Step 2*: user u and CA acquire biometric feature set u'_F and RS'_F respectively.
- *Step 3 and 4*: user u and CA conduct the STPC to compute $u'_{BC} = c(u'_D, RS'_D)$.
- *Step 5*: CA compares the u'_{BC} from *Step 4* and u_{BC} acquired in *enrollment stage*. If they are the within a pre-specified threshold, u is authenticated.

3) User Revocation: A user can always be revoked from the system and our approach is very efficient in such a scenario. The CA can simply abandon the user's record in its database. Further, the user needs not worry about his information being further misused, since no real biometric data is recorded, and the stored Bio-Capsule reveals nothing about a user's true biometric data.

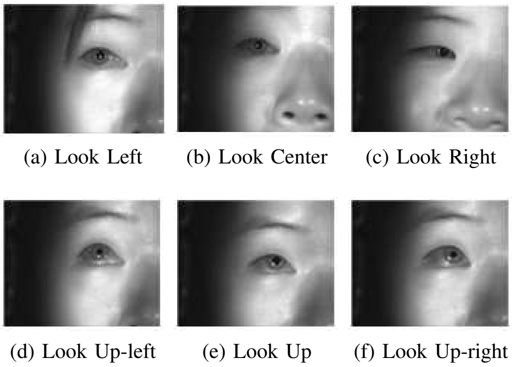
It is worthy to mention that a secure channel between the user and the authentication server can be set up if needed, such as via a public key cryptosystem, to keep the confidentiality and integrity of messages transferred between them.

From the above description, it can be seen that by incorporating secure two-party computation, the proposed approach can be easily used in non-trust environments.

V. Experimental Results and Analysis

We apply the proposed approach on practical iris data. The implementation essentially includes two stages: enrollment and verification, and three sections: feature extraction, Bio-Capsule generation, and Bio-Capsule matching. The feature extraction mainly come from our recent work [2] which is a well-performed non-cooperative iris recognition method. This method works with both frontal and off-angle iris images with low-resolution.

The experiments were conducted on an IUPUI Remote Iris Image Database. The average iris radius of the video images in the database is 95 pixels. In this experiment, for each iris six classifications of angle, frontal look, left look, right look, up-left look, up look and up-right look (e.g. Fig 4), were used. The total number of images used was 3,707 which includes both left and right eyes from 31 subjects.


(a) Look Left (b) Look Center (c) Look Right

(d) Look Up-left (e) Look Up (f) Look Up-right

Fig. 4: IUPUI remote iris image database: multiple angles

The performance of the system is measured by equal error rate (EER), false accept rate (FAR) and false reject rate (FRR). In this experiment, 10 reference feature sets are randomly generated. For each reference feature set, 3,707 images are used for both enrollment and verification. The genuine verifications are from the same eye; the impostors are the verification results from different eyes.

Fig 5 shows ROC curves of applying the proposed approach on frontal look eyes (we get similar results on other-look eyes, thus omitted). Here, each curve is obtained by varying the *threshold* of the proposed approach. These three curves are obtained by enrolling using different reference feature sets; and we get a rather stable result.

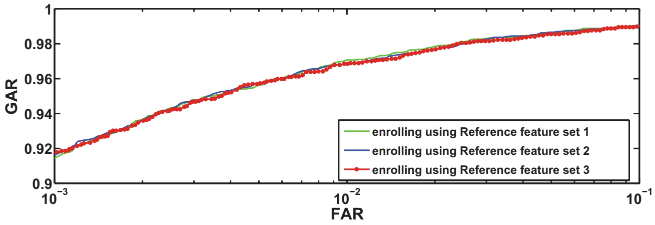


Fig. 5: IUPUI remote database frontal look eyes accuracy

The following experimental result shows that in terms of accuracy the proposed approach is comparable to and outperforms conventional biometric approaches including 1-D Log Gabor, the Regional SIFT and the Gabor Descriptor. Table I shows the EER results (the lower, the better) on all-look eyes from IUPUI database. Due to the error- and noisy-prone feature collection process, there exists intrauser variance of the within-class biometric templates; that is, biometric data collected from the same person but at different context are not exactly same, therefore the generated templates from those instable data are not exactly matched. Thus, conventional biometric authentication is mainly focused on better tolerance of the within-class variance of biometric templates while discriminating between-class distance, which could be very challenging. Considering such intrauser variance or instability of biometric templates, Bio-Capsules could become an alternative. Since the Bio-Capsules/"difference" could be more stable compared to conventional biometric templates, which will leads to improved performance. Our experimental results validate such improvements.

TABLE I: IUPUI remote database accuracy (EER) results

Classes	Regional SIFT	Gabor Descriptor	Proposed Method
Center	0.0350	0.0273	0.0209
Left	0.0454	0.0214	0.0154
Right	0.0454	0.0162	0.0155
Up-Right	0.0567	0.0540	0.0320
Up-Left	0.0610	0.0492	0.0324
Up	0.1392	0.1251	0.1008

VI. Conclusions

In this paper, we proposed a new biometrics-based authentication approach. The proposed approach derives fuzzy data from user's and Reference Subject's biometric information, and from these fuzzy data generates a Bio-Capsule for authentication. Security analysis shows that the approach is secure and privacy-preserving and experimental results on iris and complexity analysis show that the proposed approach is comparable to conventional biometric authentication approaches. We will continue to study and test the properties and efficiencies of the proposed approach and also extend our study to other biometrics, e.g., evaluate the performance of three proposed Biometric Capsule Computation methods on face, fingerprint, etc. How to enhance the system security and scalability by employing multiple Reference Subjects and how to generate a new Biometric Capsule by composing multiple Biometric Capsules are some interesting yet challenging issues which will be investigated further.

References

[1] 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*, 38:97–139, 2008.

[2] Y. Du, C. Belcher, and Z. Zhou. Scale invariant gabor descriptor-based noncooperative iris recognition. *EURASIP J. Adv. Signal Process*, 2010:37:1–37:10, February 2010.

[3] C. Gentry, P. Mackenzie, and Z. Ramzan. Password authenticated key exchange using hidden smooth subgroups. In *Proceedings of the 12th ACM conference on Computer and communications security (ACM CCS'05)*, pages 299–311, 2005.

[4] V. Govindaraju, V. Chavan, and S. Chikkerur. Biometric convolution using multiple biometrics. *Google Patents*, 2005.

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

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

[7] A. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross, and J. Wayman. Biometrics: a grand challenge. In *Proceedings of the 17th International Conference on Pattern Recognition*, pages 935–942, 2004.

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

[9] Y. Lee, K. Park, S. Lee, K. Bae, and J. Kim. A new method for generating an invariant iris private key based on the fuzzy vault system. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 38(5):1302–1313, 2008.

[10] Y. Lindell and B. Pinkas. An efficient protocol for secure two-party computation in the presence of malicious adversaries. *In Advances in Cryptology - EUROCRYPT 2007*, 4515:52–78, 2007.

[11] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri. Cancelable templates for sequence-based biometrics with application to on-line signature recognition. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 40(3):525–538, 2010.

[12] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle. Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):561–572, 2007.

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

[14] F.M. Reza. *An Introduction to Information Theory*. Dover, New York, 2010.

[15] M. Savvides, B. Kumar, and P. Khosla. Cancelable biometric filters for face recognition. In *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on*, volume 3, pages 922–925, 2004.

[16] 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.

[17] Y. Sutcu, Q. Li, and N. Memon. Secure biometric templates from fingerprint-face features. *Computer Vision and Pattern Recognition, IEEE Computer Society Conference on*, 0:1–6, 2007.

[18] K. Takahashi, S. Hirata, H. Hino, and M. Mimura. Method, system and program for authenticating a user by biometric information. *Google Patents*, 2007.

[19] K. Takahashi and S. Hitachi. Generating provably secure cancelable fingerprint templates based on correlation-invariant random filtering. In *Proceedings of IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems*, pages 1–6, 2009.

[20] A. Yao. Protocols for secure computations. In *Proceedings of 23rd Annual Symposium on Foundations of Computer Science*, pages 160–164, 1982.