Journal of Universal Computer Science, vol. 24, no. 4 (2018), 341-356
submitted: 14/10/17, accepted: 15/4/18, appeared: 28/4/18 © J.UCS

Secure Method for Combining Cryptography with Iris Biometrics

Alawi A. Al-Saggaf
(Dammam Community College
King Fahd University of Petroleum and Minerals
Dhahran 31261, Saudi Arabia
alawi@kfupm.edu.sa)

Abstract: Cryptography and biometrics are widely used in providing information security. Cryptographic systems rely on keys for secure information. Unlike biometric systems, the keys in cryptographic systems must be exactly reproducible and not strongly linked to the user identity. Each of the two systems has some issue associated with it. Combining cryptography and biometrics in a secure way can mitigate these issues. This paper presents a secure cryptographic authentication method based on the discrete logarithm problem. Through the security analysis of the proposed scheme, we prove that the security characteristics of the proposed scheme relative to the properties of the discrete logarithm problem. Based on the proposed scheme, a biometric cryptosystem is constructed. The proposed system evaluated using CASIA iris database from 70 different eyes, with 7 samples of each eye. Experimental results demonstrate that the proposed system is more effective, promising in terms of cope up to 21.41% percent of error bits within an iris code, and can generate up to 98 bits of the cryptographic key from the iris codes.

Keywords: Cryptography, Biometrics, Discrete logarithm problem, Biometric template protection, Authentication, Template security, Error correcting codes.
Categories: D.4.6, C.2.0, E.4

1 Introduction

1.1 Motivation

The increasing popularity of cryptography and biometric systems due to the great demand for information security in many applications such as e-commerce, e-banking, e-government, e-passport, e-health and a number of forensic applications. In generic cryptographic systems, people use personal passwords or secret keys authentication methods to protect their collections of personal and potentially confidential information. However, most people use simple passwords, which are pretty easy to crack, complex passwords, which are difficult to remember. Furthermore, the secret keys are difficult to memorize because it is long and random, and therefore, need to be stored somewhere. The drawback of cryptography is that these authentication methods are not strongly linked to the user's identity. On the other hand, biometrics [Rathgeb et al., 2012] refer to "automated recognition of individuals based on their behavioural and biological characteristics such as fingerprints, iris, face, hand, voice, and gait, etc. Unlike, cryptographic–based authentication methods, biometric is user-friendly, easy to use, convenient, not

possible to share, reliable, and cannot be forgotten or lost. Unfortunately, biometric systems possess problems of their own such as improper storage, or transmission leaks may compromise security. Therefore, it is important to protect the biometric using cryptography. Furthermore, utilization of biometrics in cryptography protocols raises another problem; the ratio for authentication in biometric systems needs not to achieve 100% accuracy, as two readings of the same biometric data are rarely identical whereas cryptography needs identically reproducible and uniformly distributable data. In order to strength the link between the user identity and his cryptographic key and enhance the security and the privacy of biometrics, cryptography and biometrics are combined. Combining cryptography and biometric in a secure way can inherit the positive aspects of the two while eliminating their limitations. This paper presents a new secure cryptographic authentication scheme based on discrete logarithm problem. The proposed system achieves high security relative to the properties of discrete logarithm problem, generate secured cryptographic key, and the tolerance for error of iris biometric.

1.2 Related work

The theoretical basis construction of combining cryptography and biometrics, known as fuzzy commitment scheme (FC), proposed by Jules and Wattenberg [Juels and Wattenberg, 1999] is a general scheme of combining cryptography and biometric. In fuzzy commitment scheme, a secret key is combined with reference biometric template to create the difference vector. The difference vector is created such that the secret key can be reconstructed with the help of the difference vector and the query biometric template. The security characteristic of fuzzy commitment scheme solely relies on the cryptographic hash function. In [Juels and Sudan, 2006], Jules and Sudan drove a new scheme known as fuzzy vault (FV) from fuzzy commitment based on polynomial reconstruction. The FC and FV schemes became popular techniques for design biometrics secrecy systems [Rathgeb, and Uhl, 2011; Ignatenko, 2010; Jain et al., 2008; Jain et al., 2005]. Fuzzy commitment and fuzzy vault schemes gained a lot of significance of cryptography and biometrics research communities. The FC and FV schemes are applied to different biometric traits, like iris biometrics [Hao et al., 2006; Ignatenko and Willems, 2009; Bringer et al., 2009; Rathgeb and Uhl, 2009; Rathgeb and Uhl, 2010; Zhang et al., 2009; Adamovicb et al., 2017; Ratherb et al., 2013], fingerprint biometric [Teoh and Kim, 2007; Tong et al., 2007; Nandakuma, 2010; Li et al., 2012], and face biometric [Lu et al., 2009; Vander et al., 2006]. In 2015, [Fave et al., 2015] and [Hoang et al., 2015] applied the fuzzy commitment to finger Vein and human gait, respectively. Fave et al. did not mention the length of the cryptographic key. [Sasa et al., 2017] presented a method based on information theoretical analysis to extract homogenous regions of iris biometric and secured using fuzzy commitment scheme. They utilized the Reed Solomon codes RS(127,20) with a capacity of an error rate of 42% of the iris code. This rate will affect the system's performance and not be practical. Several biometric template protection systems have been proposed [McGuffey et al., 2015; Lakhera et al., 2016; Jin et al., 2016]. Recently, several approaches applied fuzzy commitment scheme to secure multimodal systems [Gomez-Barrero et al., 2017; Mai et al., 2017; Sarier, 2018].

The security characteristic of the biometric secrecy system based on fuzzy commitment scheme solely relies on the relative properties of cryptographic hash

function MD or SHA families. However, several researchers have noticed serious security flaws and vulnerabilities in most widely used MD and SHA families [Preneel, 1999; Preneel, 2009; Wang et al., 2005a; Wang et al., 2005b; Wang and Yu, 2005; Biham et al., 2005; Dobbertin, 1996; Klima, 2006]. Moreover, in response to an SHA-1 vulnerability announced in Feb. 2005, NIST (National Institute of Standard and Technology) was apparently not confident in the strength of SHA-1 [NIST, 2007].

1.3 Paper contribution

The contributions of this paper are outlined below:

1. Propose a secure cryptographic authentication scheme based on the discrete logarithm problem.
2. Provide a theoretical analysis of the security characteristics of the proposed scheme in terms of the statistical hiding and the computational binding.
3. Apply the proposed scheme to biometric systems to construct a new biometric cryptosystem using Iris based biometrics.
4. The proposed system evaluated using CASIA iris database from 70 different eyes, with 7 samples of each eye.
5. Experimental results demonstrate that the proposed system is more effective, promising in terms of cope up to 21.41% percent of error bits within an iris code, and can generate up to 98 bits of the cryptographic key from the iris codes.

1.4 Paper organization

The rest of the paper is organized as follows: In section 2, we briefly discuss some mathematical preliminaries to review and analyse the proposed method. We then present the proposed method in section 3. In section 4, we state theorems regarding the security characteristics of the proposed method. In section 5, we apply the proposed method to biometric systems. Experimental evaluation results and discussions of the proposed reported in Section 6. Finally, a conclusion is given in Section 7.

2 Preliminaries

This section briefly describes some mathematical preliminaries which are essential for describing and analyzing the proposed method.

2.1 The discrete logarithm problem

Definition 1 Discrete Logarithm: Let G be a finite cyclic group of order n. Let α be a generator of G and let $\beta \in G$. The discrete logarithm of β to the base α, denoted $\log_\alpha \beta$, is the unique integer x, $0 \le x \le n-1$, such that $\beta = \alpha^x$ [Menezes et al., 1996].

Definition 2 Discrete Logarithm Problem (DLP): Given a prime number p, a generator α of Z_p^*, and an element $\beta \in Z_p^*$. Find the integer x, $0 \le x \le p-2$, such that $\beta = \alpha^x \pmod p$ [Menezes et al., 1996].

2.2 Error correcting codes

Error correcting codes are used for detecting and correcting errors when data transmitted from one place to another over a noisy channel.

Important terms and definitions.

Definition 3: A block code $C(n.k)$ over an alphabet of q symbols is a set of q^k n-vectors called codewords. Associated with the code is an encoder $g : \{0,1\}^k \to C$ which maps a message m, a k –tuple, to its associated codeword [Moon, 2005].
Definition 4 (Hamming distance): Given code set $C(n,k)$ as defined above, The Hamming distance between any two words c_i and c_j of the code set C is given by

$$H_{dist}(c_i, c_j) = \frac{1}{n}\sum_{r=1}^{n} | c_i^r - c_j^r | \qquad (1)$$

Definition 5 (Decoding function): Let $C(n.k)$ be a block code set with $q \in \{0,1\}$. A decoding function $f : \{0,1\}^n \to C \cup \perp$ which maps a message c', a n-tuple, to correct codeword c, if c' and c are sufficiently close according to appropriate metric. Otherwise maps to invalid codeword $\perp$.
Definition 6: The maximum number of errors that can be corrected in the corrupted codeword is called error correction threshold of the error correcting code C, and denoted by t_{sh}.

Bose - Chaudhuri, and Hocquenghem (BCH) codes

A BCH codes are cyclic codes and specified by chosen generator polynomial. It is a polynomial code over a finite field (*GF*). A narrow sense BCH code over $GF(q)$ of length n capable of correcting at least t_{sh}-errors is specified as follows [Moon, 2005]:

1. Determine the smallest $m (m \ge 3)$ such that $GF(q^m)$ has a primitive nth root of unity λ.
2. Select a non-negative integer b. Frequently, $b = 1$.
3. Write down a list of $2t_{sh}$ consecutive powers of λ:

   $\lambda^b, \lambda^{b+1}, ..., \lambda^{b+2t_{sh}-1}$.

   Determine the minimal polynomial with respect to $GF(q)$ of each of these powers of λ.

4. The generator polynomial $P(x)$ is the least common multiple (LCM) of these minimal polynomials. The code is a $(n, n-\deg(P(x)))$ cyclic code, where $\deg(P(x))$ is the degree of the polynomial $P(x)$.

Usually we use $BCH(n,k)$ to denote a BCH code, where n is the code length, and k is the message length.

2.3 Statistical distance

Let X and Y be two random variables over the same sample space ψ, and let D_1 and D_2 be their associated discrete probability distributions. Then, we defined and denoted the statistical distance between D_1 and D_2 as follows:

$$S_{dist}(D_1; D_2) = \sum_{a \in \psi} \left| \text{Prob}[\text{X} = a] - \text{Prob}[\text{Y} = a] \right| \tag{2}$$

3 The Proposed Method

In this section, we will provide details of the proposed scheme. There are three procedures in the proposed scheme, namely the setup, commit, and open procedures. Also, there are three parties, the sender **S** and the receiver **R**, and the trust third party **Ted** will run setup procedure to generate the system parameters and publish it to both parties. The proposed scheme consists of the function, $F:\left(\{0,1\}^n \times \{0,1\}^n\right) \to \left(\{0,1\}^n \times \{0,1\}^n\right)$, defined as follows:

$$F(c, x) = (\varepsilon, \delta), \tag{3}$$

where $\varepsilon = F_k(m, x) = \alpha^m \beta^x \pmod p$ and $\delta = x - c$ is the difference vector.

To set the system parameters, the trusted third party executes the following procedure.

[Setup procedure]

1. **Ted** generates two prime numbers p and q such that $p = 1 \pmod q$.
2. **Ted** finds a random generator $\alpha \in G_q \setminus \{1\}$, where $\alpha \in G_q$ is a subgroup of the order q in Z_p^*.
3. **Ted** computes an element $\beta = \alpha^a \in Z_p^* \setminus \{1\}$, where $a \in Z_q$ randomly chosen (β is a generator element of G_q).
4. **Ted** sends the system parameters (p, q, α, β) to the sender **S** and the receiver **R**.

[Commit procedure]

To commit to a message $m \in M_k \subseteq Z_q$, ($M_k \subset \{0,1\}^k$ is the message space), the sender encode the message into a codeword $c = g(m) \in C \subseteq \{0,1\}^n$ and chooses a random witness $x \in X_n \subseteq Z_q$, ($X_n \subset \{0,1\}^n$ is the witness space), and then computes the commitment $F(c, x) = \left(\alpha^c \beta^x, x - c\right) = (\varepsilon, \delta)$. The commitment send to the receiver.

[Open procedure]
To open the commitment (ε,δ), the sender reveals the witness x', which is sufficient "close" to the original x according to an appropriate metric distance (e.g. Hamming distance $H_{dist}(x,x') \le t_{sh}$), but not necessary identical. Using the difference vector δ the witness x' should be able to reconstruct the codeword $f(c') = f(x'-\delta) = f((x'-x)+c)$ and then translate $x'' = \delta + f(c')$ in the direction of x. The receiver computes the commitment $\varepsilon' = F_k(f(c'), x'')$ and verifies $\varepsilon' \stackrel{?}{=} \varepsilon$. If it fails, the commitment will not open using x'. Otherwise, the commitment is successful opened and therefore the secret message $m = m' = g^{-1}(f(c'))$.

4 Security Analysis

In the design of any commitment scheme, hiding and binding properties are the most important security aspects to be considered. In this section we will discuss the security of the proposed scheme, to simplify our analysis, It should be noted that the codeword c and the witness x are drawn at random from the set $\{0,1\}^n$. These sets are finite and all their associated probabilities distributions are discrete. Furthermore, the operation ($\oplus$) is defined and denoted as "exclusive OR", Pr[.] is the probability of an event and $|.|$ denoted the size of the set.

4.1 Hiding property

The hiding property of the proposed scheme characterizes the resistance against attempts carried out by an adversary receiver **R*** to determine either the codeword c or the witness x. We assume that the adversary receiver **R*** knows the function, F, and has an access to the commitment pair (ε,δ). The security analysis of hiding property comprises two aspects: First, we prove that an adversary receiver **R*** gets almost NOT statistical advantage about the committed codeword or witness from the difference vector δ. Second, we prove that an adversary receiver **R*** cannot distinguish between the sender's committed value based on the hardness of solving discrete logarithms.

Lemma 1: Suppose that X and Y are two independent random variables over the same sample space ψ. Let Z be a random variable obtained by "exclusive OR" of X and Y. Then the three random variables X, Y, and Z are pair-wise independent.
Proof: Let X and Y are two independent random variables over the same sample space ψ. So we have, $\text{Prob}[X = u, Y = v] = \text{Prob}[X = u]\text{Prob}[Y = v] \le \frac{1}{|X||Y|}$ (4)

Now, let $Z = w$, such that $w = u \oplus v$, and thus $v = w \oplus u$.
Since the variables $X = u$ and $Y = w \oplus u$ are independent random variables, therefore X and Z. Similarly, Y and Z are independent.

Theorem 1 Suppose that X (witness space) and C (error correcting code set) are two independent random variables over the same sample space $\{0,1\}^n$. Given that $\mathrm{Z}=\{\delta = x \oplus c; x \in \mathrm{X} \text{ and } c \in C\}$ is another a random variable obtained by "exclusive OR" of elements of C and X. Then the probability that the difference vector reveals information about c or x is not more than 2^{-k}.

Proof:

Assume that X and C be two independent random variables over the same sample space $\{0,1\}^n$.

Since $|\mathrm{C}| = 2^k$ clearly $k \le n$. Let $\mathrm{Z} = \{\delta : \delta = c \oplus x\}$ be a random variable obtained by "exclusive OR" of elements $c \in \mathrm{C}$ and $x \in \mathrm{X}$. Then Z, X, and C are pair-wise independent random variables (Lemma 1). Then, we have

$$\Pr[\mathrm{X} = x \mid \mathrm{Z} = \delta] = \Pr[\mathrm{X} = x] \le 2^{-n}, \tag{5}$$

and

$$\Pr[\mathrm{C} = c \mid \mathrm{Z} = \delta] = \Pr[\mathrm{C} = c] \le 2^{-k}, \tag{6}$$

Therefore

$$\begin{aligned} &\Pr[\mathrm{X} = x \mid \mathrm{Z} = \delta \text{ or } \mathrm{C} = c \mid \mathrm{Z} = \delta] \\ &= \mathrm{Max}\{\Pr[\mathrm{X} = x], \Pr[\mathrm{C} = c]\} \le 2^{-k} \end{aligned} \tag{7}$$

(Max : denoted the maximum of two values) … hence proof

Theorem 2 Given $c \in \mathrm{C}$ and $x \in \mathrm{X}$ is chosen randomly, an adversary receiver **R*** is able to determine the codeword c from the commitment ε in probability time. Then an adversary R* gets absolutely zero advantages about the committed codeword c.

Proof:

Given that $c = g(m) \in C$, let $D(c)$ be a probability distribution on the code set C, defined as $D(c) = \mathrm{Prob}[C = c : F_k(c, x) = \varepsilon]$ and let $\rho_{\varepsilon,c}$ be the size of pre-image set $\Omega_\varepsilon(c) = \{x : F_k(c, x) = \varepsilon\}$.

Thus for any ε_0, $D(c_0)$ is defined by

$$\begin{aligned} D(c_0) &= \mathrm{Prob}[C = c_0 : F_k(c_0, x) = \varepsilon_0, \text{ for some } x \in \mathrm{X}] \\ &= \sum_{x \in \mathrm{X}} \mathrm{Prob}[x]\mathrm{Prob}[F_k(c_0, x) = \varepsilon_0 \mid x] \end{aligned} \tag{8}$$

For some value $\mathrm{x}_0 \in \mathrm{X}$, we have

$$\begin{aligned} \mathrm{Prob}[F_k(c_0, x_0) = \varepsilon_0 \mid x_0] &= \mathrm{Prob}[x_0 : F_k(c_0, x_0) = \varepsilon_0] \\ &= \begin{cases} 2^{-k} & \text{if } x_0 \in \Omega_{\varepsilon_0}(c_0) \\ 0 & \text{Otherwise} \end{cases} \end{aligned} \tag{9}$$

Thus,

$$
\begin{aligned}
D(c_0) &= \text{Prob}[F_k(c_0,x) = \varepsilon_0, \text{ for some } x \in \text{X}] \\
&= \sum_{x \in \text{X}} \text{Prob}[x]\text{Prob}[F_k(c_0,x) = \varepsilon_0 \mid x] \\
&= 2^{-k} \sum_{x \in \Omega_{\varepsilon_0}(c_0)} 2^{-k} = 2^{-2k} \rho_{\varepsilon_0,c_0}
\end{aligned} \tag{10}
$$

Assume that the receiver can find two codewords c_1 and c_2 in C, such that $H_{dist}(c_1,c_2) > t_{sh}$ and $F_k(c_1,x_1) = F_k(c_2,x_2) = \varepsilon$ for some $x_1, x_2 \in \mathbf{X}$. Thus,

$$
\begin{aligned}
S_{dist}(D(c_1),D(c_2)) &= \sum_{\varepsilon \in \text{E}} |\text{Prob}[F_k(c_1,x) = \varepsilon] - \text{Prob}[F_k(c_2,x) = \varepsilon]| \\
&= \sum_{\varepsilon \in \text{E}} |\sum_{x \in \text{X}} \text{Prob}[x]\text{Prob}[F_k(c_1,x) = \varepsilon] - \sum_{x \in \text{X}} \text{Prob}[x]\text{Prob}[F_k(c_2,x) = \varepsilon]| \text{ Since,} \\
&\le \sum_{\varepsilon \in \text{E}} |2^{-2k} \sum_{x \in \Omega_\varepsilon(c_1)} 1 - \sum_{x \in \Omega_\varepsilon(c_2)} 1| = 2^{-2k} \sum_{\varepsilon \in \text{E}} |\rho_{\varepsilon,c_1} - \rho_{\varepsilon,c_2}| = 0
\end{aligned}
$$

for any $c \in \text{C} \subseteq Z_q$ and for randomly uniformly chosen a witness $x \in \text{X} \subseteq Z_q$. Then $\varepsilon = F_k(c,x)$ is uniformly distributed in G_q. Therefore $\rho_{\varepsilon,c_1} = \rho_{\varepsilon,c_2}$. Hence the proof.

4.2 Binding Property

The binding property of proposed scheme characterizes the resistance against attempts carried out by an adversary receiver **A*** to determine a codeword c' with $H_{dist}(c,c') > t_{sh}$, such that $F_k(c,x) = F_k(c',x') = \varepsilon$, for some $x, x' \in \text{X}$.

Theorem 3 For $c \in \text{C}$ and $x \in \text{X}$ is chosen randomly, an adversary sender **S*** is able to open the fuzzy commitment $F(c,x) = (\varepsilon,\delta)$ using different witness $x' \in \text{X}$ such that $H_{dist}(x,x') > t_{sh}$ in probability time. Then it is equivalent that the adversary **S*** is able to solve the discrete logarithm problem.

Proof:

Let $c \in \text{C}$ and $x \in \text{X}$ is chosen randomly such that $\varepsilon = F_k(c,x)$.

Given $x' \in \text{X}$, such that $H_{dist}(x,x') = H_{dist}(c,c') > t_{sh}$ and

$$
\begin{aligned}
&F_k(c',x') = F_k(c,x) \\
&\alpha^{c'}\beta^{x'} = \alpha^{c}\beta^{x} \pmod p
\end{aligned} \tag{11}
$$

There, one can compute the discrete logarithm problem $\dfrac{c'-c}{x-x'} \rightarrow \log_\alpha \beta \pmod p$ and the inverse of $(x - x')$ exists, which contradiction to the assumption of discrete logarithm problem.

5 Application of the proposed scheme in biometric systems

In this Section, we will present the biometric cryptosystem based proposed scheme using iris –based biometric. The implementation of the developed scheme involves the system initialization phase, the enrolment phase and the authentication phase. Detailed steps of these phases are described as follows and are in Figure 1.

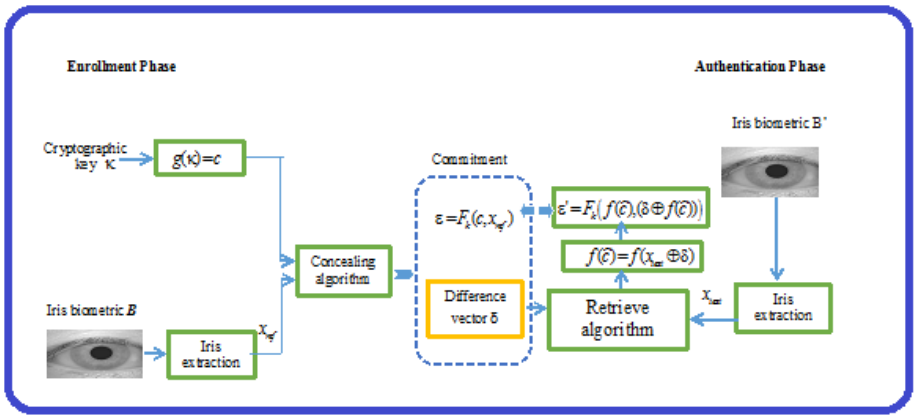

Figure 1: The Proposed Biometric Cryptosystem

5.1 Initialization system phase

In the system initialization phase, the commonly required parameters will generate as described below in algorithm 1.

Algorithm 1:

Input: Security parameter encoded by unary 1^k.

- Generate randomly two prime numbers q and p of length k, such that $p = 1 \pmod{q}$.
- Generate an element α of the subgroup G_q as follows
  - Choose randomly $1 \le a \le p-1$
  - Compute $\alpha = a^{\frac{p-q}{2}} \neq 1 \pmod{p}$
- Generate an element β of the subgroup G_q as follows
  - Choose randomly $1 \le b \le q-1$
  - Compute $\beta = \alpha^b \neq 1 \pmod{p}$

Output: Parameters p, q, α, and β.

5.2 Enrolment Phase

At the start of enrolment phase in the proposed system as described in algorithm 2, the user input iris biometric B is acquired, feature extraction is performed using the algorithm reported in [Michael et al., 2010], and output a 4096-bit iris code, we use the first 4095-bit to represent the reference iris code x_{ref} of the specified user. Concurrently, a random cryptographic key $\kappa \in \{0,1\}^k$ is chosen prepared using a $BCH(4095,k)$ error correction encoded function $g : \{0,1\}^k \rightarrow C$. The result is a

codeword $c \in \mathrm{BCH}(4095, k)$, is then combined with reference iris code x_{ref} (both bit-streams are of length 4095) as an inputs of so-called concealing algoritm to produce the crisp commitment and the difference vector.

Algorithm 2:

Input: Iris biometric B and the cryptographic key κ.

- Iris code x_{ref} extracted from Iris biometric data B.
- A cryptographic key κ is prepared using *BCH* codes and the result is a codeword c.
- Compute the difference vector $\delta = x_{ref} \oplus c$
- Compute the crisp commitment $\varepsilon = F_k(c, x_{ref})$.

Output: (ε, δ)

5.3 Authentication Phase

During the authentication phase as described in algorithm 3. The user input iris biometric B is acquired, feature extraction is performed using the algorithm reported in [Michael et al., 2010] resulting in a 4095-bits test iris code x_{test}. The test iris code x_{test} is used within so-called retrieval algorithm is "exclusive OR" denoted by "$\oplus$" to extract the codeword $c' = x_{test} \oplus \delta = (x_{test} \oplus x_{ref}) \oplus c$.

Once c' is extracted, the error correction decoded function of $BCH(4095, k)$ is used to compute $f(c') = f(x_{test} \oplus \delta)$. Then, $f(c')$ is used within so-called translating algorithm to compute $x'_{test} = \delta \oplus f(c') = x_{ref} \oplus (c \oplus f(c'))$.

Non-valid user will receive a codeword $f(c')$, such that $H_{dist}(f(c'), c) > t_{sh}$. To check whether x_{test} represented the valid person, $\varepsilon' = F_k(f(c'), x'_{test})$ is computed and matches against the stored ε. If $\varepsilon' = \varepsilon$, Then the sample x_{test} is accepted and the cryptographic $\kappa = g^{-1}(f(c'))$ is released. Otherwise the user is rejected.

Algorithm 3:

Input: Iris biometric B and fuzzy commitment $y = (\varepsilon, \delta)$.

- Iris code x_{test} extracted from iris biometric B.
- Compute the codeword $f(\hat{c}) = f(x_{test} \oplus \delta)$.
- Compute $x'_{test} = \delta \oplus f(\hat{c})$
- Compute $\varepsilon' = F_k\left(f(\hat{c}), x'_{test}\right)$.
- Decision making against $\varepsilon' \stackrel{?}{=} \varepsilon$.

Output: The user is authenticated or rejected.

6 Experimental Results and Discussion

In this Section, we report an evaluation of the proposed system implementation against CASIA Iris-Ver1 database (CASIA). The proposed system was implemented as an experimental trial, written entirely in MATLAB® 7.7.0.471 (R2008b). For the performance evaluation of the proposed scheme an iris database, we used consists of 490 iris samples from 70 different samples, with 7 samples from each eye. We use to compute the Hamming distance between two iris codes A and B as

$$H_{dist} = \frac{1}{n}\sum_{i=1}^{n}(code(A_i) \oplus code(B_i)), \tag{12}$$

where $code(A_i)$ and $code(B_i)$ are the i[th] bit in iris codes of person A and B, respectively.

The intra-class Hamming distances are computed by chosen an iris samples from the same eyes and the inter-class Hamming distances by chosen samples from different eyes. We carried out 1470 comparisons for the same eye and 118,335 comparisons between different eyes. The result of the distributions of the intra-class and inter-class Hamming distances is shown in Figure 2. This makes our scheme's performance less as we have to handle more error bits in the iris codes.

The most important measurements of the biometric system are False Acceptance (FA) and False Rejection (FR) rates. The False Acceptance rate is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. The False rejection rate is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user.

In Figure 3, the False Acceptance (FA) and the False Rejection (FR) rates of the whole system are plotted. Table 1 shows that the proposed scheme can cope up to 21.41% percent of error bits within an iris code, and can generate up to 98 bits of the cryptographic key from the iris codes. The corresponding the FR and the FA rates equal to 28.33% and 1.16%, respectively. This performance of the proposed system is more efficient compared with [Tong et al., 2007; Lu et al., 2009] and is not very satisfying when it compared with the results of other biometric cryptosystems [Hao et al., 2006; Bringer et al., 2009; Rathgeb and Uhl, 2009], because the extracted iris

codes handle high bit-error rates. In addition, the proposed biometric cryptosystem is still reached setting up a border for being capable of correcting a total number around of 877 bits errors and hence it's effective and promising. Table 2 shows the comparison performance of the proposed system with the biometric cryptosystems [Hao et al., 2006; Bringer et al., 2009; Rathgeb and Uhl, 2009; Tong et al., 2007; Lu et al., 2009]. The proposed system is required two modular computations to compute the commitment, which is slower than these biometric cryptosystems. But many Government Information Technology (IT) systems need to employ well-established cryptographic schemes to protect the integrity and confidentiality of their data that they process, such as e-passport, e-commerce and e-backing.

Threshold	**FR rate**	**FA rate**
0.0000	1.0000	0.0000
0.1247	0.8888	0.0000
0.1701	0.6272	0.0000
0.1873	0.5166	0.0006
0.2141	**0.2833**	**0.0116**
0.2176	0.2611	0.0395
0.2342	0.1888	0.1565
0.2420	0.1667	0.2589
0.2459	0.1556	0.3188
0.2498	0.1333	0.3678

Table 1: The FA, and the FR rates of the Proposed Biometric

	Biometric char	Error correction code	Complexity of the algorithm	Cryptography key length(bit)	Sample siz	FA/FR rates (%)
[Hao et al., 2006]	Iris	Hadamard and Reed-Solomon	MD5	140	70	0/0.47
[Rathgeb and Uhl, 2009]	Iris	Hadamard and Reed-Solomon	SAH-1	128	100	0/4.64
[Bringer et al., 2009]	Iris	Reed–Muller	---	40	No-ideal images	0/5.62
[Lu et al., 2009]	Face	BCH	SHA-256	36	68	0/30
[Tong et al., 2007]	Fingerprint	--	---	----	---	0.1/ 78
[Fave et al., 2015]	Finger Vien	Product Codes	----	---	60	0.01/4.3
[Hoang et al., 2015]	Gait	BCH	SHA	139	38	0/16.2
[Sasa et al., 2017]	Iris	Reed Solomom	----	400	----	0/3.75
Proposed system	Iris	BCH	DLP	98	70	1.16/28.3

Table 2: Comparison between the proposed system and some biometric cryptosystem

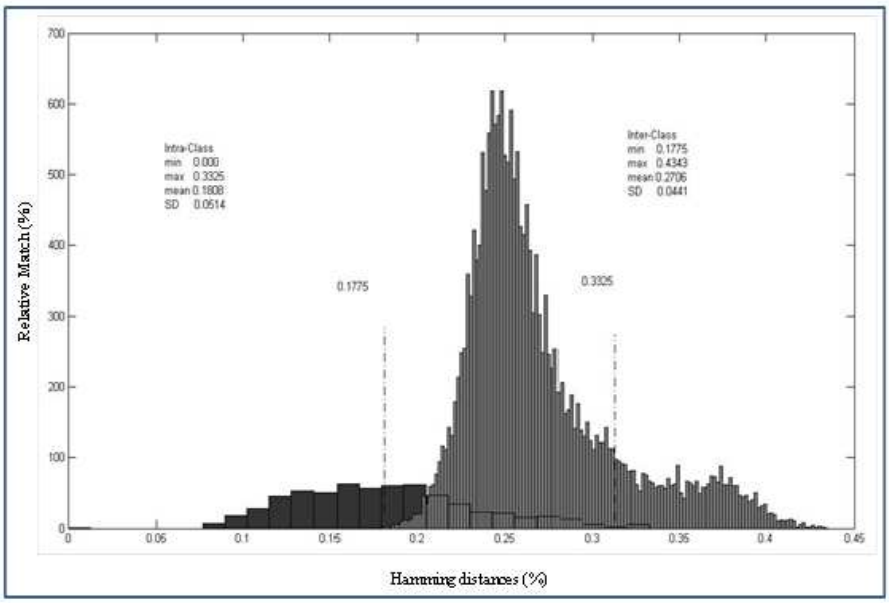

Figure 2: The Inner and Outer Hamming distance distributions

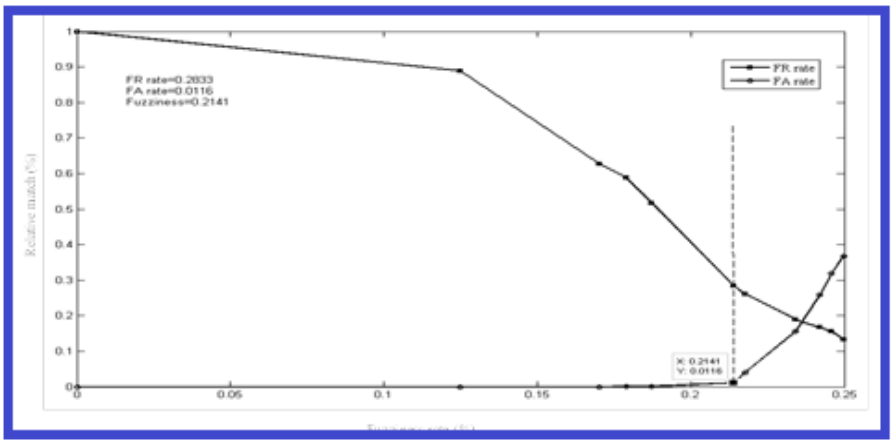

Figure 3: The FR and the FA rate of the Proposed Biometric Cryptosystem

7 Conclusion and Future work

This paper presents a secure cryptographic authentication scheme based on the discrete logarithm problem. In method treats the problem of combining cryptography and biometrics. Through the security analysis of the proposed scheme, we showed that the security characteristics of the proposed scheme relative to the properties of the discrete logarithm problem. Based on the proposed scheme, we construct biometric cryptosystem based on the proposed scheme. The proposed system evaluated using CASIA iris database from 70 different eyes, with 7 samples of each eye. Experimental results demonstrate that the proposed system is more effective, promising in terms of cope up to 21.41% percent of error bits within an iris code, and can generate up to 98 bits of the cryptographic key from the iris codes. Furthermore, the performance rates of the proposed biometric cryptosystem are relatively high compared with the related biometric cryptosystems because of the relatively high bit-error rates, above than 877 errors occurred in each iris codes. However, it needs more efforts in enhancing the iris codes for better performance as a future work.

Acknowledgment

The author would like to thank King Fahd University of Petroleum and Minerals for supporting this research.

References

[Biham et al., 2005] Biham, E., Chen, R., Joux, A., Carribault, P., Lemuet, C., Jalby, W.: "Collision of SHA-0 and reduced SHA-1", In R. Cramer (ed) EUROCRYPTO'05, LNCS, 3494, (2005), 36-57.

[Bringer et al., 2009] Bringer, J., Chabanne, H., Cohen, G., Kindarji, B., Źemor, G.: "Optimal iris fuzzy sketches", In Proc 1st IEEE Int Conf on Biometrics: Theory, Applications, and Systems, (2009),1-6.

[Dobbertin, 1996] Dobbertin, H.: "The Status of MD5 after recent attack," CryptoBytes 2, 2(1996), 1-6.

[Fave et al., 2015] Favre, M., Picard, S., Bringer, J., Chabanne, H.: "Balancing is the key: Performing finger vein template protection using fuzzy commitment", In IEEE International Conference on Information Systems Security and Privacy (ICISSP), (2015), 1-8.

[Gomez-Barrero et al., 2017] Gomez-Barrero, M., Maiorana, E., Galbally, J., Campisi, P., Fierrez, J.: „Multi-biometric template protection based on Homomorphic Encryption"' Pattern Recognition, 67, (2017), 149-163.

[Hao et al., 2006] Hao, F., Anderson, R., Daugman, J.: "Combining cryptography with biometrics effectively", IEEE Trans. on Computing, 55,9(2006), 1081-1088.

[Hoang et al., 2015] Hoang, T., Choi, D., Nguyen, T.: "Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme", International Journal of Information Security, 14, 6 (2015), 549-560.

[Ignatenko and Willems, 2009] Ignatenko, T., and Willems, F.: "Achieving secure fuzzy commitment scheme for optical pufs", In Proceeding of Int Conf on Intelligent Information Hiding and Multimedia Signal Processing, (2009),1185-1188.

[Ignatenko, 2010] Ignatenko, T., "Information Leakage in Fuzzy Commitment Schemes", IEEE Transaction on Info. Forensics and Security 5,2(2010), 337-348.

[Jain et al., 2005] Jain, A., Ross, A., and Uludag, U.: "Biometric template security: Challenges and solutions", In proc. of European Signal Processing Conf., (2005).

[Jain et al., 2008] Jain, A., Nandakumar, K., Nagar, A.: "Biometric template security", EURASIP Journal on Advances in Signal Processing, 17(2008).

[Jin et al., 2016] Jin, Z., Teoh, J., Goi, M., Tay, H.: „Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation“, Pattern Recognition, 56, (2016) 50-62.

[Juels and Sudan, 2006] Juels, A., and Sudan, M.: "A Fuzzy Vault Scheme," Designs, Codes and Cryptography, 38,2(2006), 237-257.

[Juels and Wattenberg, 1999] Juels, A., and Wattenberg, M.: "A fuzzy commitment scheme", In Proc. 6th ACM Conf. Computer and Communications Security, G. Tsudik, Ed., (1999), 28–36.

[Klima, 2006] Klima, V.: "Tunnels in Hash Functions: MD5 collisions within a minute," IACR ePrint archive, http://eprint.iacr.org/2006/105.pdf, (2006).

[Lakhera et al., 2016] Lakhera, M., Rauthan, S., Agarwal, A.: "An Efficient Cryptographic Algorithm for Securing Biometric Template Using AES and Scrambling the Pixels of Row and Column“, In IEEE Int. Conf. Micro-Electronics and Telecommunication Engineering (ICMETE), (2016), 228-231.

[Li et al., 2012] Li, P., Yang, X., Qiao, H., Cao, K., Liu, E., Tian, J., "An effective biometric cryptosystem combining fingerprints with error correction codes", Expert Systems with Applications, Elsevier. 39(2012), 6562–6574.

[Lu et al., 2009] Lu, H., Martin, K., Bui, F., Plataniotis, K., Hatzinakos, D.: "Face recognition with biometric encryption for privacy-enhancing self-exclusion", In Proc. of the16th Int Conf on Digital Signal Processing (2009).

[Mai et al., 2017] Mai, G., Lim, H., Yuen, C.: „Binary feature fusion for discriminative and secure multi-biometric cryptosystems“, Image and Vision Computing, 58, (2017), 254-265.

[McGuffey et al., 2015] McGuffey, C., Liu, C., Schuckers, S.: "Hardware Accelerator Approach Towards Efficient Biometric Cryptosystems for Network Security“, Journal of computing and information technology, 23, 4 (2015), 329-340.

[Menezes et al., 1996] Menezes, A., Paul, C., Vanstone, S.: "Handbook of applied cryptography", CRC press, (1996).

[Michael, 2010] Michael, B., Dragos, C., Francis, G., Thomas, P., William, S.: "Iris Recognition", M.Sc. Thesis, Computing Science Group Project, Imperial College London, (2010).

[Moon, 2005] Moon, K., "Error Correction Coding, Mathematical Methods and Algorithms", John Wiley & Sons, Inc., (2005).

[Nandakuma, 2010] Nandakuma, V.: "A fingerprint cryptosystem based on minutiae phase spectrum", In Proc. of IEEE Workshop on Information Forensics and Security (2010).

[NIST, 2007] NIST (National Institute of Standards and Technology), SHA-3 Competition. http://csrc.nist.gov/groups/ST/hash/timeline.html, (2007).

[Preneel, 1999] Preneel, B., "The stat of cryptographic hash functions", In Lectures on Data Security: Modern Cryptology in Theory and Practice, LNCS, Berlin: Springer 1561 (1999), 158-192.

[Preneel, 2009] Preneel, B., "The State of Hash Functions and the NIST SHA-3 Competition (Extend abstract)", Information Security and Cryptography, LNCS, 5487, (2009), 1-11.

[Ratherb et al., 2013] Ratherb, C., Andreas, U., Peter, W.: "Iris-biometric fuzzy commitment schemes under image compression", In Proc. of Iberoamerican Congress on Pattern Recognition. Springer Berlin Heidelberg, (2013), 374-381.

[Rathgeb and Uhl, 2009] Rathgeb, C., and Uhl, A.: "Systematic construction of iris-based fuzzy commitment schemes", In Proc of the 3rd Int Conf on Biometrics, LNCS, 5558(2009), 947-956.

[Rathgeb and Uhl, 2010] Rathgeb, C., and Uhl, A.: "Adaptive fuzzy commitment scheme based on iriscode error analysis", In Proc of the 2nd European Workshop on Visual Information Processing, (2010), 41-44.

[Rathgeb et al., 2012] Rathgeb, C., Andreas, U., Peter W.: "Iris biometrics: from segmentation to template security", Springer Science & Business Media, 59 (2012).

[Rathgeb, and Uhl, 2011] Rathgeb, C., and Uhl, A.: "A survey on biometric cryptosystems and cancelable biometrics", EURASIP Journal on Information Security. 3(2011),1-25.

[Sarier, 2018] Sarier, N. D.: „Multimodal biometric Identity Based Encryption“, Future Generation Computer Systems, 80, (2018), 112-125.

[Sasa et al., 2017] Sasa, A., Milosavljevic, M., Veinovic, M., Sarac, M., Jevremovic, A.: "Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics", IET Biometrics, 6, 2(March 2017), 89-96.

[Teoh and Kim, 2007] Teoh, A., and Kim, J., "Secure biometric template protection in fuzzy commitment scheme," IEICE Electron Express, 4, 23(2007), 724-730.

[Tong et al., 2007] Tong, V., Sibert, H., Lecoeur, J., Giraut, M.: "Biometric Fuzzy Extractors Made Practical: A Proposal Based on FingerCodes", In proc. of International Conference, Seoul, Korea, LNCS, 4642, (2007) 604-613.

[Vander et al., 2006] Vander, M., Kevenaar, T., Schrijen, G., Akkermans, T., Zuo, F.: "Face biometrics with renewable templates", In Proc on Security, Steganography, and Watermarking of Multimedia Contents, 6072, (2006), 205-216.

[Wang and Yu, 2005] Wang, X., and Yu, H.: "How to Break MD5 and other Hash Functions", In Carmer, R. (ed) EUROCRYPT'05, LNCS, 3494, (2005), 19-35.

[Wang et al., 2005a] Wang, X., Yao, A., Yao, F.: "Cryptanalysis of SHA-1 Hash Function, Technical Report", National Institute of Standard and Technology (NIST), Available at http://csrc.nist.gov/groups/ST/hash/documents/Wang_SHA1-New-Result.pdf, (2005).

[Wang et al., 2005b] Wang, X., Yin, L., Yu, H.: "Finding Collisions in the full SHA-1", In Proc. V. Shoup (ed) CRYPTO'05, LNCS, 3621, (2005), 17-36.

[Zhang et al., 2009] Zhang, I., Sun, Z., Tan, T., Hu, S.: "Robust biometric key extraction based on iris cryptosystem", In Proc of the 3rd Int. Conf. on Biometrics, LNCS, 558(2009),1060-1070.