Research Article

Secure Method for Biometric-Based Recognition with Integrated Cryptographic Functions

Shin-Yan Chiou

Department of Electrical Engineering, Chang Gung University, 259 Wen-Hwa 1st Road, Kwei-Shan, Taoyuan 333, Taiwan

Correspondence should be addressed to Shin-Yan Chiou; ansel@mail.cgu.edu.tw

Received 30 January 2013; Accepted 22 April 2013

Academic Editor: Zhirong Sun

Copyright © 2013 Shin-Yan Chiou. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Biometric systems refer to biometric technologies which can be used to achieve authentication. Unlike cryptography-based technologies, the ratio for certification in biometric systems needs not to achieve 100% accuracy. However, biometric data can only be directly compared through proximal access to the scanning device and cannot be combined with cryptographic techniques. Moreover, repeated use, improper storage, or transmission leaks may compromise security. Prior studies have attempted to combine cryptography and biometrics, but these methods require the synchronization of internal systems and are vulnerable to power analysis attacks, fault-based cryptanalysis, and replay attacks. This paper presents a new secure cryptographic authentication method using biometric features. The proposed system combines the advantages of biometric identification and cryptographic techniques. By adding a subsystem to existing biometric recognition systems, we can simultaneously achieve the security of cryptographic technology and the error tolerance of biometric recognition. This method can be used for biometric data encryption, signatures, and other types of cryptographic computation. The method offers a high degree of security with protection against power analysis attacks, fault-based cryptanalysis, and replay attacks. Moreover, it can be used to improve the confidentiality of biological data storage and biodata identification processes. Remote biometric authentication can also be safely applied.

1. Introduction

Various aspects of everyday life are gradually being digitized as our life experiences and creative efforts are accumulated in personal computers, digital media devices, and mobile devices. People use passwords and other authentication methods to protect these collections of personal and potentially confidential information. Traditional confidentiality and authentication methods (e.g., personal passwords) are less than secure. In addition to requiring the user to remember a variety of passwords, which can result in user error, passwords can be stolen and pure password authentication is vulnerable to unauthorized breach. However, these problems can be resolved through the use of “physiological passwords” through unique personal biometric identification methods such as recognition of the user’s face, fingerprints, personal signature, or iris, which are very difficult to either replicate or steal. Therefore, several biometrics-based remote user authentication schemes [1–9] have been designed.

In general, however, traditional biometric identification methods only allow for direct comparison via a proximal end-user device and cannot be combined with cryptographic techniques. As long as biometric techniques allow for a degree of tolerance for error, the data are subject to disruption, rendering it impossible to accurately compare the scanned input with the original sample. In addition, registering the biometric feature values of the original biometric data to the biometric device for certification may encounter the following threats.

- (1) Hackers could crack the registered biometric feature data stored on the biometric device.
- (2) During matching, biometric data has a tolerance for error, making it impossible to use more secure means of encryption such as hash functions to protect biometric data, thus potentially allowing attackers to monitor private biometric data during the process of remote authentication.

In 2002, Lee et al., [1] proposed a type of remote authentication method based on fingerprints and smart cards. However, this method required precise system time synchronization. Later, in 2003, Kim et al., [10] proposed an ID-based authentication system integrating smart cards, passwords, and fingerprints. This system, however, was vulnerable to power analysis attacks [11] or fault-based cryptanalysis [1, 12]. At the same time, Scott [13] showed how this system was vulnerable to replay attacks.

In 2010, Li and Hwang [7] proposed a biometrics-based remote user authentication scheme using smart cards. However, in 2011, Das [8] pointed out that their scheme is insecure due to the security drawbacks in password change phase and in verification of biometrics and proposed another improved scheme which provides mutual authentication and is secure against attacks of server masquerading, parallel session, and the stolen password. However, in 2012, An [9] showed that Das's scheme [8] does not provide mutual authentication and is vulnerable to various attacks and proposed enhanced scheme to solve their security problems.

This paper presents a new secure authentication method applying cryptographic techniques to biometric feature. The proposed method combines the advantages of biometric identification and cryptography. By adding a subsystem to existing biometric systems, the proposed approach achieves the high security of cryptographic techniques and the tolerance for error of biometric recognition.

For example, this method can be combined with dual-factor biometric and cryptographic identification to achieve security. This not only simultaneously provides biometric and cryptography authentication but also during the authentication process protects the biometric data through cryptographic encryption (e.g., hash). This method provides a high degree of security and is resistant to power analysis attacks, fault-based cryptanalysis, and replay attacks. Because the proposed method can be combined with cryptographic techniques, the biometric authentication can also apply cryptography techniques to ensure secure remote biometric matching.

Once the method has been integrated, if an attacker seeks to force access to obtain the database's presaved biometric feature data, the attacker can only get access to the hashed or encrypted confidential information. By applying this method, biometrics can be combined with a cryptographic system thus enhancing the secure storage and use of biological feature data and effectively preventing malicious programs or attackers from stealing the biometric values or posing as legitimate users.

The proposed method combines biometrics matching to achieve cryptographic functions, such as encryption, authentication, identification, signature, hash, and key generation, which can be used in banks to replace IC cards, seals, and other means of dual identification, thus ensuring privacy, integrity, nonrepudiation, and so forth. These technologies can be implemented through hardware or software applications and combine biometric systems in current use. Thus, the contributions of the proposed method are as follows.

- (1) Simultaneously achieve the functions of cryptography technology and biometric recognition.
- (2) Cryptography operations for biometric data encryption, signatures, and so forth.
- (3) Error tolerance in biometric data matching.
- (4) Easily integrated into existing biometric systems.
- (5) Strengthens the confidentiality of biometric data storage. Even if an attacker accesses the registered biometric data stored in the biometric device, he will be unable to decrypt the biometric data or impersonate an authorized user.
- (6) Strengthens the confidentiality of biological information in the recognition process. Even if an attacker intercepts data during the biometric matching process, he will be unable to decrypt the biometric data or impersonate an authorized user.
- (7) Reduces vulnerability to power analysis attacks, fault-based cryptanalysis, and replay attacks.
- (8) Can be safely used to maintain confidentiality in remote biometric authentication. Even if an attacker eavesdrops during the remote authentication process, he will be unable to access biometric data or impersonate an authorized user.
- (9) Combines biometric recognition with cryptography technology but does not influence the error accept rate (EAR) or error reject rate (ERR) of the original biometric recognition.

1.1. Difference between Biometric Recognition and Cryptography Authentication. Biometric systems refer to the use of biometric recognition technology to authenticate a person's identity through his or her unique biological characteristics (e.g., fingerprints, palm prints, iris, personal signature) in lieu of a password. This approach can thus authenticate the user's identity without requiring the user to remember multiple passwords. This authentication method usually first obtains a threshold range to discriminate between acceptable and unacceptable inputs. However, repeated use, improper storage, or transmission leaks may compromise security.

The difference with cryptographic technology is that these authentication ratios do not need to achieve 100% accuracy. That is, a certain degree of error in data matching is tolerated. (Biometric and cryptography authentication methods are compared in Table 1.)

2. Related Work

2.1. Traditional Biometric Methods. As shown in Figure 1, the processes of traditional biometric methods include the following subsystems: (1) data collection, (2) signal processing, (3) biometric feature extraction, (4) biometric feature registration/biometric feature input, and (5) matching and decision (i.e., comparing biometric features to determine whether they match). Generally speaking, one needs to first register/store biometric feature data (in the registration phase) for matching. Once this is completed, the biometric device

FIGURE 1: The processing of a conventional biometric method.

allows the user to input his or her biometric feature data (in the matching phase) for comparison of the biometric features against those in the registration phase (in the compare biometric feature function) to determine if they match. If the biometrics of the prestored biometric features in the registration phase and those in the matching phase inputted by the user are found to match, then the device outputs a recognition result of “Authentication Successful.” Otherwise, the biometric device outputs a recognition result of “Authentication Failed.” Generally speaking, the steps in the registration phase and in the matching phase are processed similarly. For example, the matching phase is divided into the following steps: data collection, signal processing, biometric feature extraction, and biometric feature input. In terms of biometric feature matching, for the matching of the biometric feature registration data and the biometric feature input data, biometric authentication usually determines acceptability based on a threshold value.

Biometrics differs from cryptographic techniques in that, for biometric authentication, the ratio of credential matching does not need to be 100%; that is, the match between the two data sets can tolerate a certain degree of error. For example,

TABLE 1: Comparison between biometrics recognition and cryptography authentication.

	Cryptography authentication	Biometrics recognition
Authentication method	Digital	Analog
Authentication rule	Without error tolerance	With error tolerance
Data processing	Data is disordered	Data is processed but not disordered
Adoption of cryptography technique	Data can be encrypted and signed	Data cannot be encrypted or signed

suppose a registered biometric feature of 35 and a threshold value of 5, if the inputted biometric feature is within the range of 30 to 40, it is considered a biometric match with the registered biometric feature. However, if the biometric data is below 30 or exceeds 40, it is determined to be inconsistent with the registered feature values. In cryptographic

FIGURE 2: Structural matching methods.

authentication, if the registered password is 35 and the input value is 37, the input is considered to be inconsistent with the registered password, and the only allowable match would be an input value of 35.

As shown in Figure 1, the biometric processing device integrated with cryptographic technology consists of the following five parts: (1) data collection subsystem, (2) signal processing subsystem, (3) biometric feature extraction subsystem, (4) biometric feature registration/input subsystem, and (5) matching and decision subsystem.

(1) Data Collection Subsystem

The data collection subsystem collects the registered biometrics (e.g., fingerprints, facial image, iris image) for matching with the input biometric. The subsystem generally uses a biometric sensor to read one or more aspects of the subject's biometric data.

(2) Signal Processing Subsystem

The signal processing subsystem reads the biometrics and processes them through actions such as Gaussian smoothing, histogram equalization, normalization, binarization, opening, thinning, thinning repair, and feature point retrieval.

(3) Biometric Feature Extraction Subsystem

A given biometric consists of many types of features such as the terminal and bifurcation points of fingerprint minutiae. General algorithms are used to retrieve the terminal and bifurcation points for feature matching. The biometric feature extraction subsystem is used to match the feature points or feature values of the retrieved biometric features.

(4) Biometric Feature Registration/Input Subsystem

The biometric feature registration subsystem stores the processed biometric features for future identification. The biometric feature input subsystem stores the inputted and processed biometric features for comparison in next step.

TABLE 2: Eight types of fingerprint minutiae.

Terminal	Bifurcation	Short ridge	Crossover
Spur	Dot	Island	Bridge

(5) Matching and Decision Subsystem

The matching and decision subsystem matches the inputted and processed biometric features with the registered biometric features stored in the database. If the match meets the required conditions, the match is validated.

2.2. Fingerprint Recognition. Biometric identification can be accomplished through the recognition of various characteristics including fingerprints and palm prints. Fingerprint minutiae are composed of the fine geometric features created by fingerprint ridges. Early on, Galton proposed identifying fingerprints based on four types of features: the beginnings and ends of ridges, forks, islands, and enclosures. However, Hrechak and Mchugh later proposed the use of eight minutiae: terminals, bifurcation, short ridges, crossovers, spurs, dots, islands, and bridges (see Table 2).

Fingerprint recognition uses minutiae-matching algorithms such as the alignment-based matching algorithm [14], the Gabor filter-based approach [15], and the structural matching algorithm [16–19]. Among these, the structural matching algorithm (see Figure 2) is roughly divided into two stages. The first stage uses local feature matching to identify a central feature point with a positioning effect, while the second stage compares all the features at this central point and calculates a matching score.

2.3. Biometric-Based Cryptographic Key Generation. Chang et al. [20] proposed using a collected number of biometrics as a training sample to achieve “biometric-based cryptographic key generation.” As shown in Figures 3 and 4, this method uses multiple biometrics (including those for legitimate users) to find a conversion set through a mechanism which identifies highly distinguishing features. This allows each one-dimensional feature of the postbiometric conversion to effectively distinguish between legitimate and illegitimate users. The average features of legitimate users are then used to authenticate the identity of the legitimate user as a mechanism for generating multibyte passwords. (This group conversion must be stored in the biometric database.) However, this approach must be applied to the biometric data of multiple users to achieve differentiation. Also, because the error value calculation is determined based on the mean and variance of each biometric, therefore each user must provide multiple biometric samples to generate the associated means and variances.

2.4. Fuzzy Extractors. Dodis et al. [21] proposed a cryptographic key generation mechanism called fuzzy extractors. This system uses biometric values and self-selected authentication values as input data. During recognition, it uses a cryptographic key and self-selected authentication values to recognize biometric values within a set error range. Furthermore, this system can use cryptographic keys and input biometric values (within a predetermined error range) to restore the original biometric values.

As shown in Figure 5, this method first selects an authentication value x and then uses the Gen function, with x and the registered biometric value w to generate a key v as follows:

$$\text{Gen}: v = w \oplus C(x), \quad (1)$$

where $C(\cdot)$ is the encoding function of a type of error correction code (e.g., Hamming code).

Next, within an error range t , using the Rep function causes v and x to recognize the inputted biometric value w' (where distance $(w, w') \leq t$). The Rep function is as follows:

$$\text{Rep}: D(w' \oplus v) = x, \quad (2)$$

where $D(\cdot)$ is a type of error correction decoding function.

In case the original biometric value w is lost, w can be restored through inputting biometric value w' of the cryptographic key v and the error range t through the Rec function. The Rec function is as follows:

$$\text{Rec}: \text{Rec}(w', v) = v \oplus C(D(w' \oplus v)) = w. \quad (3)$$

However, this method cannot be integrated into current biometric systems. Moreover, this method's operating system not only requires the use of key v and authentication value x to perform authentication (and thus requires the storage of key v), but this comparison method is also vulnerable to leaking biometric value w (through the use of biometric value w' and key v).

FIGURE 3: Structure of cryptography key generation based on biometric features.

2.5. Application to Combine Iris Recognition and Cryptography. Hao et al., [22] proposed an application combining iris recognition and cryptography (see Figure 6). The concept for this method is similar to that of the fuzzy extractor in that they both use an error control code to accept biometric values within a range of errors.

This system first uses a cryptographic key κ and the iris biometric value θ_{ref} to obtain the authentication value θ_{lock} and stores θ_{lock} and the key's hash value $h(\kappa)$ in the IC card, based on the following relationship:

$$\theta_{\text{lock}} = \theta_{\text{ps}} \oplus \theta_{\text{ref}}, \quad (4)$$

where θ_{ps} is the value for the key κ via RS and Hadamark coding.

During recognition, the XOR value of θ_{lock} and the inputted iris biometric value θ_{sam} can be decoded as κ' through RS and Hadamark decoding to determine if $h(\kappa')$ is equal to $h(\kappa)$. If the difference between the inputted iris biometric value θ_{sam} and the original iris biometric value θ_{ref} is less than or equal to a tolerable error range of the error control code, thus the input will be decoded as the original κ value and considered correct.

However, this method is only suitable for iris matching and cannot be directly combined with existing systems. The RS code is used as a means to calculate network transmission errors for each byte, which differs from error calculation methods in other biometric environments.

3. Proposed Scheme

This paper presents a secure cryptography-integrated biometric recognition method with cryptographic functions. This method is able to integrate biometric matching with cryptographic technology to achieve dual-factor authentication. This integrated technology can also be combined with more advanced cryptographic techniques to produce more secure and diverse applications. The proposed method is divided into two parts for description purposes. The first part is basic process of improved biometric security (IBS), while the second part is advanced process of integrated cryptographic technology (ICT).

The IBS process is divided into two phases: the registration phase and the matching phase. The registration phase first provides a set of biometric data. Based on a threshold value t , we define several numerical ranges, each of which has a quantization value. If the biometric data fall within one of these numerical ranges, then the quantized value for that numerical range is used as a quantized feature data to replace the biometric feature data. Next, one-way function operations are used to convert the quantized feature data to hashed feature data (H_F). Then, the difference between the quantized

FIGURE 4: Example of cryptography key generation mechanism.

FIGURE 5: Fuzzy extractor.

feature data and the biometric data is calculated to obtain an adjustment value (V_{AD}). Finally, this adjustment value V_{AD} is stored with the hashed feature data H_F .

Matching phase and registration phase are largely similar. First we provide a registered hashed feature data H_F and adjustment value V_{AD} , and the biometric data is then captured. The biometric data is adjusted based on this adjustment value V_{AD} . Next, (similarly) based on the threshold value t , multiple numerical ranges are defined, each of which is a quantized value. If the adjusted biometric data fall within one of the numerical ranges, then the quantized value of this value range is taken as the quantized feature to replace the adjusted biometric data. This is followed by one-way function operations to convert the quantized feature into hashed feature data H'_F . Finally, the registered hashed data H_F is compared with the hashed feature data H'_F .

In the ICT process, the biometric data must first go through IBS process before it can be used in this process. This process integrates the cryptography technology for signature application using the biometric data, which is composed of the “registration” and “signature and verification” stages. The application provides biometric-based cryptographic fields for the signatory and the verifier.

Before describing the processes of IBS and ICT, we define the notations used in our proposed protocol in Table 3.

3.1. Process of Improved Biometric Security (IBS). To improve the security of storage of biometric feature data, biometric feature values must first be processed before being integrated

TABLE 3: Notations.

Notations	Meaning
t	Threshold value
p	The interval of the quantitative mode
w/w'	Biometric feature extraction data
w_q/w'_q	Data after value quantization
w_a	Fine-tuned values
ID_A	The ID of user A
PK_A	The public key of user A
W_E	Internal registered biodata to be recognized
W_I	Input biodata for matching the internal biodata
$W_E^{(j)}/W_I^{(j)}$	W_E/W_I in the stage j
$W_{Ei}^{(j)}/W_{Ii}^{(j)}$	Related data value of the i th point of $W_E^{(j)}/W_I^{(j)}$
$cert_A$	Certificate of user A
time	Validity period of certificate
n_A	Product of two large primes as A 's parameters
$h(\cdot)$	Cryptographic one-way hash function
$\lfloor \cdot \rfloor$	Floor function
$\lfloor \cdot \rfloor_{PK}$	Encryption function using public key PK
$sig_{SK}(\cdot)$	Signature using private key SK

with cryptography technology. This method uses numerical quantization and quantization adjustment processes to ensure that all acceptable values within the threshold are quantified to the same value without compromising security. This quality can use hash or encryption functions to prevent the theft or leakage of the registered data prestored in the database. During matching, the values must be exactly correct in order to pass, thus improving the comparison rate of

FIGURE 6: Iris recognition combining cryptography.

FIGURE 7: Schematic diagram of the processing of the proposed method.

hardware or software. Because some biometric values are quantized to a correct value without error, these values not only can use hash or encryption functions for protection but can also be further applied through other cryptographic techniques or other numerical derivations such as signatures, key generation, and key exchange.

Figure 7 shows a schematic diagram of the biometric processing methods of the proposed cryptography-integrated technology. The processed values can be directly applied to biometric recognition. This processing mode (shown in Figure 7) can be divided into eight parts as follows: (1) data collection subsystem, (2) signal processing subsystem,

(3) biometric feature extraction subsystem, (4) numerical quantization subsystem, (5) adjustment subsystem, (6) hash subsystem, (7) biometric feature registration/input subsystem, and (8) matching and decision subsystem, where (1) the data collection subsystem, (2) the signal processing subsystem, and (3) the biometric feature extraction subsystem are the same as those mentioned in Section 2.1. Thus, below, we limit our explanation to subsystems (4)–(8).

(4) Numerical Quantization Subsystem

The numerical quantization subsystem performs value quantization on the processed signal (as w_q and w'_q).

These quantized values can then be used with cryptographic techniques. Assume that the signal comparison allows for an error range of plus or minus t and a sampling value range between $(0, L)$. Then the interval of the quantitative mode is p , the signal value is quantized as $0, p, 2p, \dots, np$, where $p = 2t$, $n = \lfloor L/p \rfloor$ (where $\lfloor \cdot \rfloor$ is a floor function). If a signal value w between $(0, L)$ satisfies $(kp - p/2) \leq w < (kp + p/2)$, then this signal value w should be quantized as $w_q = kp$. For example, for some signal value $(28, 37, 19, 62, 54)$ and $t = 5$ (i.e., $p = 10$), the signal value is quantized as $(30, 40, 20, 60, 50)$. (Generally speaking, if a biometric value allows an error range of $\pm t$, then $p = 2t$ can be used to obtain the quantization interval.) If the quantized range defined by the threshold is used for quantization, then the ERR and EAR obtained using this method will have no impact.

(5) Adjustment Subsystem

The adjustment subsystem records the fine-tuned value w_a from the quantizing process. This fine-tuned value can be quantized to restore the reduced recognition rate to the original recognition rate without compromising security. The recommended calculation method for the fine-tuned value is $w_a = w_q - w$. For example, given a signal value $w = (28, 37, 19, 62, 54)$ and $p = 10$, the signal value is quantized as $w_q = (30, 40, 20, 60, 50)$, then the adjustment value w_a is $(2, 3, 1, -2, -4)$. Given an inputted value $w' = (24, 33, 21, 66, 58)$, $p = 10$, and the adjustment value $w_a = (2, 3, 1, -2, -4)$, then the adjusted value $w'_p = (26, 36, 22, 64, 54)$ which is quantized as $w'_q = (30, 40, 20, 60, 50)$.

Using the numerical quantization and adjustment process guarantees that all accepted values remain within the threshold value and are quantized at the same level of quality without compromising security. (Given an acceptable error range of plus or minus t , correctly guessing a value between a sampling value $(0, L)$ has a probability of approximately $2t/L$; following quantization, correctly guessing the quantized value between a sampling value of $(0, L)$ has a probability of approximately $1/n$, where $n = \lfloor L/p \rfloor = \lfloor L/2t \rfloor$. The probability of correctly guessing the unquantized value is identical to that of the quantized value; therefore, the quantized action does not compromise security.)

(6) Hash Subsystem

The value w_q produced by the hash function is $h(w_q)$. Using the hash function can maintain biometric confidentiality and prevent leaking or theft of the pre-saved registered feature values stored in the database. Because a hacker would only be able to manage the registered feature data stored in the biometric device, he would be unable to obtain the original biometric value. During comparison, the values must be exactly correct in order to pass, thus improving the hardware or software comparison rate. Other functions (e.g.,

FIGURE 8: Registration phase.

encryption functions) can be used to substitute for this hash function.

(7) Biometric Feature Registration/Input Subsystem

Applied to the proposed method, the stored values for registration are $h(w_q)$ and w_a . This function is similar to the one previously described in Section 2.1.

(8) Matching and Decision Subsystem

Applied to the proposed method, this system's comparison mode determines whether $h(w_q)$ and $h(w'_q)$ are the same. This function is similar to the one previously described in Section 2.1.

Figure 1 shows the processing of a conventional biometric method, while Figure 7 demonstrates schematic diagram of the processing of the proposed method. As shown in Figure 1, a threshold value and a biometric matching method decide the EAR and ERR. We combine threshold and quantization (as shown in Figure 7) to quantify registered and input biodata within threshold to the same value and use biometric matching methods to compare data after hashing these values. Therefore, the hashed values can be applied to cryptography technology, and the combination of biometric recognition and cryptography technology does not influence the EAR or ERR of the original biometric recognition.

3.2. Process of Integrated Cryptographic Technology (ICT). Once the complete quantified features have been hashed (in biometric feature registration subsystem), dual authentication can be achieved through the integration of cryptographic techniques. This method can be separated into a "registration" phase and a "signature and authentication" phase as follows.

3.2.1. Registration Phase. As seen in Figure 8, user A first personally registers with CA and transmits message $\text{reg} = \text{ID}_A, \text{PK}_A, [W_E]_{\text{PK}_A}$ to CA, where ID_A is the ID of user A , PK_A is user A 's public key, W_E is the registered and internally stored biodata to be recognized, and $[W_E]_{\text{PK}_A}$ represents the encrypted signal W_E using the user's public key PK_A . Next, CA's certificate $\text{cert}_A = \text{reg} \parallel \text{time} \parallel \text{sig}_{\text{SK}_{\text{CA}}}(\text{reg} \parallel \text{time})$ is transmitted to user A , where $\text{sig}_{\text{SK}_{\text{CA}}}(M)$ represents the signature of signal M using CA's private key SK_{CA} , and time represents the certificate's validity period.

3.2.2. Signature and Verification Phase. Generally speaking, a single type of biometric comparison may have more than one matching stage (e.g., structural comparison has a dual-stage comparison). Assume that this biometric has two stages,

FIGURE 11: First stage matching content.

process, even if an attacker intercepts data during the process, he will be unable to decrypt the biometric data or impersonate an authorized user.

4.1.3. Reduces Vulnerability to Power Analysis Attacks, Fault-Based Cryptanalysis, and Replay Attacks. Since only $h(w_q)$ and w_a are registered and stored, an attacker will be unable to use power analysis attacks or fault-based cryptanalysis to break the system. Moreover, because different random numbers r_i are used in each matching process (as seen in Figures 9 and 10), even if an attacker eavesdrops during the process, he will be unable to use these data to access biometric data or impersonate an authorized user. Therefore, this system is replay-attack resistant.

4.1.4. Can Be Safely Used to Maintain Confidentiality in Remote Biometric Authentication. As only w_a is transmitted and different random numbers r_i are used to protect biometric data during remote biometric authentication process (as shown in Figures 9 and 10), even if an attacker eavesdrops during the process, he will be unable to access biometric data or impersonate an authorized user.

4.2. Comparison. According to the nine contributions expressed in Section 1, we compare our protocol with the protocols of biometric-based cryptographic key generation (BCKG) [20], fuzzy extractors (FZ) [21], and application to combine iris recognition and cryptography (ACIRC) [22]. The results are summarized in Table 4, where Tech. and (1)–(9), respectively, denote technique and the nine contributions described in Section 1. As seen in Table 4, all schemes offer the error tolerance in biometric data matching (as shown in item (3)) because the main usage of these schemes are in biometric matching. As seen in items (2), (4), (8), and (9), only the proposed scheme provides these functions since our scheme is used to integrate into existing biometric systems with confidentiality and cryptography technologies.

5. Applications of the Proposed Method in Structural Comparison

Some methods for biometric identification are suitable for use in the proposed method (e.g., minutiae matching algorithms such as structural matching algorithm [23, 24], the improved

TABLE 4: Comparison of functions.

Tech.	BCKG	FZ	ACIRC	Proposed scheme
(1)	✓			✓
(2)				✓
(3)	✓	✓	✓	✓
(4)				✓
(5)	✓		✓	✓
(6)	✓		✓	✓
(7)	✓		✓	✓
(8)				✓
(9)				✓

structural matching algorithm [25, 26], and the onion layer algorithm [27–29]).

If the proposed method is used in the structural matching algorithm, the first stage matching content is hashed before matching, and the first stage matching results obtain the optimal core position, which is then used in the second stage matching. Similarly, the second stage matching content can also be hashed before matching. If the quantitative range set by the threshold is used for quantization, then the ERR and EAR will not change with the application of this method. As an example, the structural matching algorithm is applied to the proposed method.

The structural matching algorithm is divided into two stages. The first stage matches local features to identify a core point with the positioning effect. The second stage uses this core point to conduct overall feature matching and obtain a matching score.

For example, assume that the number of feature points of the input and registered fingerprint are n_I and n_E , respectively, and assume that first stage takes five matching data. Then $W_I^{(1)} = W_{I1}^{(1)} || W_{I2}^{(1)} || \dots || W_{In_I}^{(1)}$ and $W_E^{(1)} = W_{E1}^{(1)} || W_{E2}^{(1)} || \dots || W_{En_E}^{(1)}$, where $W_{Ij}^{(1)} = w_{Ij1}^{(1)} || w_{Ij2}^{(1)} || w_{Ij3}^{(1)} || w_{Ij4}^{(1)} || w_{Ij5}^{(1)}$ and $W_{Ej}^{(1)} = w_{Ej1}^{(1)} || w_{Ej2}^{(1)} || w_{Ej3}^{(1)} || w_{Ej4}^{(1)} || w_{Ej5}^{(1)}$. Using the hash function we can let $h_{Ej-1.2.3}^{(1)} = \text{hash}(w_{Ej1}^{(1q)} || w_{Ej2}^{(1q)} || w_{Ej3}^{(1q)})$, $h_{Ej-4}^{(1)} = \text{hash}(w_{Ej4}^{(1q)})$, $h_{Ej-5}^{(1)} = \text{hash}(w_{Ej5}^{(1q)})$ and $h_{Ij-1.2.3}^{(1)} = \text{hash}(w_{Ij1}^{(1q)} || w_{Ij2}^{(1q)} || w_{Ij3}^{(1q)})$, $h_{Ij-4}^{(1)} = \text{hash}(w_{Ij4}^{(1q)})$, $h_{Ij-5}^{(1)} = \text{hash}(w_{Ij5}^{(1q)})$, where $w^{(1q)}$ represents the quantized value of $w^{(1)}$. Then Figure 11 shows the matching of cp_1 and cp_1' .

In the second stage matching, we can let $W_{Ij}^{(2)} = \{\text{hash}(w_{Ij1}^{(2q)}) || \text{hash}(w_{Ij2}^{(2q)}) || \dots || \text{hash}(w_{Ijn_I}^{(2q)}) - \text{hash}(w_{Ijj}^{(2q)})\}$, $W_{Ej}^{(2)} = \{\text{hash}(w_{Ej1}^{(2q)}) || \text{hash}(w_{Ej2}^{(2q)}) || \dots || \text{hash}(w_{Ejn_E}^{(2q)}) - \text{hash}(w_{Ejj}^{(2q)})\}$, where $w_{Ijl}^{(2)}$ and $w_{Ejl}^{(2)}$ are the relationship values between the core point (the j th point) and its neighboring feature point (the l th point) (e.g., type, distance, relationship angle, etc.) for the input fingerprint and the registered fingerprint, respectively, in second stage matching, and $w_x^{(2q)}$ represents the quantized value of $w_x^{(2)}$.

6. Conclusions

This paper proposes a new biometric authentication method with the security of cryptographic technology, simultaneously achieving the functions of cryptographic technology and biometric recognition. This method is very simple to implement through the addition of a subsystem to existing biometric systems. The proposed method offers increased security, with resistance to power analysis attacks, fault-based cryptanalysis, and replay attacks. This method can also strengthen the confidentiality of stored biometric data and recognition processes and also offers secure remote biometric identity authentication. Fingerprint structural matching is presented as an application example for reference of a technical implementation. The proposed concept can be applied to any combination of biometrics and cryptographic techniques to securely exploit the advantages of both technologies.

Acknowledgments

This work was partially supported by the National Science Council under Grant NSC 101-2221-E-182-071 and by the CGURP project under Grant UERPD2B0021. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

- [1] J. K. Lee, S. R. Ryu, and K. Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," *Electronics Letters*, vol. 38, no. 12, pp. 554–555, 2002.
- [2] W. C. Ku, S. T. Chang, and M. H. Chiang, "Further cryptanalysis of fingerprint-based remote user authentication scheme using smartcards," *Electronics Letters*, vol. 41, no. 5, pp. 240–241, 2005.
- [3] M. K. Khan and J. Zhang, "An efficient and practical fingerprint-based remote user authentication scheme with smart cards," in *Information Security Practice and Experience*, vol. 3903 of *Lecture Notes in Computer Science*, pp. 260–268, 2006.
- [4] A. Baig, A. Bouridane, F. Kurugollu, and G. Qu, "Fingerprint-Iris fusion based identification system using a single hamming distance matcher," *International Journal of Bio-Science and Bio-Technology*, vol. 1, no. 1, pp. 47–58, 2009.
- [5] J. Pedraza, M. A. Patricio, A. de Asís, and J. M. Molina, "Privacy and legal requirements for developing biometric identification software in context-based applications," *International Journal of Bio-Science and Bio-Technology*, vol. 2, no. 1, pp. 13–24, 2010.
- [6] C. C. Chang, S. C. Chang, and Y. W. Lai, "An improved biometrics-based user authentication scheme without concurrency system," *International Journal of Intelligent Information Processing*, vol. 1, no. 1, pp. 41–49, 2010.
- [7] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1–5, 2010.
- [8] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," *IET Information Security*, vol. 5, no. 3, pp. 541–552, 2011.
- [9] Y. An, "Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards," *Journal of Biomedicine and Biotechnology*, vol. 2012, Article ID 519723, 6 pages, 2012.
- [10] H. S. Kim, S. W. Lee, and K. Y. Yoo, "ID-based password authentication scheme using smart cards and fingerprints," *ACM Operating Systems Review*, vol. 37, no. 4, pp. 32–41, 2003.
- [11] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.
- [12] S. M. Yen and M. Joye, "Checking before output may not be enough against fault-based cryptanalysis," *IEEE Transactions on Computers*, vol. 49, no. 9, pp. 967–970, 2000.
- [13] M. Scott, "Cryptanalysis of an ID-based password authentication scheme using smart cards and fingerprints," *ACM SIGOPS Operation System Review*, vol. 38, no. 2, pp. 73–75, 2004.
- [14] N. K. Ratha, K. Karu, S. Chen, and A. K. Jain, "A real-time matching system for large fingerprint databases," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 18, no. 8, pp. 799–813, 1996.
- [15] C. J. Lee and S. D. Wang, "Gabor filter-based approach to fingerprint recognition," in *Proceedings of the IEEE Workshop on Signal Processing Systems (SiPS '99)*, pp. 371–378, 1999.
- [16] G. Cao, Y. Mei, Z. Mao, and Q. S. Sun, "Fingerprint matching using local alignment based on multiple pairs of reference minutiae," *Journal of Electronic Imaging*, vol. 18, no. 4, Article ID 043002, 2009.
- [17] A. K. Hrechak and J. A. McHugh, "Automated fingerprint recognition using structural matching," *Pattern Recognition*, vol. 23, no. 8, pp. 893–904, 1990.
- [18] L. C. Jain, "An automated matching technique for fingerprint identification," in *Proceedings of the 1st International Conference on Knowledge-Based Intelligent Electronic Systems*, pp. 21–23, May 1997.
- [19] A. Wahab, S. H. Chin, and E. C. Tan, "Novel approach to automated fingerprint recognition," *IEE Proceedings Vision, Image & Signal Processing*, vol. 145, no. 3, pp. 160–166, 1998.
- [20] Y. J. Chang, W. Zhang, and T. Chen, "Biometrics-based cryptographic key generation," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '04)*, pp. 2203–2206, June 2004.
- [21] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT '04)*, Interlaken, Switzerland, May 2004.
- [22] F. Hao, R. Anderson, and J. Daugman, "Combining cryptography with biometrics effectively," Tech. Rep. UCAMCL-TR-640, University of Cambridge, Computer Laboratory, Cambridge, UK, 2005.

- [23] W. Shalaby and M. O. Ahmad, "A multilevel structural technique for fingerprint representation and matching," *Signal Processing*, vol. 93, no. 1, pp. 56–69, 2012.
- [24] Q. Wang, G. Liu, Z. Guo, J. Guo, and X. Chen, "Structural fingerprint based hierarchical filtering in song identification," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '11)*, pp. 1–4, IEEE, 2011.
- [25] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, 2009.
- [26] Q. Tong and J. Zhu, "Research of improved gabor based on fingerprint image enhanced algorithm in wavelet domain," in *Proceedings of the International Conference on Computational Problem-Solving (ICCP '12)*, pp. 17–18, IEEE, 2012.
- [27] H. Khazaei and A. Mohades, "Fingerprint matching and classification using an onion layer algorithm of computational geometry," in *Proceedings of the 13th International CSI Computer Conference*, 2008.
- [28] A. Panchenko, L. Niessen, A. Zinnen, and T. Engel, "Website fingerprinting in onion routing based anonymization networks," in *Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society*, pp. 103–114, ACM, 2011.
- [29] S. Mazaheri, B. S. Bigham, and R. M. Tayebi, "Fingerprint matching using an onion layer algorithm of computational geometry based on level 3 features," *Communications in Computer and Information Science*, vol. 166, no. 1, pp. 302–314, 2011.