SECURITY OF BIOMETRICS USING MULTIMODAL APPROACH

AbdulHaseeb Ahmed  
Electrical Engineering  
Air University  
Islamabad, Pakistan  
haseeb@mail.au.edu.pk

Hafiz Malik  
Electrical and Computer Engineering  
University of Michigan-Dearborn  
Dearborn, USA  
hafig@umd.umich.com

Abstract—Biometric based access control systems (BACS) are widely used for robust and reliable identity verification, but these systems also raise some serious privacy concerns. The biometric templates, used for access control process, are stored in the system database which is vulnerable to variety of attacks. This paper presents a two stage solution for securing biometric templates. The proposed method first models the fuzziness of template bits, which is used to select stable template bits. Channel coding based on low density parity check coding is then used to protect selected template against adversary attacks. To enhance the security of the proposed method further, both human irises are used for the access control process. Security performance of the developed algorithm is evaluated using publicly available CASIA database. Simulation results show that the proposed method provides stronger computational security than existing iris template security method.

Keywords—Biometric, Security, Privacy, BACS, Channel Coding, LDPC

I. INTRODUCTION

Epidemic growth in identity theft and security requirements in variety of applications ranging from international border crossings to access control have prompted an urgent need of reliable identity management systems. Identity verification of a person is a key element in any identity management system. Traditional identity verification systems rely on passcode (e.g. passwords, personal identification numbers (PIN), ID cards, etc.) for identity verification, but these systems are prone to brute fore dictionary attacks. Biometrics systems, on the other hand, require substantially more effort to mount such attacks. This is mainly due to non-reducibility and uniqueness nature of biometric traits (e.g. fingerprint, face, iris, retina, hand geometry, voice and gait). In addition, biometrics cannot be forgotten, they can be hard to guess, and they are hard to forge. Widespread deployment of biometric identification systems, however, has prompted many privacy concerns. This is mainly due to inability of existing biometric identification systems to protect user biometric traits against known attacks. In biometric identification literature this problem is known as "the secure biometric storage problem". For example, a biometric based identity verification system (commonly used by commercially available products including laptops, mobile phones, etc.) derive biometric key (or biopasscode) from the user's biometric and use it either to encrypt data stored on system or to grant access. The original biometric, in general, is stored on the system to grant authorized access or decrypt the data. To authorize access (also referred as enrolment phase), a second biometric reading is taken from the user (or query biometric) and compared it with the biometrics stored in the associated database. Access is granted if stored biometric and the query biometric are close enough (also referred as verification phase). Adversary uses variety of attacks to get hold of biometric used in the database of biometric based access control system (BACS). The nature of these attacks may differ, but the basic objective of hackers remains the same, that is, gaining access to systems and making malicious usage of the stolen biometrics.

A number of security algorithms have been developed to secure biometric template against adversary attacks, however achieving a fool proof security of the biometric templates against adversary attacks is still a challenging task. Few notable approaches include Jain and Pankanti’s [1] method which uses smart card to store biometric template. Simplicity is one of the features of this method, however cost inefficiency for large scale applications is one of limitations of this method. Juels and Wattenberg [2] presented a "fuzzy commitment" based scheme which uses combination of channel coding and hash function to conceal biometric template to achieve biometric security. Sensitivity to fuzziness in the biometric templates and implementation complexity are the major limitations of the fuzzy commitment base methods. Jeuls and Sudan addressed the biometric template fuzziness problem of the fuzzy commitment method in the "fuzzy vault" based approach [3] which employs polynomial interpolation to address the fuzziness of biometric template. Complexity is still one of the limitations of the fuzzy vault based methods. Recently, Martinian et. al. [4] and Nagar et. al. [5] proposed syndrome based scheme to secure the biometrics template. The syndrome based scheme first selects relatively stable bits in the template, the stable bits are then transformed using error correcting codes. One of the salient feature of syndrome based approach is that it does not require the template to store in a direct form. Rathgeb and Uhl [6] presented "interval based mapping" scheme, which
provides good level of security, however cannot suppress the false rejection rates and inherent complexity. Rathgeb and Uhl [7] also presented a statistical attack against fuzzy commitment schemes. Hugo Proença and Luis Alexandre [8] discuss the experimental results from the Noisy Iris Challenge Evaluation. They showed that the fusing recognition methods are better than the any isolated recognition strategy.

A. Problem Model

The most caustic attack on the BACS is to get control of biometric template stored in the biometric template database. Capturing devices introduce fuzziness in the captured biometric scan. Moreover, scans of the same biometric, captured under same setting, are roughly 30% different from each other [9], which makes securing biometric templates stored in the database a challenging task. The biometric template is a shared secret between user and the BACS. An unauthorized access to the BACS database (containing insecure biometrics) leads to serious privacy and security breaches. As unauthorized access to biometrics is unavoidable for practical systems, therefore biometrics are stored in an indirect form (or transformed domain). Higher computational security of the stored form, even adversary get access to the database, is a desirable feature of the next generation BACS.

One possible solution to achieve higher computational security of biometric templates is to use multiple biometrics (a.k.a. multimodal approach). The multimodal based system does provide higher computational security but at the cost of higher false rejection rate. This is because use of multiple biometrics (say both irises) also increases fuzziness in the templates used for access control, therefore leads to higher false rejection rates. Main contribution of this paper is to address aforementioned limitation of multimodal based biometric systems by reducing fuzziness in the biometrics templates used for accessing BACS.

The proposed method uses a novel stability technique to model the fuzziness in the biometric template. The fuzziness in a template is reduced by extracting the stable bits. The stable bits are defined as those bits which are insensitive to additive noise. Channel coding is then employed to secure the template by mapping it into some other space. For the sake of simplicity, human iris is consider for proposed method description and performance evaluation, though the proposed method is applicable to other biometric traits such as fingerprint, face, etc.

The paper is organized as follows: Section II provides a detailed description of the proposed stable bit selection technique and channel encoding used to secure biometrics. Experimental Results are shown in Section III. And, concluding remarks are discussed in Section IV.

II. Proposed Method

Shown in Fig. 1 is the block diagram of proposed framework. Contribution of this paper is highlighted in gray color.

Description of the each stage is outlined next.

![Figure 1. Shown is the block diagram of the biometric based access control system (BACS)](image)

A. Preprocessing

The biometric scan of a human eye is taken through a capturing device e.g. infrared camera. The true biometric (input to the capturing device) is represented as \( b \) and the captured biometric is represented as \( m \). The captured biometric, \( m \), is a combination of true value, \( b \), and capturing device artifacts, \( n_d \), i.e., \( m = b + n_d \). Segmentation is the first step in generating iris template from the input iris scan. The objective of segmentation is to localize the iris of an eye. Segmented image is then normalized to ensure comparison in a constant dimensions. Frequency-scale filtering based on Gabor filtering is then applied to the normalized image. The Gabor filter provides the optimum representation of data in space-scale. The Gabor filtering can be expressed as,

\[
G(x, y) = e^{-\pi A} e^{-2\pi i B}
\]

where

\[
A = \frac{(x - x_0)^2}{a^2} + \frac{(y - y_0)^2}{b^2}
\]

\[
B = u_0(x - x_0) + v_0(y - y_0)
\]

where \((x_0, y_0)\) denotes the position in the image, \((a, b)\) indicates the effective width and length, respectively, and \((u_0, v_0)\) specifies modulation.

Phase coding is applied to the output of Gabor filter to generate a binary template of size \( r \times \theta \) where \( r = 1, 2, \cdots, 20 \), and \( \theta = 0, 1, \cdots, 239 \). It is important to mention that the binary templates exhibit inherent fuzziness, this fuzziness can be attributed to the device artifacts, \( n_d \). The fuzziness in the biometric template is the major source of false rates, i.e., false rejection rate \( f_{rr} \), and false acceptance rate, \( f_{ar} \). In addition, fuzziness in the biometric template is the fundamental obstacle in extracting biometric encryption key or securing storage of biometrics for BACS.
B. Stable Bits Extraction

To characterize fuzziness in the biometric, the complex output of Gabor filter is analyzed. It has been observed through extensive experimental simulations that complex coefficients, of the iris image, in the vicinity of interfaces of four quadrants are relatively more sensitive to capturing device artifacts. To illustrate this fact, we added 28 dB additive white Gaussian noise to the test iris scan. The Gabor filter output for both the test iris scan and the equivalent noisy iris scan are shown in Figs. 2 and 3. Shown in Fig. 2 is the constellation plot of output of the Gabor filter applied to the test iris scan (‘S1001L01.jpg’), and shown in Fig. 3 is the equivalent the constellation plot of output of the Gabor filter applied to the equivalent noisy iris scan.

Figure 2. Shown is the constellation plot of test iris scan (‘S1001L01.jpg’ scan of CASIA database [10])

Figure 3. Shown is the constellation plot of equivalent noisy iris scan subjected to 27 dB additive noise

It can be observed from Figs. 2 and 3 that coefficients near to the boundaries of four quadrants are more sensitive to the additive noise than the coefficient away from phase encoding region thresholds (boundaries). The proposed scheme exploits this localized fuzziness in the biometrics to extract a relatively stable template.

Figure 4. Shown is the basic idea of stability bits extraction from the input iris scan

Let \( \phi(\cdot) \) defines a function use to extract stability bits. The stability bit extraction process discards the coefficients within guard-band region and keeps the remaining coefficients in the complex plan. The effectiveness of the proposed stability region selection method has been tested through extensive simulations, using CASIA database[10]. Shown in Fig. 5 is the plot of stable coefficients selected for iris scan (‘S1001L01.jpg’) of CASIA database[10] using proposed method. The 4-ary phase quantization is then applied to encode the selected stable coefficients using gray codes [11]. The encoding process maps converts complex coefficients to binary template.

Figure 5. Shows is the stable coefficients of iris scan (‘S1001L01.jpg’) of CASIA
C. Securing The Template

The resulting stable bits cannot be stored in a direct form, as it can be stolen or spoofed by the hacker/attacker. To address this issue, error correcting codes are used to store the stable binary template in the transformed domain. The idea of syndrome decoding is used to achieve this goal. The syndrome of the stable binary template is calculated using low density parity check code (LDPC) [12]. Let \( f(.) \) be the function that transforms a binary template to its equivalent syndrome, and let \( H \) be the random parity check matrix, employed to compute syndrome, \( S \). It is important to mention that here \( S \) is a bit string which conceal the biometric template. Let \( z \) be the the sequence of stable bits, then computing syndrome from \( z \) can be expressed as,

\[
S = H \ast z
\]

During the authentication phase, the similar processes are applied to extracting stable binary template from the query biometric and then computing syndrome using methods described in Sections II-C and II-A. Let the \( z' \) be the sequence of stable bits extracted from the query template (input template during authentication phase) and \( g(\ldots) \) denotes the belief propagation decoder to correct errors in the query template. The output of the belief propagation decoder is then use to compute syndrome for the query template as follows,

\[
S' = H \ast z'
\]

where \( S' \) is the syndrome of the query template.

The syndrome of the query template is then compared with the access control database to authenticate (or grant access) to a legitimate user [4], [13]. To further improve the security of the biometric system, two-iris approach (both the left and the right irises) is used. The two-iris approach exploits the randomness in both iris of the same human [9]. The two-iris approach provides better cryptographic security as compared to the single-iris approach. It has been shown [9] that both human irises are mutually independent of each other; therefore using both irises will result in more security bits hence better computational security. In other words, there are more number of bits for hacker to guess. In addition, the two-iris approach also provides more robustness as it results in lower false rejection rates as compared to the single-iris. Hence, the proposed method provides the better combination of security and robustness.

III. EXPERIMENTAL RESULTS

A. Security-Robustness Criterion

The effectiveness of the proposed method is measured in terms of security and robustness of the BACS. To achieve this goal, probability of authentication failure (or robustness) and probability of security failure are used to quantify the performance of the proposed method. These performance metrics are defined as:

1) Probability of Authentication Failure: The authentication failure, \( \varepsilon_{auth} \), is defined as the probability of decoder failure to recover the shared secret for a legitimate user, which can be expressed as,

\[
\varepsilon_{auth} \triangleq \{ z \neq g(m', f(m)) \}
\]

2) Probability of Security Failure: The security of a system is defined as the number of attempts, by the attacking algorithm, to achieve a reasonable probability of success. Let us assume that an attacking algorithm has access to \( \varphi(\cdot), f(\cdot), g(\cdot, \cdot) \) and \( S \); then the event of successfully guessing the biometric can be defined as,

\[
\varepsilon_{sec} \triangleq \{ z \in attacking_{alog}(\varphi(\cdot), f(\cdot), g(\cdot, \cdot), S) \}
\]

Shown in the Fig. 6 is the performance of a BACS (biometric based access control system) as a function of \( \varepsilon_{auth} \) and \( \varepsilon_{sec} \). Here different pairs of \( \varepsilon_{auth} \) and \( \varepsilon_{sec} \) values result an \textit{operating curve} of a given BACS. The area under the performance curve, \( A_p \), can also be used to gauge the performance of the biometric system, i.e., larger \( A_p \) value means better performance and vice versa. Therefore, according to Fig. 6 method 3 provides better security-robustness performance than the method 1.

![Figure 6. Shown is the security (code rates) vs robustness plot (using theoretical data)](image)

B. Dataset

For experimental performance evaluation of the proposed method, the Chinese Academy of Sciences (CASIA) database [10] is used. All the images in the CASIA database have been taken specifically for iris recognition research. The boundaries of iris, pupil, and sclera are clearly distinguished. The CASIA database consists pairs of 1200 iris scans, stored as gray-scale JPEG images with 8-bit resolution. These images were captured in two sessions, in an indoor environment, under near infrared illumination using a self-developed iris camera.
C. Simulation Results

To evaluate performance of the proposed method, we analyzed each pair of images (left and right iris scans) in the database for template generation. In first experiment, we analyzed the robustness performance of the proposed scheme as a function of guard-band \( L \). For this experiment, the stable-bit templates were generated with following guard-band values, \( L \in \{2, 6, 10, 14, 18, 20\} \times 10^{-3} \). Shown in Fig. 7 is the plot of average false rejection rate of the proposed scheme as a function of \( L \). It can be observed from Fig. 7 that average false rejection rate decreases as \( L \) increases.

In the second experiment, we compared the performance of the proposed scheme with the Martin et. al.’s syndrome based approach [4] using single iris. Shown in Fig. 8 is the robustness performances of both schemes. Here, both plots are generated with code rates, \( 3, 4, 5, 6, 7, 8 \times 10^{-2} \), and security-robustness curve of the proposed scheme is generated using \( L = 0.003 \). The security of BACS is interms of code rates. If we increase the code rates, we will get the greater number of security bits. It can be observed from Fig. 8 that the proposed scheme performs significantly better than its counterpart. Better robustness performance of the proposed scheme can be attributed to the fuzziness reduction in the template using for encoding. In third experiment, we compared the performance of both schemes using both irises. Shown in Fig. 9 is the robustness plots of both schemes as a function of coding rate. These plots are generate using same set of parameters as in the second experiment. It can be observed from Fig. 9 that the proposed scheme outperforms its counterpart. It is important to mention that using both irises provide robustness performance gain over single iris whereas robustness performance deteriorates for Martin’s approach when compared with its single iris performance.

IV. Conclusion

In this paper, a new method for extracting stable bits and securing BACS is proposed. The method for extracting stable bits or determining stable regions is quite simple and easy to implement. This stable bits method shows better performance when compared with the existing method. In addition, the use of two irises provides better security as well as robustness performance, that is, the two-iris approach reduces the false rejection rates, with greater level of security. The CASIA database is used to test the performance measurement of proposed solution. The result shows that the proposed solution provide better security as compared to the previous syndrome based coding scheme.

REFERENCES


