Hybrid Multimodal Template Protection Technique Using Fuzzy Extractor And Random Projection

G. Karthi, M. Ezhilarasan
Research scholar, Pondicherry Engineering College ,
Professor & Head, Department of Information Technology,
Pondicherry Engineering CollegeKarthisan@yahoo.co. IEEE

Abstract— Due to the popularity of biometric authentication system, it is extremely important to protect the biometric template available in the networks. Template protection technique is a critical issue in biometric authentication system. Basically the protection technique can be categorized into Biometric CryptoSystem (BCS) and Cancelable Biometrics(CB). In this paper, an efficient hybrid template protection technique which combines both Biometric CryptoSystem (BCS) and Cancelable Biometrics (CB) was proposed. The proposed system uses key generating cryptosystem and feature transformation method. The limitation of the feature transform was overcome by this approach. We focus on these techniques using Iris, Fingerprint (i.e. multimodal Biometrics) as traits. The Experimental Results shows no degradation in results by combining both the Biometric CryptoSystem (BCS) and Cancelable Biometrics (CB). It is important that the biometric authentication system should withstand the attacks and the template theft by the adversary.

Index terms-- Multimodal biometrics, Privacy, Random Projection (RP), Fuzzy Extractor, Template.

I. INTRODUCTION

In recent years, authentication has become increasingly important issue. In many applications, it is extremely important to verify the identity of a person that what he/she claims to be. The Traditional approach, the use of passwords and pins has increasingly suffered from flaws like forgotten or easily guessed passwords. Therefore, there has been an intense study of alternative methods. One alternative to passwords is biometrics (it is what we have rather than what we claim). Biometrics means "life measurement" refers to identification of individuals by their traits or physiological characteristics. Biometrics is based on the fact that we have such as fingerprint, face, hand/finger geometry, iris, retina, signature, gait, palmprint, voice pattern, ear, hand vein, and the DNA information of an individual to establish identity.

The critical issue in the Biometric system is protecting the templates from various vulnerabilities [1].

- Presenting fake biometrics at the sensor: In this mode of attack, a fake biometric can be reproduced at the sensor as input to the system.
- Replaying old data: previously stored data is replayed to the system for feature extraction process.
- Overriding the feature extraction process: The feature extractor is override by preselecting the features set from the biometric data.
- Tampering with the biometric feature representation: The original feature extracted from the input signal is replaced by fraudulent feature set or different feature set.
- Overriding the matcher: In this mode of attack, the matcher is attacked and the decision is preselected by the intruder irrespectively of the input.
- Modifying the stored template: Here, the attacker tries to modify the templates stored in the databases.
- Attacking the channel between the stored templates and the matcher: The stored templates can be modified when it is sent to the matcher through a communication channel.
- Overriding the final decision: The result of the decision by the matcher is override by the hacker, (ie) whatever the result the output will be the hacker’s desired result.

A. Template Protection Schemes

Like passwords and pin, the biometric data once compromised can’t be revoked. The template must be stored in a way that it can be cancellable and revocable.
There are many schemes for protecting the biometric templates as shown in Figure 1. The template protection schemes broadly classified into two categories namely, Cancelable Biometrics (CB) or feature transformation and Biometric Cryptosystem (BCS).

A Template Protection Technique should satisfy the following:

(i) Diversity: The same protected template cannot be used across different applications.

(ii) Reusability: If the current protected template is compromised, then a new protected template can be reissued.

(iii) One-way Transformation: It is possible to obtain the protected template and helper data from the biometric data but the reverse must be impossible.

(iv) Performance: The protected template's FAR and FFR rate should not deteriorate when compared with the original biometric data.

The various Template Protection Technique and their limitations was tabulated in Table 1. In this paper we overcome the disadvantage of salting technique is once the key is stolen the template is no longer safe. Instead of storing the key, the key is generated from his/her biometric at the time of authentication. By doing this we can avoid the limitation of Feature transformation Technique.

### Table 1: Template Protection Techniques

<table>
<thead>
<tr>
<th>Approach</th>
<th>Template security depends on</th>
<th>Entities to be stored</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature Transformation</td>
<td>Secrecy of user specific token/key.</td>
<td>Transformed Template, secret key.</td>
<td>Once the key is stolen the template is no longer secure.</td>
</tr>
<tr>
<td>Non invertible Transform</td>
<td>Non</td>
<td>Transformed Template,</td>
<td>Non</td>
</tr>
</tbody>
</table>

B. **Biometric CryptoSystems (BCS)**

Biometric cryptosystem is a biometric template protection technique which either produces a digital key from a biometric or binds a digital key to the biometric. Most of the BCSs require biometric dependent public information, which is used to retrieve or generate keys, which is referred to as helper data. The Helper Data doesn't reveal any information about the original template but needed for the reconstruction of the digital keys.

The Authentication process is done by verifying the key validities instead of the biometric comparisons; the output is either the correct key or a failure message. Based on how helper data are derived, BCSs are classified as key-binding or key-generation systems.

#### Key-generation Schemes

In this scheme, the helper data and the given template generate the keys. The helper data are derived from the biometric template. The key-generating helper data is also referred as “fuzzy extractor or secure sketch”. The fuzzy extractor extracts a uniformly random string from a biometric input while stored helper data assist the reconstruction. In contrast, in a secure sketch, helper data are applied to recover the original biometric template. Key generating biometric cryptosystems usually suffer from low discriminability which can be assessed in terms of key stability and key entropy. Key stability refers to the extent to which the key generated from the biometric data is repeatable. Key entropy relates to the number of possible keys that can be generated. The advantage here is it can also be very useful in cryptographic applications.
C. Feature Transformation or Cancelable Biometrics

Cancelable Biometrics (CB) consist of intentional, repeatable distortions of biometric signals based on transforms which provide a comparison of biometric templates in the transformed domain. The inversion of such transformed biometric templates must not be feasible for potential imposters. In contrast to templates protected by standard encryption algorithms, transformed templates are never decrypted since the comparison of biometric templates is performed in transformed space which is the very essence of CB. The application of transforms provides irreversibility and unlinkability of biometric templates. Obviously, CB are closely related to BCSs.

Feature Transformation or Cancelable Biometrics is a template protection technique, used to protect the biometric templates by use of transformation functions. The transformation function uses an external key/pin which provides non-invertibility property to the protected template. The external key/pin is user specific, so multiple templates can be generated by using different keys for the same user biometric. In this technique the biometric template can be revocable, since the technique depends on the transformation function and user specific key, by using different user specific key we can produce new protected template, if the existing template is compromised. The enrollment ( Encoding) and authentication (decoding) process is shown in the figure 2.

Figure 2: Feature Transformation or Cancelable Biometrics

The security of the template depends on the secrecy of the user specific key, if the user specific key is known to the imposter; the original biometric template can be recovered from the protected template.

The remainder of this paper is organized as follows. In Section 2, presents the literature survey. Section 3 introduces the proposed methods and provides detailed analysis. Experimental results, are presented in Section 4. Finally, conclusions are presented in Section 5.

II. LITERATURE SURVEY

In this section survey of template protection techniques on face , fingerprint and multimodal biometric systems. Various schemes are there for protecting the template. Let us discuss some of the techniques which are applied on fingerprint, face and multiple trait (face and fingerprint). A biometric system is proposed [2] has a tool for security. An overview of biometrics is provided and discuss some of the salient research issues that need to be addressed.

A. Biometric CryptoSystem (BCS)

Alvarez Marino et al. [3] a crypto-biometric scheme, based on fuzzy extractors, by using iris templates is proposed. here the user can get his key or secret data which was stored can be retrieved using his biometrics by fuzzy extractor scheme.

Yagiz Sutcu et al [4] proposed error tolerant cryptographic primitive secure sketch to protect the templates. A general framework to design and analyze secure sketch for biometric templates was given, and with a concrete construction for face biometrics as an example.

Yagiz Sutcu et al. [5] proposes secure sketch on face and fingerprint features. For the minutiae based Fingerprint they applied the geometric transformation and the SVD based face features they applied the secure sketch. By fusing the two biometrics at the feature level, they yield a better security and their biometrics can be stored safely.

Yang Bo et al [6] proposes a fully fuzzy extractors for biometric template security. The public string which is used by the fuzzy extractor is authenticated by the receiver using some part of strings owned by him.

B. Transformation techniques

Ratha et al. [7] proposed and analyzed three noninvertible transforms for generating cancelable fingerprint templates. The three transformation functions are cartesian, polar, and functional. In Cartesian transformation, the minutiae space (fingerprint image) is tessellated into a rectangular grid and each cell (possibly containing some minutiae) is shifted to a new position in the grid corresponding to the translations set by the key. The polar transformation is similar to cartesian transformation with the difference that the image is now tessellated into a number of shells and each shell is divided into sectors. Since the size of sectors can be
different (sectors near the center are smaller than the ones far from the center), restrictions are placed on the translation vector generated from the key so that the radial distance of the transformed sector is not very different.

A random multispace quantization technique proposed by Teoh et al. [8]. In this technique, the authors first extract the most discriminative projections of the face template using Fisher discriminant analysis and then project the obtained vectors on a randomly selected set of orthogonal directions. This random projection defines the salting mechanism for the scheme.

Song Wang et al. [9] proposes a alignment free cancelable fingerprint using densely infinite to one mapping approach.

Andrew Teoh et al. [10] propose a new technique called fuzzy hash derived from the cryptographic hasing function. Here the fuzzy hash performs four functions on the biometric templates the Random Projection, Quantization, permutation and applied Error Correcting Coding.

Martin et al [11] addressed privacy concern for a self-exclusion scenario of face recognition through combining face recognition with a simple biometric encryption scheme called helper data system. The combined system is described in detail with focus on the key binding procedure.

Beng Jin et al. [16] proposes a multispace random projection for producing cancelable biometrics. Takahashi et. al. [17] introduced a quotient polynomial ring which reduces the complexity of the transformation algorithm.

C. Hybrid Technique

Feng et al [12] propose a hybrid approach which combines both the biometric cryptosystem approach and the transform-based approach. A hybrid algorithm is designed and developed based on random projection of the features set, discriminability-preserving (DP) transform, and fuzzy commitment scheme. The proposed algorithm not only provides good security, but also enhances the performance through the DP transform. The fuzzy scheme is supported by the transformation technique and the random projection feature points.

Karthik Nandakumar et al [13] proposed a scheme for securing multiple templates of a user as a single entity, this is achieved by generating a single multi-biometric template using feature level fusion and securing the multi-biometric template using the fuzzy vault construct.

And also implemented a fully automatic fuzzy vault system for securing the fingerprint minutiae and iriscode templates. A salting transformation based on a transformation key is used to indirectly convert the fixed-length binary vector representation of iriscode into an unordered set representation that can be secured using the fuzzy vault.

III. HYBRID TECHNIQUE

The hybrid technique which combines both Biometric Cryptosystem (BCS) and Cancelable Biometrics (CB) for multimodal biometric template protection. We use fuzzy extractor technique and salting technique is used for biometric template protection. The fingerprint and Iris traits are used for authentication process. First, the Iris code is generated from Iris and then Key generation process (fuzzy extractor) is applied on Iris code to produce a key. The key generated by Fuzzy Extractor will be used as user specific token for Random Projection. In RP, the fingerprint feature set will be given as input with the key, and they produce the secure template to be stored in the database as shown in figure 3. By this method, we provide better privacy to the template stored in the database.

Figure 3: Hybrid Technique

A. Fuzzy Extractors

Fuzzy or Secure extractors extracts randomness R from w (to use it as key) and later reproduce it using w’ close to the original w as shown in figure 3.

Fuzzy sketches enables computation of a public string P from a biometric template w, such that from another reading w’ sufficiently close to w it is possible to reconstruct the original reading. Furthermore the knowledge of P, should not reveal too much information on the original reading w. Fuzzy extractors address the problem of non uniformity by associating a random uniform string R to the public string P still keeping all the properties of fuzzy sketches. Indeed, fuzzy extractors can be built out of fuzzy sketches and enable the recovering of the secret uniform random string R, from
the knowledge of the public string P and a reading w’ sufficiently close to w.

A (M, w, w’, t, e) fuzzy extractor is a pair of algorithms:
- Gen is a function randomized function, on input w belongs to M, extracts random string R and a helper string P.
- Rep is a function Regeneration function, on input w and P reproduces and outputs R that was generated using Gen(w) if dist(w, w’) >= t

\[\text{Gen}(w):\]
1. Execute sketch func. S SS(w; r1), where r1 denotes random function used by Secure sketch.
2. Using a extractor Ext a random string R is extracted from w, i.e., R. Ext(w; r2), where r2 denotes random function used by Extractor.
3. Output public P = (S; r2) and secret R.

\[\text{Rep}(w, P):\]
1. Execute w Rec(w’, S). If Rec fails (i.e., when dist(w, w0) > t), stop.
2. Extract random string R from w using r2 as R Ext(w, r2) and outputs R.

**B. Fuzzy Extractors**

Johnson et al. [14] Proposed the Random Projection (RP) method. Random Projection (RP) is an effective and precise technology when Comparing to other dimensionality reduction technology such as PCA [15]. In random projection, through a random matrix M X N the original m-dimensional data is projected to a d-dimensional subspace. Random matrix is generated by random number generator which is controlled by user key K. Here the user key is generated from the biometric traits of that person during authentication process instead of storing the key. The random matrix can be obtained by following approach

1. Set each entry of random matrix to an i.i.d. N(0,1) value.
2. Orthogonalize the d rows of the matrix
3. Normalize the rows of the matrix to unit length.

**IV. EXPERIMENTAL RESULTS**

For experimental results we have taken CASIA Iris database and for the fingerprint FVC2004 database is used to evaluate the proposed scheme.

<table>
<thead>
<tr>
<th>Database</th>
<th>FAR</th>
<th>FRR</th>
<th>BCH Encoder (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FVC2004</td>
<td>1%</td>
<td>2%</td>
<td>128</td>
</tr>
</tbody>
</table>

The False Acceptance Rate (FAR) and False Rejection Rate (FRR) for the fingerprint is shown in the table 2. The performance of the authentication system does not degraded by combining the Biometric CryptoSystem (BCS) and Cancelable Biometrics (CB). If the number bits for Error Correction Encoder is increased then the FRR & FAR is improved. The privacy of the template is better when compared to the existing system.

**V. CONCLUSION**

Biometric Template Protection is a very challenging issue in Biometric Authentication System (BAS). Because of this protecting Biometric Template have increasingly gained popularity. In this paper, we propose a hybrid technique, which uses Biometric Cryptosystems and Feature Transformation. In Feature Transformation, if the user specific token is theft means the template is no longer safe. Here, the user specific key is generated from the biometric traits of that person during authentication process instead of storing the key. The Experimental Results shows no degradation in FAR & FRR by combining both the Biometric Cryptosystem and Cancelable Biometrics.

**REFERENCES**


