Abstract— In this paper we present an effective scheme that preserves the biometric templates more secured. We present a new algorithm called Enhanced Blind Encryption Algorithm for securing biometric templates between client and server and using that for authentication. There are four phases involved in this process namely, enrollment, identification, matching and fusion. During enrollment, biometric traits (fingerprint and iris) will be uploaded and encrypted using Enhanced Blind Encryption Algorithm. During fusion, Borda count and Logistic regression methods are applied combinably in identifying the accurate results. Results indicate that the proposed system can be effectively used even for low-quality images.

Keywords— multimodal, cryptosystem, rank-level fusion, fingerprint, iris, Borda count, EBEA

I. INTRODUCTION

Multibiometrics systems accumulates traits from more than one biometric trait in order to establish the true identity of an individual[15]. Compared to unibiometrics systems having only single biometric trait, multibiometrics systems provides higher identification accuracy and larger coverage[15]. Multibiometrics systems are followed in many large-scale authentication systems.

While multibiometric systems have improved the accuracy and reliability of biometric systems, security of biometric traits information is breached. A biometric system suffers from following 2-attacks namely:

Intrusion attack: If an intruder hacks into a biometric database, he/she can easily forge a biometric trait claiming as his/her own trait[15].

Function creeping: Exploiting the biometric trait information for unintentional purposes.

Security of multibiometrics templates is especially crucial or important since they contain information regarding multiple biometric traits of the same individual. Multibiometrics template/traits protection is the main objective of this work. [1][15].

We have developed our system as a means of checking authentication for client-server communication. Flow of the paper is organized as follows. Section 2 gives a complete picture of multibiometrics fusion methods and different attacks on biometric template during storage and authentication process.

Section 3 presents the proposed crypto-algorithm for storing biometric template securely. Section 4 analyzes the performance evaluation of the proposed multibiometrics cryptosystems. Finally, conclusions are discussed in section 5.

II. BASICS OF FUSION AND CRYPTOSYSTEM

A. Multibiometrics

A system that combines traits from multiple sources of biometric in order to establish the true identity of an individual[2]. Multibiometrics system combines the information presented by multiple biometric sensors, algorithm, instances, traits to establish the true identity of an individual[14]. Multibiometrics systems can improve many of the limitations of unibiometric systems. A multibiometrics system provides the following advantages over unibiometric systems.

i. Improve accuracy

ii. Non-universality

iii. Continuous monitoring: Relying on Multibiometrics enables user authentication, by using another biometric trait.

iv. Noisy data: Biometric samples obtained from different sensor can be used, in case of the first sensor working properly and the other sensor not working properly due to destruction of biometric trait while capturing.

v. Fault tolerance: Multibiometrics authentication system is fault tolerant.

vi. High resistance to spoofing: It is highly difficult to spoof more than one biometric trait from different sources[3].

A multibiometrics system relies on the evidence presented by multiple sources of biometric traits. A multibiometric system can be classified into the following categories: [14].

Multi-sensor systems: Employing multiple sensors for capturing individual’s single biometric trait[14].

Multi-algorithm systems: Consolidating multiple features obtained from multi-feature extraction algorithms to establish true identity of an individual[14].
Multi-instance systems: Using multiple instances of the same biometric trait of an individual[14].

Multi-sample systems: Obtaining multi-samples of a single biometric trait Eg: For face identification, side-ways and front-ways of face can be captured by a single sensor[14].

Multimodal systems: Establishing identity based on the results of multiple biometric traits. For example, combining face and iris to establish the true identity of an individual[14].

Hybrid systems: Hybrid system is used to give a combined effect/ subset of the above methods[4][14].

B. Level of fusion

By the type of biometric information available, five levels of fusion may be defined[14]. Fusion can be categorized into two:

- Fusion before matching or Pre-Fusion
- Fusion after matching or Post-Fusion

Pre-Fusion or Fusion before matching schemes includes sensor level and feature level. Post-Fusion or Fusion after matching schemes includes fusion at match score level, rank level and decision level.

Sensor Level Fusion: Fusion of biometric trait from different sensors to establish true identity of an individual. Eg: iris biometric trait captured using UV light and normal way [21][22].

Feature Level Fusion: Fusion of biometric feature from different feature-extraction algorithm[14][21][22].

Match-Score Level Fusion: Each sensor provides different match scores for each trait. These match scores can be consolidated to establish true identity of an individual [21][22].

Decision Level Fusion: Each classifiers output will be combined to provide the final authentication result of an individual[21][22].

Rank Level Fusion: Combines ranks of each biometric trait to establish true identity of an individual[19][21][22].

C. Rank-level Fusion

Rank-level fusion combines ranks from different modalities to establish true identity of an individual[6]. Here, the proposed system uses borda count method and logistic regression method to integrate the rank of individual matcher.
**Highest Rank Method:** In this method each possible matched trait will be assigned a maximum rank by different matchers.

**Borda Count Method:** This method uses an average of ranks for each matched user.

**Logistic Regression Method:** In this method a weighted value for each trait will be assigned. Finally, the value will be multiplied by the ranks of individual user and average will be taken[19][21].

<table>
<thead>
<tr>
<th>IDENTITY</th>
<th>BORDA COUNT METHOD</th>
<th>LOGISTIC REGRESSION METHOD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Fused score</td>
<td>Rank</td>
</tr>
<tr>
<td>Person 1</td>
<td>3/2=1.5</td>
<td>1</td>
</tr>
<tr>
<td>Person 2</td>
<td>9/2=4.5</td>
<td>5</td>
</tr>
<tr>
<td>Person 3</td>
<td>8/2=4</td>
<td>4</td>
</tr>
<tr>
<td>Person 4</td>
<td>4/2=2</td>
<td>2</td>
</tr>
<tr>
<td>Person 5</td>
<td>6/2=3</td>
<td>3</td>
</tr>
</tbody>
</table>

**Fig 2.3 Rank-level Fusion [21]**

In the Borda count method, from the figure 2.3 these ranks are added and then divided by 2 (number of biometrics) and it returns 1.5, which is the first rank. For the logistic regression method, the weights 0.15 and 0.5 are assigned for iris and retina. For “Person 2,” the rank is 4 and 5 from iris and retina. For the reordered rank calculation, initial ranks are multiplied by their respective weights (4 multiplied by 0.15, 5 multiplied by 0.5). Then, these two new ranks of “Person 2” is added and divided by 2 (number of biometrics) and the result is 1.55, which is considered as rank 2 (Second from the lowest) [19][21][7].

**D. Attacks on Biometric Template**

The vulnerability of the biometric system and the various attacks point as shown in figure 2.4 in the biometric system are discussed here.

**E. Blind Encryption Algorithm**

Blinding is a method by which a process will be computing a function for a client/user in an encrypted form irrespective of output or input. Blinding technique can also prevent side-channel attacks. [8] [16][17].

There are various attacks possible on a unibiometric system compared to multibiometric system [20].

Possible attacks are providing a fake biometric trait, where an attacker will provide a spoofed trait Eg: for fingerprint identification – silicone type of fingers can be presented, Replaying old data, where an old biometric trait captured will be presented to the feature extractor process of biometric system, feature set tampering, where features obtained from trait will be mishandled by an attacker, channel attack, where the trait will be attacked while database storage, overriding, where an hacker can override matcher/final decision of his/her own’s decision[20].

**FIG 2.4 Attacks on the biometric system [20]**

**FIG 2.5 Blind Encryption Algorithm**

From the fig 2.5 blind encryption algorithm takes as follows, initially the client has an input x and the server has function f. Client would like server to compute y=f(x) given by step 1 without revealing either x or y. Then the server blinds the message as encoding it to some other input E(x) in step 2; the encoding E must be a split-up on the input space f, like a permutation which is random.
Server gives \( f(E(x)) \), on which client applies a decoding function \( D \) to obtain \( D(f(E(x))) = y \) as given by step 3.

### III. PROPOSED WORK

**Rank level fusion of Multibiometrics Cryptosystems**

The following diagram is the architecture of Rank level fusion of Multibiometrics Cryptosystems. It has four basic processes:

1. **Enrollment**
2. **Identification**
3. **Matching**
4. **Fusion**

![Fig 3.1 Architecture of Rank Level Fusion of Multibiometrics Cryptosystem](image)

Each process requires different level of security according to the possibility of attacks can involve. In enrolling the correct sample is to be provided as it is to be matched with the instances provided in every identification process. While identification process, the unauthenticated person should be rejected. It should not provide any authentication to wrong person. It should have high Acceptance rate and low Rejection rate. During matching, more importance is given on identifying the correct template. It should avoid the chance of mismatching. In fusion, the right person is to be authenticated. Encryption takes place in client side while decryption in server side.

**Enrollment:** In enrollment process, the first proposed biometric trait is taken and it is called as sample. It is stored in dataset which is known as template. The second step in enrollment is to extract the common unique feature of the trait. The proposed cryptosystem algorithm is then applied on the sample biometric trait. The encryption is done on each pixel of the iris sample.

It uses enhanced blind encryption algorithm where two levels of encryption is followed. Encryption is done here for avoiding attacks on the stored dataset in order to reject the unauthenticated person. The encrypted iris trait is sent to the server and is stored. The similar process is carried for the second biometric trait and the encrypted fingerprint image is stored in the server dataset.

**Identification:** During identification, the user provides his traits. Hence this process loads the second instance of two different biometric traits say, iris and fingerprint. This second instance of trait images is to compare with the sample traits for authentication. Encryption is applied again for the second instance and encrypted traits images are sent to server for authorization. This process requires more security as unauthenticated person may try to authenticate the system.

**Matching:** This process is carried out at the server after the identification process. Matching involves decryption of both trait images which has encrypted from client. As like encryption, decryption also takes place in two levels. Comparison between the sample trait image and the provided image is carried out. If both the instances are identical then it is given the lowest rank and other person’s similar images are given lower ranks. The person with the lowest rank is the authorized person. The iris and fingerprint images are matched individually and the fusion is done after the ranks are allocated for each trait.

**Fusion:** The two appropriate ranks are fused and the result is the identification of right person. Fusion algorithm includes Borda Count and Logistic Regression methods. Borda Count method uses the sum of the ranks assigned by individual matchers to calculate the final value. Logistic regression method is a generalization of the borda count method. In this method, a weighted sum of the individual ranks is calculated. The weights are calculated during the training phase using logistic regression method.

**A. Enhanced Blind Encryption Algorithm**

The Cryptosystem algorithm involves Enhanced Blind Encryption Algorithm. The encryption and decryption function has been doubled so it takes two levels of encryption and decryption than the normal Blind Encryption algorithm.

The person of the image does not know how the encryption has been carried out in the second level which is done at the server. In similar the server does not know the first level of encryption done by client. The input image, \( x \) is taken and the function going to be applied on trait image \( X \) be \( F \). The output from the step 1 is \( Y = F(X) \).
Then encrypted trait image, $E(X)$ is sent to server. The server then computes, $Z$ by the function $Y$. The obtained double encryption result is $E(Z)$ at the client. The first level decryption carries out in server side which gives the result $D(f(E(Z))) = Y_0$. Again the decryption takes place which yields $Y$ from $D(f(E(X)))$.

**Figure 3.2 Enhanced Blind Encryption Algorithm**

Our proposed system works better in terms of feature extraction, providing security to biometric template and it involves novel rank-level fusion method by which our proposed system provides higher security threshold level and secure communication between client and user.

**IV. RESULTS AND DISCUSSIONS**

The proposed system involves pattern-based algorithm for fingerprint recognition and phase-based iris recognition algorithm for iris recognition. For fusion of biometric traits, rank-level fusion is used. Borda count and logical regression method is used for fusing two biometric traits. The proposed system has been implemented using .NET framework. For fingerprint FVC 2006, 2004, 2002 datasets were used and for iris CASIA datasets were used.

We proposed a new algorithm named Enhanced Blind Encryption Algorithm for storing biometric template more securely. In this algorithm each individual biometric template will be encrypted twice say, at the client side and it will be decrypted twice say, at the server side. The general parameters used for biometric system are Genuine Accept Rate, False Accept Rate, False Rejection Rate, Equal Error Rate, secure communication and security threshold level. The description of each parameter used for comparison

**Genuine Accept Rate:** The rate at which the present biometric trait is authenticated. In our proposed system the GAR is 99.5% compared to GAR 98.5% in existing system.

**False Rejection Rate:** FRR, is the measure that the biometric security system will incorrectly reject an access attempt by an authorized user. In our proposed system FRR is 3.25% for fingerprint and 1.75% for iris traits.

**Equal Error Rate:** The value indicates that the proportion of false acceptances is equal to the proportion of false rejections.

**Table 4.1 Comparison of the security threshold level of different biometric traits used**

<table>
<thead>
<tr>
<th>Database</th>
<th>Existing System</th>
<th>Proposed System</th>
</tr>
</thead>
<tbody>
<tr>
<td>FVC 2006</td>
<td>51</td>
<td>59</td>
</tr>
<tr>
<td>FVC 2004</td>
<td>51</td>
<td>59</td>
</tr>
<tr>
<td>FVC 2002</td>
<td>51</td>
<td>59</td>
</tr>
<tr>
<td>CASIA</td>
<td>88</td>
<td>92</td>
</tr>
</tbody>
</table>

It can be seen from the table 4.1 that the security threshold level of FVC 2006, 2004, 2002 is 59% which is more compared to the existing system. Similarly, for iris dataset the security threshold level is 92% which is more compared to the existing system.

**i. Database Performance Evaluation**

We evaluated the performance between security threshold level and Genuine Acceptance Rate of the proposed multimodal biometric cryptosystem using rank-level fusion by the following graphs.

**Figure 4.1 Representation of security threshold level**

It is noted from the above line graph that for CASIA dataset the threshold level was more compared to existing system and for FVC 2006,2004 and 2002 datasets the threshold level is 8% more than the existing system.
From the above graph the GAR for FVC 2006 dataset was 98.5% in existing system but in proposed system it is 99.5%. Similarly, for FVC 2004 dataset the security threshold level 97.5% but in proposed system it is 98.5%. For CASIA dataset the security threshold level is increased.

From the above graph FRR was 2% for CASIA dataset and 4% for FVC 2006 dataset in existing system.

But in our proposed system FRR is 1.75% for CASIA and 3.25% for FVC.

V. CONCLUSION

We have proposed a rank-level fusion framework in which the biometric template is more secured by Enhanced Blind Encryption Algorithm (EBEA). It protects multiple biometric traits using a single secure sketch. From the comparison results our proposed system provides better performance in terms of Genuine Acceptance Rate of 99.5%. Experimental results show that it is simultaneously possible to improve the matching performance and template security using the multibiometrics cryptosystems. There are some issues that can be investigated further: (i) methods to improve the security analysis by providing more enhanced cryptosystem algorithm. (iii) noise removal can be enhanced.

REFERENCES


