Highly secured crypto-IRIS based authentication system

S.Kavin hari hara sudhan(1), K.P.Rajasekar(2), R.Balaji(3)

(1),(2),(3) M.Tech student in Computer Science and Engineering

(1) Dr.MGR Educational and Research Institute Chennai, Tamilnadu, INDIA

(2) SRM University, Chennai, Tamilnadu, INDIA

(1) mailmekavin.s@gmail.com, (2) rajasekar88@gmail.com, (3) mailmebalaji89@gmail.com

Abstract

Nowadays bio-metric authentication systems are widely used in order to provide authentication without possessing any physical materials. Bio-metric authentication systems are mainly concentrating on security, revocability, privacy, and accuracy. In this paper, we propose a provably two way secured biometric authentication system, which addresses the concerns of user’s privacy, template protection, trust issues, network security, and accuracy. The system is highly secure in the sense, biometric details are going to be encrypted twice, the system won’t reveal any additional information about the user or biometric, to the authenticating server’s database or to the insecure network. In this system two different encryption algorithms have been used both in the client and server side. One is public key cryptography another one is private key cryptography. User’s privacy as concern it is revealing only the identity of the user. In template protection this protocol will store the template as encrypted form. Protocol will provide trust between remote user and server, while a remote user cannot be reliably identified without biometric information. Since network security as concern protocol is not revealing the plain biometric details while it is passed through the network. The proposed approach has no restrictions on the biometric data used and it is applicable for multiple biometrics (face, iris, hand geometry, and finger print). Authentication by using two way encryption will give additional layer of security when comparing with existing system.

KEY TERMS: accuracy, authentication, biometrics, crypto systems, privacy, protocol, public key cryptography, revocability, security.

1. Introduction

Iris identification technology is a tremendously accurate biometric. Iris recognition leverages the unique features of the human iris to provide an unmatched identification technology. So accurate are the algorithms used in iris recognition that the entire planet could be enrolled in an iris database with only a small chance of false acceptance or false rejection. The technology addresses the FTE (Failure to Enroll) problems which lessen the effectiveness of other biometrics. Only the iris recognition technology can be used effectively and efficiently in large scale identification implementations. The tremendous accuracy of iris recognition allows it, in many ways, to stand apart from other biometric technologies.

British biometric passports have hacked by lucas grunwald, a consultant with a german security company, he discovered a method for cloning the information stored in new passports[11]. FastCompany.com is reporting that the biometric data of almost every Israeli citizen has been compromised and is now available on the Internet. Clearly, as more governments, such as India and Germany, collect more biometric data on their citizens, the security of such information will continue to be an issue[12]. We are concentrating our proposed work towards this issue.

Biometric authentication systems are gaining widespread popularity in recent years due to the advances in sensor technologies as well as improvements in the matching algorithms [1] that make the systems both secure and cost-effective. They are ideally suited for both high security and remote authentication applications due to the non-reputable nature and user convenience. Most biometric systems are assumed to be secure but there are chances of getting hacked. There are two places
to be attacked one is communication link attack and another one is server's database attack. In order to protect from this type of attacks we are proposing this system. However a variety of applications of authentication need to work over partially secure or insecure networks such as ATM networks or the Internet. Authentication over insecure public networks or with untrusted servers raises more concerns in privacy and security. The primary concern is related to the security of the plain biometric templates, which cannot be replaced, once they are compromised. The privacy concerns arise from the fact that the biometric samples reveal more information about its owner (medical, account, etc.) in addition to the identity. Widespread use of biometric authentication also raises concerns of tracking a person, as every activity that requires authentication can be uniquely assigned to an individual (see Table 1).

Table 1

<table>
<thead>
<tr>
<th>No</th>
<th>Advantages</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Template protection</td>
<td>It is the process of storing biometric information securely, one cannot revoke the enrolled plain biometric. Critical information could be revealed if the server’s biometric template database is compromised.</td>
</tr>
<tr>
<td>2</td>
<td>User’s privacy</td>
<td>each and every individual has different biometrics, so the privacy of the user can be easily maintained.</td>
</tr>
<tr>
<td>3</td>
<td>Trust between client and server</td>
<td>denial of service should be overcome by using public key cryptography.</td>
</tr>
<tr>
<td>4</td>
<td>Accuracy</td>
<td>false acceptance rate (FAR) and false rejection rate (FRR) should be minimized.</td>
</tr>
</tbody>
</table>

To clarify our problem, let us consider the following usage scenario:

“Person A” wants to create an account in “Person B’s mail”, that requires biometrics based authentication. However, “A” neither trusts “B” to handle his biometric data securely, nor trusts the network to send his plain biometric. The primary problem here is that, for “A”, “B” could either be incompetent to secure his biometric or even curious to try and gain access to his biometric data, while the authentication is going on. So “A” does not want to give his biometric data in plain to “B”. On the other hand, “B” does not trust the client as he could be an impostor. He could also repudiate his access to the service at a later time. For both parties, the network is insecure. A biometric system that can work securely and reliably under such circumstances can have a multitude of applications varying from accessing remote servers to e-shopping over the Internet. Table 1 summarizes the primary concerns that need to be addressed for widespread adoption of biometrics. For civilian applications, if the user is able to authenticate himself using a strongly encrypted version of his biometric (say using RSA [3]), then many of the concerns on privacy and security can be addressed. However, this would require the server to carry out all the computations in the encrypted domain itself. Unfortunately, encryption algorithms are designed to remove any similarity that exists within the data to defeat attacks, while pattern classification algorithms require the similarity of data to be preserved to achieve high accuracy. In other words, security/privacy and accuracy seem to be opposing objectives. Different secure authentication solutions try to make reasonable trade-offs between the opposing goals of security and accuracy, in addition to make specific assumptions about the representation or biometric being used.

We overcome this seemingly unavoidable compromise by designing the classifier in the plain feature space, which allows us to maintain the performance of the biometric. We show that it is possible to achieve a practical solution using distribution of work between the client (sensor) and the server (authenticator), using our proposed randomization scheme. In client we are using strong public key encryption known as RSA algorithm and in server we are using private key cryptography known as triple DES.

Figure 1. Biometric Authentication System
1.1 Characteristics of biometrics

- **Performance**: biometric details will give better performance in terms of accuracy and speed.
- **Acceptability**: which indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives.
- **Universality**: every individual has their own biometric details.
- **Distinctiveness**: no two persons are having the same biometric details.
- **Permanence**: biometric details won’t change time to time.
- **Collectability**: biometric details can be easily measured.

Table 2: Comparison between various biometrics

<table>
<thead>
<tr>
<th>Biometric characteristic</th>
<th>Universality</th>
<th>Persistency</th>
<th>Collectability</th>
<th>Performance</th>
<th>Acceptability</th>
<th>Circumvention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Iris</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Retinal Scan</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Signature</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Voice</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Thermo grain</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Mediu m</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>


2. Related Works

A wide variety of systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user, and not anyone else. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones, and ATMs. In the absence of robust personal recognition schemes, these systems are vulnerable to the wiles of an impostor. Biometric recognition, or simply biometrics, refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. By using biometrics it is possible to confirm or establish an individual’s identity based on “who he is”, rather than by “what he possesses” (e.g., an ID card) or “what he remembers” (e.g., a password). Even though there are chances of hacking plain biometric details from the database. To overcome this drawback we are proposing encrypted version of the iris to be stored.

The second existing work in the area of encryption-based security of biometric templates tends to model the problem as that of building a classification system that separates the genuine and impostor samples in the encrypted domain. However, a strong encryption mechanism destroys any pattern in the data, which adversely affects the accuracy of verification. Hence, any such matching mechanism necessarily makes a compromise between template security (strong encryption) and accuracy (retaining patterns in the data). The primary difference in that approach is that they are able to design the classifier in the plain feature space, which allows us to maintain the performance of the biometric itself, while carrying out the authentication on data with strong encryption, which provides high security/privacy.

Over the years a number of attempts have been made to address the problem of template protection and privacy concerns. Despite all efforts, puts it, “a template protection scheme with provable security and acceptable recognition performance has thus far remained elusive”. In this section, we will look at the existing work in light of this security-accuracy dilemma, and understand how this can be overcome by communication between the authenticating server and the client. Detailed reviews of the work on template protection can be found.

To provide trust between client and the server, in the existing paper they used trusted third party (TTP). It requires more computation and there is a chance of TTP can be hacked. This scenario can be overcome by public key cryptography which is used in the proposed system.

Proposed system addresses the concerns mentioned in Table 1.

1) The ability to use two different strong encryptions in client and server side addresses template protection issues as well as privacy concerns.

2) Non-reputable authentication can be carried out even between non trusting client and server using a public key cryptography solution.

3) Two way encryption enhances the security. It provides provable protection against replay and client side attacks even if the keys of the user are compromised.

4) As the enrolled templates are encrypted using a key, one can replace any compromised template,
providing revocability, while allaying concerns of being tracked.

5) Accuracy of the system can be maintained as the authentication takes place in the decrypted domain.

3. Proposed Work

The proposed system works with the following scenario. The client and server are communicating with each other, while doing the enrollment and authentication. Each and every individual has been assigned with unique user name, password. Individual’s iris has been appended with unique user name and password during enrollment. The iris has been safe guarded by using two different encryption algorithms in both client and server side in order to secure the iris both in network and database.

During authentication, One who wants to authenticate himself has to give his username, password and his iris to the authenticating server. Matching will take place in the server and on success on authentication is confirmed.

We will see elaborately by using some algorithms;

3.1 The Algorithm

Algorithm 0

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Start</td>
</tr>
<tr>
<td>2.</td>
<td>Call algorithm 1 (enrollment).</td>
</tr>
<tr>
<td>2.1</td>
<td>Call algorithm 5 (minutiae extraction) in client side.</td>
</tr>
<tr>
<td>2.2</td>
<td>Call algorithm 3 (RSA algorithm) in client side.</td>
</tr>
<tr>
<td>2.3</td>
<td>Call algorithm 3 (RSA algorithm) in server side.</td>
</tr>
<tr>
<td>2.4</td>
<td>Call algorithm 4 (3DES algorithm) in server side.</td>
</tr>
<tr>
<td>2.5</td>
<td>Store encrypted data in database.</td>
</tr>
<tr>
<td>3.</td>
<td>Call algorithm 2 (authentication).</td>
</tr>
<tr>
<td>3.1</td>
<td>Call algorithm 5 (minutiae extraction) in client side.</td>
</tr>
<tr>
<td>3.2</td>
<td>Call algorithm 3 (RSA algorithm) in client side.</td>
</tr>
<tr>
<td>3.3</td>
<td>Get encrypted data from database.</td>
</tr>
<tr>
<td>3.4</td>
<td>Call algorithm 4 (3DES algorithm) in server side.</td>
</tr>
<tr>
<td>3.5</td>
<td>Do matching.</td>
</tr>
<tr>
<td>4.</td>
<td>Reply authentication confirmation.</td>
</tr>
</tbody>
</table>

Algorithm 1: Enrollment

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Client collects multiple samples of biometric from User.</td>
</tr>
<tr>
<td>2.</td>
<td>Call algorithm 1 (enrollment).</td>
</tr>
<tr>
<td>2.1</td>
<td>Call algorithm 5 (minutiae extraction) in client side.</td>
</tr>
<tr>
<td>2.2</td>
<td>Call algorithm 3 (RSA algorithm) in client side.</td>
</tr>
<tr>
<td>2.3</td>
<td>Call algorithm 3 (RSA algorithm) in server side.</td>
</tr>
<tr>
<td>2.4</td>
<td>Call algorithm 4 (3DES algorithm) in server side.</td>
</tr>
<tr>
<td>2.5</td>
<td>Store encrypted data in database.</td>
</tr>
</tbody>
</table>

Algorithm 2: Authentication

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Client computes feature vector x1…n from input Iris.</td>
</tr>
<tr>
<td>2.</td>
<td>Requesting for key from the server.</td>
</tr>
<tr>
<td>3.</td>
<td>Each feature Xi is encrypted E1(Xi) and sent to Server.</td>
</tr>
<tr>
<td>4.</td>
<td>Server computes D1(Xi) and get Xi.</td>
</tr>
<tr>
<td>5.</td>
<td>Server gets equivalent E2(Xi) from database.</td>
</tr>
<tr>
<td>6.</td>
<td>Again computes D2(Xi) and get Xi by using triple DES.</td>
</tr>
</tbody>
</table>
Step 7: matching has been done. Store the result in S
Step 8: if S > α then
Step 9: return Accepted to the client
Step 10: else
Step 11: return rejected to the client
Step 12: end if.

Where α is minimum threshold.

While doing authentication plain biometric details have been given along with the username and password. It has to be encrypted using RSA algorithm with the key from server. Then encrypted minutiae has been forwarded to the authenticating server. In the server side RSA decryption has been carried out, then that result has been compared with already stored minutiae details of intended user. Here minimum threshold(α) has been used. If result is greater than minimum threshold then the user has been notified with “accepted” comment, else “rejected” comment will be forwarded to the client.

Algorithm 3: RSA algorithm

Key Generation:
Step 1: Select two prime no’s p & q
Step 2: Calculate n as product of p & q, i.e. n=pq
Step 3: Calculate m as product of (p-1) & (q-1)
    i.e. m = (p-1)(q-1)
Step 4: Select any integer e<m such that it is co-prime to m, i.e. gcd(e,m) = 1
Step 5: Calculate d such that de mod m = 1, i.e. d = e⁻¹ mod m
Step 6: The public key is {e,n}
       The private key is {d,n}

Encryption:
Plaintext = P & P<n
Ciphertext = C & C = P^e mod n

Decryption:
Ciphertext = C
Plaintext = P & P= C^d mod n

Algorithm 4: Triple DES

• Key size: 64 bits - 56 key bits and 8 parity bits.
• Effective key size: 56 bits.
• Block size: 64 bits.
• Rounds in the algorithm: 16.
• Type of cipher: Permutation and Substitution.

Use of multiple length keys leads us to the Triple-DES algorithm, in which DES is applied three times. If we consider a triple length key to consist of three 56-bit keys K1, K2, K3 then encryption is as follows:

• Encrypt with K1
• Decrypt with K2
• Encrypt with K3

Decryption is the reverse process:

• Decrypt with K3
• Encrypt with K2
• Decrypt with K1

Algorithm 5: feature extraction from iris

Step 1: plain iris image has been taken.
Step 2: It has to be subjected to preprocessing unit

2.1. Image size has been altered.

2.2. Clarity of image has been maintained.
Iris Localization

Both the inner boundary and the outer boundary of a typical iris can be taken as circles. But the two circles are usually not co-centric. Compared with the other part of the eye, the pupil is much darker. We detect the inner boundary between the pupil and the iris. The outer boundary of the iris is more difficult to detect because of the low contrast between the two sides of the boundary. We detect the outer boundary by maximizing changes of the perimeter-normalized along the circle. The technique is found to be efficient and effective.

Iris Normalization

The size of the pupil may change due to the variation of the illumination and the associated elastic deformations in the iris texture may interface with the results of pattern matching. For the purpose of accurate texture analysis, it is necessary to compensate this deformation. Since both the inner and outer boundaries of the iris have been detected, it is easy to map the iris ring to a rectangular block of texture of a fixed size.

Image Enhancement

The original image has low contrast and may have non-uniform illumination caused by the position of the light source. These may impair the result of the texture analysis. We enhance the iris image reduce the effect of non-uniform illumination.

3.2 Design

The proposed work has been designed in two architecture diagrams, one for enrollment and another one for authentication by using a software tool called edrawmax version 5.0.

Architecture

3.3 Implementation

The implementation has been done with the help of above two architecture diagrams. All experiments are done on an Intel Pentium dual core processor, with 2GB RAM and 160GB hard disk. In the software requirements wise windows XP operating system has been used. For front end designing purpose Visual studio 2008, and for back end data storage purpose SQL server 2005 has been used. The development language C# has been used. For RSA algorithm and 3DES, We used open source software codes from internet. For test data we used Biometrics ideal test website with the URL of http://biometrics.idealtest.org. In this implementation we have succeeded with the all five parameters which has been given in the table 1.

3.4 Result Analysis

When we are trying to adopt our technology we got this type of system performance. The system performance can be measured by means of False acceptance rate(FAR), and False rejection rate(FRR).
In our proposed system accuracy has taken as main criteria.

**False Acceptance Rate (FAR)**

The graph has been drawn with x-axis as number of persons using the system and y-axis as number of persons who are falsely accepted. From this result we can conclude that the FAR of the existing system is 0.012 and of the proposed system is 0.007.

**False Rejection Rate (FRR)**

The graph has been drawn with x-axis as number of persons using the system and y-axis as number of persons who are falsely rejected (FRR). From this result we can conclude that the FRR of existing system is 0.03 and of proposed system is 0.018.

The above graph depicts the false acceptance rate and false rejection rate of existing and proposed system. By comparing this two we can conclude that the FAR and FRR of proposed system is less than existing system.

4. **Conclusion and Future Works**

The main advantage of the proposed system involves two-level security and accuracy. Very strong encryption schemes have been used in order to provide more security. The accuracy can be achieved by means of matching algorithms. The system won’t reveal about biometric details of the person to the database. In the same way client does not know what is happening in the server. In our system we used dynamic warping based matching and variable length features of iris.

The proposed work is extremely secure under a variety of attacks and it can be used in various biometric traits. In future it can be applied to other biometrics like finger print, palm print, face recognition systems. It can applied with any other strong cryptographic algorithms.

In future instead of encryption we can use some compression algorithms and CRC (cyclic redundancy check) for high speed processing with security.

5. **References**


Authors Profile:

(1)Author S. Kavin Hari Hara Sudhan is a M.Tech student in computer science engineering, Dr. MGR University, Chennai, Tamil Nadu, India. Has published 1 International journal, 1 International conference and 3 papers in national conferences. This author can be contacted through mailmekavin.s@gmail.com

(2)Author K.P.Rajasekar is a M.Tech student in computer science engineering, SRM University, Tamilnadu, India. This author can be contacted through rajasekar88@gmail.com

(3)Author R.Balaji is a M.Tech student in computer science engineering, Dr. MGR University, Chennai, Tamilnadu. Has published 1 International conference and 2 national conferences. This author can be contacted through mailmebalaji89@gmail.com