ABSTRACT—Cryptography is the science of keeping secrets. It is mainly related to data security when transmitting data over networks. During data transmission intruders may possibly acquire information without the knowledge of sender and receiver. So it needs some mechanism to prevent unauthorized access. The security system deals with Multi-Modal biometric features namely Finger-Knuckle-Print and Finger Print for recognition and verification. This approach proves to be more secure. For every transaction, random key will be generated from the user’s samples and it could be highly distinct. Random Triangle Hashing method is used for random key generation [15]. Shuffling process is used for key management and reliable transaction. This system keeping secret the content of information from unauthorized parties, identifying data origin and preventing an entity from denying previous actions.

KEY WORDS: Finger-Knuckle-Print, Finger Print, Multi-Modal biometric features, Random Triangle Hashing, Shuffling Process.

I. INTRODUCTION

Security is an essential factor for reliable communication over networks. Cryptography is an autonomic element in order to build security. It also deals for user recognition. It is consider as one of the fundamental building block of internet security. There are three classes are cryptographic algorithms are available namely Secret key, Public key and Hash function. Symmetric cryptographic systems use the same key i.e. the decryption key is derived from the encryption key). Public key cryptographic systems use a different key i.e. the decryption key cannot be derived from the encryption key. Hash function takes as variable size message as input and delivers a fixed size hash value [1].

Biometrics is a powerful tool for human verification and authentication. It is done with the help of human biometric templates namely Finger-Knuckle-Print, Finger Print, Iris, Palm Print etc.

Recently more research going on hand based samples, because it is highly sensitive and distinct. Moreover, hand based samples provides high accuracy in their results and provides more advantageous for verification. Cryptography needs for reliable communication, but cryptography alone is not enough to achieve it. In such a way, cryptography deals with security levels and biometric handles identity of human.

Biometric key generation is mainly used for user identification. The generated key is totally differs from biometric features. So the key is never ever overridden with cryptographic systems.

II. PROPOSED SYSTEM

The main attention of this approach is to achieve secure communication during data transmission, typically the internet.
This approach uses multi-modal biometric features namely Finger-Knuckle-Print and Finger Print. The key will be generated from Finger-Knuckle-Print and Finger print for transaction. This key will be generated randomly for every transaction. The biometric key will be combined with key generated from the user’s data. So it could be secure for sharing files between sender and receiver.

III. KEY GENERATION

Key generation process takes four steps to accomplish it. The first step deals all necessary image processing activities like Image enhancement, visualizing the objects; i.e. differentiate the objects and so on. The next step is completely differing for Finger-Knuckle-Print and Finger Print. Image segmentation takes place for Finger-Knuckle-Print, because the bending surface of the knuckle portion is highly sensitive and it can be perfect for key generation. In such a way, Minutiae points are extracted from Finger Print for distinguishing the ridges. Distinguish the objects which are present in the biometric samples helps us to achieve key generation.

Overview of Finger-Knuckle-Print

Palm lines or Knuckle lines which are present in the bending surface of the finger.

A. Image Enhancement

This process helps us to improve the texture of Finger-Knuckle-Print present between the knuckle lines or palm lines. The objective of image enhancement is to achieve better image from human perception. This is done by manipulating it.

B. Image Segmentation

The session key will be generated from the knuckle portion of the finger. It is mainly because of the bending surface of the fingers are highly distinct in nature. This process achieves greater compatibility for key generation.

Overview of Finger Print

Fingerprints basically consist of ridges (raised skin) and furrows (lowered skin) that twist to form a distinct pattern.

Steps in Minutiae Extraction
1. Image Processing.
2. Minutiae Extraction
3. Post Processing

B. Random Triangle Hashing Method

It follows concept of cancellable biometrics in
the finger print domain. This approach enforces one-way property (non-invert ability) of the biometric sample.

C. Key Generation

The session keys are generated using Random Triangle Hashing Method [14].

IV. SHUFFLING PROCESS

In shuffling process the binary values of 5 and 9 are 5(0101) and 9(1001).

As shown in figure 5 random triangle hashing method [15] selects 5, 9 as the chosen co-ordinates. In shuffling process the binary representation of 5(0101) and 9(1001) are selected.

Steps

- Consider binary value of 5 as one block and 9 as one block.
- Parse the 1st block, if it is 1 append 1 to the 2nd block else if it is 0 append 0 to the 1st block itself.

<table>
<thead>
<tr>
<th>5</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>0101</td>
<td>1001</td>
</tr>
</tbody>
</table>

As shown in figure 5 random triangle hashing method [15] selects 5, 9 as the chosen co-ordinates.

V. ENCRYPTION

The transaction key is generated from the biometric templates namely Finger-Knuckle-Print and Finger Print along with the sender’s data. Encrypting the combined key is done with the help of blowfish algorithm [1]. This improves to achieve secure communication.

1. Blowfish Algorithm
2. RSA Algorithm

Encryption Process

Plain text (XOR) key (binary values) = Cipher Text

Example

Plain Text = 1010001100
Binary Key = 0101110011
XOR Operation
1010001100
0101110011
Answer: 1111111111

Decryption Process

Cipher Text (XOR) key (binary values) = Plain Text

Example

Cipher Text = 011111111111
Binary Key = 00101110011
XOR Operation
1111111111
0101110011
Answer: 1010001100

VI. EXPERIMENTAL RESULTS

Fig. 10 Key Generation from Finger-Knuckle-Print

C#.Net Screen Shot
Multi-Modal Crypto-Biometric system Based on Session Key Navigation For Secure Transaction

VII. CONCLUSION

In this paper, we proposed a Multi-Modal biometric system for secure transaction. This system provides more attention in terms of security, when compared to single instance biometric systems. The key is extracted from Finger-Knuckle-Print and Finger Print. This approach uses uniqueness of the user and how it can be efficiently used for secure transaction and authentication. In future it will be extended with other biometric samples like Iris, Palm Print, and Retina etc.

REFERENCES


![Fig. 12 Encryption and Decryption](image)

A simple client server communication establishment for file transfer using the generated dynamic session keys. The keys are encrypted and/or decrypted by both client and server for security conscious.

Table – I

<table>
<thead>
<tr>
<th>Segmented Image of the Finger-Knuckle-Print</th>
<th>Segmented Image of the Finger Print</th>
<th>Number of Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>70</td>
<td>70</td>
<td>15</td>
</tr>
<tr>
<td>75</td>
<td>65</td>
<td>17</td>
</tr>
<tr>
<td>80</td>
<td>70</td>
<td>19</td>
</tr>
<tr>
<td>85</td>
<td>76</td>
<td>21</td>
</tr>
<tr>
<td>90</td>
<td>85</td>
<td>24</td>
</tr>
</tbody>
</table>

The above table shows the number of keys needed for various X (Finger-Knuckle-Print) and Y (Finger Print) co-ordinates for a single Finger-Knuckle-Print.