ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

IJIRSET

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st & 22nd March Organized by

K.L.N. College of Engineering and Technology, Madurai, Tamil Nadu, India

Multi-Modal Crypto-Biometric System Based On Session Key Navigation for Secure Transaction

M.Natarajan[1] , T.Mekala[2] , R.Vikram[3]

[1]PG Scholar, M.Kumarasamy College of Engineering, Karur, Tamilnadu, India.

[2]Asst. Professor, M.Kumarasamy College of engineering, Karur, Tamilnadu, India.

[3]PG Scholar, M.Kumarasamy College of Engineering, Karur, Tamilnadu, India

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 possible to 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 generates 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, detecting the alteration of data, 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.

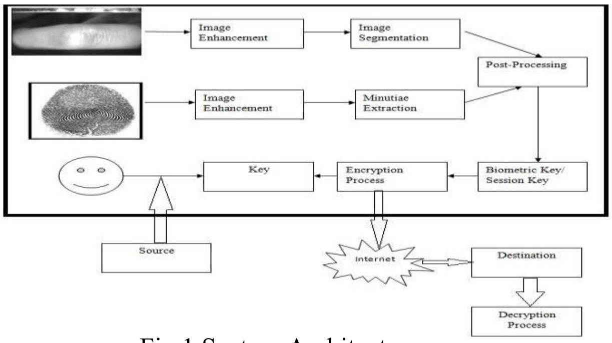


Fig.1 System Architecture

This approach uses cryptography and biometrics in order to achieve secure and reliable communication.

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

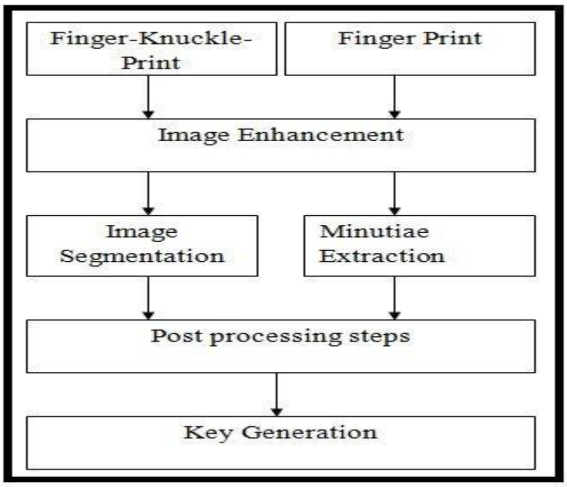


Fig. 2 Key Generation

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 the Finger-Knuckle-Print

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

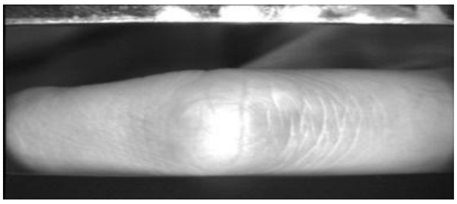


Fig. 3 Finger-Knuckle-Print

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.

Fig.4 Overview of Finger Print

A. Minutiae Extraction

It improves the quality clarity of the Finger Print based on the frequency and orientation of the local ridges and extracts the correct minutiae.

Steps in Minutiae Extraction

1. Image Processing.

2. Minutiae Extraction

3. Post Processing

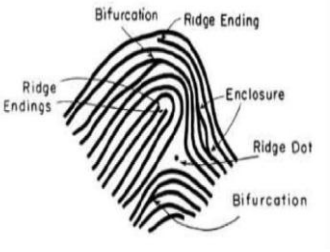


Fig.5 Example for Minutiae points

Fig. 6 Input Image

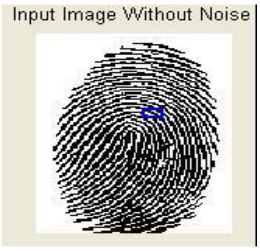


Fig.7 Noise removal image

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 Hasing Method [14].

IV. SHUFFLIN PROCESS

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

As show 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.

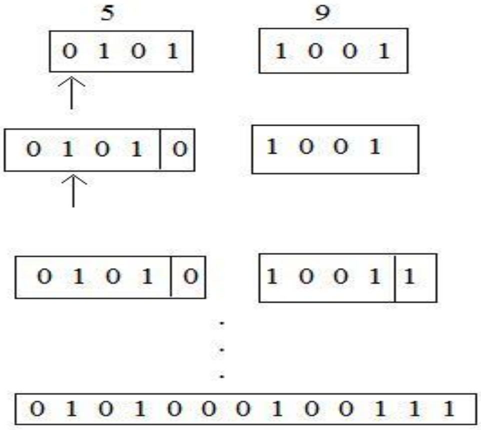


Fig.8 shuffling process

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

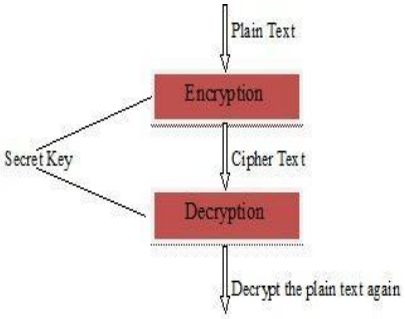


Fig. 9 Encryption Process

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 = 01111111111

Binary Key = 00101110011

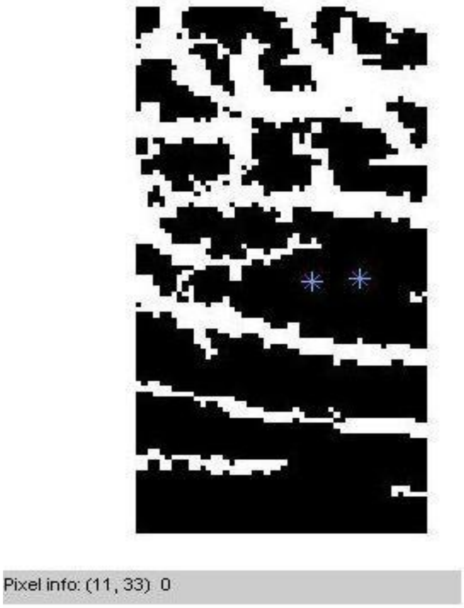
XOR Operation

1111111111

0101110011

Answer: 1010001100

VI. EXPERIMENTAL RESULTS



Pixel info: (11, 33) 0

Fig.10 Key Generation from Finger-Knuckle-Print

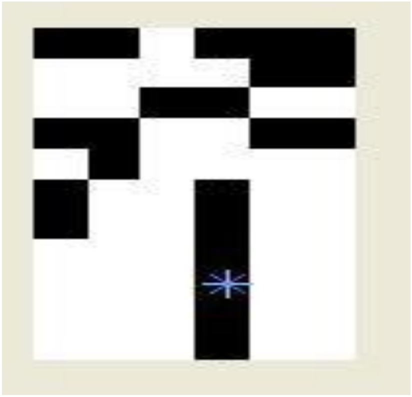
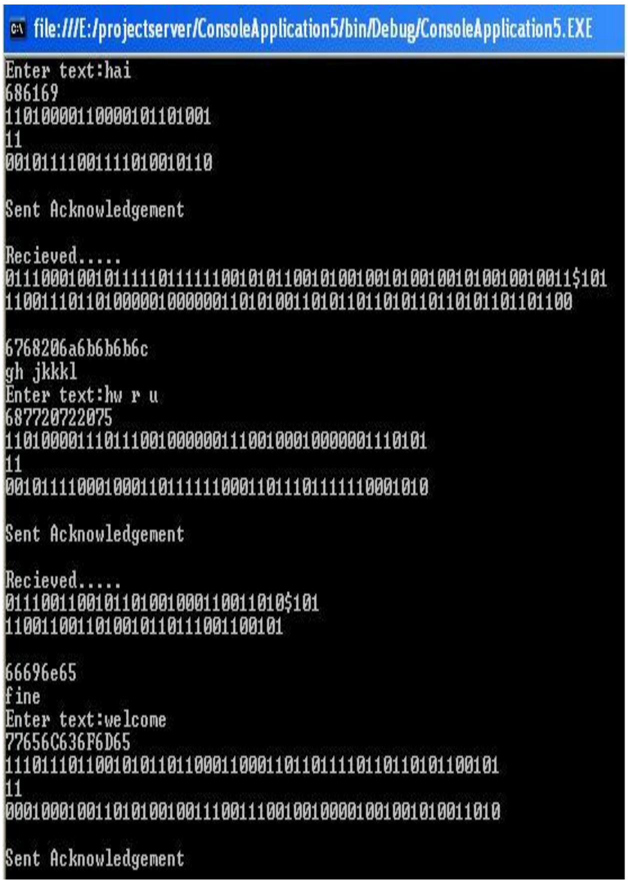


Fig.11 Key Generation from Finger-Print C#.Net Screen Shot


file:///E:/projectserver/ConsoleApplication5/bin/Debug/ConsoleApplication5.EXE

```
Enter text:hai
686169
11010000110000101101001
11
00101111001111010010110

Sent Acknowledgement

Recieved.....
011100010010111110111111001010110010100100101001001010010010011$101
110011101101000001000000110101001101011011010110110101101101100

6768206a6b6b6b6c
gh jkkkl
Enter text:hw r u
687720722075
11010000111011100100000011100100010000001110101
11
00101111000100011011111100011011101111110001010

Sent Acknowledgement

Recieved.....
0111001100101101001000110011010$101
1100110011010010110111001100101

66696e65
fine
Enter text:welcome
77656C636F6D65
1110111011001010110110001100011011011110110110101100101
11
0001000100110101001001110011100100100001001001010011010

Sent Acknowledgement
```

Fig. 12 Encryption and Decryption

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

Key Generation Process

Segmented Image of the Finger-Knuckle-Print	Segmented Image of the Finger Print	Number of Keys
70	70	15
75	65	17
80	70	19
85	76	21
90	85	24

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.

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

[1] T.Mekala and N.Madhu Suganya, "Secure Transaction Using Dynamic Session Key", International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue-4, March 2013..

[2] E-channel System of the Hong Kong government, http://www.immd.gov.hk/ehtml/20041216.ht m

[3] A. Kumar and Y. Zhou, "Personal identification using finger knuckle orientation features ",ELECTRONICS LETTERS 24th September 2009 Vol. 45 No. 20.

[4] Rui Z, Tao L, Shunyan H, Jianying S, " A Novel Approach of Personal Identification Based on the Fusion of Multifinger Knuckleprints" Advances in information Sciences and Service Sciences(AISS) Volume3, Number10,November 2011.

[5] M.Bhavani and Mrs.ShobaRani, "Human Identification Using Finger and Iris Images" International Journal of Computer Trends and Technology- volume4, Issue3- 2013.

[6] A. Muthukumar and S. Kannan, "Finger Knuckle Print Recognition With Sift and K-Means Algorithm" ICTACT Journal on Image and Video Processing, February 2013, Volume: 03, Issue: 03 583

[7] Shubhangi Neware, Dr.Kamal Mehta and Dr.A.S.Zadgaonkar, "Finger Knuckle Identification using Principal Component Analysis and Nearest Mean Classifier" International Journal of Computer Application (0975-8887) Volume 70-No.9, May 2013.

[8] Mrs.S.S.Kulkarni and Dr.Mrs.R.D.Rout, "Secure Biometrics: Finger Knuckle Print" International Journal of Advanced Research in Computer and Communication Engineering Vol.1, Issue 10, December 2012.

[9] Ajay Kumar, Senior Member, IEEE, and Ch. Ravikanth, "Personal Authentication Using Finger Knuckle Surface" IEEE Transactions on Information Forensics and Security, Vol. 4, No. 1, March 2009.

[10] Rui Zhao, Kunlun Li , Ming Liu and Xue Sun, "A Novel Approach of Personal Identification Based on Single Knuckleprint Image" Asia-Pacific Conference on Information Processing, 2009.

[11] Lin Zhang, Lei Zhang, and David Zhang, "Finger-Knuckle-Print: A New Biometric Identifier", Biometrics Research Center, Department of Computing, The Hong Kong Polytechnic University, Hong Kong, China.

[12] Lin Zhang, Lei Zhang, and David Zhang, "MonogenicCode: A Novel Fast Feature Coding Algorithm with Applications to Finger-Knuckle-Print Recognition" IEEE Transaction 2010.

[13] A.Morales, C.M. Travieso, M.A. Ferrer and J.B. Alonso, " Improved Finger-Knuckle-Print Authentication based on Orientation Enhancement" ELECTRONIC LETTERS, Vol. 47, No. 6, 17th March 2011.

[14] Zhe Jin, Andrew Beng Jin Teoh, hian Song Ong, and Connie Tee,"Secure Minutiae- Based Fingerprint Templates Using Random Triangle Hashing" IVIC 2009, LNCS 5857, pp. 521–531. Springer-Verlag Berlin Heidelberg 2009.