iJRASET
International Journal For Research in
Applied Science and Engineering Technology

Volume: 5 Issue: IV Month of publication: April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4096

www.ijraset.com
IC Value: 45.98

Volume 5 Issue IV, April 2017
ISSN: 2321-9653

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secured Fingerprint based Crypto System with Reversible Watermarking Scheme

Lakshmi Saranya. R [1], Rini. R [2], Kalimuthu. T [3]
[1,2,3] Department of ECE, SCADCET, Tamil Nadu, India

Abstract: As the growth of technology every information is passed widely through the internet. To ensure the secure data transmission, cryptography is the most effective solution. Cryptographic key plays an important entity to overcome channel attacks. High security is difficult in randomly generated cryptographic keys. Here random key needs to be stored in a protected place or it must transported through a shared communication line. As an alternative to this, the generation of finger print based key using the biometric information of sender/receiver is introduced. Thus avoiding key storing and at the same time without compromising the strength in security. Biometric based cryptographic key generation has some difficulties to maintain privacy of biometrics and key generation at receiver in present error data. Biometric key is generated from matching process that enrolls highly secured cryptosystem. Implementation of this proposed work has been analyzed using reversible watermarking scheme.

Key words: Biometric key, cryptosystem, reversible watermarking, cryptographic key, Biometrics.

I. INTRODUCTION

Information security and a secure transmission of data become very important in information and communication technology. A third party can trap data or steal important data stored in a computer. To prevent this, it is advocated to encrypt the messages to provide information security. This type of protection is usually provided using cryptography.

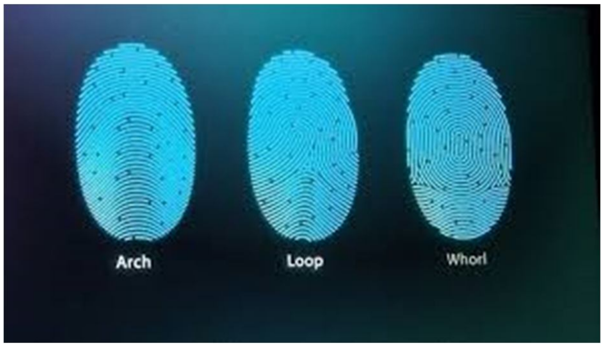


Fig 1 Types of fingerprint

Finger print recognition process, the most famous biometric authentication technique is performed to produce better stability and individuality. Finger print recognition process can be classified into two methods

A. Texture Based Recognition
B. Minutiae Based Recognition

Compared to texture based finger print recognition, minutiae based recognition is reliable. So that water marking fingerprint matching method is motivated in present work.

Water marking is the process of in which the information verifies the owner is embedded into the digital image or signal. These signals could be either video or picture. Water marking is used to verify the identity and authenticity of the owner of a digital image. Water marking technique can be classified into various categories. It can be categorised according to be water marked as below,

C. Text Watermarking
D. Image Watermarking
E. Audio Watermarking

F. Video Watermarking

Watermarking algorithm consists of different parts

G. Watermark

H. Encoder

I. Decoder

J. Crypto-Biometric System

Biometric is being integrated with cryptography (called crypto-biometric system) to alleviate the limitations of the above-mentioned systems. Biometric is the unique measure of the identity of individuals with their behavioral and physiological traits like face, fingerprint, iris, retina, palm-print, speech. Cryptography is intended to ensure the secrecy and authenticity of message. Cryptographic key used for securing information during encryption and decryption will usually be long and is very difficult to remember. Protecting the confidentiality of this key is a major concern. This can be efficiently solved by Biometric Cryptosystems. Biometric cryptosystems combine biometrics and cryptography to benefit from the strengths of both fields. In such systems, while cryptography provides high security levels, biometrics brings in non repudiation and eliminates the need to remember passwords or to carry tokens. Instead of storing cryptographic keys, keys will be generated dynamically with the help of biometrics to secure the template and biometric system. Biometric cryptosystems can be used for biometric template security.

II. EXISTING MODEL

A key binding system based on n-nearest minutiae structure of fingerprint," E. Liu et al., ,pattern Recognit Lett, volume 32, no 5,666-676,..2011[7]. In this paper [7] they design a system with n-nearest minutiae structure of a finger print and the majority of matching time is spent on the searching of paring minutiae. Three levels of secure sketch are applied to encryption domain. and Shamir's secret sharing scheme is used to bind and recover a key based on template minutia structures.Two-level construction is used to tolerate noises in a minutia structure, and Shamir's secret sharing scheme is adopted for key binding and recovering. The stored information should be independent to that of nearest structure; improve the security level against brute force attack of a structure .[3] Emanuele maiorana, patrizio campisi, alessandro neri "Iris template protection using a digital modulation paradigm" IEEE international conference on acoustic, speech and signal processing (icassp)2014.In this paper they use the biometric crypto system uses the digital modulation paradigm . The effectiveness of this approach is evaluated by performing tests on the Interval subset. This cryptosystem, inspired by the digital modulation- channel coding - transmission - channel decoding - demodulation chain of digital data transmission over a noisy channel.It stores the additional data this is the disadvantage of digital modulation .

Dual layer structure check (dlsc) fingerprint verification scheme designed for biometric mobile template protection, school of computer science and itrmit university melbourne, kai xi and jiankun hu Australia,2013[6].In this paper crypto system uses fingerprint verification algorithm based on composite features which are reliable, distortion tolerant and registration free. This paper investigated a new minutiae based local structure represented by composite features. [5] A Security-Enhanced Alignment-Free Fuzzy Vault-Based Fingerprint Cryptosystem Using Pair-Polar Minutiae Structures., Cai Li, Jiankun Hu.,v, March 2016.In this paper [5] they design a fingerprint based system using pair-polar (P-P) minutiae structures and the finger print is encrypted using fuzzy vault and Shamir's secret sharing Scheme. The security of fuzzy vault scheme is based on the infeasibility of the polynomial reconstruction problem The security of fuzzy vault scheme is based on the infeasibility of the polynomial reconstruction problemThe disadvantage of this paper is template/key protection without Registration.

A new bio cryptosystem-oriented security analysis framework and implementation of multibiometric cryptosystems based on decision level fusion IEEE, jiankun hu, josef pieprzyk, and willy susilo, [2] cai li, student member" IEEE transactions on information forensics and security, vol. 10, no. 6, june 2015.In this paper point out limitations of entropy-based security analysis and propose a new security analysis framework that combines information-theoretic approach with computational security. To construct a fingerprint-based multi biometric cryptosystem (MBC) using decision level fusion. Hash functions are employed in our construction to further protect each single biometric trait.

A dissection of fingerprint fuzzy vault schemes" the university of auckland new zealand, [4] vedrana krivokuća, waleed abdulla, akshya swai 2014. In this paper the fuzzy vault construction is adopted for the protection of fingerprint data.An alignment-free fingerprint cryptosystem based on fuzzy vault scheme, Journal of network and computer applications, peng li , xinyang , kaicao , xunqiangtao, ruifangwang , jietian 33 (2010) 207–220[1]. In this paper, an alignment-free fingerprint cryptosystem based on fuzzy vault scheme is developed fusing the local features.

III. PROPOSED MODEL

The proposed model is used to hide and secure the information. The objective of the proposed technique is to implement a highly secured finger print based cryptosystem using advanced encryption algorithm and reversible watermarking technique. The Fig 2 block diagram which helps to understand the proposed system.

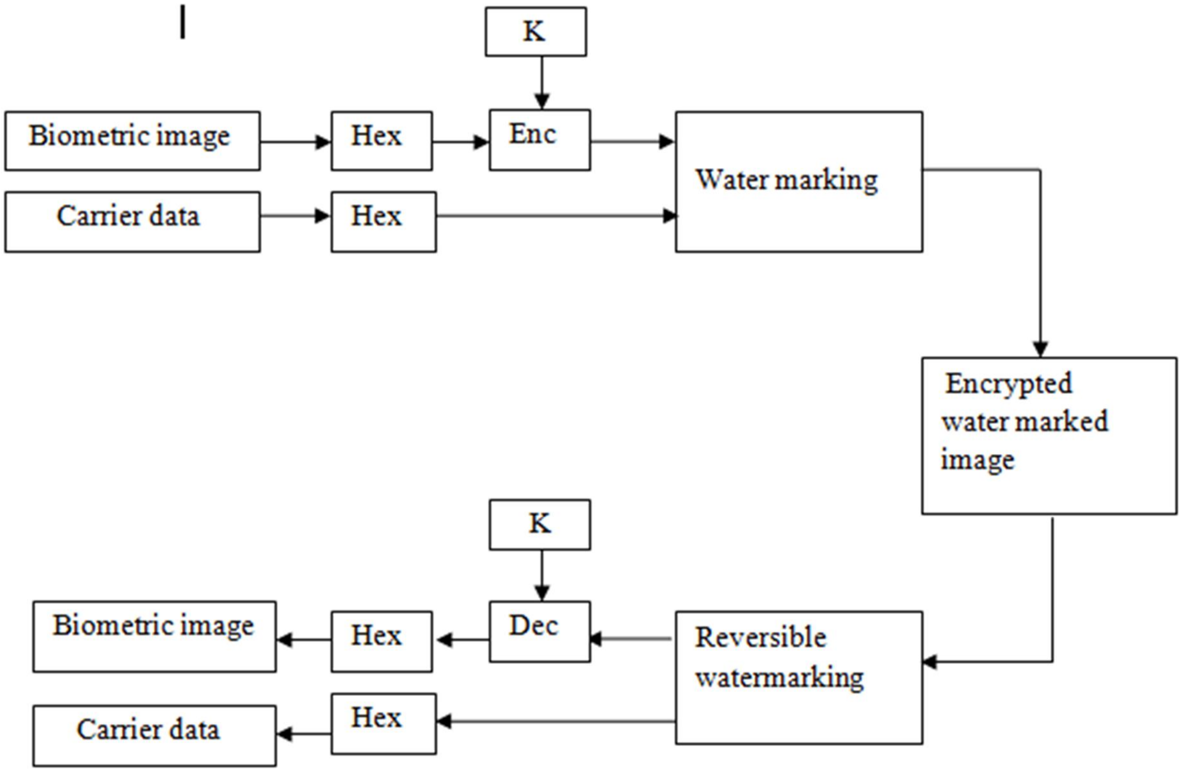


Fig 2- Block Diagram of the Proposed System

The following are the processing steps of the proposed system.

A. At the sender side, the biometric image and the carrier data are converted into hexadecimal values using MATLAB software.
B. Then the hexadecimal values are encrypted using advanced encryption algorithm.
C. The encryption process: Biometric image-Biometric hex value-Add round key-Shift row and Mixed column-Encrypted hex value-Encrypted biometric image.
D. Then the encrypted biometric image is watermarked using watermarking process.The watermarked output image is highly secured. No one can easily detect the information.At the receiver side, apply a reversible watermarking technique to obtain the original biometric image.
E. Finally we get the original biometric image and carrier data are received at the receiver side with high security.

Fig 3(A) Input image

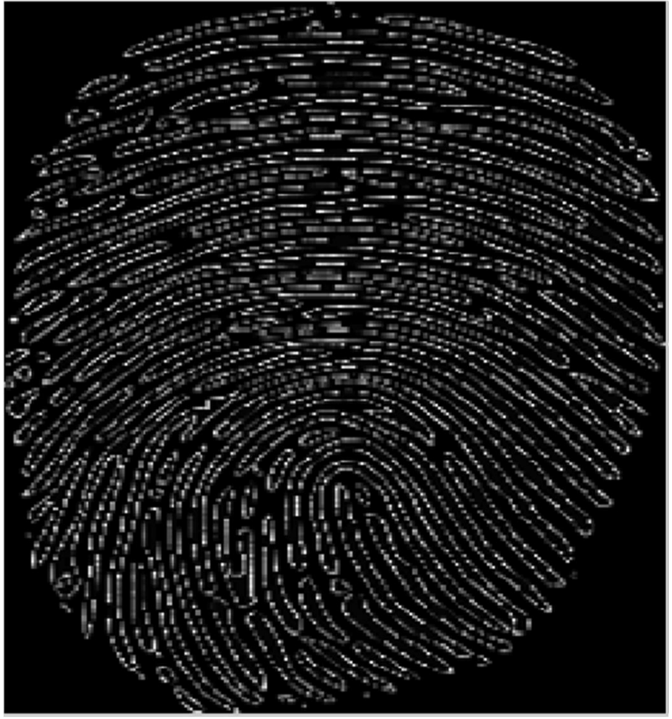


Fig 3(B) Encrypted image

The Fig 3(A) shows the input image. The finger print image is in scalable vector graphics in an extensible markup language(xml). This is the document formatting format. The svg images can be created and edited with any text editor. This images can be printed with high quality at any resolution. The Fig 3(B) shows the encrypted image. The encrypted text file is given to the MATLAB .Here the text file is converted into image. This finger print image is called as encrypted image.

IV. CONCLUSION

Highly secured finger print based crypto system is proposed using advanced encryption algorithm. The proposed technique improves the security than the fuzzy vault scheme by matching process in minutiae structure. The protection of the biometric image is done by the fingerprint based reversible watermarking. The security mechanism is also maintained and the verification is satisfied.

REFERENCES

[1] Peng Li , XinYang , KaiCao , XunqiangTao, RuifangWang , JieTian, 2010 “An alignment-free fingerprint cryptosystem based on fuzzy vault scheme” Journal of Network and Computer Applications 33 , 207–220.

[2] Cai Li, Student Member, IEEE, Jiankun Hu, Josef Pieprzyk, and Willy Susilo, june 2015.“A new biocryptosystem-oriented security analysis framework and implementation of multibiometric cryptosystems based on decision level fusion” IEEE transactions on information forensics and security, vol. 10, no. 6.

[3] Emanuele Maiorana, Patrizio Campisi, Alessandro Neri,2014 “Iris template protection using a digital modulation paradigm” IEEE International Conference on Acoustic, Speech and Signal Processing (ICASSP)

[4] Vedrana Krivokuća, Waleed Abdulla, Akshya Swai, 2014 “A dissection of fingerprint fuzzy vault schemes” The University of Auckland New Zealand.

[5] A Security-Enhanced Alignment-Free Fuzzy Vault-Based Fingerprint Cryptosystem Using Pair-Polar Minutiae Structures”., Cai Li, Jiankun Hu., MARCH 2016, IEEE transactions on information forensics and security, vol. 11, no 3

[6] Kai Xi and Jiankun Hu, 2013 “Dual layer structure check (dlsc) fingerprint verification scheme designed for biometric mobile template protection” School of Computer Science and ITRMIT University Melbourne, Australia.

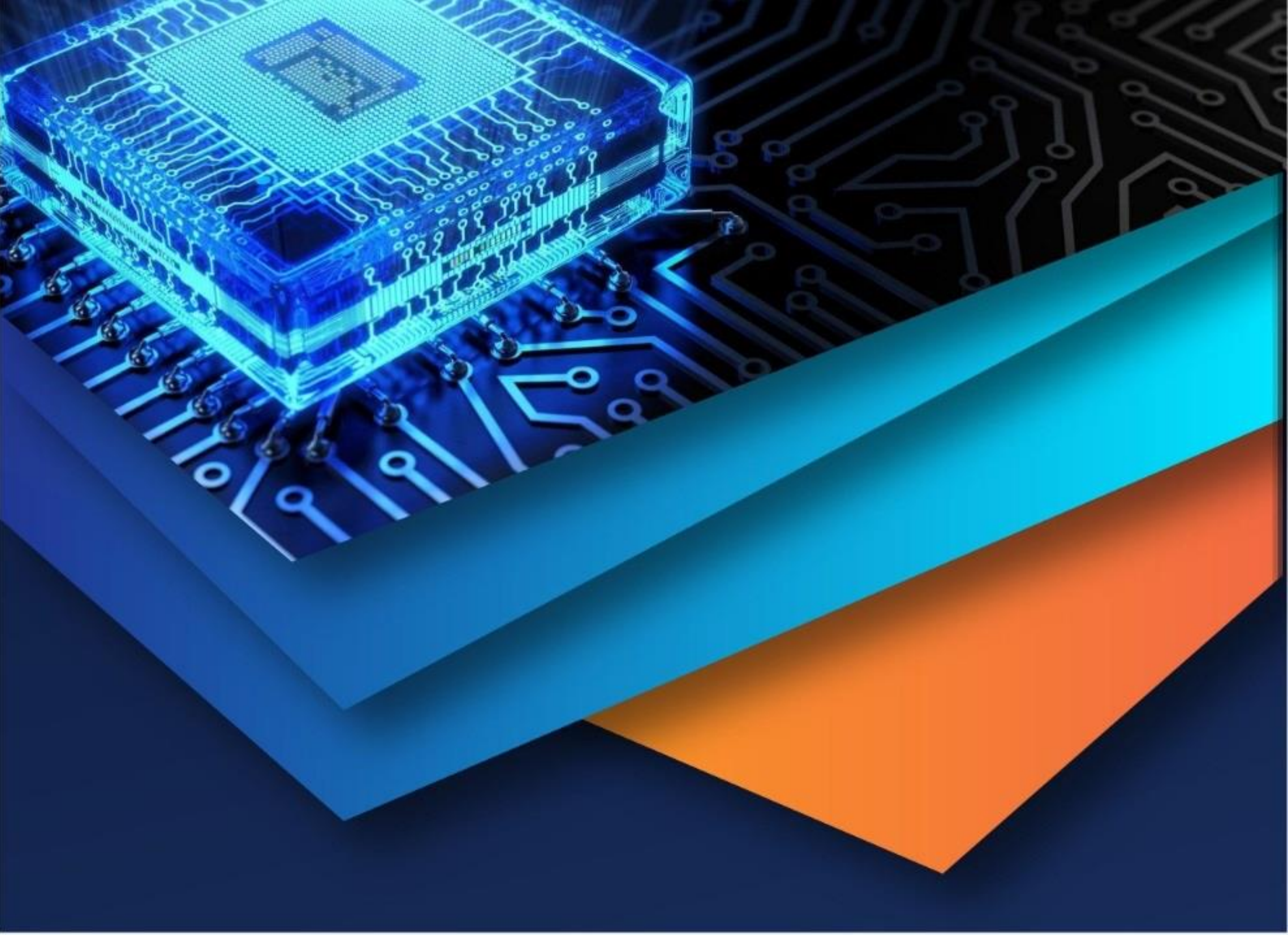
[7] Eryun Liu , Heng Zhao , Jimin Liang , Liaojun Pang , Min Xie , Hongtao Chen , Yanhua Li, Peng Li,Jie tian, 2011 “A key binding system based on n-nearest minutiae structure of fingerprint”Pattern Recognition Letters 32,666-675.

[8] Prabhiseek singh,R.S.Chandha,”A survey of digital watermarking techniques and applications and attacks”.,International journal of Engineering and Innovative technology(IJEIT),volume2,Issue 9,March 2013.

[9] D.Kundur,D.Hatzinakos,”Digital watermarking for telltale tamper proofing and authentication” In proceeding of the IEEE,(1999),pp.1167-1180.

[10] Manpreet kaur,Sonia jindal,Sunny bahal,”A study of digital image watermarking”,volume 2,Issue 2, Feb 2012.

[11] Balamurugan.G,Senthil.M,”A fingerprint based reversible watermarking system for the security of medical information”, World conference on futuristic in research and innovation for social welfare(WCFTR)2016.



10.22214/IJRASET

INDEX COPERNICUS
45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY