A FINGERPRINT BASED REVERSIBLE WATERMARKING SYSTEM FOR THE SECURITY OF MEDICAL INFORMATION

BALAMURUGAN.G
Assistant Professor
Department of Computer Science and Engineering
Christ College of Engineering and Technology
Pondicherry University
Pondicherry, India
gbalamurugan1991@gmail.com

SENTHIL.M
Associate Professor/Head of the Department
Dean (School of Computing)
Department of Computer Science and Engineering
Christ College of Engineering and Technology
Pondicherry University
Pondicherry, India
christhodcse@gmail.com

Abstract— **As the growth of technology every information is passed widely through internet. To provide the security to the information many cryptography algorithms is introduced. Now various researches are going on for the protection to the medical information. As it was under a wide research field, to perform the security to the medical information using the finger print biometric and reversible watermarking techniques in the MDBMS and providing CIA. To provide integrity for the medical data and to detect the medical image modification using the finger prints biometric based cryptosystem and reversible watermarking technique. Proposed system uses the finger print biometric for authentication, symmetric as well as public key for cryptography process and reversible watermarking the encrypted data into medical image. To provide CIA methodology for the MDBMS and also ensuring conformation SMS to the patient for the convenient, that their information had reached safely to the corresponding destination. Implementation of proposed work has been analyzed using performance measures and implementation is carried out.**

Index Terms— MDBMS, CIA, SMS, cryptography.

I. INTRODUCTION

Medical Database Management System plays a vital role in current research filed. To provide the secure transaction and maintainability of patients information and then to secure medical image from critical issues like malpractice liability, image retention etc [1, 2]. In order to avoid the issues we combine three different research domains namely fingerprint biometric for authentication, cryptosystem for confidential data and reversible watermarking for the integrity. Under serious analysis and study of three domains we contributed this proposal.

Image processing consists of a wide variety of techniques and mathematical tools to process an input image. An image is processed as soon as we start extracting data from it. As an emerging technology, digital watermarking includes the ideas and models of different subject coverage, such as cryptography, network technology, algorithm design [3, 4]. Digital watermarking hides the copyright data into the digital data through a definite algorithm [7]. The secret data to be embedded can be some text, author's serial number, company logo, images. This protected information is inserted into the digital data to ensure identification and verification of the owner and copyright security. The watermark can be concealed in the digital data either visible or invisible form. For a robust watermark embedding, a virtuous watermarking technique is desired to be applied. The watermark can be embedded whichever in spatial or frequency domain.

II. PROPOSED WORK

To provide integrity for the medical data and to detect the medical image modification using the biometric based cryptosystem and watermarking technique. Ensuring conformation SMS to the patient for the convenient, that their information have reached safely to the corresponding destination. Transformation of medical image and the related information about the patient form one hospital to another hospital for concerning purpose. Providing medical image, patient information and finger print of particular patient. The finger print biometric system is used to provide the symmetric key encryption of the information and that information gets watermarked (invisible watermark) into the medical image. The watermarked image and the encrypted key is transferred to the another hospital and the notification is sent to the corresponding patient via SMS. Then in the receiver side, the information is store in the database. Recognition of finger print and corresponding authorization technique is carried to check the authorization.

978-1-4673-9214-3/16/$31.00 © 2016 IEEE

If it is valid match the information is decrypted and retrieved the actual information else the authorization failed. It provide input with medical image, information and biometric of patient. The biometric key is generated using row wise DCT is used to provide the symmetric key encryption and then the information is gets watermarked (invisible watermark) into the medical image. The symmetric key we used is encrypted using the public key. The watermarked image and the encrypted key is sent to the another hospital where they have to reach and the notification is sent to the corresponding patient. Then in the receiver side, they store in the database and decrypt the key using the private key. They compare the input biometric and check the authorization If matched the information is decrypted and retrieved the actual information and the medical image If not matched the authorization failed Message is displayed.

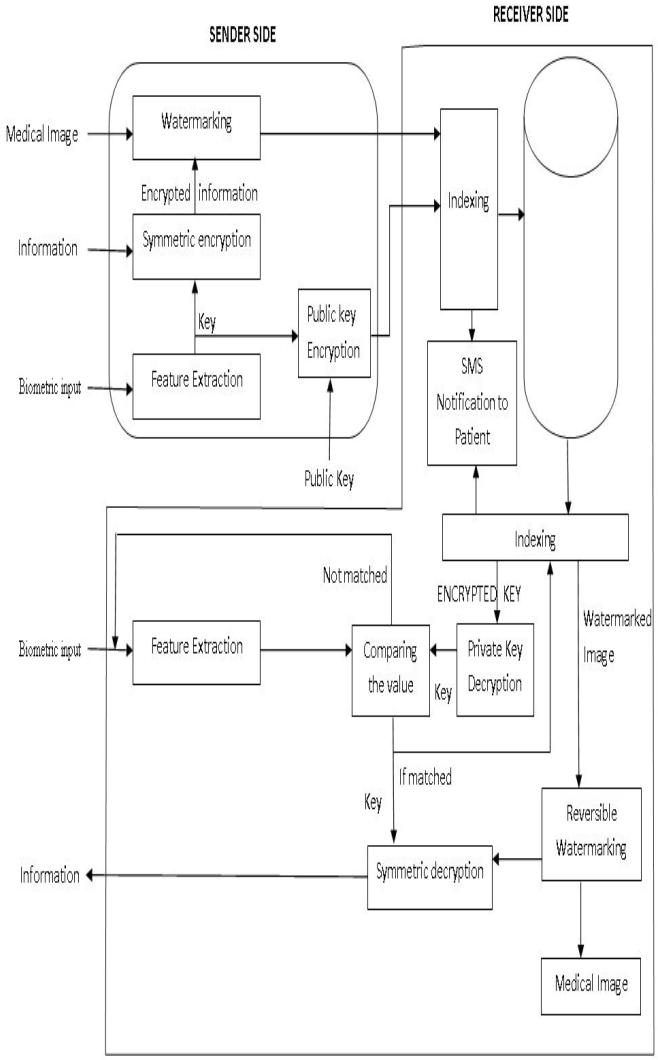

FIGURE 1: BLOCK DIAGRAM FOR THE PROPOSED WORK

III. MODULES

There are totally seven modules as they are listed following,

1. Finger Print Extraction
2. Information Encryption
3. Watermark Embedding
4. Sender/Receiver Process
5. SMS Notification
6. Reversible Watermarking
7. Information Decryption

IV. MODULES DESCRIPTION

A. FINGER PRINT EXTRACTION

To provide the authentication and authorization and allow only the authorized user can access the information of the patients so we propose the biometric authentication for this system. We have selected fingerprint as the biometrics feature for generating cryptographic key. We have extracted minutiae points from the fingerprint and used that point set for generating cryptographic key. Fingerprint biometric is widely used in various fields for security [5, 6]. A Fingerprint contains patterns of valley and ridges on the surface of finger lips.

B. IMAGE PREPROCESSING

For image preprocessing Histogram Equalization and Filters are used to enhance the image. Binarization is applied on fingerprint image. Then Morphological operation is used to extract Region of Interest.

C. HISTOGRAM EQUALIZATION

Histogram equalization mechanism is used for improving the contrast of images, where usable data of the image represented by neighbor contrast values. It focuses on pixel value to expand. The Fingerprint image uses bimodal specification. Histogram equalization transforms range from 0 to 255 which will increase visualization effect.

Figure 2: Sample Finger Print before and After Histogram Equalization

Median Filter is nonlinear, digital filter methodology employed to eliminate noise from image or other signals. The values present in frames are ordered in numeric order the median value, the sample in the center of the frame is chosen as output.

D. REGION OF INTEREST

The steps in this are Binarization and Morphological operation

E. BINARIZATION

All minutiae extraction algorithms works on binary images, black pixels present in the image which denotes ridges, and then the white pixels that denote valleys. Binarization is a mechanism that converts a grey level image into a binary image. Hence Binarization process involves analyzing grey level values of each pixel, if values are greater than the global threshold set binary value as 1 or 0 vice versa.

F. MORPHOLOGICAL OPERATION

Neighborhood operations are generally designed to alter the appearance of an image for visual considerations; morphological operations are used to recognize the structure or form of an image. There are three essential morphological functions: erosion, dilation, and hit-or-miss. Morphological operations are performed on binary images where the pixel values are either 0 or 1.

For ease, refer to pixels as 0 or 1, and will show a value of zero as black and a value of 1 as white. While most morphological operations focus on binary images. Binary morphological operators are applied on binarised fingerprint image [8, 9, 10].

Thinning is a mechanism carried out in morphological operation that is used to eliminate selected foreground pixels from binary images, somewhat like erosion or opening. It can be used for several applications, but is predominantly useful for skeletonisation. Thinning applied to binary images, and produces another binary image as output.

G. MINUTIAE POINTS EXTRACTION

Thinning eradicates the redundant pixels of ridges till they are just one pixel wide. Ridge thinning algorithm is applied and in each scan of full fingerprint image, the algorithm marks down redundant pixels in each small frame and finally removes all those marked pixels after several scans. After fingerprint ridge thinning minutiae points are focused.

H. MATRIX & KEY GENERATION:

The key generation algorithm is as follows Extracted minutiae point's co-ordinates are maintained in a vector

M_p- Minutiae points set

S_p - Size of M_p

KL=key length

K_v-Key Vector

L_k -Length of key vector

Z - (X, Y) co-ordinate of a minutiae point

Step1: Read the Minutiae points

Step2: Find the point H with highest x+y

Step3: Draw a line from origin (0, 0) to the H and call it as L

Step4: Sort the Minutiae points and Store in an array A.

Step5: value= KL / Np

Vector=KL % Np

Step6: For i=1 to value

For j=1 to Sp

Read point X from Array A and Check the point whether it is above or below the line L. If it is above the line or on the line put value as „0 else value is „1 .Store them in array K.

Final key=Append the key vector of length vector to value of K.

From this we obtained 128-bit key value from the fingerprint biometric template for the information encryption.

V. PRINCIPALS OF FINGER PRINT BIOMETRICS

A fingerprint is combination of ridges and valleys on the surface of the finger. Ridges are termed as the upper skin vision layer segments of the finger and valleys are the lower segments. The ridges form minutia points which are defined as ridge endings and ridge bifurcations. Many types of minutiae exist, including dots, lakes, spurs, bridges and crossovers.

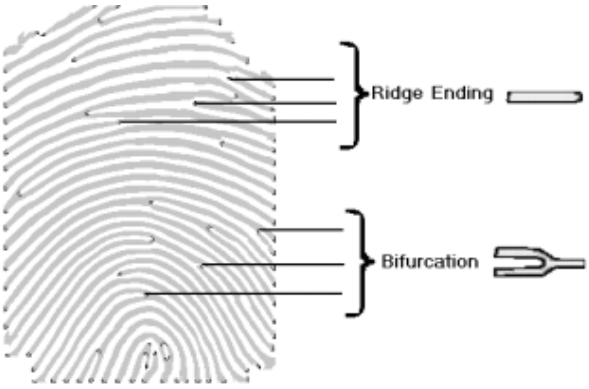

Figure 3: Finger print image.

VI. INFORMATION ENCRYPTION

To provide the confidential information of the patients we propose an encryption for information of the patients using symmetric key. The functions of biometric systems are determining, measuring and codification of the unique characteristics of individuals with one already recorded. In biometric cryptosystems, a cryptographic key of 128-bit is generated using finger print biometric template. It cannot be revealed without a successful biometric authentication.

VII. WATERMARKING

Reversible watermarking is used for the embedding the encrypted information of the patients in the medical image [11, 12].

In this the original image is divided in to sub blocks and then we use wavelet transform and singular value decomposition for the medical image and then using the reversible watermarking approach called quantization algorithm for embedded the data in the medical image and we perform inverse SVD and also the inverse transform to maintain the reversible property and finally we obtained the watermarked medical image [13, 14]. In this we embed only 16-bytes of patient's data in the medical image.

A. WATERMARKED EMBEDDING PROCESS:

Step 1: The original image (I) is divided into sub-blocks Bk, where k =1, 2... N, N =Ww X Wh, Ww and Wh are the width and height of the watermark, respectively.

Step 2: Two-level wavelet transform is applied to each sub-block. We select coefficients in the low frequency part to enhance robustness against additive noise, filtering, and JPEG compression.

Step 3: Perform SVD on the low frequency wavelet coefficient of each block to generate SVs (Sk).

Step 4: Watermark bits are embedded by quantization using the reversible watermarking algorithm; the SV's of wavelet approximate co-efficients are selected to be quantized since the first Sv's are most robust to geometric distortion.

Step 5: Apply SVD calculation to obtain updated SVs for the host signals

Step 6: the IWT is performed to obtain the watermarked host medical image (I*)

VIII.SENDER/RECEIVER PROCESS

The watermarked image and the encrypted key is sent to the another hospital where they have to reach and the notification is sent to the corresponding patient. Then in the receiver side, they store in the database and decrypt the key using the private key.

IX. SMS NOTIFICATION

The SMS is used to carry out for the notification to the user for their convenient.

X. REVERSIBLE WATERMARKING

Reversible watermarking is used for the retrieved the encrypted information of the patients in the medical image [15].

A. WATERMARKED EXTRACTION PROCESS:

Step 1: The watermarked host medical image (I) is partitioned into sub-blocks Bk, Where k =1, 2..., Ww X Wh.

Step 2: Two-level wavelet transform is performed to each sub block Bk. The approximate coefficients are selected for SVD calculation.

Step 3: Perform SVD on the low frequency of each block to generate SVs (Sk).

Step 4: The SVs (Sk) is then normalized according to

$$S_N^{**k} = \| S^{**k} \|$$

Step 5: The final message is obtained

XI. INFORMATION DECRYPTION

They compare the input biometric and check the authorization If matched the information is decrypted and retrieved the actual information and the medical image If not matched the authorization failed Message is displayed.

XII.PERFORMANCE METRICS

A. Biometric Analysis

The performance of fingerprint recognition is evaluated using the false acceptance rate (FAR) and false rejection rate (FRR).The false acceptance rate is the measure that the biometric security will incorrectly recognize an access attempt by an unauthorized addict. FAR typically is stated as the ratio of the number of false acceptance to the number of identification attempts.

The false rejection rate or FRR is the measure of the biometric security will incorrectly decline an access attempt by an authorized addict. FRR typically is declared as the ratio of the number of false rejections divided by the number of identification attempts.

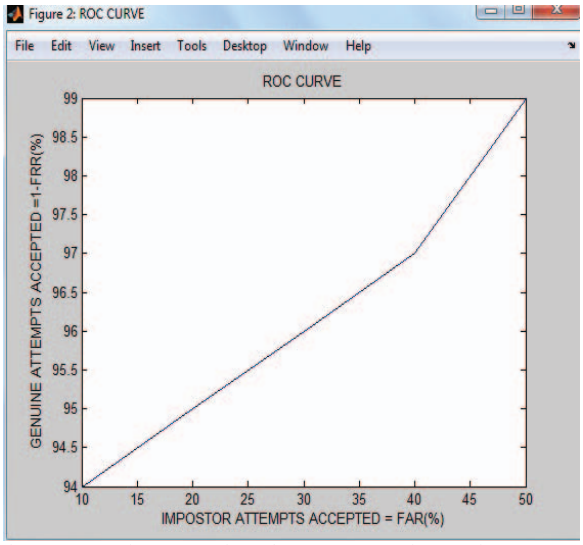

Figure 4: Receiver Operating Characters curve for genuine attempts.

B. Image quality analysis

PSNR of original image and PSNR of watermarked Image is compared the original content of medical image is not affected.

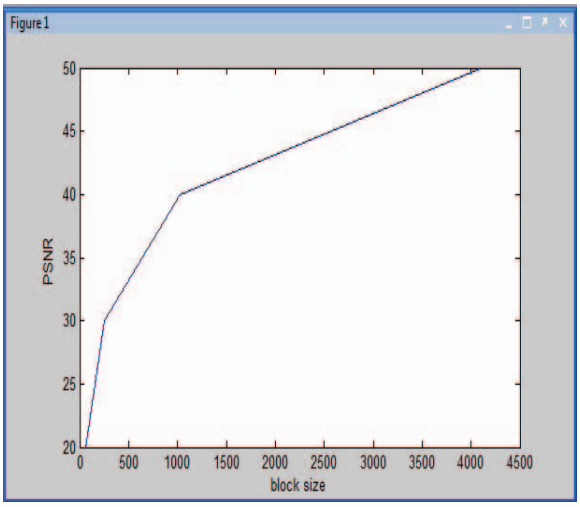

Figure 4: Image Analysis.

XII .Implementation Results

The proposed work is implemented with the help of DOTNET framework. The proposed work can be used as an application for the medical information transmission in the field of e-health care.

A. Home page

It consists of many options like Add new Patient, Add New Doctor, etc. The transformation such as sending and receiving the details of patient's information with cryptographic analysis are manipulated.

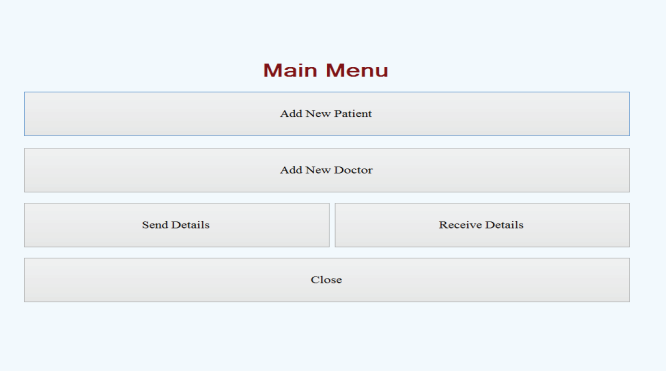

Figure 4: Home Page

B. ADD New Patient and Doctor Information page

In this Patient ID is generated automatically. Then the Patients name, address, date of birth, Mobile number and Medical information is given in the Patient information Page. And also Doctor Information is entered in the add new doctor information page.

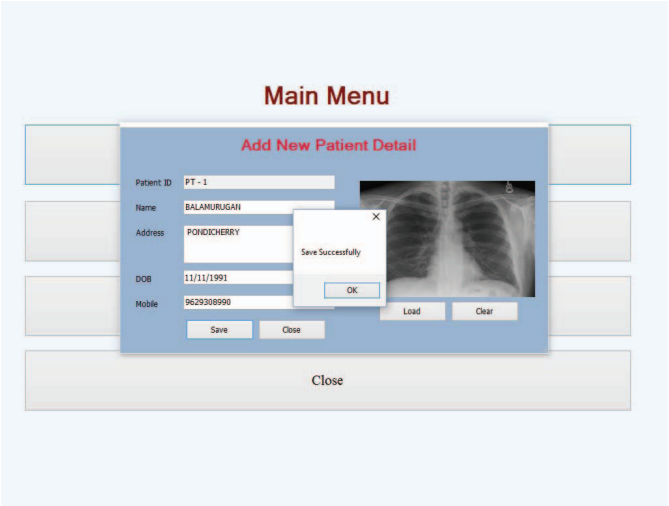

Figure 5: Patient detail Page

Figure 6: Doctor Detail Page

C. 128-key generation from Fingerprint Biometrics

A cryptographic key Generation of 128-bit from the Fingerprint Template for symmetric encryption process.

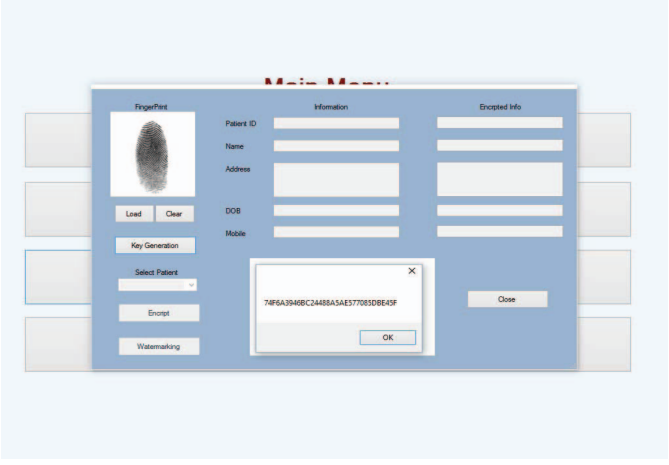

Figure 7: 128-Key generation

D. Embedding and Extraction of Medical Information

In this we embedded 48 bytes of medical information in the medical image using reversible watermarking technique. Using the 128-bit Key of fingerprint template encryption process is carried out. Then this information is transferred to the hospital using the Public key infrastructure. Using the Indexing function the data is stored in the database. The Proposed Methodology helps to transfer the medical information in the secure environment.

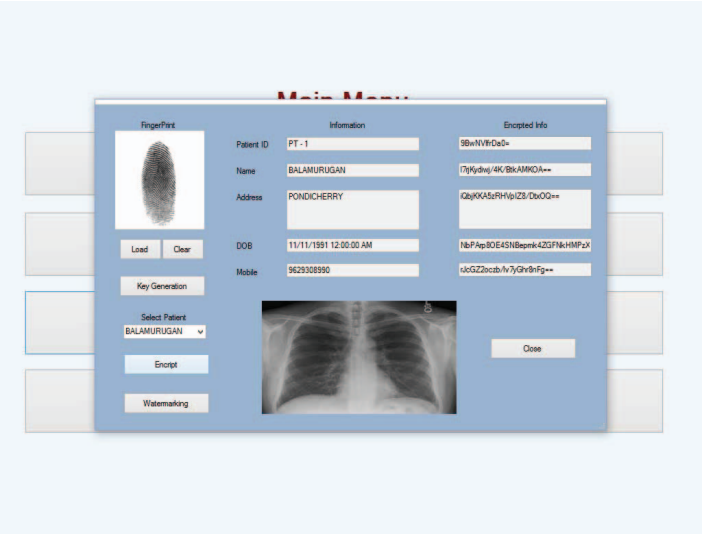

Figure 8: Embedding the encrypted Medical information in medical image

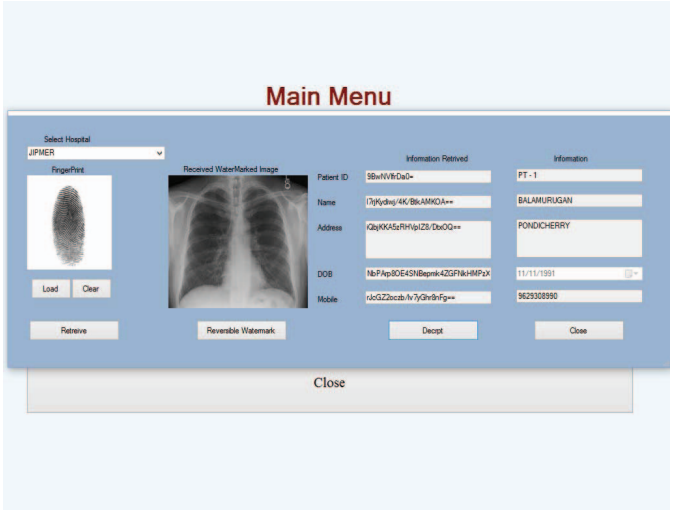

Figure 9: Extraction the Plain Medical information from medical image

CONCLUSION

Fingerprint based reversible watermarking for protection of medical image and data provides reliable solution from illegal issues. It also ensures notification SMS to the patient about the transformation of their details. From this, the security mechanism is maintained and then it satisfies the verification and validation issues in medical data transformation. As a future work the medical data can be extended to embed in the medical image and we can increase the performance.

ACKNOWLEDGMENT

I deliver my truthful thanks to DR.A.RAVICHANDRAN M.E., Ph.D., M.I.S.T.E., M.I.E., Director (Christ College of Engineering and Technology & Christ Institute of Technology) for providing the wonderful opportunity and kind guideline for research article preparation

REFERENCES

[1] *G.Balamurugan, Dr.K.B.Jayarraman, V.Arulalan An Iris based Watermarking system for the security issues of teleradiology, International Journal of Applied Engineering Research, ISSN 0973-4562 Vol.9,No2,2014*

[2] *N.Hussain, W.Boles and C.Boyd, A review of medical image watermarking requirement for Teleradiology, J.Digital Image.Vol.26, No2 pp.326-343.2013*

[3] *"A Survey of Reversible Watermarking Techniques, Application and Attacks", in ICARCSET '15 (ACM), March 06 - 07, 2015, Unnao, India.*

[4] *R.G. Schyndel, A. Tirkel, and C.F Osborne, —A Digital Watermark□, Proceedings of IEEE International conference on Image Processing, ICIP-1994, pp. 86-90, 1994.*

[5] *Christine I. Podilchuk, Edward J. Delp, —Digital watermarking: Algorithms and applications□, IEEE Signal processing Magazine, July 2001.*

[6] *Jiang Xuehua, —Digital Watermarking and Its Application in Image Copyright Protection□, 2010 International Conference on Intelligent Computation Technology and Automation.*

[7] *Ensaf Hussein, Mohamed A. Belal, —Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey□, IJERT, And ISSN: 2278-0118, Vol. 1 Issue 7, September-2012.*

[8] *C.-T. Li and F.M. Yang., —One-dimensional Neighborhood Forming Strategy for Fragile Watermarking□. In Journal of Electronic Imaging, vol. 12, no. 2, pp. 284-291, 2003.*

[9] *X. Li, W. Zhang, X. Gui, B. Yang, A novel reversible data hiding scheme based on two-dimensional difference-histogram modification, IEEE Trans.Inform. Forensic Secure. 8 (7) (2013) 1091–1100.*

[10] *M.U. Celik, G. Sharma, A.M. Tekalp, E. Saber, Lossless generalized-LSB data embedding, IEEE Trans. Image Process. 14 (2) (2005) 253–266.*

[11] *C. De Vleeschouwer, J.E. Delaigle, B. Macq, Circular interpretation of histogram for reversible watermarking, in: IEEE Fourth Workshop on Multimedia Signal Processing, 2001, pp. 345–350*

[12] *R. Chamlawi, A. Khan, A. Idris, Wavelet based image authentication and recovery, J. Comput. Sci. Technol. 22 (6) (2007) 795–804.*

[13] *Baiying Lei, Ee-Leng Tan , Siping Chen , Dong Ni, Tianfu Wang, Haijun Lec "Reversible watermarking scheme for medical image based on differential evolution" vol. 3,no. 2, pp. 113–140,jul 2014*

[14] *Omer Abu Shqeer "Judgment of Extracting Encryption Keys from Image Data", IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.2, February 2014*

[15] *Priyanka.M, Lalitha Kumari.R, Lizyflorance.C and John Singh. K" A New Randomized Cryptographic Key Generation Using Image" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 6, November 2013*

[16] *Dolly Choudhary Shamik Tiwari Ajay Kumar Singh "A Survey: Feature Extraction Methods for Iris Recognition" International Journal of Electronics Communication and Computer Technology, 12*