International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume1, Issue 9 (December '2015)

WATERMARKING BASED ENHANCED MULTIMODAL BIOMETRIC AUTHENTICATION TECHNIQUE

M.Marimuthu,
Assistant Professor,
Department of Computing,
Coimbatore Institute of Technology,
Coimbatore,Tamilnadu,India.

A.Kannammal,
Professor,
Department of MCA,
Coimbatore Institute of Technology,
Coimbatore,Tamilnadu,India.

Abstract: Image encryption plays a crucial role in the field of information security. Most of the existing image encryption techniques have some kind of security flaws and performance related issues. This paper proposes three level of security; Image scrambling is first level security and second level security is chaotic based image encryption. Third level security is achieved using random LSB based watermarking. Fingerprint is considered as original image and iris is considered as chaotic image. Fingerprint and iris are scrambled; In order to obtain encrypted image, scrambled iris and fingerprint image values are substituted using XoR operation. Finally encrypted image is embedded in face image. The decryption is reverse process of encryption process and it restores the image to its original form. The proposed approach is evaluated using standard security measures and statistical methods; result shows that proposed approach performs better than existing method in the cryptography domain.

Keywords: Biometrics, Fingerprints, Image encryption, Image scrambling, Watermarking

I. INTRODUCTION

In recent years, with the fast development of technology and particularly digital image processing technology, people holds some useful results and the image security is becoming a hot research topic involving mathematics, cryptography and information hiding techniques. The proposed technique includes image scrambling, information hiding and image watermarking etc., [1]. Among these techniques, the scrambling technique is one of the basic method for cover huge image information, which can be applied in the pre-process or post-process of digital image processing, information hiding, digital watermarking etc., The primary goal of image scrambling algorithm is to generate a disordered image which prevents human visual system or computer vision system from understanding the true meaning of the image. The scrambled image only can be recovered if the receiver has the knowledge of scrambling method and scrambling variables [2].

Chaos based encryption algorithms are becoming popular nowadays due to its better security and performance aspects. The main characteristics of chaos like complexity, sensitivity to the initial conditions and control parameters, pseudo randomness and unpredictable property are required to provide an efficient encryption scheme [4]. Chaotic behavior of a system is the sophisticated nature of a nonlinear system that looks random. One important feature of chaos is a small variation of any variable changes the outputs considerable [5].

In image watermarking, the information is hidden exclusively in an image which is called the cover image. After embedding the secret information, the cover image is called stego-image. To be a useful watermarking system, it must provide a better method to embed data imperceptibly, and the secret message must be able to convey the meaning after extraction from the cover image. The basic idea of image data hiding is to hide the secret image under the mask of the cover image [6, 7].

The rest of the paper is organized as follows: Section 2 gives a brief introduction about the Literature Review. Section 3 proposes the improved scheme and Section 4 describes the experimental setup. Section 5 discusses the results of proposed method Finally, Section 6 concludes the work.

II. LITERATURE STUDY

An image block encryption algorithm based on three-dimensional Chen chaotic dynamical system is proposed by Jun Peng et al., [8]. The proposed algorithm works on 32-bit image blocks with a 192-bit secret key and the key is employed to derive the Chen's system to generate a chaotic sequence, its output is passed to a specially designed function G; it uses new 8x8 S-boxes to generate chaotic maps. In order to improve the robustness against different cryptanalysis and to produce desirable avalanche effect, the function G is iteratively performed several times and its final output serve as the key

streams to encrypt the original image block. The results show that it offers higher level of security for key space analysis, differential attack analysis, information entropy analysis and correlation analysis

Ismail Amr Ismail et al., [9] introduced a chaos-based stream cipher, composing two chaotic logistic maps and a large enough external secret key for image encryption. The external secret key is used to derive the initial conditions for the chaotic maps, and is employed with the two chaotic maps to confuse the relationship between the cipher image and the plain image. In the encryption phase, the pixels are encrypted using an iterative cipher module based feedback and data dependent inputs mechanism for mixing the current encryption parameters with previously encrypted information. To make the cipher more robust against any attack, the secret key is modified after encryption of each pixel of the plain image. Result reveals that it outperforms for key space analysis, statistical analysis and differential attacks.

An image encryption algorithm based on Rubik's cube principle is recommended by Khaled Loukhaoukha et al., [10]. The original image is scrambled using the principle of Rubik's cube. Then, XOR operator is applied to rows and columns of the scrambled image using two secret keys. This scheme achieves better encryption and perfect hiding ability; also it can resist exhaustive attack, statistical attack and differential attack.

Faraoun Kamel Mohamed et al., [11] suggested a scheme based on reversible one-dimensional cellular automata. The proposed scheme is fully parallelizable since the encryption/decryption tasks can be executed using multiple processes running independently for the same single image. The parallelization is made possible by defining a new RCA based construction of an extended pseudorandom permutation (PRP) that takes a nonce as a supplementary parameter. The defined PRP exploit the chaotic behavior and the high initial condition's sensitivity of the RCAs to ensure perfect cryptographic security properties. It provides the ability to perform a selective area decryption since any part of the ciphered-image can be deciphered independently from others

Digital images encryption with password protection using 1D SHA-2 algorithm coupled with a compound forward transform is proposed by Abbas Cheddad et al., [12]. A spatial mask is generated from the frequency domain by considering advantage of the conjugate symmetry of the complex imagery part of the Fourier Transform. This mask is then XORed with the bit stream of the original image. Exclusive OR (XOR), a logical symmetric operation, that yields 0 if both binary pixels are 0s or if both are ones and 1 otherwise. This can be verified simply by modulus (pixel1, pixel2, 2). Finally, confusion is applied based on the displacement of the cipher‟ s pixels in accordance with a reference mask. This method offers a balanced perceptibility effect on the cover image while embedding the bits.

Fast compressed sensing approach using structurally random matrices and Arnold transform is developed by Nitin Rawat et al., [13]. First, dimension reduction is utilized to compress the digital image with scrambling effect. Second, Arnold transformation is used to give the reduced digital image into more complex form. Then, the complex image is again encrypted by double random phase encoding process embedded with a host image; two random keys with fractional Fourier transform have been used as secret keys. At the receiver side, the decryption process is recovered by using TwIST algorithm. This proposed method is secure, fast, complex and robust compare to existing methods.

Mohammad Ali Bani Younes et al., [14] introduces a block-based transformation algorithm based on the combination of image transformation and a well known encryption algorithm called Blowfish. The original image was divided into blocks, which is rearranged into a transformed image by using a transformation algorithm, and then the transformed image was encrypted by applying Blowfish algorithm. High entropy values are achieved and correlation between image elements was significantly decreased for the proposed approach.

III. PROPOSED METHOD

a) Arnold Transformation Algorithm

The Arnold scrambling algorithm converts the original image into scramble image which is not able to understand the meaning of the image by human visual system or computer vision system. The Arnold scrambling transform can be represented as in equation 1.1

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \quad (1.1)$$

Where x, y is {0,1,2,….N-1} and (x, y) is the coordinate of the pixels in the original space, (x',y') is the coordinate of the pixels after the iterative scrambling computation, N is the size of a square image also known as the image dimension. The scrambling algorithm is used as the secret key (key1) in the proposed scheme.

N	2	3	4	5	6	7	8
Cycle	2	4	3	10	12	8	6
N	32	40	48	50	56	60	64
Cycle	24	30	12	450	24	60	48
N	9	10	11	12	16	24	25
Cycle	12	30	5	12	12	12	50
N	100	120	125	128	256	480	512
Cycle	150	60	250	96	192	120	384

Table 1 Arnold Transform Cycle

After several rounds of iterative calculations, the original image was scrambled. The experimental results and theory analysis proved that it is a one-to-one and period transformation that is when the iterative calculations run to a certain step, the original image can be restored. Table 1 shows the correspondences between the certain size images and their cycles.

From the table 1 it is clearly observed that, there is no function relationship between the image dimension and the variation of the cycle, and for some images the cycle of their transformation are very long and require a large amount of computing time, which is a problem to the watermarking algorithm. Practically, we must choose a certain size of the watermarking image to reduce the computational complexity.

The scrambling level or cycle is an essential factor in order to measure the quality of the scrambling algorithm and also, it is known from the period of Arnold scrambling that an image has a variety of scrambling levels after the Arnold scrambling. The best degree of scrambling refers to the number of iterations when the scrambling effect is optimized. To solve the anti-Arnold transformation, the period of matrix is computed. Its contra-matrix is used to solve anti-Arnold transformation, in which the original image is recommenced. Only using anti-Arnold transformation with iteration in the same proposition recommence the original image. For the matrix of the Arnold Transformation is given below

$$a=\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

hence the anti-Arnold transformation is given by equation 1.2

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \quad (1.2)$$

The equation 1.2 transformation and the Arnold transformation as in equation 1.1 have the same period, so equation 1.2 is anti-Arnold transformation. If one image iterates m steps to get scrambled state with Arnold transformation, it can restore its original state with the same steps from the scrambled state by anti-Arnold transformation, with no work to compute the image's period.

b) Chaotic Image based Encryption

One of the common gray value replacement methods is that one image needed to be encrypted using bit-exclusive-or operation with chaotic sequence. The advantage of this method is that it has high speed of encryption and decryption and can be implemented very easily. An improved algorithm based on 3x3 neighborhood bit exclusive-or and bit rotate operation is implemented. Bit rotate factor is introduced in the algorithm. The original image is assumed to be f(i, j) with 256 gray levels; its size is XxY pixels, where f(i, j) represents the gray value of the pixel. (i, j) is the coordinate of pixel, i=0,1….X-1, j=0,1….Y-1. Chaotic image has 256 gray levels and (X+2)x(Y+2) size, where i=0,1,….X+1; j=0,1,….Y+1. The positions of f(i, j) and c(i+1,j+1) are overlapped.

The bits of the encrypted image are represented by K_1, K_2,….K_n , Where n is the number of bits in the image. The encrypted image k(i, j) is in the coordinate (i, j). The encryption process involves exclusive-or operation of the original image f(i, j) and chaos image c(i, j). The original image and chaos image are made to perform exclusive-or operation as per relation given in Table 2

K_1	f(i, j) ⊕ c(i, j)
K_2	f(i, j) ⊕ c(i, j+1)
K_3	f(i, j) ⊕ c(i, j+2)
K_4	f(i, j) ⊕ c(i+1, j)
K_5	f(i, j) ⊕ c(i+1, j+2)
K_6	f(i, j) ⊕ c(i+2, j)
K_7	f(i, j) ⊕ c(i+2, j+1)
K_8	f(i, j) ⊕ c(i+2, j+2)

Table 2 Bits of Encrypted image

The symbol ⊕ represents the exclusive OR operation bit by bit. The bit rotate factor of the encrypted image k(i, j) in (i, j) is determined by Equation 1.3

$$(i, j) = \text{mod}(a, 8) \quad (1.3)$$

Where a is the average of pixels of c(i+1, j+1) in 3*3 neighborhood as given in equation 1.4

$$a=\frac{\begin{pmatrix} c(i,j)+c(i,j+1)+c(i,j+2)+ \\ c(i+1,j)+c(i+1,j+2)+ \\ c(i+2,j)+c(i+2,j+1)+c(i+2,j+2) \end{pmatrix}}{9} \qquad (1.4)$$

the encrypted image values k1,k2,…k8 are rotated to the right to obtain 8 new bit arrangements r1, r2…r8. After the above steps have been performed, the gray value of the encrypted image k(i, j) is determined by using the following equation 1.5

$$k(i,j)=\sum_{x=1}^{8} r_y 2^{8-x} \qquad (1.5)$$

3.3 Random LSB Embedding Steganography Scheme

There are several techniques available for information hiding or watermarking in digital media. The basic method of information hiding is steganography. Steganography allows insertion of additional data in the image without altering the original content of the image [15]. Random LSB is highly secure and very easy to implement. This method embeds the fixed-length of secret bits in the same fixed length LSB of pixels in random manner. Among other embedding methods Least Significant Bit (LSB) substitution method is a very popular way of embedding secret messages with simplicity. The fundamental idea here is to insert the secret message in the least significant bits of the image. This method of choosing consecutive bytes of the image data, from the first byte to the end of the message, to embed the information, called sequential LSB embedding is easily detectable by steganalysis software and hence not secure.

In order to make the above steganographic algorithm more robust, a new technique in which the secret data can be spread out among the image data in a random manner is proposed. Pseudorandom numbers are used to select the pixels for hiding the message. By this way, it is difficult for the steganalysis software to detect the location of secret message. Since the pixels containing the information are not sequential, it is difficult for steganalysis software to detect the stego-image.

In this method, a new approach for selecting pixels according to a password is used. The sender and receiver share a secret key that specifies only certain pixels to be changed. Using the password would cause to select the pixels in a random manner. In this method, information is in random order pixels in each block, and extracting the hidden information is difficult. The advantage of this work is that the pixels are filled in a random order and cannot decode without knowing the password.

The watermark embedding procedure is explained as below

1. Read the cover image I, of size N x N
2. Scramble the fingerprint (original image) and iris (chaotic) image with Arnold Algorithm for key times and gain the scrambled image. The key considered here is the age.
3. Substitute the values of chaotic image into original image using XoR operation and get watermark.
4. Re-formulate the watermark into a vector of zeros and ones.
5. Embed the watermark in random manner using Least Significant Bit (LSB) of cover image.
6. Obtain the watermarked image (Stego-image).
7. Send it to the receiver.

Figure 1 and figure 2 shows image encryption and decryption process of proposed method

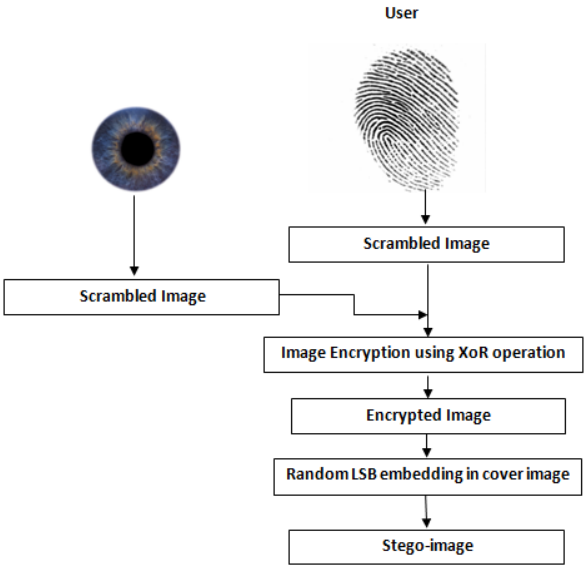


Figure 1 Image Encryption and Steganography during Enrollment

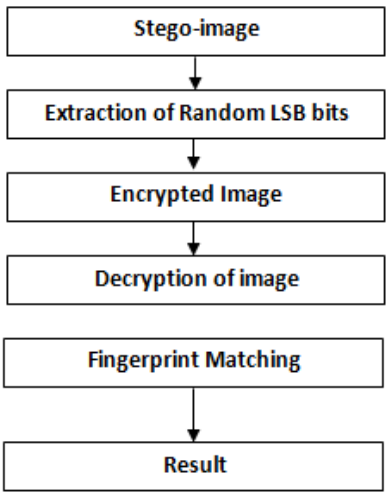


Figure 2 Image decryption and Steganography during Verification

IV. EXPERIMENTAL RESULTS AND DISCUSSION

The performance of proposed technique fingerprint is used as watermark it is available from public-domain database FVC2002 [16] which contains 40 different gray-scale fingers and 8 impressions of each finger(40x8=320 fingerprints). The images in DB1, DB2, DB3 and DB4 are 388x374, 296x560, 300x300, 288x384 and each fingerprints have a resolution of 500 dpi. Iris images of CASIA-Iris-Interval were captured with close-up iris camera [17] . The most compelling feature of the iris camera is that it is designed by a circular NIR LED array, with suitable luminous flux for iris imaging. The Yale Face Database contains 165 grayscale images in GIF format of 15 individuals. There are 11 images per subject, one per different facial expression or configuration [18].

Entropy

The Quality of image encryption is commonly measured by entropy over the cipher text image. Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image. A higher value of entropy indicates that the image is more random and the encrypted image is protected against statistical attacks. The entropy values obtained are tabulated in Table 3 and Figure 3.

DB1	Without Scrambling	With Scrambling	Chaotic Image Encryption (Proposed)
101_1.tif	3.28	3.58	7.83
102_1.tif	3.63	3.85	7.56
103_1.tif	4.64	4.79	7.60
104_1.tif	4.36	4.63	7.51
105_1.tif	4.12	4.40	7.72

Table 3 Entropy values for Proposed Algorithm

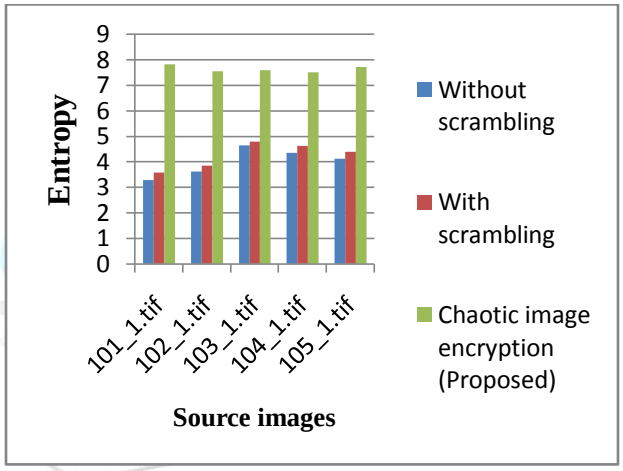
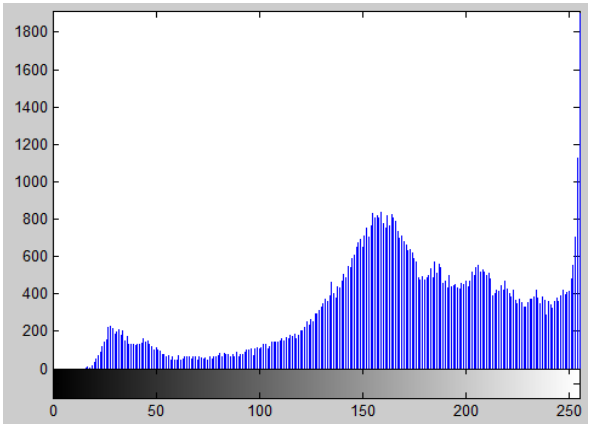


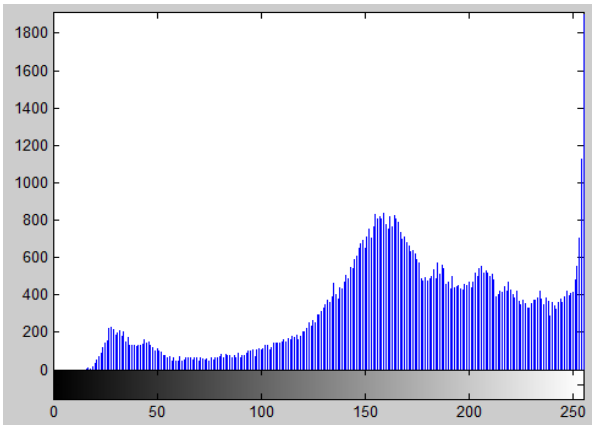
Figure 3 Entropy values for Encryption

Histogram Analysis

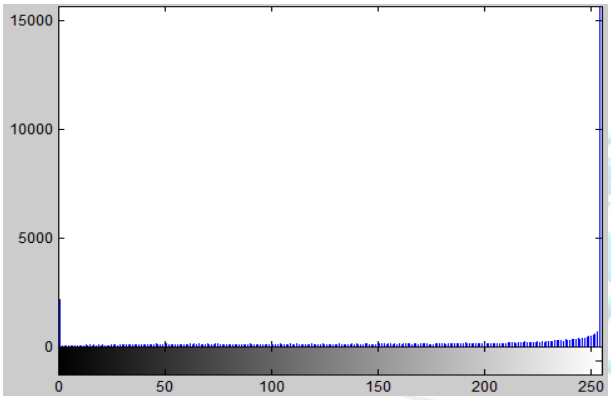
The histogram for stego images are calculated and histogram of an image is shown in Figure 4



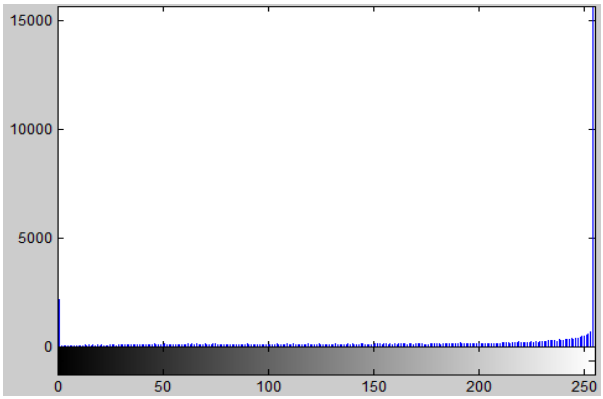
a)



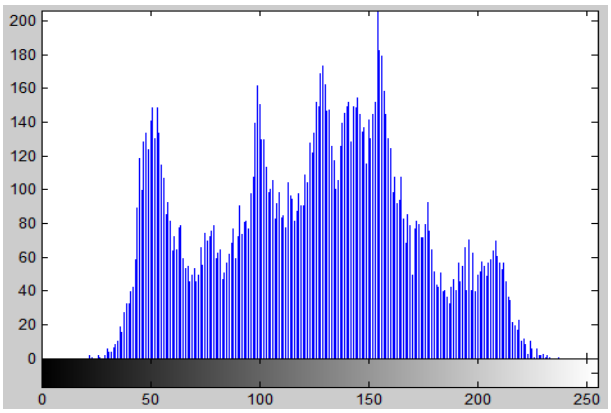
b)



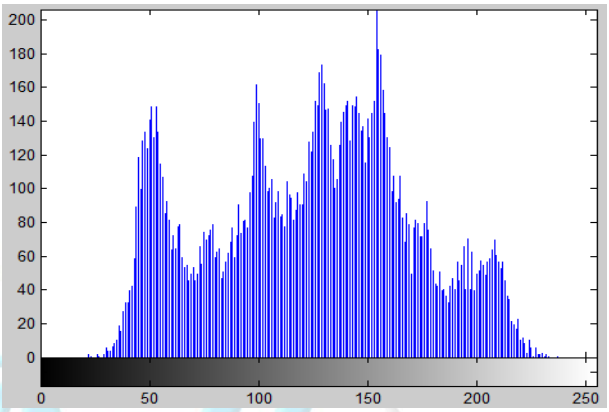
c)



d)



e)



f)

Figure 1.4 a) Chaotic Image b) Chaotic Image after Scrambling c) Watermark Image d) Scrambled Watermark Image e) Cover Image f) Stego-image

MSE

The Mean Square Error (MSE) represents the cumulative squared error between the compressed and the original image. MSE is calculated by the equation 1.7 and shown in Table 1.5 and Figure 1.6

$$MSE = \frac{\sum_{M,N}|I_1(m,n)-I_2(m,n)|^2}{M*N} \quad (1.7)$$

Where, M is the width of image, N is the height and M x N is the number of pixels of the image.

PSNR

Peak Signal to Noise Ratio (PSNR) is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation.

Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of a logarithmic decibel scale. A higher PSNR value indicates that the reconstruction is of higher quality. Typical values for the PSNR in a lossy image and video compression are between 30 and 50 dB, where higher is better. Acceptable values for wireless transmission quality loss are considered to be about 20 dB to 25 dB. PSNR is most commonly used as a measure of quality of reconstruction of lossy compression. The signal in this case is the original data, and the noise is the error due to hiding. PSNR values are shown in the Table 1.5 and Figure 1.7

$$PSNR=10 \log_{10}\left(\frac{R^2}{MSE}\right) \qquad (1.8)$$

Where, R is the maximum fluctuation in the input image data type.

Cover Images	MSE for LSB Watermarking	MSE for Random LSB Watermarking (proposed)	PSNR for LSB Watermarking	PSNR for Random LSB Watermarking (proposed)
Image 1	0.98	0.94	26.45	35.21
Image 2	0.97	0.95	25.21	38.42
Image 3	0.97	0.95	24.57	39.45
Image 4	0.98	0.94	25.68	40.05
Image 5	0.98	0.93	26.53	39.19

Table 5 MSE and PSNR Values

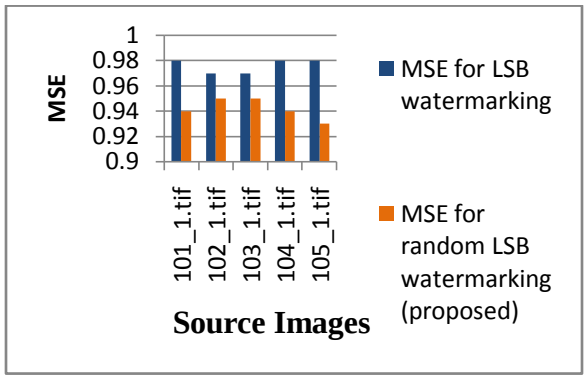


Figure 6 MSE Values for Various Images

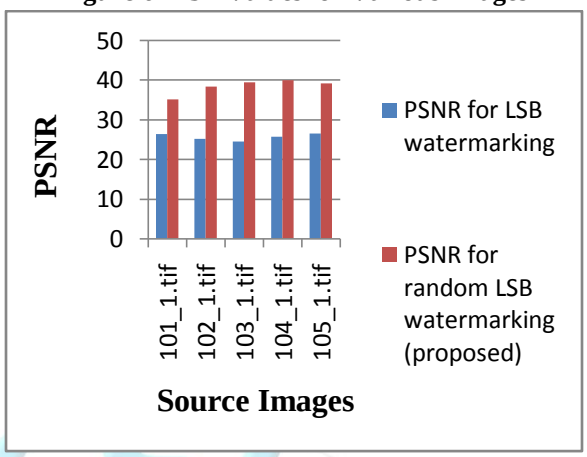


Figure 7 PSNR Values for Various Images

V. CONCLUSION

Communication increases through open networks day by day due to large amount of data. Security plays a major role between the unauthorized users and legitimate users. In this chapter new image encryption method was proposed. Initially Arnold transformation is applied for scrambling both original image and chaotic image. Next by substituting improved gray value using chaotic image, scrambled original image was converted into new encrypted image. Finally, this image was watermarked into the cover image using enhanced random LSB embedding algorithm. Attacker cannot extract the watermark from the stego-image due to random LSB embedding. It provides a primary security to the image. Even if extracted it cannot provide meaningful information to the attacker because of dual encryption of gray value substitution and scrambling transformation.

REFERENCES

[1] P. Premaratne, M. Premaratne, "Key-based scrambling for secure image communication," Emerging Intelligent Computing Technology and Applications, pp.259-263, 2012.

[2] Li-Ping Shao, Zheng Qin, Hong-Jiang Gao, Xing-Chen Heng, "2D Triangular Mappings and Their Applications in Scrambling Rectangle Image" Information Technology Journal 7(1) : pp.40-47, 2008

[3] Mehdi Khalili, "A Secure and Robust CDMA Digital Image Watermarking Algorithm based on DWT2, YIQ Color Space and Arnold Transform" Signal & Image Processing : An International Journal (SIPIJ) Vol.2, No.2, pp.131 – 147, 2011.

[4] Parameshachari B D, K M Sunjiv Soyjaudah, Sumitrha Devi K A, "Secure Transmission of an image using Partial Encryption based Algorithm", International Journal of Computer Applications, Vol.63, no.16, pp.1-6, 2013.

[5] N.K. Pareeka, Vinod Patidara, K.K. Suda, "Image Encryption using Chaotic Logistic Map", Image and Vision Computing, pp.926-934, 2006.

[6] Himanshu, Balasubramanian Raman, "Indexing Scheme for Iris Using Discrete Cosine and Discrete Wavelet Transform" , Proceedings of the International Conference on Soft Computing for Problem Solving (SocProS 2011), Advances in Intelligent and Soft Computing Volume 131, 2012, pp. 391-399, December 2011.

[7] Mishra, T.K., Majhi, B. Panda, S., "A comparative analysis of image transformations for handwritten Odia numeral recognition" Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp.790 – 793, August 2013.

[8] Jun Peng, Du Zhang and Xiaofeng Liao, (2011) "A novel algorithm for block encryption of digital image based on chaos", International Journal of Cognitive Informatics and Natural Intelligence, Vol. 5, No. 1, pp. 59-74.

[9] Ismail Amr Ismail, Mohammed Amin, Hossam Diab, "A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps" International Journal of Network Security, Vol.11, No.1, PP.1 -10, July 2010.

[10] Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle" , Journal of Electrical and Computer Engineering, pp. 1-13, 2012.

[11] Faraoun Kamel Mohamed, "A parallel block-based encryption schema for digital images using reversible cellular automata", Engineering Science and Technology, an International Journal, Volume 17, Issue 2, pp. 85–94, June 2014.

[12] Abbas Cheddad, , Joan Condell , Kevin Curran , Paul McKevitt, "A hash-based image encryption algorithm", Optics Communications Volume 283, Issue 6, pp. 879–889, March 2010.

[13] Nitin Rawat , Pavel Ni , Rajesh Kumar, "A Fast Compressive Sensing Based Digital Image Encryption Technique using Structurally Random Matrices and Arnold Transform" pp.1-13 2014

[14] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, February 2008

[15] Yusuf Perwej, Firoj Parwej, Asif Perwej, "An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection", The International Journal of Multimedia & Its Applications (IJMA) Vol.4, No.2, pp.21-38, April 2012.

[16] FVC2002, "http://bias.csr.unibo.it/fvc2002/," 2002.

[17] CASIA Database, "http://biometrics.idealtest.org/"

[18] Yale Face Database "http://vision.ucsd.edu/datasets/yale_face_dataset_original/yalefaces.zip"