ISSN: 0976-9102 (ONLINE)
DOI: 10.21917/ijivp.2016.0194

DATA HIDING IN ENCRYPTED IMAGES USING ARNOLD TRANSFORM

Siva Shankar S[1] and A. Rengarajan[2]
[1]*Department of Computer Science and Engineering, Bharath University, India*
E-mail: sss_siva85@yahoo.co.in
[2]*Department of Computer Science and Engineering, Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, India*
E-mail: rengu_rajan@yahoo.com

Abstract

Digital image steganography has several applications in information security and communication. Data hiding in encrypted images ensure that both the cover image and the secret message can be recovered at the receiver end. This work presents a novel data hiding and image encryption scheme using random diffusion andTwo dimensional Arnold cat mapping transform. The secret message bits are placed in the least significant bit positions of the cover image. Then a shared key is used to generate random 8 bit random integer stream and is added to the stego image in the random diffusion step. Arnold cat mapping transformation is done to scramble the pixels. The two steps of random diffusion and Arnold transform mapping are done alternatively several times to completely encrypt the image contents. The process is reversed at the receiver end to get both the secret messageand the cover image with little loss. The random diffusion step overcomes the limited period of the Arnold transform.Theembedding capacity of one bit per pixel is achieved. Security analysis is carried out which shows that the encryption is highly secure. The number of collisions is low thus preventing brute force attacks. The original cover image is recoverable with minimal losses.

Keywords:

Digital Images, Steganography, Arnold Transform, Data Hiding, Image Encryption

1. INTRODUCTION

Steganography is the embedding of secret message in ordinary communication medium [1]. It never raises suspicion in a passive observer. Digital images have high capacity, redundancy and prevalence. Millions of photographs are being uploaded on a daily basis in the internet based social media. Image pixels are highly correlated and hence additional data can be stored without compromising on the visual quality of the image [2]. So they are ideally suited to be the medium of secret communication. Several digital image steganographic methods have been proposed in the literature.

Image encryption is an important technique to sending images over secure channels. Several encryption and decryption algorithms have been proposed for images. There is a particular need for techniques that combine data hiding and encryption. The hiding must be reversible so that the original image can be recovered after decryption and the hidden message is recovered as well. This is useful in many applications such as image tamper proofing, preserving privacy of medical images, image forensics etc [3].

The scenario considered in this work is explained briefly. The sender Bob sends an encrypted image with hidden message over an unsecured channel to Alice. Alice and Bob share a secret key. Alice uses the shared key to successfully extract the hidden message as well as the decrypted image. The loss of information in the decrypted image is minimal. Eve is an observer who has complete read access to the medium. However she does not possess the knowledge of the secret key. The details of the method is known to public including Eve, but that does not allow her to either read the secret message or recover the image even partially.

Least Significant Bit Replacement [4] is the most commonly used steganographic technique. It involves the hiding of secret message bits in the least significant bit (LSB) plane of the image. Thus if the pixel intensity value is 144 and the message bit is 1 then the pixel value is changed to either 145 or 143 so that it's LSB matches with the message bit. The alteration of the LSB causes little distortion in the image. The change in the image is not detectable to a subjective evaluation by a human observer. Several sophisticated statistical analysis methods known as steganalysis can distinguish between stego images from normal cover images. However it is not feasible to check every image in the network in real time.

The Arnold transform [5] is an image scrambling technique that can be used to encrypt and decrypt image data. The transform is area preserving and invertible without loss of information. It is also known as cat map. The mapping can be done successively several times to completely obscure the image beyond recognition. Alice has the information about the number of times the transform is applied and can successfully recover the original image.

This paper presents a system that uses Arnold transform to encrypt an image. The number of times the transform is applied depends on a secret message expressed in a higher base. In order to identify the correct number of times the transform is applied, check bits are added to the LSBs.The literature survey is done in section 2. The drawbacks of existing system are discussed in section 3. The proposed system is presented in section 4, results and discussion are presented in section 5 and conclusion is given in section 6.

2. LITERATURE SURVEY

Several techniques have been proposed to combine image encryption with data hiding.

Ma et al. [6] gave a general framework by finding the compressible features of an image and vacating room before encryption for the secret message. Lossless compression was employed. Tian et al. [7] introduced pixel expansion based method to reversibly hide large amount of data. The embedding can be repeated more than one time for additional capacity. Tsai et al. [8] introduced modified histogram shifting. The pixel intensity histogram and prediction based error histogram were

used. This method identifies a vacant intensity level and shifts pixels to create a vacant room next to the peak level. The pixels are then shifted between the peak and the next zero levels according to the message bits.

Chen et al. in [5] proposed a method to encrypt a color image based on Arnold transform and interference method. A color image is decomposed into red, green and blue channels and encryption is applied to the channels separately. Guo et al. in [10] proposed a color image encryption scheme using discrete fractional random transform (DFRT) [11] and Arnold transform. The images are encrypted in IHS color space. While Arnold transform scrambles the image by changing the pixel positions, DFRT changes both the positions as well as values of the pixels. Guodong Ye proposed in [12] an image scrambling method based on chaos map, which drastically changed the statistical characteristics of the pixels. Liu et al. in [13] designed image encryption scheme using Arnold transform and color blend operation in discrete cosine transform domains. Tang et al. in [14] introduced random strategies to strengthen the security of the encryption. MR Li et al. in [15] utilized the gyrator transform and Arnold transform to enhance the security of image encryption. Arnold mapping was extended to three dimensions by Chen et al. in [16].

This paper is based on Arnold transform applied on blocks of the image. Before encryption a special signature bit sequence called the check bits are embedded in LSBs of the image. The security aspects of the proposed system are briefly analyzed.

3. EXISTING SYSTEM

3.1 THEORETICAL BACKGROUND

The Arnold transform is a classical 2D invertible chaotic map defined as:

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

The inverse transform is defined as:

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

The transformations are area preserving and strongly chaotic. The drawback of the Arnold transform for use in encryption is the low period. For example a 256×256 grayscale image has a period of 192, i.e. after 192 times the shuffled image is reduced back to the original image. So an attacker only needs to manually check for a maximum of 192 times by reversing the mapping and visually verifying the image.

There are no known formulae to calculate the period of Arnold mapping from the image dimension n. However some special case rules for the period τ were found as

$$\tau = 3n \text{ if and only if } n = 2*5^k \; k = 1, 2,\ldots \quad (3)$$

$$\tau = 2n \text{ if and only if } n = 5^k \text{ or } n=6*5^k \; k = 1, 2,\ldots \quad (4)$$

$$\tau \leq \frac{12n}{7} \text{ for all other choices of } n \quad (5)$$

The Fig.1 shows the orbit followed by the pixel location (1,1). The position number 192 coincides with the number 1 as it is the period. The emergence and the sudden disappearance of chaos in Arnold like mapping is the subject of much study.

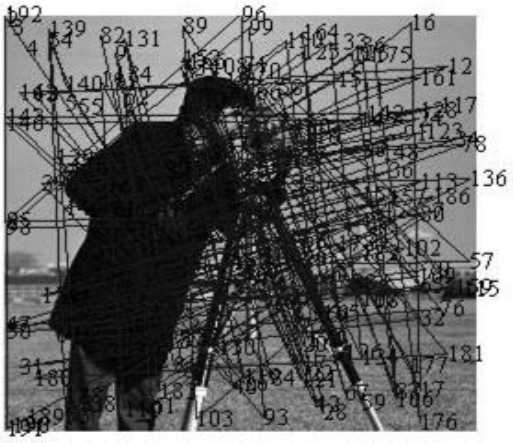


Fig.1. Orbit of (1,1) for the repeated application of Arnold Mapping

3.2 DRAWBACKS OF EXISTING SYSTEM

The two dimensional Arnold transform only scrambles the positions and leaves the grayscale values intact. This allows Eve to confirm whether the image was a particular one in her possession.

This makes brute force attacks likely to deduce the original image by randomly applying inverse Arnold transform several times and checking against a standard natural image model. This work presents a method which replaces the LSB of the image blocks by the secret message and then applying Arnold transform followed by random diffusion a certain number of times according to the secret message digit.

4. PROPOSED SYSTEM

4.1 LSB MATCHING EMBEDDING

LSB Replacement is the method of simply replacing the least significant bits of the image pixels with the message bits. For example if the pixel value is 150 and the message bit is 0 then the modified pixel value will still be 150. If the message bit is 1 then the LSB of 150 is replaced with 1 to make the new value of 151. In LSB matching however, the two options of modified values 149 and 151 are both considered. Both options have LSB equal to the message bit. The choice is random made with a pseudo random generator. This modification alleviates the odd/even asymmetry which compromised the security of LSB replacement [17].

4.2 EMBEDDING PROCEDURE

Arnold Mapping has low period and hence not suitable for image encryption by itself [18]. To enhance the security, the additional step of random diffusion is included. The pixel values are distorted through the addition of a pseudorandom integer sequence in the range of [0, 255] modulo 256. The pseudo random sequence is generated using the shared secret key K as the random seed. Thus Alice and Bob will be able to generate the exact same sequence. Bob will be able to reverse the

encryption process however Eve without the knowledge of *K* will not be in a position to decrypt the image and obtain the hidden message.

The embedding procedure is as follows

Step 1: The secret message is embedded in the LSB of the cover image using LSB matching.

Step 2: A pseudo random generator is setup with the shared key *K* as the seed.

Step 3: Arnold transform is used to scramble the pixels once.

Step 4: A random unsigned 8 bit integer sequence is added to the pixels modulo 256. Steps 3 and 4 are repeated *n* times.

Step 5: The resulting image is output as the encrypted image.

The block diagram for the embedding procedure is given in Fig.2.

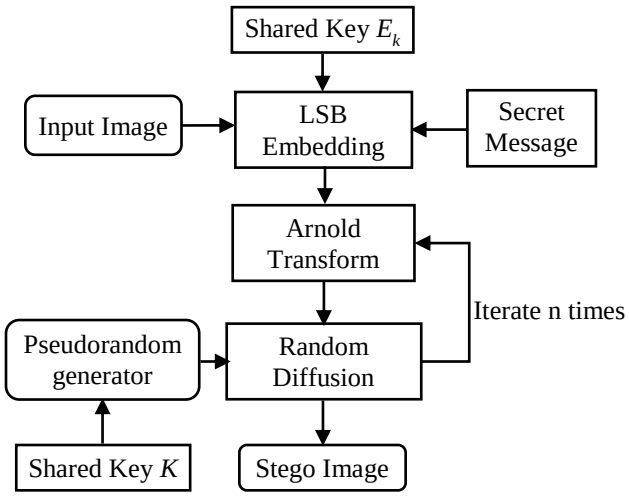


Fig.2. Block Diagram of the Embedding Procedure

The LSB embedding step is done with shared key E_k so that it can be extracted only with its knowledge by the receivers. This is an additional security layer for the embedded message. The image can be decrypted without the knowledge of E_k.

4.3 EXTRACTION PROCEDURE

The extraction procedure is as follows

Step 1: The pseudo random generator is setup with shared key *K* as the seed.

Step 2: The entire sequences of random unsigned 8 bit integers are generated to be used in the reverse order.

Step 3: The random sequence is subtracted from the pixels modulo 256.

Step 4: The inverse Arnold transform is applied. Steps 3 and 4 are repeated n times.

Step 5: The secret message bits are extracted from the LSB of the decrypted image.

The block diagram for the extraction procedure is given in Fig.3.

The encryption process is lossy but the loss is limited to the least significant bit plane. This amounts to an addition of ±1 to the grayscale values. The maximum mean squared error is 1 and the peak signal to noise ratio is higher than $10\log_{10}(255^2) = 48.13$dB. Thus the proposed method achieves the dual objectives of image encryption and data hiding. The embedding capacity is equal to 1 bit per pixel (bpp). This is sufficient in applications like medical image transmission where sensitive metadata or annotations has to be transmitted along with private medical images [19]. It is also suitable for tamper proofing images by sending hashes computed at the sender side along with the image [20].

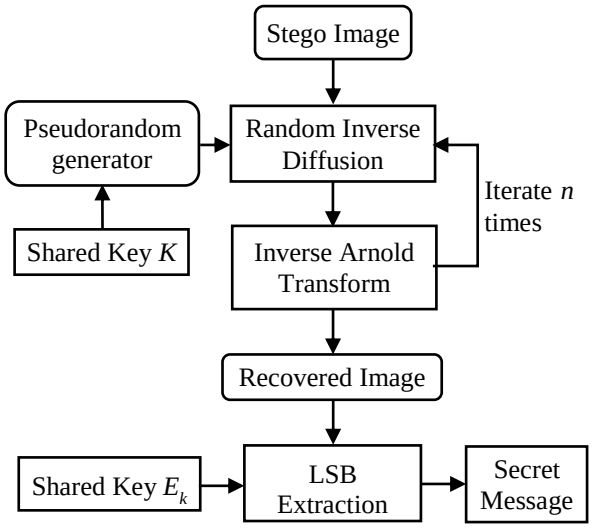


Fig.3. Block Diagram of the Extraction Procedure

5. RESULTS AND DISCUSSIONS

5.1 EXPERIMENTAL RESULTS

A dataset containing 100 test images was formed with images from USC - SIPI database [9] and popular images. The proposed method was implemented in MATLAB 7.0. The Fig.4 shows the result for cameraman image.

The performance of the method is measured using the following measures. Peak Signal to Noise ratio (PSNR) between images *A* and *B* is defined as,

$$psnr = 10\log_{10}\left(\frac{255^2}{mse}\right) \tag{6}$$

where, Mean Squared Error (MSE) is defined as

$$mse = \frac{\sum_{i=1}^{|A|}(A_i - B_i)^2}{|A|}. \tag{7}$$

The embedding capacity is measured in terms of bits per pixel.

$$capacity = \frac{|m|}{|A|} \tag{8}$$

where, *m* is the embedded message in the cover image *A*.

The improvement in encryption due to the random diffusion step can be visually verified from Fig.4 and Fig.5. The Fig.4(e) and Fig.5(e) show the result with only Arnold mapping step without the random diffusion while Fig.4(f) and Fig.5(f) show the full result. The PSNR is below 10 dB which indicates the

content of the image cannot be visually identified by unauthorized observers.

The random diffusion step can only reversed by genuine receivers who have access to the shared secret key *K*. The pseudo random sequence generated with *K* as the random seed has to be used to be modulo subtracted from the inverse Arnold mapping in every iteration. In the absence of the random diffusion step an unauthorized observer could invert Arnold mapping several times and visually recognize the stego image and then extract the embedded message bits. The period of Arnold mapping is below 200 for image sizes up to 256×256. Some of the content structure of the original image will still be visible after several Arnold mapping iterations. Thus the random diffusion step ensures the security of the proposed method.

The Arnold mapping ensures that the image pixels are thoroughly scrambled after every step to remove any correlation with the original image contents. Thus it enhances the security of the proposed method.

The data hiding is effectively decoupled from the image encryption scheme using the additional shared key E_k. Thus the receivers can be given permission only to decrypt the image without access to the embedded message.

The embedding capacity is 1 bit per pixel (bpp). This enables the hiding of the data as shown in Table.1.

Table.1. Maximum Embedding Capacity of the Proposed Method

Data Type\Cover Size	128×128	256×256	512×512
Image	45×45	90×90	180×80
Text	2 KB	8 KB	32 KB

5.2 PERFORMANCE ANALYSIS

The performance measures for few of the test images and the overall average performance for the entire dataset is given in Table.2. It can be seen that the PSNR is consistently below 10dB for encrypted images. The Table.2 also shows the maximum blockwise PSNR of the proposed method compared to plain Arnold mapping. Thus it demonstrates that the encryption is uniform in all parts of the image whereas in the plain Arnold method sometimes image structures appear in some part of the image.

Table.2. Performance comparison of the Proposed Method

Image	PSNR (Proposed)	PSNR (Arnold)	Max Block PSNR (Proposed)	Max Block PSNR (Arnold)
Lake	9.10	9.30	9.8	13.5
Lena (Color)	8.03	8.35	9.2	16.1
Pirate	9.25	9.45	9.6	11.4
Walk bridge	9.45	9.90	9.7	13.2
Overall	9.68	9.84	10.1	14.5

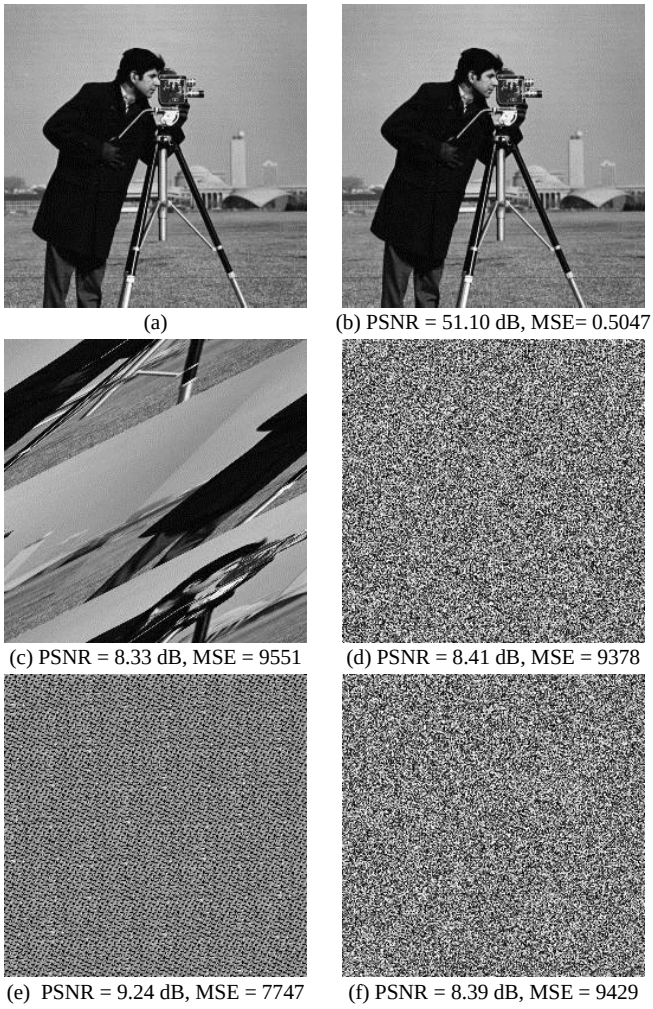
The variation of MSE and PSNR with the number of iterations for Arnold mapping and the proposed method is shown in Fig.6 to Fig.9. The images used are 256×256 cameraman and Lena images. The periodicity of the Arnold mapping is compared against the consistent randomness in the proposed method.

5.3 COMPUTATIONAL EFFICIENCY

The running times of the proposed method are shown in Table.2. MATLAB 2013 software running on Core i5 system with 4GB RAM is used as the benchmark.

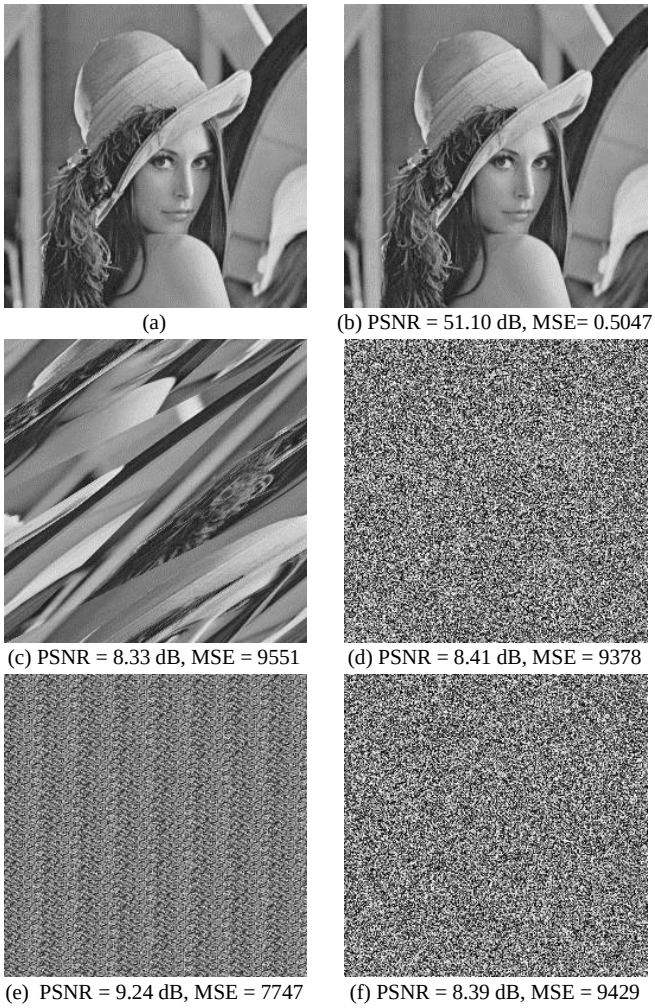
Table.3. Computational Time taken for the proposed embedding algorithm

Image	Computation Time (s)
Lake	3.2
Lena (color)	6.1
Pirate	3.1
Walk bridge	3.2



(a) (b) PSNR = 51.10 dB, MSE= 0.5047
(c) PSNR = 8.33 dB, MSE = 9551 (d) PSNR = 8.41 dB, MSE = 9378
(e) PSNR = 9.24 dB, MSE = 7747 (f) PSNR = 8.39 dB, MSE = 9429

Fig.4. (a) Cover Image (b) LSB Matching Stego Image (c) Single Arnold mapping (d) Single Arnold + Random Diffusion (e) Arnold Only Encryption (f) Arnold + Random Diffusion Encryption



(a) (b) PSNR = 51.10 dB, MSE= 0.5047

(c) PSNR = 8.33 dB, MSE = 9551 (d) PSNR = 8.41 dB, MSE = 9378

(e) PSNR = 9.24 dB, MSE = 7747 (f) PSNR = 8.39 dB, MSE = 9429

Fig.5. (a) Cover Image (b) LSB Matching Stego Image (c) Single Arnold mapping (d) Single Arnold + Random Diffusion (e) Arnold Only Encryption (f) Arnold + Random Diffusion Encryption

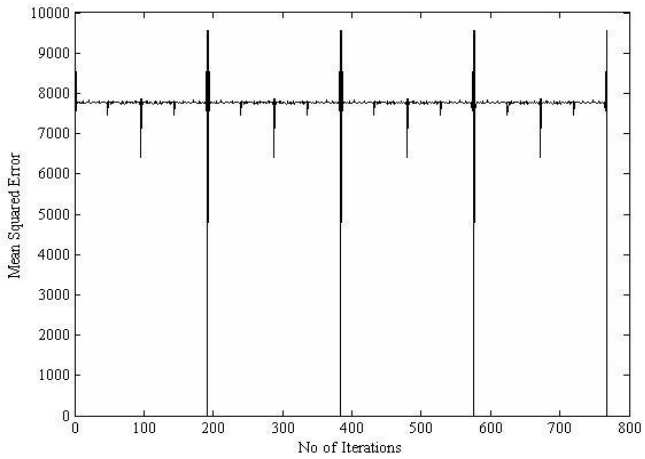


Fig.6. MSE variation with Arnold Mapping

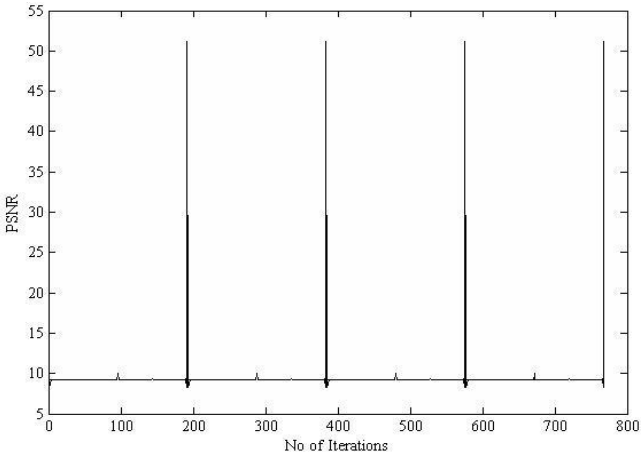


Fig.7. PSNR variation with Arnold Mapping

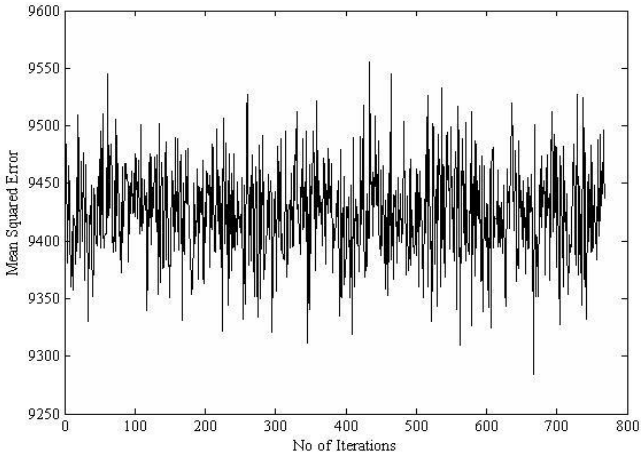


Fig.8. MSE variation with Proposed Method

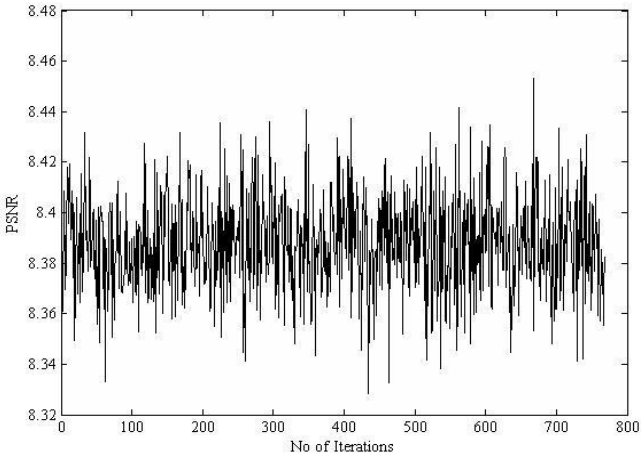


Fig.9. PSNR variation with Proposed Method

6. CONCLUSION AND FUTURE WORK

This paper presented a steganographic method to combine data hiding and encryption of digital images. Only the genuine receivers with access to the shared key can extract both the message and the original cover image. The image is recovered with minimal losses. Arnold Mapping is used to ensure that the image pixels are thoroughly scrambled and the random diffusion

step overcomes the limited period of the mapping. Thus the cryptographic security is enhanced. Experimental results demonstrate the effectiveness of the proposed method. Future efforts can be made to increase the embedding capacity.

REFERENCES

[1] Stefan Katzenbeisser and Fabien Petitcolas, "*Information Hiding Techniques for Steganography and Digital Watermarking*", 1st Edition, Artech House, 2000.

[2] T. Morkel, J.H.P. Eloff and M.S. Olivier, "An Overview of Image Steganography", *Proceedings of 5th Annual Information Security South Africa Conference*, pp. 1-10, 2005.

[3] Yang Ren Er, Zheng Zhiwei, Tao Shun and Ding Shilei, "Image Steganography Combined with DES Encryption Pre-processing", *Proceedings of 6th International Conference on Measuring Technology and Mechatronics Automation*, pp. 323-326, 2014.

[4] Seon Su Ji, "A Study of Optimal Image Steganography based on LSB Techniques", *Journal of the Korea Industrial Information Systems Research*, Vol. 20, No. 3, pp. 29-36, 2015.

[5] W. Chen, C. Quan and C.J. Tay. "Optical Color Image Encryption based on Arnold Transform and Interference Method", *Optics Communications*, Vol. 282, No. 18, pp. 3680-3685, 2009.

[6] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, Fenghua Li, "Reversible Data Hiding in Encrypted Images by Reserving Room before Encryption", *IEEE Transactions on Information Forensics and Security*, Vol. 8, No. 3, pp. 553-562, 2013.

[7] Jun Tian, "Reversible Data Embedding using A Difference Expansion", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 13, No. 8, pp. 890-896, 2003..

[8] Piyu Tsai, Yu Chen Hu, and Hsiu Lien Yeh, "Reversible Image Hiding Scheme using Predictive Coding and Histogram Shifting", *Signal Processing*, Vol. 89, No. 6, pp. 1129-1143, 2009.

[9] Allan G. Weber, "USC-SIPI image database: Version 4", Available at: http://sipi.usc.edu/reports/pdfs/Scanned/USC-SIPI-244.pdf

[10] Qing Guo, Zhengjun Liu and Shutian Liu, "Color Image Encryption by using Arnold and Discrete Fractional Random Transforms in IHS Space", *Optics and Lasers in Engineering*, Vol. 48, No. 12, pp. 1174-1181, 2010.

[11] Liu, Zhengjun, Haifa Zhao, and Shutian Liu, "A Discrete Fractional Random Transform", *Optics Communications*, Vol. 255, No. 4, pp. 357-365, 2005.

[12] Guodong Ye, "Image Scrambling Encryption Algorithm of Pixel Bit Based on Chaos Map", *Pattern Recognition Letters*, Vol. 31, No. 5, pp. 347-354, 2010.

[13] Zhengjun Liu, Lie Xu, Ting Liu, Hang Chen, Pengfei Li, Chuang Lin and Shutian Liu, "Color Image Encryption by using Arnold Transform and Color-Blend Operation in Discrete Cosine Transform Domains", *Optics Communications*, Vol. 284, No. 1, pp. 123-128, 2011.

[14] Zhenjun Tang and Xianquan Zhang, "Secure Image Encryption without Size Limitation using Arnold Transform and Random Strategies", *Journal of Multimedia*, Vol. 6, No. 2, pp. 202-206, 2011.

[15] Huijuan Li and Yurong Wang, "Double Image Encryption based on Iterative Gyrator Transform", *Optics Communications*, Vol. 281, No. 23, pp. 5745-5749, 2008.

[16] Guanrong Chen, Yaobin Mao and Charles K. Chui, "A Symmetric Image Encryption Scheme based on 3D Chaotic Cat Maps", *Chaos, Solitons and Fractals*, Vol. 21, No. 3, pp. 749-761, 2004.

[17] Sorina Dumitrescu, Xiaolin Wu and Nasir Memon, "On Steganalysis of Random LSB Embedding in Continuous-Tone Images", *Proceedings of International Conference on Image Processing*, Vol. 3, pp. 641-644, 2002.

[18] Zhi-Hong Guan, Fangjun Huang and Wenjie Guan, "Chaos-Based Image Encryption Algorithm", *Physics Letters A*, Vol. 346, No. 1, pp. 153-157, 2005.

[19] Meghdad Ashtiyani, Parmida Moradi Birgani and Hesam M. Hosseini, "Chaos-based medical image encryption using symmetric cryptography", *Proceedings of 3rd International Conference on Information and Communication Technologies: From Theory to Applications*, pp. 1-5, 2008.

[20] Deepa Kundur and Dimitrios Hatzinakos, "Digital Watermarking for Telltale Tamper Proofing and Authentication", *Proceedings of the IEEE*, Vol. 87, No. 7, pp. 1167-1180, 1999.