



A Novel Method of Securing Digital Images Using Multi Image Crypto-Stego Techniques

Anand B. Joshi¹, Dhanesh Kumar²
Department of Mathematics and Astronomy
University of Lucknow,
Lucknow, Uttar Pradesh, India

Abstract: In the present era of digital world the security of digital images is a challenging task. In this paper we propose a new method of securing digital image using the steganographic and cryptographic methods. In this method Arnold 3D Cat Map is applied on the digital image which performs the dual encryption, firstly it performs the permutation and secondly it performs the substitution of image pixels. After this we use steganography method to hide the encrypted image, for this we use the multiple RGB images and take the steganographic key and then we use the least significant bit substitution method to hide the digital image on multiple RGB images. The statistical analysis and security analysis of the proposed method is given in this paper to prove the robustness of the proposed method.

Keywords: Digital image, 3D Arnold Cat Map, Cryptographic hash function, Steganography

I. Introduction

In the present era of communication the security of digital data over open and unsecured networks like internet, is of main concern. Steganography means hide data from attacker. Different kinds of methods are available to protect data some methods are encryption, decryption, steganography and methods based on use of simultaneous cryptography and steganography. In this research paper we have present a method based on cryptography and steganography algorithms. The meaning of cryptography is converting the data from readable format to unreadable that is we encrypt the data but the encrypted data visible to all. The meaning of steganography is hiding secret data in any form like text, image, audio, and video. In steganography the secret data is hide behind the cover image, this combination is called stego image. The stego image can be transmitted over unsecured networks like - internet to specified destination and received by the receiver. Under cryptography for encryption of digital images we have used 3D Arnold Cat Map (3D-ACM). Firstly 3D-ACM shuffles the image pixels and then encrypts the pixels. Under steganography we have used least significant bits (LSBs) substitution method. For applying this method we take three cover images. The least significant bit of the secret data is concealed behind the cover images. The proposed crypto-stego system minimizes the possibility of secret message being retrieved by attacker. In this proposed technique we have done encryption using 3D-ACM and then this encrypted data is hiding into the cover images using LSBs method. This technique processed in such a way that protects that secret message can never be obtained without using proposed decryption technique.

II. Organization of the Paper

In section III under preliminaries, we have explained about 3D-ACM for image scrambling and substitution, cryptographic hash function for Arnold Cat Map iteration and steganography: least significant substitution method for hiding image. In section IV, we have presented our proposed method and its implementation. This section also discussed about the key generation and sharing method and arrangement of the procedure for hiding and recovery of secret image. In section V, we have discussed about some experimental results based on proposed crypto-stego techniques. In section VI we have discussed about statistical analyses such as entropy analysis, histogram analysis, MSE analysis, PSNR analysis, and correlation coefficient analysis and pixel intensity correlation graph. Comparison between presented crypto-stego techniques with some existing technique is given in section VII. The conclusion of the proposed approach is given in section VIII and finally the references are given in section IX.

III. Preliminaries

3D-Arnold Cat Map

Many authors have suggested the 3D Arnold Cat Map (3D-ACM)[3], [4] for image scrambling. In this paper we use 3D-ACM with two new control parameters a and b which is given below

$$\begin{bmatrix} x'_1 \\ x'_2 \\ x'_3 \end{bmatrix} = \begin{bmatrix} 1 & a & 0 \\ \beta & a\beta + 1 & 0 \\ a & b & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

This 3D-ACM first performs the image pixels permutation and then image pixels substitution. In this 3D-ACM $[x_1, x_2]^T$ is pixels location before mapping and $[x'_1, x'_2]^T$ is pixels location after mapping. The third parameter inserted is x'_3 which is given by $x'_3 = (ax_1 + bx_2 + x_3) \bmod M$. Here x_3 is the intensity of the pixel before mapping and x'_3 is the intensity of the pixel after mapping. M is the maximum value of the intensity that is $M=256$.

Cryptographic Hash Function

Hash function is defined as: A function which maps data of any arbitrary size to data of fixed size. A cryptographic hash function [9] is a special class of hash function which may be split into two classes: unkeyed hash functions, whose specification dictates a single input parameter (a message) and keyed hash functions, whose specification dictates two distinct inputs, a message and a secret key. Message Digest 5 (MD5) function is one of the unkeyed hash function. MD5 was designed by Ronald Rivest [11] in 1991. In this paper we are using MD5 Algorithm. We apply "MD5" hash function on the secret image (message), and get binary string of fixed length and then we convert this binary string into decimal number for determining Arnold iteration.

Steganography

Steganography [1], [2], [13] is the technique for hiding a digital data like file, message, image, audio or video within another digital data like file, message, image, audio or video. Steganography is a Greek origin word which means "secret writing". The main objective of steganography [12] is to communicate securely in such a way that the original secret message is not visible to the adversary. That is adversary should not be able to determine any sense between cover image (image not containing any secret message) and stego image (cover image that contain secret message). In this research paper we have used image steganography. Image steganography is divided into two types: Spatial domain and Transform domain. Spatial domain further divided into three types: LSB (least significant bit) substitution, LSB matching, and PVD (pixel value difference). Transform domain is divided into two types: DCT (discrete cosine transform) and DWT (discrete wavelet transform). A number of ways exists to hide information in which we are presenting LSB substitution method using 24-bits true color image. The principle involve in this method is to replace all least significant bits of pixels of cover image with bits of secret message. Changing in LSB of any pixel of cover image does not change the original cover image color as it does only change maximum by 1 bit which would be similar color as original. This stego image looks like same as original cover image so adversary cannot detect if there is any secret information in that image or if he found that still they will not able to fetch the secret information from stego image because of encryption and hiding method. Suppose we have three pixels of true-color (RGB) image which are adjacent to each other. Take binary representation of the chosen pixels which are given below.

10000110	10001100	01000110
10001110	10010100	01001011
10010011	10011010	01001111

Now suppose we want to hide the 8-bits secret message 10100110. If we change the LSBs of the RGB image with 8-bits of secret message then we get the following pixels. Here, bits in bold represents that bits have been changed.

100001 10	100011 01	010001 11
100011 10	100101 00	010010 11
100100 10	100110 11	010011 10

IV. Proposed Algorithm and Implementation

Key Generation and Sharing

The method for the generation of the keys for crypto-stego technique is given as follows:

1. In 3D-ACM the parameters a and b are chosen as secret keys.
2. Calculate the Hash "MD5" of secret message (digital image) which is used for 3D-ACM iteration.
3. 3D-ACM encryption is symmetric key encryption that is keys are same in both sides (sender and receiver).
4. Steganography keys are generated using the permutation on eight symbols that is stego keys $K_i \in S_8$ for $i = 1$ to 40320 where the permutation group on eight symbols of order 40320 is S_8 .

For example:

$K_1 = \{1R2, 2R3, 3R1, 4G1, 5G2, 6G3, 7B1, 8B2\}$, $K_2 = \{2R1, 3G1, 1B1, 6G2, 8R2, 5B2, 4G3, 7R3\}$

$K_3 = \{4G1, 6B1, 5R1, 1R2, 3B2, 7G2, 8R3, 2G3\}$, $K_4 = \{5R1, 3R3, 2G1, 1B1, 6R2, 8G2, 4B2, 7G3\}$

Here meaning of 1R2: least significant bit of red component of cover image 2 is substitute by first bit of encrypted image, meaning of 2R3: least significant bit of red component of cover image 3 is substitute by second bit of encrypted image and similarly other.

5. Proposed steganography method is based on symmetric key so chosen stego key is same in both side (sender and receiver).

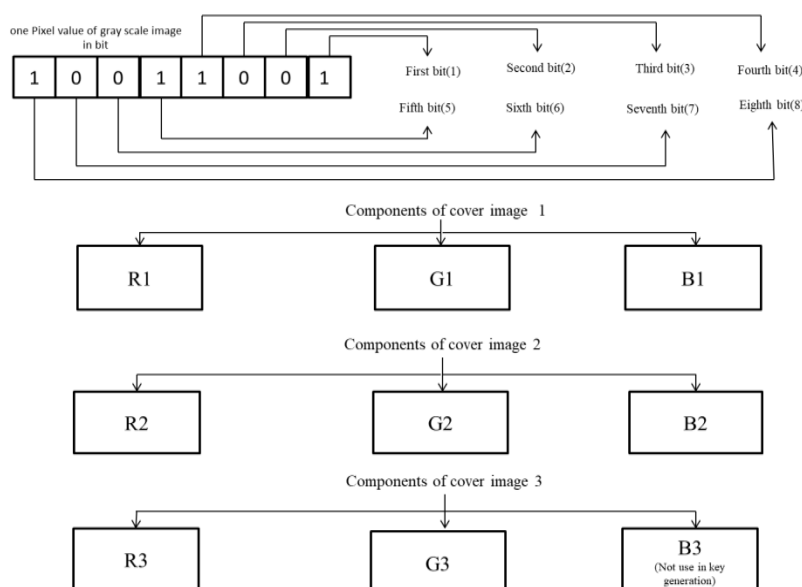


Figure 1: Stego key generation process

Proposed Crypto-Stego Method

In this paper we propose a new crypto-stego method to send a secret image using multiple cover images. First the secret digital image [6] is encrypted by using 3D-ACM and then this encrypted secret image is hidden on multiple RGB images by using steganography LSB method by choosing the steganographic keys from the permutation group on 8 symbols. The details of the proposed algorithm are given as follows:

Secret digital image + 3D-ACM = encrypted digital image

Cover image + encrypted digital image + stego key = crypto-stego-image

In the proposed method we take 3D-ACM given below by taking $\alpha = 1$ and $\beta = 1$

$$\begin{bmatrix} x'_1 \\ x'_2 \\ x'_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 2 & 0 \\ a & b & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \pmod{N}$$

We use 3D-ACM for encryption of secret digital image of size N. This 3D-ACM performs dual encryption, firstly it performs the permutation and secondly it performs the substitution. We permute the secret image s times using 3D-ACM. Number of times 's' is computed by using Hash function [5] of the image.

$$r = \text{Hash}[\text{Image}, \text{"MD5"}]$$

$$s = (r) \pmod{c}$$

Where c is the cyclic order of ACM for given square image.

The substitution in the pixel is given by $x'_3 = (ax_1 + bx_2 + x_3) \pmod{M}$, where a and b are secret keys. After applying 's' time's 3D-ACM on secret image we get encrypted image. After get encrypted image we use steganography. For use steganography we take binary representation of the encrypted digital image. In this proposed steganography method sender chose stego key among the stego keys $K_i \in S_8$ and hide the secret encrypted image based on the pattern given in the stego key.

In this proposed method we take encrypted digital image (square image) obtain after applying 3D-ACM on secret digital image (square image) and three RGB cover images of size same as secret digital image. Take the binary representation of encrypted digital image and separate the RGB-components of the cover images and take binary representation of each components of each cover image. Suppose the sender choose the stego key K_2 , according to second stego key the first bit of first pixel of R-component of cover image 1 is substituted by second bit of first pixel of encrypted digital image. The first bit of second pixel of R-component of cover image 1 is substituted by second bit of second pixel of encrypted digital image. This process is continue up to the order of the encrypted digital image (encrypted digital image and cover images have same order). The first bit of first pixel of G-component of cover image 1 is substituted by third bit of first pixel of encrypted digital image and first bit of second pixel of G-component of cover image 1 is substituted by third bit of second pixel of encrypted digital image.

image. This process is continuing up to the order of the encrypted digital image. According to the chosen stego key remaining bits of encrypted digital image substitute the LSBs of the components of cover images.

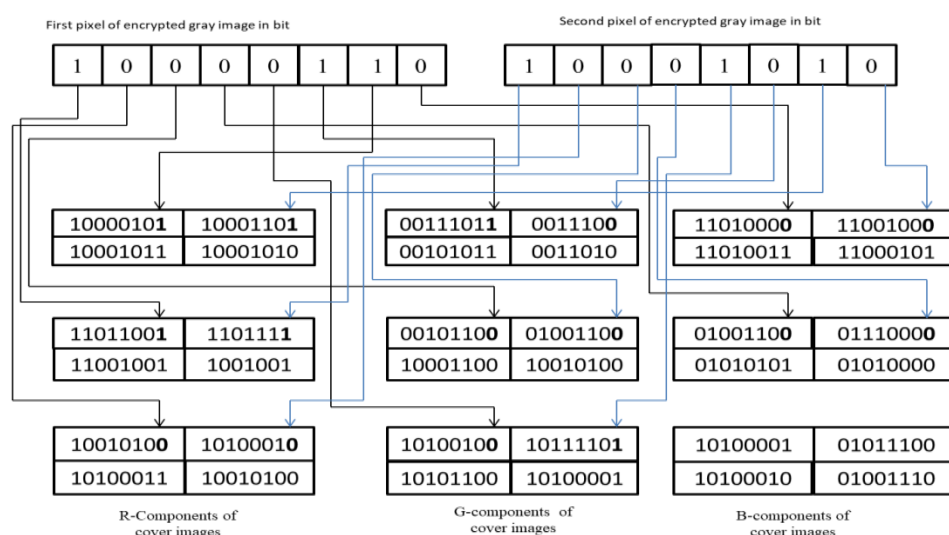


Figure 2: Hiding Process using three cover images

Recovery of Secret Image of the Proposed Crypto-Stego Method

Receiver obtains three crypto-stego-images send by sender. Receiver separates the components of all the crypto-stego-images. Take binary representation of all components of the crypto-stego-images and follow the pattern given in chosen stego key, obtain encrypted image. After getting encrypted image we apply 3D inverse Arnold Cat Map which has given below.

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 2 & -1 & 0 \\ -1 & 1 & 0 \\ a & b & 1 \end{bmatrix} \begin{bmatrix} x'_1 \\ x'_2 \\ x'_3 \end{bmatrix} \pmod{N}$$

The original pixel values are given by $x_3 = (x'_3 - ax_1 - bx_2) \pmod{M}$. After s time's 3D-iACM is applied on encrypted image we get decrypted image.

Implementation of Proposed Method

Implementation of the Proposed Algorithm from Sender Side

1. Take a digital image (secret image) (I) of size N.
2. Find the hash of the image using "MD5" method.
 $r = \text{Hash} [\text{Image}, \text{"MD5"}]$
 $s = (r) \pmod{c}$, Where c is the cyclic order of ACM for given square image.
3. Apply 's' time's 3D-ACM to scramble the pixels of the digital image.
4. Substitution in the pixels of the scrambled image given by the equation $x'_3 = (ax_1 + bx_2 + x_3) \pmod{M}$, we get encrypted image.
5. Take three RGB cover images of size N in which encrypted image is to be hiding.
6. Separate the R, G, B components of each cover image.
7. Take binary representation of encrypted image and all components of cover images.
8. Choose any stego key from the multiple stego keys $K_i \in S_8$.
9. Follow the pattern of key, substitute the LSBs of cover images by encrypted image bits.
10. With the new pixels values generate crypto-stego-images.
11. The crypto-stego-images generated using proposed crypto-stego method is send to the receiver.

Implementation of the Proposed Algorithm from Receiver Side

1. Receiver receives the crypto-stego-images.
2. Separate the R, G, B components of the crypto-stego-images.
3. Take binary representation of all components of each crypto-stego-image.
4. Use the stego key retrieve the binary data and then encrypted image.
5. Apply s times 3D-iACM on encrypted image obtain decrypted image.

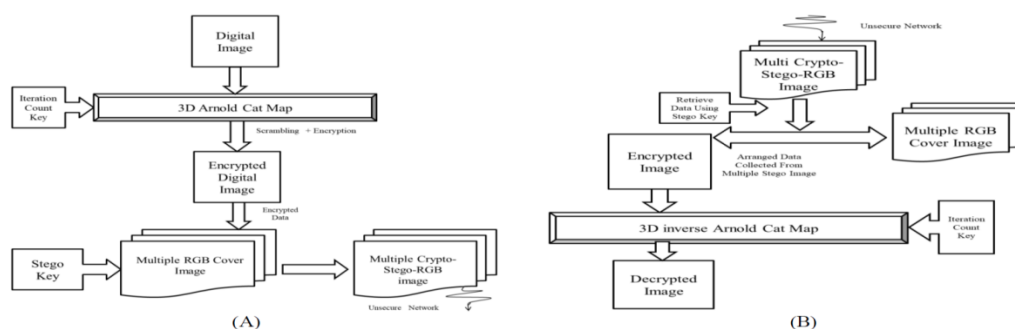


Figure 3: Hiding process with encryption and recovery process with decryption

V. Experimental Results

We apply our proposed crypto-stego technique in two digital images Lena and Lion image. Experimental results on these images are given below.



Figure 4: (A):- (a) Lena image(Secret message) (b) Image after 3D-ACM encryption (c) Cover RGB image 1 (d) Cover RGB image 2 (e) Cover RGB image 3 (f) Crypto-stego-image 1 (g) Crypto-stego-image 2 (h) crypto-stego-image 3, (B):-(a) Crypto-stego-image 1 (b) Crypto-stego-image 2 (c) Crypto-stego-image 3 (d) Retrive image from crypto-stego-images (e) Decrypted image after 3D-iACM.

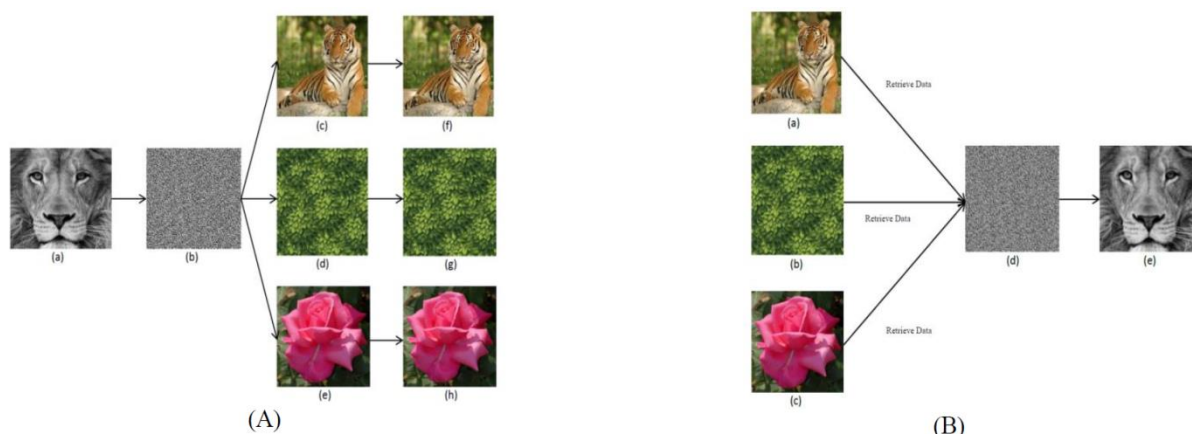


Figure 5: (A):-(a) Lion image(Secret message) (b) Image after 3D-ACM encryption (c) Cover RGB image 1 (d) Cover RGB image 2 (e) Cover RGB image 3 (f) Crypto-stego-image 1 (g) Crypto-stego-image 2 (h) crypto-stego-image 3, (B):-(a) Crypto-stego-image 1 (b) Crypto-stego-image 2 (c) Crypto-stego-image 3 (d) Retrive image from crypto-stego-images (e) Decrypted image after 3D-iACM.

VI. Statistical Analyses

Entropy Analysis

Mathematical equation for computation of entropy is given by Shannon [10].

$$H(Y) = - \sum_{i=1}^N P(y_i) \log_2 P(y_i)$$

Where $P(y_i)$ is the probability mass function.

Table shows that the entropy values of cover images and crypto-stego images are nearly equal. It means cover images and crypto-stego images look similar. Thus adversary cannot make out that any data is hidden in cover images.

Image		Cover Image	Crypto-Stego Image
Cover Image-1 and Crypto-Stego Image-1	R	7.7649	7.7656
	G	7.5581	7.5586
	B	7.4277	7.4281
Cover Image-2 and Crypto-Stego Image-2	R	6.8826	6.9407
	G	6.9241	6.9672
	B	5.7657	5.8109
Cover Image-3 and Crypto-Stego Image-3	R	7.7219	7.7251
	G	7.0584	7.0599
	B	7.4186	7.4196

Table 1: Entropy of cover images and crypto-stego images

Histogram analysis

An image histogram is the graphical distribution of intensities and plots the number of pixel for each intensity value. From the figures histogram of multiple cover images and crypto-stego images are resemble with each other. Thus, one cannot make out that any data is hidden in cover images.

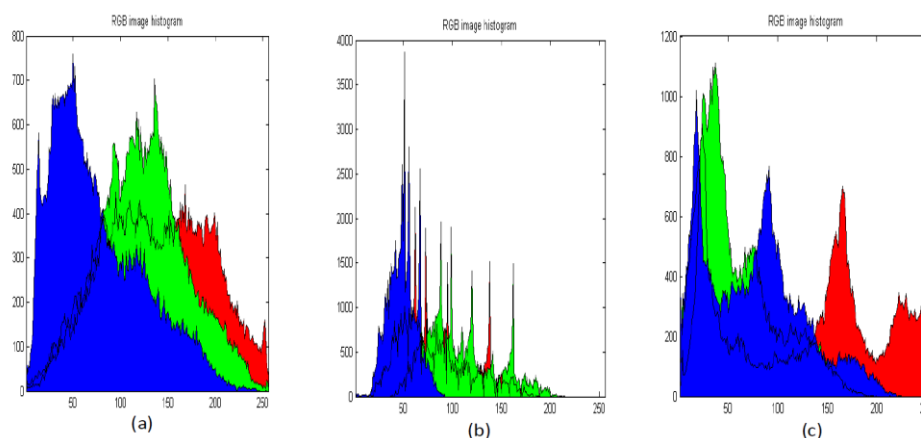


Figure 5: Histogram analysis of cover images: (a) Cover image 1 (b) Cover image 2 (c) Cover image 3

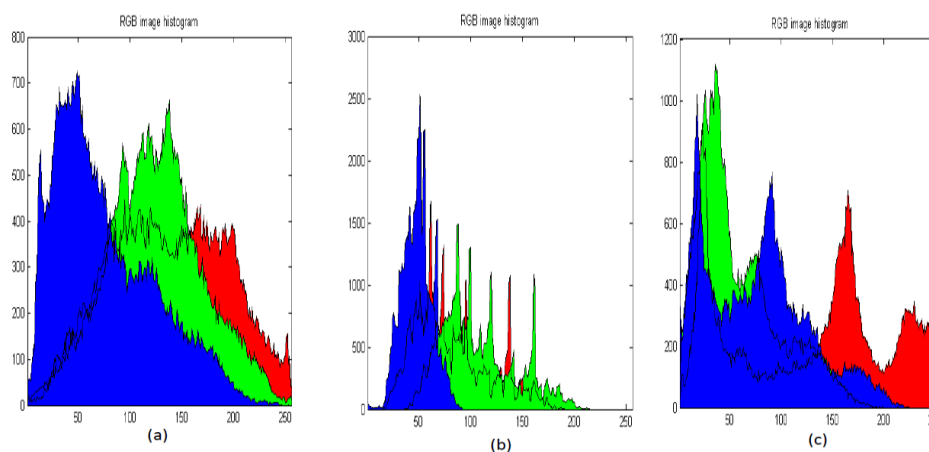


Figure 6: Histogram analysis of crypto-stego-images: (a) Crypto-stego-image 1 (b) Crypto-stego-image 2 (c) Crypto-stego-image 3

Mean square error, peak signal to noise ratio and correlation coefficient analysis

There are various quality measurement variable available for example peak signal to noise ratio (PSNR), mean square error (MSE) and correlation coefficient, to find out how well an image is reproduced with respect to the

reference image. PSNR is defined as ratio of amount of significant signal information to noise. Lower the value of MSE and higher the value of PSNR shows that both the images are similar. The PSNR and MSE between the cover image and crypto-stego-image for red(R), green (G), and blue (B) components are computed from

$$PSNR = 10 \log_{10} \frac{(255)^2}{MSE}$$

$$MSE = \frac{1}{MN} \sum_{x=1}^M \sum_{y=1}^N [f(x,y) - \hat{f}(x,y)]^2$$

Where $f(x,y)$ is cover image and $\hat{f}(x,y)$ is crypto-stego image and M, N are the number of pixels of the frame. The values of correlation coefficient vary from -1 to 1. Two adjacent pixels are strongly correlated horizontally, vertically and diagonally in cover image as well as crypto-stego-image. This shows that both images are very similar to each other. Thus, one cannot make out that any data is hidden in cover images.

Correlation coefficient (C_{AB}) of RGB-components of cover image A and crypto-stego-image B are computed from

$$C_{AB} = \frac{\sum_i^m \sum_j^n (A_{i,j} - \bar{A})(B_{i,j} - \bar{B})}{\sqrt{[\sum_i^m \sum_j^n (A_{i,j} - \bar{A})^2][\sum_i^m \sum_j^n (B_{i,j} - \bar{B})^2]}}$$

Where $A_{i,j}$ and $B_{i,j}$ are the pixels in the i^{th} -row and j^{th} -column of cover image A and crypto-stego-image B respectively, $\bar{A}$ and $\bar{B}$ are respectively, mean of cover image and crypto-stego-image and m, n represent the number of rows and columns in the image.

Components	MSE	PSNR	Correlation Coefficient
Red	0.4978	51.1941	0.9999
Green	0.5018	51.1594	0.9998
Blue	0.4999	51.1763	0.9999

Table 2: Statistical analysis for secret data: analysis between cover images1 and crypto-stego-image1

Components	MSE	PSNR	Correlation Coefficient
Red	0.4969	51.2020	0.9998
Green	0.4993	51.1809	0.9998
Blue	0.4987	51.1864	0.9988

Table 3: Statistical analysis for secret data: analysis between cover image2 and crypto-stego-images2

Components	MSE	PSNR	Correlation Coefficient
Red	0.0000	∞	1.0000
Green	0.4998	51.1766	0.9998
Blue	0.0000	∞	1.0000

Table 4: Statistical analysis for secret data: analysis between cover image 3 and crypto-stego-image 3

Pixel intensity correlation graph

Pixel intensity correlation graphs represent relation of pixels within image in horizontal, vertical and diagonal direction. Pixel intensity relation graph for all cover images in each direction horizontal, vertical and diagonal matches pixel intensity relation graph for all crypto-stego-images in horizontal, vertical and diagonal direction respectively. This shows robustness to any kind of attack as no one is aware of presence of any kind of data.

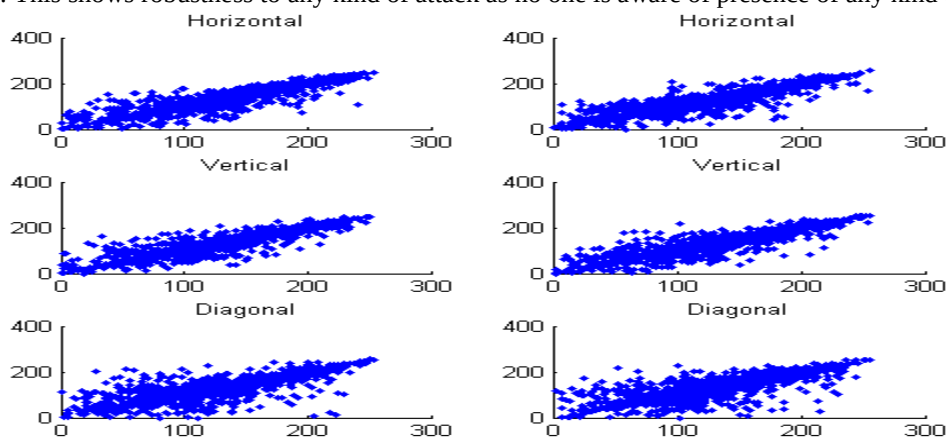


Figure 7: Pixel intensity distribution between cover image 1 and crypto-stego-image 1 in horizontal, vertical and diagonal direction

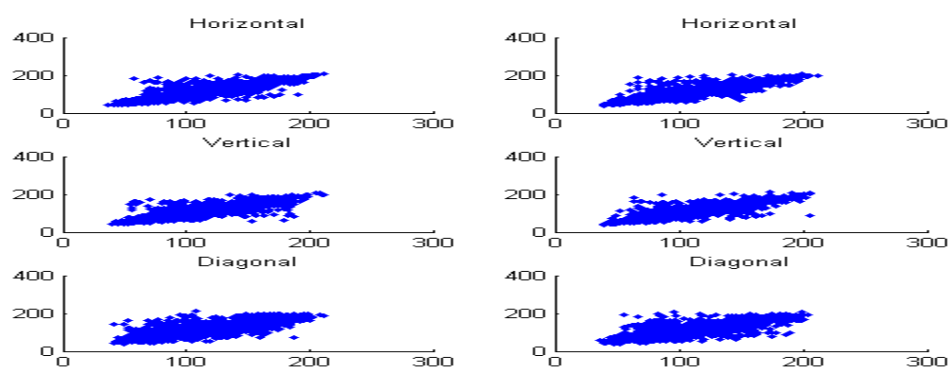


Figure 8: Pixel intensity distribution between cover image 2 and crypto-stego-image 2 in horizontal, vertical and diagonal direction

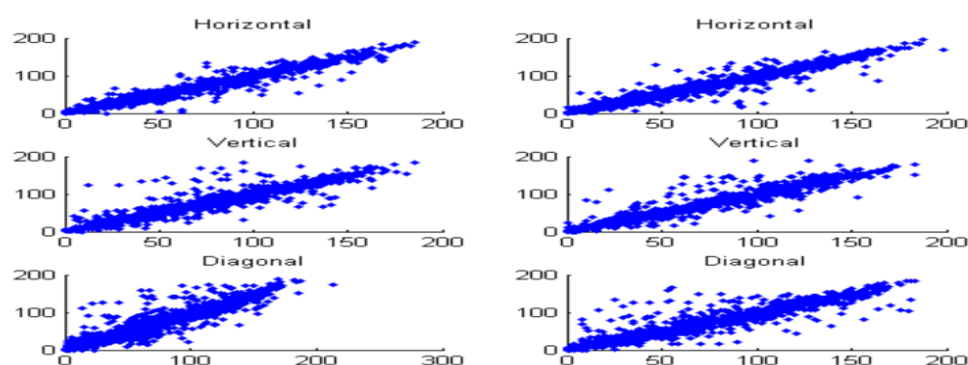


Figure 9: Pixel intensity distribution between cover image 3 and crypto-stego-image 3 in horizontal, vertical and diagonal direction

VII. Comparison

We compare our proposed method with some other existing methods. We have considered some earlier developed methods, Mingwei T. [7], Sahil Kataria[8] for comparison to proposed crypto-stego-system. Now, Mingwei T. have developed a high capacity image steganography using multilayer embedding, which can enhance the performance of information hiding system and Sahil Kataria has given a steganography algorithm for hiding secret message inside image using random key. The paper [7] developed secure image steganography using multilayer embedding. The paper [8] developed secure steganography algorithm using random key. But, our designed crypto-stego-system provides multilayer security for digital image. In the proposed crypto-stego-system if the adversary knows about stego key but no information about iteration key and secret parameters of 3D-ACM then he/she cannot recover the original data from crypto-stego-image. So the presented crypto-stego-system is more robust and appropriate than these already developed methods.

VIII. Conclusion

This paper provide novel image hiding technique based on cryptography and steganography. We use 3D-ACM for image pixel permutation and substitution by introduce two parameters in 3D-ACM and Hash function is used for ACM iteration. Steganography is used for hiding encrypted image. We use LSBs substitution method with stego key for hiding the encrypted image under the three RGB cover images. The process of hiding and recovery is implemented and tested for more than one images and give the consistent result on every image. Entropy analysis, histogram analysis, MSE analysis, PSNR analysis, correlation coefficient analysis and pixel intensity correlation graph analysis show that the proposed method is a robust method of securing digital images.

IX. References

- [1] C.C. Cghang, H.W. Tseng. "A Steganographic Method for Digital Image Using Side Match, Pattern Recognition Letters," 25(2004) 1431-1437
- [2] Rosziati Ibrahim, teoh Suk Kuan. "Steganography Algorithm to Hide Secret Message inside an Image," Computer Technology and application 2(2011) 102-10.
- [3] Hongjuan Liu, Zhiliang Zhu, Huiyan Jiang, Beilei Wang. "A Novel Image Encryption Algorithm Based on Improved 3D Chaotic Cat Map," The 9th International Conference for Young Computer Scientist. IEEE, 2008, pp. 3016-3021.
- [4] Pawan N. Khade and Prof. Manish Narnaware, "3D Chaotic Functions for Image Encryption," International Journal of Computer Science Issues 3, vol. 9, no. 1, May 2012
- [5] B. Kaliski and M. Robshaw, *Message Authentication with MD5*, RSA Labs Crypto Bytes, vol. 1 no. 1, Spring 1995.
- [6] Stephen Johnson (2006), *Stephen Johnson on Digital Photography*, O'Reilly. ISBN 0-596-52370-X.
- [7] Mingwei T., H. Jie and S. Wen, "A High Capacity Image Steganography Using Multilayer Embedding," Optik 125 (2014) 3972–3976.

- [8] Sahil Kataria, Balvinder singh, Tarun Kumar, Narpal Singh Shekhawat, "A Steganography Algorithm for Hiding Secret Message Inside Image Using Random Key," International Journal of Engineering Research and Technology ISSN: 2278-0181 Vol. 3 issue 12 Dec. 2014.
- [9] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press Series for Discrete Mathematics and its Applications, ISBN 0-8493-8523-7.
- [10] Shannon CE(1948), *A mathematical theory of communication*, Bell Syst Tech J 27(3):379-423.
- [11] Rivest R., *The MD5 Message-Digest Algorithm*, RFC 1321, DOI 10.17487/RFC1321, April 1992.
- [12] EE. Kisik Chang, J. Changho, L. Sangjin, "High Quality Perceptual Steganographic Techniques," Springer, Vol. 2939, 2004, pp.518-531.
- [13] G. C. Kessler, "Steganography: Hiding Data Within Data," An edited version of this paper with the title Hiding Data in Data originally appeared in the April 2002 issue of Windows NET Magazine September 2001.