Two Phase Security of Images Using Encryption & steganography in Image Processing

Dhvani C. Panchal[1], Chaita Jani[2], Hemin Panchal[3]

[1] *ME Research Scholar, Computer Engineering, KIRC, Gujarat, India*
[2] *Assistant Professor, Computer Engineering, KIRC, Gujarat, India*
[3] *BE Research Scholar, Computer Engineering, GIT, Gujarat, India*

ABSTRACT

Security is major concern for the transmission of multimedia data. To protect multimedia content from intruder is much more crucial task. Many cryptographic techniques are already available for providing security to multimedia content. Here we proposed the technique to improve security with the help of Encryption & Steganography. Both of these techniques are used at two different phases. In phase-I, encryption is used for converting the input image into cipher image with the help of encryption key. Chirikov mapping is used for encryption of image. In phase-II, steganography is used for hiding the encryption key of phase-I into cipher image with the help of DWT. This provides security to images from intruder with the help of two important cryptographic techniques i.e. Encryption and Steganography. The goal of the system for the implementation is not only protecting image but the key also. It also reduces the cost for transmission of key and adds some level of security for protection of key and image also.

Keyword: - *Encryption, Decryption, encryption key, chirikov mapping, Steganography, Stego-key, DWT.*

1. INTRODUCTION

In multimedia transmission the sending and receiving of multimedia data is not so easy task. As the data exchange in electronic way is rapidly increasing day by day, it is also important to protect the confidentiality of data from unauthorized access. This exchange process has pass through some complexities like data integrity, non-repudiation, authentication, authorization, active/passive attacks, snooping from intruder etc. many cryptographic techniques are available for providing the security of images. Encryption, authentication, key distribution, steganography, etc. are some of cryptographic techniques. One technique used here is encryption. Hence encryption of data is done to confirm security in open networks like internet where the multimedia applications are ever growing day by day. Image encryption is the technique which provides security to images with the help of converting the original image into unreadable form of image which is difficult to understand. That is converting input image into cipher image which is un recognizable form. Applications of image encryption can also be extended to military communication, multimedia systems, medical science, telemedicine, internet communication etc. [1].

Another technique used here is steganography. Steganography is an art of hiding secret information inside a carrier like image, audio, video. Image steganography is technique of hiding data into a carrier which is in the form of image. Hidden data can be in the form of text, image, video, audio etc. The text data is used as hidden information here and image is used as a carrier. Image Steganography can be represented as ‘Stego-image = Cover image + Secret message + Stego key’. With the help of Stego key the text data which we want to hide into cover medium is embedded without affecting the cover image. The aim of steganography is that the cover medium must not change.

Here, we propose an approach for enhancing the security of image by encryption and steganography. The overall work is divided into two-phases. In phase-I, image (jpeg, png , gif, bmp, tif) is taken as a input, known as input image . This input image will be converted into un recognizable form which is known as cipher image (encrypted image) with help of encryption. Encryption key is used for converting input image into cipher image (encrypted image). In phase-II, steganography is used for the purpose of enhancing security of cipher image and encryption key. Here, encryption key will be hidden in to cipher image with the help of steganography. Stego key is used here for hiding process.

Overall system is built to protect not only image but the key also. An attempt has been for protecting the key, that means if we are protecting the key then it implies security of image. This shows, it is obvious that if you are securing the key, then image will be automatically get secured at some point.

1.1 Image Encryption Using Chirikov Mapping Based On Chaos Theory

Encryption techniques for images can be divided into two groups: chaos methods and non-chaos methods. Encryption of images can also be classified according to the percentage of the data that is encrypted in the form of full encryption and partial encryption.

A chaotic system is a dynamic system that exhibits random behavior as a result of its sensitive dependence on its initial conditions and can never be specified with infinite precision. The behavior of chaotic system is unpredictable; thereby it resembles noise. Cryptographic algorithms and chaotic maps have some similar properties such as sensitivity to changes in the initial conditions and pseudorandom behavior and control parameters, unstable periodic orbits with long periods. The basic principle for image encryption using chaos is depend upon the ability of some dynamic systems to produce sequence of numbers which are random in nature. Messages are encrypted using these sequences. Because of the pseudorandom behavior, the output of the system seems random in the attacker's view whereas it appears as defined in the receiver's view and decryption is possible. An important difference between cryptography and chaos maps is that encryption transformations are defined on finite sets whereas chaos maps have meaning only for real numbers[12]. Figure shows the process of converting *input image* into *cipher image* with the help of key generator.

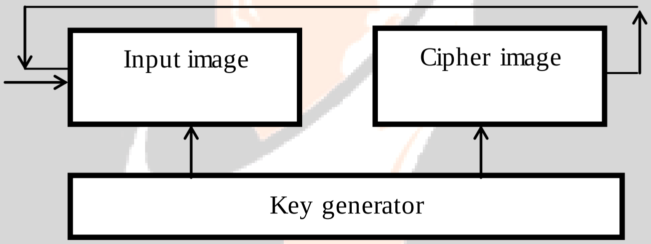


Fig.-1: Image encryption using chaos mapping

The encryption function for chirikov mapping is given by,

$$x_{i+1} = (x_i + y_i) mod\ N \qquad (1.3)$$

$$y_{i+1} = \left(y_i + Ksin\frac{2\pi x_{i+1}}{N}\right) mod\ N \qquad (1.4)$$

Where N is length of width of a square image and K is positive integer. The inverse transform for decryption is given by

$$x_{i+1} = \left(x_i - y_i + Ksin\frac{2\pi x_i}{N}\right) mod\ N \qquad (1.6)$$

$$y_{i+1} = \left(y_i - Ksin\frac{2\pi x_i}{N}\right) mod\ N \qquad (1.7)$$

1.2 Image Steganography

Steganography can be referred as hiding information into another information. That means steganography is an art of hiding one type of data into another type of data. The data which we want to hide is known as hidden data and the data in which the hidden data will get hidden is known as cover data. Both these data can be in the different formats like text, image, audio, video etc.

Image steganography is a technique of hiding any type of data in to image. This means that cover medium for hiding any type of data must be in image format. The hidden data can be text, image etc. One of the main goal of steganography s that the cover media of steganography must not change. The main difference between steganography and encryption is that, in encryption input image will be changed into an un-recognizable form of image which we can't understand. But in steganography, the cover image will be same as we have taken and it is easy to recognize. These shows that the image which we have taken as cover image will not change while we are hiding some data into it. So, it is difficult to find that some information is actually hidden to image. The process of steganography can be represented like this.

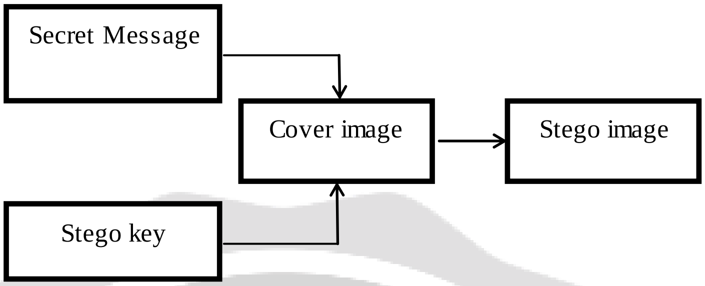


Fig -2: General model for steganography

Many techniques are available for steganography due to popularity. Some of them are listed below [4][14].

1. Spatial domain image steganography
   A. Least significant bit (LSB)
   B. Pixel value differencing (PVD)
   C. Edges based data embedding method (EBE)
   D. Random pixel embedding method (RPE)
   E. Mapping pixel to hidden data method (PMM)
   F. Labeling or connectivity method
   G. Pixel intensity or gray level value (GLV) based
   Method
   H. Texture based method
   I. Histogram based methods
   J. Spread Spectrum based methods
2. Transform domain techniques
   A. Discrete Cosine transform (DCT) based technique
   B. Integer Wavelet Transform (IWT) based techniques
   C. Discrete Curvelet Transform (DCVT) Based
   D. Discrete Wavelet Transform (DWT) based techniques
   techniques
   D.. Discrete Fourier transform (DFT) based technique.
   E. Discrete Wavelet transform (DWT) based technique
3. Spread spectrum
4. Statistical distortion
5. Cover generation

2. LITERATURE REVIEW

In the paper presented by Priya R Sankpal and P. A. Vijaya, an attempt has been made to review the aspects and approaches of the design used for image encryption. A survey is presented based on chaotic mapping techniques of encryption. In this survey paper, the existing chaos based image encryption schemes have been discussed and analyzed to validate their performance against different types of attacks. All the encryption schemes are useful for real time image encryption and each scheme is unique in its own way which is appropriate for different applications. Security can be enhanced by having multiple chaotic maps for image encryption [1].

In the paper presented by Minal Govind Avasare and Vishakha Vivek Kelkar, An image encryption scheme based on chaotic standard map is proposed. Bit level permutation not only changes the locations of the image pixels, but also modifies their values. Such a design can enhance the randomness, even under finite precision implementation. Due to features of bit level permutation, they proposed a bit level confusion and dependent diffusion to enhance the security of cryptosystem. Bit confusion operation reduces the computation redundancy in this stage. Results of our analyses indicate that the new scheme has a satisfactory security level with a low computational complexity, which renders it a good candidate for real-time secure image transmission applications. So, it is a challenge for a research to design an encryption scheme which maintains good tradeoff among tunability, visual degradation, compression friendliness, format compliance, encryption ratio, speed, and cryptographic security [2].

In the paper presented by Pradeep H Kharat and Dr.S.S.Shriramwar, they implement three non linier differential chaos based encryption technique where for the first time 3 differential chaoses is used for position permutation and value transformation technique. In the data hiding phase, data which is in the binary forms embedded into Encrypted image by using least significant bit algorithm. They Tabulate correlation coefficient value both horizontal and vertical position for cipher and original image and compare performance of their Method with some existing methods. The given approach is very simple, fast, accurate and it have been applied together as a double algorithm in order to serve best results in highly unsecure and complex environment [3].

In the paper presented by C.P.Sumathi, T.Santanam and G.Umamaheswari, an attempt to analyze the various techniques used in steganography and to identify areas in which this technique can be applied, so that the human race can be benefited at large. Classifications of stenographic techniques are presented as per their functional criteria. Comparison between different techniques is listed depending upon their pros and PNSR value in chronological order [4].

In the paper presented by Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin, Ashis Kumar Mandal and Md. Delowar Hossain, a new Steganography technique is being developed to hide large data in Bitmap image using filtering based algorithm, which uses MSB bits for filtering purpose. This method uses the concept of status checking for insertion and retrieval of message. This method is an improvement of Least Significant Bit (LSB) method for hiding information in images. It is being predicted that the proposed method will able to hide large data in a single image retaining the advantages and discarding the disadvantages of the traditional LSB method. Various sizes of data are stored inside the images and the PSNR are also calculated for each of the images tested. Based on the PSNR value, the Stego image has higher PSNR value as compared to other method. Hence the proposed Steganography technique is very efficient to hide the secret information inside an image [5].

3. PROPOSED SYSTEM

In proposed system, we have used two techniques for ensuring the security of images and they are encryption and steganography. We have used chirikov mapping from chaotic mapping system. Chirikov mapping has large key space compared to other techniques and it has higher key sensitivity. Due to large key space it will be difficult to find key for intruder and because of higher key sensitivity, the system will be sensitive to the minor changes. That means if we do minor change into key then it will affect image in large range. Which is also difficult to intruder for un authorized access to image. Then for the purpose reducing cost of key distribution we have used steganography. Here, we have used DWT (Discrete Wavelet Transformation) for steganography. Which divides the encrypted image into for sub parts and then Encryption Key is hidden to them. After that all four parts will be concatenate to one image and this image is send over the internet. The overall System flow diagram is shown in Figure 4.

Steps for proposed system at sender side:

1. Take input image & Encryption key.
2. If Encryption key>10000?
3. If no then display Error.
4. If yes then Encrypt input image into cipher image with the help of Encryption key. Chirikov mapping is used here for encryption process.
5. Then hide the encryption key into cipher image with the help of Steganography(DWT).
6. Send cipher image, Encryption Key

Receiver side is opposite of sender side.

Here, all major different types of image formats are supported like .JPG,.PNG,.GIF,.BMP,.TIF. Figure 5 shows the results of grayscale image. We have taken cameramen.Tif image as input image in (A) and its encrypted image is shown in (B) the decrypted image is also shown in (C) which shows, there us no difference between encrypted image and decrypted image. One important point to note it down here is that some level of difference is there for the process of encryption in grayscale & RGB image. In RGB, LAB colorspace is used for better results. The limitations of chirikov mapping that is it only works for 2D images, is overcome by using LAB concept here. In RGB image, it first takes RGB image as input & then convert it into LAB image then Encryption is applied to LAB image & this

Encrypted LAB image is send over the internet. Figure 6 shows the results of RGB image with the help of LAB colorspace. Figure 6 shows the results, we have taken fruit.jpg as input(A), the Encrypted LAB image of input image is shown in (B), decrypted LAB image is shown in (C), and last original image is shown in (D). following Figure shows the overall system flow diagram.

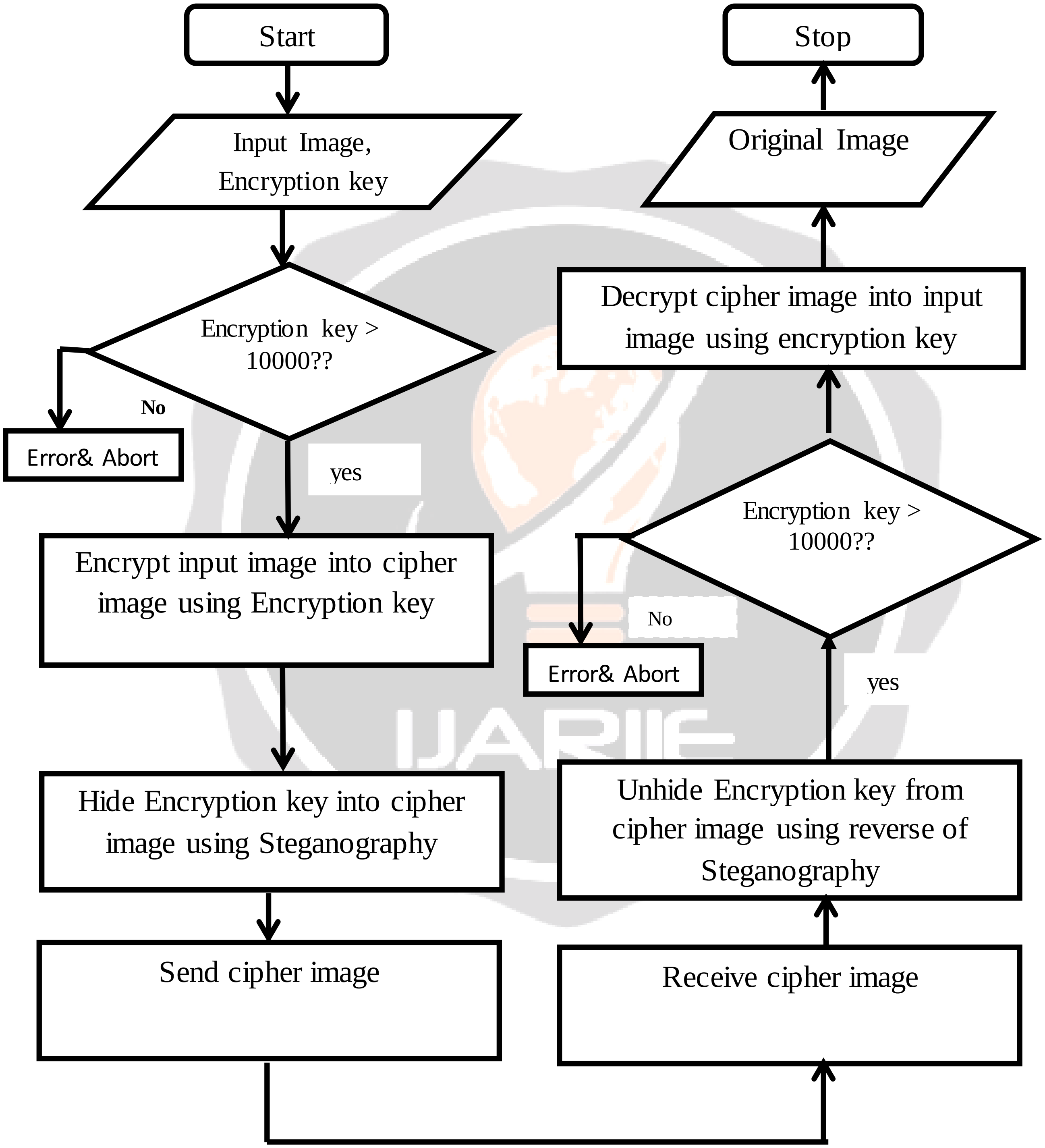
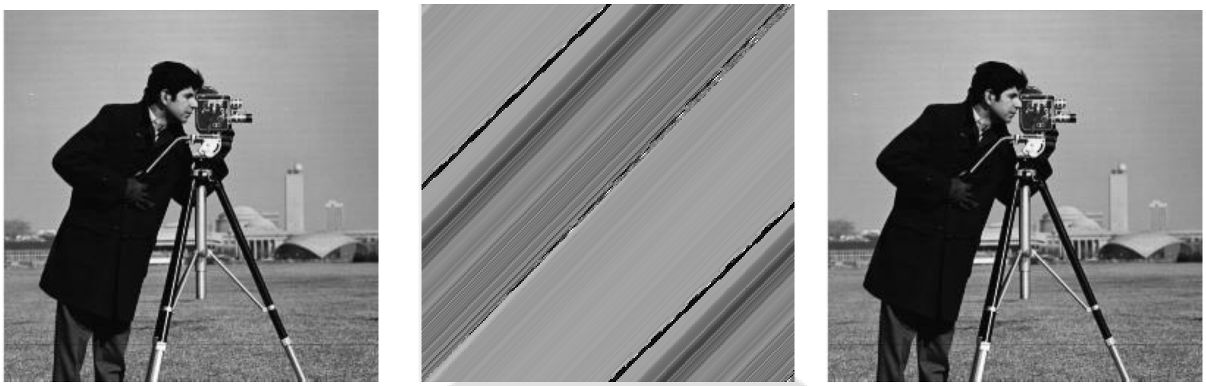
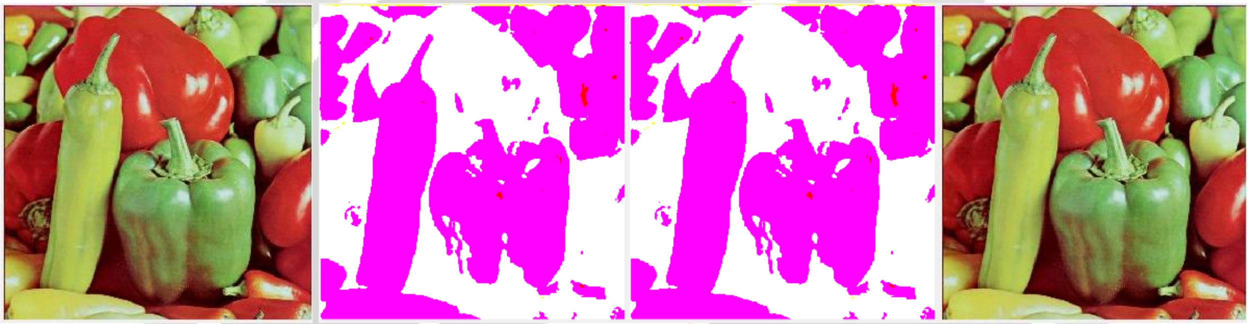

Start
Input Image, Encryption key
Encryption key > 10000??
No
Error& Abort
yes
Encrypt input image into cipher image using Encryption key
Hide Encryption key into cipher image using Steganography
Send cipher image
Receive cipher image
Unhide Encryption key from cipher image using reverse of Steganography
yes
Encryption key > 10000??
No
Error& Abort
Decrypt cipher image into input image using encryption key
Original Image
Stop

Fig -3: system flow diagram



A Input image B Encrypted image C Decrpted image

Fig -4: A, B,C: Grayscale image Encryption



A Input image B:Encrypted LAB image C:Decrypted LAB image D: Decrpted image

Fig -5: A,B,C,D: RGB image Encryption using LAB color space

4. CONCLUSION

Large key space is provided along with high key sensitivity which makes system more reliable against intruder attacks. Due to steganography, cost & time of key distribution will be reduced. It is remarkable that, chirikov mapping works for gray scale image, we overcome this point by using LAB concept. LAB colorspace also adds some level of accuracy to image representation which adds better output results. Due to Discrete Wavelet Transformation, the steganography also adds some more level security to proposed sysem.

5. ACKNOWLEDGEMENT

It gives me great pleasure in expressing thanks and profound gratitude to my parents, my family members and guide for their valuable guidance and continual encouragement throughout part one of the Major projects. I am heartily thankful to them for their time to time suggestions and the clarity of the concepts of the topic that helped me a lot during this study, thanks to all of these without whom this project would have been a distant reality because of them I am able to complete my research work successfully.

6. REFERENCES

[1] Priya R Sankpal and P. A. Vijaya, "Image Encryption Using Chaotic Maps: A Survey", International Conference on Signals and Image Processing, 2014.

[2] Minal Govind Avasare and Vishakha Vivek Kelkar, “Image Encryption using Chaos Theory”, International Conference on Communication, Information & Computing Technology (ICCICT), Jan. 16-17,2015

[3] Pradeep H Kharat and Dr.S.S.Shriramwar, “A secured Transmission of data using 3D chaotic map encryption and data hiding technique”, International Conference on Industrial Instrumentation and Control (ICIC) College of Engineering Pune, India. May 28-30,2015

[4] C.P.Sumathi , T.Santanam and G.Umamaheswari , “A Study of Various Steganographic Techniques Used for Information Hiding” international Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

[5]md. Rashedul islam, ayasha siddiqa, md. Palash uddin, ashis kumar mandal and md. Delowar hossain,” an efficient filtering based approach improving lsb image steganography using status bit along with aes cryptography”, 3rd international conference on informatics, electronics & vision 2014

[6] Pawan N. Khade and Prof. Manish Narnaware, "3D Chaotic Functions for Image Encryption", International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, PP 323-328, May 2012.

[7] Zhou Zhe, Yang Haibing, Zhu Yu, Pan Wenjie and Zhang Yunpeng, "A Block Encryption Scheme Based on 3D Chaotic Arnold Maps", International Asia Symposium on Intelligent Interaction and Affective Computing, 2009.

[8] Chong Fu, Jun-jie Chen, Hao Zou, Wei-hong Meng, Yong-feng Zhan, and Ya-wen, “A chaos-based digital image encryption scheme with an improved diffusion strategy”, Optical Society of America, Vol. 20, No. 3 /pp 2363 – 2378, 30 January 2012.

[9] Pawan N. Khade and Prof. Manish Narnaware, “3D Chaotic Functions for Image Encryption”, International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, PP 323-328, May 2012.

[10] Sunny Dagar, “Highly Randomized Image Steganography using Secret Keys”, IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014.

[11] Fabien A.P.Petitcolas, Ross J.Anderson and Markus G.Kuhn, “Information Hiding – A Survey”, Proceedings of the IEEE, special issue on protection of multimedia content, pp.1062-1078,1991.

[12] Chong Fu, Jun-jie Chen, Hao Zou, Wei-hong Meng, Yong-feng Zhan, and Ya-wen, “ A chaos-based digital image encryption scheme with an improved diffusion strategy”, Optical Society of America, Vol. 20, No. 3 /pp 2363 – 2378, 30 January 2012.

[13] Anjali Tiwari, Seema Rani Yadav and N.K. Mittal, “A Review on Different Image Steganography Techniques”, International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 7, January 2014.

[14] Abhinav Srivastava, “A survey report on Different Techniques of Image Encryption”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 6, June 2012.

[15] M Bin Younas and Jawad Ahmad, Comparative “Analysis of Chaotic and Non-chaotic Image Encryption Schemes” 978-1-4799-6089-7/14/$31.00, 2014.