An Approach Providing Two Phase Security of Images Using Encryption and Steganography in Image Processing

[1]Dhvani Panchal, [2]Chaita Jani, [3]Hemin Panchal
[1]ME Research Scholar, [2]Assistant Professor, [3]BE Research scholar
[1]Department of Computer Engineering,
[1]KITRC, Kalol. INDIA

***Abstract* - Security is major concern for the transmission of multimedia. To protect multimedia content from intruder is much more crucial task. Many cryptographic techniques are already available for security of multimedia content. This paper proposes Two-phase security of images by using encryption & steganography. It provides security of images from intruder with the help of two important cryptographic techniques i.e. Encryption and Steganography. Here, both 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. 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.**

***Keywords* - Image encryption, Encryption key, Image steganography, Stego key, Chirikov mapping**

I. INTRODUCTION

In multimedia transmission the sending and receiving of multimedia data is not so easy. As the data exchange in electronic way is rapidly increasing, 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 in this paper is encryption. Hence encryption of data is done to confirm security in open networks such as the internet where the multimedia applications are ever growing day by day. Image encryption is a technique that provides security to images by converting the original image into an image which is difficult to understand. That is converting input image into cipher image which is un recognizable form. Applications of image encryption can extended to military communication, multimedia systems, medical science, telemedicine, internet communication etc. [1].

Another technique in this paper is used 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 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'. Stego-key is used to control the hiding process so as to restrict detection and /or recovery of the embedded data to parties who know it. 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.

In this paper 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) 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* with help of encryption. *Encryption key* is used for converting *input image* into *cipher 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.

II. LITERATURE SURVEY

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, existing chaos based image encryption schemes have been discussed and analyzed to check their performance against different types of attacks. All the encryption schemes are useful for real time image encryption and each scheme is unique, which is appropriate for different applications. Security can be increased by using 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 modifies their values also. This design can enhance the randomness, even under finite precision implementation. Because of features of bit level permutation, they proposed a bit level confusion and diffusion to increase security. Bit confusion operation can reduces the computation redundancy in this stage. Result shows that new scheme has a satisfactory security level with a lower computational complexity. So, it is a challenge for a research to design an encryption scheme which can maintain a good tradeoff among tunability, speed, visual degradation, format compliance, encryption ratio, compression friendliness, 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 3 differential chaoses is used for position permutation and value transformation technique. In the data hiding phase, data in the binary forms embedded into Encrypted image by using least significant bit algorithm (LSB). They also Tabulate correlation coefficient value both horizontal and vertical position for cipher and original image and they 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 also identify the areas in which this technique can be used, so 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 can be predicted that proposed method will able to hide large data in a single image increasing advantages and decreasing 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. Depending upon the PSNR value, Stego image has higher PSNR value as compared to other method. Hence the proposed Steganography technique is really very efficient to hide the secret information inside an image [5].

In the paper presented by Sunny Dagar, they propose a new approach for image steganography in which they uses two secret keys to randomize the bit hiding process. Because of two secret keys improves security of secret information. This approach uses red, green and blue values of a pixel and also performs some calculations. Depending upon this calculation, the secret information bits will be placed at random position of the pixel. This approach maintains high data hiding capacity just like LSB(least significant bit) substitution but maintains a much better security level also , which is not present in LSB substitution LSB substitution technique is predictable. They have used PSNR value to determine the quality of Stego image and they compare it with other efficient image steganography techniques also. The result shows that this technique is highly efficient compared to other techniques[10].

III. 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.

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 map 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.

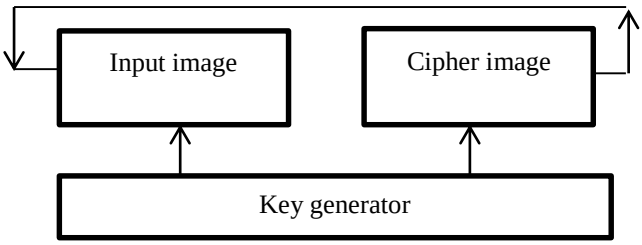

Figure 1. Image encryption using chaos mapping

Chirikov mapping from chaotic system First we will do transformation;

$$a_{i+1} = (a_i + b_i) mod 2\pi \quad (1.1)$$

$$b_{i+1} = (b_i + K \sin(a_i + b_i)) mod 2\pi \quad (1.2)$$

where k is control parameter satisfying k>0, and the ith states and b i both take real values in [0, 2π) for all i. For k = 0, the map is linear and only periodic and quasi-periodic orbit exist.
The encryption function for chirikov mapping is given by,

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

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

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

$$x_{i+1} = \left(x_i - y_i + Ksin\frac{2\pi x_i}{N}\right) mod\ N \quad (1.5)$$

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

IV. IMAGE SEGANOGRAPHY

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.

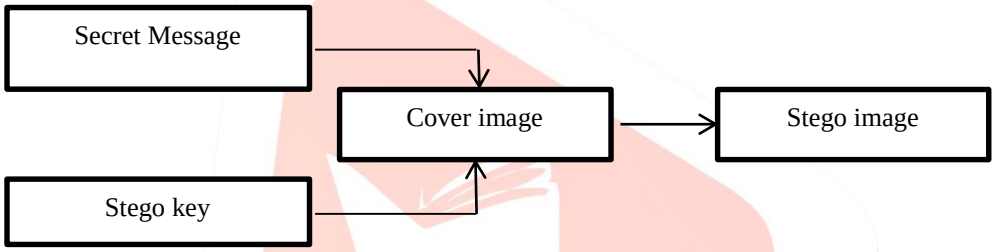

Figure 2. General model for steganography

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 techniques
   D.. Discrete Fourier transform (DFT) based technique.
   E. Discrete Wavelet transform (DWT) based technique..
3. Spread spectrum
4. Statistical distortio
5. Cover generation

V. PROPOSED WORK

In proposed work, we will use two techniques for ensuring the security of images and they are encryption and steganography. We will use 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 will use steganography. Here, we will implement the LSB technique with the random selection of pixel. The least significant bits of random pixel will be replaced by *Encryption key*.

Steps for proposed system at sender side:

1. Take *input image*.
2. Encrypt *input image* into *cipher image* with the help of *encryption key*. Chirikov mapping is used here for encryption process.
3. Check that *input image* is un-recognizable or not. If it is not un-recognizable then apply encryption process up to predefined throughput.
4. Then hide the *encryption key* into *cipher image* with the help of *stego key*.
5. Send cipher image and stego key.

The receiver side process is reverse of sender side. The overall procedure of proposed work is depicted in Fig. 3.

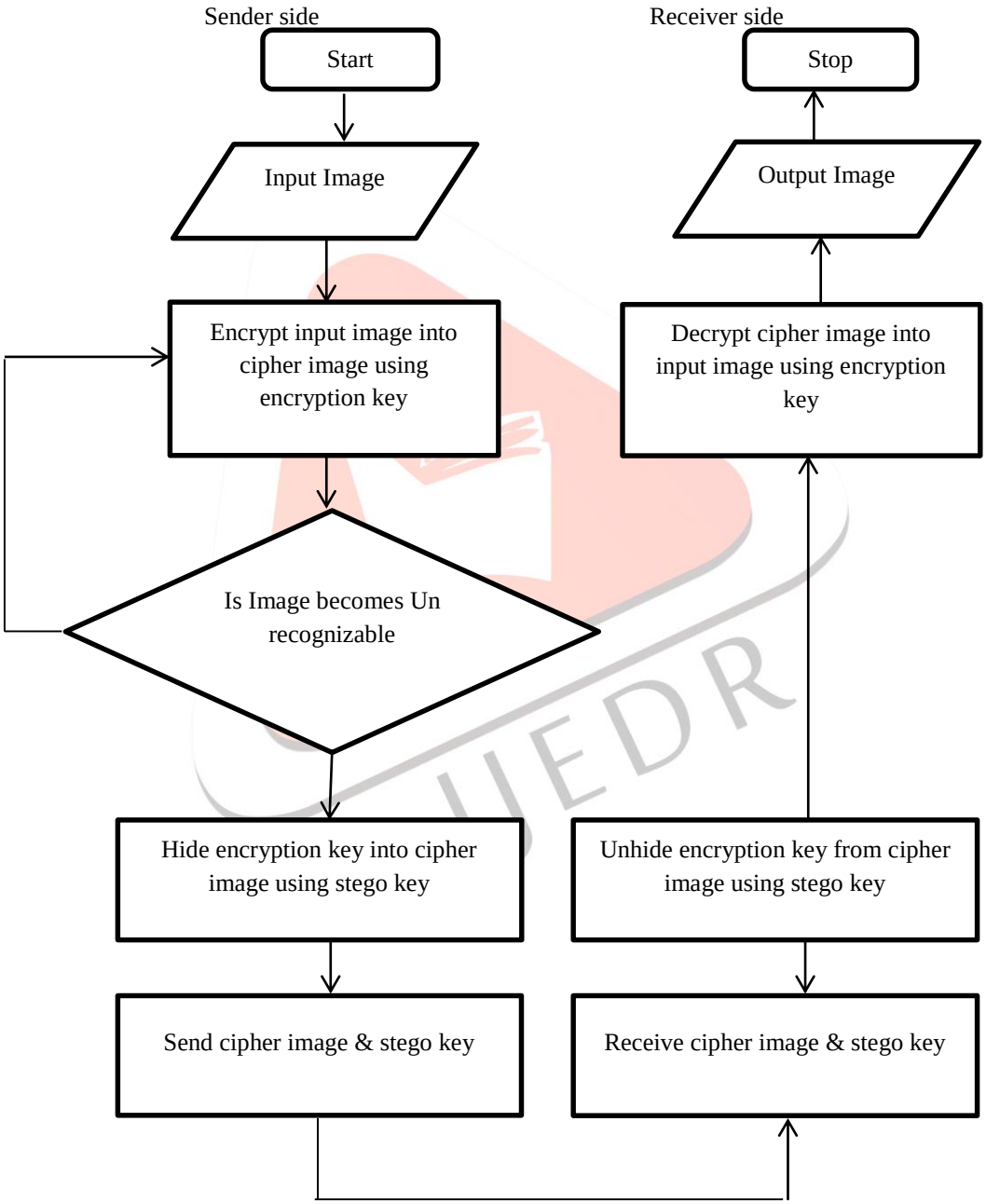

Figure 3. Over all process of system using encryption &and steganography

VI. CONCLUSION

In this paper, we use image encryption techniques for converting input image into cipher image. For that purpose we have use chirikov standard mapping from chaotic mapping system which has large key space in it and also high key sensitivity. This makes system more reliable against intruder attacks. Then we use image steganography for enhancing the security of system. The

encryption key will be hidden into cipher image without affecting it. This will reduce the cost of key distribution and also saves time for transmission of key between sender, receiver and third party distributer.

VII. ACKNOWLEDGEMENT

The authors would like to thank Principal, and teaching staff of Computer Science and Engineering department for providing their valuable guidance and support to carrying out this work.

REFERENCES

[1] Priya R Sankpal, P. A. Vijaya," Image Encryption Using Chaotic Maps: A Survey", International Conference on Signals and Image Processing,2014.
[2] Minal Govind Avasare, Vishakha Vivek Kelkar," Image Encryption using Chaos Theory", International Conference on Communication, Information & Computing Technology (ICCICT), Jan. 16-17,2015.
[3] Pradeep H Kharat, 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 Steganography Techniques Used for Information Hiding ", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.
[5]Md. Rashedul Islam, Ayesha 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]Jitha Raj.T, PG Scholar, E.T Sivadasan, Asst. Professor," A Survey Paper on Various Reversible Data Hiding Techniques in Encrypted Images"
[7]Zhou Zhe, Yang Haibing, Zhu Yu, Pan Wenjie, 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, 30 January 2012 / Vol. 20, No. 3 /pp 2363 – 2378.
[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, Jaipur, India.
[11] Fabien A.P.Petitcolas, Ross J.Anderson and Markus G.Kuhn, (1999) "Information Hiding – A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, pp.1062-1078
[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, 30 January 2012 / Vol. 20, No. 3 /pp 2363 – 2378.
[13] Anjali Tiwari, Seema Rani Yadav, 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.