Advance Data Hiding in Spatial Domain Image Using Chaotic Map

Mrs Nilam C. Patil [1], Mr.Vijaykumar V. Patil [2]

Abstract— **In any communication, security is the most important issue in today's world. The information security has become one of the most significant problems in data communication. Lots of data security and data hiding algorithms have been developed in the last decade. Cryptography and steganography are the two major techniques for secret communication. In this paper, the secret image is first encrypted by using AES algorithm which has very good performance and is a most powerful technique compared to other Algorithms. Now this encrypted image is embedded using chaos based steganography. Our proposed model gives two layers of security for secret. The main aim of proposed method to increase security of embedding and extraction phase using AES encryption and 1D logistic map. In order to evaluate performance the proposed algorithm performs series of tests. These tests includes visual test using histogram analysis, information entropy and encryption quality, PSNR and MSE**

***Index Terms*— Cryptography, Steganography, AES, Chaos, 1D Logistic map.**

I. INTRODUCTION

The security of data transmission is most important in communication networks. A communication system is reliable as long as it provides high level of security. Usually, users communicate personal information or important documents. In this case; security, integrity, authenticity and confidentiality of the exchanged data should be provided over the transmission medium. Nowadays, internet multimedia is very popular; a significant amount of data is exchanged every second over a non secured channel, which may not be safe. Therefore, it is essential to protect the data from attackers. To provide more security, two methods are use such as cryptography and steganography.

Steganography is the art of hiding information imperceptibly in a cover medium. The word "Steganography" is of Greek origin and means "covered or hidden writing". The main aim in steganography is to hide the very existence of the message in the cover medium. Steganography includes a vast array of methods of secret communication that conceal the very existence of hidden information. Traditional methods include use of invisible inks, microdots etc. Modern day steganography techniques try to exploit the digital media images, audio files, video files etc. [1,2]

Manuscript received Dec, 2015.

***1.Mrs Nilam C. Patil**, PG Student , Electronics and Telecommunication Department, KIT's College of Engineering, Kolhapur Kolhapur, Maharashtra, India.*

***2.Mr. Vijaykumar V. Patil**, Assistant Professor , Electronics Department KIT's College of Engineering, Kolhapur, Kolhapur, Maharashtra, India.*

Cryptography is the art and science of achieving security by encoding message to make them non-readable [1]. Means it is used to protect the user data .Cryptography involves two basic functions that are encryption and decryption. Encryption is the process of transforming plain data (which is readable original data file) into the cipher text (data which is unreadable).Whereas decryption is just opposite process of encryption process in which we retrieve the original plain text from cipher text. Cryptography is basically used to hide the original data into a coded data so that unauthorized access can be prevented

The combination of these two methods will enhance the security of the data embedded. This combined will satisfy the requirements such as capacity, security, and robustness for secure data transmission over an open channel.

II. RELATED WORKS

In recent years have seen a rapid growth of communications security and the threat of a trespasser gain access to secret information has been an ever present concern for the data communication experts. Nowadays internet is a popular communication channel. Transmitted data are easy to be copied or destroyed by unauthorized persons. Therefore, how to transmit data secretly by internet becomes an important topic. Encryption may provide a safe way, which transforms data into a cipher text via cipher algorithms [3]. However, it makes the messages unreadable and suspicious enough to attract eavesdropper's attention. To overcome this problem, steganography offers different approaches to transmitting secret messages. Steganography is a technique that imperceptibly hides secret data into cover media by altering its most insignificant components for communication, such that an unauthorized user will not be aware of the existence of secret data. Many successful steganography methods have been proposed. The methods of insertion are various [4]. We can classify them according to the domain of insertion, the hiding methods as well as the image format. The purpose from the methods of insertion is to make secret data invisible and the cover image still unchangeable for the human visual system. In fact, there are many proposals as in exploiting the special encoding of the image in their methods. Thanks to the important specification of spatial and frequency domains, it is interesting to exploit these specifications to dissimulate secret data. For instance, inserting data in the spatial domain [4] is relatively simple than inserting it in frequency domain. They are easy in their implementation, and they are not time consuming. The dissimulation in this scheme works directly on image pixels. Earlier methods exploiting spatial domain were based on the LSB insertion schemes. LSB embeds secret data by replacing k LSBs of a pixel with k secret bits directly [5]. The LSB embedding achieves good balance between the payload

ISSN: 2278 – 7798

capacity and visual quality. The LSB image pixels which are subsequently adjusted for data embedding will be vulnerable against all kind attack. Therefore, in the researches done by so many researchers, the unsystematic data embedding in image LSB has attracted a lot of attention .so many steganography researches employ the fact that in the area which have drastic gray phase changes (such as edges) we can hide more data compared to the smooth ones. [6] in trying to find the surfaces with more drastic changes of the gray area, some conducted researches used the neighboring pixel differences method [7] and in some others for separating the surfaces with drastic changes from the smooth ones, the mean score technique is used between the neighboring (adjacent) pixels. [7]. In both groups after contrasting the two areas and based on their algorithm the data will be embedded in the areas. A technique based on unsystematic data embedding in image LSB has been proposed in which embedding a character in an Image is measured by two chaotic signals and the primary quantities of the two signals will be specified by two hidden keys. What comes next is a short description of the chaotic function and then the proposed technique will be offered and in the final section the empirical results of the proposed technique will be evaluated in different images.

III. CHAOS AND STEGANOGRAPHY

Chaos is a phenomenon related to nonlinear dynamic system [8]. Chaotic systems are sensitive to changes in initial conditions or parameters, an effect which is commonly referred to the butterfly effect. In fact, small differences in initial conditions provide extreme changes on final results. Sensitivity to initial conditions means that each point in such a system is arbitrarily and closely approximated by other points with significantly different future trajectories. Thus, an Arbitrarily small perturbation of the current trajectory may lead to significantly different future behavior. This character is exploited in many domains such us weather forecast, forecast of seizures, predicting the behavior of financial markets and, recently, chaos is employed in information hiding to increase security [9]. Many approaches have worked to exploit the characteristics of chaotic systems to scramble their domain of insertion. Chaos can be applied in security schemes to choose pixels that can be modified or the blocs according to the method of insertion. There are many maps that can exhibit chaotic behaviors such as Tent map, Gauss map, Logistic map [10]. The logistic map is one of the simplest forms of a chaotic process. The 1D logistic map is discrete time analogue of population growth model. It is a non-linear chaotic discrete system that shows random behavior. The equation of logistic map is below:

$$X_{n+1} = \lambda X_n (1 - X_n)$$

Where Xn is the initial value which is used as a secret key in this algorithm , λ is the control parameter which affects the randomness and n is the number of rounds .As the value of the λ increases the randomness(number of periods) increases .λ lies in the range [11,12].The sequence formed by the 1D logistic map is used for diffusion in the encryption process.

IV. THE PROPOSED METHOD

In this section we explain the methodology for the proposed technique and also draw the block diagram of proposed technique. The proposed method embedded Secret image into host image; it is combined between cryptography and steganography in order to provide higher capacity, robustness, and security. In proposed algorithm, secrete image is encrypted using AES. Then apply 1D logistic map method to hide encrypted secrete image into host image.

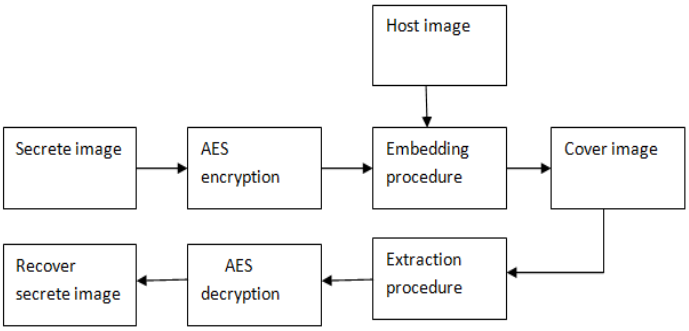


Fig. 1 The block diagram of proposed method

Every method of steganography is based on two processes such as embedding procedure and extracting procedure.

Figure 2and 3 summarize the embedding procedure and extraction procedure using chaos 1D logistic map.

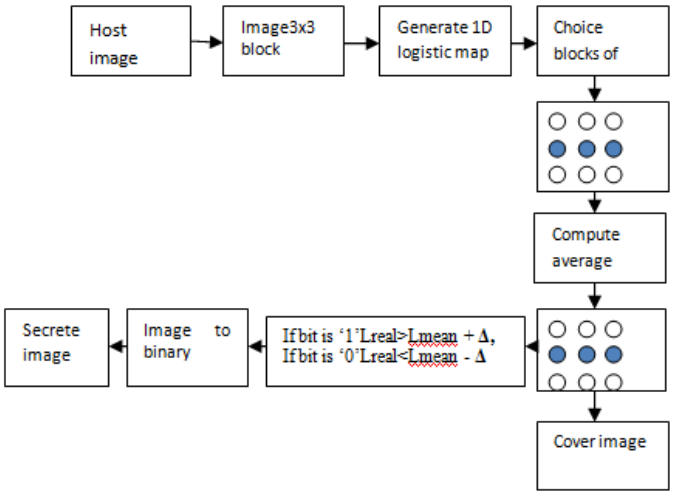


Fig. 2 Embedding procedure

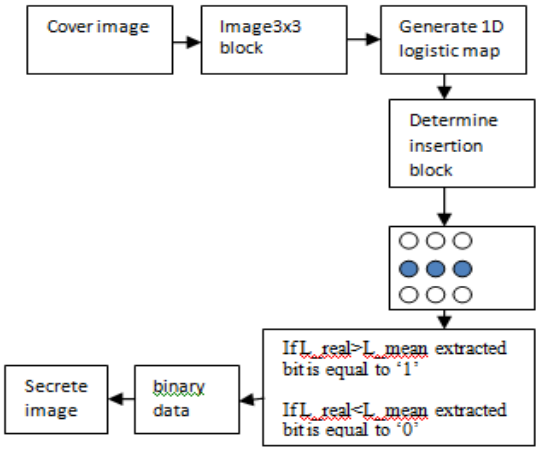


Fig. 3 Extraction procedure

ISSN: 2278 – 7798

A. Algorithm steps of Embedding procedure with Encryption.

Step1: Divide the host image into blocks of 3 x 3.
Step 2: Generate the logistic map.
Step 3: Choose the blocks where we will insert the secret data through the random numbers generated by logistic map
Step 4: Calculate L-mean1, L-mean2 and L- mean3 from the selected blocks.
Step 5: The secret image is encrypted by AES.
Step 6: The encrypted secrete image is converted into binary format.
Step 7: Insert the three bits of secrete message into the chosen blocks of host image.

The modification of pixels will be based on the changing values of pixels by applying the following equations,

- If inserting bit is '1' change the luminance L_ real to have L_ real >L_ mean + Δ.
- If inserting bit is '0' change the luminance L_ real to have L_ real < L_ mean - Δ.
- L_ real is the original pixel value of choose blocks, these choose blocks generate by the logistic map. Δ is taken from 5 to 10% of L_ real.

B. Algorithm steps of the extracting procedure (recover secrete message) with decryption

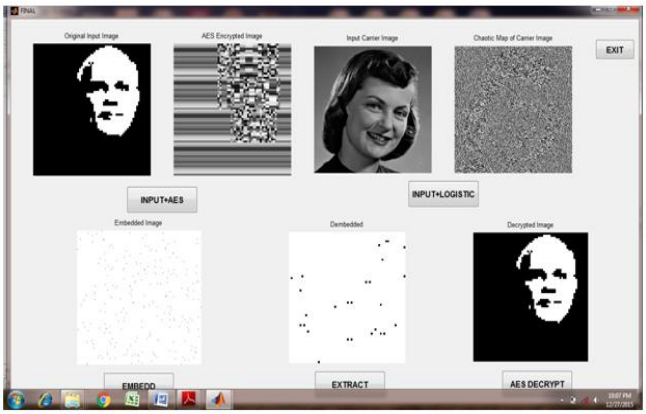
Step1: Divide the cover image into blocks of (3×3).
Step2: Generate the logistic map.
Step3: Identify blocks that have changed generated by the logistic map.
Step4: Calculate L_mean1, L_mean2 and L_mean3 for each selected block.
Step5: Apply the following equations to detect the inserted bits.

- If L_real > L_mean then the extracted bit is '1'.
- If L_real <L_mean then the extracted bit is '0'.

Step6: These detected bits are decrypted by AES.

V. Experimental Results

In this paper, we have used MATLAB for simulating dynamic systems and the analysis and visualization of experimental data. Experimental results are given in this section to demonstrate the performance of our proposed method. In proposed method secrete image is encrypted using AES, then encrypted secrete image hide into host image using 1D logistic map. For test purpose we choose secrete image having size 64x64,host image having size 260x270.Figure 4 shows Matlab experimental result are as follows:



The performance evaluation of steganography is depending on three parameters such as embedding capacity, MSE and PSNR. Performance evaluation parameters of steganography. The parameters under which the performance of the Steganography Techniques is obtained are as follows,

Embedding Capacity

It is the maximum size of the secret data that can be embed in cover image without deteriorating the integrity of the cover image. It can be represented in bytes or Bit per Pixel (bpp).

***Mean Square Error (MSE*)**

It is defined as the square of error between cover image and stego-image. The distortion in the image can be measured using MSE and is calculated using following equation.

$$MSE=\Sigma \left([f(i,j) - F(i,j)] \right)^2 / N^2$$

In this equation, cover image f (i, j) that contains N by N pixels and a reconstructed or stego image F (i, j) where F is reconstructed by decoding the encoded version of f (i, j). The root means squared error (RMSE) is the square root of MSE. Some formulations use N rather N^2 in the denominator for MSE.

$$RMSE= SQRT (MSE)$$

Peak Signal Noise Ratio (PSNR)

It is defined as the ratio of peak square value of pixels by MSE. It is expressed in decibel. it measures the statistical difference between the cover and stego image, is calculated using following Equation.

$$PSNR=10\log10 (255/RMSE)$$

Cover image	Secrete image	Number of bytes Embedded	PSNR	MSE
Lena.bmp	Baby.bmp	4096	35.61	7.21e+02
Lady.bmp	Modi.bmp	16384	37.73	9.43e+03

Table 1. Result of Performance parameter

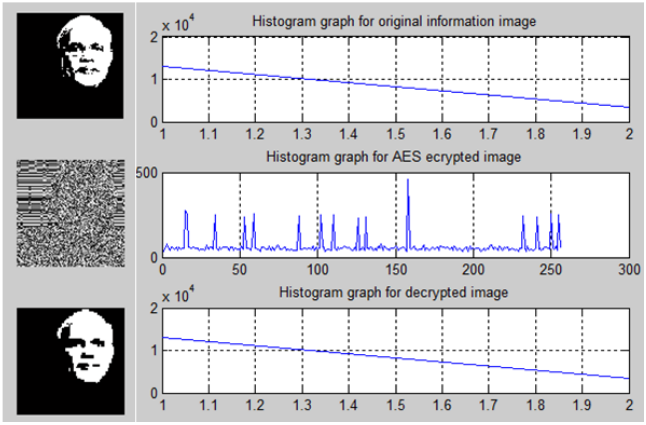
VI. Security Analysis

As we know, a good encryption scheme should resist all kinds of known attacks, such as statistical attack, plaintext attack, ciphers text-only attack differential attack and various brute-force attacks. We used the following quantitative measures to evaluate the security of the proposed image encryption scheme.

A. Visual test by using Histogram analysis

Histogram analysis is employed to illustrate its original secrete image recover decrypted secrete image. The histogram of the original secrete mage, encrypted secrete image and decrypted image is shown in Figures as follows.
Comparing the three histograms, we find that histogram of encrypted image is fairly uniform and is significantly different from that of the original image, and that the encrypted images transmitted do not provide any suspicion to the attacker, which can strongly resist statistical attacks. Also recovered decrypted image is having histogram is same as original secrete image.

ISSN: 2278 – 7798



B. *Information Entropy*

It is well known that the entropy H of symbol source S can be calculated as:

$$H(s) = \sum_{i=0}^{255} P(s_i) \log_2 \frac{1}{P(s_i)}$$

Where p (si) represents the probability of symbol si. Information entropy of image can show the distribution of gray scale value. The more the distribution of gray scale value is uniform, the greater the image has information entropy, vise verse. Generally speaking, the gray scale values do not distribute uniformly for an image and their information entropy is small. Therefore, if the information entropy of encrypted image becomes larger, image distribution of gray scale value will be more uniform, which make attackers cannot obtain much image information by entropy analysis. By calculations, the information entropy of encrypted image is equal to 7.9993, which means that information leakage in the encrypted process is negligible and the encryption system is secure from the entropy attack.

C. *Measurement of encryption quality*

Image encryption quality measure is a figure of merit used for the evaluation of image encryption techniques. With the application of encryption to an image a change takes place in pixels values as compared to those values before encryption. Such change may be irregular. This means that the higher the change in pixels values, the more effective will be the image encryption and hence the encryption quality. So the encryption quality may be expressed in terms of the total changes in pixels values between the original image and the encrypted one. A measure for encryption quality may be expressed as the deviation between the original and encrypted image .The quality of image encryption may be determined as follows:

Let P and C denote the original image and the encrypted image respectively, each of size H×W pixels with L grey levels.

The encryption quality represents the average number of changes to each grey level *L* and it can be expressed mathematically as:

$$Encryption\ \ Quality = \frac{\sum_{L=0}^{255} |H_L(C) - H_L(P)|}{256}.$$

We will define HL (P) as the number of occurrence for each grey level L in the original image (plain-image), and HL(C) as the number of occurrence for each grey level L in the encrypted image (cipher-image).

The encryption quality test was performed using the input image of size 64x64. The encryption quality of the proposed scheme is 63.999.

VII. Conclusion

In this paper, we have introduced secure data hiding using encrypted secrete image. Security is very important for efficient communications. Cryptography and steganography are two methods use for of data security. In this proposed system cryptography and steganography methods are combined to give better Security to secret data. In proposed scheme secret message is encrypted before hiding it into the cover image which gives high security to secret data. Advanced encryption standard (AES) is used to encrypt secret image and 1D logistic map is use to hide encrypted secret message into host image. The present study is designed to combine the features of both cryptography and steganography, which will provide a higher level of security. The main advantage of this System is that, the method used for encryption is AES, it is very secure and the 1D logistic map is use for Steganography techniques are very hard to detect

Acknowledgment

It gives me immense pleasure to express my sincere thanks with deep sense of gratitude to *Prof. Vijaykumar V. Patil Asst. Professor in Department of Electronics Engineering*, for his valuable guidance, encouragement and keen personal interest during the course of this project work, I thank him hearty for his unstinting co-operation and guidance.

REFERENCES

[1] Domenici Daniele Blois , Luca Iocchi, Image based Steganography and cryptography, Computer Vision theory and applications volume 1 , pp. 127-134 .
[2] Kharrazi, M., Sencar, H. T., and Memon, N. (2004). Image Steganography: Concepts and practice. In WSPC Lecture Notes Series.
[3] Christof Paar, Jan Pelzl, "The Advanced Encryption Standard" Textbook for Students and Practitioners.
[4] Chung-Ming Wang Iuon-Chang Lin, Yang- Bin Lin. "Hiding data in spatial domain image". Computer Standards Interfaces, May 2008.
[5] Kevin Curran Paul McKevitt Abbas Cheddad, Joan Condell. "Digital image steganography :survey and analysis of current methods". Signal Processing, August 2009.
[6] Wen-Jan Chen, Chin-Chen Chang, T. Hoang Ngan Le. "High payload steganography mechanism using hybrid edge detector". Expert systems with applications 2009.
[7] Nien-Lin Hsueh Ching-Chiuan Lin. "A lossless data hiding scheme based on three-pixel block differences". Pattern Recognition 41 (2008) 1415_1425, September 2007.
[8] Josef, Scharinger, "Fast encryption of image data using chaotic Kolmogorov flows," in Proceedings of Electronic Imaging, pp.278-289,1997.
[9] Ioannis Pitas Aidan Mooney, John G. Keating."A comparative study of chaotic and white noise signals in digital watermarking". Chaos, Solutions and Fractals 35 (2008) 913_921, May 2006.
[10] Chen Shi Gang, Maps and Chaos, National Defence Industry Publishing House, 1989.
[11] Hao Bai-lin,. Starting With Parabolas---- An Introduction to Chaotic Dynamics, Shanghai Scientific and Technological Education Publishing House, 1993.
[12] Wei-mou ZHANG and Bai-lin HAO, Applied Symbolic Dynamics, Shanghai ' Scientific and Technological Education Publishing House, 1993.

ISSN: 2278 – 7798

BIOGRAPHY

Mrs. Nilam C.Patil received her B.E. Electronic Engineering from Dr. D.Y.Patil College of Engineering, Kolhapur, Maharashtra, INDIA in 2009 and pursuing M.E. in Electronics & Telecommunication from KIT's College of Engineering, Kolhapur in the year of 2013-2015. Her Interested areas include Image processing and network security.

Mr. Vijaykumar V. Patil obtained M.E. in Electronics Engineering from Shivaji University, Kolhapur. Currently he is working as Assistant Professor in KIT's College of Engineering, Kolhapur since more than 10 years. He presented many research papers in various national and international journals and conferences. His Interested areas include Image processing and Cryptography.

ISSN: 2278 – 7798