IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SECURE DATA HIDING USING ENCRYPTED SECRETE IMAGE

Mrs. Nilam C.Patil [*], Mr.Vijaykumar V.Patil

[*] *PG student (E&TC), KIT's College of Engineering,*Assistant Professor (E&TC), KIT's College of Engineering,Kolhapur (MAH.) [INDIA].*

ABSTRACT

Steganography and Cryptography are two popular methods to sending information in a secrete way. Steganogaphy is use to hide secrete message and Cryptography is use to encrypt the message before sending. In this paper, we present a secure data hiding using encrypted secrete image. First, secrete image encrypted using AES algorithm. Then, encrypted image hide into host image using chaotic map. This method based on the use of AES and chaotic map. So our approach to increase the security of the embedding and extracting scheme.

KEYWORDS: Steganography, Cryptography, Chaotic map, AES, Data Hiding.

INTRODUCTION

With the rapid development of internet and communication technology, protect transmitted information becomes an important issue. To solve these problems cryptography and steganography methods are use to provide security and confidentially of secrete data [1]. The main features of a steganography system are to hide confidential information in a digital host file. It aims not only to protect the secrecy of a message but also to make it undetectable.

In this paper, we focus on one particular aspect of security, which is the transmission of hidden secrete image in a host file. This area is very broad and Multiple solutions have been designed and implemented for several decades, based mainly on cryptography and steganography [2]. The rest of this paper is organized as follows: The Literature review of steganography and cryptography are discussed in section2. The proposed method is presented in section3. Experimental analysis and discussion is given in section 4. Finally, conclusion will be presented in section 5.

MATERIALS AND METHODS

Steganography

Steganography is the art of hiding information in such a way that hidden message in host is undetectable. In Greek, 'stego' means 'covered' or 'secret' and 'graphy' means to 'write' and therefore, steganography becomes "covered or secret writing". The information to be hidden is embedded into the cover object which can be a text matter, some image, or some audio /video file in such a way that the very existence of the message is undetected by maintaining the appearance of the resulted object exactly same as the original. The main goal of steganography is to hide the fact that the message is present in the transmission medium.

Cryptography

Cryptography scrambles a message so it cannot be understood. Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data

Comparison of Steganography and Cryptography

Steganography and cryptography are closely related. Cryptography scrambles messages so it can't be understood. Steganography on the other hand, hide the message so there is no knowledge of the existence of the message. With cryptography, comparison is made between portions of the plaintext and portions of the cipher text. In steganography, comparisons may be made between the host image and cover image. The end result in cryptography is the cipher text, while the end result in steganography is the cover image. The message in steganography may or may not be encrypted. If it is encrypted, then a cryptanalysis technique is applied to extract the message.

Combination of Steganography and Cryptography

To provide more security in private communication can combine Encryption and steganography. Encrypted data is more difficult to understand. There are several tools by which we can encrypt data before hiding it in the chosen medium. In some situations, sending an encrypted message will across Suspicion while an invisible message will not do so. Both methods can be combined to produce better protection of the message. In case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques.

PROPOSED METHOD

Steganography and cryptography are two different methods. One hides the existence of the message and the other distorts the message itself.

There are many cryptography techniques available such as AES, DES and RSA among them AES is one of the most powerful techniques.[3].In Steganography we have various techniques in different domains like spatial domain, frequency domain etc. to hide the message. For instance, inserting data in spatial domain relatively simple in frequency domain [4].

AES algorithm for Cryptography

This standard specifies the Rijndael algorithm [5], a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. The input, the output and the cipher key for Rijndael are each bit sequences containing 128, 192 or 256 bits with the constraint that the input and output sequences have the same length. In general the length of the input and output sequences can be any of the three allowed values but for the Advanced Encryption Standard (AES) the only length allowed is 128[6].

Advantages of using AES algorithm

1. AES is more secure.
2. Reasonable Cost.
3. AES having high efficiency.
4. AES support larger key size.
5. Simplicity in design.

Chaos based Steganography

Chaos is a phenomenon related to non linear dynamic system [7,8]. The chaos is characterized by many properties as ergodicity, sensitivity to initial conditions and parameters, random appearance. These properties make chaotic system a favorable candidate for their use in secure application as data hiding. Chaos can be applied in security scheme to choose pixel that can be modified according to method of insertion. There are many maps are use to exhibit chaotic behavior such as Tent map, Gauss map, Logistic map….. [8].Logistic map is one of the simplest forms of a chaotic process.

One-Dimensional Chaotic maps

Logistic map is one dimensional chaotic map. Logistic map is a sort of dynamical system that is very simple and extensively studied. It is defined as follows,

$$\mathbf{x}_{n+1} = \mathbf{\mu x}_{n} \ (\mathbf{1- x}_{n})$$

Here, $0 \leq \mu \leq 4$ x_n ϵ (0,1There into,O P 5 4 is named bihrcate parameter and x E (0,l) . Definition is idem.

Research on chaotic dynamical system shows that Logistic maps stand in chaotic state when 3.5699456< PI4. That is to say, sequence { x ,n=0,1,2,3;..} generated by Logistic maps with initial conditions xg is nonperiodic and nonconvergent. It has extreme sensitive dependency to initial conditions XO.[9]

Secure data hiding using encrypted secrete image design by us.

The main aim of this paper is to introduce a secure communication system that employs both cryptography and steganography to encrypt and embed the secret message to be transmitted. In this system, the encryption process is achieved using AES, which presents a high speed and high level of security. The embedding process is achieved using chaos based steganography. The proposed system consists of four stages as shown in Figure 1 and 2. Note that the main stages are encryption, embedding, extraction and decryption. The following algorithm describes these stages.

Algorithm steps,

Step1: Secrete image is encrypted using AES.

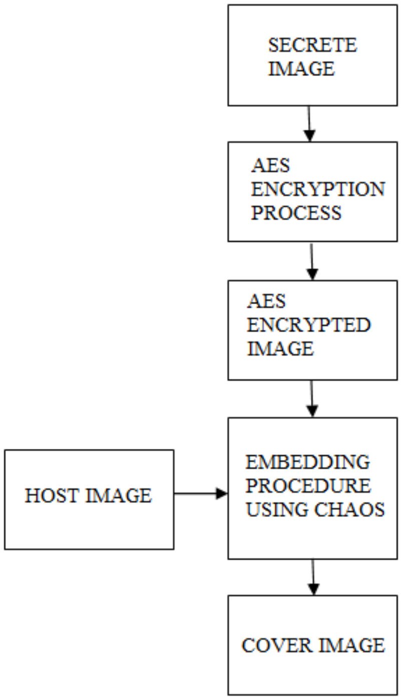
Step2: Implement embedding procedure using chaos based logistic map.

Step3: Implement extraction procedure using chaos based logistic map.

Step4: Decrypt extraction image using AES.

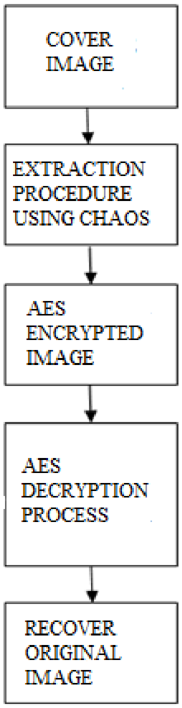
Step5: Recover secret image.

Figure 1:



Proposed block diagram of Embedding Procedure

Figure 2:



Proposed block diagram of Extracting Procedure

EXPERIMENTAL RESULTS AND DISCUSSIONS

To evaluate the performance of the proposed system in this paper, two host images such as Cameraman, Lena, Peppers and Baboon are use. Here, embed a secrete encrypted image. In this paper, the image is firstly encrypted, after that it is hidden in host image. Then, the hidden image is extracted and then decrypted. This represents a hybrid system that combines cryptographic and steganographic algorithms together to improve the security of the information. This combination is tested using PSNR and MSE analysis.

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.

$$\mathbf{MSE=\Sigma\ (\ [f\ (i,\ j)\ -\ F\ (i,\ j)]\ )^2\ /\ N^2}$$

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 mean 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):

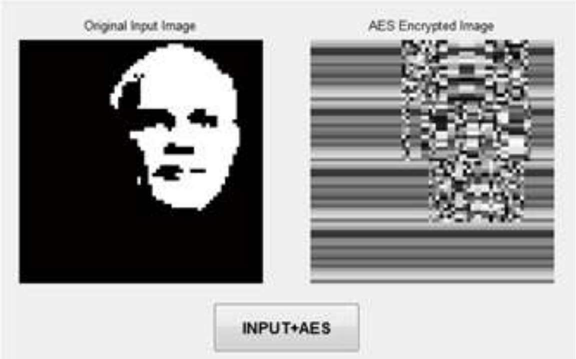
It is defined as the ratio of peak square value of pixels by MSE. It is expressed in decibel. it measures the statistical difference between the cover and stego-image, is calculated using following Equation.

PSNR=10log10 (255/RMSE).

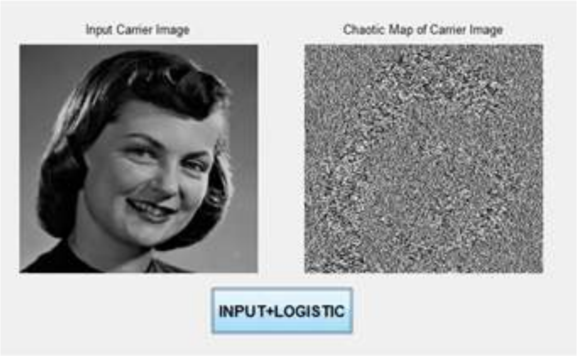
In the proposed method secrete image is encrypted using AES as follows.

In the proposed system secrete image is encrypted using AES, then apply 1D logistic map on host image after that embedding procedure is performing by using chaos method. The experimental result is as shown in figures 3and 4

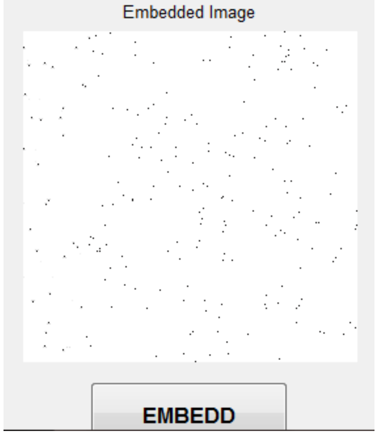
Figure 3:



a. Secret image encrypted using AES

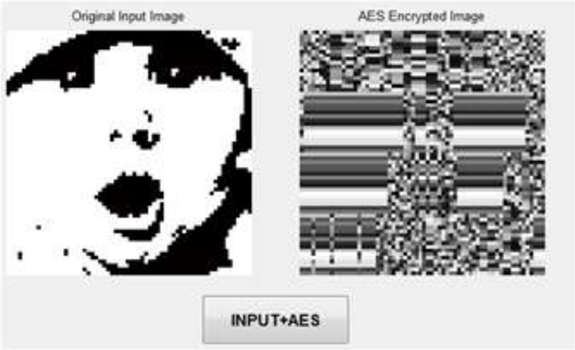


b. 1D logistic map apply on host image

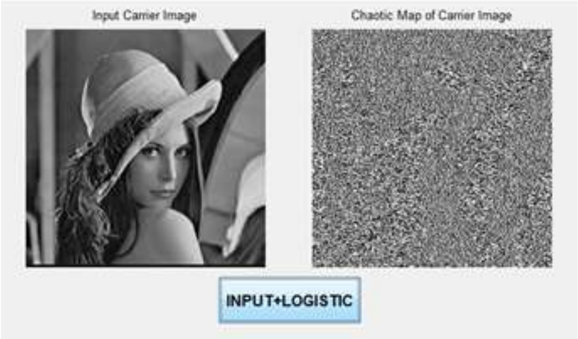


c. Embedding procedure

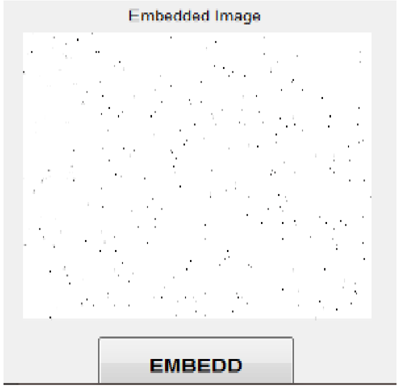
Figure 3:



a. Secret image encrypted using AES



b. 1D logistic map apply on host image



c. Embedding procedure

Table 1. the results of steganography performance parameter

Cover image	Secrete image	Number of bytes embedded	PSNR	MSE
Lena.bmp (256x256)	Baby.bmp (64x64)	4096	13.134	3.744
Lady.bmp (510x510)	Modi.bmp (128x128)	16384	11.345	3.084

ADVANTAGES OF PROPOSED METHOD

1. Cryptography and steganography are combined in order to increase the strength of the algorithm.
2. The proposed solution is highly secure because of it's a combination of two highly secured techniques such as
   a. AES is use for cryptography
   b. 1D logistic map use for manipulation for Steganography.
3. Simple, short, and effective private key used to extract the secret message.

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 Crypto/Stegno 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.

ACKNOWLEDGEMENTS

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 heartly 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-MingWang Iuon-Chang Lin, Yang-Bin Lin. "Hiding data in spatial domain image". Computer Standards Interfaces, May 2008.
5. National Institute of Standards and Technology, Advanced Encryption Standard, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 26 November 2001.
6. Ioannis Pitas Aidan Mooney, John G. Keating."A comparative studyof chaotic and white noise signals in digital watermarking". Chaos, Solutions and Fractals 35 (2008) 913_921, May 2006.
7. Kevin Curran Paul McKevitt Abbas Cheddad, Joan Condell. "Digital image steganography :survey and analysis of current methods". Signal Processing, August 2009.
8. Wen-Jan Chen, Chin-Chen Chang, T. Hoang Ngan Le. "High payload steganography mechanism using hybrid edge detector". Expert systems with applications 2009.
9. Josef, Scharinger, "Fast encryption of image data using chaotic Kolmogorov flows," in Proceedings of Electronic Imaging, 1997, pp.278-289.