SECURE COMMUNICATION USING SECRET KEY STEGANOGRAPHY

Madhusudhan Mishra[1], Gangadhar Tiwari[2] and Arun Kumar Yadav[3]
[1]Department of Electronics and Communication Engineering, NERIST, Itanagar (A.P.), India
[2]Department of Information Technology, NIT Durgapur (W.B.), India
[3]Department of Computer Science and Engineering, M.G.I.M.T., Lucknow, India

ABSTRACT
This paper proposes a novel steganographic technique for secure data communication by combining Secret Key cryptography with Digital Image steganography. At the sender's end, the proposed scheme first encrypts the secret messages using Advanced Encryption Standard algorithm (AES), then embeds it into randomly chosen least significant bits (LSB) of the cover image using stego key. At the recipient's end, first the secret message is extracted using stego key then decrypted using cipher key. The cipher key for message encryption is 256 bits long. The random distribution of message bits inside the cover image makes steganalysis harder. The location of image pixel values for embedding/extracting the encrypted secret message is determined by random numbers generated using Discrete Logarithm Calculation Technique. Simulation results indicate that the stego image is perceptually similar to cover image. The perceptual fidelity of the stego images and its robustness to various image processing distortions are measured in terms of Peak Signal to Noise Ratio (PSNR) and Mean Structural Similarity Index (MSSIM) and the results are found satisfactory. Further, the proposed scheme is secure against known cryptanalytic and steganalytic attacks.

KEYWORDS: *Secure Communication, Image Steganography, Advanced Encryption Standard, Least Significant Bit Modification, Discrete Logarithm.*

I. INTRODUCTION

Secure data transmission over communication channels has been a critical issue since the beginning of digital era. With the continuous evolution of cryptographic algorithms, data communication is made secure and private. Cryptography is a vital tool to protect information from unauthorized access by converting them into unintelligible messages. However, such message raises suspicion during transmission. Further, researchers suggest that every cryptographic algorithm can be successfully attacked. Thus the communication link is reliable till the cryptographic algorithm is unbreakable.

A secure data transmission system consists of two stages. The first stage involves encrypting the secret message and sending it from sender to receiver. The second stage comprises of receiving the encrypted message and decrypting it at receiver's end. A successful attack requires interception of encrypted message and decrypting it to extract the original message. Since a cryptographic algorithm can be successfully attacked the communication system becomes insecure. Thus there arises the need to hide the existence of the secure communication system in plain sight. This is where steganography is required. Steganography is the method of concealing hidden messages inside other digital media. It stresses on preserving the message secrecy rather than making the hidden information secure against attacks. Not only it hides the logic of secret message, but also encapsulates it into cover images. The combination of cryptography with steganography increases the security of a secure communication channel; as a successful attack would require inverting the process of data hiding and data extraction.

Thus breaching becomes harder since it requires identification of carrier that conceals the secret message before its extraction and deciphering.

Rest of the paper is organized as follows. Section 2 discusses related work. The proposed model and its block diagram are given in Section 3. Simulation results are presented in section 4. A discussion on results is presented in Section 5. This paper ends in Section 6 with conclusion.

II. RELATED WORK

In order to communicate secretly, recent researches suggest the use of Least Significant Bit Modification (LSB) Technique. LSB steganography is a commonly used method on hiding secret data inside other media formats that uses the least significant bits of visual/audio streams, replacing them with secret data. It makes use of fact that least significant bits in an image could be thought of random noise and changes to them would not affect the perceptual quality of image. In the following section we discuss some pioneer works in this area.

Tian et al proposed an image steganographic scheme based on LSB modification technique in combination with the use of simple XOR based cryptography to strengthen the system [1]. However, the proposed scheme is insecure against brute-force and signature identification attacks. Huang et al proposed LSB based audio steganographic scheme where the telephone audio stream is used as data carrier, and the secret messages are hidden into the LSBs [2]. However this scheme does not employs any cryptographic algorithms making it insecure i.e. once the covert communication is identified, using the same algorithm the data can be easily extracted. Kamran et al proposed a technique based on using Distributed LSB for Data Hiding in Images which has better hiding capacity and causes less degradation in the resulted stego image by using the lower bits to hide secret bits as per the new rule which takes into account the intensity level of each pixel [3]. The proposed algorithm is reversible as the secret data is recovered properly. In order to protect the stego image from channel induced interference, channel encoding and modulation techniques can be used. In the recovery process each pixel is inspected for its intensity value. The last three bits are extracted if a pixel belongs to the first range. This process continues till exhausting first range pixels after which the second range of pixels are found and the lower four bits are extracted. However, security is a major concern as it does not uses encryption key. Further, it assumes a communication channel to be perfect which is not possible due to noise. Castiglione et al proposed another steganographic technique where email headers are used as secret data carriers in combination with the usage of encryption algorithms and a strong password system [4]. However, this approach is limited to closed communication system. Moreover, the encryption is performed using symmetric fixed-key algorithms that reduce the strength of the security of the system. Zin et al proposed a steganographic scheme where the secret message is encrypted using RC-4 algorithm and then embedded into a bitmap file using three different methods i.e. data hiding using simple LSB, data hiding using Pseudo Random Number Generator and data hiding using scattered LSB method [5]. However, this scheme is limited to bitmap files only and the data sizes are dependent on size of cover image. Further, it is insecure against geometric attacks.

From the above analysis, it is apparent that the existing data hiding methods are insecure and unreliable for secure data communication. We propose a solution to this in the next section.

III. PROPOSED MODEL

In the proposed model, the communication system consists of two parts viz. sending and receiving. Here the sender uses three inputs for data communication, the secret message to transmit, a cover image to hold the data and the receiving party's decryption key. The decryption key consists of two parts viz. stego key for message extraction from stego image and cipher key for message decryption. Both the keys are sent to receiver using a shared secure communication channel. In the first part we discuss the AES Encryption and Decryption for message encryption and decryption and Random LSB Insertion and Embedding Technique for data hiding. We then discuss the proposed operations at sending and receiving part with block diagram below in detail.

A. AES Encryption

It is based on the block cipher Rijndael and works in a substitution-permutation network [6-8]. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. It has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. It operates on a 4×4 column-major order matrix of bytes, termed the *state* .The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext [9-10]. The proposed model employs 256 bit keys for message encryption. The algorithm for message encryption consists of following steps:
Step1. Generate the substitution tables.
Step2. Define the round constant vector and correct key.
Step3. Compute the expanded key schedule.
Step4 Create a polynomial matrix.
Step5. To generate AES cipher for plaintext, 14 round transformations is performed where each round consist of four steps viz. Substituting bytes, Shifting rows, Mixing columns, and Adding round key.
During decryption, each round comprises of four steps:
Step1. Inverting shift rows.
Step2. Inverting the substituted bytes.
Step3. Adding the round keys.
Step4. Inversing the mixed columns.
In the 3rd step, resultant of step1 and step 2 are XORed with four words from the key schedule [15].

B. Random LSB Insertion Technique using Discrete Logarithm

If I is the cover image, m is the encrypted message and k is the stego key, the stego-image I' is mathematically defined by Equation (1)

$$I' = f(I, m, k) \quad (1)$$

The simple LSB insertion technique hides the message using sequence-mapping technique in the pixels of a *cover-image* which allows steganalyst to retrieve the message due to simplicity of the algorithm [11-12]. To tackle this menace, the encrypted data is hidden in pixels of the *cover-image* generated using discrete logarithm calculation. Discrete logarithm generates random numbers without any repetition. With this set of random numbers, a random-mapping can be done [13]. Mathematically we define discrete logarithm as follows:
If a is a primitive root of the prime number p, then the numbers $a \bmod p$, $a^2 \bmod p$, …, $a^{p-1} \bmod p$ are distinct and consist of the integers from 1 through $(p - 1)$ in some permutation. Therefore, if a is the primitive root of p, then its powers $a, a^2, \ldots\ldots\ldots a^{p-1}$ are all relatively prime to p with distinct numbers. For any integer y and a primitive root a of prime number p, a unique exponent i is determined so that

$$y = a^i \bmod p \quad (2)$$

where $0 \le i \le (p - 1)$. The exponent i is referred the discrete logarithm.
The key steps of random LSB insertion technique are as follows:
Step1. Select the cover image to embed the secret message.
Step2. Select a key such that its value lies between size of message m and Image I.
Step3. Determine a prime number p, by searching for the 1st prime number greater than key, k.
Step4. Then a primitive root, a, is derived as per equation (2).
Step5. The primitive root, a, is then used to generate a set of random numbers y_i. This set of random numbers determines the position of pixel where the message bits are embedded. The discrete logarithm ensures that distinct pixel is chosen.
Step6. The message bits are inserted in the cover-image using the relation defined in equation 3:

$$M_i \rightarrow Iy_i \quad (3)$$

where M_i is the ith bit of the message, and Iy_i is the ith random number generated.
Extracting hidden message from stego image requires the corresponding decoding key, k, employed during the encoding process. This key is then used for selecting the positions of the pixel where the secret bits are hidden. For data extraction, the above algorithm is employed in reverse order.

C. Sending and Receiving

During the sending stage, the secret data is sent through an insecure communication channel. The key tasks include encryption of secret message using AES algorithm and steganographic embedding using Random LSB insertion technique [16]. Figure 1a represents the operations at sender's end. After the receipt of Stego image, the recipient first, extracts out of the encrypted message with the help of Stego Key and then decrypts it with the cipher key. Figure 1b represents the operations at recipient's end.

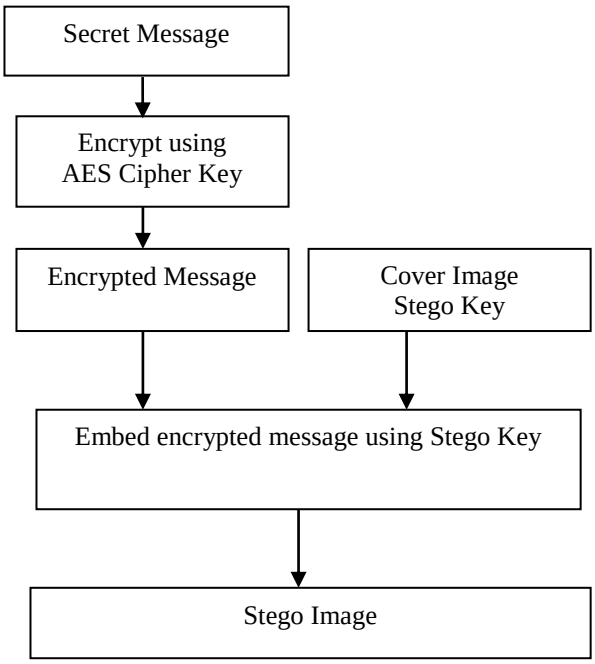

Figure1a Operations at Sender's End

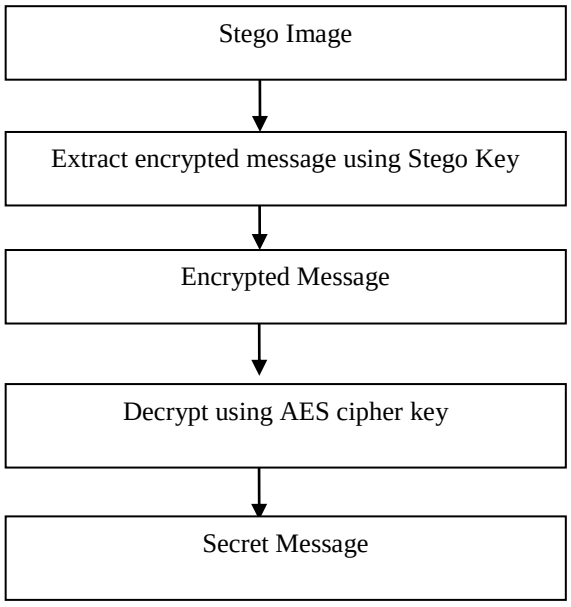

Figure 1b Operations at Receiver's End

IV. SIMULATION RESULTS

We performed simulation on Matlab R2011a, under the Windows 7 professional with dual Core CPU and 4 GB RAM. The sample images of size 512×512×3 from USC SIPI image database are used. First we measure the perceptual quality of stego images using Peak Signal to Noise Ratio (PSNR) and Mean Structural Similarity Index (MSSIM). Then these stego images were subjected to various attacks to check the robustness of the scheme and results are listed in **Table-1 and Figure-2.** From the simulation results, it is evident that this scheme meets most of the key requirements of a Secure Communication System including perceptual quality, robustness and security.

Table-1 Values of Quality Metrics under different Test Conditions

Original Image (512×512)	Stego Image		PSNR value for Attacked Images			
	PSNR (in dB)	MSSIM	Salt & Pepper Noise	Poisson Noise	Gaussian Noise	Speckle Noise
Airplane	35.80	0.9982	25.30	25.10	26.02	25.41
Cameraman	35.90	0.9976	25.16	27.53	26.63	25.37
Elaine	36.68	0.9979	25.48	25.28	26.43	25.65
Lena	35.85	0.9927	25.25	27.30	25.80	25.38
Peppers	38.63	0.9991	27.07	28.50	27.50	27.66

(a) Original Image (b) Stego Image

Figure-2

V. DISCUSSION ON RESULT

The Key aspect of this proposed model includes the following:

- Secret message is encoded by sender, but only recipient can decode it using Stego key.
- AES Encryption System with 256 bits key size is used to encrypt/decrypt the secret message. Hence the scheme is secure against cryptanalytic attacks.
- The stego images are perceptually similar to normal images and hence undistinguishable.
- Random dispersion of message bits in cover images makes harder for steganalyst to extract the original message.
- The LSB technique based steganography offers high speed data embedding and extraction and higher data hiding capacity.

VI. CONCLUSION AND FUTURE SCOPE

This paper proposes a provably secure communication system that can solve the menace of data interception and successfully thwart third party attacks during transmission over insecure digital communication links. Irrespective of cryptographic strength of the system, if an attacker intercepts the encrypted data, it can successfully extract it once the strong encryption system is successfully attacked. The proposed system employs Random LSB Technique based image steganography that provides an additional security layer by hiding the encrypted message inside cover images. The resultant stego-images are perceptually similar to cover images hence undetectable to human visual system and robust to various image processing distortions. A successful attack on such a communication system would require interception, identification, extraction, reverse engineering and decoding. Mingling cryptography with steganography creates a secure communication system, offering higher reliability when compared with respect to stand-alone cryptographic schemes. This combination offers two tier security, first using cipher key and second using stego key, thereby making the breaching near impossible.

In future work, we propose to focus on increasing the efficiency and robustness of the scheme. The research work will encompass algorithm enhancement to employ entire image for data hiding and reducing the time required for random number generation. Focus will also be laid upon its implementation in multi party communication system, its Steganalysis using current techniques, identifying those faults and eradicating them.

REFERENCES

[1] H. Tian, K. Zhou, Y. Huang, D. Feng, J. Liu,(2008), "A Covert Communication Model Based on Least Significant Bits Steganography in Voice over IP", *IEEE 9th International Conference for Young Computer Scientists*, pp. 647-652

[2] Y. Huang, B. Xiao, H. Xiao, (2008), "Implementation of Covert Communication Based on Steganography", *IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1512-1515

[3] MKamran Khan, M Naseem, IM Hussain & A Ajmal, (2011), "Distributed Least Significant Bit Technique for Data Hiding in Images", *IEEE Multi topic Conference (INMIC)*, pp. 149 – 154

[4] A. Castiglione, U. Fiore, F. Palmieri, (2011), "E-mail-based Covert Channels for Asynchronous Message Steganography", *5th IEEE International Conference on Innovative Mobile and Internet Services in Ubiquitous*

Computing, pp. 503-508
[5] Wai Wai Zin & Than Naing Soe, (2011) "Implementation and Analysis of Three Steganographic Approaches", *3rd IEEE International Conference Computer Research and Development (ICCRD),* , pp. 60-64
[6] National Institute of Standards and Technology: Specification for the Advanced Encryption Standard (AES). *http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, (2001).*
[7] V. Rijmen(2001): The block cipher Rijndael, *http://www.esat.kuleuven.ac.be/~rijmen/rijndael/, (2001).*
[8]J. Daemen, V. Rijmen, (2002), The Design of Rijndael: AES – The Advanced Encryption Standard, *Springer,*
[9] B. Schneier (1996), Applied Cryptography, *Addison-Wesley*.
[10] D. R. Stinson(2006) , Cryptography: theory and practice, *Chapman and Hall CRC*.
[11] R. Chandramouli, N. Memon, (2001), "Analysis of LSB Based Image Steganography Techniques", IEEE pp. 1019-1022
[12] R.J. Anderson, F.A.P. Petitcolas, (1998) "On the Limits of Steganography", *IEEE Journal of Selected Area in Communications*, pp. 474-481.
[13] E. Cole, R. D. Krutz, (2003), "Hiding in Plain Sight: Steganography and the Art of Covert Communication", *Wiley Publishing Inc*.
[14] M B M Amin, P S Ibrahim, PM Salleh, M R Katmin, (2003), "Steganography: Random LSB Insertion Using Discrete Logarithm", *Conference on Information Technology in Asia*, Malaysia, pp. 234-238.
[15] A. Kak, "AES: The Advanced Encryption Standard", Lecture Notes on Computer and Network Security, Purdue University, 2013
[16] SF Mare, M Vladutiu & L Prodan, (2011), "Secret data communication system using Steganography, AES and RSA", 17th IEEE International Sym. for Design and Technology in Electronic Packaging, pp 339-344

AUTHORS

Madhusudhan Mishra has completed his B.Tech in Electronics and Communication Engineering from North Eastern Regional Institute of Science and Technology, (NERIST) Nirjuli, Arunachal Pradesh in 2004 and M.Tech in Signal Processing from IIT Guwahati. He worked in Sankara Institute of Technology, Kukas, Jaipur for some years and joined NERIST as Assistant Professor in 2006. His main interest of research area includes Digital Signal and Image Processing.

Gangadhar Tiwari received his B.Sc. degree in Mathematics from Guwahati University in 2006 and his M.Sc. degree in IT from Punjab Technical University, Jalandhar in 2011. Currently, he is pursuing PhD at National Institute of Technology, Durgapur, India. His research interests include Computer Security, Digital Image and Signal Processing.

Arun Kumar Yadav completed his B.Tech degree in Computer Science and Engineering from V.B.S Purvanchal University, Jaunpur, U.P in 2006. He worked as Assistant Professor in A.I.T., Kanpur from August 2010 till 2012 and now working as Assistant Professor at M.G. Institute of Management and Technology, Lucknow, India. His research interests include Computer Security, Cryptography and Digital Image Processing.