International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)

A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.

Research Paper

Available online at: www.jrrset.com

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105

Volume 6, Issue 9
May 2018.
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395

Received on: 03.09.2018 Published on: 28.09.2018 Pages : 7 - 12

# SECURE DIRECT TRANSMISSION USING PUBLIC KEY STEGANOGRAPHY

**ReshmaChandran, R Usha Nandhini, J.R.Nishanth, J Jarin Joe Rini**

Electronics and communication engineering
Dhanalakshmi Srinivasan College of Engineering

**Abstract: -** With the spread of digital data around the world through the internet, the security of the data has raised a concern to the people. Many methods are coming up to protect the data from going into the hands of the unauthorized person. Steganography and cryptography are two different techniques for data security. The main purpose in cryptography is to make message concept unintelligible, while Steganography aims to hide secret message. Digital images are excellent carriers of hidden information. We propose a method of combining Steganography and cryptography for secret data communication. In this paper, we propose a high-performance JPEG Steganography along with a substitution encryption methodology. The approach uses the discrete cosine transform (DCT) technique which used in the frequency domain for hiding encrypted data within image. Experimental results show that the visual and the statistical values of the image with encrypted data before the insertion are similar to the values after the insertion thus reduces the chance of the confidential message being detected and enables secret communication. The effectiveness of the proposed method has been estimated by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR)**.**

**Key points: -** Steganography, Cryptography, plaintext, encryption, decryption, ciphertext, substitution cipher, discrete cosine transform, JPEG, quantization, Mean square error and Peak Signal to Noise Ratio.

## INTRODUCTION

Due to the ease in data transmission the digital communication links are widely used nowadays however, the data transmitted through these links are insecure and prone to attacks. To communicate data secretly and to preserve information privacy is hence pivotal but had received less attention of researchers in the past few decades. With the advent of cryptographic algorithms, security and privacy of data is achieved. Cryptography is a powerful tool that protects information by restricting access by changing them into unintelligible messages. However, these encrypted messages raises doubt during transmission. Further, researchers suggest that every cryptographic algorithm can be successfully attacked and has a relatively small lifecycle thus, limiting the reliability of the communication link until the cryptographic algorithm is secure.

A secret data transmission system comprises of two stages. The first stage involves encrypting the secret message and sending it from sender to receiver. In the second stage, the encrypted message is received at receiver's end and IS decrypted. Thus a successful attack involves encrypted message interception and its decryption. However, a cryptographic algorithm can be successfully attacked that makes the communication system insecure. Thus we need a mechanism to conceal the existence of the secret message

During communication in plain view. This arise the need for Steganography. It is the process of concealing secret messages inside other digital media imperceptibly and focuses on preserving the message secrecy rather than protecting it against attacks. It successfully hides secret message besides encapsulating it into cover images. The blend of Steganography with cryptography thereby ensures secret data communication; as a successful attack would involves hidden data inversion and data extraction. Thus breaching becomes harder since it requires recognition 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.

## I RELATED WORK

A vital criterion for performance measurement of a Steganography system is the statistical invisibility of the secret data. Digital Image have higher degree of redundancy and hence most suitable for Steganography. There exist many Steganography techniques that permit hiding secret data in image having their own merits and demerits. In this section we discuss some pioneer works available in literature. Least Significant Bit modification (LSB) technique is the most widely used steganographic algorithm which employs the fact that least significant bits of an image are random noise and changing them does not change the perceptual quality of the images. LSB based methods can be either LSB Replacement or LSB Matching where the former replaces the LSB of the pixels with the message to be sent while the later increment/decrement the pixels randomly with secret bits. Amin et al proposed a scheme that randomly replaces the LSBs of cover image with secret message. The pixel position of image where the message is to hidden is selected randomly using Discrete Logarithm [1]. The random distribution of message bits inside the cover images makes harder to detect and extract the original message. Kamran proposed another technique based on Distributed LSB data hiding in digital images. This method offers higher data hiding capacity and causes less degradation to the stego image as it uses lower bits to hide secret message depending upon the intensity level

of each pixel [2], In Castiglione et al method email headers were used as secret data carriers, It also employs encryption algorithms and a strong password system [3]. However, these techniques are not robust, and the secret data is lost with image manipulation and destroyed by simple attacks i.e. these schemes are not secure against visual, statistical and image processing attacks. Moreover, either these schemes do not employ cryptographic algorithms or the employed algorithms are not strong enough to thwart cryptanalytic attacks [4]. To overcome this, transform domain techniques are proposed that first transform the images and embeds the secret message in more significant parts of cover image. Thus these techniques are robust and secure against geometric and image processing attacks. Most of the techniques focus on employing redundancies in discrete cosine transforms (DCT) domain and JPEG images. In JPEG compression, the DCT transforms consecutive sub-image blocks into 64 DCT coefficients and secret message are hidden inside these coefficients' insignificant bits. The resultant stego image has no visible distortions. McKeon et al proposed a method based on 2D Discrete Fourier Transform (DFT) to generate steganography in digital videos [5]. However this scheme is unsuitable since fourier cause round off errors. Another variant names JSteg algorithm that uses JPEG images was proposed. Although the algorithm was secure against visual attacks, it is insecure against statistical attacks. It can be detected using l test. Wayner et al found that the coefficients of JPEG compression lies on bell curve and the concealed information embedded by JSteg distorts it. It is observed that data hiding in DCT level is effective provided its coefficient is chosen carefully [6, 7]. Another algorithm named Out Guess that employs pseudo random number generator to select DCT coefficients is proposed. This scheme enables random dispersion of data. However, it is not secure against statistical attack proposed by Provos et al that employs extended l test [8]. Westfield et al

Proposed to use F5 algorithm based upon subtraction, permutative straddling and matrix encoding. It hides data by decreasing the absolute value of coefficient by 1, only into non-zero AC DCT coefficients chosen randomly [9, 10]. The application of matrix encoding minimizes the changes made to message length. It offers high Steganographic capacity, fast speed and is independent of image file format and message length. Further it is secure against known visual and statistical attacks. Thus we propose to employ F5 algorithm for steganography in combination with public key cryptographic schemes. We propose our model in the next section.

## II PROPOSED MODEL

The key components of proposed communication model include sending and receiving. The sender employs three inputs for secret data communication, the message to transmit, a cover image that holds the data and the receiver's decryption key. The decryption key has two components viz. stego key for message extraction from stego image and cipher key for message decryption. The decryption key is shared with receiver through a shared secure communication channel. First, we discuss RSA algorithm for message encryption/decryption and F5 Technique for data hiding. We then propose our communication model and its block diagram. Substitutions and transpositions encryption are regarded as the building blocks of Classical cryptography technique [31]. A transposition cipher hides information by reordering the letters of the message. In a transposition cipher the plaintext remains the same, but the order of characters is shuffled around [13]. Thus the frequency analysis on the cipher text would reveal that each letter has approximately the same [11]. A substitution cipher is one in which each character in the plaintext is substituted for another character in the cipher text [13]. A substitution cipher is an encryption scheme that uses only substitution transformations. The two other techniques related with transposition and substitution for obscuring the redundancies in a plaintext message are diffusion and confusion [30]. Diffusion dissipates the redundancy of the plaintext by spreading it out over the cipher text. The simplest way to cause diffusion is through transposition. Confusion obscures the relationship between the plaintext and the cipher text.

## RSA Algorithm

Public Key Cryptography is based on the principle of one- way functions that can be easily computed while their inverse function is difficult to calculate. It employs two different keys related mathematically such that one is used for encryption and the other for decryption [11, 12]. RSA is an asymmetric algorithm based on Chinese Remainder Theorem i.e. factoring two large prime numbers [13]. The key sizes ranges from 1024 to 4096 bits and it is secure so far as per NIST [14]. In our model we propose to employ RSA algorithm with key size 1024 bits. It involves three key steps viz. Key Generation, Encryption and Decryption. During the Key Generation phase, two big distinct prime numbers (a and b) with equal bit lengthare randomly chosen and multiplied using the relation,

c=axb where c is used as the modulus for both the private and public keys. We next compute cp (c) such that rp (c) = rp(a)rp(b) = (a - 1)(b - 1), where rp is Euler's totient function. Next we randomly select an integer e satisfying the relation 1 < e < rp(c) and gcd (e, rp(c)) = 1; with e now being as public key exponent. Finally we compute the multiplicative inverse (d) of e(modulo rp(c)) such that, dJ-= e (mod rp(c)) and d now being the private key exponent. We then destroy, a and band preserve c and e as the public key and c and d as the private keys. Mathematically, if p is the plaintext message and mrepresents the cipher text then Encryption/Decryption are accomplished using (1) and (2).

$m:=pe(modc)$ (1)

$p:=md(modc)$ (2)

F5 Algorithm

If I is the cover image, m is the encrypted message and k is the stego key, the stego-image l' is mathematically defined by (3)

$1'= f(1,m,k)$ (3)

The key steps of F5 algorithm are as follows:
Step1. Perform JPEG compression till coefficient quantization.
Step2. Employ a cryptographically secure pseudo random number generator with stego key obtained from the 3, Initiate permutation using number of coefficients and random generator, Establish the parameter q from carrier medium capacity and message length such that the code word length is p = 2" - 1. Insert the message with (1, p, q) matrix encoding technique.

Load the buffer with p nonzero coefficients.
Generate a hash from q bit-places.
Perform bit by bit XOR operation on consecutive q message bits with the hash value.
The buffer is kept as it is if the sum is zero, else if the sum of buffer's index is 1 . . . n, then its element's modulus value is decremented.
Check for shrinkage. If exists, perform buffer adjustment else proceed to next coefficients behind the original buffer, Continue with step 5(a-e) till message data is not exhausted.
Complete rest of the steps of JPEG compression.
Message extraction requires the stego key used in the encoding process and is the inverse process of embedding.
C. Sending and Receiving
In this sending phase, the secret message passes through an insecure communication link to reach the recipient. The key operations at this stage involve secret message encryption by RSA public key and data hiding using F5 algorithm. We represent the sender's end operation diagrammatically using Fig.la. On the receipt of Stego image, the recipient needs to extract secret data from stego image using Stego key and decrypt it using RSA private key. The receiver’s end operations are diagrammatically represented using figure 1.

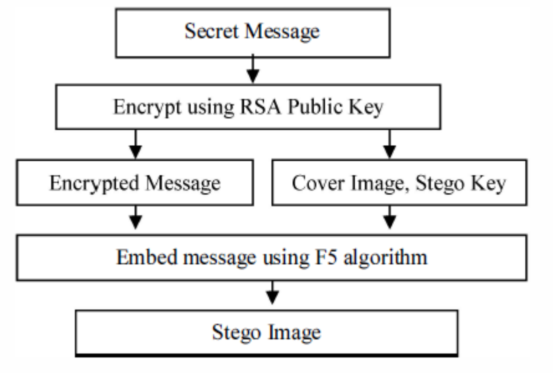


Fig 1: sender’s end operations

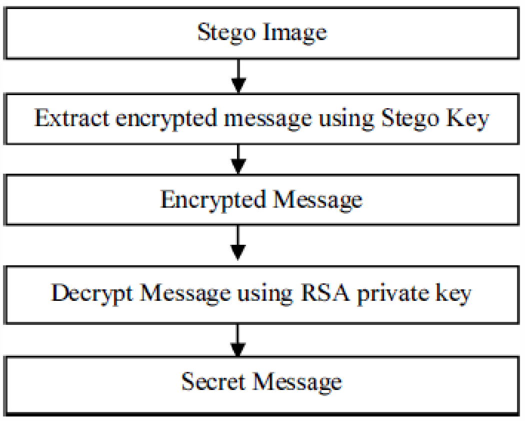

Stego Image
Extract encrypted message using Stego Key
Encrypted Message
Decrypt Message using RSA private key
Secret Message

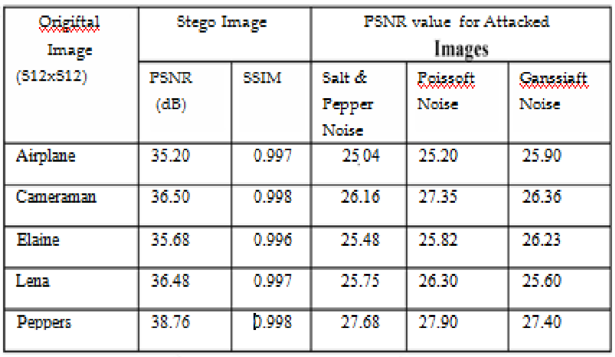
Fig 2: receiver’s end operations

## III SIMULATION RESULTS

We performed simulation on Java JDK 1. 7, under the Windows 7 professional with dual Core CPU and 4 GB RAM. The cover images of size 512x512x3 from USC SIPI image database (freely available at http://sipi.usc.edu/database) are used. Initially we measured the perceptual fidelity of stego images using Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index (MSSIM). Then these stego images were subjected to common image processing attacks to check the robustness of the scheme and the results are listed in Fig. 2 and Table-I. From the simulation results, it is clear that the proposed scheme is ideal for security, better perceptual fidelity and robustness
Secret data communication as it meets key requirements including security, better perceptual fidelity and robustness.

Fig. 2. Simulation Result on Lena

TABLE I. VALUES OF QUALITY METRICS UNDER DIFFERENT TEST CONDITIONS



| Origiftal Image (512x512) | Stego Image | | PSNR value for Attacked Images | | |
|---|---|---|---|---|---|
| | PSNR (dB) | SSIM | Salt & Pepper Noise | Poissoft Noise | Ganssiaft Noise |
| Airplane | 35.20 | 0.997 | 25.04 | 25.20 | 25.90 |
| Cameraman | 36.50 | 0.998 | 26.16 | 27.35 | 26.36 |
| Elaine | 35.68 | 0.996 | 25.48 | 25.82 | 26.23 |
| Lena | 36.48 | 0.997 | 25.75 | 26.30 | 25.60 |
| Peppers | 38.76 | þ.998 | 27.68 | 27.90 | 27.40 |

## V. DISCUSSION ON RESULT

Some vital points of the proposed model are presented below:

- Data hiding is unidirectional i.e. Secret message encoded by sender can only be decoded using Stego key by the recipient.
- RSA algorithm with 1024 bits key size is employed to encrypt/decrypt the secret message. As per National Institute of Standards Technology (NIST) USA, with the best public cryptanalysis only 768 bit key can be broken. Hence the scheme is cryptographically secure.
- Stego images are perceptually analogous to cover images and hence difficult to distinguish.
- F5 algorithm employs Password- based permutation which equalizes the change density.
- Message dispersion is more uniform compared to Key-driven and parity block schemes.

This scheme is independent of message size and carrier file format. Offers high data hiding capacity embeds more bits per change and secure against known visual and statistical attacks.

## IV CONCLUSION

This paper proposes a novel technique for secret data communication that can thwart specialized reverse engineering techniques by resolving the data interception problem. During data transmission if data is intercepted it can be successfully extracted by attacking the cryptographic algorithm. We proposed an image steganography scheme based on F5 algorithm that hides the encrypted message inside cover images imperceptibly. Breaching the communication system would involve intercepting, identifying, extracting, reverse engineering and decoding.
Thus combining cryptography with steganography offers an ideal system for secret data transmission with higher consistency with respect to stand-alone cryptographic techniques. Thus this scheme provides two tier security, first using cryptographic key and second using stego key where the secret message is encrypted before embedding and decrypted after decoding.

## V REFERENCES

[1] M B M Amin, P S Ibrahim, PM Salleh, M R Katmin ,"Steganography: Random LSB Insertion Using Discrete Logarithm", Conference on Information Technology in Asia,pp. 234-238,2003

[2] M Kamran Khan, M Naseem, 1M Hussain and A Ajmal, "Distributed Least Significant Bit Technique for Data Hiding in Images", Multitopic Conference,IEEE,pp. 149-154,2011.

[3] A Castiglione, U Fiore, F. Palmieri, "E-mail-based Covert Channels for Asynchronous Message Steganography", 5th IEEE International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing,pp. 503-508,2011

[4] S Goel, A Rana, M Kaur, "Comparison of Image Steganography Techniques", International Journal of Computers and Distributed Systems,VoU (1),2013

[5] RT McKeon,"Strange Fourier steganography in movies" Proceedings of the IEEE International Conference on ElectrolInformation Technology, pp. 178-182, 2007

[6] P Wayner, "Disappearing cryptography", 2nd ed , Morgan Kautinann Publishers,2002.

[7] N. F. Johnson,S. Katzenbeisser. "A Survey of steganographic techniques." in Information Hiding Techniques for Steganography and Digital Watermarking, pp. 43-78,2000

[8] N. Provos, "Defending against statistical steganalysis", Center for Information Technology Integration, University of Michigan, technical report,2001.

[9] A Westfeld,"F5-A steganographic algorithm: High capacity despite better steganalysis", Proceedings of 4th International Workshop on Information Hiding,USA,pp. 289-302,2001

[10] Fridrich,T. Pevny and 1 Kodovsky,"Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities", Proceedings of ACM 9th Workshop on Multimedia & Security,USA,pp. 3-14,2007.

[11] B. Schneier "Applied Cryptography",Addison-Wesley,(1996).

[12] D. R. Stinson,"Cryptography theory and practice", Chapman and Hall CRC, 2006.

[13] R. Rivest, A Shamir, L. Adelman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM,pp. 120-126,1978.