A ES
ISSN: 2096-3246
Volume 54, Issue 02, December, 2022
Special Issue

PUBLIC KEY STEGANOGRAOHY APPROACH FOR SECURE DATA TRANSMISSION

T.Joby Titus
Dhanalakshmi Srinivasan College of Engineering, Coimbatore, Tamil Nadu, INDIA

R.Arun Prasath
Dhanalakshmi Srinivasan College of Engineering, Coimbatore, Tamil Nadu, INDIA
jobyece007@gmail.com

V.K. Maurya
Babu Banarasi Das University, Lucknow (U.P.) India

Abstract: - The abundant digital data access through Internet has raised the issue of secured data transmission. The most promising methods for secured data transmission are Steganography and cryptography. In cryptography technique makes the data unintelligible and in steganography technique the secret message is hidden. The excellent carriers of hidden information is through Digital Images. In this proposed approach the steganography and cryptography technique are combined together as high-performance JPEG steganography along with a substitution encryption methodology. A discrete cosine transform (DCT) technique is used with frequency domain for hiding encrypted data within image. Based on the experimental analysis the encrypted visual and the statistical values of the image before the insertion is similar to the values after insertion and reduces the chance of the confidential message being detected and enables the secret communication. The proposed methodology analyzes the Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR) to estimate the effectiveness of proposed method.

Key points: - Steganography, Cryptography, plaintext, encryption, decryption, ciphertext, substitution cipher, discrete cosine transform, JPEG, quantization

1. 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. The secured data transmission with secured data storage involves the demanding factor for large data access. The most demanding method for data security and privacy is possible by cryptographic algorithms. This algorithmic approach protects the information by restricting access and converting into unintelligible messages. The reliability of communication link depend on the cryptography algorithm and it has relatively small lifecycle, most often the communication link is attacked and makes the data transmission insecure.

The secured way of data transmission includes two stages. In stage-1 the secret message is encrypted and send it to receiver from sender. The second stage is to decrypt the receivers end. The inefficiency in cryptographic algorithm happens at send end or at receiver end in encrypted or decrypted message. The need of steganography leads to conceal the secret message and the steganography method is the process of concealing secret messages in digital media and focuses on preserving the message

secrecy rather than protecting it against attacks. The technique of combining steganography with cryptography ensures secret data communication in which the breaching becomes harder as it require recognition of carrier that conceals the secret message before its extraction and deciphering. The rest of the paper is organized as follows. In Section 2 discusses the related work. The details of proposed model and its block diagram are in Section 3. The simulation results are presented in section 4. The analysis of results in Section 5 and section 6 concludes the proposed work.

2. RELATED WORK

The most demanding parameter for performance measurement in steganographic system is the statistical invisibility of the secret data. A greater degree of redundancy is available for digital images and hence it is most suitable for steganography. Steganography method uses different approaches for hiding the secret data and it has its own merits and demerits. Few steganographic approaches applied for data security are reviewed and directs the path for proposed methodology. One of the steganographic approach uses Least Significant Bit modification (LSB) technique. In this approach the LSB bits indicates the random noise and modifying this bit does not change the perceptual qualities of image. The LSB bit modification approach uses two techniques, LSB replacement or LSB Matching. In LSB replacement approach the secrets bits are included randomly as increment/decrement value in the message. Amin et al., proposed the technique of random replacement of LSB bit cover image with secret message. The pixel position of image where the message is to hidden is selected randomly using Discrete Algorithm [1]. It is harder to detect and extract the original message based on the random distribution of message bits inside the cover images.

Kamran, et.al. proposed a method that 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., the email headers are used as secret data carriers and employs an encryption algorithm with a strong password system [3]. In this technique due to image manipulation the secret data is lost by simple attacks and these schemes are not secure against visual, statistical and image processing attacks. Most of the techniques doesnot use either cryptographic algorithms or the algorithms are not strong enough to protect from attacks [4]. The limitations in cryptographic algorithm is overcome by transform domain techniques. In this approach the images are first transformed with secret message embedded in significant parts of cover image. These techniques are strong and secure against symmetrical and image processing attacks. The technique for secured data system choose redundancies in discrete cosine transforms (DCT) domain and JPEG images. The JPEG compression technique uses DCT to transform consecutive sub-image blocks into 64 DCT coefficients and secret message are hidden inside these coefficients' insignificant bits and results in stego image with no visible distortions. McKeon et.al. proposed a method to generate steganograpgy in digital videos using 2D Discrete Fourier Transform (DFT) and this approach suffers from fourier cause round off errors [5]. Wayner et al analyzed the coefficients of JPEG compression is indicated on bell curve and JSteg distorts the concealed information embedded by it. Based on the analysis the data hiding in DCT level is effective if the coefficient is chosen carefully [6, 7]. Our proposed approach uses an algorithmic approach with pseudo random number generator to select the DCT coefficients. This scheme enables random dispersion of data for secured data transmission. Westfield

et al proposed a method to use F5 algorithm based upon subtraction, permutative straddling and matrix encoding. It hides the data by decreasing the absolute value of coefficient by 1, only into non-zero AC DCT coefficients chosen randomly [9, 10]. The variation in message length is minimized by applying the matrix encoding scheme. This technique leads to high Steganographic capacity, fast date speed and is independent of image file format and message length. This approach is more secured 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.

3. PROPOSED MODEL

The proposed communication model includes sending and receiving data through secured data communication link. 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 uses stego key and cipher key. Message extraction is done using stego key and message decryption is done using cipher key. 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 that includes substitutions and transpositions encryption blocks of Classical cryptography technique. In transposition cipher approach the information is hidden by reordering the letters of the message. In this approach the plaintext remains the same and the characters are shuffled around. In an substitution cipher each character in the plaintext is substituted for another character in the ciphertext [13]. In this encryption scheme only substitution transformations are used. The other techniques are related with transposition and substitution method for obscuring the redundancies in a plaintext message are diffusion and confusion. Diffusion dissipates the redundancy of the plaintext by spreading it out over the ciphertext. The simplest way to cause diffusion is through transposition.

3.1 RSA Algorithm

Public Key Cryptography is referred as one- way functions that can be easily computed while their inverse function is difficult to calculate and uses two different keys for encryption and decryption. RSA is an asymmetric algorithm based on Chinese Remainder Theorem in which key is generated based on factoring two large prime numbers. The key sizes ranges from 1024 to 4096 bits. In our proposed RSA algorithm is employed with the key size 1024 bits. The algorithm uses Key Generation, Encryption and Decryption process during the Key Generation phase,

In this approach consider two big distinct prime numbers (a and b) with equal bit length randomly chosen and multiplied using the relation,

$c=axb$ ……..(1)

where c relates the modulus for both the private and public keys.

We next compute cp (c) such that

$rp(c) = rp(a)rp(b) = (a - 1)(b - 1)$…….(2)

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)) ……(3)

and d now being the private key exponent. We then destroy, a and b and preserve c and e as the public key and c and d as the private keys. Mathematically, if p is the plaintext message and m represents the cipher text then Encryption/Decryption are accomplished using (4) and (5).

m:=pe(modc) ……(4)

p:=md(modc) ……(5)

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 (6)

1'= f(1,m,k) ……(6)

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.

3.2. Sending and Receiving

The sending end operations is carried out through an insecure communication link to reach the receiver. The key operations at this stage involves secret message encryption by RSA public key and data hiding using F5 algorithm. Fig 1 and 2 represent the sending end and receiver end operations and 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.

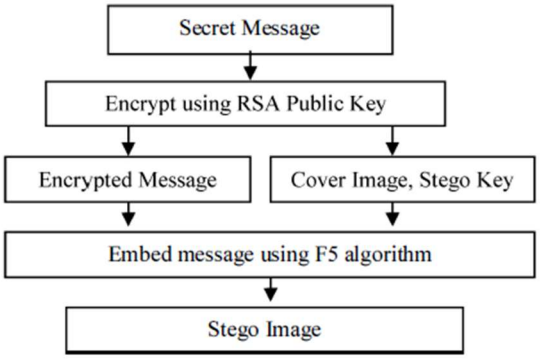

Fig 1 :sender's end operations

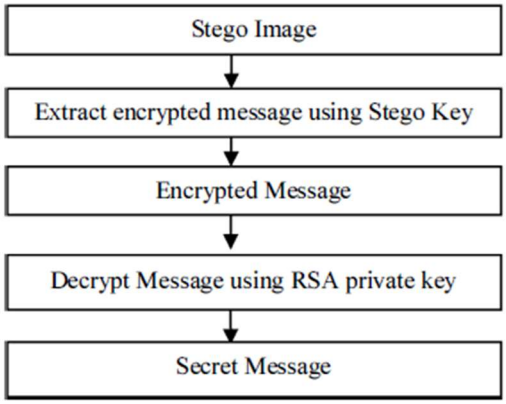

Fig 2: Receiver's end operations

4. SIMULATION RESULTS

The simulation of proposed approach is done by considering the cover images of size 512x512x3 from USC SIPI image database. The perceptual fidelity of stego images were analyzed using Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index (MSSIM). The robustness of the proposed approach is analyzed by involving the stego images to common image processing attacks and the results are listed in Fig. 3 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 meets the key requirements including security, better perceptual fidelity and robustness.

Fig 3: Simulation result of Stego Image

Table 1: Stego Image with PSNR values

Original Image(512*512)	Stego Image		PSNR value for Attacked Images		
	PSNR(dB)	SSIM	Salt &Pepper Noise	Poison Noise	Gaussian Noise
Airplane	35.20	0.996	25.03	25.20	25.90
Cameraman	36.50	0.989	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	0.998	27.68	27.90	27.40

The key features of proposed methodology is listed here :

- Data hiding is unidirectional and the receiver end with stego key can decode the Secret message.
- The proposed work uses RSA algorithm with 1024 bits key size to encrypt/decrypt the secret message. Compared with public cryptanalysis standard of National Institute of Standards Technology (NIST) USA, only 768 bit key can be broken.
- Stego images are perceptually equivalent to cover images and hence difficult to distinguish.
- F5 algorithm employs Password- based transformation which equalizes the change density.
- Compared to Key-driven and parity block schemes, message dispersion is more uniform.

This scheme provides high data hiding capacity, embeds more bits per change and is independent of message size and carrier file format and it is one of the secured system from visual and statistical attacks.

5. 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. The proposed image steganography approach using F5 algorithm imperceptibly to hide the encrypted message inside cover images. Breaching the communication system would involve intercepting, identifying, extracting, reverse engineering and decoding. The choice of cryptography with steganography provides an ideal system secured 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] R. Rivest, A Shamir, L. Adelman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM,pp. 120-126,1978.

1. [12] Alkhamese, A.Y.; Shabana, W.R.; Hanafy, I.M. Data Security in Cloud Computing Using Steganography: A Review. In Proceedings of the 2019 International Conference on Innovative Trends in Computer Engineering (ITCE), Aswan, Egypt, 2–4 February 2019.
2.
3. [13] Bolton, T.; Dargahi, T.; Belguith, S.; Al-Rakhami, M.S.; Sodhro, A.H. On the Security and Privacy Challenges of Virtual Assistants. Sensors 2021, 21, 2312