DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4472

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

DATA HIDING IN IMAGE USING CRYPTOGRAPHY AND STEGANOGRAPHY: AN INVESTIGATION

Manoj Kumar Ramaiya
Research Scholar, Computer Engineering
Suresh Gyan Vihar University
Jaipur, India

Dr. Dinesh Goyal
Director, Center for Cloud Infrastructure & Security
Principal, Engineering
Suresh Gyan Vihar University
Jaipur, India

Dr. Naveen Hemrajani
HOD Computer Engineering
JECRC University
Jaipur, India

Abstract: The aegis of data over unsecure transmission network has continually a key concern in the consideration of cyber professionals. With the expeditious promising practice of the cyber world in all personnel and professional drives, the distress for the unauthorized ingression and later exploitation by an intruder, has further put pressure on the industry or researchers for developed new methods and techniques to bulwark the information from intruders involves in cybercrime.

Cryptography is the art dealt with the converting a confidential information into inaudible forms. This unintelligible information might engender distrustful in the mind of opponents when it transfers on insecure communication media and only valid recipient can only by decoding it. Conversely, Steganography embed confidential information in to a cover image and hides its subsistence. As a mundane hiding of secrete data is apply in communication on text, image or multimedia contents digital signature and authentication.

Mutually Cryptographic and Steganographic methods distributes the satisfactory security but are vulnerable to attackers when information flow over insecure communication media. Efforts to amalgamate these techniques i.e. Steganography and Cryptography, gives the ultimate results in security improvement. The steganographic techniques currently used mainly accentuation on embedding mechanism with less consideration to pre-processing of confidential information. The advantage of pre-processing offer robustness, high security level and flexibility in the safety system

Keywords: Cryptography, DES, Multiple Encryption, Digital Image Steganography, Discrete Wavelet Transforms.

I. INTRODUCTION

From the ancient age protection of secret information during transmitting it to legitimate receiver at a remote place has been in the main considerations of despatchers. So very rudimentary to modern day extremely precise computer based techniques have been established. The former three to four decade led to the widespread transfer of information across the world. The extraordinary development of the internet also produce and eased various E-Commerce applications, this demand the guarantee of safe keeping of data and any further misuse possible from this theft data. Further the communication between private parties authoritatively mandating unconditional secrecy additionally demand the data transmission in amended or encoded mode.

In multimedia communication the requisite of secrecy and confidentiality increases adscititious paramountcy primarily in unsafe communication network like World Wide Web. Current age of ecumenical connectivity, of viruses, intruders, eavesdropping and digital fraud or cyber-crime needs to safe - sentinel information from releasing into criminal hand.

Cryptographic systems [1] converts confidential information in to unintelligible form so it cannot be recognize by intruders , while steganographic system hides the secret information in to other digital media, so it cannot be apparent before the opponents. The word steganography [2] derived from the Greek word *Steganos* which means *"covered"* and *Grafia* means *"writing"* i.e. Steganography means *"covered writing"* [3] . The secret information embed in to other media like cover image in such a way that the resulting stego image should not deviate much from cover image. Cryptographic and Steganographic methods are extensively used in the field of information hiding and has accredited consideration from the commercial and academic society in the past.

II. RELATED WORKS

Considering the strengths and impotency of cryptographic and steganographic, investigators endeavored to merging them, so that the incipient techniques would concurrently retain the strength of steganography and cryptography while surmounting the respective deficiencies

The literature surveyed deal with methods involving only cryptographic methods or steganographic systems. Both of the methods have scarcity in terms of safety and robustness against attacks. Effort to merging two methods to guarantee more secure encoding method will be made. In the most of the cases, methods involved works on plaintext and very fewer attempts been made to encode images.

Mostly recommended methods in literature survey involves cryptographic and steganographic can be classified into five major classes, four class's associated with special domain while fifth one is related to the transform domain. These classes are as briefly describe as below:

1. Idea using the two systems is often, Shouchao Song et al. [4] proposed an algorithm by hybridization of cryptographic and steganographic methods based on Least Significant Bit toning method. The algorithm attains the encryption and embedding in single stage which take less computation time as compare to existing methods. Another systems explain by Malik and Singh [5] encrypting the text using blowfish encryption algorithm and LSB technique of steganography which is non readable and secure further enhance the security.

2. Encryption of text using DES and data hiding using Least Significant Bit insertion, Seth Dhawal et al. [6] guarantee more security over unsafe and open communication channel by hybridization of cryptographic and steganographic methods, they suggest the DES cryptographic algorithm used for text encryption and for embedding encrypted message in the cover image LSB substitution is used.

3. The techniques recommends compacting the signal before encrypting and employing steganographic techniques. Hikmat Farhat and Khalil Challita [7] offered multiple encryption. After Encryption the encrypted text secret message is embedding multiple cover images.

4. Ankit Uppal et al. [8] presented a new method by merging the RC5 enhance algorithm for encrypting the text message and Least Significant Bit method for embedding results a highly secure communication method.

5. Dipti Kapoor Sarmah and Neha Bajpai[9] suggested an techniques by incorporating AES encryption for secrete message. The resultant ciphertext is then embedded into the cover image by using Discrete Cosine Transform. The little modified techniques is offered by Pye Pye Aung and Tun Min Naing [10], using the same AES algorithm for encryption and this encrypted message is hide into cover image using DCT.

Literature discloses that a lot of research applying the idea of joining cryptographic and steganographic technique by first encrypting the secret information and then hiding it in the digital media are suggested. But they do the encryption and embedding is achieved independently and no study employing them concurrently have never been tried up until now.

Secondly most of the hybrid system uses cryptographic system to encrypt text message and hide the ciphertext by LSB steganography. To our information no techniques proposed cryptography for encrypting image (image encryption). Proposed system uses cryptographic techniques for encrypting secrete message i.e. image and then hiding this encrypted image is hide in to cover image by using LSB embedding.

III. DES (DATA ENCRYPTION STANDARD) AND MULTIPLE ENCRYPTION

The DES Algorithm [11, 12] is intended to encryption and decryption blocks of data containing of 64 bits by using a 56-bit key. Decryption of block must be carried out using the identical key as used for encryption process, but ordered of using the key is reverse because the decryption method is the inverse of the encryption method.

A block which is enciphered is inputted to an *IP* (initial permutation), then to special function based on permutation and substitution (*F*) and finally to an IP^{-1} (reverse initial permutation). The key based calculation termed as function *F*, also called the cipher function. The function K_S is called the key schedule. Finally, a definition of the cipher function f is given in terms of primitive functions which are called the selection functions S_i and the permutation function *P*.

A. Initial / Inverse Initial permutation

The 64 – bit passes through an initial permutation (*IP*) that reorders the bits to yield the 64 bit permutated output that input to stage comprising 16 round of same special function (f_k). The output of the sixteenth round will now inputting to reverse initial permutation (IP^{-1}) by which the original ordering of the bits is restored.

B. The function f

The complex module of DES is function *f* which comprises of a combination of substitution and permutation functions.

$$L_i = R_{i-1},$$

$$R_i = L_{i-1} \text{ XOR } F(R_{i-1}, K_i)$$

Where *L* and *R* are the leftmost 32- bit and rightmost 32-bit of the 64 - bit first block of the eight consecutive pixel of the secrete image. The 32 bits of *R* input expanded to 32 to 48 bits by applying expansion and permutation. Expansion is carried out involving repetition of rightmost 16 bits. The resultant 48 bits are XORed with K_i. This 48 – bits output inputted to substitution function (S-Box) produce a 32 – bit output, which is again permuted to produce 32 – bit.

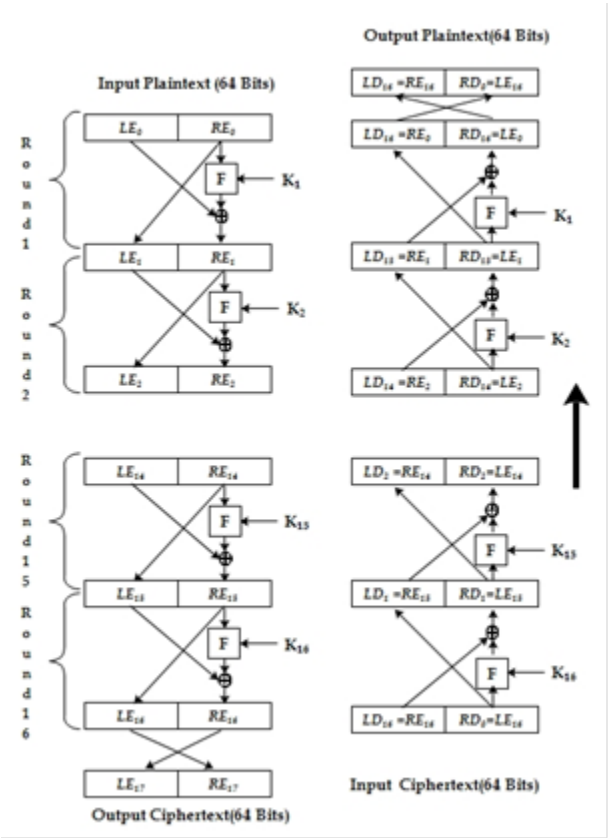

Figure 1. DES Structure

C. S- box Operation

Substitution operation comprises of set of eight S-Boxes, each of which accept 6 bits as input and give 4 bit as output. first and last bits of input to box S_i form a two bit binary number to select one of four substitution defined by four row in the table for S_i . The middle four bit select one of sixteen columns from 4*16 definition table of DES S-boxes. The S – Box definition table contain only decimal value from 0 to 15 hence binary output of substitution operation contain only 4 bit.

The 32 bit output from the eight S boxes is then permuted and XOR with leftmost (*L*) 32 bits is now input as 32 bits *R* for

next round. One complete execution of DES gives eight pixel value of secrete image into respective pixel values of encrypted secrete image.

DES given the possible susceptibility to brute-force attack, there has been significant attention in finding an alternate to DES. One approach is to finding completely new algorithm and AES is example of that. Other alternative to use existing DES with multiple encryption and multiple keys. The initial standard that describes algorithm ANS X9.52 available in 1998 is "Triple Data Encryption Algorithm (TDEA)". FIPS PUB 46-3 also describe 3-DES.

Triple DES uses a key package that contain of three keys. K_1, K_2 and K_3 all of having 56 bits. These keys are applying in three different variant. The encryption of plaintext takes places as:

$$Ciphertext = EK_3\,(DK_2\,(EK_1\,(\,Plaintext)\,)\,)$$

Means DES first encrypt with K_1 , secondly DES decrypt with K_2 and then DES encrypt with $K3$. The plaintext will be recovered by decrypt with K_3 , encrypt with K_2 then decrypt with K_1.

$$Plaintext = DK_1\,(EK_2\,(DK_3\,(\,Ciphertext)\,)\,)$$

Each triple Des encryption encrypt one block of 64 bits of data. The TDEA offer three different variants with respect to keys.

- All three Keys are independent
- K_1 and K_2 are independents and $K_3 = K_1$.
- All three keys are equal i.e. $K_1=K_2=K_3$.

Triple DES is advantageous because it has significant sizes key length, which is longer than most key length associated with other encryption methods, i.e. 3×56=168 independent key bits ensuing in a dramatic increase in cryptographic strength and obvious to the meet-in-the-middle attack.

IV. SUMMARY OF SHORTCOMINGS OF BOTH THE SYSTEM

1. The Cryptographic techniques are mainly applied on the text message and are secure. However rare attempt has been made to encrypt images.

2. The Steganography is rather very simple are predictable and thus not very secure. The techniques is being used primarily for hiding data.

3. These Cryptographic and Steganographic techniques are well developed for communicating data over non secure transmission channel independently. They do provide security to a fair level but are inadequate for the present needs of information era or digital need.

4. All the obtainable methods of steganography concentrate on the embedding technique with less concern to the pre-processing, such as encryption of secrete image.

5. The conventional Steganographic methods does not provide the pre-processing which is required in image based steganography for better security, flexibility and robustness.

6. Rare attempt has been used to combine the two techniques few attempts have been made combining the two techniques by employing cryptographic techniques [28, 35] on text and embedding message into cover image using steganography.

V. PROPOSED SOLUTION

In order to attain the better of two techniques, combination of the two have also been tried. However they remains susceptible to the attacks and could be breached with the knowledge of algorithms and little luck. This lead to the motivation for further improving the existing techniques so that a real time implementation algorithm can be developed which is safe from the attacks and vulnerability.

By knowing the strengths and weakness of Cryptographic and Steganographic system a solution may be evolved in future using hybrid steganographic model based on multiple encryption of secrete image using 3- DES (triple Data Encryption Standard) and Discrete Wavelet Transforms to solve the problem.. The suggested system may overcome the shortcoming and retain strengths of both techniques.

VI. CONCLUSION AND ANALYSIS

Proposed model shall be strong Steganography method because it possess strength of both steganography and cryptography and without knowing the secrete keys package the recovery of secrete image with the help of stego image is impossible. Furthermore cover image quality is also not be degraded due to deviation in two LSB of each pixel which replicates only 0 – 3 difference in pixel value.

In the proposed solution 3-DES and DWT based hybrid steganographic model may be designed over the strength of conventional DES and bundle of secrete key for encrypting secrete image, improves quality of image and security compare to existing systems. Steganography, especially combined with the cryptography is a powerful tool which enables to communicate safely with the little computational overload in the system.

VII. ACKNOWLEDGMENT

The principal author acknowledgment is due to Dr. Dinesh Goyal, Director, Center for Cloud Infrastructure & Security, Principal, Engineering, Suresh Gyan Vihar University, Jaipur, India and Dr. Naveen Hemrajani, Head , Computer Engineering, JECRC University, Jaipur (India) for the valuable guidance, encouragement and blessing to carry the research.

VIII. REFERENCES

[1] N. Provos and P. Honeyman, "Hide and Seek: an Introduction to Steganography", IEEE Security and Privacy Vol 1 No. 3, pp.32–44, 2003.

[2] Ross J. Anderson and Fabien A.P. Petitcolas, "On The Limits of Steganography", IEEE Journal of Selected Areas in Communications, Vol. 16 No. 4,pp 474-481, May 1998.

[3] J.C.Judge, "Steganography: past, present, future", SANS Institute publication, /http://www.sans.org/reading_room/whitepapers/stenganography /552.phpS, 2001.

[4] Shouchao Song, Jie Zhang, Xin Liao, Jiao Du and Qiaoyan Wen, "A Novel Secure Communication Protocol Combining Steganography and Cryptography", Advanced in Control Engineering and Information Science , Procedia Engineering 15 , pp. 2767 – 2772, 2011.

[5] Ajit Singh and Swati Malik, " Securing Data by Using Cryptography with Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 5, pp 404-409 , May 2013.

[6] Dhawal Seth, L. Ramanathan and Abhishek Pandey, "Security Enhancement: Combining Cryptography and Steganography",

International Journal of Computer Applications (0975 – 8887) Volume 9– No.11, pp. 3-6, Nov 2010.

[7] Khalil Challita and Hikmat Farhat, "Combining Steganography and Cryptography: New Directions", International Journal on New Computer Architectures and Their Applications (IJNCAA) Vol. 1 No., pp.199-208, 2011.

[8] Ankit Uppal, Rajni Sehgal, Renuka Ngapal and Aakash Gupta, "Merging Cryptography& Steganography Combination of Cryptography: Rc6 Enhanced Ciphering and Steganography: JPEG", International Journal of Advanced Computational Engineering and Networking, Vol. 2, Issue-10, pp. 85-87, Oct.-2014.

[9] Dipti Kapoor Sarmah and Neha Bajpai, "Proposed System for Data Hiding Using Cryptographyand Steganography", International Journal of Computer Applications (0975 – 8887) Volume 8– No.9, pp. 7- 10, Oct 2010.

[10] Pye Pye Aung and Tun Min Naing, " Novel Secure Combination Technique of Steganography and Cryptography", International Journal of Information Technology, Modeling and Computing (IJITMC), Vol. 2, No. 1. Pp 55-62, February 2014.

[11] William M. Daley and Raymond G. Kammer, "Data Encryption Standard (DES)", Federal Information Processing Standards Publication FIPS Pub 46-3 National Institute Of Standards And Technology, pp. 1-22, 25 October 1999.

[12] Manoj Kumar Ramaiya, Naveen Hemrajani and Anil Kishore Saxena, "Improvisation of Security aspect in Steganography applying DES ", IEEE International Conference on Communication Systems and Network Technologies (CSNT – 2013) , pp. 431 – 436, 2013.

[13] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering 4, 3: 275-290, 2006.