Suresh Gyan Vihar University, Jaipur
International Journal of Converging Technologies and Management (IJCTM)
Volume 3, Issue 1, 2017
ISSN : 2455-7528

Enhancing Security of Steganographic System using TDEA

Manoj Kumar Ramaiya[1], Dr. Dinesh Goyal[2], Dr. Naveen Hemrajani[3]

[1]Research Scholar, Computer Engineering, SGVU, Jaipur
[2]Principal, School of Engineering, SGVU, Jaipur
[3]Head Computer Engineering, JECRC University, Jaipur

Abstract: The security of data over unsafe communication network has always been a primary concern in the attention of researchers. With the rapidly growing practise of the internet in all personnel and business drives, the concern for the illegal access by an intruder and later misuse, has further put strain on the industry for developing means and techniques to overcome this.
Cryptography involves transforming a confidential data into unintelligible forms or ciphertext might produce suspicious in the mind of opponents. On the other hand, Steganography implant secrete message in to a cover media and hides its presence. As a normal practise, data embedding is employed in communication, image, text or multimedia contents for the purpose of copyright, authentication and digital signature etc. Both techniques provides the sufficient degree of security but are vulnerable to intruder's attacks when used over unsecure communication channel. Attempt to combines the two techniques i.e. Cryptography and Steganography, did results in security improvement. The existing steganographic algorithms primarily focus on embedding strategy with less consideration to pre-processing of data which offer flexibility, robustness and high security level. The proposed work presents a unique techniques for image steganography based on "Triple Data Encryption Algorithms (TDEA)" using the strength of multiple encryption enhancing the security level over unsafe communication channel.

Keywords: Image Steganography, Cryptography, LSB insertion, DES, Multiple encryption, TDEA.

I. INTRODUCTION

Keeping an information safe while communicating it to somebody at a distance has been in the attentions of individuals since the early age, so very rudimentary to present day highly specified computer based methods have been developed. The past three or four decade led to the wide spread transfer of data from one end to the other end of the world. The remarkable growth of the internet also generate and eased various E- Commerce applications. This demand the assurance of security of data and any misuse possible from this theft data. Further the communication between private parties demanding absolute privacy also necessitate the data transmission in modified or encoded mode.

In multimedia communication the necessity of privacy and confidentiality gains additional importance mainly in open, unsecure communication network like internet. Present era of universal connectivity, of viruses, intruders, eavesdropping and digital fraud need to safe-guard information from releasing into erroneous hand.

Cryptography techniques [6,7] scramble a source message in to unintelligible form so it cannot be understood while steganography hides the message in to other media, so it cannot be perceived. The term steganography [2,4] derives from the Greek *Steganos* which means "covered" and *Grafia* means "writing" i.e. Steganography means "covered writing " [5] . Thus the stego image should not differ much from cover image.
Cryptography and Steganography are extensively used in the field of information hiding [1] and has received attention from the businesses and academic world in the past. Former conceals the original data but latter conceal the very fact that data is hidden.

II. RELATED WORKS

There are large number of steganographic techniques proposed in literature. Image steganography is a method for hiding information into a cover image. Least Significant-Bit (LSB) based methods [22] is common steganographic practise in spatial domain due to its easiness and hiding capacity. All the obtainable methods of steganography concentrate on the embedding method with less concern to the pre-processing, such as encryption of secrete image.
More recently, researcher's hides [5] secret messages in image by replacing the least significant bit of each byte of the image pixel with the bits of the message. The original image is not significantly changed. Most image format identify more shades of colour than the human eye can notice. The message is successfully be extracted this at the receiver end. Steganography goes well beyond simple embedding text in an image.

Suresh Gyan Vihar University, Jaipur
International Journal of Converging Technologies and Management (IJCTM)
Volume 3, Issue 1, 2016
ISSN : 2455-7528

Considering the strengths and weakness of steganography and cryptography, researchers tried to combining them in practice, so that the new method would simultaneously possess the advantages of steganography and cryptography while overcoming the respective weaknesses.

Idea employing the two techniques in tandem, The techniques describe by Singh and Malik [13] uses blowfish encryption algorithm for encrypting the text message rendering it non readable and secure. The LSB techniques of steganography further enhance the security.

Text encryption with DES and LSB insertion Dhawal Seth et Al [14] combines cryptography and steganography, so as to ensure more security over insecure communication channel. DES cryptographic algorithm being used for encrypting the text message in conjunction with LSB substitution for embedding the encrypted message in the cover image.

Most of the hybrid system uses cryptographic algorithms to encrypt text message and hide the ciphertext by LSB steganography. To our knowledge 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.

A. DES and TDEA

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 TDEA.

Triple DES uses a key package that consist of three keys. K_1, K2 and K_3 all of having 56 bits. These keys are applying in three different variant. The encryption of plaintext takes places as :

$$\text{Ciphertext} = EK_3\,(DK_2\,(EK_1\,(\text{Plaintext}))\,)$$

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

$$\text{Plaintext} = DK_1\,(EK_2\,(DK_3\,(\text{Ciphertext}))\,)$$

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
- K1 and K2 are indepents and K3 = K1.
- All three keys are identical i.e. $K_1=K_2=K_3$.

Triple DES is beneficial because it has important 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.

B. Peak Signal to Noise Ratio (PSNR) :

The dimension of the quality between the cover image f and stego-image g of sizes N x N is derived by PSNR [18] as:

$$\text{PSNR} = 10 \times \log\,(255^2 / \text{MSE})$$

$$\text{Where MSE} = \sum_{N=0}^{N-1} \sum_{N=0}^{N-1} (f(x,y)g(x,y))^2 / N^2$$

Where f(x,y) and g(x,y) characterize the pixel value at the position (x, y) in the cover-image and the stego-image correspondingly. The PSNR is stated in dB. PSNR is descriptive of the quality of image i.e. the higher the PSNR, lower in the difference between cover image and stego image and vice – versa.

III. PROPOSED HYBRIDE MODEL

Proposed steganographic model is based on Triple Data Encryption Algorithms (TDEA) as depicted as follows:

Suresh Gyan Vihar University, Jaipur
International Journal of Converging Technologies and Management (IJCTM)
Volume 3, Issue 1, 2016
ISSN : 2455-7528

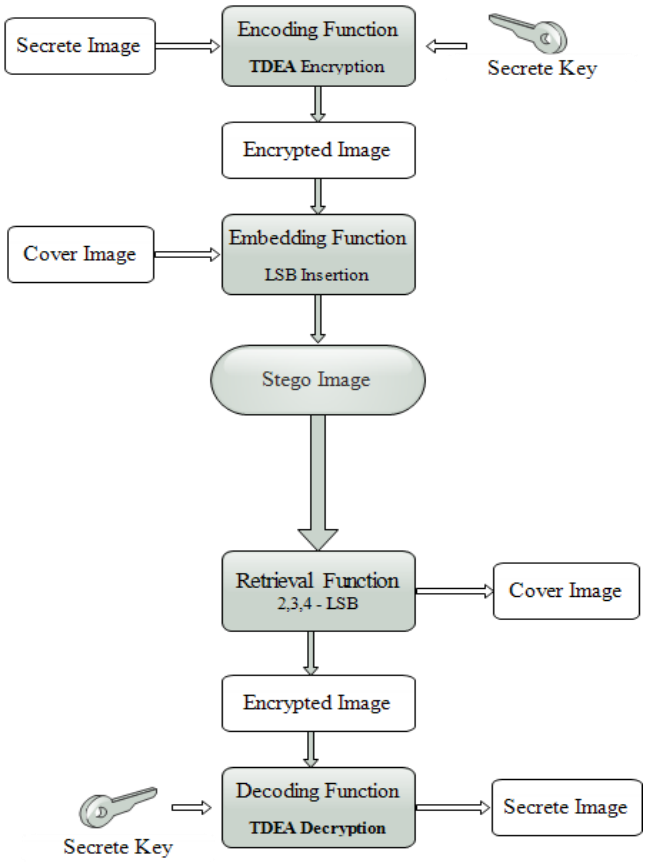


Figure 1. Proposed Steganography Model

A. *Encoding Function*

Initially the secrete image is chosen (e.g. of 64×64). The intensity value of each pixel of secrete image is changed from decimal to binary. Now taking eight consecutive pixel values from secrete image, one block of 64 bits is formed. Input this block to triple DES encoding [19] function described below.

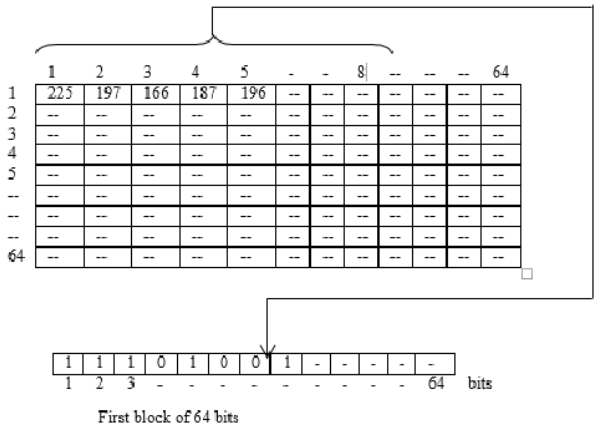


Figure 3.2: Formation of Input Block for DES

One complete execution of Triple DES with three keys gives eight pixel value of secrete image into respective pixel values of encrypted secrete image.

B. *Embedding Function using LSB Method*

1) Bit Division: Taking the cipher encrypted image, the values are converted from decimal to binary

The binary value of $(173)_{10} = (10101101)_2$

Next divide this 8 bit value into 4 part taking 2 bits in each

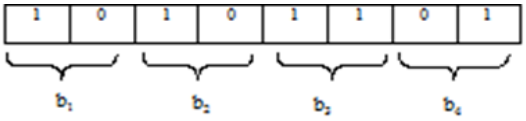
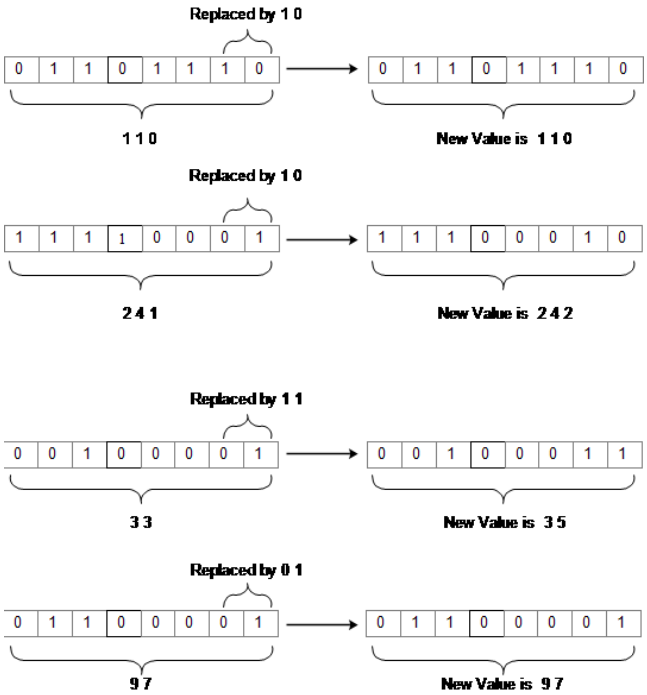


Figure 3.6: Bit Division for LSB Embedding

After bit division, value of b1 = 10, b2 = 10, b3 = 11, b4 = 01 are getting.

2) Insertion of Bit value into the cover image: After receiving the values of b1, b2, b3, b4, these values are inserted into the cover image. The 2 bit LSB of the four consecutive pixels in cover image are replace. Taking the pixels one by one from the cover image, the 2 LSB bits are replaced by 10,10,11,01 respectively.



Suresh Gyan Vihar University, Jaipur
International Journal of Converging Technologies and Management (IJCTM)
Volume 3, Issue 1, 2016
ISSN : 2455-7528

Figure 3.7: Insertion of Bits into cover Image

3) Formation of Stego Image: After receiving the new pixel value the stego image is formed by replacing these values at their original position. Likewise the pixels value on by one from encrypted secrete image and insertion into the cover image and replaced them. Result becomes the stego image

Encoding & Embedding Algorithm [19]:

Input: A gray level Secrete Image (m × n), A gray Level Cover of size (2m × 2n);

Output: Stego Image of size (2m × 2n);

1. Input eight pixel value of the secrete image to form block of 64 bits to the image encoding Function (TDEA), which produces the encrypted secrete image.
2. Divide each pixel value of encrypted secrete image into 4 parts containing 2 bits each.
3. Insert these pixel values into the LSB position of first four pixels in the cover image one by one.
4. End.

C. *Image Recovery Function*

At the receiving end, decoding of stego image perform the following process:

1) Generate the 2 LSB bits from the stego Image :
The pixels value are handled one by one from the stego image. Convert these pixel value from decimal to binary values and take 2 LSB bits from first four consecutive pixel values:

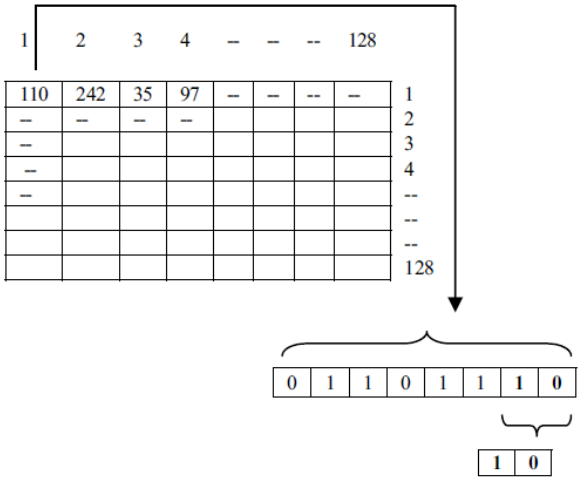


Figure 3.8: LSB (2- bits) Extraction of Stego Image

Similarly taking next three pixels. i.e. 242, 35, 97;

$(242)_{10}$ = $(1\ 1\ 1\ 1\ 0\ 0\ 1\ 0)_2$
$(35)_{10}$ = $(0\ 0\ 1\ 0\ 0\ 0\ 1\ 1)_2$
$(97)_{10}$ = $(0\ 1\ 1\ 0\ 0\ 0\ 0\ 1)_2$

Getting,

b1 = 1 0; b2 = 1 0; b3 = 1 1; b4 = 0 1;

2) Concatenation of bits:

Now concatenating the input, the 8 bits of first pixel value of encrypted secrete image is acquired as

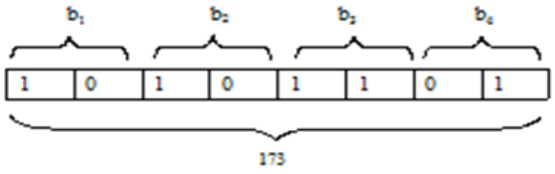


Figure 3.9: Concatenation of Bits (Extracted)

3) Reformation of Encrypted Secrete Image:

Now the generated value is placed into first position. Similarly taking the next four pixel value from stego image, the process is repetitive and the whole encrypted secrete image is recovered.

D. *TDEA Decoding Function*

1) Creation of Secrete image:

Now the eight consecutive pixel value from encrypted secrete image are again inputted to TDEA decoding

function with same constraint and keys one by one (but used in reverse order) to obtained respective eight pixels value of original secrete image.

Image Retrieval / Decoding Algorithm [19]:

Input: Stego Image of size (2m × 2n);

Output: A grey level Secrete Image (m × n);

Steps:

1. Input each pixel and take 2 bit LSB from 4 consecutive pixel value of the stego image.
2. Concatenated four 2bit LSB to get 8 bits of each pixel of encrypted secrete image.
3. Now taking eight consecutive pixel value form block of 64 bits are input to decoding Function (TDEA) using same parameter but keys value used in reverse order getting first eight pixel value of secrete image and so on.
4. End.

IV. RESULTS AND ANALYSIS:

Proposed model is robust Steganography technique because without knowing the secrete keys package the extraction of secrete image from the stego image is impossible. Furthermore quality of cover image is also not degrading due to variation in two LSB of each pixel which replicates only 0 – 3 difference in pixel value.

Moreover the proposed system is capable of not just scrambling data but it also changes the intensity of the pixels which contributes to the safety of the encryption.

TABEL I CAPACITY & PSNR

Name of Image	Size (Pixel)	Capacity	PSNR In DB
Baboon.jpg	64× 64	25 %	54.58
Cameraman.jpg	64× 64	25 %	55.01
Lena.jpg	64× 64	25 %	59.28

V. CONCLUSION:

In the proposed Triple DES based steganographic model the strength of conventional DES and bundle of secrete key for encrypting secrete image, improves image quality 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. This model also counter to the meet in the middle attack with 168 bit key security.

References

[1] D. N.F. Johnson, S. Jajodia, Exploring steganography: seeing the unseen, IEEE Computer 31 (2) (1998) pp.26–34.

[2] Ross J. Anderson, Fabien A.P. Petitcolas , “On The Limits of Steganography “, IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 1998.

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

[4] N. Provos, P. Honeyman, “Hide and Seek: an Introduction to Steganography”, IEEE Security and Privacy 1 (3) (2003) 32–44.

[5] Cheddad, A., Condell, J., Curran, K. & Mc Kevitt, Paul, 2010. “Digital image steganography: survey and analysis of current methods”, Signal Processing, 2010, 90(3), pp.727-52.

[6] Mohammed AbuTaha, Mousa Farajallah, Radwan Tahboub, Mohammad Odeh, “Survey Paper: Cryptography Is the Science of Information Security “, International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (3): 2011, pp. 298 – 309.

[7] E. Thambiraja , G. Ramesh , R. Umarani , “A Survey on Various Most Common Encryption Techniques “ , International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 7, July 2012 , pp. 226-233.

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

[9] D.Coppersmith, “The Data Encryption Standred (DES) and its Strength against attack “, IBM Journal Research Development Vol 38 No. 3, May 1994, pp. 243- 250.

[10] Rijndael,” ADVANCED ENCRYPTION STANDARD (AES) “, Federal Information Processing Standards FIPS Publication 197 November 26, 2001, pp. 1-47. National Institute of Standards and Technology, Information Technology Laboratory (ITL).

[11] H. Al-Barhmtoshy, E. Osman, and M. Ezzat, "A Novel Security Model Combining Cryptography and Steganography ", 2004, pp- 483-490.

[12] Cheddad, A., Condell, J., Curran, K. & Mc Kevitt, P. " Securing information content using new encryption method and steganography", In Proceedings of the 3rd IEEE International Conference on Digital Information Management. London, UK, 2008d. 13-16 Nov. pp. 563-568.

[13] Ajit Singh, Swati Malik, " Securing Data by Using Cryptography with Steganography ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013. Pp 404-409. Dhawal Seth, L. Ramanathan, Abhishek Pandey, "Security Enhancement: Combining Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887) Volume 9– No.11, November 2010, pp. 3-6.

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

[15] Khalil Challita, Hikmat Farhat," Combining Steganography and Cryptography: New Directions", International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): pp.199-208.

[16] Smita P. Bansod , Vanita M. Mane, Leena R. Ragha ,"Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity ", 2012 IEEE International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India. Pp 1-6.

[17] A. Joseph Raphael, Dr. V. Sundaram, "Cryptography and Steganography – A Survey ", International Journal Comp. Tech. Appl., Vol 2 (3), 626-630.

[18] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena , " Security Improvisation in Image Steganography using DES " , 3rd IEEE International Advance Computing Conference (IACC - 2013) ,Jan 2013, Gaziabad New Delhi , India ,pp 1082 – 1087.

[19] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena , " Improvisatio of Security Aspect in Steganography applying DES " , IEEE International Conference on Communication Systems and Network Technologies (CSNT - 2013) ,April 2013, Machine Intelligence Research Lab Gwalior , India ,pp 431 – 436.

[20] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena "Secured Steganography Approach using AES " , accepted for publication in International journal of Computer Science Engineering and Information Technology Research journal, Transstellar Journal Publications and Research Consultancy Private Limited, (www.tjprc.org), TJPRC Global Research Community, which has offices all over the world - USA, UK, Singapore, Qatar and India with Impact Factor (JCC) - 6.3925, as published by www.journal-metrics.com.

[21] M. S. Sutaone, M.V. Khandare, "Image Based Steganography Using LSB Insertion Technique ", IEEE. pp 146-151.

AUTHORS INFORMATION

Manoj Kumar Ramaiya is currently pursuing Ph.D. in Image Steganography Technique using Strength of DES from SGVU Jaipur. He received his B.E. degree in Computer Science and Engineering from Barkatullah university Bhopal and also M.Tech in Computer Science in Engineering from Rajiv Gandhi Prodhyogiki Vishvvidyalaya Bhopal. Research Area of interest are Image Steganography, Cryptography, Information and Network security.