JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-6, Issue-1 E-ISSN: 2347-2693

Image Security Implementing Steganography and Cryptographic Methods

A. Balasubramani[1*], **Ch.D.V. Subba Rao**[2]

[1*]Faculty of Computer Science & Engineering, SVPCET, PUTTUR, India
[2]S.V.U.College of Engineering, S.V.University, TIRUPATI, India

**Corresponding Author: balunbkr@yahoo.co.in*

Available online at: www.ijcseonline.org

Received: 03/Jan/2018, Revised: 06/Jan/2018, Accepted: 18/Jan/2018, Published: 31/Jan/2018

***Abstract* —** Steganography is that the art of concealment the actual fact communication is going down, by concealment info in other info. Many different carrier file formats can be used, but digital pictures are the foremost well-liked because of their frequency on the web. This paper introduces 2 new strategies wherever in cryptography and steganography are combined to encode the information as well on hide the information in another medium through image process. This paper securing the image by encryption is finished by DES formula victimisation the key image. The encrypted image may be hide in another image by victimisation LSB techniques, so that the secret's terribly existence is hid. The coding may be done by the same key image victimisation DES formula.

Keywords- Steganography, Cryptography, image hiding, Least-significant it(LSB) scheme.

I INTRODUCTION

The word Steganography springs from Greek suggests that "Hidden Writing" [1] and dates back to 440 B.C. [2]. Some earlier examples as reportable in [3] include: shaving scalp of a most trusty slave to print a secret message and anticipating the hair to grow once that he was sent to allies World Health Organization retrieves it by reshaving his head; engraving messages on wood pill so covering it wax. The receiver retrieves it by melting the coated wax. A comprehensive insight on unconventional stenographic schemes has well been elucidated in [4].

Steganography is associate degree ancient art [5] that with age has currently been evolved into a science [6] to avert detection of hidden information. [7] Delivered nomenclature for steganography whereas Simon [8] gave the primary model for steganography by discussing the state of affairs of Alice and Bob control in separate jail cells had to speak through lawman Wendy. Varieties of stenographic system are mentioned in [9] as pure (with no Stego key), personal key and public key severally whereas 3 techniques for steganography as well as insertion, substitution and canopy generation are mentioned in [10]. Cryptography, having Greek origin and with same origination amount as that of steganography, suggests that "Secret Writing" [11] the essence of that is to mute secret data in distinction to steganography whose sole perseverance is to hide the actual fact that such data will very exist. Although opposite to every different in their approach, these 2 serves well as a double edged weapon to safeguard data security frontiers [12-14].

The mammoth growth of web as communication medium has insentiently provided a gap for surreptitious communication that has been exploited fully by lecturers and experts through style of file formats (as hidden data carrier) that exist for text, image, audio and video etc. storage and illustration. This paper besides presenting associate degree innovative secure theme for LSB primarily based image steganography, conjointly expounds on predominant idea relating to detection which for affirmative bulk of on-line information exchange.

The paper is organized as, section 2 discusses about Proposed Work, section 3 discusses about Experimental Results after implementation, section
4 discusses about Conclusion and future work.

II PROPOSED WORK

A. DATA ENCRYPTION STANDARD (DES)

The Data encryption standard (DES) shall consist of the subsequent encryption formula (DES). These devices shall be designed in such how that they will be employed in a system or network to produce cryptanalytic protection to binary coded data. The strategy of implementation can depend on the applying and surroundings. The devices shall be enforced in such how that they may be tested and valid as accurately acting the transformations laid out in the subsequent algorithms.

The formula is meant to code and decipher blocks of information consisting of sixty four bits beneath control of a 64-bit key1. Deciphering should be accomplished by victimization an equivalent key as for enciphering, however with the schedule of addressing the key bits altered in order that the deciphering method is that the reverse of the enciphering method

A block to be enciphered is subjected to associate degree initial permutation science, then to a fancy key dependent computation and eventually to a permutation which is that the inverse of the initial permutation IP-1. The key- dependent computation are often merely defined in terms of a operate f, known as the cipher function, and a operate KS, known as the key schedule.

A description of the computation is given initial, along with details on however the algorithmic rule is employed for encipherment. Next, the employment of the algorithmic rule for decipherment is delineated. Finally, a definition of the cipher operate f is given in terms of primitive functions that square measure known as the choice functions Si and the permutation operate P. Si, P and KS of the algorithm square measure contained

. Blocks square measure composed of bits numbered from left to right, i.e., the left most little bit of a block is bit one.

In this projected paper, DES cryptography (decryption) algorithmic rule takes 8-bit block of plaintext and a 10-bit key to provide associate degree 8-bit cipher text. The encryption algorithmic rule involves five functions: associate degree initial permutation (IP); a fancy operate fK, which involves each permutation and substitution that depends on a key input; an easy permutation function that switches (SW) the 2 halves of the data; the operate fK once more and eventually, the inverse permutation of science (IP-1). The operate fK takes 28-bit keys that square measure obtained from the initial 10-bit key.

The 10-bit secret's initial subjected to permutation (P10) then a shift operation is performed. The output of the shift operation then passes through permutation operate that produces a 8- bit output (P8) for the primary sub key (K1). The output of the shift operation agaifeeds into another shift and (P8) produce the ordinal sub key (K2) [18]

In this projected paper, every computer memory unit (pixel) of all the 3 matrices(R,G,B matrices of payload) area unit encrypted exploitation DES rule and a picture comprised of encrypted pixels is made. The key used to inscribe every constituent is of 10-bit length and is obtained from the pixels of key image. The pixel values of red, inexperienced and blue intensities of every constituent of key image area unit combined to urge a 24-bit worth. The first 10 bits area unit elect because the key to inscribe the red intensity constituent of payload image. The center 10 bits will be the key to inscribe the inexperienced intensity constituent of payload and eventually the last 10 bits is that the key to encrypt blue intensity constituent of payload image. So the size of key image should be same as that of payload. If not, then the key image can get resized. Each pixe (24-bit) of the key image is split into 3 keys(10- bit each).In this paper, the encrypted image is embedded at intervals another image referred to as cover-image for carrier image. Cover-image carrying embedded secret image is noted as stego- image.

a) Simplified DES-Type Algorithm

Suppose that a message has 12 bits and is written as L_0R_0 , where L_0 consists of the first 6 bits and R_0 consists of the last 6 bits.

The key K has 9 bits. The *i*th round of the algorithm transforms an input $L_{i-1}R_{i-1}$ to the output L_iR_i using an 8-bit key K_i derived from K.

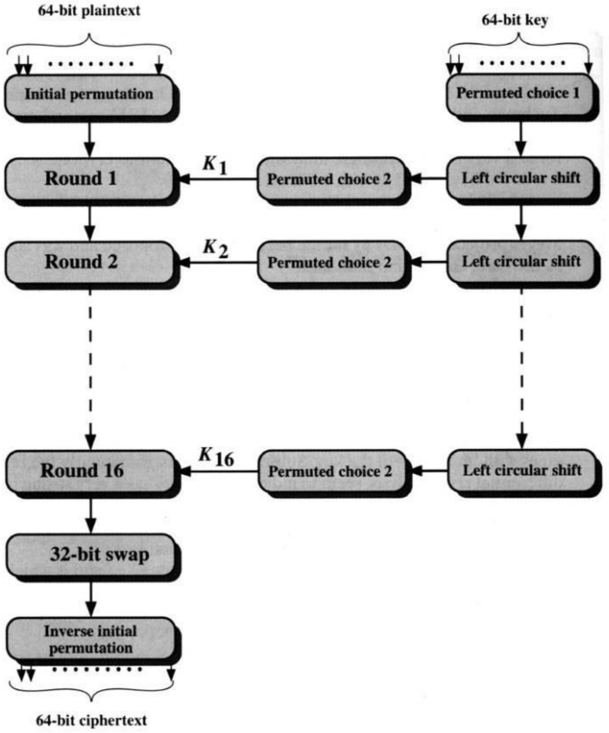
The main part of the encryption process is a function $f(R_{i-1},K_i)$ that takes a 6-bit input R_{i-1} and an 8-bit input K_i and produces a 6- bit output which will be described later.

The output of the *i*th round is defined as:

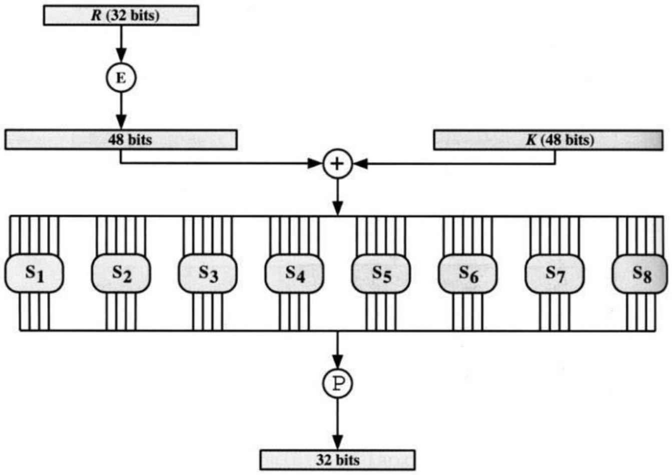
$$L_i = R_{i-1} \text{ and } R_i = L_{i-1} \text{ XOR } f(R_{i-1},K_i)$$

The decryption is the reverse of encryption. $[L_n]$ $[R_n$ XOR $f(L_n, K_n)] = \dots = [R_{n-1}]$ $[L_{n-1}]$

b) Encryption



Encryption process



Encryption round

c) The Operations of f Function

$E(L_i)=E(011001)=E(01010101)$ (Expander)

S-boxes

S_1 101 010 001 110 011 100 111 000
100 110 010 000 111 101 011

S_2 100 000 110 101 111 001 011 010
101 011 000 111 110 010 001 100

The input for an S-box has 4 bits. The first bit specifies which row will be used: 0 for1^{st}

The other 3 bits represent a binary number that specifies the column: 000 for the 1st column, 001 for the 2nd column, … ϭϭϭ for the 7th column. For example, an input 1010 for S_1 box will yield the output 110.

The key K consists of 9 bits. K_i is the key for the ith round starting with the ith bit of K. Let K=010011001, then K_4=01100101.

$E(R_{i-1})$ XOR K_i =10101010 XOR 01100101
= 11001111

$S_1(1100)=000$

$S_2(1111)=100$

Thus, $R_i = f(R_{i-1},K_i)=000100$, $L_i =R_{i-1} =100110$

$L_{i-1}R_{i-1}$ = бϭϭϭббϭббϭϭб → ;?□ L_iR_i
100110011000 d)

Decryption

The same algorithm as encryption.

Reversed the order of key (Key_{16}, Key_{15}, … Key_1).

For example:

IP undoes IP^{-1} step of encryption.

1st round with SK16 undoes 16th encrypt round.

B. EMBEDDING THE ENCRYPTED IMAGE INCARRIER IMAGE

LSB may be a straightforward approach to embedding information in an exceedingly cowl image. The constituent values of encrypted image is hidden within the lsb of pixels of carrier image by merge it with the ordinal lsb of carrier pixel.If the the scale of the encrypted image is mxn ,then the scale of carrier image should be mxnx8 as every encrypted computer memory unit needs eight bytes (pixels)of carrier image. Thus if the carrier image size isn't eight times the size of the payload , then it's to be resized. In this procedure
LSB rule helps for securing the originality of image.

C. EXTRACTING THE ENCRYPTED IMAGE IN CARRIER IMAGE

The extracting is reverse to embedding the encrypted image. In extracting, the carrier image in which the information is hidden is given as a computer file. Here the given image is initial encrypted so the encrypted image is hidden within the carrier image. Finally the hidden encrypted image is decrypted. The smallest amount important
bit technique by which the encoded bits within the image is decoded and turns to its original state and offers the output as a image. The coding and cryptography so as to secure from unauthorized access.

III. EXPERIMENTAL RESULTS

In this projected paper securing the image by encryption is finished by DES algorithmic rule victimization the key image. The encrypted image is hide in another image by victimization LSB techniques, so that the secret's very existence is hid. Finally the hidden encrypted image is decrypted as shown during a figure.

FIGUR
E-1

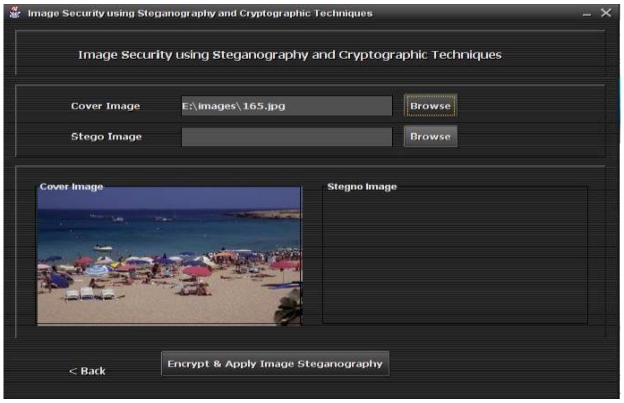


Image Security using Steganography and Cryptographic Techniques

Image Security using Steganography and Cryptographic Techniques

Cover Image: E:\images\165.jpg

Stego Image:

FIGU2

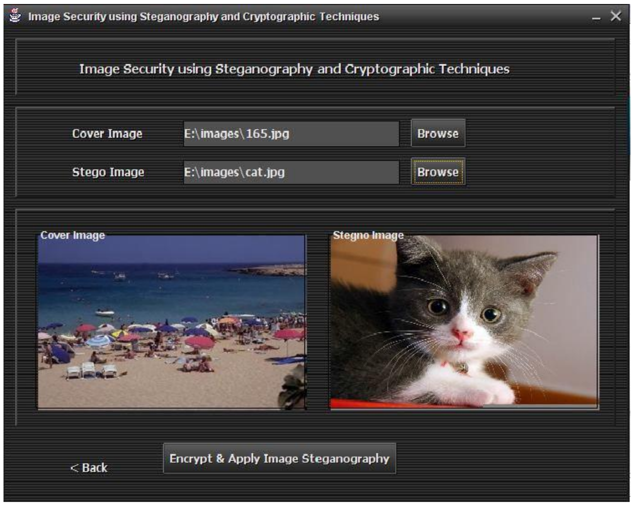


Image Security using Steganography and Cryptographic Techniques

Image Security using Steganography and Cryptographic Techniques

Cover Image E:\images\165.jpg

Stego Image E:\images\cat.jpg

FIGURE-3

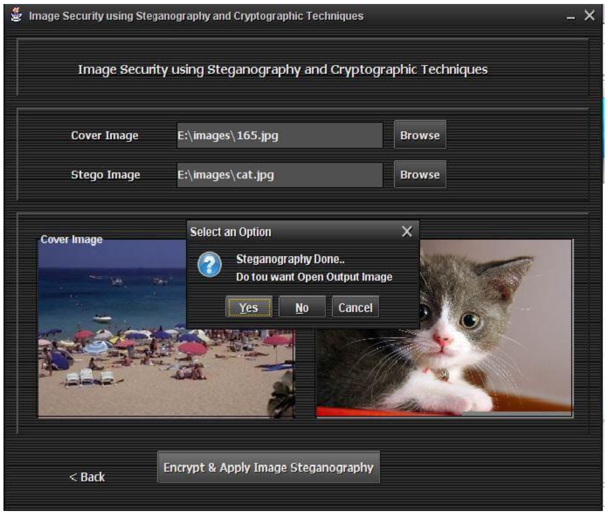


Image Security using Steganography and Cryptographic Techniques

Image Security using Steganography and Cryptographic Techniques

Cover Image E:\images\165.jpg

Stego Image E:\images\cat.jpg

Select an Option

Steganography Done..
Do tou want Open Output Image

FIGURE-4

FIGURE-5

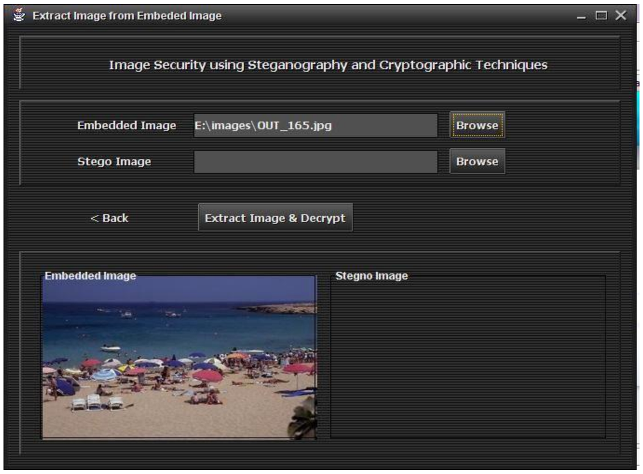

Extract Image from Embeded Image

Image Security using Steganography and Cryptographic Techniques

Embedded Image E:\images\OUT_165.jpg

Stego Image

FIGURE-6

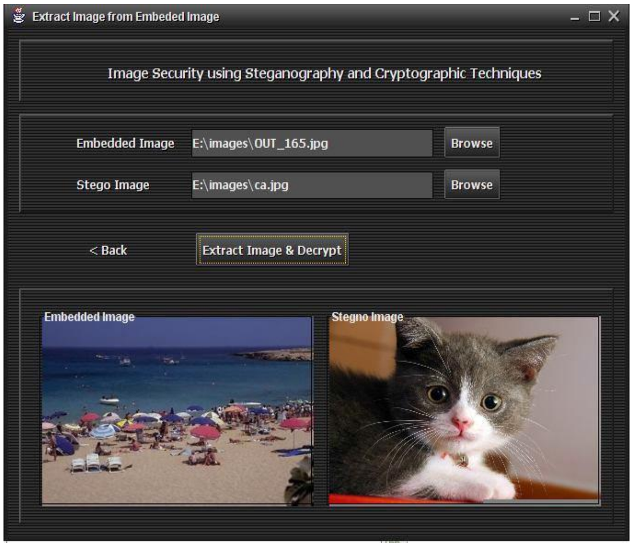

Extract Image from Embeded Image

Image Security using Steganography and Cryptographic Techniques

Embedded Image E:\images\OUT_165.jpg

Stego Image E:\images\ca.jpg

FIGURE-7

IV. CONCLUSION

In this paper, we tend to project the mix of cryptography and steganography has been achieved by victimization the DES algorithmic program and LSB technique. Data encryption customary (DES) is employed to write secret image and LSB technique is employed to cover encrypted secret image into cowl image. To yield higher imperceptibility the projected methodology provided a higher similarity between the duvet and stego pictures as a result.when steganography is combined with secret writing an honest security was achieved between 2 parties just in case of secret communication, it is hardly attracted from auditor by optic.

Finally we will conclude that the projected technique is effective for secret electronic communication. The future work can be to increase this methodology to arrange the text that's obtained by the secret writing of image, to form a word or meaty sentence and new ways is done by aside from LSB methodology.

REFERENCES

[1] C. Kurak and J. McHugh, A cautionary note on image downgrading, in: Proceedings of the IEEE 8 Annual Computer Security Applications Conference, 30 Nov-4 Dec, 1992, pp. 153- 159.

[2] J.C. Judge, Steganography: Past, present, future. SANS Institute publication,http://www.sans.org/reading_room/ whitepapers/stenganography/552.php, 2001.

[3] Km. Pooja ,Arvind Kumar , “Steganography- A Data Hiding Technique” International Journal of Computer Applications ISSN 0975 – 8887, Volume 9– No.7, November 2010.

[4] N.F. Johnson and S. Jajodia, Exploring steganography: Seeing the unseen, IEEE Computer, 31(2)(1998) 2634.

[5] N. Provos and P. Honeyman, Hide and seek: An introduction to steganography, IEEE Security and Privacy, 01 (3)(2003)32-44.

[6] N.F. Johnson and S.C. Katzenbeisser, “A survey of steganographic techniques”, in: S. Katzenbeisser and F.A.P. Petitcolas, (ed.) (2000) Information hiding techniques for steganography and digital watermarking, Norwood: Artech House, INC.

[7] P. Moulin and R. Koetter, Data-hiding codes, Proceedings of the IEEE, 93 (12)(2005)2083-2126.

[8] R. Chandramouli, M. Kharrazi, N. Memon, “Image Steganography and Steganalysis: Concepts and Practice “ , International Workshop on DigitalWatermarking, Seoul, October 2004.

[9] R.J. Anderson and F. A. P. Petitcolas (2001) On the limits of the Stegnography, IEEE Journal Selected Areas in Communications,16(4), pp. 474-481.

[10] S.B. Sadkhan, Cryptography: Current status and future trends, in: Proceedings of IEEE International Conference on Information & Communication Technologies: From Theory to Applications, Damascus. Syria, April 19-23,2004, pp. 417-418.

[11] T. Morkel, J. H. P. Eloff, M. S. Olivier, ”An Overview of\ Image Steganography”, Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, SA

Author Profile

A.Balasubramani working as Professor in the Department of Computer Science & Engineering, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Andhra pradesh.

Dr Ch.D.V.Subba Rao working as Professor, in the Department of Computer Science & Engineering, S.V.U.College of Engineering, Sri Venkateswara University, Tirupati, Andhra pradesh.