ISSN:2320-0790

An International Journal of Advanced Computer Technology

Image Steganography Based on Transform Domain, Blowfish and AES for second level security

Janki Gajjar
Research Scholar, Computer Science Engineering Dept, NSIT College, India

Abstract*:* Steganography is technique for secret communication. It hides the existence of the communication between parties. So viewer cannot detect the existence of the message and also not detect the communication channel. So attacker cannot modify and see the secret information. In image steganography, secrecy is accomplished by hide the secret message in cover image using steganography techniques. There are different types of steganography techniques each have their merits and demerits. Using Steganography techniques on cover image we can improve the security and robustness. For improving second level security we are using cryptography. Cryptography is used to convert the secret message in cipher text means unreadable form of message. Cryptography introduces many algorithms. This algorithm converts the secret message in cipher text. In our proposed method we are using Blowfish and AES algorithm for converting the message in cipher text and then hide this cipher text in cover image using DCT steganography technique. Using this combine technique we can get the stego-image. Here using this proposed method we can get the security and robustness in terms of message when we retrieve the message from the stego-image.

Keywords*:* Steganography, Cryptography, DCT, PSNR, MSE, Blowfish, AES.

I. INTRODUCTION

Now a day, communication is the essential need for each and every one. But for exchanging information through communication channel everyone needs that this channel in which information is exchanged that channel is secure means no one can detect that information. So for safe communication channel we want that no one can detect the existence of the channel. For that steganography is used. Steganography is technique for hiding the existence of communication between parties. In our daily life there are many options for secure communication like telephone, email and etc. But sometimes it is not secure at certain level. For transferring data in safe and secure way two techniques can be used. These techniques are cryptography and steganography. For a significant length of time individuals create inventive routines for secret communication. In that a path, to the point that not concerned persons are not able to recognize the presence of this data by analyzing the data detection. The rest of this report highlights quickly some authentic fact and attacks on methods [2]. The steganography is used to storing the information in wide range of computerized information like audio, video, image and protocol. But sometime it will helpless for different type of attack. For that digital steganography is used. In digital steganography the secret information is embedded in another computerized data by passing secret id inside data so that sender can prove their copyright ownership.

A. Difference between Cryptography and Steganography

The purpose of cryptography and steganography is to provide secret communication. Steganography is Hiding a secret message in multimedia object in such a way that no one can detect the presence of the hidden message. Cryptography is "The process or skill of communicating in, or decrypting secret writing or ciphers." The distinction between cryptography and steganography is an important one, and is summarized by the following table.[9]

B. Motivation

Steganography is a technique for hiding the communication between the parties who exchanging the information. The internet provides large information to people. And this information is also transfer from people to people over internet. But sometime attacker attack on the message. So for security purpose if we transfer the message in image, audio, video or other multimedia file than no one can detect that the message is behind the multimedia file. So using this we can get the security on data. If attacker gets access to our multimedia file then also attacker can't get our original information because the message is under the background of image. So attacker cannot get original message easily.

C. Application of Steganography:

- Confidential Communication and Secret Data Storing[1]
- Protection of Data modification[1]
- Access Control System for Digital Content Distribution[1]
- E-Commerce ex. Online shopping[1]
- Media ex. Encrypt the disk media[1]
- Database Systems for password storage.[1]
- Digital watermarking. [1]

D. Objectives

The main objective of the dissertation is to propose a new solution for our day to day life for secure communication and exchanging information. For secure communication here we uses a steganography and cryptography techniques. For transferring message in secure manner we proposed a new technique. First we encrypt the message using blowfish algorithm or AES algorithm then embed the message in image using DCT steganography technique. So we can get the stego-image. Then this stego image is transferred to the receiver side. So if attacker sees the image then also attacker cannot get the original message in number of tries. Receiver side reverse process is done to retrieve original message.

II. PROPOSED WORK

There are many steganography transformations for improving the quality of image and for more security. But form literature survey we can conclude that, first, steganography is best technique to hide information over cryptography. Secondly, Transform Domain technique has advantages over spatial domain. Third point, DCT is best technique for best quality image by comparing the PSNR over other transformation techniques. And last Blowfish has better performance than other algorithms for second level security for image steganography. Here AES is also included for cryptography of text. So we can compare the result of different cryptography method to encrypt the data.
The major challenges of steganography are:-

Security of Hidden Communication: So as to avoid from raising the suspicions of busybodies, while avoiding the careful screening of algorithmic location, the hidden substance must be undetectable both perceptually and measurably. Steganography methods ought to deliver high subtle Stego-image.

Size of Payload: Dissimilar to watermarking, which needs to install just a little measure of copyright data, steganography goes for concealed correspondence and in this way as a rule obliges adequate implanting limit. Prerequisites for higher payload and secure correspondence are regularly conflicting. Contingent upon the particular application situations, a tradeoff must be looked for.
Robustness: Stego-image should provide robustness to image processing techniques like compression, cropping, resizing etc. i.e. when any of these techniques are performed on stego-image, secret information should not be destroyed completely.

There is no technique of steganography which provide all the three properties at high level. There is an exchange off between the limit of the implanted information and the robustness to specific attacks, while keeping the perceptual nature of the stego-medium at an adequate level. It is most certainly not conceivable to achieve high strength to flag adjustments and high insertion limit at the same time.
In this project my task is to implement techniques of transform domain steganography (DCT substitution) and blowfish algorithm taking secret information as a data file and as an image and to do comparisons between them in terms of embedding capacity and quality of produced stego-image and robustness to attacks. Here I also uses an AES algorithm for alternate of Blowfish.

To, hide or protect the information, cryptography is providing the several level of security. Here we have used the image steganography for the hide the communication between two parties so that attacker can't see the communication as well as provide second level security we use the cryptography to encrypt the message and use steganography technique to store the encrypted information behind the Image. The scope of dissertation work is we can try to combine the two cryptography algorithm for more security. And provide a solution for different type of attack.

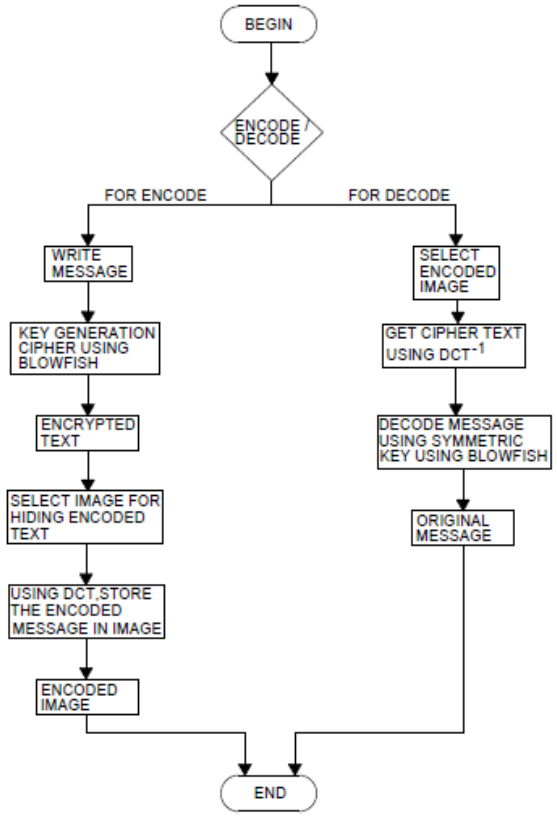


Fig. 1 Flowchart of Proposed System Using Blowfish Algorithm

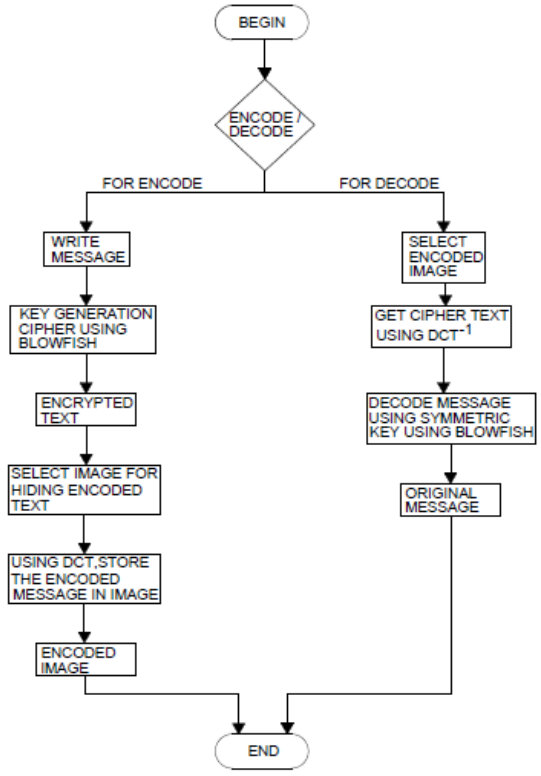


Fig. 2 Flowchart of Proposed System Using Blowfish Algorithm

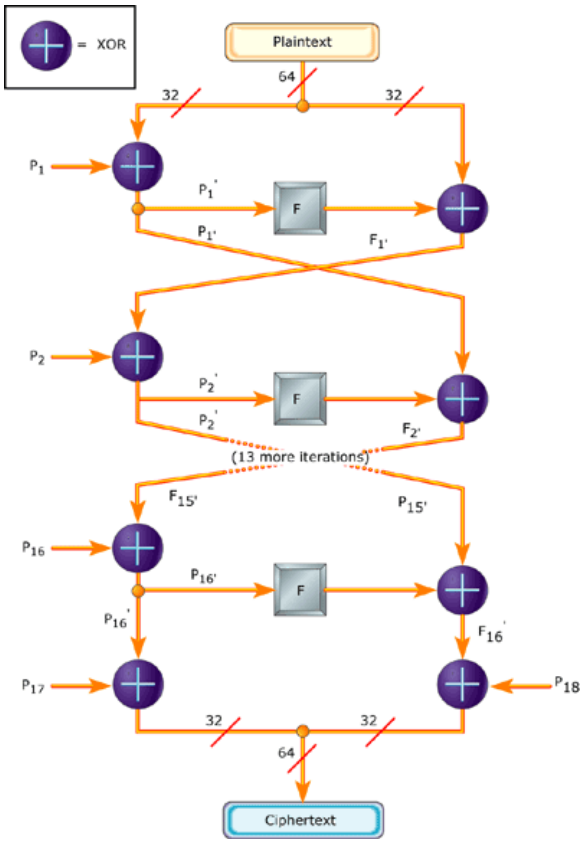


Fig. 3 Blowfish Algorithm

A. *DCT Steganography*

DCT based calculation as a rule separates the picture into 8*8 squares and conceals information in each 8*8 piece with the assistance of quantization. However wavelet based calculation generally hides the information in the coefficients for that threshold(limit quality) is utilized to figure out if the coefficient ought to be utilized to conceal the worth. DCT more often than not takes more processing and complex than the wavelet based. In lossy pressure, the DCT based calculation beats the better PSNR contrast with DWT. Additionally them two are truly strong to the JPEG pressure. While the wavelet based one still shows lower result on PSNR values. [11]

B. *Blowfish Algorithm*

Blowfish was made in 1993 by Bruce Scheier as a quick, distinctive alternative for existing encryption computations such AES, DES and 3 DES and etc.Blowfish is a symmetric square encryption computation sketched out in thought with, Quick: It encodes data on incomprehensible 32-bit microchips at a rate of 26 clock cycles each byte. Lessened: It can continue running in less than 5K of memory. Essential: It uses extension, XOR, lookup table with 32-bit operands. Secure: The key length is variable, it can be in the extent of 32~448 bits: default 128 bits key length. It is suitable for applications where the key does not change routinely, like correspondence join or a modified record scrambled. Unpatented and free of royalty.[14]

C. AES Algorithm

AES is another cryptographic count that can be used to secure electronic data. Specifically, AES is an iterative, symmetric-key square figure that can use keys of 128, 192, and 256 bits, and encodes and decode data in bits of 128 bits (16 bytes). Not at all like open key figures, which use several keys, symmetric-key figures use the same key to scramble and translate data. Encoded data returned by piece figures have the same number of bits that the information data had. Iterative figures use a circle structure that again and again performs stages and substitutions of the data information.[13]

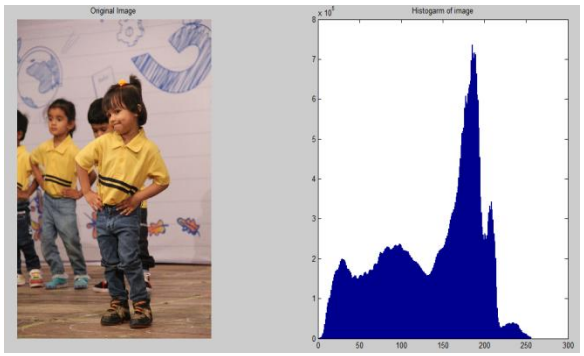


Fig. 4 Histogram of Original Image

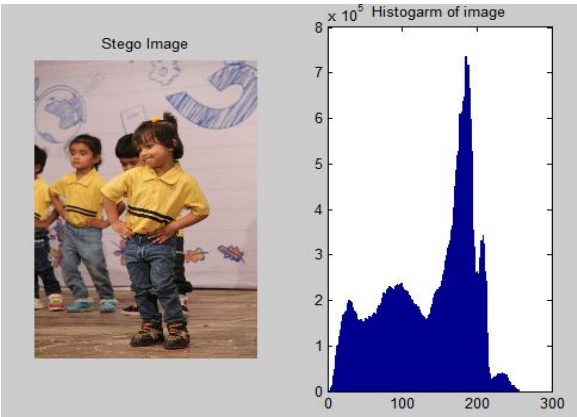


Fig. 5 Histogram of Stego Image

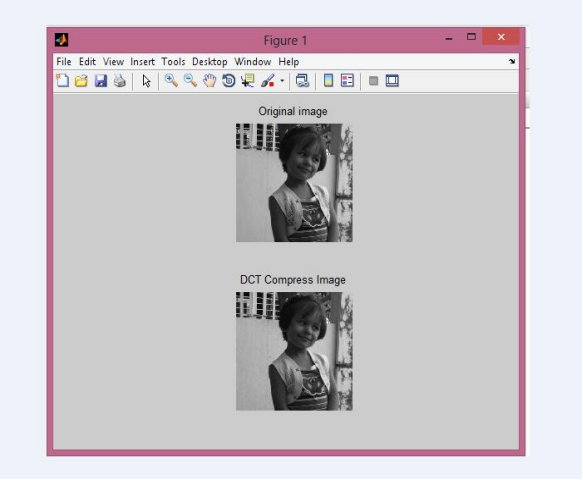
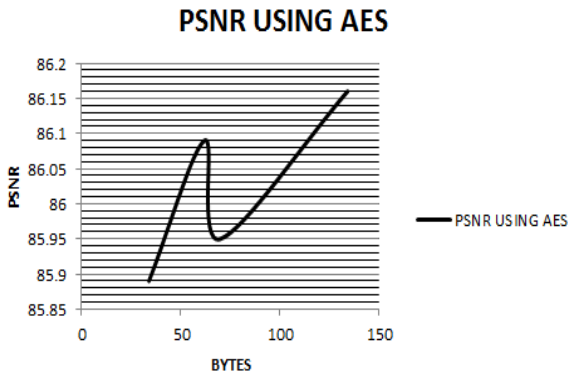
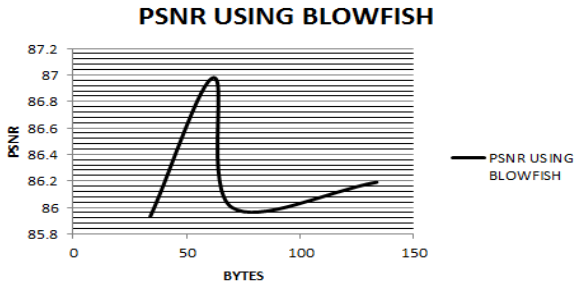


Figure 6 Comparison of original image and DCT compress Stego Image





III EXPERIMENTAL RESULT

NO	IMAGE	MESSAGE	PSNR USING AES	PSNR USING BLOWFISH
1		Hi Good Morning. I am JankiGajjar	85.89	85.93
2		Hello all today is very beautiful day. The weather is so nice.	86.09	86.98
3		I called you yesterday. Did you get my message? I am migrating to USA.	85.95	86.00
4		Great teams do not hold back with one another they admit their mistakes, their weaknesses and their concerns without fear of reprisal.	86.16	86.19

Table 1. PSNR Value comparison of both approaches

Result shows that visual quality of stego-image produced by transform domain techniques are less than that of produced by spatial domain techniques. In transform domain technique we can get the best quality of image.

IV. CONCLUSION & FUTURE ENHANCEMENT

The proposed method use combination of DCT and Blowfish algorithm. Here I also include the result of DCT and AES algorithm. This system encrypts the secret message before embedding in the image. Here image steganography use Blowfish algorithm or AES algorithm for encryption and decryption of the secret message. From comparative analysis of some cryptography technique, Blowfish and AES has better performance than other algorithms. The combining DCT with Blowfish provide secure transmission of secret message. Here we also provide the approach of combining DCT with AES for better and secure transmission of secret message.

The future work may be extended by other transformation techniques. And for cryptography we use Blowfish and AES algorithm.

REFERENCES

[1] JasleenKour, DeepankarVerma "Steganography Techniques-A Review Paper", International Journal of Emerging Research in Management & Technology, vol-3, May 2014.

[2] Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt "Digital Image Steganography: Survey and Analysis of Current Methods", signal processing, vol-90, march 2010.

[3] NavneetKaur, Sunny Behal "A Survey on various types of Steganography and Analysis of Hiding Techniques" International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 - May 2014

[4] Anjali Tiwari, Seema Rani Yadav, N.K. Mittal "A Review on Different Image Steganography Techniques "International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 7, January 2014

[5] StutiGoel,ArunRana,ManpreetKaur " A Review of Comparison Techniques of Image Steganography " *IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 6, Issue 1 (May. - Jun. 2013)*

[6] GurmeetKaur* and AartiKochhar" Transform Domain Analysis of Image Steganography " International Journal for Science and Emerging ISSN No. (Online):2250-3641 Technologies with Latest Trends" 6(1): 29-37 (2013)

[7] Maulik P. Chaudhari, Sanjay R. Patel ''*A Survey on Cryptography Algorithms* "International Journal of Advance Research in Computer Science and Management Studies , vol-2, march-2014

[8] Pratap Chandra Mandal" Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish "*Journal of Global Research in Computer Science ,vol-3, Aug-2012.*

[9] LokeshKumar "Novel Security Scheme for Image Steganography using Cryptography Technique" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012 ISSN: 2277 128X

[10] Joseph Raphael and Dr. V. Sundaram, "Cryptography and Steganography – A Survey" A.JosephRaphael,Dr.VSundaram, Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630, ISSN:2229-6093

[11] Saejung, S. ; Dept. of Comput., Silpakorn Univ., NakhonPathom, Thailand ; Boondee, A. "On the comparison of digital image steganography algorithm based on DCT and wavelet" 2013 International Computer Science and Engineering Conference (ICSEC): ICSEC 2013 English Track Full Papers

[12] Md. Rashedul Islam1, Ayasha Siddiqa2, Md. Palash Uddin3, Ashis Kumar Mandal4 and Md. Delowar Hossain5 "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography" 3rd INTERNATIONAL CONFERENCE ON INFORMATICS, ELECTRONICS & VISION 2014

[13] McCaffrey, James. "Keep your data secure with the new advanced encryption standard." *MSDN Magazine* 11 (2003).

[14] Guthaus, Matthew R., et al. "MiBench: A free, commercially representative embedded benchmark suite." *Workload Characterization, 2001. WWC-4. 2001 IEEE International Workshop on*. IEEE, 2001.

[15] Gunjal, Monika, and Jasmine Jha. "Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm."

[16] MrsArchana S. Vaidya, Pooja N. More, Rita K. Fegade, Madhuri A. Bhavsar, Pooja V. Raut "Image Steganography using DWT and BLOWFISH Algorithms" *IOSR Journal of Computer Engineering (IOSR-JCE)*