Secure Data Transmission techniques using AES cryptography along with Image Steganographic analysis

Manju Bala

I. P. College for Women, University of Delhi, Delhi, India

Abstract— **With the advent of internet to the most part of the world and its usage in vast variety of fields, the sensitive information being communicated through network has also increased exponentially. As the data travels through network of nodes i.e. routers, gateways etc., the third party (intruder) may get unauthorized access to the confidential data. The increase in private data communication has invited security measures so that the sensitive information may not land in intruder's hands. Cryptography and steganography have both come a long way in making the data transmission secure. They both have been used in isolation as well as in combination. Their blending has provided two level security and therefore stronger privacy. The intruder mostly "pick and choose" data from network. The encrypted information using cryptography technique is unreadable by the intruder but the sender or receiver may still be susceptible to various passive attacks and even make it unreadable for the recipient. The data chosen by intruder for further attacks is mostly encrypted as that will contain the confidential data being communicated. Steganography is hiding the private data in image, audio, video etc. which serves the purpose of hiding the existence of confidential information. This work incorporates color image steganography on the private data which is encrypted using AES (Advanced Encryption Standard) to provide two level data security over the network. Diffie helman algorithm is used for sharing key. The Steganography techniques for images, LSB(least significant bit), DCT(Direct Cosine Transform) and DWT(Direct wavelet transform) are compared and analyzed for various parameters like PSNR(Peak Signal to Noise Ratio), SSIM(Structural similarity index) etc. Steganography overcomes the limitation of cryptography by hiding the fact that some confidential transmission is taking place. Hence these two techniques alone cannot work as efficiently as they do together.**

Keywords: **cryptography, AES, steganography, DCT, DWT, LSB, Peak Signal to noise ratio, SSIM, Diffie Helman, stego object**

I. Introduction

Massive amounts of digital data is being collected and stored in huge computer data bases and transmission of data taking place between terminal devices and computers that are connected together in complex communications networks. Without appropriate security measures, the data is susceptible to interception when in transmission, or data may be physically removed or copied while in storage. This would result in undesirable exposures of data and potential invasions of privacy. Data are also vulnerable to unauthorized deletion, alteration or addition during transmission or storage. This can result in illegal access to computing resources and services, distortion of personal data or business records, or the conduct of fraudulent transactions, which may also lead to increase in credit authorizations, funds transfers' modification, and the issuance of unauthorized payments. the security measures that have come up as a solution are cryptography and steganography, which uses methods for rendering data unintelligible to unauthorized parties.

In the absence of strong security measures, an eavesdropping third party may get to know substantial information about the operational procedures of the system, including passwords, to overthrow any weak security mechanisms which may lead to catastrophic loss to a person or an organization. Cryptography and steganography forms the backbone of secret communication and their amalgam have provided wonderful results.

Some of the conventional methods for data security while transmission over a network involves either cryptography or steganography and their combination is rarely used. This work combines both the approaches to add a second line of defense and maintaining the confidentiality of information while transferring over the network. This work presents various methods where steganography and cryptography are blended to perform encryption and also to hide the data in the image. Hence providing two levels of security to the data being transferred. Thereby resulting in a more secure system as compared to when used alone.

II. Related WOrk

A. Selecting a Template (Heading 2)

X. Qing, et al., [1] gave a new approach where message is concealed in RGB components of an image thereby making use of all the planes and hence taking advantage of limits of Human visual system. In [20] author suggested LSB approach with some improvement is published. The suggested work states confidential data is only embedded in blue component of the RGB model. This approach helps in decreasing the deterioration of the output stego image as only blue components are being used to insert the confidential data in the image carrier. H.

Yang, et al. [14] proposed a variation of LSB steganography known as adaptive LSB image steganography, which uses a pixel adjustment approach for improvement of encoded image quality. This technique also helps in providing high payload capacity. Nouf A. Al-Otaibi, et al. [19], developed a new approach of blending steganography and cryptography resulting in two-layer data security for concealing the secret data on personal computers. They divided the system in 2 layers i.e., steganography layer and cryptography layer. LSB algorithm is used is used for steganography layer. For cryptography DES is used. Authors has also done study to improve hidden data capacity. Drawback of this method is that DES is not fully secure hence this method may fail to secure private data. K. B. Raja, et al. [18] made use of various blending of steganographic techniques like LSB, DCT and also the compressing is carried out to provide better security. In [16] one of the paper authors integrated RSA cryptography and audio steganography. The secret data is converted to encrypted text with the help of RSA algorithm and the encrypted text is hidden in audio using LSB audio technique. By combining steganography and cryptography it produces the higher level of security. In [13] authors proposed a new approach of image steganography on gray image combined with cryptography. The secret data is converted to cipher text using Vernam cipher and the data is encoded in the cover image using LSB with shifting. Here the sender and the receiver shares one-time pad key for Vernam cipher. The authors claim that message concealing capacity of this approach has increased drastically.

III. Methodology

In our research, we have used cryptography algorithms (like AES, Diffie-helman algorithm) and steganographic algorithms for images (like LSB, DCT, DWT).

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

A. *Embeding Process*

Both cryptography and steganography approaches are joined by performing encryption of the message using cryptography and concealing the encrypted text based on steganography. Diffie helman was first used for exchangenging the key.The Advanced Encryption Standard(AES) is used for performing encryption. The conversion of plain text to cipher text therefore takes place ttext using AES. The cipher text is then hidden in a cover image which could have any format like jpg, bmp, png etc. The stegno method could be any of the steganography algorithms(LSB, DCT, DWT) based on the suitability considering several performance factors like capacity, security and robustness. The output is the stego image embedded with the cipher text. The main issue arisen here s that how to select the technique for steganography. So proper evaluation is required for the aforesaid tehniques from which conclusions can be drawn so that proper techniques could be used according to the requirement. The figure 1 depicts the process of embedding the secret message in a cover image for the said approach.

B. *Extracting Process*

The extraction of message take place in reverse order of embedding process. The stego image with hidden cipher text is fed to the steganography algorithm chosen in the embedding process. The corresponding decoding method returns the cipher text which is then pass through AES decryption method to get the secret or plain text.

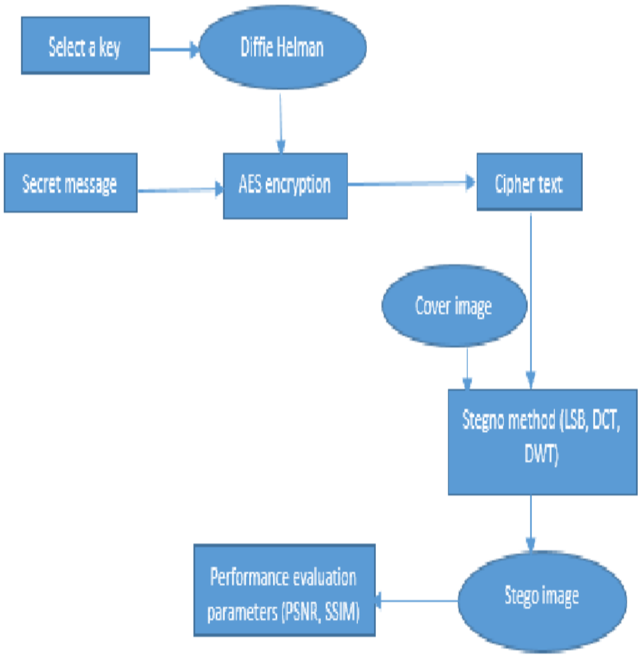


Fig. 1. Embedding Processes

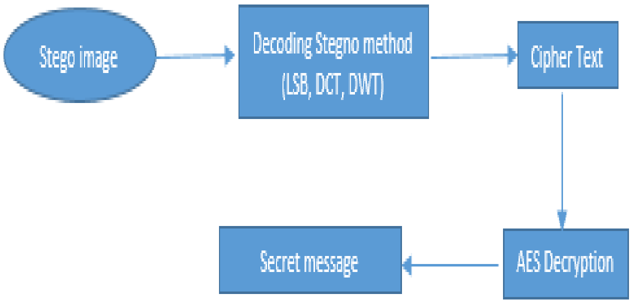


Fig. 2. Extracting Process

IV. Performance Analysis Measures

The performance evaluation should be carried out so that proper technique could be selected as and when required. All the three algorithms i.e., LSB, DCT and DWT need to be compared against various parameters for instance payload capacity, robustness, PSNR, SSIM etc.

Capacity: It represent the amount of encryption that could be embedded in the image. Its formula is given as:

$$Capacity = \frac{total\ no\ of\ bits\ embedded\ in\ the\ cover\ image}{total\ no\ bits\ in\ the\ cover\ imge}$$

MSE(Mean Square error): It refers to the square of error between cover image and the stego image. MSE helps to measure the distortion in the image. Its formula is given by equation 2

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-K(i,j)]^2 \quad (2)$$

I(i,j) and *K(i,j)* are the pixel values of cover image and stego image respectively. M and N represents the number of rows and columns in the input image.

PSNR(Peak Signal to noise ratio): It is defined as the ratio of the peak or maximum signal to noise with respect to original and stego image [8]. PSNR is measured in decibels (dB). Its formula is depicted as:

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right) = 20\log_{10}\left(\frac{MAX}{\sqrt{MSE}}\right) \quad (3)$$

MAX is the largest possible value in an image, *MSE* is the mean square error between pixel of two images.

SSIM(Structural Similarity Index): The SSIM is a method developed for estimating the perceptual quality of digital image and other media [3]. The computation of SSIM index is done on various windows of an image. If we are given two windows a and b of same size MxM then similarity measure would be computed by equation 4:

$$SSIM(a,b) = \frac{(2\mu_a\mu_b + c_1)(2\sigma_{ab} + c_2)}{(\mu_a^2 + \mu_b^2 + c_1)(\sigma_a^2 + \sigma_b^2 + c_2)} \quad (4)$$

μ_a and μ_b are the mean of the two windows a and b respectively, σ_a and σ_b are the variance of the two windows a and b respectively, $\sigma_a\sigma_b$ is the covariance of a and b, $C_1=(k_1L)^2$ and $C_2=(k_2L)^2$ where $L= 2^{\text{no of bits per pixel}}-1$ and $k_1=0.01$, $k_2=0.03$.

Here M is the no. of outcomes whose MRE is less than or equal to 0.25, and N is the total number of outcomes for a particular dataset. In the same way, MRE of PRED (50) and PRED (75) is less than or equal to 0.50 and 0.75 respectively. Finally, the estimated accuracy is proportionate to *PRED* (x) and inversely proportionate to *MMRE*.

V. Experimental Result and Analysis

Below images are used to carry out the analysis of various method of steganography with 50 bytes of secret text. Below table shows the properties of images used in testing. All the test images used are of different format for better analysis.

Fig. 3. Sample Images

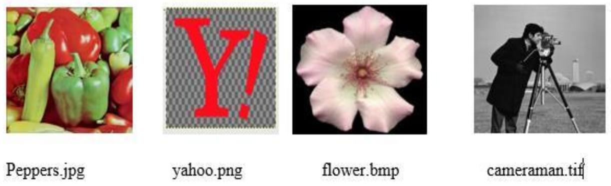


TABLE 1 SAMPPLE IMAGES PROPERTIES

Image type	Image size	Total pixels
Peppers.jpg	256KB	262144
yahoo.png	183KB	187704
Flower.bmp	21.7KB	22201
Cameraman.tif	64KB	65536

The LSB based Substitution steganography is applied on the four images with different format and various performance evaluation parameters are evaluated as shown in table 2.

TABLE 2. MSE AND PSNR FOR LSB

Image type	MSE	PSNR
Peppers.jpg	0.1716	60.5565
yahoo.png	0.0352	67.4334
Flower.bmp	0.3432	57.5468
Cameraman.tif	0.0205	65.0084

TABLE 3. MSE AND PSNR FOR DCT

Image type	MSE	PSNR
Peppers.jpg	3.7913	40.8593
yahoo.png	25.9718	29.2145
Flower.bmp	22.2600	29.8843
Cameraman.tif	8.7765	38.6976

TABLE 4. MSE AND PSNR FOR DWT

Image type	MSE	PSNR
Peppers.jpg	0.7635	49.3025
yahoo.png	0.0364	65.3225
Flower.bmp	0.8354	43.0435
Cameraman.tif	0.0139	66.6861

Fig. 3. PSNR comparison for different techniques for peppers.jpg

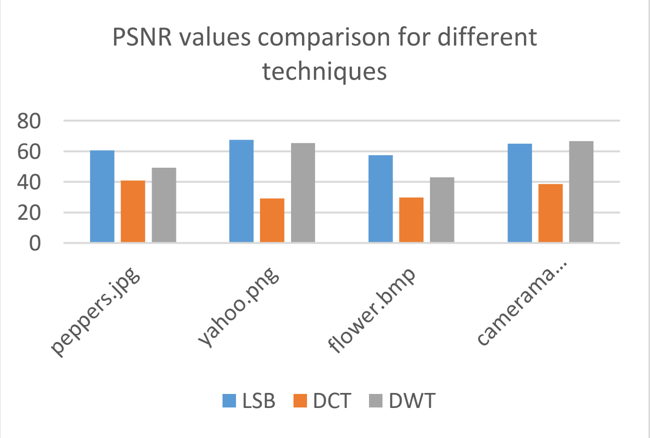


Fig. 4. PSNR comparison for various size of secret data

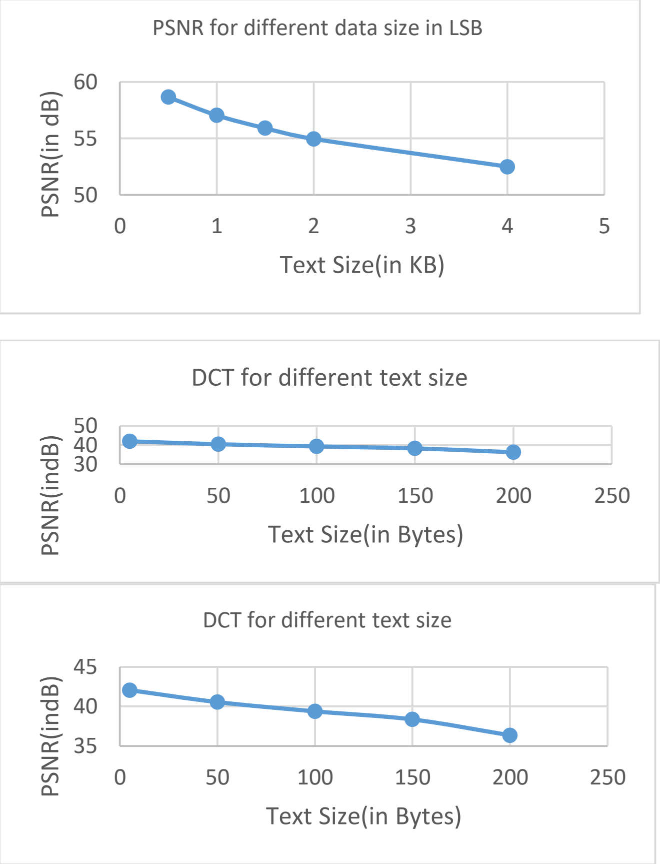


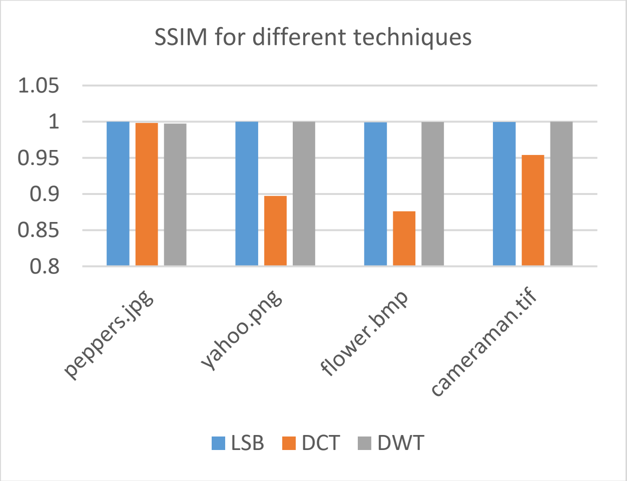
TABLE 5. SSIM VALUES FOR LSB, DCT and DWT TECHNIQUES

Image type	SSIM for LSB	SSIM for DCT	SSIM for DWT
Peppers.jpg	1.0000	0.9981	0.9997
yahoo.png	0.9999	0.8975	1.0000
Flower.bmp	0.9991	0.8762	0.9996
Cameraman.tif	0.9998	0.9540	0.9999

TABLE 6. COMPRASION WITH SEVERAL OTHER PARAMETERS

Parameters	LSB	DCT	DWT
Payload capacity	High	Medium	Low
Robustness	Low	Medium	High
Imperceptibility	High	Low	High
MSE	Low	High	Low
PSNR	High	Low	High
SSIM	Medium	Low	High
Encoding and decoding time	Low	High	Low

Fig. 5. SSIM comparison for different technique for different image format



VI. REFRENCES

[1]. X. Qing, X. Jianquan and X. Yunhua, "A High Capacity Information Hiding Algorithm in Color Image", Proceedings of 2nd IEEE International Conference on E-Business and Information System Security, Wuhan, China, 2010.

[2]. Patel H, Dave P. Steganography Technique Based on DCT Coefficients. International Journal of Engineering Research and Applications, 2(1):713–7, 2012.

[3]. https://en.wikipedia.org/wiki/Structural_similarity

[4]. X. Luo, F. Liu, C. Yang, S. Lian, and Y. Zeng, "Steganalysis of adaptive image steganography in multiple gray code bit-planes," Multimed. Tools Appl., vol. 57, no. 3, pp. 651-667, 2012.

[5]. Swanson M, Kobayashi M, Tewfik A Multimedia data embedding and watermarking technologies, Proc IEEE 86(6):1064–1087, 1998.

[6]. Moresh Mukhedkar, Prajkta Powar and Peter Gaikwad, "Secure non real time image encryption algorithm development using cryptography & Steganography", IEEE INDICON, 2015.

[7]. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[8]. https://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio

[9]. Kamaldeep Joshi, RajkumarYadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication", IEEE ICIIP, 2015.

[10]. Chih-Ching Thien and Ja-Chen Lin, A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function, Pattern Recognition 36, 2875-2881, 2003.

[11]. Mandal J.K. and Sengupta M., "Authentication/Secret Message Transformation Through Wavelet Transform based Sub-band Image Coding (WTSIC).", Proceedings of International Symposium on Electronic System Design, IEEE Conference Publications, pp 225 – 229, 2010.

[12]. Y. Lee, L. Chen, "High capacity image steganographic model", IEEE Proceedings on Vision, Image and Signal Processing, 147, 288 -294,2000.

[13]. Singla, Deepak, and RupaliSyal. "Data Security Using LSB & DCT Steganography in Images." International Journal Of Computational Engineering Research 2, 359-364, 2013.

[14]. H. Yang, X. Sun and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Journal of Radio Engineering, vol. 18, no. 4, (2009).

[15]. N. A. Al-Otaibi and A. A. Gutub, "2-Leyer Security System for Hiding Sensitive Text Data on Personal Computers", Lecture Notes on Information Theory, vol. 2, no. 2, (2014).

[16]. Ankit Gambhir and Sibaram Khara, "Integrating RSA Cryptography & Audio Steganography", IEEE ICCCA, 2016.

[17]. Nikhil Patel, Shweta Meena, "LSB Based Image Steganography Using Dynamic Key Cryptography", International Conference on Emerging Trends in Communication Technologies (ETCT), 2016.

[18]. K. B. Raja, C. R. Chowdary, K. R. Venugopal and L. M. Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", Proceeding of 3rd IEEE International conference on Intelligent Sensing and Information Processing (ICISIP), 2005.