International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

Analysis of Different Image Steganography with Encryption Techniques

Diksha Singh[1], Indira Bhattacharya[2], Manika Bhardwaj[3]

[1]B. Tech (Final Year), Information Technology, ABES Engineering College,Ghaziabad, Uttar Pradesh, India
[2]B. Tech (Final Year), Information Technology, ABES Engineering College, Ghaziabad, Uttar Pradesh, India
[3]Assistant Professor, Dept. of Information Technology, ABES Engineering College, Ghaziabad, Uttar Pradesh, India

---

Abstract *-: Digital communication witnesses a noticeable and continuous development in many applications in the Internet. Hence, a secure communication session must be provided. Steganography and Cryptography are two important techniques that are used to provide network security. This paper provides a fair performance comparison between various cryptography with steganography algorithms such as DES, AES, RSA and Blowfish. The resulting image of each encryption technique is analyzed through various quality parameters like MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio).*

Keywords: Cryptography, Encryption, AES, DES, Blowfish, Steganography, Least Significant Bit (LSB), Peak Signal Noise Ratio (PSNR), Mean Square Error (MSE),Secret Message, Cover file , Stego file, Stego key

1. INTRODUCTION

The security of data transmitted across a global network has turned into a key factor on the network performance measures. So, the confidentiality and the integrity of data are needed to prevent eavesdroppers from accessing and using transmitted data. In this paper, we have implemented various Cryptography techniques along Steganography which makes the message transmission highly secured. Encrypting the message makes it harder to decode for any eavesdropper and then hiding it in an image file conceals the very existence of such a file.

Problem Statement and Solution

Different encryption algorithms when used with steganography have different effect on the quality of the final obtained stego image. The quality in terms of the difference between the original and the final image plays an important role in concealing the existence of a stego file and its detection. Higher the difference between the original and final image makes it easier for detection of the stego file.

Primarily there are two measurement parameters calculate difference between two images:

1. **PSNR (Peak Signal-to-noise Ratio)**
   The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images.
   This ratio is used as a quality measurement between the original and a compressed image.
   The higher the PSNR, the better the quality of the compressed, or reconstructed image.
2. **MSE(Mean Square Error)**
   The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error.

This paper gives an analysis on PSNR and MSE values for steganography images when encrypted with 3 different encryption techniques:

A) DES

The **Data Encryption Standard** is a symmetric-key algorithm for the encryption of digital data. Although its short key length of 56 bits makes it too insecure for modern applications, it has been highly influential in the advancement of cryptography.

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

B) Blowfish

Blowfish is a symmetric-keyblock cipher, designed in 1993 by Bruce Schneier and included in many cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use.

C) AES

The **Advanced Encryption Standard** (**AES**), also known by its original name **Rijndael** is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. The number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

2. LITERATURE SURVEY

Under literature review we studied the various research papers on Cryptography, Encryption and Image Steganography to know the various efforts which has been made in this field:-

In [1] authors proposed a method for integrating together cryptography and steganography through image processing. In particular, they present a system able to perform steganography and cryptography at the same time using images as cover objects for steganography and as keys for cryptography .They showed that such system is an effective steganographic one (making a comparison with the well-known F5 algorithm) and is also a theoretically unbreakable cryptographic one.

In [2] authors provided a fair performance comparison between the various cryptography algorithms such as the AES, RSA, RC2, DES, 3DES, DSA where both types of symmetric and asymmetric techniques. They compared these parameters for both the symmetric key encryption and for the asymmetric key encryption. The parameters such as the tunability, key length, computational speed, and the type of attacks on the security issues are provided. As a result, the better solution to the symmetric key encryption and for the asymmetric key encryption was provided.

In [3]authors focused on the LSB modification technique provides an easy way to embed information in images, but the data can be easily decoded. The proposed scheme used in this paper encrypts the secret information before embedding it in the image. Certainly, the time complexity of the overall process increases but at the same time the

security achieved at this cost is well worth it. This cryptographic scheme can be used for other steganographic techniques also.

In [4] authors presented an analysis of LSB based steganography in color image. They used LSB based Steganography to embed the text message in least significant bits of digital picture. Least significant bit (LSB) insertion is a simple, common approach to embedding information in a carrier/cover file. Comparative analysis was made to demonstrate the effectiveness of the proposed methods. The effectiveness of the proposed methods had been estimated by computing the mean square error (MSE) and PSNR (peak signal to noise ratio),the analysis shows PSNR and MSE improved in the LSB methods.

3. PROPOSED METHODS

3.1 Algorithms Used

Encryption Technique AES, DES, Blowfish have been used and for performing Steganography, Least Significant Bit (LSB) techniques was used to implement this system.

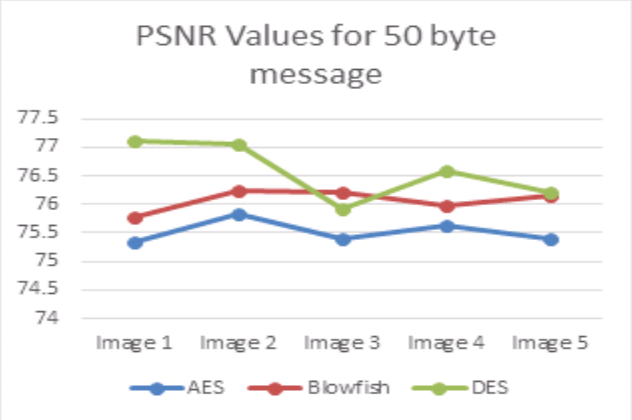
3.2 Simulation Setup

Image Pixel	225 X 225
Image Type	jpeg
Message Bytes	50 bytes, 500 bytes, 15000 bytes
Encryption Algorithm	DES, Blowfish, AES
Simulation Tool	Java Cryptography Encryption(JCE)

3.3 Impact of encryption with Steganography techniques for 50 bytes message length

The following graphs show the variation in PSNR and MSE values, when encrypted with DES, Blowfish and AES for 5 images of same pixel size but different hue patterns. The points to be noted are:

- For smaller file size, DES gives higher PSNR value and lower MSE values in general.
- AES does not work so well with steganography for smaller file size giving lower PSNR and higher MSE values.
- Hence, DES is more preferable for steganography for smaller message length.



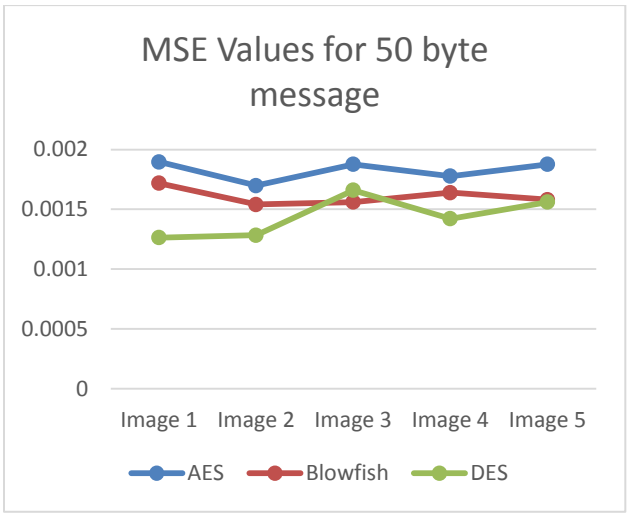


Image quality using DES with LSB steganography

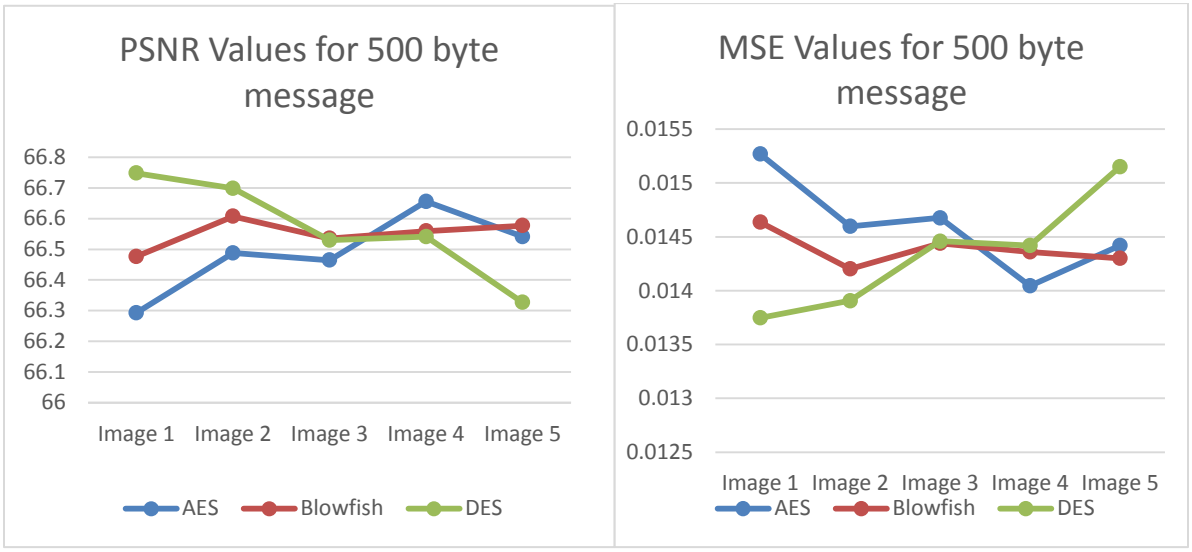
Image quality using Blowfish with LSB steganography

Image quality using AES with LSB steganography

3.4 Impact of encryption with steganography techniques for 500 bytes message length

The following graphs show the variation in PSNR and MSE values, when encrypted with DES, Blowfish and AES for 5 images of same pixel size but different hue patterns. The points to be noted are:

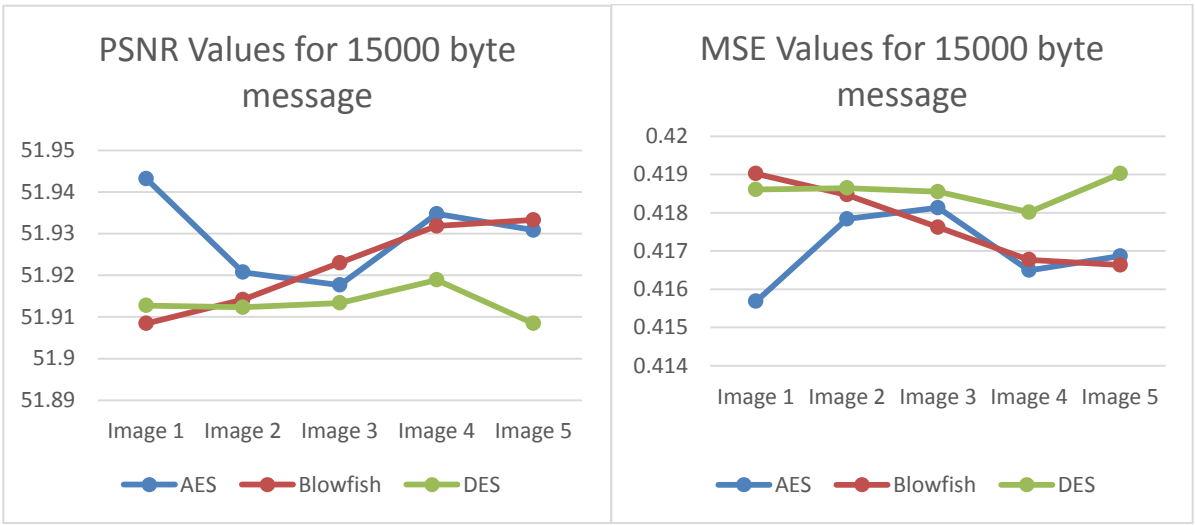
- For medium file size, the PSNR MSE values vary according to different hue patterns and do not show variation for different encryption techniques.



3.5 Impact of encryption with steganography techniques for 15000 bytes message length

The following graphs show the variation in PSNR and MSE values, when encrypted with DES, Blowfish and AES for 5 images of same pixel size but different hue patterns. The points to be noted are:

- For large file size, the PSNR MSE values vary according to different hue patterns though AES noticeably shows better results in some cases.



4. CONCLUSION

The LSB modification technique provides an easy way to embed information in images, but the data can be easily decoded. To make the transferred message more secure, the message bytes are first encrypted and then hidden in image files. There are various encryption techniques available for cryptography that affect the quality of the

steganography image. In general, for smaller message lengths, DES provides higher PSNR and MSE values thus making steganography more efficient.

5. FUTURE WORK

For this paper we have implemented LSB technique for hiding message files. In future other steganographic techniques like DCT, DWT, DFT etc. can be applied. The Asymmetric encryption techniques like RSA and Diffie-Hellman are out of the scope of this paper but could be added in future.

6. REFERENCES

[1]DomenicoBloisi and Luca Iocchi, “Image based Steganography and Cryptography”.
[2] AL.Jeeva, Dr.V.Palanisamy and K.Kanagaram, “Comparative Analysis of Performance Efficiency and Security Measures of some Encryption Algorithms”.
[3]Shailender Gupta, Ankur Goyal, Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography" in I.J.Modern Education and Computer Science, 2012, 6, 27-34, June 2012
[4] Naitik P Kamdar, Dipesh G. Kamdar and DharmeshN.khandhar, “Performance Evaluation of LSB based Steganography for optimization of PSNR and MSE” in Journal of information ,Knowledge and research in electronics and communication engineering , Volume –02, Issue-02 ,Nov 12 - Oct 13