Enhanced Information Hiding Using Symmetric Encryption Technique and Least Significant Bits Steganographic Design Approach

Ojeniyi Joseph Adebayo, Adeniji Adedapo Bolaji, & Idris Suleiman
Department of Cyber Security Science
Federal University of Technology
Minna, Nigeria
Ojeniyija@futminna.edu.ng, Adenijiadedapobolaji@yahoo.com, Sidris27@gmail.com

Ganiyu, S.O, and Alabi, I.O
Department of Information and Media Technology
Federal University of Technology
Minna, Nigeria
Shefiu.ganiyu@futminna.edu.ng, Isiaq.alabi@futminna.edu.ng

ABSTRACT

The security of information on the network has been a major issue due to mass distribution of information on the internet. Steganography and Cryptography are two important areas of study when it comes to security of the message communicated on the internet. Steganography deals with hiding of the existence of the message while Cryptography deals with changing the message to unreadable form. This research work uses Data Encryption Standard (DES) for the cryptography to encrypt the message after which a Least Significant Bit (LSB) embedding technique to hide the encrypted message inside a RGB image. The advantage of this approach is that it helps to increase the capacity of data that can be hidden in the cover and also increases robustness against eavesdropper.

Keywords: Steganography, Cryptography, Data Encryption Standard, Least Significant Bit, RGB image

1. BACKGROUND TO THE STUDY

In recent years communication has been done on the internet which involved sending of information from one person to another. As a result of this, criminal or attacker use this medium to perpetrate evil act by gaining unauthorized access into the information and cause harm to the person, organization or government. Security on the internet is very important and techniques like steganography, cryptography e.t.c have been employed years back to secure the information. Cryptography deals with changing of information to unreadable format and Steganography deals with hiding the message inside cover page (Text, Image, Audio and Video) and the algorithm employed to hide and extract the secret message in the cover page is called stego system. Image steganography is used in this research work and C# programming language is used to program the software application in Microsoft visual studio software Platform.

2. STATEMENT OF PROBLEM

The advent of internet has made it easier for people to access information globally. Because of this ease of access to information. Attackers find it easier to tamper with the confidentiality, integrity and availability of information. It therefore becomes important to come up with measures that can help secure this information from falling into wrong hands.

3. OBJECTIVE

The objective of this paper is to design and develop an application that encrypt information using Data Encryption Standard and to embed the encrypted information using Least Significant Bits.

4. RELATED WORK

Manmta and Parvinder (2013) discuss on how to improve Least Significant Bits Steganography technique for RGB color of images; LSB technique is one of the simple approaches of embedding message inside a cover file and due to its easy vulnerability by image manipulation. Improvement on this technique was a big achievement for Parvinder and Manmta. Format like BMP and GIF are the image conversion used. Insertion of message can be done in a gray scale, 8bits or 24bits image. When comparing LSB with other steganograhpy techniques like Bit Plane complexity segmentation (BPCS), discrete cosine transforms (DCT), IWT embedding e.t.c Stuti, Manpieet and Arun (2013) compare some of this image steganography embedding approaches by hiding a text file inside a cover image and perform a comparative analysis of three techniques LSB, DCT and DWT embedding techniques. The purpose was to solve the problem of low robustness and capacity and also to make the message in the stego image hard for human eye to detect.

In terms of capacity in Steganography, Shamim and Kattamanchi (2012) work on high capacity of data hiding using a LSB steganography. The peak signal to noise ratio and mean square error were used to perform the comparative analysis of the quality of the stego file. Another important aspect is the estimation of the bits that can be embedded inside the pixel of an image file; Ankita (2012) work on the pixel value differences of an image steganography using a secret key. The estimation was done using the largest difference value in the other three pixels that are close to the pixel target that was used and the high embedding capacity of data is enhance also by using the edge area of the image. One of the methods LSB that hide pixel of the image is called RGB method. This method search for identical bits between the message.

Koji and Malleswara (2013) proposed a novel secured RGB Least Significant Bits Steganography to enhance the quality of the stego image. When optimal adjustment pixel was introduced to the simple substitution of Least Significant Bit method, the quality of the image files were enhanced and when the method was compare with LSB benchmark method, a more efficient and quality of stego image were arrived act. One of the necessary thing in steganography is the stego key and this key is share between the sender and the receiver, although the security of the used algorithm lie in the hand of the steganographer. Smriti (2011) proposed a high capacitive and confidentiality of steganography using private key system by hiding the message in the spatical domain of the image used as the cover and 140bits key digital key signature is used to verify the stego image integrity. Marghny and Mohamed (2011) discuss on how to use genetic optimal key permutation to enhance data hide by LSB substitution approach. Genetic algorithm was proposed as a mean of selecting the best key and optimized method was used to test the standard of the image as well as key space and data size which help to strengthen the stego key against attack. Jawaha and Nagesh (2011) carried out a comparative analysis on three symmetric key technique which are DES, AES and Blowfish and it was discovered that Blowfish perform better in terms of block size, key size and speed when compared to the rest method. Shah and Bhavika (2012) work on how to improve the DES to enhanced better security and more robustness. This was carried out by using two key of four state 0,1,2,3 instead of the normal DES one key of two state 0,1 to replace the XOR operation in 16 round of DES algorithm.

5. METHODOLOGY

The architecture of this steganography work comprised of three stages which are encryption, embedding and extraction stages

5.1 Encryption Aspect

Symmetric key encryption also known as private key encryption was used in this application to encrypt the message and is defined as an encryption system that make use of one secret key to encrypt message and also decrypt it. Secret key on the other hand can either be word, number or a sequence of random letters put together. The algorithms applied in symmetric encryption system can be block algorithm called Block Cipher and stream algorithm called Stream Ciphers. Our application used block cipher and this block cipher break information down into blocks mostly 64bits and encrypt the data in each block. The DES and AES are commonly used in block cipher; we used the DES technique in this software.

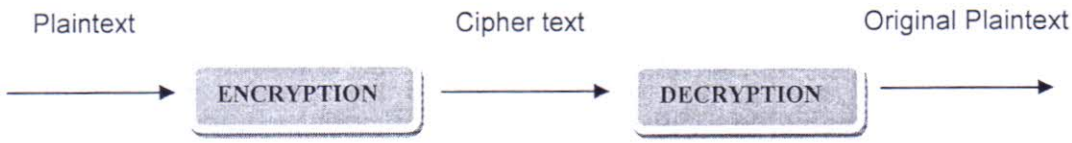

Fig 1 Cryptography process chart

5.2 Embedding Aspect

Embedding implied Insertion of secret message (Cipher text) into the cover (image). Image covers that are used in steganography are divided into three categories which are the Grey scale, binary and RGB (Red- Green- Blue) image. In this project work we used the RGB image that has a 24bits value and the white part of the image is represented by (11111111- 11111111-11111111) binary form while the black part is represented by (00000000-00000000-00000000). One of the advantage of RGB is that the image resolution is not changed if there is a slight change that occur with the RGB image and this help to maintain the quality of the image. There are many techniques used to embed information inside an image file in steganography and some of them are BPCS (Bit Plane Complexity Segmentation), LSB (Least Significant Bits) and IWT embedding. The software application used LSB embedding technique. Least Significant Bits design approach used the least significant bit plane of the image file by embedding the information inside the image directly.

5.3 Extraction Aspect

The receiver of the stego image needs to have the secret encryption key. Applied the secret key brings out the message and decrypt it. The format of the working process is shown below
The extracting process follows two steps which are:

5.3.1 Step 1

The stego key is applied to separate the image and encrypted message with the use of similar algorithm with the sender; the algorithm move through the image pixels till it find eight (8) consecutive zeros in the process picking LSB for pixel element(R, G and B) and join it to the empty value and once the eight bits of the value is done, it convert it back to character.

5.3.2 Step 2

The Cipher text is then decrypted by the encryption key. Since the 64bits is divided into two 32bits called Feistel scheme, the decryption take place similarly to the encryption process. The ciphertext is inputted back into the DES algorithm and the same permutation is performed, the difference is that the sub keys are applied in reverse manner or order. So if the password the receiver applied match the password that the sender used the message is decrypted.

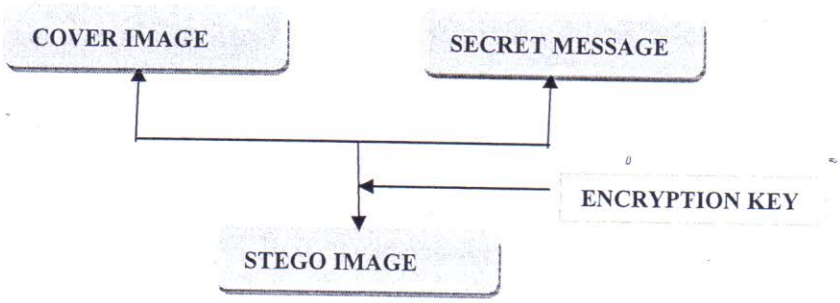

Fig 2 Extracting process chart

6. ALGORITHM AND MODEL DEVELOPMENT

Figure 3 below shows the model of the data encryption standard used in this work to encrypt the plaintext to ciphertext

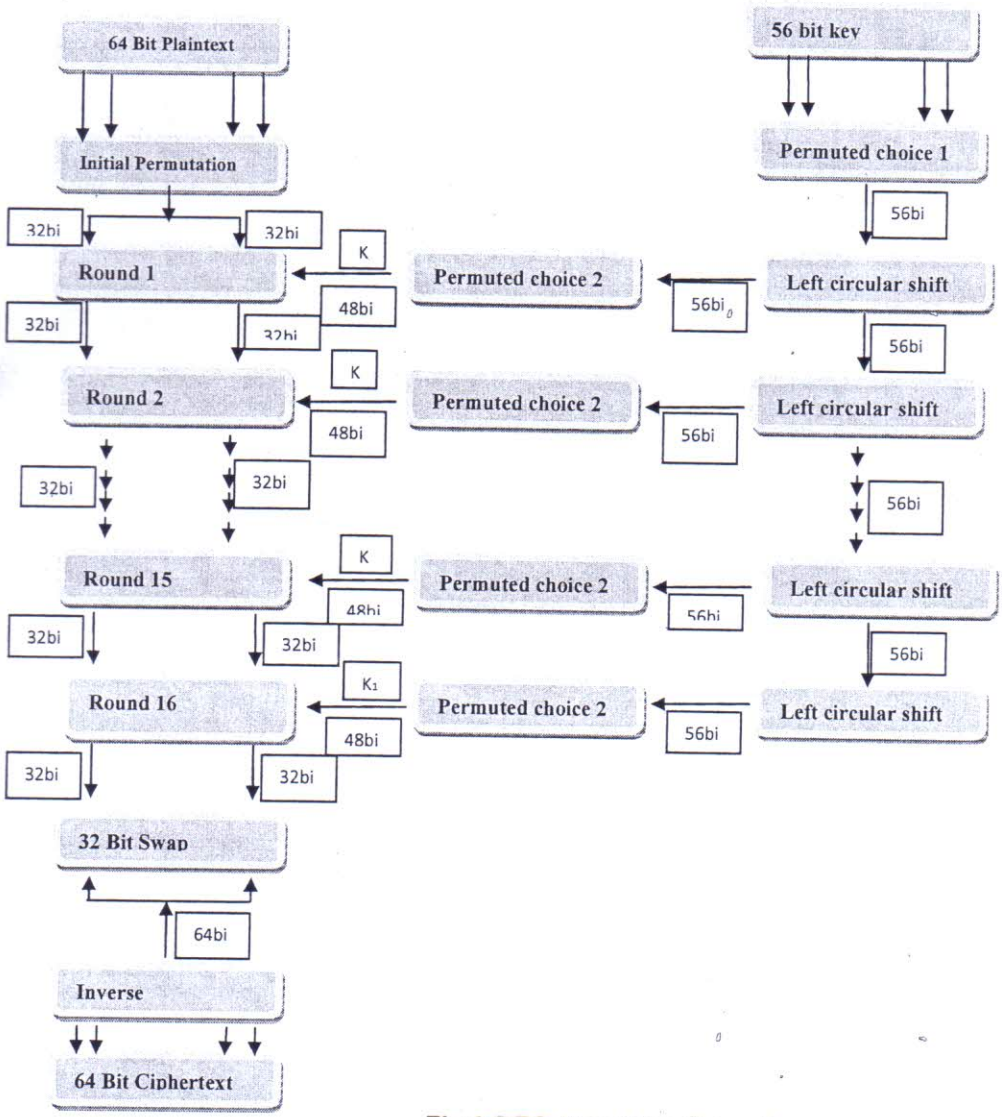

Fig 3 DES Algorithm flow diagrams

To embed the cipher text using the least significant bit techniques, the following steps are taken:

i. Select proper image cover file
ii. Perform the scan of the image row by row so that it can be encode in binary manner
iii. Encode the secret message inside the binary notation
iv. Calculate the size of the secret message and image.
v. Consider one pixel of the image selected
vi. Perform the segmentation of the image into Red, Green and Blue parts (RGB)
vii. Hide the secret message two by two inside each position of the pixel at the significant position of the last two.
viii. Set the image with the newly values that has be consider
ix. Set and save the image.

7. EXPERIMENTAL FRAMEWORK

The proposed model was experimented using Microsoft visual studio. The plaintext was encrypted using data encryption standard technique. The cipher text generated after the encryption was embedded using least significant bit method. Figure 5.1 below shows the encryption and message hiding interface while figure 5.2 shows the Extracting and decrypting interface.

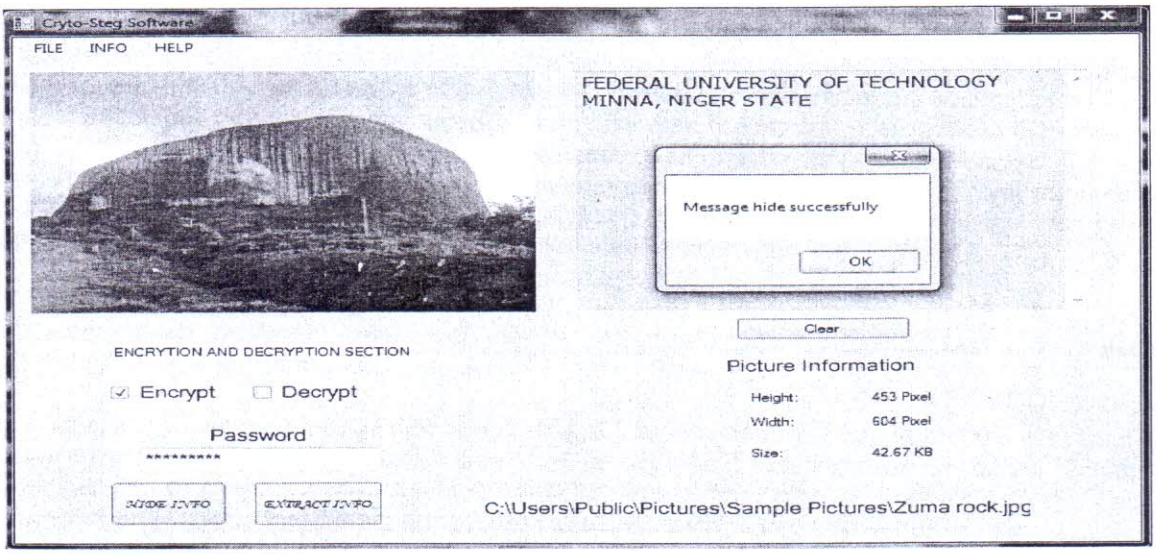

Figure 4

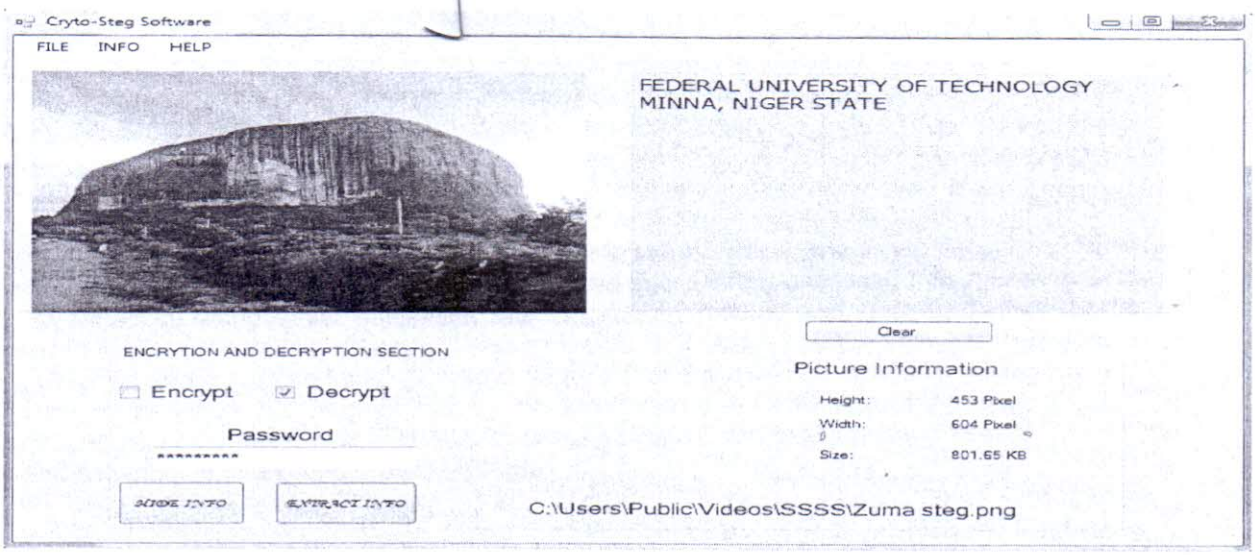

Figure 5

8. RESULTS AND DISCUSSION

8.1 Encryption and Hiding

In this section we discuss how the software can be used to encrypt message and hide the ciphertext inside an image file. From figure 5.1 above, we first upload our image from our system folder into the Picture Box. Once the image is uploaded we can now type the message we want to hide inside the Data TextBox, type the password inside the Password TextBox then click on the Encrypt CheckBox. After that, click on HIDE INFO Button. The Steganography-Cryto software will encrypt the message and then hide it inside the image. A Message Box pup up tell us that the message has be hide successfully. We then SAVE the new image called stego image in another folder

8.2 Extracting and Decrypting

In this section we explained how we can use the software to extract the cipher text of the message and decrypt it back to plaintext:

From figure 5.2, we first upload the stego image into the Picture Box. After that, we input the password used to hide the message inside the Password Text Box, and click on Extract button; the cipher text will displace on the Data Text Box. To decrypt the cipher text we click on the Decrypt Check Box and click on the Extract button. We have the message in plaintext and our image back.

Fig 6. Original image

Fig 7 Stego image

Figure 6 and 7 shows the image before and after embedding. They is no significant difference between the two image to the human eye and as such it will be difficult for an attacker to know it is carrying a message.

9. CONCLUSION

In conclusion steganography and cryptography have played a major role in the security of sensitive information communicated via internet. This work have successfully examined how message security can be enhanced using Least Significant Bits embedding method and Data Encryption Standard method to secured the secret message. One key (stego key) is used by the software to perform both the encryption and the embedding. The advantage is that the available space for hiding the written message on the image can be maximize by the application due to the size of the stego image. We recommend that compression should be incooperated before embedding, it will help to reduce the size and enhance better security of the message.

REFERENCE

[1] Ankita, S. (2012). Pixel value differencing image steganography using secret key. *International Journal of Innovative Technology and Exploring Engineering , 2*(1), 2278 - 3075.

[2] Atallah, M. (2012). A new method in image steganography with improved image quality. *Applied Mathematical Sciences , 6*(79), 3907 - 3915.

[3] Code project (2014). *Code project.Net 2014*. Retrieved from http://www. codeproject.com

[4] Dilbag, S. and Ajit, S. (2010). A Secure Private Key Encryption Technique for Data Security in Modern Cryptosystem. *BVICAM's International Journal of Information Technology, 2*(2), 0973 – 5658.

[5] Jawahar, T. and Nagesh, K. (2011). DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. *International Journal of Emerging Technology and Advanced Engineering, 1*(2), 2250 - 2459.

[6] Koyi, L. P. and Malleswara, R. (2013). A novel secured RGB LSB steganography with enhanced stego-image quality. Koyi Lakshmi Prasad et al Int . *Journal of Engineering Research and Applications, 3*(6), 2248 - 9622.

[7] Mamta, J.U. and Parvinder, S. S (2013). An improved LSB based steganography technique for RGB Color Images. *International Journal of Computer and Communication Engineering, 2*(4), DOI: 10.7763/IJCCE.2013.V2.238

[8] Manoj, K. M., Shiv, K. and Neetesh, G. (2011). An image steganography tool using adaptive encoding approach to maximize Image hiding capacity. *International Journal of Soft Computing and Engineering, 1* (2), 2231 - 2307.

[9] Marghny, M., Fadwa, A. and Mohamed, B. (2011). Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation. *International Arab Journal of e-Technology, 2*(1), 11-17

[10] Programmer2Programmer(2014). *Programmer2Programmer 2014*. Retrieved from http://www. Programmer2Programmer.Net

[11]Shah, K. and Bhavika, G. (2012). New approach of data encryption standard algorithm. *International Journal of Soft Computing and Engineering, 2*(1), 2231 - 2307.

[12] Shamim, A. L. and Kattamanchi, H. (2012). High capacity data hiding using LSB steganography and encryption. *International Journal of Database Management Systems, 4*(6), DOI: 10.5121/ijdms.2012.4605

[13] Smriti, G. (2011). High capacitive and confidentiality steganography using private key. *International Journal of Computer and Communication Engineering, 1*(1), 2249 - 7838.

[14] Stuti, G., Arun, R. and Manpreet, K. (2013).A comparison of image steganography techniques. *International Journal of Computer and Communication Engineering, 3*(1), 2278 - 5183.