International Conference on Information and Communication Technology and Its Applications (ICTA 2016)

Federal University of Technology, Minna, Nigeria

November 28 – 30, 2016

A Secure Method to Hide Confidential Data Using Cryptography and Steganography

John K. Alhassan[1], Idris Ismaila[2], Victor O. Waziri[3], and Adamu Abdulkadir[4]

Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria

[1]jkalhassan@futminna.edu.ng, [2]ismi.idris@futminna.edu.ng, [3]victor.waziri@futminna.edu.ng, [4]abdulcybersec2015@gmail.com

***Abstract*—The rate at which encrypted messages are being sent over the internet and other electronic means will easily capture the attention of hackers and possibly make them try to disrupt or even hack those messages so as view the original message. Steganography is designed to hide the presence of a message by hiding the secret message inside an innocent file. For effective security, steganography is sometimes combined with cryptography. In this paper, steganography and cryptography are combined to provide a robust system capable of encrypting a secret message using RSA algorithm. To hide the message, advanced LSB method is used. The original message is encrypted at the initial stage and then separated into two portions P1 and P2. An XOR operation is applied to the first portion (P1) using the odd location and to the second portion (P2) using the even position of the LSB+1.The Position of the LSB is then used to hide the XORed encrypted message.**

Keywords-cryptography; RSA algorithm; steganography; Least Significant Bit

I. Introduction

Cryptography and steganography are used to manipulate information so as to scramble or hide it. These techniques have a goal which is to protect the confidentiality, integrity and availability of information from unauthorized access [1].

Intruders or hackers can be successful easily due the fact that the information they usually obtain from computer systems is in a form that can be read easily and understood [2]. They may decide to reveal such information to their friends, modify it in order to misrepresent organizations, individuals, or even use it to carry out a serious attack. A viable solution to this issue is the use of advanced steganography. Advance steganography is defined as a technique of hiding information in digital form and then encrypting it. Contrary to cryptography, its goal is not to keep the information hidden from others but for them not to think the information even exist [3]. Steganography is derived from two Greek words steganos meaning “covered” and graphia which means “writing”, We could therefore define steganography as “covered writing”. The goal of steganography is hide the existence of a message. Digital images, videos, sound etc. are used as a carrier file to embed confidential information. Cryptography is a technique for encrypting plaintext and generating cipher text. A data that can be read easily and understood without the need for any software to decipher or decode it is known as plaintext or clear text. Changing the plaintext or clear text into one that cannot be easily understood is known as cipher text [4]. The method of disguising the clear text or plaintext so as to hide its substance is known as encryption. Generally, Cryptography scrambles information by maintaining the secrecy of such information and enable it to be transferred across an insecure channel so that unauthorized parties cannot understand it [5]. There are two other techniques that are related to steganography. These are watermarking and fingerprinting. They are concerned with the protection of intellectual property [6].

The two main branches of cryptography are cryptanalysis and cryptology. Cryptanalysis refers to applying different method so as to break into a system or cipher text without having the knowledge of the key. This is also referred to as breaking the cryptosystem [5]. Below are the four parts of all cryptographic process.

- Plaintext: Clear text or unscrambled text to be sent to another person or entity over the network. It could be a simple text document, personal information, a simple text document to be transmitted over the network.
- Cipher text: Cipher text refers to information that have been scrambled and difficult to understand by others unless with the knowledge of the correct key e.g. encrypted text to be transmitted over the network.
- Key: This refers to formula, mathematical value or process that can be used to encode or decode a message. Keys are used to convert messages or information to a cipher text [7].
- Cryptographic Algorithm: This could take a form of formula which can be used to encrypt or scramble a plain message into a form that cannot be easily understood by anybody unless with the knowledge of the key.

Basically, cryptographic algorithms can be broadly divided into two categories:

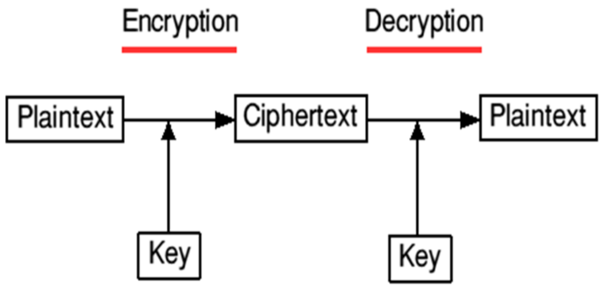

Figure 1. Basic concept of cryptography, adapted from [5].

- Stream algorithms (cipher): It operates on plaintext considering one byte at a time, where 1 byte can be special character, number, or character.
- Block algorithms (cipher): This algorithm operates on clear text, usually in groups of bytes called Blocks (Block algorithm). 64 bytes is the block size for modern algorithms, small enough to work with but large enough to deter code- breakers. Unfortunately, these days especially with the speed of the microprocessors, it is easy to break a 64-byte algorithm using the method of brute force.

For securing data, the following types of cryptographic schemes are used.

- Secret Key Cryptography (SKC): This is also referred to as symmetric- key cryptographic scheme which used a single key to perform both encryption and decryption. An example of this type of cryptosystem is AES (Advance Encryption Standard).

Fig. 2 is the illustration of the steps in secret key cryptography for a secure data transmission.

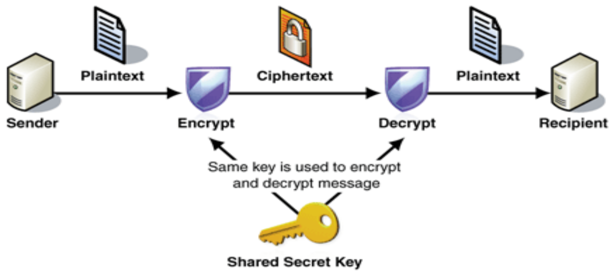

Figure 2. Symmetric cryptography, adapted from [5].

Even though this system is designed to improve the data security, its main problem lies on the distribution of keys between a sender and receiver. Therefore, for secure communication the key security becomes an issue with this approach.

A. *Public key Cryptography (PKC):*

This is also referred to as asymmetric key cryptography. It is designed to use public key for encryption and a private or secrete key for decryption. Both the public and private keys are required for the process [8]. A person with the possession of the public key can encrypt the message but cannot decrypt it. It can only be decrypted by the person with the knowledge of the private key. Examples of public key cryptosystems includes RSA, Elgamal Encryption, Diffie-Hellman. etc. Fig. 3 shows how the process works.

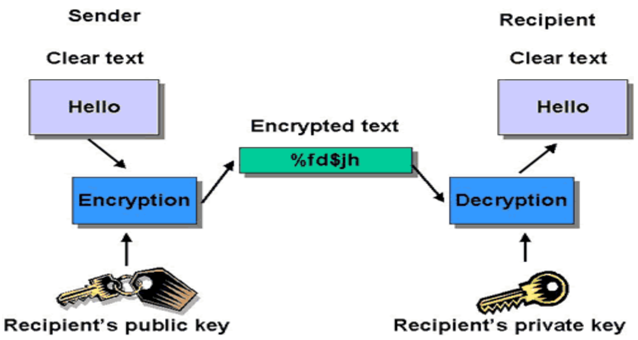

Figure 3. Asymmetric cryptosystem, adapted from [5].

B. *Steganography*

The goal of steganography is to hide information by making it difficult to observer to detect that information is present. Steganography is closely related to cryptography though they differ in terms of operation [6]. Fig. 4 shows the overview of the steganography system.

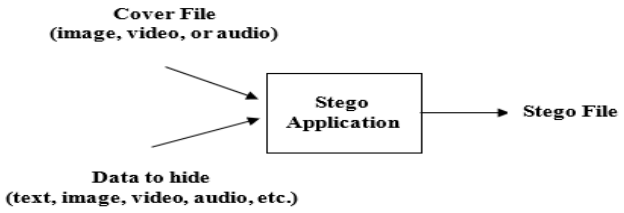

Figure 4. Steganography model, adapted from [5].

Covert object is a name given to the object through which message is hidden. The image that is obtained through embedding secret object or image into covert image is known as stego image [9]. The message that is hidden could be plaintext, image or cipher text.

Steganography system commonly used today are as follows:

- Audio Steganography: Unused audio bits are used to embed a secret message. This is due to the fact that every file have some area where messages can be hidden also known as unused bit.
- Image steganography: This is used to hide secret messages into a carrier image. The resulting image is called stego image.
- Video Steganography: This involves dividing the video into image frames and audio, thus the embedding is performed using the audio file.

II. LITERATURE REVIEW

Many works had been proposed and carried out in the area of steganography and cryptography. In the research work of [10], the researchers proposed an efficient data hiding system based on audio steganography and cryptography. The performance and efficiency of the system was evaluated for effectiveness and their results clearly shows that the application of cryptography and steganography to the system makes it more secured. They recommended the system to be used for establishing a secure communication on the Internet.

[11] in their research paper entitled “A novel security scheme for secret data using cryptography and steganography’’ proposed a security model. The authors combined Steganography and Cryptography. The confidential information was encrypted using Advanced Encryption Standard (AES) algorithm. Their model provided a two-layer security for secrete data. In addition, the system provided extraordinary insertion capacity and high class stego images.

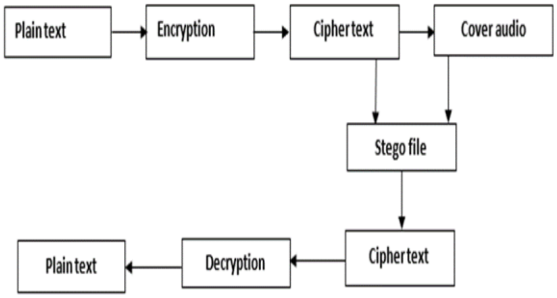

Figure 5. Flow of their system, adapted from [10].

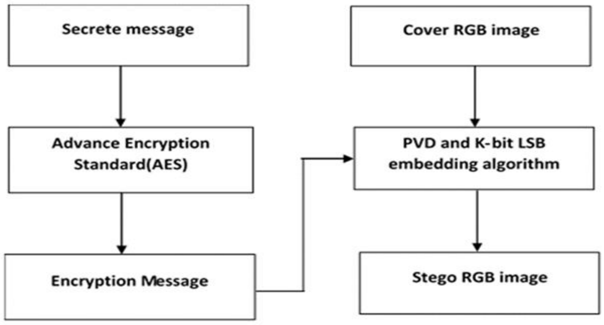
Secrete message
Advance Encryption Standard(AES)
Encryption Message
Cover RGB image
PVD and K-bit LSB embedding algorithm
Stego RGB image

Figure 6. Message embedding algorithm, adapted from [11].

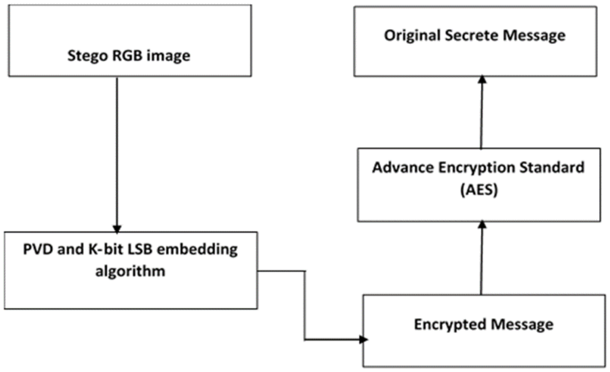
Stego RGB image
PVD and K-bit LSB embedding algorithm
Encrypted Message
Advance Encryption Standard (AES)
Original Secrete Message

Figure 7. Message extraction algorithm, adapted from [11].

In another paper by [12], the authors proposed an algorithm called Hash Least Significant Bit (H- LSB) with affine cipher that will provide more security to data in a networked environment. A number of images with different sizes of data hidden were tested on the system. Hence the system was efficient in hiding data inside an image.

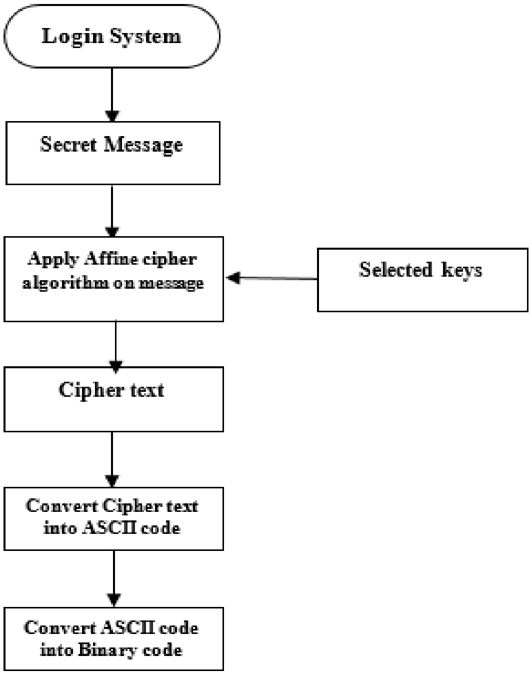
Login System
Secret Message
Apply Affine cipher algorithm on message
Selected keys
Cipher text
Convert Cipher text into ASCII code
Convert ASCII code into Binary code

Figure 8. Flow of the encryption phase, adapted from [12].

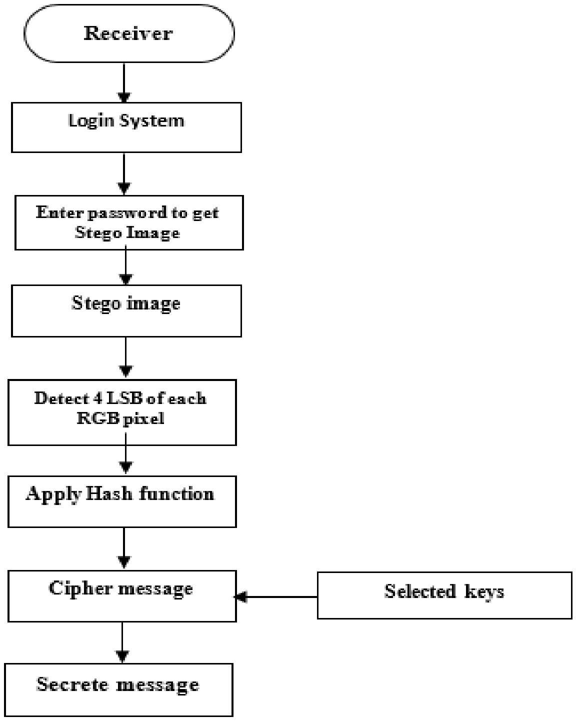

Figure 9. Flow of the decryption phase, adapted from [12].

[13] in their research proposed a steganographic method based on gray-level modification for true color images. Image transposition and secret key was used. The system used bitxor operation, stego key-based encryption and bit shuffling which were hidden in the host image pixel. Five

security level was utilized The proposed technique was evaluated using different image assessment metrics which produced interesting results based on imperceptibility and security.

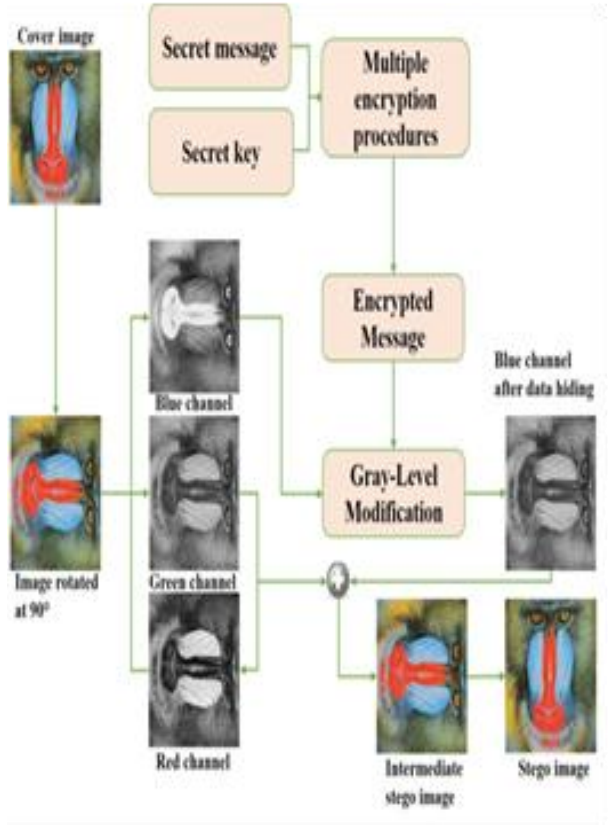

Figure 10. Pictorial representation of the framework, adapted from [13]

III. METHODOLOGY

A. Introduction

A secure and robust method for hiding information is the main aim of the proposed scheme. To achieve the requirement for steganography such as security, robustness and capacity, we considered combining steganography and cryptography.

In our proposed method, inserting the information into image file was achieved using the LSB bit manipulation. The message is encrypted using RSA algorithm. Image file as well as text files are converted into their binary equivalent before embedding. RSA was used to encrypt the information, the encrypted information is then inserted into the image file using the LSB algorithm. The extraction of the information is done at the side at the receiver. This required the hidden information file to be chosen first. After file selection, advance LSB is used to remove the scrambled information, which is then scrambled using RSA.

The proposed method for the embedding and extraction of information in image is presented below

B. Flowchart of the System

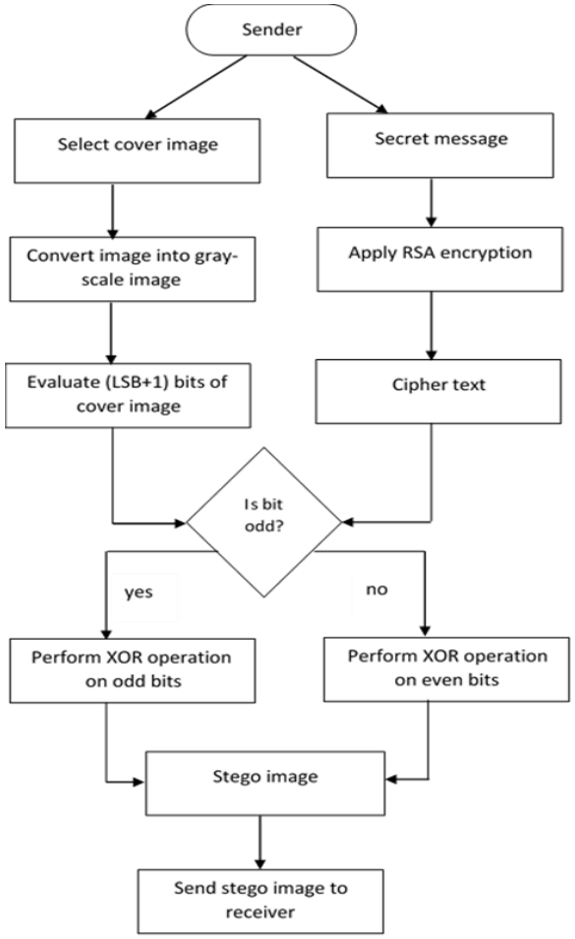
Sender
Select cover image
Secret message
Convert image into gray-scale image
Apply RSA encryption
Evaluate (LSB+1) bits of cover image
Cipher text
Is bit odd?
yes
no
Perform XOR operation on odd bits
Perform XOR operation on even bits
Stego image
Send stego image to receiver

Figure 11. The proposed text embedding flowchart

C. The Proposed Algorithm

LSB coding and RSA algorithm were used for the proposed algorithm. The text is scrambled using the RSA algorithm. Based on the system, the secret text is embedded inside an image. It is then converted into binary equivalent. To make it more secure, an XOR operation is applied. The message is scrambled with the help of RSA which is then inserted into the image file then into binary. The scrambled message is inserted into the file LSB bit of the separate block. The name given to the inserted image file is also called stego image

D. RSA Algorithm

RSA are initials for Ron Rivest, Adi Shamir, and Leonard Adleman. It is an asymmetric cryptosystem which means two keys are involved for encryption and decryption. It requires two large prime numbers to be selected after which the product is used to form a private and public key, which can be used to perform encryption and decryption of the information.

Below are the brief steps involved in RSA Algorithm.

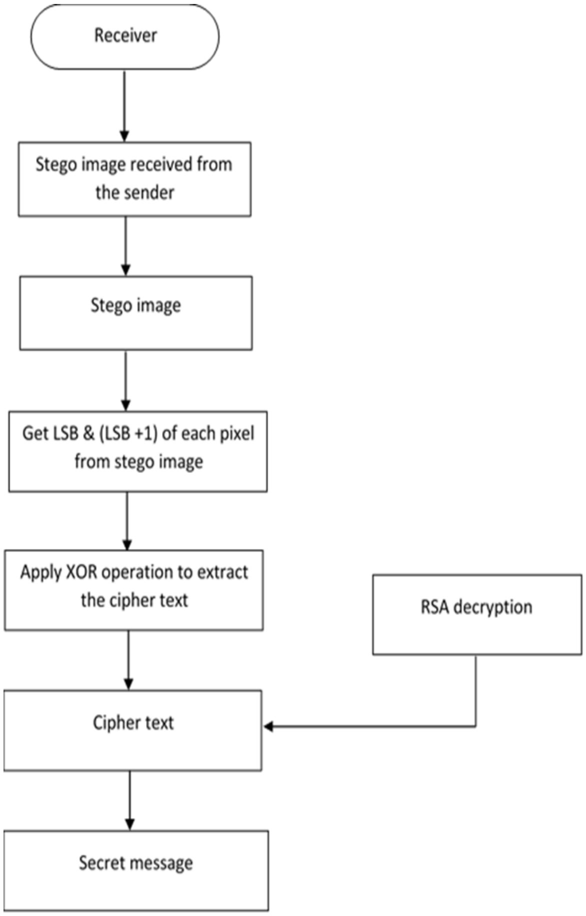
Receiver
Stego image received from the sender
Stego image
Get LSB & (LSB +1) of each pixel from stego image
Apply XOR operation to extract the cipher text
RSA decryption
Cipher text
Secret message

Figure 12. The proposed text extraction flowchart

1. *Select two distinct huge prime number p and q.*
2. *Calculate the modulo n as* $n = p * q$
3. *Calculate* $f(z) = (p-1) * (q-1)$.

Choose a random e satisfying $f(n)$ *and relatively prime to* $f(n)$ *i.e.,* $\gcd(e, f(z)) = 1$

4. *Calculate the number d such that* $d = e^{-1} \bmod f(n)$
5. *Encryption*: *Cipher text* $C = M^e \bmod n$
6. *Decryption* : *Message* $= c^d \bmod n$

E. Advance LSB Algorithm

The message embedding algorithm:
*Step One**:** Enter the encrypted message by means of RSA*
Step Two: Choose a cover image
*Step Three**:** From the cover image take pixels*
*Step Four**:** From the pixels take (LSB+1) bit.*
Step Five: divide encrypted text (two equal parts).
*Step six**:** Compute the XOR operation for the first portion of the encrypted message plus the pixel's odd position value*
Step seven: Compute XOR operation for the second portion of the encrypted message plus the pixel's even position value
Step eight: Obtain the entire xored of both the odd and even position pixel.
Step Nine: From the even position of the LSB bit pixel, save the xored value of the even.

F. Message Extraction Algorithm

Step One: Get the stego image
*Step Two**:** Obtain the LSB & (LSB + 1) embedded message bit of pixel*
Step Three: Use the XOR operation on the LSB & (LSB+1) bits
*Step Four**:** Obtain an XOR values of the entire pixel values*
*Step Five**:** From the XOR value, retrieve the bits.*
*Step six**:** Decrypt the retrieved data using RSA algorithm*
Step Seven: Secrete message obtained at this stage.

IV. RESULT

The actual cover image and the stego image based on the PSNR and MSE values have been shown together with their histogram which are also shown in figures.

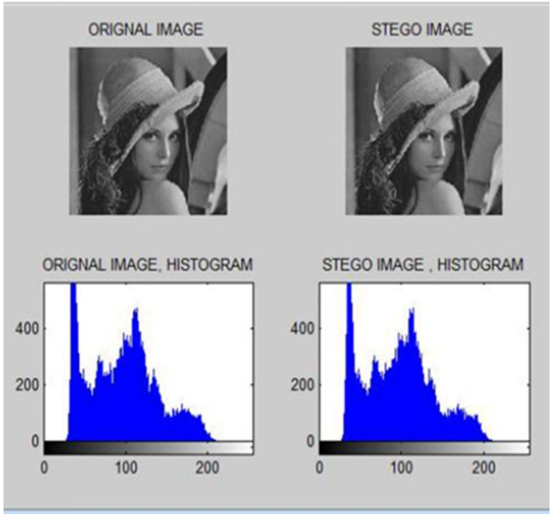

Figure 13. Histogram of the original image and stego image. PSNR between original and stego image is given as = 52.33dB MSE between original and stego image is = 0.1657

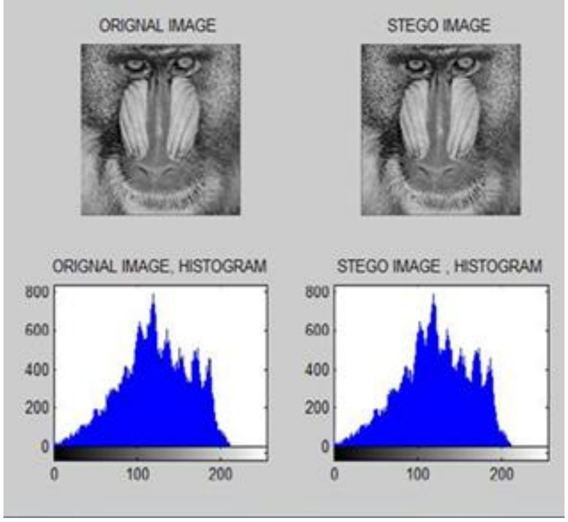

Figure 14. Original image and Stego image with their histogram PNSR between original and stego image is = 51.331dB MSE between original and stego image is =0.15942

V. CONCLUSION

Image steganography based on advanced LSB technique has been proposed and accomplished. The system which is achieved using advance LSB technique has the ability embed secret messages into cover images with no generation of any serious change. In this work, a novel method for concealing message within an image with fewer alteration in the bits of the image have been developed. This makes the technique safer and more robust than considering only LSB. The use of cryptographic technique which is the RSA algorithm helps in securing the secret information by making it difficult to understand the message without the key. This is due to the fact that RSA algorithm is a secure algorithm. The use of XOR operation in addition to the RSA algorithm makes the method more reliable especially when it sending information in an unsecured channel is needed.

REFERENCES

[1] C. A. Oluwakemi, A. S. Kayode, and O. J. Ayotunde, “Efficient data hiding system using cryptography and steganography”, International Journal of Applied Information Systems IJAIS411, 2012, pp. 6- 11.

[2] A. Chadha, Mallik, S., Chadha, A., Johar, R., and M. M. Roja, “Dual-Layer Video Encryption using RSA Algorithm.” arXiv preprint arXiv:1509.04387. 2015.

[3] K. S. Dipti, and B. Neha, “Proposed system for data hiding using cryptography and steganography”, International journal of computer application. 2010. Vol. 8, issue 9, pp .7-10.

[4] T. Jawahar, and K. Nagesh, “DES, AES and blowfish: Symmetric key cryptography algorithms simulation based performance analysis,” International journal of emerging technology and advance engineering, vol. 1, issue 2, pp. 6 – 12.

[5] A. Mehndiratta, ”Data Hiding System Using Cryptography and Steganography: A Comprehensive Modern Investigation”, 2015.

[6] V. Tyagi,"Data Hiding in Image using least significant bit with cryptography." International Journal of Advanced Research in Computer Science and Software Engineering 2.4, 2012, pp. 120-123.

[7] A. Monika, and M. Pradeep, “A comparative survey on symmetric key encryption techniques”, International journal on computer science and engineering,” 2012, vol. 4, issue 5, pp.877-882.

[8] A. J. Raphael, and V. Sundaram, “Cryptography and steganography – A survey,” International journal of computer technology application, 2011, vol. 2, issue 3, pp. 626- 630

[9] J. Mamta, and S. S. Parvinder, “An improved LSB based steganography technique for RGB color images,” International journal of computer and communication engineering, vol. 2 issue 4, pp. 513-51

[10] S. A. Laskar, and Hemachandran, K. (2012). “High Capacity data hiding using LSB Steganography and Encryption”, International Journal of Database Management Systems, vol. 4 (6),

[11] V. S. Phad, R. S. Bhosale , and A. R. Panhalkar, “A novel security scheme for secrete data using cryptography and steganography”. International Journal on Computer Network and Information Security, vol. 2, issue 6. pp 36-42.

[12] A. Muhammad, Abdullah, and R. H. HamaAziz, “New Approach to encrypt and decrypt data in image using cryptography and steganography Algorithm”, 2016, vol. 143 (4), pp. 11-17.

[13] K. Muhammad, Ahmad, J., Sajjad, M., and M. Zubair, “Secure image steganography using cryptography and image transposition”. arXiv preprint arXiv:1510.04413.