Vol 8. No. 3 – September, 2015
African Journal of Computing & ICT

www.ajocict.net

Secret Communication Using Image Steganography

E.P. Musa
Department of Computer Science
Ramat Polytechnic
Maiduguri, Borno State Nigeria

S. Philip
Department of Computer Science
Federal University Kashere
Gombe State, Nigeria
Simon Philip <simonphilip102@gmail.com>

ABSTRACT

Information security is one of the major concerns in this era of IT. The world now depends more and more on the computer and the related systems directly or indirectly for living. Cryptography and steganography are the most popular or widely used information security scheme or techniques. Steganography as a subject of consideration was born out of information security research as the previous mathematical techniques were vulnerable, and were hacked by cryptanalysts as computing knowledge developed over time. Steganography is the act of covert communications, meaning that only the communicating parties are aware of the communication. LSB replacement is adopted as an approach for embedding a message in a cover image. The algorithms for hiding data or message in a cover image, and extracting a message from a stego-image were implemented using C# programming language. In this paper, only 24-bit RGB bitmap files that use 1 byte (8-bits) for each of the 3 colours are allowed. In this type of bitmap image file, each pixel in the image is represented by 3 bytes – a byte each for the Red (R), Green (G), and Blue (B) components of its colour. This paper presents an experimental application of image steganography in a secure communication between two parties.

Keywords: Least Significant Bit (LSB), Steganography,Information Security, Encryption & Decryption

African Journal of Computing & ICT Reference Format:
E.P. Musa & S. Philip (2015): Secret Communication Using Image Steganography. Afr J. of Comp & ICTs. Vol 8, No. 3. Pp 1-8.

1. INTRODUCTION

Information security is one of the major concerns in this era of IT. The world now depends more and more on the computer and the related systems directly or indirectly for living. IT application stretches its tentacles from marketing to businesses, agriculture, weather exploration, scientific research, security, health and communications. The social media, distributed systems, intelligent systems, expert systems, decision support systems, executive information systems, transaction processing systems etc, are heavily depended upon in the contemporary world in day-to-day life as they have become part of man's life, especially in the developed countries. Steganography is the act of covert communications, meaning that only the communicating parties are aware of the communication. To accomplish this, the message is typically hidden within innocent-looking stego-image. Thus, the most important attribute of steganography is un-detectability, means that no algorithm exists that can determine the existence of a hidden message in an object [1].

Steganography as a subject of consideration was born out of information security research as the previous mathematical techniques were vulnerable, and were hacked by cryptanalysts as computing knowledge developed over time. According to *[2]* one example is the Vigenere cipher, historically known as the *chiffre indechiffrable* (undecipherable cipher) for centuries until it was cracked by Charles Babbage in 1854 and in a more general form by Kasiski in 1863. Despite the fact that the Vigenere cipher was not broken for 300 years, it is actually quite easy to cryptanalyze and recover the key that has been used.

Within the first week of July 2013 in Nigeria, complaints by bank customers were reported in *[3]* across the country and banks of details of personal account information demanded by scammers pretending to be their bankers over the internet. Once a customer gives such information he or she becomes vulnerable to fraud by such miscreants. Recently, American newspapers as reported in *[4]* carried the news about hackers who stationed themselves at ATM machines in different parts of the world and within cities in America and made away with money estimated forty five million ($45m) US dollars.

They made an ATM card that ATM machine security doesn't need to authenticate nor restrict amount to withdraw per day and smart enough to make away with such huge amount of money in hours.

2. RELATED WORK

Neil et al [5] on the subject Exploring Steganography: Seeing the Unseen, he referred to steganography as a 'covert writing' and that cryptography and steganography are cousin in the spycraft. In his research, he paid more attention to the selection of cover image as there is the tendency for some cover images ending in broadcasting the hidden message. He said that images are array of numbers representing light intensities at various points. He also noted that JPEG is lossy and most steganographers neither use them nor encourage its use but the 24 bit image format such as BMP image file formats does the job well. In his experiment, 25 files and 2 message files were carefully selected.

The first message file was 518 kb text message while the second was an image file. Using s-tools in the experiment he found out that there is a limitation of data size to hide in the cover image. He also laid emphasis on the need of security on the stego-image so as to protect the innocent looking stego from being intercepted, so there is a need to encrypt and decrypt in the source code when planning any stego project. They also asserted the need for hiding top secret project-device, aircraft, covert operation, using some steganographic method on an ordinary audio cassette tape. The alterations of the expected contents of the tape cannot be detected by human ears and probably not easily by digital means. Part of secrecy is of course in selecting the proper mechanisms.

Luis et al in their paper [6] a public-key steganography protocol allows two parties, who have never met or exchanged a secret, to send hidden messages over a public channel so that an adversary cannot even detect that these hidden messages are being sent. Unlike previous settings in which provable security has been applied to steganography and introduce computational security conditions for public-key steganography that is secure from the adversaries that have access to decoding oracle. Here the two parties communicate without prior exchange of secrets. The paper try to see how a passive adversary who only watch if steganography is used in the communication or not, and show secure exchange of key under Integer Decisional Diffie-Hellman (DDH) assumption. Trapdoor one-way permutations in mathematical function that is a probabilistic polynomial time was also applied. The RSA was used as the trapdoor one-way permutation family for pseudorandom number generation. ElGamal-based random-bits encryption was used, demonstrated with clear procedure of input and output for encryption and decryption.

The researchers employed the use of hybrid encryption schemes. They were able to model and defeat chosen-stegotext attacks where an intruder is not only active but monitors all communication between the parties and can even impersonate and change the messages passed across. Other work done was the chosen Hidden text and Chosen-Stegotext Security. The idea of 'must have a key' exchange between the communicating parties was established. The challenge raised was for the communicating parties to publish public keys for encryption and signatures without raising suspicion. This is where they opted that PKI (public key infrastructure) which publishes such public keys for every party is employed.

Christian et al in [7] as Neil also in their paper stated that steganography should be seen as a complement of cryptography. In his work on Digital Steganography he reiterated the Simmons "Prisoners' Problem": Two people locked up in a jail far apart want to communicate on plan to escape without the warder aware. He also see a stego-system as a cryptosystem with output property as such view it as a triple algorithm for key generation. Here only the two prisoners have the output of the key generation algorithm. They equally used the theoretic notions of probabilistic polynomial-time algorithm. The attack for the research was the chosen-message attacks, the adversary here may influence the embedded message but has no access to the algorithms for encoding and decoding and research is also subjected to passive attacks. The security that was targeted at achieving was perfectly, statistically and computationally secure steganography. Algorithms were developed for both input and output for the computationally secure steganography while the other two are more of theory than application.

3. ALGORITHM FOR STEGANOGRAPHY

As stated in [8], LSB substitution is the process of adjusting the least significant bit pixels of the cover image. It is a simple approach for embedding message into the image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8^{th} bit of each byte of the image is changed to the bit of secret message. For 24 bit image, the colours of each component like RGB (red, green and blue) are changed. LSB is effective in using BMP images since the compression in BMP is lossless. But for hiding the secret message inside an image of BMP file using LSB algorithm it requires a large image which is used as a cover. The simple algorithm for OPA explains the procedure of hiding the sample text in an image. This is the reason we employ using it.

Step1: A (LSB) are substituted with the data to be hidden.
Step2: The pixels are arranged in a manner of placing the hidden bits before the pixel of each cover image to minimize errors.
Step3: Let n LSBs be substituted in each pixel.
Step4: Let d= decimal value of the pixel after the substitution.
d1 = decimal value of last n bits of the pixel.
d2 = decimal value of n bits hidden in that pixel.
Step5: If (d1~d2)<=(2^n)/2
then no adjustment is made in that pixel
Else
Step6: If(d1<d2)
d = d – 2^n
If(d1>d2)
d=d+2^n.

This'd' is converted to binary and written back to pixel. This method of substitution is simple and easy to retrieve the data and the image quality better so that it provides good security.

4. METHODOLOGY

In this paper, LSB Replacement technique was adopted as the embedding method. The LSB replacement technique was used because of its simplicity.

The researchers used RSA encryption algorithm to encrypt the message before embedding it in a cover-image. RSA was chose as an encryption technique because of its encryption and decryption speed, and also its minimum storage requirement for the cipher text. C# was chosen as the programming language used to develop an application that demonstrates the use of image steganography in a secure communication.. The paper used only BMP images as the only cover image, and the data or document to be hidden inside the cover image are limited to not more than 35% of the size of the cover image. The algorithms for hiding data or message in a cover image (section 3.1), and extracting a message from a stego-image (section 3.2) were adopted in this paper.

4.1 Algorithm for Hiding the Secret Message as in *[9]*

Then procedure involved here includes:

1. Read the original image and the image/message which is to be hidden in the original image
2. Shift the image to hide in the cover image by X bits.
3. Hide the original image or cover image with 240 which is 11110000 So four MSB's set to 0. Because of this, only four LSB's are considered further.
4. The shifted hidden image and the result of step 3 are bitored. This makes changes only in the X LSB bits so that the image is hidden in the original image [10].

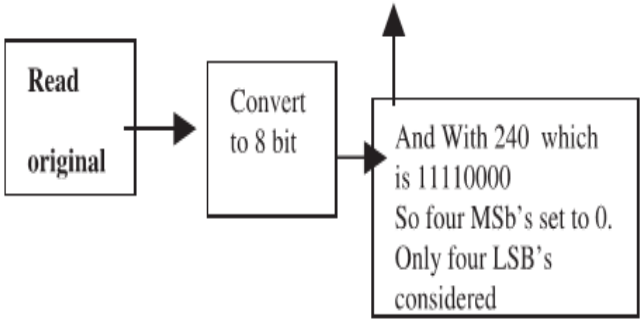

Figure 1: Block Diagram Showing How the Data is Hidden in The LSB

4.2 Algorithm for Extracting the Secret Message as in *[8]*

a) The stego-image is bit shifted by 4 bits since it was shifted by 4 bits to insert it into the original image.
b) This image is then ANDED with 255 i.e. 11111111, which gives the original image. It is ANDED with 255 because initially all the LSB's were made 0. Now it is recovered back.
c) To get the unit8 format we convert it back to unit8 which is the extracted image.

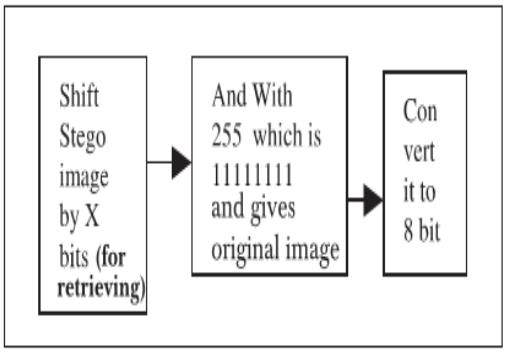

Figure 2: Block Diagram Showing the Algorithm for Retrieving Data From LSB

4.3: RSA Algorithm

We adopted this technique as the encryption technique to encrypt the message before embedding it. This algorithm is an asymmetric cryptographic algorithm that uses both private and public keys. The public key is used for encryption while the private is for decryption. The Key generation, encryption, and decryption algorithms are as follows:

4.3.1: Key Generation Algorithm

1. Generate two large random prime integers "p" and "q" of approximately equal size such that their product is the required bit length (e.g. 1024 bits) but p should not be equal to q i.e. $p \neq q$
2. Compute: $n = p \times q$
3. Compute phi $\varphi(n)$: $\varphi(n) = (p - 1)(q - 1)$
4. Choose an integer "e" between 1 and $\varphi(n)$ such that "e" and $\varphi(n)$ are coprime

i.e. $1 < e < \varphi(n)$ such that: $\gcd(e, \varphi(n)) = 1$

5. Compute the secret exponent "d":

i.e. $1 < d < \varphi(n)$ such that: $e \cdot d \equiv 1 \pmod{\varphi(n)}$

Meaning $de \% \varphi(n) = 1$ or $d = e^{-1} \bmod \varphi(n)$

6. The public key is $K_P = (n, e)$
7. The private key $K_S = (n, d)$

Where

"n" is the system modulus or simply modulus

"e" is the public or encryption exponent

"d" is the private or decryption exponent

"p, q and $\varphi(n)$" are kept private

After the keys are generated, the HOD can publish the public key $K_P = (n, e)$ to the public and keep his private (Secret) key $K_S = (n, d)$ secret. The DEAN can now encrypt his message with the HOD's public key using the below algorithm:

4.3.2 Encryption Algorithm

1. The DEAN obtains the HOD's public key $K_P = (n, e)$
2. Represents his message M_i as positive integer such that $M_i < n$
3. Compute the cipher $C_i = M_i^e \bmod n$
4. The cipher C_i is then reconverted from number to text (cipher text)

4.3.3 Decryption Algorithm

1. The HOD obtains the DEANS ciphered text C_i
2. Represent the ciphered text as a positive integer
3. Use his private key K_P to compute $M_i = C_i^d \bmod n$
4. The plain number M_i is then reconverted from number to text (plain text)

5. SYSTEM FLOWCHART

This section presents the steps or procedure the application runs through in form of a flowchart as shown in figure 3. The flowchart in figure 3 shows how the application allows secret communication using image steganography.

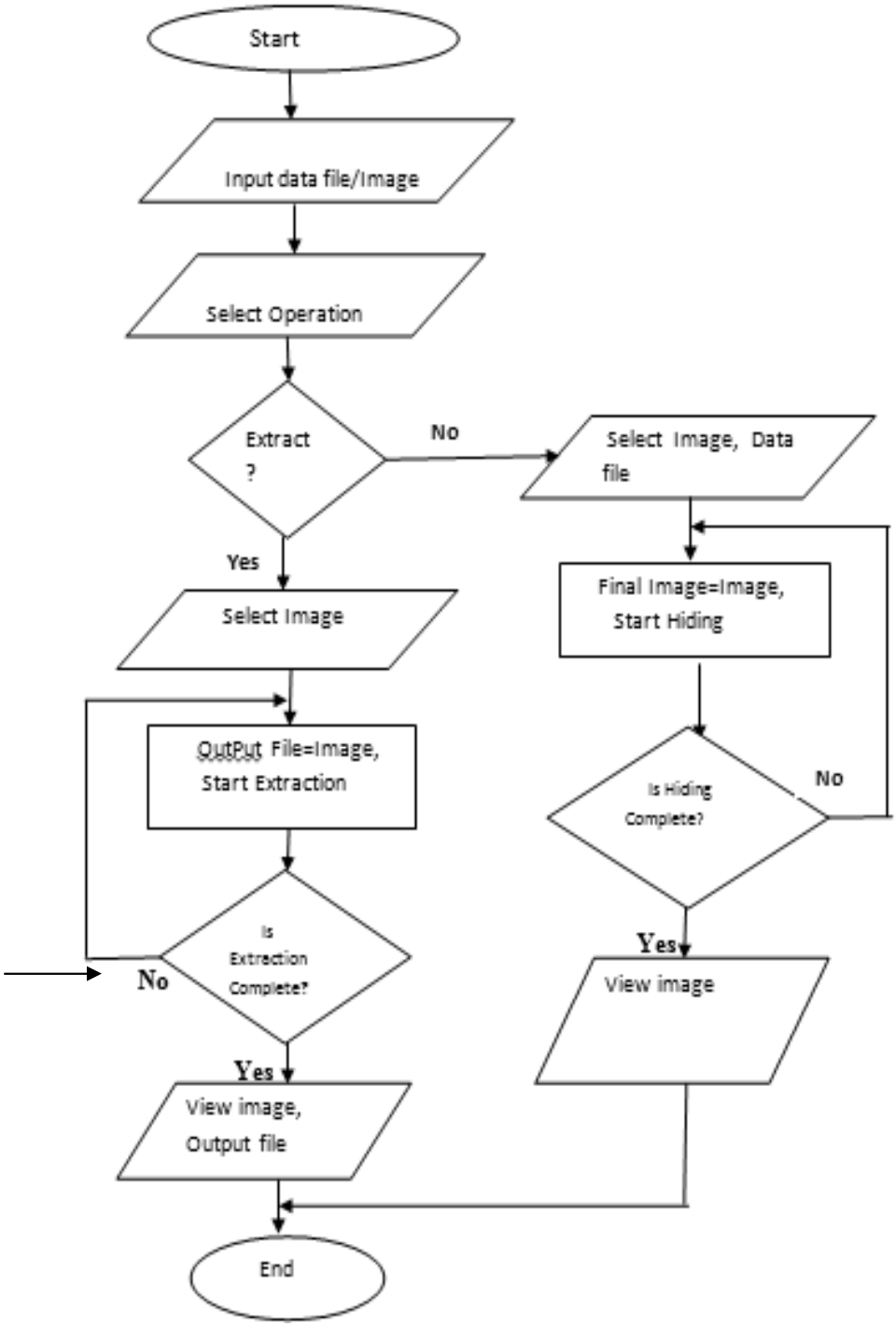

Figure 3: System flowchart

6. IMPLEMENTATION

The algorithms for hiding data or message in a cover image, and extracting a message from a stego-image were implemented using C# programming language. In this implementation, only 24-bit RGB bitmap files that use 1 byte (8-bits) for each of the 3 colours are allowed. In this type of bitmap image file, each pixel in the image is represented by 3 bytes – a byte each for the Red (R), Green (G), and Blue (B) components of its colour.

The application was tested and found to be working without errors and enables secret communication using image steganography. The result of the implementation is discussed in section 6.1.

6.1: Test Result

This section presents the test result of the application. Figure 4 allows users (Senders) to hide data or a message in a cover image in order to have a secure communication. Figure 5 allows users (Receivers) to extract the hidden data or message from the cover image (stego-image) in order to see the actual message embedded in the cover image.

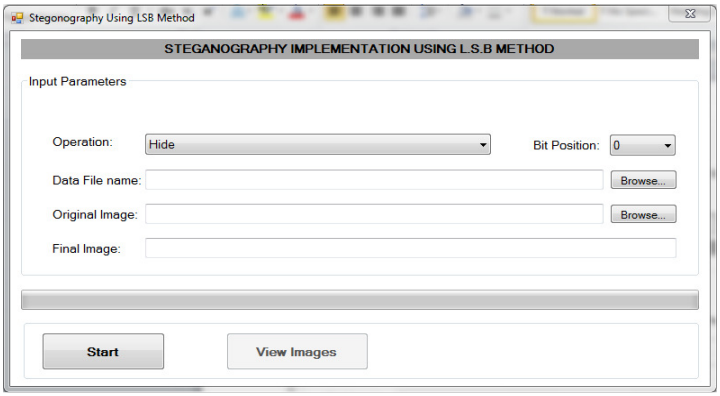

Figure 4: Interface for Hide Operation

The Hide operation user interface consists of the following elements:

a) Operation drop-down list: this is used to indicate which operation to perform. The possible options are (i) Hide (ii) Extract.
b) Bit Position drop-down list: this is used to indicate the bit position in the image pixel bytes where the data will be hidden.
c) Data File name: this field is used to select the data file we wish to hide in the image. The Browse button next to this field can be used to open a File Dialog box containing files on the computer from which the data file can be picked from.
d) Original Image: this field is used to select the image file in which data will be hidden. The Browse button next to this field can also be used as stated above.
e) Final Image: this field is used to indicate the name of the file to store the modified image after the data is hidden in it.
f) A progress bar to indicate the progress of the Hide or Extract operation depending on the selection made.
g) Start button: this button is used to fire the start of the selected operation.
h) View Images button: this button is used to open a window that displays the Original input image and Final output image side by side for comparison.

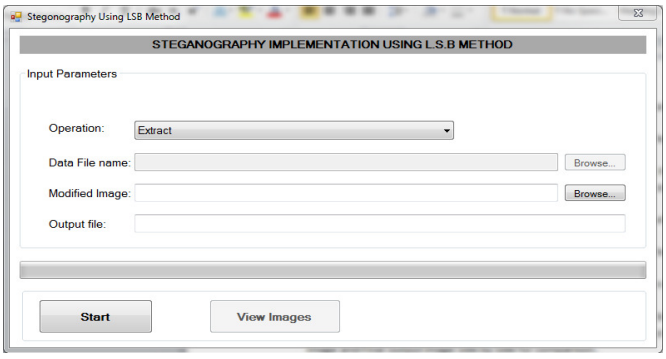

Figure 5: The extract operation interface

The extract operation interface consists of the following components:

a) Operation drop-down list: this is used to indicate which operation to perform. The possible options are (i) Hide (ii) Extract.
b) Data File name: this field will be disabled as it is not used by this operation.
c) Modified Image: this field is used to select the image file that contains the hidden data or message. The Browse button next to this field can be used to open a File Dialog box containing files on the computer from which the modified image file can be picked from.
d) Output file: this field is used to indicate the name of the file to store the data or message after its extraction from the modified image.
e) A progress bar to indicate the progress of the Hide or Extract operation depending on the selection made.
f) Start button: this button is used to fire the start of the selected operation.
g) View Images button: this button will be disabled as it is not used by this operation.

6.2 Cover-images in BMP File and Their Corresponding Stego-images Used in the Experiment. In this experiment, data files were hidden in the original images. In the first image which is the trademark logo of an Apple, a data file of 12.8kb was hidden, while in the second image which is the picture of Miss Godiya, a data file 45.1kb was hidden. Data file position in the images were tweaked in the RGB of the original images, hence introducing levels of noise in the original images proportional to the significance of the bits they are placed.

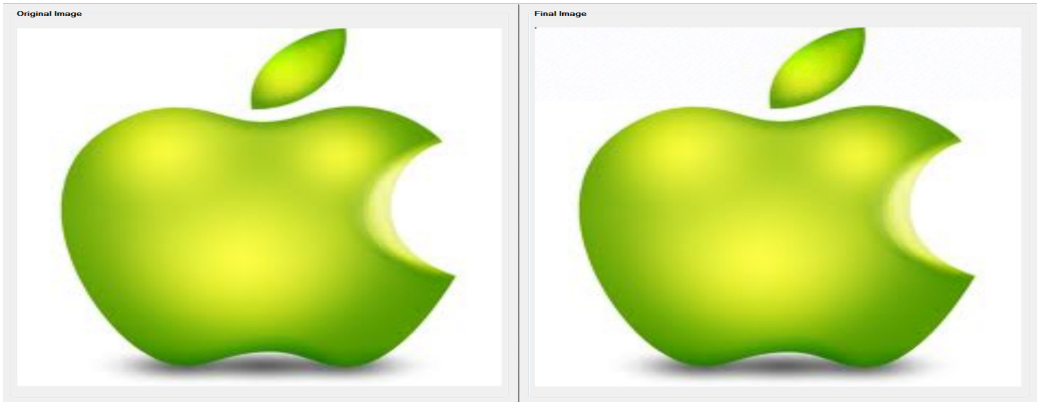

Figure 6: Apple original or cover image is 148Kb and Stego-image is also 148Kb, but the LSB replaced is the 3rd index or 6th MSB.

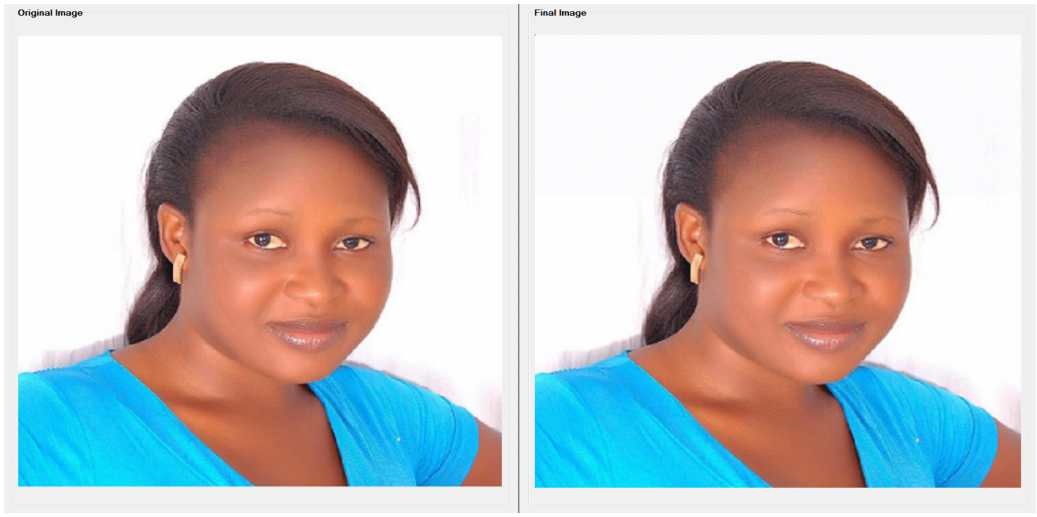

Figure 7: Miss Godiya's image or Cover image is 1. 08Mb and the Stego-image or final image is also 1.08 Mb, LSB used is the 3rd index or 6th MSB.

7. CONCLUSION AND FUTURE WORK

Steganography is one of the techniques used for securing data or information over the internet. In this paper, an experimental implementation of image steganography in securing data or information over a communication channel was carried out by using various types of input images as cover images and we discovered that;

(i) JPEG is not friendly with our program because the stego-image decreased in size by more than 50% of its original cover image. And when message is to be extracted from the stego-image the message is nowhere to be found it has evaporated.

(ii) The PNG files run well but the corresponding stego-images increase size to the original cover image.

(iii) BMP files when used: the files were stable i.e. the size of their corresponding stego-image was same with original images and extracted hidden-data were not in any way changed, meant the message successfully delivered.

This conforms to the literatures reviewed that discouraged the use of JPEG files as cover images in image steganography.

The researchers recommend that the message should be compressed in order to reduce the size of the message before embedding it in a cover-image.

REFERENCES

[1] Rajarathnam Chandramouli, Mehdi Kharrazi and Nasir Memon. Image Steganography and Steganalysis: Concepts and Practice. T. Kalker et al. (Eds.): IWDW 2003, LNCS 2939, pp. 35–49, 2004. (c) Springer-Verlag Berlin Heidelberg 2004.

[2] Dr Konstantin Blyus, Cryptography (G1032 and 860G1) Lecture notes 2012/2013 Session University of Sussex, Department of Mathematics. 2013. Unpublished.

[3] Techbaron.com: Woes of a Nigerian Internet Banking Customer.

[4] In Hours, Thieves Took $45 Million in A.T.M. Scheme - NYTimes.com http://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-t...

[5] Neil, F. and Jajodia, J. S. Exploring Steganography: Seeing the Unseen. George Mason University USA. 0018-9162/98/$10.00 © 1998 IEEE

[6] Luis, von A. and Nicholas, J. H. Public-Key Steganography. Computer Science Dept, Carnegie Mellon University, Pittsburgh PA 15213 USA

[7] Christian, C. Digital Steganography. IBM Research Zurich Research Laboratory CH-8803 Ruschlikon, Switzerland cca@zurich.ibm.com February 17, 2005.

[8] Neeta, D., Snehal, K. and Jacobs, D. *Implementation of LSB Steganography and Its Evaluation for Various Bits.* I EEE Digital Information Management, 2006 1st International Conference on, Bangalore, Pp173 – 178, 6-6 Dec. 2006.

[9] Daniela Stanescu, Mircea Stratulat, Voicu Groza, Joana Ghergulescu, Daniel Borca. Steganography in YUV color space. ROSE 2007 - IEEE International Workshop on Robotic and Sensors Environments. Ottawa - Canada, 12-13 October 2007

[10] Amirthanjan, R. Akila, R & Deepikachowdavarapu, P., 2010. A Comparative Analysis of Image Steganography, International Journal of Computer Application, 2(3), pp.2-10.