Secure Data Transfer Over the Internet Using Image CryptoSteganography

Osuolale, A. Festus

Abstract — The art of hiding information has been on for centuries and improvement and advancement have always accompanied information security to ensure the message gets to the intended recipient without compromise. Over the years, cryptography and steganography are the two major methods for securing, hiding and transmission of messages separately. The methods used information in order to cipher or cover their existence respectively. Cryptography is an art and science of hiding messages to introduce secrecy in data and/or information security while steganography is simply the art of secret writing, Crypto-steganographic method is aimed at amalgamating both the cryptography and steganography methods for a better information security. The primary purpose of this paper is to build up a new method of hiding secret text messages in an image, by combining cryptography and steganography. A new algorithm is proposed and implemented to achieve this. LSB method is used to hide the encrypted message into images while MSE and PSNR are used to acquire the quality of images.

Keywords - steganography, transmission, cryptography, algorithm, LSB, MSE and PSNR, images

1 Introduction

The internet is simply a large collection of networked computers. Man has grown to depend on the internet on a continual basis and have incorporated it into their lives. Due to this dependence upon the internet, terrorists have made the internet a potential attack platform [4].
Security, as of now, is the techniques developed to securely guard information and information systems store on computers. Potential threats consist of the destruction of computer hardware, software, theft, unauthorized use, or disclosure of data. Computer and the information they contain are often considered confidential systems because their use is typically restricted to a limited number of users. This confidentiality can be exposed to danger in a variety of ways. For example, data and information can be exposed by hackers, viruses and worms. Therefore, security can be defined as the resistivity degree to, or protection from harm. Security is one of the basic needs of man since creation. The case between the first two children (Cain and Abel) of the first human creature, Adam attest to this. It is also a statement of fact that security dynamics have evolved over the years [1].

Steganography is an ancient art and young science of communication which is hidden. A broad definition of the subject includes all means to communicate in a way such that the existence of the message cannot be noticed or identified.

Cryptography is an art and science of hiding messages to introduce secrecy in data and information security is known as cryptography. The word 'cryptography' was derived by combining two Greek words, 'Krypto' which means hidden and 'graphene' which means writing.

- *Osuolale, A. Festus is currently pursuing his PhD in Computer Science in the Department of Computer Sciences, the Federal University of Technology Akure, Nigeria, Cell line - +234 803 846 6943. E-mail: aofestus@futa.edu.ng*

1.1 Steganography

Steganography was gotten from two Greek words; steganos, which means "covered or secret", and graphy meaning (writing and or drawing). In a simple way, steganography is hidden writing, either it consists of invisible ink on paper or copyright information secretly hidden in an audio file, image file and or video file. Steganography is an ancient art and young science of communication which is hidden. A broad definition of the
subject includes all means to communicate in a way such that the existence of the message cannot be noticed or identified.

Cryptography, which actually ensures the confidentiality of the message, steganography includes another level and layer of security by keeping confidential even the fact that secret communication takes place. The corresponding protection goal is called undetectability

Today, steganography is most often linked with the high-level technology variety, where data is hidden within other data in a file. For example, a word document might be hidden inside an image file, as in the preceding story. This is mostly done by replacing the most redundant or least important bits of data in the original

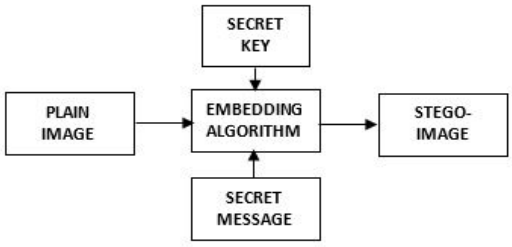


Fig. 1 Simple Stego System

file bits that are hardly missed by the human ear or eye

with hidden data bits. Figure 1 depicts simple stego system.

1.2 TYPES OF STEGANOGRAPHY

i. **Messages in Text:** Secret messages can be hidden in text format by rearranging the text of the carrier file, while maintaining the framework. One type of steganography is a program known as Spam Mimic. Based on a set of rules called a mimic engine by Peter Wayner, it encodes your message into what looks like your typical, quickly deleted Spam message. However, hiding a message in plain text is a thing of past, as people are suspicious of irrelevant text.

ii. **Messages in Images:** most used security measure in steganography.

iii. **Messages in Audio:** data is secretly hidden in the third layer of encoding process of MP3 file. Messages in audio are always sent along with immediate surrounding area noise. The data is hidden in the heart of the third layer encoding process of MP3 file, namely the internal loop during compression. The internal loop limits the input data and increases the step size until the data can be coded with the available number of bits. The data is compressed, encrypted and then hidden in MP3 Bit Stream.

iv. **Messages in Video:** adding data into multimedia data has gained attention increasingly lately. This method of encryption is just same as that of audio steganography. Video files are generally very good carrier files since they have a lot of irrelevant bits.

1.3 CATEGORIES OF STEGANOGRAPHY

Secret key steganography usual uses a well-known public algorithm, and relies on a secret key chosen by the two parties communicating beforehand. This key is needed to both embed and extract the hidden information, and if the right key is not used, it cannot be known if data is actually hidden in a given cover object.

Public key steganography requires the sender using the recipient's public key to embed the information, which can only be recovered using the recipient's private key. This is analogous to how the public key architecture works in cryptography. The interesting characteristic with public key steganography is that even the sender should not be able to observe the secret message in the resulting stego object.

Pure steganography does not require any prior exchange of information between the two parties communicating and relies on secret through obscurity. This means that the algorithms are not generally known, and therefore the level of testing is also unknown, making the tool unproven. One has to go on faith alone in those involved in the tool's creation to be assured covert communication. numerous instances of the false sense of security through obscurity can be cited.

1.4 CRYPTOGRAPHY

This is an art and science of hiding messages to introduce secrecy (figure 2) in data and information security is known as cryptography. The word 'cryptography' was derived by combining two Greek words, 'Krypto' which means hidden and 'graphene' which means writing.

The origins of cryptography are found in Egyptian and Roman civilizations. The first known evidence of

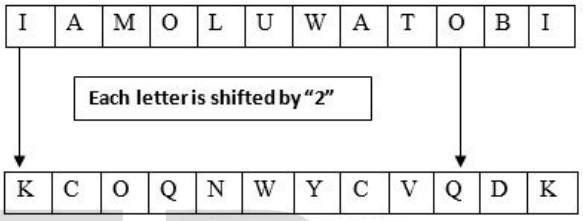


Fig. 2 Ceaser's Cipher

cryptography can be linked to the use of 'hieroglyph'. Some four thousand (4000) years ago, the Egyptians used to communicate by messages written in hieroglyph [5].
The four major security objectives of Cryptography are: Data integrity, Confidentiality, Non-repudiation and Authentication. The three classifications of cryptography are Symmetric-key cryptography, Public-key (asymmetric-key) cryptosystems and Hash function.

Cryptography primitives (Table 1) are the tools and procedure required in Cryptography that can be selectively used to provide a set of security services desired:

i. Encryption
ii. Digital Signatures
iii. Hash functions
iv. Message Authentication Codes (MAC).

Table 1
Primitives that can achieve a particular security service on cryptography

Primitives	Encryption	HASH function	MAC	Digital Signature
Confidentiality	Yes	No	No	No
Integrity	No	Sometimes	Yes	Yes
Authentication	No	No	Yes	Yes
Non-repudiation	No	No	Sometimes	Yes

1.5 Crypto-Steganography

Cryptography and steganography can be used to provide security to data, but each of them has a problem. Cryptography problem is that, the cipher text looks meaningless, so the attacker will suspend the transmission or make more careful checks on the information from the sender to the receiving party. Steganography problem is that once the presence of hidden information is known or even suspected, the message is become revealed. In this research, a combination technique for data security is been proposed using Cryptography and Steganography techniques to improve the information security. Firstly, the Advanced Encryption Standard (AES) algorithm would be remodified and used to encrypt the private message. Secondly, the encrypted message would be hidden using a steganographic method. Therefore, two levels of security would be provided using the proposed hybrid technique. In addition, the proposed technique provides high embedding capacity and high quality stego images. By combining cryptography and steganography, the data encryption can be done by a system (figure 3) and then embed the encrypted text in an image or any other media with the help of stego key [9]. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over the internet [8].

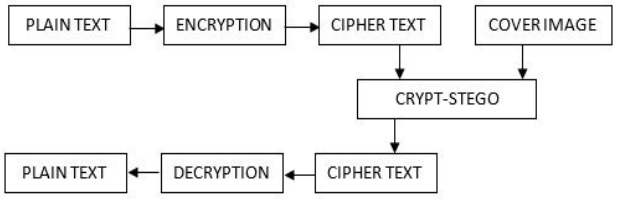


Fig. 3 Crypto-Steganographic System

2 Related Works

[12], With The development of data techniques the problem of data security becomes more and more important. The use of data has grown widely in the past years. Furthermore, many users can easily use tools to synthesize and re-edit multimedia information. Thus, security has become one of the most important problems for sharing new information technology. It is necessary to protect this information while communicated over insecure channels.

[6] proposed a model for security enhancing in image steganography that uses the neural network and visual cryptography. Visual cryptography is a renowned technique to protect data which is image based. The secret data is encrypted using AES algorithm. The cover image is divided into blocks and energy coefficient for each block is identified using IWT. The neural network is used to identify the best location in host image in order to embed the secret data. LSB embedding technique is used to embed the secret data into high energy locations of cover image. Inverse IWT is applied on stego image in order to negate the effects of IWT. Later stego image is brought back to original shape by using data re-arrangement process. During decryption the 2 shares of image are retrieved and inverse visual cryptography is applied and later message is extracted and decrypted.

[16] proposed a technique for protection of image in open wireless channel. The secret image is embedded in the cover image using LSB technique from spatial domain. Then the stego image is divided into 8*8 blocks. The divided stego image is encrypted by double random phase encoding. Double random phase encoding transforms the image into white stationary noise. In the first phase of double random phase the image is multiplied by first random phase mask. Then the, multiplied image is transferred from time domain to frequency domain by applying Fourier transform. In the final phase the image is convolved with the second random phase mask.

[14] presented an enhanced safe data transfer scheme in smart Internet of Things (IoT) environment. They proposed a technique that employ an integrated approach of steganography and cryptography during data transfer between IoT device & home server and home server & cloud server. The sensed data from IoT device is encrypted and embedded in the cover image along with message digest of sensed data and send to the home server for authentication purpose. At the home server the embedded message digest and encrypted data version is extracted. The received digest is compared with newly computed digest to ensure data integrity and authentication. The same procedure is carried out between home server and cloud server.

[2] integrated RSA cryptography and audio steganography. The secret message is converted to cipher text using RSA algorithm and the cipher text is hidden in audio using LSB audio technique. By combining steganography and cryptography it produces the higher level of security.

[7] proposed a new method of image steganography on gray images combined with cryptography. The secret message is encrypted using Vernam cipher and the message is embedded in the cover image using LSB with shifting. Here the sender and the receiver share one-time pad key for Vernam cipher. The authors claim that data hiding capacity of their method has increased to 100%.

[17] presented 2 new approaches to secure data. In the

first approach each byte of the secret image is encrypted using S-DES algorithm to produce an array of encrypted pixels. Each element of array is then divided into 2 parts where first part contains first 4 MSB's and second part contains remaining LSB's. Then each pixel value is converted with alphabets from A to P where A is assigned to 0000 and P to 1111. The output will be an encrypted image containing text. The encrypted image is then embedded in cover image by XOR method. In the second approach they simply encrypted the secret image using S-DES algorithm and embed it in the cover image as stated above.

[10] has given a hybrid approach for image security that provides good encryption quality. The secret image is encrypted using blowfish algorithm to produce the cipher image. Then the encrypted image is embedded using LSB technique in the cover image. Blowfish algorithm is lossless and highly secured encryption technique.

[15] proposed a method that increase the security of data transfer by combining cryptography and steganography. Mp3 file is taken as the cover media and the secret message is encrypted using AES algorithm using a key that has been processed by MD5 hash function. The secret message was inserted in the homogeneous frame in mp3 files with addition of a key code. The MD5 algorithm is a widely used cryptographic hash function used to verify data integrity.

[11] came up with space domain steganography. Secret image and carrier image are taken of same size. Pseudo random noise sequence of both image is generated which is dependent on key. A single plane (R or G or B) is selected from both the images. Given plane of the carrier image (CI) is divided into set of 16 pixels and then selection of the pixels is done in the similar manner as they appear. Similarly given plane of secret image (SI) is sliced into a set of 16 pixels based upon column select sequence and row select sequence sequences. Then selected pixel will be ciphered using second key and then embedded into the carrier image.

3 The Proposed System

Cryptography and steganography guarantees perfect secrecy by using the AES algorithm and Least Significant Bit algorithm, which is the technique adopted for this work.

3.1 ADVANCE ENCRYPTION STANDARD (AES)

Figure 4 shows the schematic structure of the Advanced Encryption Standard (AES). The original name of AES was Rijndael, as it was named after the developers of the algorithm; Vincent Rijmen and Joan Daemen. AES uses symmetric key encryption where the same key is used for encrypting and decrypting the data, and the main challenge is to exchange that key with complete privacy as if this key is found then all the encryption process is compromised and useless [3].

The most popular adopted symmetric encryption algorithm most encountered nowadays is the Advanced Encryption Standard (AES). It is found to be at least six time faster than triple DES. A replacement for DES was needed as its key size was too small. With increasing computing ability, it was considered weak against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow [13].

The attributes of AES include symmetric key symmetric block cipher, 128-bit data, 128/192/256-bit keys, faster and stronger than triple-des, provide full specification and design details and software implementable in C, Java and Web Programming Languages.

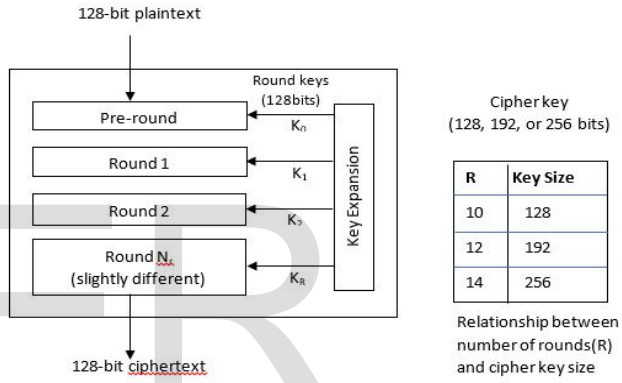


Fig. 4 AES Schematic Structure

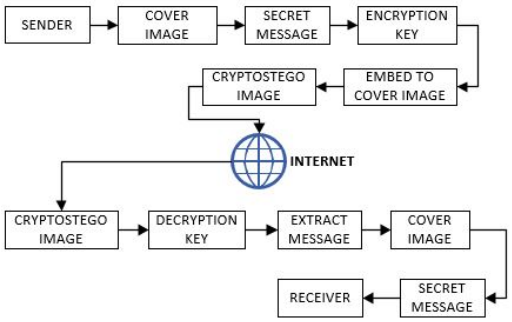
3.2 Proposed Algorithm

Encrypt AES (byte in [4*Nb], byte out [4*Nb], word w[Nb*(Nr+1)])

```
Begin
        Input
        Byte state [4,Nb]
        State = in
        AddRoundKey
        Sub Bytes input
        Shift rows to right
        Mix column by 4 bytes on each
row
        Add round key
        Sub bytes
        Shift rows
        Mix columns
        Output = cipher text
End
```

3.3 System Architecture

This section involves the architecture of the application and how the activity flow would be. Figure 5 is a diagrammatic representation of the system architecture.



3.4 THE LSB TECHNIQUE

Least significant bit (LSB) insertion, shown in figure 6, is a simple approach to embedding information in an image. For example, a simple plan proposed, is to place the embedding data at the least significant bit (LSB) of each pixel in an image. The resulting image is called stego-image. Altering LSB doesn't change the quality of image to human perception but this plan is sensitive a variety of image processing attacks like cropping etc. We will be highlighting more on this technique for the various image formats.

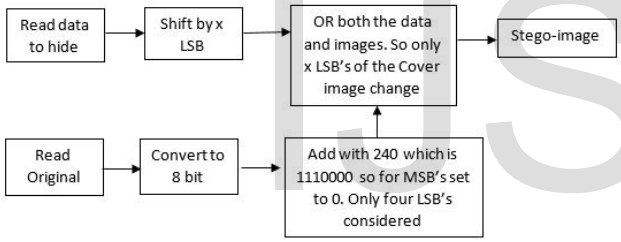


Fig. 6 LSB Technique of embedding data into an image

3.5 THE MATHEMATICS OF CIPHER

A higher level finite field, having polynomials with coefficients in GF(2^8); which would have the function:

$$a(x) = a_3x^3 + a_2x^2 + a_1x^1 + a_0 \quad (1)$$

Each of a_1 are bytes, which are elements of GF(2^8); Addition comes in and we have the function:

$$a(x) + b(x) = (a_3 \oplus b_3)x^3 + (a_2 \oplus b_2)x^2 + (a_1 \oplus b_1)x + (a_0 \oplus b_0) \quad (2)$$

If it now has to do with multiplication, it would result in the same way as multiplying two polynomials. Thereafter, we reduce to degree 4 by using mod x^4+1. And when it is a fixed polynomial, the multiplication process can turn into Matrix Vector multiplication.

3.6 IMAGE ANALYSIS

LSB in Bitmap Images

The BMP file format also called bitmap, is an image file format used to store bitmap digital images. Since BMP is not generally used the hunch might arise, if it is transmitted with an LSB stego. When images are used as the transporters in Steganography, they are generally maneuver by changing one or more of the bits of the byte or bytes that make up the pixels of an image. The message can be stored in the LSB of one colour of the RGB value or in the parity bit of the entire RGB value. A BMP is capable of hiding quite a large amount of data or message. LSB in BMP is most fit for applications. The

Fig. 5 System Architecture

major difference is that while one focuses on the amount of information to be transferred, the other does not but on the secrecy of the data. The more we have in the number of bits, the, the greater possibility that the altered bits are discoverable even with human eyes. Using LSB, the main aim of Steganography transmission of a message to a receiver excluding or bypassing the third party even when there is awareness that a message being transmitted is achieved.

3.7 LSB in PNG

Portable Network Graphics (PNG) is an extensible file format for the lossless, portable, well-compressed storage of raster images. It provides a patent-free replacement for GIF and

can also replace many common uses of TIFF. PNG was created to perfect and replace GIF. Since PNG is widely used, the doubt might not arise if it is transmitted with an LSB stego. When images are used as the carrier in Steganography they are generally altered by changing one or more of the bits of the byte or bytes that make up the pixels of an image. A PNG is capable of hiding a large message. LSB in PNG is most applicable for applications where the focus is on the amount of message to be transferred and not on the secrecy of that message. If more number of bits is changed it may result in a larger possibility that the changed bits can be seen with the human eye. But with the LSB, the main focus of Steganography is to transmit a message to a receiver without a third party even knowing that a message is being passed is being achieved.

3.8 LSB in GIF

Graphics interchange format (GIF) is one of the machine independent wrapped formats for storing images. GIF images only have a bit depth of 8, amount of data that can be hidden is lesser than with Bitmap. Inserting data in GIF images using LSB results in almost the same result as those of using LSB with BMP. LSB in GIF is a very powerful algorithm to use when embedding an amount of information in a grayscale image. GIF images are

indexed images where the colors used in the image are stored in a range. It is sometimes called a colour lookup table. Each pixel is denoted as a single byte and the pixel data is an index to the colour range. The colors of the palette are typically arranged from the most used colour to the least colors used to reduce lookup time. Extraordinary care is to be taken if the GIF images are to be used for Steganography. This is because of the problem with the palette style. If the LSB of a GIF image is changed using the palette style, it may lead to an entirely different colour. This is because the index to the colour palette is changed. The change in the resulting image is visible if the adjacent palette entries are not alike. But the change is not detectible if the adjacent palette entries are alike.

3.9 Image Quality Evaluation

For comparison of stego-image with cover results requires a degree of image quality, commonly used measures are Mean-Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR) and histogram.

Table 2
Comparison of LSB Techniques for various file formats

	LSB IN BMP	LSB IN PNG	LSB IN GIF
Percentage Bias Less Resultant Image	High	Mid	High
Hiddenness	High	Mid	Mid
Steganalysis Revelation	Very Low	Very Low	Very Low
Image Alteration	Very Low	Very Low	Very Low
Volume of Embedded Data	High	Mid	Mid
Payload Volume	High	Mid	Mid
Independent of File Format	Very Low	Very Low	High

3.10 Mean-Square Error

The mean-squared error (MSE) between two images I_1(m, n) and I_2(m, n) is:

$$MSE = \sum_{M,N}[I1(m,n) - I2(m,n)^2] \div (M * N) \quad (3)$$

where M and N are the number of columns and rows in the input images, respectively. Mean-squared error rest strongly on the image intensity scaling. A mean-squared error of 100.0 for an 8-bit image (with pixel values in the range 0-255) looks awful and horrible; but a MSE of 100.0 for a 10- bit image (pixel values in [0,1023]) is barely detectible.

3.11 Peak Signal-to-Noise Ratio

Peak Signal-to-Noise Ratio (PSNR) dodges this problem by scaling the MSE according to the image range.

$$PSNR = 10 \log_{10} \frac{R^2}{MSE} \quad (4)$$

PSNR is calculated in decibels (dB). PSNR is a good measure for comparing restoration results for the same image, but between-image comparisons of PSNR are of less meanings.

3.12 Evaluation of Different Techniques

There are different types of steganographic algorithms available. One should choose the best available algorithm for the given application. Following characteristics are to be assessed while selecting a particular file format for Steganography. Steganography says that the secret message is to be hidden and it should give an output which would result in a distortion less image. The distortion must not be detectible with the human eye. The amount of data embedded in the image also plays a great role. The algorithm determines how much amount of data could be inserted in the image resulting in a distortion less image. The algorithm for Steganography must be such that the steganalysis algorithms should not be successful on it or against it, i.e. the Steganography algorithms must not be pruned to attacks on steganalysis. During communication, the intruder could check the original image to remove the hidden information. He/she may alter the image. This alteration may include cropping or rotation etc. of the images. The alterations done may cause the image distortion. Steganographic algorithms chosen must be such that it overcomes such manipulation and the Steganographic data reaches the destination in the required format [12].

4 Implementation and Result

Web programming languages such as HTML, CSS and JavaScript, were used to write the codes and the interface is represented in figure 7. All these can be implemented with the use of Visual Studio Code.

A user is required to upload an image file, then the level of secrecy is selected. The message to be transferred is typed in into the message box, after this, the user inputs his/her password for encryption and embedding secret message into the image. Finally, the user clicks the button “Write Message to Image”. After the appropriate measure have been taken, the user would be required to download a new image which carries the secret message, which is the “Crypto-Stego image” The algorithm used for the LSB technique makes it very difficult for the human eye to detect changes in the images sent and received over the internet.

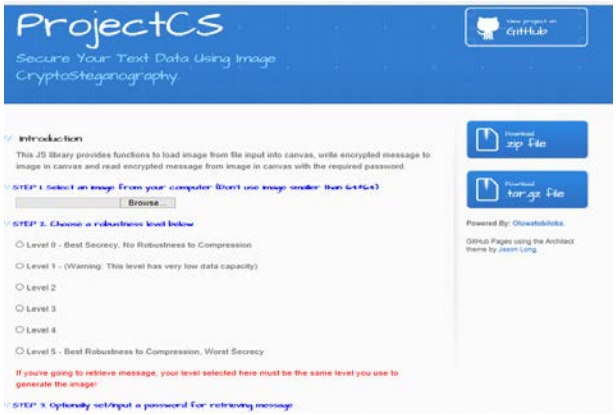


Fig. 7 System Landing Page

The Crypto-Stego image is being sent over the internet to a receiver, and the receiver must ensure he/she chooses the same level of secrecy as the sender so as to decrypt message easily, otherwise, the receiver would only see encrypted messages. Also, receiver must input the password to decrypt and e able to view the message.

5 CONCLUSIONS

In this paper, it can be deduced that crypto-steganographic can be very secure enough to protect data from third parties so as to improve the confidentiality and integrity of messages. And of course, some algorithms were used to overcome some lags in cryptography and steganography security and these algorithms can also be adopted in other future researches and projects.

Many different techniques exist and will continue to be developed, while the ways of detecting hidden messages are also advancing quickly. However, since detection can never give a guarantee of finding all hidden information, it can be used together with methods of defeating cryptography and steganography, to minimize the chances of hidden communication taking place. Even then, crypto-steganography, where the secret key will merely point out parts of a cover image which form the message, will pass undetected, because the cover image contains no information about the secret message which is being passed. With the suggested algorithm, we found that the stego image does not have a detectible distortion on it (as seen by the naked eyes).

Different crypto-steganographic articles were studied and were categorized into different techniques. As many new application areas are identified like internet banking, mobile communication security, cloud security etc., the insight into the crypto-steganographic principles will definitely guide us to identify new areas and to improve its applications in the already existing application areas also.

REFERENCES

[1] Alese B.K (2014). Computer and Network Security. First Bank of Nigeria. Federal University of Technology, Akure.
[2] Ankit Gambhir and Sibaram Khara (2016), "Integrating RSA Cryptography & Audio Steganography", IEEE ICCCA.
[3] Avi Kak (2017). AES: The Advanced Encryption Standard. In Computer Network and Security. (pp. 10-51). Purdue University.
[4] Geers Kenneth, (2011), Strategic Cyber Security. (pp.1-100). NATO Cooperative Cyber Defence Centre of Excellence. CCD COE Publication.
[5] G. JULIUS CAESAR 2011, Cryptography. Security Engineering: A Guide to Building Dependable Distributed Systems (pp.1-42). New York, NY:
[6] K.S. Seethalakshmi, Usha. B, Sangeetha. K. N, (2016) "Security Enhancement in Image Steganography Using Neural Networks and Visual Cryptography", IEEE Int. Conf. Computation System and Information Technology for Sustainable Solutions (CSITSS).
[7] Kamaldeep Joshi, Rajkumar Yadav (2015), "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication", IEEE ICIIP.
[8] Marwa E. Saleh, Abdelmgeid A. Aly, & Fatma A. Omara (2016). Data Security Using Cryptography and Steganography Techniques. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 6, 2016. (pp. 390-397).
[9] Md. Khalid Imam (2014). A Crypto-Steganography: A Survey. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 7, 2014, 2-8.
[10] Moresh Mukhedkar, Prajkta Powar and Peter Gaikwad (2015), "Secure non-real-time image encryption algorithm development using cryptography & Steganography", IEEE INDICON.
[11] Nikhil Patel, Shweta Meena (2016), "LSB Based Image Steganography Using Dynamic Key Cryptography", International Conference on Emerging Trends in Communication Technologies (ETCT).
[12] Rainer Böhme (2010). Advanced Statistical Steganalysis information security and cryptography. New York, NY: Springer. DOI: 10.1007/978-3-642-14313-7
[13] Raphael Chung-Wei Phan (2002). Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis Students. Kuching, Sarawak, Malaysia.
[14] Ria Das, Indrajit Das (2016), "Secure Data Transfer in IoT environment: adopting both Cryptography and Steganography techniques", IEEE Int. Conf. on Research in Computational Intelligence and Communication Networks (ICRCICN).
[15] Rini Indrayani, Hanung Adi Nugroho, Risanuri Hidayat, Irfan Pratama (2016), "Increasing the Security of MP3 Steganography Using AES Encryption and MD5 Hash Function", International Conference on Science and Technology-Computer (ICST), IEEE.
[16] Sadaf Bukhari, Muhammad Shoaib Arif, M.R. Anjum, and Samia Dilbar, (2016) "Enhancing security of images by Steganography and Cryptography techniques", IEEE Int. Conf. Innovative Computing Technology (INTECH).
[17] Vipul Shanna and Madhusudan (2015), "Two New Approaches for Image Steganography Using Cryptography" IEEE Int. Conf. Image Information Processing.