

The Application of Least Significant Bit (LSB) Algorithm in Mitigating Security of Data over the Internet

Gideon G. Amah* Barbara N. Amah**

* (Excellent College of Science and Health Technology, Gboko

* (Excellent College of Science and Health Technology, Gboko

Corresponding Author: Gideon G. Amah

ABSTRACT : Data transfer over the Internet is ever increasing because it is easier, cheaper and faster in transferring data to the intended destination. Several activities are carried out on the Internet including transfer of documents, online transactions among others. Security has become the most significant problem in transferring data or in carrying out any transactions over the Internet because unauthorized persons can hack or attack or intercept thereby making the data useless, hijack the session or causing denial of service (DOS) or distributed denial of service (DDOS) among other attacks on the data or the organization. Attempts have been made by researchers in developing models of hiding data including cryptography and steganography. The paper proposes a system to mitigate these challenges of security of data over the Internet using Least Significant Bits (LSB) algorithm. The approach creates a stego image in which data is hidden and protected from the third party using the 4LSB which is a robust method in embedding a reasonable amount of data using the AND, OR and Shift operations which is not perceivable with the human eyes.

KEYWORDS: security, steganography, hiding Internet, algorithm, least significant bit

Date of Submission: 30-06-2019

Date of Acceptance: 19-07-2019

I. INTRODUCTION

The basic need of every growing area in today's world is communication [1]. Communication, production and storage of data over the Internet has made life easier, faster, flexible and cheaper. As these activities (production, storage and communication) become more extensive and important in the functioning of society, the problem of protecting the information from unintended users becomes more complex. Since we use many insecure pathways for transferring and sharing information using Internet [1]. In this modern society, protection of information involves many interdependent policy and technological issues relating to information confidentiality, integrity, anonymity, utility authenticity. Besides, it has some security problems which require keeping the inside information of work more safe and secure [2]. Detection and prevention of data leakage is the important one of these.

1.1 Background of The Study

Communication, production and storage of data over the Internet has made life easier, faster, flexible and cheaper. As these activities (production, storage and communication) become more extensive and important in the functioning of society, the problem of protecting the information from unintended users becomes more complex.

In this modern society, protection of information involves many interdependent policy and technological issues relating to information confidentiality, integrity, anonymity, utility authenticity

II. STEGANOGRAPHY SECURITY

Steganography [3] comes from the Greek words Steganos (Covered) and Graptos (Writing). The term Steganography came into use in 1500's after the appearance of Trithemius book on the subject Steganographia [4]. The word Steganography technically means covered or hidden writing. Its ancient origins can be traced

back to 440 BC. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries for fun by children and students and for serious espionage by spies and terrorists. The majority of today's steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication. In modern approach, depending on the nature of cover object, steganography can be divided into five types: Text Steganography, Image Steganography, Audio Steganography, Video Steganography and Protocol (TCP/IP) Steganography [2]. So, in the modern age so many steganographic techniques have been designed which works with the above concerned objects. With respect to Steganography there is a problem of unauthorized data access. Steganography is method used for secure communication [5].

Text steganography using files is not often used since text files have small amount of redundant data.

Audio/video steganography is very complex in use.

Protocol (TCP/IP) steganography using the traffic in network hiding information which may lead to leakage of confidential information.

Image steganography most efficient and mostly used in hiding data. It is quite simple and most secret way of transferring information over the Internet. Image steganography have these types:

- Spread spectrum -Patch work
- Transform domain JPEG
- Image domain-LSB and MSB in BMP
- LSB and MSB in JPEG [2]

There are several steganographic methods of achieving results of mitigating security over the Internet.

2.1 The transformation domain techniques Embeds secret information in the frequency domain of the signal. Transform domain methods hide messages in significant areas of the cover image which makes them more robust to attacks such as cropping, compression, and some image processing.

2.2 Statistical methods is the evolvement of information by changing several statistical properties of a cover and uses a hypothesis testing in the extraction process. This process can be achieved using the modification of the cover image such that changes in the statistical characteristics are noticeable significantly. Here if "I" is transmitted then the cover is changed otherwise it is left as such.

2.3 The Least Significant Bit (LSB) works by insertion of a common and simple approach to embed information in an image file [4]. The LSB as an eight bit inside an image is changed or substituted to a bit of the secret message. By using a 24 bit image, 3 bit can be stored in each pixel by substituting a bit of each of the colours Red, green and blue components since each is represented by byte. The least significant Bit as a steganography approach work by replacement of bits of unused or users data in such as (graphics, text, sound etc) with bits of various invisible information.

III. STEGANOGRAPHY SYSTEM ARCHITECTURE

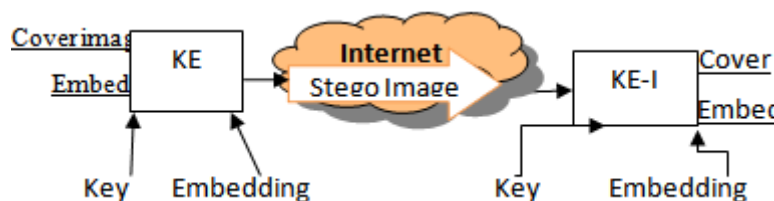


Fig 2.1 Steganography System Architecture

Where;

KE: the steganographic function embedding process

KE-I: is the steganographic function extracting process

Cover image: is the cover image in which the embedding will be hidden embed is the message to be hidden.

Stego Image: is the cover image with the hidden message.

The **Mathematical formulation** can be seen as;

Cover image + embedded message + stego key = stego image.

From the above, the cover image could be any innocent looking carriers (images, audio, video text) in which the secret message will be embedded. The message is that information hidden which could be a plaintext, cipher text (encrypted) images, or anything than could be embedded in bit streams. The cover image and the embedded message created stego carrier (stego image) while a stego key is required in the embedding and extracting process.

3.1 The LSB substitution Method

The LSB algorithm consist of an embedding process choosing as a subset $\{j_1, \dots, j_{l(m)}\}$ of cover elements and performing the substitution operation $LSB(C_{j_i}) = m_i$ (m_i can be 0 or 1). Changing of bit can be more than one than bit of the cover image or element. Example by storing two message bits in the two significant bits of one cover image or element.

The extracting process, the LSB of the chosen cover image or elements are extracted and used to reconstruct the secret message.

3.1.1 Embedding Algorithm

Input: cover image

For $i = 1$ to length (m) do Compute index j_i where to store the i th message bit of m $S_{j_i} \leftarrow LSB(C_{j_i}) = m_i$ End for

Output: stego image

3.1.2 The embedding process

Using every cover starting from first one, since the number of bits in the secrete is typically less than the length of the cover, the strategy would lead to a situation where the embedding process will be finished long the end of the cover and the first of the cover will have different statistical properties that the second parts where no modification have been made.

3.2 Random Interval Method of LBS Substitution.

Here both communication partner share a stego key that would be used for a pseudorandom number generator than can create random sequence $K_1, \dots, K_l(m)$ and use the cover image with indices as:

$j_i = K_i; j_i = j_{i-1} + K_j$ for $2 \leq j \leq \text{length}(m)$

input cover image C

Input stego image S

Generate random sequence K_i using seedk Generate random sequence K_i using seedK

$n \leftarrow k_i$

$n \leftarrow K_i$

For $i = 1$ to length (m) do For $i = 1$ to length (m) do

$S_n \leftarrow LSB(C_n) m_i$

$m_i = LSB(S_n)$

$n \leftarrow n + k_i$

$n \leftarrow n + k_i$

End for

End for

Output stego image

Output message m

Embedding Algorithm

Extraction Algorithm

3.3 The Proposed Algorithm Using The 4 LSB

We make use of the four 4 least significant bit of 24 bit colour image to hold 4 bit secret message by overwriting the information that had already existed. For the analysis, it is noted that the impact of substituting the 4-least significant bit will mitigate security of data over the Internet and the human eyes cannot perceive these changes therefore the message is hidden successfully.

3.4 Proposed System Architecture

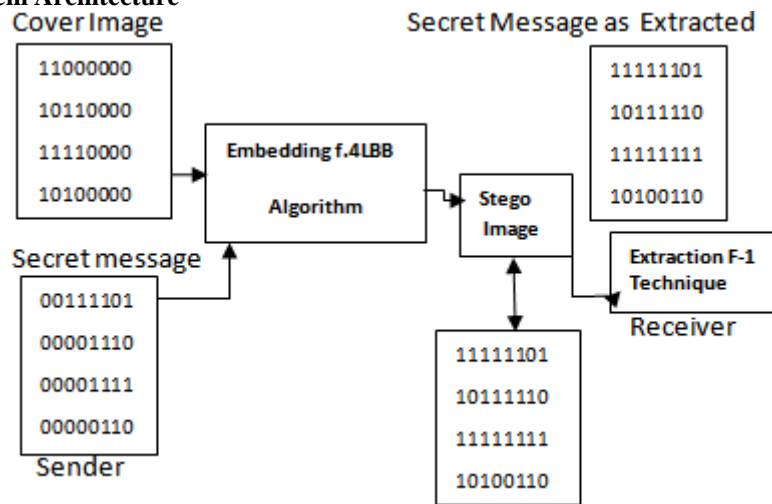


Fig 3.1: The Proposed Stego Image Architecture

3.5 Embedding Algorithm

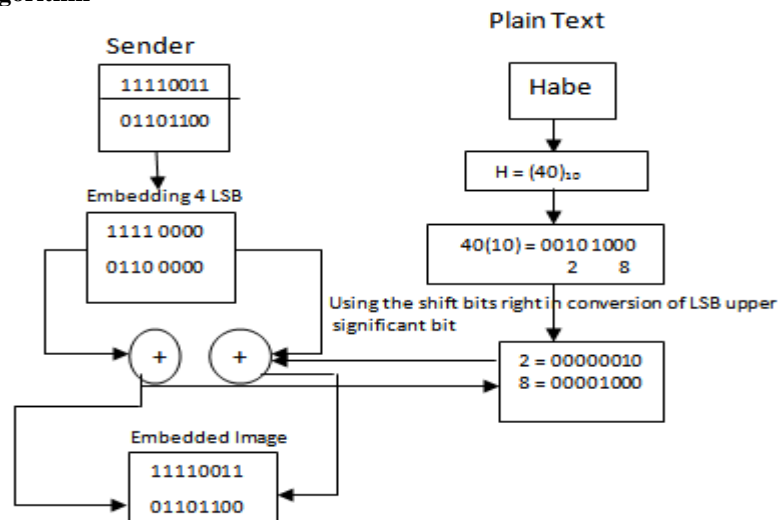


Fig3.2 The Proposed embedding Architecture

In the algorithm which consist of:

1. Cover image converted to streams of bits.
2. To adjacent bit are using in hiding information.
3. Characters of the secret message are consisted to decimal number.
 $40_{10} = (0010\ 1000)_2$
4. The secret message in then added to the secret message.

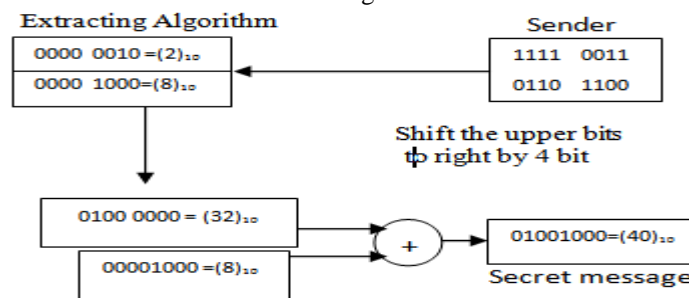


Fig3.3 The Proposed Extracting Algorithm Architecture

The algorithm extract hidden information thus;

- Two adjacent pixels were taken from the stego image
- A shift in the first pixel by 4 to the right as 11110011 shift to the right by 4
- An addition operation is done with 15 (1111) to the second pixel (01101100) AND $(00001111)_2 = (00001000)_2$
- Results of step 2 and step 3 is then added to obtain $(01000000)_2 + (00001000)_2 = (01001000) = (40)_{10} = H$

IV. RESULTS


In our proposed algorithm we could hide information using the 4LSB successfully using the AND, OR and SHIFT operations.

We took the 4LSB alone in embedding the plain text in the cover image producing a stego image.

$$(40)_{10} \text{ AND } (15)_{10} = (01001000)_2 \text{ AND } (00001111)_2 = (00001000)_2 = (8)_{10}$$

We also took the 4 LSB and perform a shift operation by 2 as;

$$(40)_{10} \text{ with SHIFT to right by 2} = (00000010)_2 = (2)_{10}$$

The secret message could be hidden to the cover image through the application of the OR operation as  demonstrated in the embedding and extracting algorithm.

The message could be embedded and extracted successfully using the substitution method of 4LSB which is a robust algorithm.

V. CONCLUSION

Date transfer over the Internet is rapidly increasing because it is cheaper, easier and faster in transferring data to the desired destination. Security is very important issue while transferring data or carrying out any transaction on the Internet because unauthorized persons can hack or attack making data useless or causing denial of service (DOS) or distributed denial of service (DDOS) among other attacks on the data or the organization.

Our proposed system will mitigate these security challenges of security of data over the Internet using the Least Significant bit. Our algorithm create a stego image in which data is hidden and protected from a third party (hacker) using the LSB which is a robust method of embedding a reasonable amount of data that is not noticeable by the human eye.

REFERENCES

- [1]. Nutan Manwade and Swati Nigam (2015), LSB Image Steganography with DES Cryptography. International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) 5(7):761-764
- [2]. Anil Kumar , Rohini Sharma (2013) A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3
- [3]. Chandra Sekhara ReddyT., Prasad D. and Venkateswara ReddyB. IJCTA Journal.
- [4]. Nutan Manwad and Swati Nigam (2015), LSB Image Steganography with DES Cryptography. International Journal of Advanced Research in Computer Science and Software Engineering Research (IJARCSSE). 5(7):761-764
- [5]. Wawge P.U. and Rathod A.(2012) Cloud Computing Security with Steganography and Cryptography AES Algorithm Technology. World Research Journal of Computer Architecture. 1(1):11-15
- [6]. Thangadurai, K. and G. Sudha Devi (2014). An Analysis of LSB Based Image Steganography Techniques. Computer Communication and Informatics. (ICCCI) International Conference on, IEEE.

Gideon G. Amah " The Application of Least Significant Bit (LSB) Algorithm in Mitigating Security of Data over the Internet" American Journal of Engineering Research (AJER), vol.8, no.07, 2019, pp.111-115