ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

An Adaptive Stegnography Method for Hiding Message Using LSB Matching Algorithm

S. SriGowthem, B. Sundarraj, Sundararajan.M, Arulselvi S

Assistant Professor, Dept. of CSE, Bharath University, Chennai, Tamil Nadu, India

Assistant Professor, Dept. of CSE, Bharath University, Chennai, Tamil Nadu, India

Director, Research Center for Computing and Communication, Bharath University, Chennai, Tamil Nadu, India

Co-Director, Research Center for Computing and Communication, Bharath University, Tamil Nadu, India

ABSTRACT: This paper presents a new approach for hiding message in digital image in spatial domain. In this method two bits of message is embedded in a pixel in a way that not only the least significant bit of pixel is allowed to change but also the second bit plane and fourth bit plane are allowed to be manipulated, But the point is in each embedding process only one alternation in one bit plane is allowed to happen. This fast and very versatile solution achieves state-of-the-art results in steganographic applications while having linear time and space complexity w.r.t. the number of cover elements. We report extensive experimental results for a large set of relative payloads and for different distortion profiles, including the wet paper channel. As it is compared by the method LSB-Matching, the results shows this method has an acceptable capacity of embedding data and hardly is detectable for steganalysis algorithm. Most current coding schemes used in steganography (matrix embedding, wet paper codes, etc.) and many new ones can be implemented using this framework.

KEYWORDS: Steganography, Steganalysis, LSB-Matching, Bit Plane and Spatial Domain

1. INTRODUCTION

There exist two mainstream approaches to steganography in empirical covers, such as digital media objects: steganography designed to preserve a chosen cover model and steganography minimizing a heuristically-defined embedding distortion. Steganography is the art of secret communication. Its purpose is to hide the very presence of communication as opposed to cryptography whose goal is to make communication unintelligible to those who do not possess the right keys. Digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information can be used as “covers” or carriers to hide secret messages. After embedding secret message into the cover-image, a so-called stego image is obtained. It is important that the stego-image does not contain any detectable artifacts due to message embedding. A third party could use such artifacts as an indication that a secret message is present.

In this paper, an image is used as a carrier to hide image data. This is called Image Steganography. Least significant bit (LSB) is the simplest form of steganography. LSB is based on inserting data in the least significant bit of pixels, which lead to a slight change on the cover image that is not noticeable to human eye. Since this method can be easily cracked, it is more vulnerable to attacks. To increase the security and the size of stored data, a new adaptive LSB technique is used. Instead of storing the data in every least significant bit of the pixels, this technique tries to use more than one bit in a pixel in such a way that this change will not affect the visual appearance of the host image. It uses the side information of neighboring pixels to estimate the number of bit which can be carried in the pixels of the host-image to hide the secret data.

II. STEGANOGRAPHY

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphein meaning "to write". The first recorded use of the term was in 1499 by Joharnnes Trithemius in his Steganographia, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other covertext and, classically, the hidden message may be in invisible ink between the visible lines of a private letter.

The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

Although steganography is an ancient subject, the modern formulation of it is often given in terms of the prisoner's problem proposed by Simmons, where two inmates wish to communicate in secret to hatch anescape plan. All of their communication passes through a warden who will throw them in solitary confinement should she suspect any convert communication.

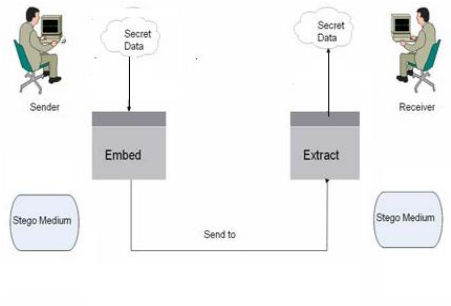

Fig 1. Steganographic mechanism

The warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A passive warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected convert communication, reports this to some outside party and lets the message through without blocking it. An active warden, on the other hand, will try to alter the communication with the suspected hidden information deliberately, in order to remove the information.

III. PROBLEM STATEMENT

3.1 Existing System

In special domain, the hiding process such as least significant bit(LSB) replacement, is done in special domain, while transform domain methods; hide data in another domain such as wavelet domain. Least significant bit (LSB) is the simplest form of Steganography. LSB is based on inserting data in the least significant bit of pixels, which lead to a slight change on the cover image that is not noticeable to human eye. Since this method can be easily cracked, it is more vulnerable to attacks. LSB method has intense affects on the statistical information of image like histogram. Attkers could be aware of a hidden communication by just checking the Histogram of an image. A good solution to eliminate this defect was LSB matching. LSB-Matching was a great step forward in Steganography methods and many others get ideas from it.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

Least significant bit (LSB) is the simplest form of steganography. LSB is based on inserting data in the least significant bit of pixels, which lead to a slight change on the cover image that is not noticeable to human eye. Since this method can be easily cracked, it is more vulnerable to attacks.

This requirement includes all characteristics of a steganographic algorithm that may result in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by a warden.

3.2 Proposed System

3.2.1 Adaptive LSB Substitution

The above LSB method can be easily cracked; it is more vulnerable to attacks. To increase the security and the size of stored data, a new adaptive LSB technique is used. Instead of storing the data in every least significant bit of the pixels, this technique tries to use more than one bit in a pixel in such a way that this change will not affect the visual appearance of the host image. It uses the side information of neighboring pixels to estimate the number of bits which can be carried in the pixel of the host-image to hide the secret data. [1]

In our method, two neighboring pixels of the input pixel are used to determine the number of bits to be embedded in the pixel. The secret information is then embedded into the host-image by a simple LSB substitution method with pixel adjustment process.

The pixel value difference between upper pixel and left pixel of the input pixel is used to determine the amount of embedding data in the pixel. If the pixel is in an edge area, more bits can be placed in the pixel than those in a smooth area. After we know how many bits can be carried by the pixel, we then embed the secret bits into the pixel by simple LSB substitution method. In order to enhance the image quality of the stego-image, the pixel adjustment process is applied to minimize the embedding error.

Cover-Object - Refers to the object used as the carrier to embed messages into. Many different objects have been employed to embed messages into for example images, audio,and video as well as le structures, and html pages to name a few.

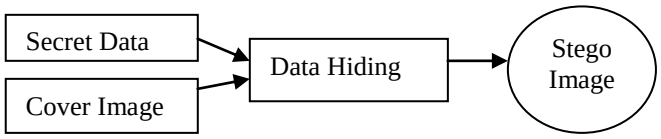

Fig 2. Stego Image Formation from Cover Image

Stego-Object - Refers to the object which is carrying a hidden message. So given a cover object,and a messages the goal of the steganographer is to produce a stego object which would carry the message.[2]

In a pure steganography framework, the technique for embedding the message is unknown to Wendy and shared as a secret between Alice and Bob. However, it is generally considered that the algorithm in use is not secret but only the key used by the algorithm is kept as a secret between the two parties, this assumption is also known as Kercho®'s principle in the fieeld of cryptography. The secret key, for example, can be a password used to seed a pseudo-random number generator to select pixel locations in an image cover-object for embedding the secret message (possibly encrypted). Wendy has no knowledge about the secret key that Alice and Bob share, although she is aware of the algorithm that they could be employing for embedding messages. The warden Wendy who is free to examine all messages exchanged be tween Alice and Bob can be passive or active. A passive warden simply examines the message and tries to determine if it potentially contains a hidden message. If it appears that it does, she suppresses the message and/or takes appropriate action, else she lets the message through without any action.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

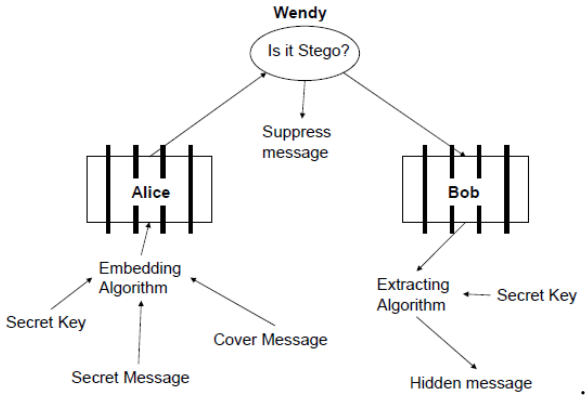

Fig 3. Stego Image process

3.3 Text LSB Substitution - Algorithm

As a simple example of LSB substitution, imagine "hiding" the character 'G' across the following eight bytes of a carrier file (the LSB s are underlined):

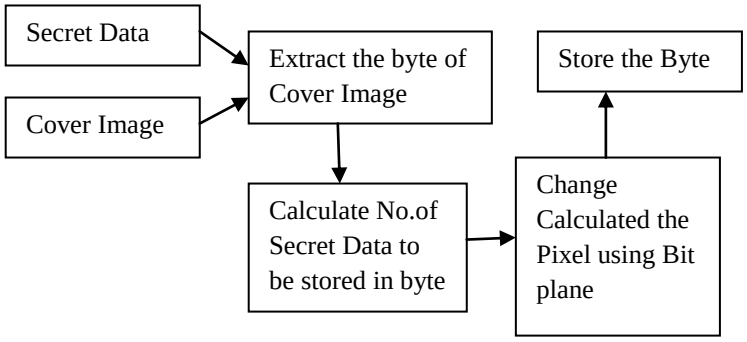

Fig 3. LSB Matching Process

10010101 00001101 11001001 10010110
00001111 11001011 10011111 00010000
A 'G' is represented in the American Standard Code for Information Interchange (ASCII) as the binary string 01000111.
These eight bits can be "written" to the LSB of each of the eight carrier bytes as follows:
10010100 00001101 11001000 10010110
00001110 11001011 10011111 00010001
In the sample above note that only half of the LSBs are actually changed.[3]

3.3.1 Image LEAST SIGNIFICANT BIT Substitution

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24 bit image, a bit of each of the red, green, blue color components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 x 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. For example a grid for pixel of 24 bit image can be as

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)
Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours.

These changes cannot be perceived by the human eye - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference. To increase the security and the size of stored data, a new adaptive lsb technique is used. Instead of storing the data in every least significant bit of the pixels, this technique tries to use more than one bit in a pixel in such a way that this change will not affect the visual appearance of the host image. It uses the side information of neighboring pixels to estimate the number of bit which can be carried in the pixels of the host-image to hide the secret data.[4,6]

3.3.2 LSB Module

Description: This Module consists of developing Two sub modules. The one is encryption module and the decryption module. These two sub modules are the main core for the application.[12]
Encryption Module - In Encryption module, its consists of Key file part, where key file can be specified with the password as a special security in it. Then the user can type the data or else can upload the data also though the browse button, when it is clicked the open file dialog box is opened and where the user can select the secret message. Then the user can select the image file through another open file dialog box which is opened when the image button is clicked. Where the user can select the bmp file and then the Hide button is clicked so that the secret data or message is hidden in Picture through LSB matching revisited technique.

Decryption Module - This module is the opposite as such as Encryption module where the Key file should be also specified same as that of encryption part. Then the user should select the encrypted image and then should select the extract button so that the hidden message is displayed in the text area specified in the application or else it is extracted to the place where the user specifies it.

In that case by changing one bit plane in a pixel, two bits of message should be transmitted. In our method there are only three ways that a pixel is allowed to be changed:[10]

- Its least significant Bit would alter (So the gray level of the pixel would increased or decreased by one level)
- The second less significant bit plane would alter (So the gray level of the pixel would increase or decrease by two levels)
- The fourth less significant bit plane would alter (So the gray level of the pixel would increase or decrease by eight levels)

So

Correct Detection rate = (nss + ncc) / ntot
ntot= nss + ncc + nsc + ncs
nss = number of stego image which detected as stego
ncc = number of cover image which detected as cover.
nsc = number of stego image which detected as cover.
ncs = number of cover image which detected as stego.

LSB replacement is a well-known steganographic method. In this embedding scheme, only the LSB plane of the cover image is overwritten with the secret bit stream according to a pseudorandom number generator (PRNG). As a result, some structural asymmetry (never decreasing even pixels and increasing odd pixels when hiding the data) is introduced,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

and thus it is very easy to detect the existence of hidden message even at a low embedding rate using some reported steganalytic algorithms.[7,9]

LSB matching (LSBM) employs a minor modification to LSB replacement. If the secret bit does not match the LSB of the cover image, then+1 or – 1 is randomly added to the corresponding pixel value. Statistically, the probability of increasing or decreasing for each modified pixel value is the same and so the obvious asymmetry artifacts introduced by LSB replacement can be easily avoided. in this paper the goal is that only one bit is going to be changed.[11]

IV. CONCLUSION AND FUTURE ENHANCEMENT

Image steganography has gotten more popular press in recent years than other kinds of steganography, possibly because of the flood of electronic image information available with the advent of digital cameras and high-speed internet distribution. Adaptive LSB substitution method is used to hide data efficiently and securely in an image. In this paper, various types of images are used as cover image and all types of data such as video, audio, etc has been stored and retrieved with good accuracy. Adaptive LSB technique performs more efficiently in both security and accuracy aspects than the traditional LSB technique. Another method which we were unable to explore was to analyze the noise of the pictures. Adding hidden data adds random noise, so it follows that a properly tuned noise detection algorithm could recognize whether or not a picture had steganographic data or not. This paper manipulates the spatial data of cover image. By using the properties of the DCT, the frequencies can be efficiently used to hide the secret data which is also more resisitant to noises.

REFERENCES

1. Information Forensics and Security, Vol. 5, No. 2, June 2010.
2. Jebaraj S., Iniyan S., Kota H., 'Forecasting of commercial energy consumption in India using artificial neural network", International Journal of 3. Global Energy Issues, ISSN : 0954-7118, 27(3) (2007) pp.276-301.
3.Chang, C.C., Tseng,H.-W.,"A Stegnographic method for digital images using side match" Pattern Recognition Lett. 25,1431-1437,2004.
4.Sharmila S., Jeyanthi Rebecca L., "GC-MS Analysis of esters of fatty acid present in biodiesel produced from Cladophora vagabunda", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 4(11) (2012) pp.4883-4887.
5. Chan,C.K.,Cheng,L.M.,"Hiding data in images by simple LSB Substitution", Patteren Recognition 37,469-474,2004.
6.Chang, C.C.,Lin.,M.H.,Hu, ?Y.-C., "A fast and secure image hiding scheme based on LSB substitution", Int.Journal of Pattern Recognit. And Artif.Intell.16(4),399-416,2004.
7.Kaliyamurthie K.P., Udayakumar R., Parameswari D., Mugunthan S.N., 'Highly secured online voting system over network", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp.4831-4836.
8.. Wang, R.Z., Lin, C.F., Lin, J.C.,Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognition 34,671-683,2001.
9.Kiran Kumar T.V.U., Karthik B., 'Improving network life time using static cluster routing for wireless sensor networks", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S5) (2013) pp.4642-4647.
10.Suk-Ling Li, Kai-Chi Leug, L.M. Cheng, Chi-kwong Chan, performance Evalution of a Steganographic Method for Digital images Using Side Match, icicic 2006, IS16-004,Aug 2006.
11.Jeyanthi Rebecca L., Susithra G., Sharmila S., Das M.P., 'Isolation and screening of chitinase producing Serratia marcescens from soil", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 5(2) (2013) pp.192-195.
12. J. Mielikainen, "LSB matching revisited," *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 285–287, May 2006.
13. Bharthvajan R, Human Resource - Strategy and Outsource, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 15273-15276, Vol. 3, Issue 8, August 2014
14. Bharthvajan R, Human Resource Management and Supply Chain Management Intersection, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 10163-10167, Vol. 3, Issue 3, March 2014
15. Bharthvajan R, Women Entrepreneurs & Problems Of Women Entrepreneurs, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 16105-16110, Vol. 3, Issue 9, September 2014
16. Bharthvajan R, Organizational Culture and Climate, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 8870-8874, Vol. 3, Issue 1, January 2014
17. C.Rathika Thaya Kumari , Dr.A.Mukunthan, M.Nageshwari, Electric and Magnetic Properties of Semiconductors and Metals in One, Two and Three Dimensions, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 271-279, Vol. 2, Issue 1, January 2013
18. C.Tamil Selvi & Dr. A. Mukunthan, Different Varieties of Plantain (Banana) and Their Estimation by Chemical Tests, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 1099-1105, Vol. 2, Issue 4, April 2013