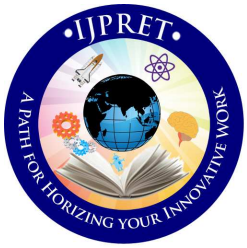
Research Article *ISSN: 2319-507X*

Vipula Wajgade, IJPRET, 2013; Volume 1(8): 228-238 *IJPRET*



INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

ENHANCING DATA SECURITY WITH ADVANCED DIGITAL IMAGE STEGANOGRAPHY

VIPULA M.WAJGADE, NAGESH D. MATHARIA, Dr. SURESH KUMAR

1. M Tech Second Year CSE, Dept of Computer Science and Engineering, SGT Institute Of Technology Institute Of Technology & Management, Gurgaon, India.
2. ME First Year IT, Dept of Info. Technology, PRMIT & R Badnera, Amravati, India
3. HOD, Dept of Computer Science and Engineering, SGT Institute Of Technology Institute Of Technology & Management, Gurgaon, India.

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

Steganography,

Cryptography,

Least Significant Bit,

Watermarks

Corresponding Author

Mr. Vipula M. Wajgade

Abstract

Data security now days have became essential transmission of data in public communication system is not secure due to interception and improper manipulation by eavesdropper. Data Security means protecting a database from destructive forces and the unwanted actions of unauthorized users. The priority of data should be the confidentiality, integrity, and availability for the same, various data security techniques has been implemented."Steganography" is a Greek origin word which means "hidden writing". Steganography word is classified into two parts as: Steganos which means "secret or covered" (where you want to hide the secret messages) and the graphic which means "writing" (text).The proposed method hides the data that is secret message based on Advanced Digital Image Steganography Method using encrypting data with digital images while identifying the identical bits between the image pixel and secret messages values. The proposed method is compared with one of the data hiding approach Least Significant Bit approach. The proposed method is very simple, also efficient and it is robust to unauthorized access or attack and improves the image quality, hence has obtained a high accuracy.

I. INTRODUCTION

Steganography does not deal with alteration of the structure of the secret message or data that is to be hidden, but hides it inside an image called as cover image so that it cannot be seen. For instance A message in a cipher text, might be suspicion on the part of the recipient but a "hidden or invisible" message created using steganographic methods will not. So it can be stated in other words that the steganography prevents an unintended recipient from detecting or from suspecting that the data exists in cover data.

A. First Steganographic Methods:

The Ancient Chinese used to write messages on fine silk, after crunching into a tiny ball it was covered with wax. The message were carried with messenger which is first swallowed as the ball of wax, the Italian scientist developed another method in sixteenth century, Giovanni Porta described another approach how to conceal a message with a hard-boiled egg using an ink made up from a mixture of one ounce of alum and a vinegar this mixture then using ink to write on the shell. As a result the ink penetrated the porous shell, and the message on the surface of the hardened egg albumen appears which could be read only when the shell was removed.

Various methods of Special "inks" were essential steganographic tools even during Second World War. During Second World War a new approach of data hiding was invented that was developed to shrink photographically a page of text into a dot which was shorter diameter less than one millimeter , and used to hide the microdot in an apparently innocuous letter.

A new and general model of a cryptographic system was then emerged, which consists of following [1] [7]:

1. Cover text (cover-data - cover-object) which is simply an original unaltered message.

2. The Embedding process in which the sender tries for hiding of the message by embedding it into a cover text which is randomly chosen text, which is done usually using a key, which results in a stego-text (stego-data or stego-object). The embedding process can be well described

using the mapping EP:CV ´ *KY* ´ *MG* ® *CV*, where *CV* is the set of possible cover- and stego-texts, *KY* is the set of keys and *MG* is the set of messages.

3.Stegotext (stego-data - stego-object) which is the output of step 2.

4.Last**y** the Recovering process (or also called as extraction) in which the receiver, will try to get the data, using the key only, and but not the cover text.

We can describe this recovery process as can be seen as mapping *DE*: *CV* ´ *KY* ® *CV*.

Security is required so that a third person watching such a communication should not be able to find out whether the sender is active, and when will be sender remain active, in the sense that he actually did embedding a message in the cover -text. That is in other words, stegotexts should be indistinguishable from cover texts.

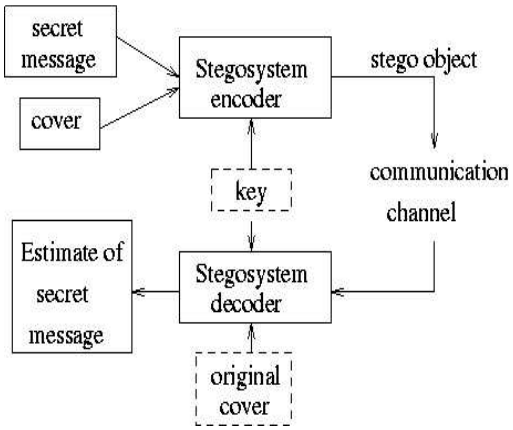


Figure 1 : Steganographic systems model

There are three basic types of stegosystems[2]

1. Pure Stegosystems (Where no key is used for data hiding.)

2. Secret-key Stegosystems (Where a secret key is used for data)

3.Public-key Stegosystems(Where public key is used for receiving and sending the data.)

B. Digital Era of Steganography-Need for More Secure and Robust Steganography.

Various aspects of secure data communication have been emerged due to

unauthorized access of data and eavesdropping. The main motivation behind developing data hiding technique that is digital image Steganography methods is according to its uses in various environments to communicate between its members, as well as, it can also be used to communicate between members of the military or intelligence operatives or various agents of the organisation to hide secret messages or in the espionage field. The vital goal of using the Steganography is to disable or avoid drawing attention to the transmission of hidden information from sender to receiver [3]. If suspicion is raised, then security of secret message must be achieved this goal has been planned to achieve the security, because if the hackers is able to notice any change in the message send by sender then this observer may try to know the hidden information inside the secret message being delivered.

The next evolution of image steganography is the advanced system that consists of the senders cover message, secret message, secret key and embedding algorithm [4]. The cover message is the carrier of the message and can be any format such as image, video, audio, text, or some other digital media. Next the secret message is the data or the information which is needed to be hidden in the appropriate digital media. Hiding algorithm uses the secret key usually to embed the message according to algorithms. The embedding algorithm is means by which secret information is usually embedded in the cover message.

In the steganographic system sender must select suitable message carrier i.e. image,audio,text,video etc before the hiding process, after suitable carrier he must select the secret messages efficiently, in some cases we need to set authentication as well as the robust password (which suppose to be known by the receiver). The most suitable effective and appropriate Steganography algorithm must be then selected that should be able to encode the message in more secure technique [5] [6]. Then the sender may then send the Stego file by means of the email or chat-rooms or chatting, or by any other latest techniques of communication. The Stego file is the carried message with the secret information. After receiving the message by the receiver, he is able to

decode the message using the suitable extracting algorithm and with the same password that is used by the sender while sending the message. The Steganography system scenario is shown in the Figure 2.

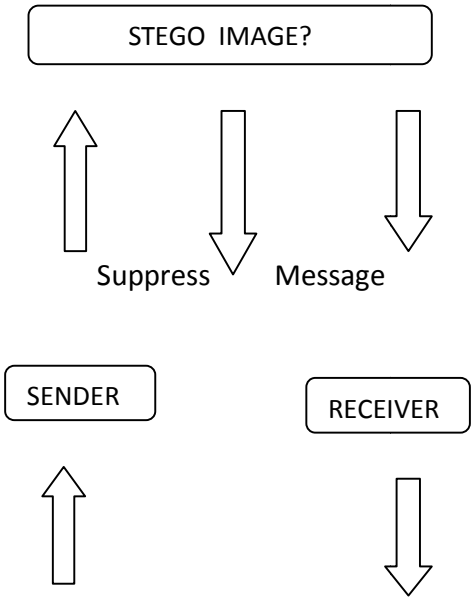


Figure 2: Steganography Scenario

We can view the application of this example as follows:

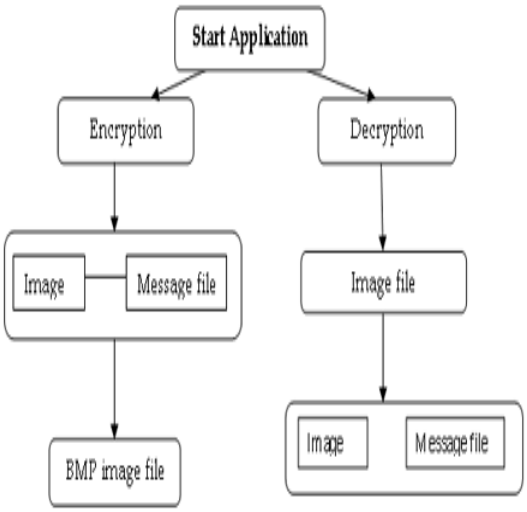


Figure 3: Steganography Example (image)

As with modern era many carrier messages formats can be used as an evolution in the recent technologies, such as Text, Image, video, audio and many others. The image file carrier is the most commonly used and popularly used for this purpose because of the simplicity and it easy to send during the communication between the sender and receiver. The images are generally divided into three main types: binary images (Black-White), Gray scale images and Red-Green-Blue (RGB) images. The binary image is distinguished by one bit value per pixel represented by 0 for black and 1 for white pixels. While on the other hand next type the gray scale images has 8 bits value per

pixel represent from 00000000 for black and 11111111 for white pixels. The recent and most common nowadays the RGB image has 24 bits values per pixel represent by (00000000, 00000000 and 00000000) for black and (11111111, 1111111 and 11111111) for white pixels. The RGB image is the most popular suitable because it unable hiding of secret information easily as it contains a lot of information with a bit change in the image resolution which does not affect the image quality and make the message more robust and secure[8][9]. Due to this quality of RGB images in this paper we used the RGB images as a carrier message to hide the secret messages by the Least Significant Bit hiding method (LSB) as well as the proposed method.

II. RELATED WORK

Many researchers have done tremendous work on hiding data inside image using Steganography techniques. The Existing steganography methods is divided into three main categories as, methods that exploits image format, methods that embeds in the spatial domain and methods which are embedding in the frequency domain. Most essentially, Image Steganography is achieved by modifying the image's Least Significant Bits (LSBs) in such a way that the carrier image remains intact visually.

A. LSB Substitution

This is one of the simplest image steganography methods based on the use of LSB, and therefore the most vulnerable. The LSB method consists of the embedding process of the sequential substitution of each Least Significant Bit (LSB-1) of the image pixel for the bit message. Due to its simplicity, this method LSB substitution can camouflage a great volume of information.

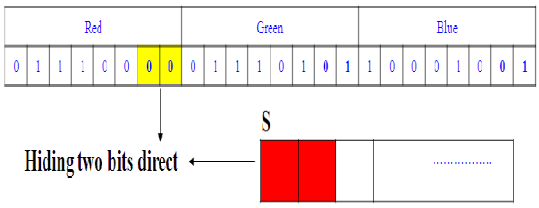


Figure 4: LSB Substitution

The technique used in LSB hiding technique is to hide the secret message directly in the least two significant bits in the image pixels, which results in the image resolution

problem, which reduce the image quality and also make the image easy to attack by unauthorised users. As a result this method is already has been attacked and broken by attackers or unauthorised users observing the network traffic. As a result a new technique that able to make the secret message more secure and to overcome the resolution problem also to enhance the quality of the image is proposed.

B. Other Methods

1. The sequential process or random process of embedding in the spatial domain can be achieved through altering the least significant bits of the bytes of image pixel values. The resultant process may be in a sequential or in a randomised form. The advantaged of using this algorithms based on this method have a high payload; the negative aspects are that the method is fragile, prone to statistical attacks and sometimes results in the visual attacks.

2. Apart from the spatial domain method second type of method, the frequency domain method has also been proposed, which is mainly based on the embedding in the coefficient in the frequency domain also called as DCT or DWT (i.e., Discrete Cosine Transformation (DCT), Discrete Wavelet Transformation (DWT)). The positive aspect of this type of technique is that it is more robust with respect to common image processing operations and lossy compression [10] [11]. Another alternative approach is the type of method which is based on adaptive Steganography. This adapts the message embedding technique to the actual content and features of the image. These methods have advantages that it can avoid areas of uniform colour and select pixels with large local standard deviation. Another method called as Edge embedding can also be used with the Adaptive Steganography.

III. THE PROPOSED SYSTEM

The negative aspects of previous system results in evolution of new technique. The LSB hiding technique results in image distortion, image resolution problem and reduced image quality, hence more efficient and secure system is proposed to enhance quality of image and to provide data hiding. The proposed system searches the identical

values between secret message and image pixels [12] [13].

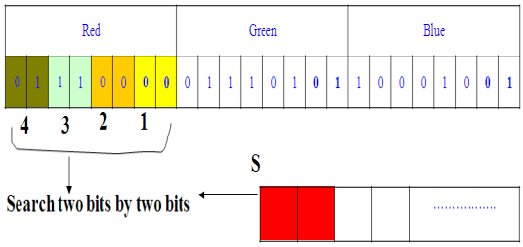


Figure 4: The Two Bits Substitution.

We can describe its process by means of algorithm as follows:

The Proposed Hiding Algorithm.

1. Start
2. Start by scanning the image from left row by row and encode it in binary.
3. Encode the secret message in binary.
4. Measure the size of the image and the size of the secret message.
5. Start with sub-iteration 1:

5.1 Randomly select the one pixel of the image then divide the image (RGB) into three parts (Red, Green and Blue parts) then start with hiding two by two bits of the secret message in every pixel while searching about the identical.

5.2 [Satisfied?] If the identical is satisfied then set new value of the image.

5.3 [Unsuccessful?] hide in the two least significant bits and set the image with the new values save the location of the hiding bits in binary table.

6. End of sub-iteration 1.

7. Set the image with the new values and save it.

8. Return

IV

. FEATURES OF THE PROPOSED SYSTEM

1. High Embedding capacity is achieved with this method.

2. The quality of image retains as it is.

3. As the data is hidden in the adjacent pixel value, so few LSB bits cannot extract the hidden data [14].

4. The secret key is needed without which extraction of data becomes impossible.

5. This approach is also needed to provide password not only the information to reach that information.

6. The communication is easy because it is difficult to detect by attackers, only receiver can detect.

7. It is responsible for enhance security.

8. This technique can be applied differently in different formats like image, audio and video file.

V. APPLICATION

•This can be applicable when no cryptographic methods are available the secure and secret communication is possible.

•Strong cryptography absentee can also be treated.

• Secret communication like military services can use this method.

• The medical field like imaging the health care systems may be benefitted from this approach of information hiding**.**

•The Communication remains confidential and data storing is kept secret.

•Data alteration can be protected.

•This technique is mostly used in modern equipments, printers.

•Confidentiality can be maintained such as copyrights.

VI. CONCLUSION

The proposed method in this paper hides the secret message on the basis of searching about the identical bits between the secret messages and image pixels values. The proposed method when compared to the LSB benchmarking method for hiding the secret message in which the secret message is hided based directly on the least two significant bits of the image pixels [15]. With this paper we can conclude that the proposed method is more simple, appropriate, efficient and accurate than LSB method, the searching about the identical bits value then start hiding, the advantage of this method is that the change in the image resolution is quite low, as well as its simplicity makes the secret message more secure and robust. This paper concluded that the LSB hiding method is the worst case of the proposed method. The positive aspects of this proposed method is efficient, simple and fast, robust to attack and improve the image quality, as a result it has obtained a high accuracy.

REFERENCES

1. W, Peter. Disappearing Cryptography: Information Hiding: Steganography & Watermarking (second edition). San Francisco: Morgan Kaufmann. 3(1992)192-213.

2. B. Dunbar. A detailed look at Steganographic Techniques and their use in an Open-Systems Environment, Sans Institute, 1(2002).

3. N Ghoshal, J K Mandal .A steganographic scheme for colour image authentication (SSCIA), Recent Trends in Information Technology ICRTIT 2011 International Conference on (2011), 826-831.

4. Spam Mimic." http://www.spammimic.com.

5. R. Ibrahim and T.S. Kuan, Steganography imaging system (SIS): hiding secret message inside an image, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2010, San Francisco, USA, 2010, pp. 144-148.

6. N Ghoshal, J K Mandal .A steganographic scheme for colour image authentication (SSCIA), Recent Trends in Information

Technology ICRTIT 2011 International Conference on (2011), 826-831.

7. W, Peter. Disappearing Cryptography: Information Hiding: Steganography & Watermarking (second edition). San Francisco: Morgan Kaufmann. 3(1992) 192-213.

8. Chen, N. Memon, E.K. Wong, Data hiding in document images, in: H. Nemati (Ed.). Premier Reference Source–Information Security and Ethics: Concepts,Methodologies, Tools and Applications, New York:Information Science Reference, 2008, pp. 438-450.

9. N.N. El-Emam, Hiding a large amount of data with high security using steganography algorithm, Journal of Computer Science 3 (2007) 223-232.