IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 3 (Jul. - Aug. 2013), PP 13-16
www.iosrjournals.org

Hiding Text within Image Using LSB Replacement

Nada ElyaTawfiq
College of Computer Science and Information TechnologyNawroz University

Abstract:*Our digital world and its hyper connectivity makes securing the digital content a paramount. Information hiding has always been seen as a way to protect sensitive data from adversaries. This research paper utilizes a new algorithm to hide atextmessagewitha gray image to achievesecurity and maintain high quality results. The new algorithm was appliedtogenerate a random key in the range of (1 to 256) to increase the level of security. This random key was used to determine the binary value of each character within the text message. Next XOR operation was applied on the numbers and the key matrix.Then, the last two bits of the gray level value was ANDed with the first two bits of the matrix to generate a randomized plain text and embed it within the original image. The usage of XOR and AND operations ensures that the resultant image has the minimum number of errors which in turn increases the quality of the image.*

I. Introduction

Nowadays, communication is made electronically over computer networks. In many cases, confidentiality, integrity and authenticity of the electronic data should be guaranteed. This can be achieved most reasonably by means of hierarchical public key infrastructures.[1]

In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different ways, therefore exploiting an unexpected weakness in the mechanism [2]. Although modern cryptographic techniques started to develop during the renaissance, but so many preferred hiding over ciphering because it arousesless suspicion.[3]

The process of information hiding may involve the following concepts:

A- **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 file structures, and html pages to name a few.

B- **Stego-object:** refers to the object which is carrying a hidden message. So given a cover object, and a message the goal of the steganographer is to produce a stego-object which would carry the message.

The larger the cover message is (in data content terms—number of bits) relative to the hidden message, the easier it is to hide the latter. For this reason, digital pictures (which contain large amounts of data) are used to hide messages on the Internet and on other communication media. It is not clear how commonly this is actually done. For example: a 24-bit bitmap will have 8 bits representing each of the three color values (red, green, and blue) at each pixel. If we consider just the blue there will be 28 different values of blue. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. Therefore, the least significant bit can be used (more or less undetectably) for something else other than color information. If we do it with the green and the red as well we can get one letter of ASCII text for every three pixels.[4]

II. Embedding data

Embedding data, which is to be hidden, into animage requires two files. The first is the innocent-looking image that will hold the hidden information, calledthe cover image. The second file is the message—theinformation to be hidden. A message may be plaintext, ciphertext, other images, or anything that can beembedded in a bit stream. When combined, the coverimage and the embedded message make a stego-image.Astego key (a type of password) may also beused to hide, then later decode, the message.Most steganography software neither supports norrecommends using JPEG images, but recommendsinstead the use of lossless 24-bit images such as BMP.The next-best alternative to 24-bit images is 256-coloror gray-scale images. The most common of thesefound on the Internet are GIF files.

In 8-bit color images such as GIF files, each pixel isrepresented as a single byte, and each pixel merelypoints to a color index table (a palette) with 256 possible colors. The pixel's value, then, is between 0 and255. The software simply paints the indicated coloron the screen at the selected pixel position. [7]

2.2 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 steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphei meaning "writing". The first recorded use of the term was in 1499 by Johannes 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 [5].

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 [5]. In the Steganography system scenario, before the hiding process, the sender must select the appropriate message carrier (i.e image, video, audio, text) and select the effective secret messages as well as the robust password (which suppose to be known by the receiver). The effective and appropriate Steganography algorithm must be selected that able to encode the message in more secure technique. Then the sender may send the Stego file by email or chatting, or by other modern techniques. The Stego file is the carried message with the secret information. After receiveng the message by the receiver, he can decode it using the extracting algorithm and the same password used by the sender. [6]

The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised, then this goal is defeated [5]. 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[5].

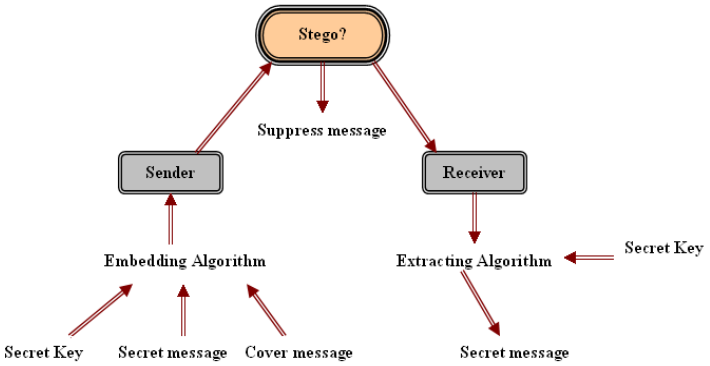

Figure 1: Steganography System Scenario [7]

2.3Data embedding security schemes

The choice of embedding algorithm in the most cases is driven by the results of the steganographic channel robustness analysis. One of the areas that improve steganographic robustness is usage of a key scheme for embedding messages. Various key steganographic schemes have various levels of protection. Key scheme term means a procedure of how to use key steganographic system based on the extent of its use. However, when the steganographic robustness is increased a bandwidth of the whole embedding system is decreased. Therefore the task of a scheme selection for achieving the optimal values of the steganographic system is not trivial.[4]

Embedding messages in steganographic system can be carried out without use of a key or with use of a key. To improve steganographic robustness key can be used as a verification option. It can make an impact on the distribution of bits of a message within a container, as well as an impact on the procedure of forming a sequence of embedded bits of a message.[4]

The first level of protection is determined only by the choice of embedding algorithm. This may be the least significant bits modification algorithm, or algorithms for modifying the frequency or spatial-temporal characteristics of the container. The first level of protection is presented in any steganographic channel [6].

The second protection level of the steganographic system, as well as all levels of protection of the higher orders, is characterized by the use of Key (password) via steganographic modification. An example of a simple key scheme, which provides a second level of protection, is to write the unmodified or modified password in the top

or bottom of the message; or the distribution of the password sign on the entire length of the steganographic channel. Such key schemes do not affect the distribution of messages through the container and do not use a message preprocessing according to the defined key (see figure The Second Protection Level Scheme). This kind of steganographic systems are used in such tasks as, for instance, adding a digital signature for proof of copyright. Data embedding performance is not changed in comparison with the fastest approach of the first protection level usage [6].

Steganographic data channels that use key schemes based distribution of a message through the container and or preprocessing of an embedded message for data hiding are more secure. When the third protection level key scheme is used it affects the distribution of a message through the container (see figure The Third Protection Level Scheme, where F (P, L) – distribution function of a message within a container; P – minimum number of container samples that are needed to embed one message sample; L – step of a message distribution within a container). Accordingly, the performance of container processing will be lower than in the case of the first and the second key schemes [8]. Taking into account that P≥L, the simplest representation of the F(P, L) function could be as following:

F(P, L) = cycle*L + step*P ……..(1)

Where cycle is a number of the current L section and step is a number of the embedded message sample.

The difference between the fourth protection level scheme and the third one is that in steganographic system there are two distribution functions of a message within a container are used. The first is responsible for a message samples selection according to some function G (Q, N), and the second function F(P, L) is responsible for position selection in a container for message sample hiding. Here Q – the size of message block to be inserted; N – the size (in bits) of one sample of the message file (see figure The Fourth Protection Level Scheme).[6]

III. Least Significant Bit Hiding Technique (LSB)

Least Significant Bit (LSB) is the most popular Steganography technique. It hides the secret message in the RGB image based on it its binary coding. Figure 2 presents an example about pixel values and shows the secret message. LSB algorithm is used to hide the secret messages by using algorithm 1. LSB makes the changes in the image resolution quite clear as well as it is easy to attack [6].

IV. Proposed Algorithm

In the proposed algorithm, a modified method of data hiding by LSB substitution method is developed to embed a secure textin the gray image, so that the interceptors will not notice about the existence of thattext [2]. The simple LSB substitution method is used to prevent illicit access of data and increase the system performance, so the effectiveness of the optimal LSB substitution in the worst case willbeproved. In the worst case, PSNR of the obtained stego-image can be computed by:

$\text{PSNR}_{\text{worst}} PSNR_{worst} = 10 \times \log_{10} \frac{255^2}{MSE}$ …….. (1)

The proposed algorithm explains how the text made secret between the sender and receiver with using key generation by embeds the text into image, then transmit that image. The operation is as follows:

The text is taken as 256 character, and by taking EBCDIC code of each character in it , then the key will generate from the value 1 to 256. The generation of random key will increase the security level of the text, after that applying the XOR operation which will increase the strength of any steganographic method.

The key generation denoted as matrix K(i,j)

Where: i = 1 to 16 and j = 1 to 16

and let K(i,j) = D

Where D assume with the form:

D = 16v + w …….. (2)

Where v & w are integers and their values between (1 to 256), i.e. convert the text into integers.

By using XOR operation between very number in the text (which denoted by M) and the key matrix which are placed in the same position :

M = M XOR K ……. (3)

The inserting text (which should be the same as the original image) is done by convert the first element M_{11} into its binary format, so will get a string of 8 binary bits. Then having the first six bits of each value and apply AND operation between the last two bits of the gray level value and the first two bits of the M_{11}. Then we concatenate the resulting two bits in the first row, the next two bits of M_{11}after the AND operation in the next row, etc…, the embedding of the text in the image goes column by column until the entire text is completed.Decryption involves revers process of encryption.

Figure (2) Original Image

Figure (3)Image with embedded text

Table (1) tabulates the PSNR for the proposed system.

Table 1: PSNR for the proposed algorithm

IMAGE	1	2
MSE	0.00178	0.0085
PSNR	75.64	78.72

V. Conclusion

This research study utilized a new algorithm to embed a text message in a gray image using a random key. The hiding process included concealing the plain text using column by column technique. The results demonstrated by the above table showed that a high level of security was achieved and the quality of the image was preserved. This research project did not take into account an image that contains noise which could be considered a direction for future work.

References

[1] V. K. Pachghare, "Cryptography and Information Security " , PHI Learning Private Linited, 2009.
[2] William Stallings, "Cryptography and Network Security", Prentice Hall, Boston Columbus Indianapolis, 2011.
[3] H. Motameni, M. Norouzi, "Labeling Method in Steganography", World Academy of Science, Engineering and technology, 2007.
[4] http://en.wikipedia.org/wiki/Steganography#Data_embedding_security_schemes
[5] Pahati, OJ (2001-11-29). "Confounding Carnivore: How to Protect Your Online Privacy". AlterNet.Archived from the original on 2007-07-16.http://web.archive.org/web/20070716093719/http://www.alternet.org/story/11986/. Retrieved 2008-09-02.
[6] Atallah M. Al-Shatnawi. "A New Method in Image Steganography with Improved Image Quality".Al-albayat University, Mafraq, Jordan."data hiding fundamentals and applications" . 2004, HusrwSencar,
[7] Neil F. Johnson and SushilJajodia, "Exploring Steganography Seeing the Unseen", George Mason Universit