National Conference on Advances in Computer Science and Applications with International Journal of Computer Applications (NCACSA 2012)
Proceedings published in International Journal of Computer Applications® (IJCA)

An Overview of Image Steganography using LSB Technique

Jayeeta Majumder
Department of Computer Science & Engineering
Haldia, West Bengal
Haldia Institute of Technology

Sweta Mangal
Department of Computer Science & Engineering
Haldia, West Bengal
Haldia Institute of Technology

ABSTRACT
Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. This paper intends to give an overview of image steganography, its uses and techniques. For a more secure approach, this paper encrypts the message using secret key and then sends it to the receiver. The receiver then decrypts the message to get the original one. The rapid development of data transfer through internet made it easier to send the data accurate and faster to the destination. This paper deals with the algorithm based on hiding a large amount of data (image, audio, text) file into color BMP image. This project gives a brief idea about the image steganographic approach that make use of Least Significant Bit(LSB) algorithm for embedding the data into the bitmap image(.bmp) which is implemented through the JDK 1.5.0_07 environment. The Least Significant Bit (LSB) embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file.

Keywords
steganography, steganalysis, stego image, cover medium, LSB technique,

1. INTRODUCTION
In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium o transfer data from one end to another across the world.Data security basically means protection of data from unauthorized users of hackers and providing high security to prevent data modification. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet.

In order to improve the security features in data transfers over the internet, many techniques have been developed like: Cryptography Steganography etc. Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats. Steganography is a method of encryption that hides data among the bits of a cover file, such as a graphic or an audio file. The technique replaces unused or insignificant bits with the secret data.

According to Johnson et al., (2001), "Steganography is the art of hoding and transmitting data through apparently innocuous carries to conceal the existence of data". The level of visibility is decreased using many hiding techniques in 'Image Modelling' like LSB 'Manipulation', 'Masking and Filtering'. These techniques are performed by different steganographic algorithms like F5, LSB, JSteg etc. and the act of detecting the information hidden through these algorithms is called 'Steganalysis'. 'Steganography' and 'Cryptography' are closely related constructs. The hidden or embedded image, audio or video files act as carriers to send the private messages to the destination without any security breach. Steganography techniques can be implemented on various file formats such as audio ('.mp3','.wmv', etc.), video ('.mpeg','.dat', etc.) and images ('.jpeg', '.bmp', etc.). However, the images are the most preferred file format for this technique. Fig:1 Graphical Version of the Steganographic System

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 graphein meaning "to write". Steganography literally means "covered languages".

Steganography Mechanism

Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text etc.) with bits of different, invisible information.

where,

fE: steganographic function "embedding" , fE-1 : steganographic function "extracting"

Cover: cover data in which emb will be hidden, emb: message to be hidden.

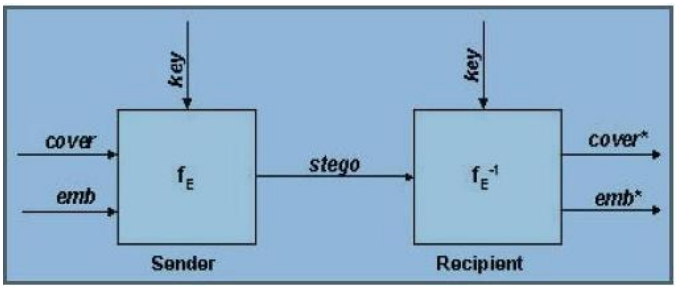

Fig:1 Graphical Version of the Steganographic System

stego: cover data with the hidden message A formula for the information hiding process might look like this:

cover medium + embedded message + stegokey = stego-medium

The cover medium is any innocent looking carriers (images, audio, video, text) in which the secret message will be embedded. A message is the information hidden and may be plaintext, cipher text, images, or anything that can be embedded into a bit stream. Together the cover carrier and the embedded message create a stego-carrier. The stegokey is any additional information required to embed the information.

Steganography algorithm with high security:

Steganography algorithm by using three layers of security has been constructed. These layers are developed from previous works[1,10] to acquire high security and they work independently to provide unbreakable security(Fig: 2).

The encryption mechanism is the first layer of security for data protection by using DES or AES algorithm[1,5]. This layer is used before hiding input data and it gives us powerful Steganography algorithm. Before describing the present algorithm, we need to show the following concepts:

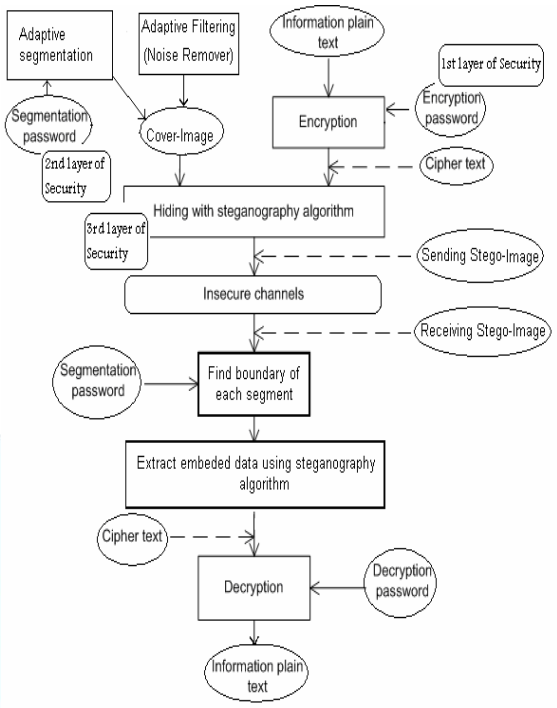

Fig: 2 Steganography with security layers

Descriptions of the steganography algorithm:

In the Steganography algorithm, two parts (data hiding at the sender side and data extracting at the receiver side). These parts are constructed and implemented to satisfy the following requirements:

1. The algorithm must reduce the chances of statistical detection.
2. The algorithm must provide robustness against a variety of image manipulation attacks.
3. The stego-image must not have any distortion artifacts.
4. The algorithm must not sacrifice embedding capacity in order to achieve the above

Requirements. The first part is used to hide data file inside Bitmap according to the following actions:

* Accept encryption password from the sender.
* Find a maximum size (number of bytes) that is accepted by the cover-image.
* Perform compression on secret data file to increase the amount of hiding secret data.
* Perform encryption on secret data file.
* Perform the following processes on the cover image from type bitmap:
  - Adaptive segmentation according to the password.
  - Adaptive filtering (noise remover).
* Perform scanning to select suitable pixels on each segment by extracting image characteristics. The candidate pixels are used to embed secret data.
* Perform hiding of the secret data into bitmap images according to color characteristics. While the second part is

used to extract data from bitmap image at the receiver side in conformity with the following actions:
* Extracting password.
* Scanning segment's pixels according to the password.
* Extracting data file.
* Decrypt the extracting data file by using the password.

Least Significant Bit Algorithm

The LSB Technique

The least significant bit i.e. the eighth bit inside an image is changed to a bit of the secret message. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue colour components, since they are each represented by a byte. An 800×600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. As an example, suppose that we have three adjacent pixels (9 bytes) with the RGB encoding.

10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011

When the number 300, can be which binary representation is 100101100 embedded into the least significant bits of this part of the image. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in **bold** have been changed)

10010101 00001100 11001000
10010111 00001110 11001011
10011111 00010000 11001010

Here the number 300 was embedded into the grid, only the 5 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. The human eye cannot perceive these changes - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the LSB without noticing the difference[12].

The present Steganography algorithm is used to hide any type of input data within a bitmap image which includes 24– bits (3 bytes of RGB colors), each byte is separated into two nibbles (four bits). The left nibble contains the highest value in the byte while the right nibble contains the lowest value in the byte. Therefore, any changes in the right nibble will cause a minimal change in a byte value. We can specify the byte effective according to the left nibble value. The nibble value is fixed by the interval [0, 15], so that we conclude that we have 16 levels of a priority, each one represents one main case (MC) out of 16. In the present work we use the following formula equation (1) to determine the index of MC that must be implemented to perform hiding in a bitmap cover-image.

$$MC = Int(ByteColor/16) + 1 \quad (1)$$

where ByteColor∈{ByteRed, ByteGreen, ByteBlue} represents the value of Color in decimal notation. To hide large amount of data, all three colors of one pixel are checked by the present Steganography algorithm to perform hiding data by depending on newcconcept which is called sub-case (SC). This concept is used to organize the pixel architect. We have defined 6 SCs that are specified according to the following:

Let us define MC^{color} = index, where $1 \leq$ index ≤ 16 and color∈ {R, G, B} where R, G, B are pixel's color equal to ByteRed, ByteGreen and ByteBlue respectively. Assume that the MC of the current color is C and X,Y are the MCs of the rest colors at the same pixel, then we can define the index of SC according to the following conditions:

1 ⇔ X, Y < C
2 ⇔ (X =C & Y < C)|(X < C & Y= C)
3 ⇔ X,Y=C
Index of SC =
4 ⇔ (X >C & Y< C) |(X< C & Y> C)
5 ⇔ (X> C & Y =C) |(X= C & Y> C)
6 ⇔ X,Y>C

Type of pixels

1- CP: - Is the Current pixel that includes the set of colors {R, G, and B}.
2- NP: - Is the next pixel of the CP.
Assume that we have a cover-image which contains three types of MC: MC1, MC2 and MC6 and we have three types of pixels: MC1 with SC3, MC2 with SC5 and MC6 with SC1. Now, we try to hide 2- bytes 01010101, 01010101.

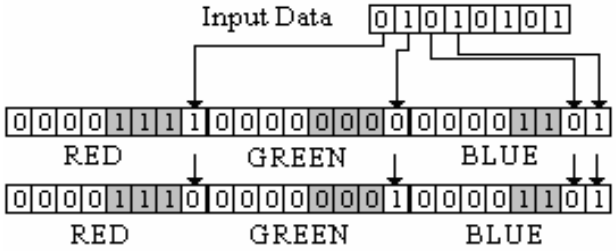

Fig. 3: Data Hiding Using MC 1 with SC 3

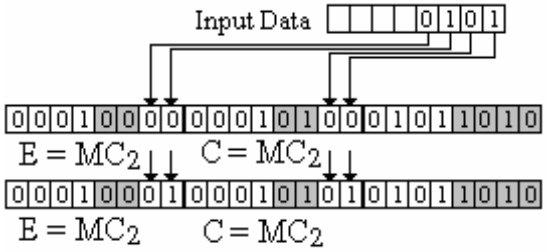

Fig. 4: Data Hiding Using MC2 with SC5

The algorithm starts hiding data inside the highest priority Pr(MC1), assume that CP includes the following values of colors (R=15,G=0,B=13), the MC of CP is MC1 with SC3. In the present Steganography algorithm, we can hide the data "01010101", as the
following:

We assign the left most bit of the input data into the right most bit of the R-byte, the bit before the left most bit is assigned to the right most bit of the G-byte and we assign the rest two bits (the right nibble of input data) into the right most two bits of the B-byte

.After hiding data in all, the MC1, it will start hiding inside the next highest priority which is MC2 in this example. Let us say that the first pixel from MC2 was in SC5 and its value was of colors (R=16, G=20, B=90), it will hide the data as the following, the least 2 bit will be modified in the current selected color and in the color which it's MC equal to the current selected color MC, as it is shown in Fig. 3

.And then after hiding the data in all the MC 2 it will start hiding inside the next high priority in this example which is MC 6, let we say that the first pixel from MC6 was in SC1 and it's value was (17, 21, 90), it will hide the data as the following, the least 2 bit will be modified in the current selected color for the current selected pixel and in the current selected color for the next pixel, as it is shown in Fig. 5.

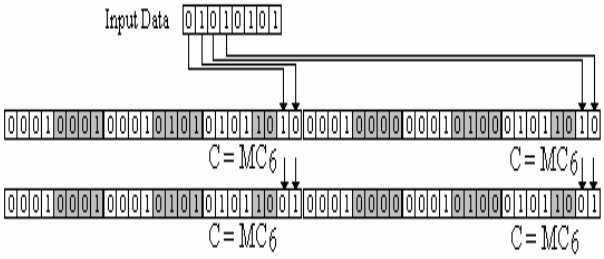

Fig. 5: Data Hiding Using MC6 with SC1

2. CONCLUSION & FUTURE WORK

In the present world, the data transfers using internet is rapidly growing because it is so easier as well as faster to transfer the data to destination. So, many individuals and business people use to transfer business documents, important information using internet. Security is an important issue while transferring the data using internet because any unauthorized individual can hack the data and make it useless or obtain information un-intended to him. The proposed approach in this paper uses a steganographic approach called image steganography. The application creates a stego image in which the personal data is embedded and is protected with a password which is highly secured. The major limitation of the application is designed for bit map images (.bmp). It accepts only bit map images as carrier file.

3. REFERENCES

[1] S-Tools (http:// digitalforensics. champlain. edu/ download/ s-tools 4.zip).

[2] Chandramouli, R. and N. Memon, 2001. Analysis of LSB based image steganography techniques. Proc. of ICIP, Thessaloniki, Greece.

[3] Dumitrescu, S., W. Xiaolin and Z. Wang, 2003. Detection of LSB steganography via sample pair analysis. In: LNCS, Vol. 2578, Springer-Verlag, New York, pp: 355–372.

[4] Ahn, L.V. and N.J. Hopper, 2004. Public-key steganography. In Lecture Notes in Computer Science. Vol. 3027 / 2004 of Advances in Cryptology - EUROCRYPT 2004, pp: 323–341. Springer-Verlag Heidelberg.

[5] Pang, H.H., K.L. Tan and X. Zhou, 2004. Steganographic schemes for file system and b-tree. IEEE Trans. on Knowledge and Data Engineering, 16: 701–713.

[6] Dobsicek, M., 2004. Extended steganographic system. In: 8th Intl. Student Conf. on Electrical Engineering. FEE CTU.

[7] Mittal, U. and N. Phamdo, 2002. Hybrid digitalanalog joint source-channel codes for broadcasting and robust communications. IEEE Trans. on Info. Theory, 48: 1082 –1102.

[8] Pavan, S., S. Gangadharpalli and V. Sridhar, 2005. Multivariate entropy detector based hybrid image registration algorithm. IEEE Intl. Conf. on Acoustics, Speech and Signal Processing, pp: 18-23.

[9] Moulin, P. and J.A. O'Sullivan, 2003. Informationtheoretic analysis of information hiding. IEEE Trans. on Info. Theory, 49: 563–593.

[10] Amin, P., N. Liu and K. Subbalakshmi, 2005. Statistically secure digital image data hiding. IEEE Multimedia Signal Processing MMSP05, China.

[11] Jackson, J., G. Gunsch, R. Claypoole and G. Lamont, 2004. Detecting novel steganography with an anomaly- based strategy. J. Electr. Imag., 13: 860–870.

[12] Deshpande Neeta, Kamalapur Snehal, Daisy Jacobs "Implementation of LSB Steganography and Its Evaluation for Various Bits" Digital Information Management, 2006 1st International conference.pp 173-178,2007.

[13] C. Cachin, "An Information-Theoretic Model for Steganography", in *proceeding 2nd Information Hiding Workshop*, vol. 1525, pp. 306-318, 1998.

[14] F.A.P Peticolas, R.J. Anderson and M.G. Kuhn, "Information Hiding – A Survey", in *proceeding of IEEE*, pp. 1062-1078, July 1999.

[15] M.M. Amin, M. Salleh, S. Ibrahim, et al., "Information Hiding Using Steganography", *4th National Conference On Telecommunication Technology Proceedings (NCTT2003)*, Shah Alam, Malaysia, pp. 21-25, January 14-15, 2003.