Comparison of LSB Steganography in GIF and BMP Images

Eltyeb E.Abed Elgabar, Haysam A. Ali Alamin

Abstract- ***Data encryption is not the only safe way to protect data from penetration given the tremendous development in the information age particularly in the field of speed of the processors and the cryptanalysis. In some cases, we need new technologies or methods to protect our secret data. There has emerged a set of new technologies that provides protection with or without data encryption technology such as data hiding. The word steganography literally means 'covered writing'. It is derived from the Greek words "stegos" meaning "cover", and "grafia" meaning "writing". Steganography functions to hide a secret message embedded in media such as text, image, audio and video. There are a lot of algorithms used in the field of information hiding in the media; the simplest and best known technique is Least Significant Bit (LSB).***

In this paper we have made a comparison and of the (LSB) algorithm using the cover object as an image. From this image, we have chosen two types: Gif and BMP. The comparison and is based on a number of criteria to find out the strengths and weaknesses when using any of the two types.

Index Terms—About four key words or phrases in alphabetical order, separated by commas.

Index Terms—About four key words or phrases in alphabetical order, separated by commas.

I. INTRODUCTION

Steganography is the art and science of hiding information by embedding messages within other, seemingly harmless message. Steganography means "covered writing" in Greek [1]. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" [2] defining it as "covered writing". The main goal of steganography is to hide the presence of a message within another message called cover message " a text file, an image file, audio file or video file", so steganography can be seen as the complement of cryptography whose goal is to hide the content of a message.

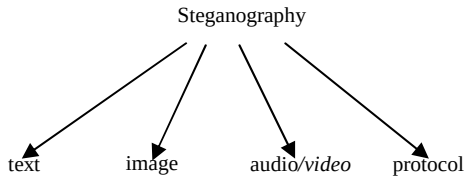

Fig.1 *Categories of Steganography*

Manuscript received September, 2013.

Eltyeb E. Abed Elgabar, Information Technology, King Abdul Aziz University, Jeddah, Saudi Arabia.

Haysam A. Ali Alamin, Information Technology, King Abdul Aziz University, Jeddah, Saudi Arabia.

A. Basic terms

- Cover-object, c: the original object where the message has to be embedded. Cover-text, cover-image,...
- Message, m: the message that has to be embedded in the cover-object. It is also called stego-message or in the watermarking context mark or watermark.
- Stego-object, s: The cover object, once the message has been embedded.
- Stego-key, k: The secret shared between A and B to embed and retrieve the message

B. The steganographic process

- Embedding function, E: is a function that maps the tripled cover-object c, message m and stego-key k to a stego-object s. $\mathrm{E}(c, m, k) = s$
- Retrieving function, D: is a mapping from s to m using the stego-key k. $\mathrm{D}(s, k) = m$
- A secret key steganographic system [12] can be defined as the quintuple $\delta = < C, M, K, E, D >$ where C is the set of possible cover-objects, M is the set of messages with $|C| \geq |M|$, K the set of secret keys, $\mathrm{E}: C \times M \times K \rightarrow C$ and $\mathrm{D}: C \times K \rightarrow M$ with the property that $D(E(c, m, k), k) = m$
- for all $m \in M, c \in C$ and $k \in K$.

II. IMAGE

A. Image definitions

To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image [4]. This numeric representation forms a grid and the individual points are referred to as pixels. Most images on the Internet consists of a rectangular map of the image's pixels (represented as bits) where each pixel is located and its color [8]. These pixels are displayed horizontally row by row. The number of bits in a color scheme, called the bit depth, refers to the number of bits used for each pixel [10]. The smallest bit depth in current color schemes is 8, meaning that there are 8 bits used to describe the color of each pixel [10]. Monochrome and grayscale images use 8 bits for each pixel and are able to display 256 different colors or shades of grey. Digital color images are typically stored in 24-bit files and use the RGB color model, also known as true color [10]. All color variations for the pixels of a 24-bit image are derived from three primary colors: red, green and blue, and each primary color is represented by 8 bits [4]. Thus in one given pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-million colors [10]. Not surprisingly the larger amount of colors that can be displayed, the larger the file size [8].

B. Image format

There are several types of image file formats that can be used for steganography and each has certain advantages and disadvantages for hiding messages. There are two types of images on the Internet available in a palette format GIF, BMP, JPEG, TIFF and PNG.

B.Graphics Interchange Format (GIF)

GIF is used for the purpose of storing multiple bitmap images in a single file for exchange between platforms and images. It is often used for storing multi-bit graphics and image data. GIF is not associated with a particular software application but was designed "to allow the easy interchange and viewing of image data stored on local or remote computer systems". GIF is stream based and is made up of a series of data packets called blocks (which can be found anywhere in the file) and protocol information. GIF files are read as a continuous stream of data and the screen is read pixel by pixel.GIF is used also because it applies lossless file compression method.

B.1General GIF format properties

- Can be compressed to a small size**.**
- Are commonly used for images presented on the web.
- GIF files allow only 8-bit indexed color.
- GIF files use lossless LZW compression .
- GIF files support transparency.
- Animated GIF files can be created by sequences of single images.
- GIF files can be saved in an interlaced format that allows progressive download of web images (low-resolution version of an image first then gradually comes into focus the rest of the data is downloaded**.**

GIF images only have a bit depth of 8, the amount of information that can be hidden is relatively less than Windows Bitmap (BMP) [13]. According to the image analysis in [13], BMP is not widely used in web application [20] and thus the suspicion might arise if it is transmitted with a LSB steganographic method. Heuristically, if more bits are altered it may result in a larger possibility that the degradation of the image can be detected with the human eye.

GIF images uses indexed color, which contain a color palette with up to 256 different colors out of 16,777,216 possible colors [14], and the Lempel- Ziv-Welch (LZW) compressed matrix of palette indices. Thus, LSB method in GIF is efficient when used for embedding a reasonable amount of data in an image [13].

C. Bitmap images (BMP)

Bitmap images are were introduced by Microsoft to be a standard image file format between users of their Windows operating system. The file format is now supported across multiple file systems and operating systems, but is being used less and less often. A key reason for this is the large file size, resulting from poor compression and verbose file format. This is, however, an advantage for hiding data without raising suspicion. To understand how bitmap images can be used to conceal data, the file format must first be explained. A bitmap file can be broken into two main blocks, the header and the data. The header, which consists of 54 bytes, can be broken into two sub-blocks. These are identified as the Bitmap Header, and the Bitmap Information. Images which are less than 16bit have an additional sub-block within the header labeled the Color Palette [11].

C.1 General GIF format properties

- BMP files are.
- a bitmap format that can be uncompressed, or compressed with RLE
- BMP files are.
  - in 1-bit black and white.
  - 8-bit greyscale.
  - 16-, 24- or 32-bit RGB color.
  - or 4- or 8-bit indexed color .
- BMP files don't support CMYK color.
- Transparency is supported for individual pixels as in GIF files.
- Alpha channels are supported in new versions of BMP.

Table 1: Comparison of GIF & BMP Images.

	GIF	BMP
File types	Graphics interchange format	Windows bitmap
File Suffix	.gif	.bmp
Standard color mode	Index color Grayscale	Index color RGB
Color Depth	8-bit color	1-32 bit color
Compression algorithms	Lossless (LZW)	Lossless (REA)

III. OVER VIEW OF LSB ALGORITHM

A digital image consists of a matrix of color and intensity values. In a typical gray scale image, 8 bits/pixel are used. In a typical full-color image, there are 24 bits/pixel, 8 bits assigned to each color components.

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image [4]. The least significant bit in other words, the 8th 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 and 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 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [9]. For example a grid for 3 pixels of a 24-bit image can be as follows:

(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:

(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 [9]. Since there are 256 possible intensities of each primary color, changing the LSB of a pixel results in small changes in the intensity of the colors. 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 [4].

In the above example, consecutive bytes of the image data from the first byte to the end of the message are used to embed the information. This approach is very easy to detect. A slightly more secure system is for the sender and receiver to share a secret key that specifies only certain pixels to be changed. Should an adversary suspect that LSB steganography has been used, he has no way of knowing which pixels to target without the secret key [5]. In its simplest form, LSB makes use of BMP images, since they use lossless compression. Unfortunately to be able to hide a secret message inside a BMP file, one would require a very large cover image.

The advantage of LSB embedding is its simplicity and many techniques use these methods [4]. LSB embedding also allows high perceptual transparency. However, there are many weaknesses when robustness, tamper resistance, and other security issues are considered. LSB encoding is extremely sensitive to any kind of filtering or manipulation of the stego-image. Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image is very likely to destroy the message. Furthermore an attacker can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image.

A. *The LSB Algorithm*

1) Select *cover-object* (GIF/BMP) c as an input.
2) Encode the c in binary[15].
3) The Secret Message, m .
4) Encode the m in binary [15].
5) Choose one pixel of the c randomly.
6) Use a pixel selection to hide information in the c .
7) Save the new image (*Stego-object*) s .

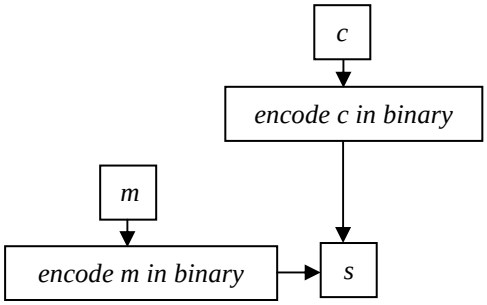

Fig.2: The LSB Algorithms

B. *LSB in GIF*

We can used GIF images for LSB steganography [17], although extra care should be taken. The main issue with the palette based approach is that if one changes the least significant bit of a pixel, it could result in an entirely different color since the index to the color palette gets modified. One possible solution to this problem is to sort the palette so that the color differences between consecutive colors are minimized. The strong and weak points regarding embedding information in GIF images using LSB is that since GIF images only had a bit depth of 8, the total amount of information that could be embedded will be less. GIF images are vulnerable to statistical as well as visual attacks, since the palette processing which has to be done on the GIF image leaves a clear signature on the image. This approach was dependent on the file format as well as the image itself, since a wrong choice of image could results in the message being visible.

C. *LSB in BMP*

Since BMP is not widely used the suspicion might arise, if it is transmitted with an LSB stego. When image are used as the carrier in Steganography they are generally manipulated by changing one or more of the bits of the byte or bytes that make up the pixels of an image. The message can be stored in the LSB of one color of the RGB value or in the parity bit of the entire RGB value. A BMP is capable of hiding quite a large message. LSB in BMP is most suitable for applications, where the focus is on the amount of information to be transmitted and not on the secrecy of that information. If more number of bits is altered, it may result in a larger possibility that the altered bits can be seen with the human eye. But with the LSB the main objective of Steganography is to pass a message to a receiver without an intruder even knowing that a message is being passed is being achieved.

Table 2: Comparison of LSB for GIF & BMP Images

	GIF	**BMP**
Efficient when amount of data reasonable	Medium	High
Percentage Distortion less resultant image	Medium	High
Steganalysis detection	Low	Low
Amount of embedded data	Low	High
Robustness against image manipulation	Low	Low
Invisibility	Medium	High
Robustness against statistical attacks	Low	Low
Independent of file format	Low	Low
Payload capacity	Medium	High
Unsuspicious files	Low	Low

"High = 2, Medium = 1 and Low = 0"

Table 3: Comparison of LSB for GIF & BMP Images

	GIF	**BMP**
Efficient when amount of data reasonable	2	0
Percentage Distortion less resultant image	2	1
Steganalysis detection	0	0
Amount of embedded data	2	1
Robustness against image manipulation	0	0
Invisibility	2	1
Robustness against statistical attacks	0	0
Independent of file format	0	0
Payload capacity	2	1
Unsuspicious files	0	0

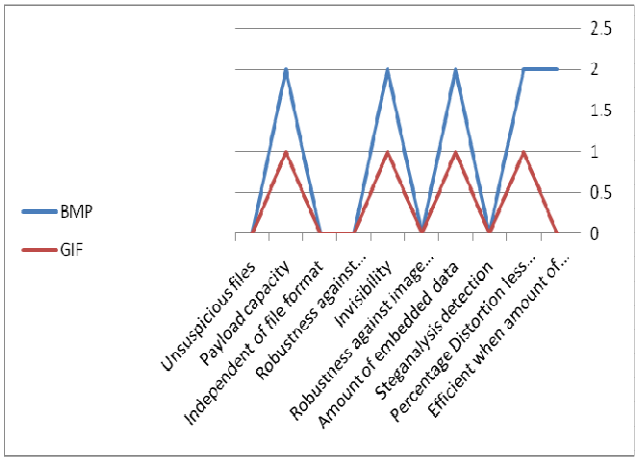

Fig.3: Comparison of LSB for GIF & BMP Images

IV. THE APPLYING AND EVALUATION

A. *The original image (before hiding)*

Fig.4"(a)" : GIF Image

Fig.4"(b)": BMP Image

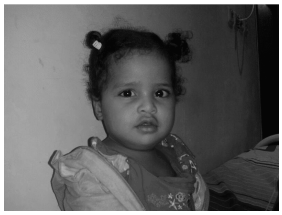

Fig.5"(a)" : GIF Image

Fig.5"(b)" : BMP Image

Table 4: Properties of GIF & BMP Images

Name	GIF(a)			BMP(b)		
	Size MB	**Dimensi-on** X*Y	**Dept-h** bpp	**Size** MB	**Dimensi-on** X*Y	**Dept-h** bpp
Fig.4	0.28	800*600	8	1.37	800*600	24
Fig.5	0.23	800*600	8	1.37	800*600	24

B. *The image after hiding*

Fig.6"(a)" : GIF Image

Fig.6"(b)": BMP Image

Fig.7"(a)" : GIF Image

Fig.7"(b)": BMP Image

V. CONCLUSION

In the images of the kind GIF we find very little data embedded, as if resistance to statistical attacks is low. When we increase the amount of data the image becomes distorted and is subject to discovery. For the images of the kind BMP, data type that can be embedded is large and the image is not distorted because of the ability of this kind of images for carrying amount of data without notice.

REFERENCES

[1] "Watermarking Application Scenaros and Related Attacks ", IEEE international Conference on Image Processing, Vol. 3, pp. 991 – 993, Oct. 2001.

[2] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf.

[3] Henk C. A. van Tilborg (Ed.), "Encyclopedia of cryptography and security", pp.159. Springer (2005).

[4] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal,February 1998.

[5] Krenn, R., "Steganography and Steganalysis", http://www.krenn.nl/univ/cry/steg/article.pdf

[6] Pallavi Hemant Dixit, Uttam L. Bombale, " Arm Implementation of LSB Algorithm of Steganography", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-3, February 2013.

[7] "Reference guide:Graphics Technical Options and Decisions", http://www.devx.com/ /Article/1997.

[8] Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June 2001.

[9] NXP & Security Innovation Encryption for ARM MCUs ppt.

[10] Owens, M., "A discussion of covert channels and steganography", SANS Institute, 2002.

[11] "MSDN:About Bitmaps" <http://msdn.microsoft. com/library/default.asp?url=/library/enus/gdi/bitmaps_99ir.asp?frame =tru>, 2007,M Corporation.

[12] V. Lokeswara Reddy, Dr. A. Subramanyam and Dr.P. Chenna Reddy, " Implementation of LSB Steganography and its Evaluation for Various File Formats", Int. J. Advanced Networking and Applications, Volume: 02, Issue: 05, Pages: 868-872 (2011).

[13] Neeta Deshpande, Snehal Kamalapur and Jacobs Daisy, "Implementation of LSB steganography and Its Evaluation for Various Bits", 1st International Conference on Digital Information Management, 6 Dec. 2006 pp. 173-178.

[14] J. E. Boggess III, P. B. Nation, M. E. Harmon, "Compression of Colour Information In Digitized Images Using an Artificial Neural Network", Proceedings of the IEEE 1994 National Aerospace and Electronics Conference, Issue 23-27 May 1994 Page(s):772 - 778 vol.2.

[15] Atallah M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 - 391.

[16] Ze-Nian Li and Marks S.Drew, "Fundamentals of Multimedia, School of computing Science Simon Faster University, Pearsoll Education, Inc, 2004.

[17] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray-scale images," IEEE Multimedia, vol. 8, no. 4, pp. 22–28, Oct. 2001.

[18] Priya Thomas," Literature Survey On Modern Image Steganographic Techniques", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 5, May - 2013 ISSN: 2278-0181.

[19] V. Lokeswara Reddy, Dr. A. Subramanyam, Dr.P. Chenna Reddy ,"Implementation of LSB Steganography and its Evaluation for Various File Formats", Int. J. Advanced Networking and Applications Volume: 02, Issue: 05, Pages: 868-872 (2011).

[20] Roshidi Din and Hanizan Shaker Hussain, "The Capability of Image In Hiding A Secret Message", Proceedings of the 6th WSEAS International Conference on Signal, Speech and Image Processing, September 2006.

DR.ELTYEB ELSAMANI ABD ELGABAR ELSAMANI, Assistant Professor(2009) in the Computer Science at Faculty of Computer Science and Information Technology, Information Technology Department - Khulais - King Abdul Aziz University- Jeddah - Saudi Arabia. Assistant Professor in the Computer Science at the Department of Computer Science, Faculty of Computer Science and Information Technology - Alneelain University - Khartoum - Sudan. . Main specialization is Information Security in particular and Encryption in specific. A member of the committee of Standard specifications for Computers Hardware and Peripherals in the National Information Center (NIC) - Khartoum -Sudan , member of Standard specifications for Network Hardware in the National Information Center (NIC) - Khartoum -Sudan, and member of Curriculum of information technology department - Faculty of Kamleen Ahlia- Gazera Sudan.

Haysam Elshakh Ali Elamin, Assistant Professor(2010) in the Computer Science at Faculty of Computer Science and Information Technology, Information Technology Department - Khulais - King Abdul Aziz University- Jeddah - Saudi Arabia. Assistant Professor in the Computer Science at the Department of Computer Science, Faculty of Computer Science and Information Technology - Alneelain University - Khartoum - Sudan. . Main specialization is Information Security in particular and Encryption in specific. A team leader at NIC (National Information Center) Sudan, hardware committee determining the minimum hardware specification - Khartoum -Sudan , member of Standard specifications for Network Hardware in the National Information Center (NIC) - Khartoum -Sudan, and team member of GRP planning committee at the the National Information Center (NIC).