A Steganography Algorithm and Cryptography Techniques for Hiding Image

Zanbaq Hekmet Thanon

Republic of Iraq - The Iraqi Ministry of Higher Education and Scientific Research- University of Information Technology and Communications

Abstract: ***Steganography can be defined as the procedure of hiding a type of communication medium (i.e. text, audio or image) inside another type of medium. This paper will be discussing (Proposed system, utilized for hiding and extracting the information. The Proposed system embeds a text within an image. Each of the sender and the receiver don't need exchanging any information prior to using the system, therefore, it can also be said that the system is purely steganographic. This paper discusses producing a stego-image so that the embedded message cannot be perceived by a random observer but can be noticed easily by the intended receiverthatknowsthe way of extracting the message. Proposed system has the goal of preventing the detection of a secret message. It is a technique to embed a text inside harmless cover-image (we used GIF, JPG and BMP image formats), and produce the stego-image (BMP image format) without making any visible changes to it. We can check the histogram for each of the cover and stego-images to verify if there is any different between them. The implementation results via MATLAB ver.8.1 package***

Keywords: Cryptography, Steganography, Stego- image, GIF, JPG, BMP, GUI, LSB

1. Introduction

Steganography can be defined as the art of hiding things inside other things, for instance, embedding a text within an image in some way. Typically, a random person wouldn't be aware of the embedded message in case it's well hidden. [1]

In general, a steganographic message will appear as something else, such as a shopping list, an article, an image, or another "cover" message.

Usually, steganographic messages are initially encrypted using a traditional method, and after that a cover-text is somehow altered for containing that encrypted message, which results in the stego-text. [2]

Computer steganography relies on a couple of principles. The first one is that files containing digital images or audio may be modified to a specific degree without compromising their functionality which is not like other kinds of data which must be exact to properly operate. The second principle is concerned with the human inability in distinguishing minimal alterations in the quality of the image colour or audio that is especially simple to benefit from in items containing repeated data, whether it is a 16-bit audio, an 8-bit or a 24-bit image. While in the subject of images, altering the LSB value of the pixel colour will not lead to any noticeable changing of that color. [3]

Images are common means of embedding messages. What should be noted is that gif-s and bmp-s are not loss images, while jpgs are lossy ones; therefore, embedding data in those images usually follows slightly different approaches. In gif-s it is typical that colors are of high importancewhile jpg-s usually embed data either more openly in the image as a picture or in the binary structure of the file [1]

The larger the cover message is (according to data contents) relative to the embedded data; the easier it is to embed the latter. Therefore, digital images (containing large data amount) are typically utilized for hiding data on the Internet and on other mediums of communication. For instance a 24-bit bitmap will include 8 bits that represent every one of the 3 colors (i.e. red green and blue). Considering the red alone there will be 2^8distinctshades of red. For example, the difference between "11111111" and "11111110" is unlikely to be detectable by the human eyes. Thus, the LSB may be utilized for something other than color information. If the attempt is also doing it with the blue and the red, the result is getting one letter of ASCII text for 3 pixels.

Putting this in a more formal way, the aim in making steganographic hiding hard to be detected is ensuring that the alterations to the cover (i.e. the original signal) because of the injection of the payload (in other words, the signal to covertly hide) seem negligible in a statistical way; which means that the alterations are not noticeable from the carrier's noise floor.[2] {for understanding the way steganography is implemented on images, one has to be aware of what digital images are on computers, an image can be defined as an array of numbers representing intensities of light at different points (i.e. pixels). {A typical image size is 640×480 pixels and 256 colours (in other words eight bits/pixel). Such imagesmayinclude about 300 kilo-bits of data. Images are usually stored in 24-bit files or 8-bit files. A 24-bit image offers the maximal space tohide data; nevertheless, it may be of a bigsize (except for the JPEG image formats)}[4]{With eight bits per pixel, there are 2^8 ⁽256) colour values. With 24 bits per pixel there are 2^{24} (16,777,216) colour values.

Colour variations for pixels are obtained from three main colours: red, green, and blue.
24 bit image example:
A 24 bit image uses 3 bytes for the representation of a color (i.e. eight bits = one byte)
1 pixel = ("00100111 11101001 11001000") redgreenblue [63s] [64]

{Those three bytes may be represented in binary, hexa-decimal, decimal forms. A white back-ground will typicallyequal the value “FFFFFF”: which is 100% red (FF), 100% green (FF), and 100% blue (FF). Its decimal value is 255, 255, 255, and its binary value is “11111111, 11111111, 11111111”, which are the 3 bytes that make up the colour white.

This definition of a white back-ground is quite close to the color definition of one pixel in an image. Pixel representation is associated with the size of the file. For instance, supposingto have a 24-bit image 1,024 pixels wide by 768 pixels high—a typical resolution for high-resolution graphics. Such imagesincludeover2 M. pixels, each of which has such a definition,and that would result a file that exceeds 2 Mega-bytes.}[4]

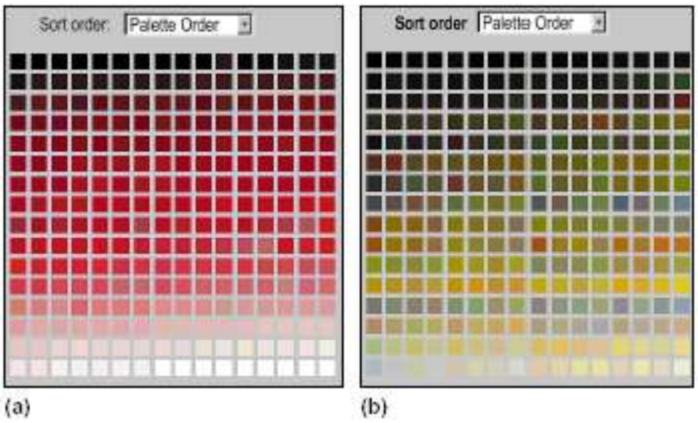
2. Data Embedding

{Embedding datathat is to be hidden, into an image needsa couple of files. The 1st one is the “innocent-looking” image which will be holding the secret data, also known as the cover. The 2ndone is the secret message—which is the data to be embedded. A message could be plaintext, cipher-text, other images, or anything whichmay be hidden in a bit sequence. After they get combined, the cover and the hidden data form a stego-image. A steganographic-key (a kind of pass-word) can be utilizedfor hiding, and afterwards decoding, the message as well.

In 8-bit colour images, every one of the pixels is denoted as one byte, and every one of the pixels simply represents a colour index table (i.e. a palette) which has 256 color possibilities. Therefore, the pixel’s value is in the range of (0-255). The software merely paints the given colour on the mpnitor at the chosen pixel location. Fig. 3.1a, a red palette, represents subtle changes in color variations: visually distinguishing between a wide range of those colours is very hard. Fig. 3.1b illustrates subtle colour variations as well as those whichappear drastic.

Taking under consideration an image where to embed information, onehas to take under consideration the image and the palette as well. As it is obvious, an image that hasbigregions of uniform colors is not a goodoption, as variances produced from the hiddendata will be perceivable in the uniformregions. It is illustrated in Fig. 3.1b that the palette for the Renoir coveris a successful choice of cover to hold data.

As soon as one selects a cover, theyhave tochoose a method to embed the datatheyneed to hide.


Sort order: Palette Order

Sort order: Palette Order

Figure: Representative colour palettes. (a) depicts a 256-color red palette and(b) a 256-color Renoir palette, called that waydue to the fact that it is derived from a 256-colour representation of Renoir’s “Le Moulin de la Galette.”}

3. Steganography in images

{Considering graphical image as a cover (the "container") made up of pixels. every one of the pixel's colors is dependent on a numerical value that is in the range between 0 and 255. An eight-bit base two number represents that value to the computer; for instance, the byte “00000000” is equal to "0". The right-most bit is the LSB, due to the fact that the 7 bits to the LSB's left includea sufficient amount ofdatafor establishing the appropriate pixel color. Swapping out the LSB's values is not effective on the pixel's appearance to the eye. Therefore, a steganography program embeds the message's bits within the least significant bit for every one of the bytes of the graphical image.

The development in the field of computers has created an incredible capability for using steganography in images and detecting that there is even a secret message is almost impossible. As soon as the knowledge that a message is embedded, disclosing the contentsof the message is an even more difficult task. That is why there are specialist that use steganalysis's to do so.

The complexity of steganography can vary; the information can be embedded only in specific spots in the image. For example the information would be less conspicuous if it was in the 'noisy' area of the image, or the information can be randomly scattered throughout the image. Any technique is accompanied with negative and positive usages.

{According to Neil F. Johnson's article, "Steganography," a 640×480 image utilizing 256 colours may be holding about 300 Kilo-Byte message or image. With a 24-bit image 1024×768 three bytes define very one of thepixel's values, therefore, every one of the pixelsincludes3 bits of the message which results in a 2 Mega-Byte file. Steganographic images have large capacities in which to embed contraband images or illegally acquired data.

4. How Much Data May Be Embedded?

There isn’t an exact answer to precisely how much data may be embedded via steganography. Nevertheless, there is a couple of rules: First, big or "busy" files may obviously contain moreamount data. The more dynamic the medium is—for example, videos vs. Images—the more places there areforembedding data.

Second, the attempt of shoehorning too much data presents detection risk via distorting the file so that the change is perceivable by tools of steganalysis, or to the naked eye. "The point at which you risk being discovered depends on the content of the cover image," Faridstated. "An image with large areas of uniform color or gray isn't so good because perturbations will be noticeable. An image with highly textured regions is better."

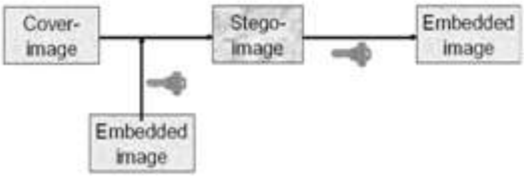
The insertion of a steganographic data to an image is a complicated task, and suitable software is required for the extraction of the embedded data. Steganography is a highlysophisticated process that isperformed by people for whom the data, and its privacy, is a matter of "life-and-death".

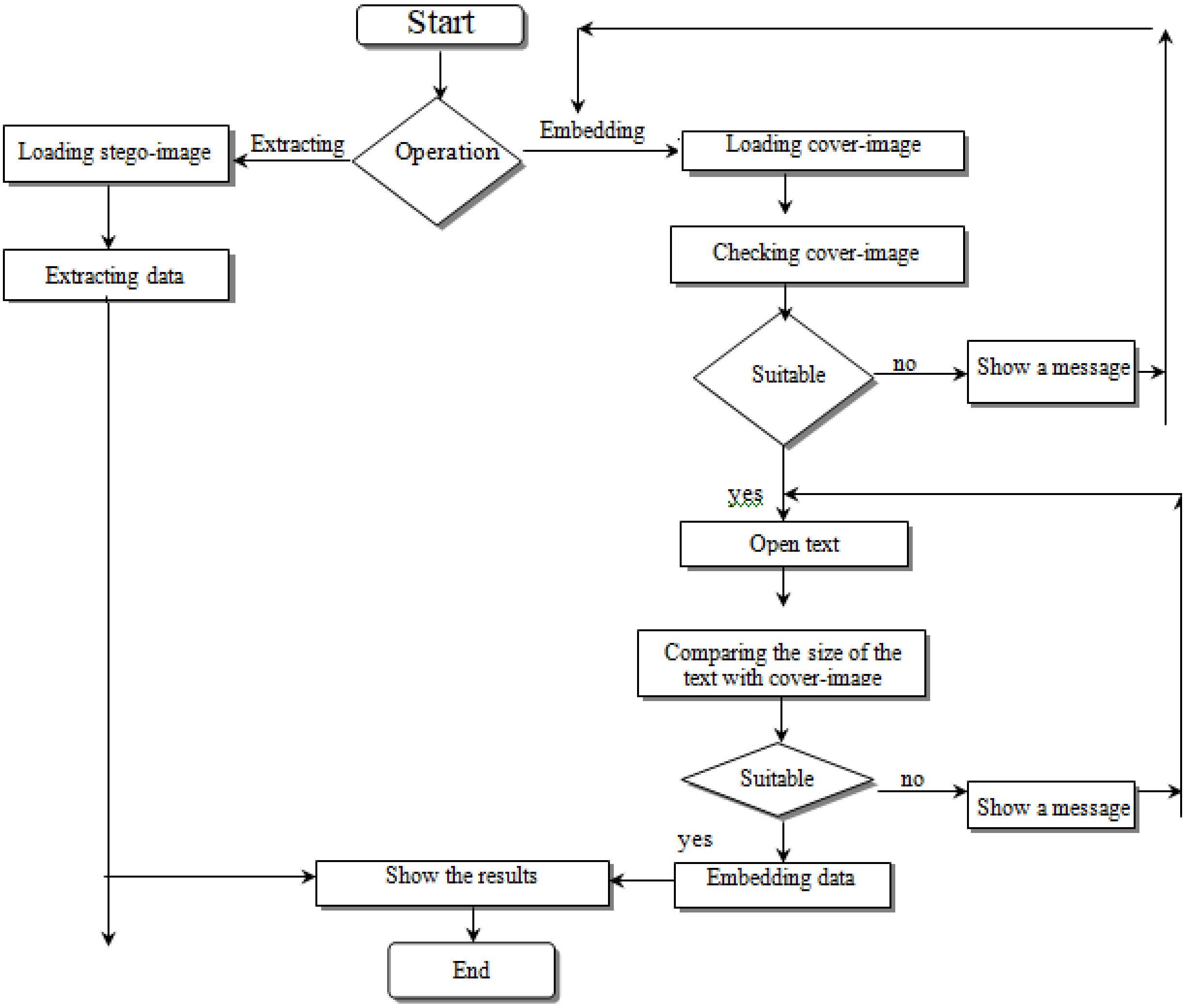
{The image file size corresponds directly to the number of pixels and the definition of the colour granularity. An ordinary 640×480 pixel image that uses a palette of 256 colours would be requiring a file nearly 307 Kilo-Bytes in size (i.e. 640 • 480 bytes), while a 1024×768 pixel high-resolution 24-bit colour image would produce a 2.36 Mega-Byte file (i.e. 1024 • 768 • 3 bytes).} {Putting data in that 32nd bit would notnoticeablyupdate the image. An eight-bit image measured 480 by 100 pixels, the size of many web page banners,is in theory capable of holding 5000 letters. This is a small image. A big 32-bit image may hold even more.}[5]

5. Proposed System for Hiding Information

Helpful Terms to Know in steganography

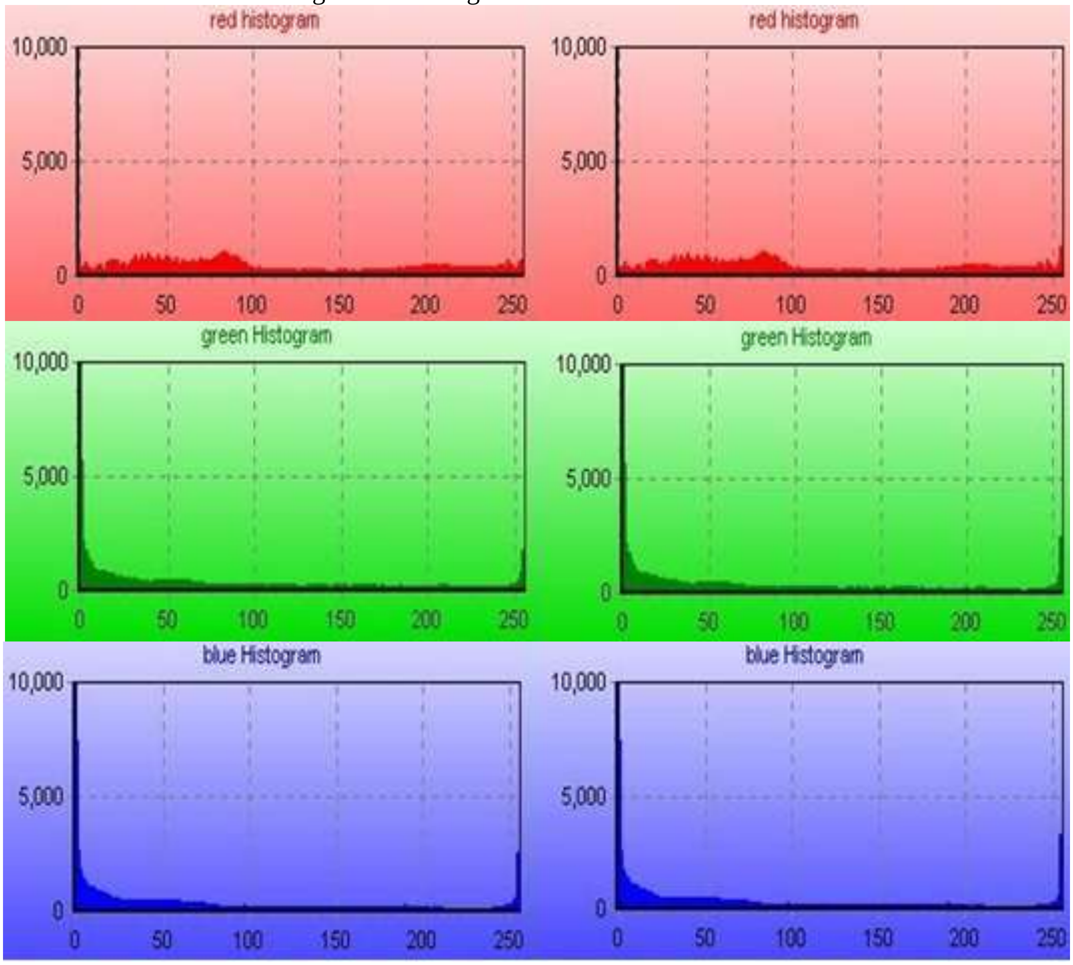
- Cover Media (cover-text, cover-image, cover-audio): innocuous data that will hold the hidden data.
- Embedded data: the message that has to be kept in secret.
- Stego-object: produced by hiding the embedded data into the cover data.
- Stego-key: utilized for controlling the hiding procedure and restricting the detection and recovery of the hidden message.





Proposed System's Flowchart

Results of embedding text into Penguins



The left histogram is for the cover-image and the right histogram is for the stego-image

6. Conclusions

Steganography is a subject of high interest and is outside of the typical cryptography and system administration. However, it is very real; this isn’t merely a thing implemented in a lab or an arcane subject of academic studies. Steganography may actually be quite real to use it in our life.

In spite of an existence of the numerous from Steganography's programs, except the building of an another program is a necessity in as much as the increasing desire on Steganography's programs, so for the tendency of the users for using it did much from their tendency for the use of Cryptography, and the reason as we said ahead of time by that the interest of a Stenography is the hiding of the message exist, so then it doesn't pull the suspicion.

The following are some points concluded from this study:
Most of the messages of the email are a text type; therefore we choose the text to be the embedded object. Steganographic images have large capacities in which to embed data. We've chosen to use BMP for the proposed system because they are of a very simple format and very easy to work with compared to other formats such as GIF and JPEG.

Using cryptography add a level of security/secrecy to the proposed system, so in the case where an embeddeddata is encrypted, it has to be decrypted in case it gets discovered.

References

[1] Kharrazi, M., Sencar, H. T., and Memon, N. (2004). Image Steganography: Concepts and practice. In WSPC Lecture Notes Series

[2] Domenico Daniele Bloisi , Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and Applications

[3] D.R. Stinson, Cryptography: Theory and Practice, Boca Raton, CRC Press, 1995.

[4] Provos, N. and Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE SECURITY &PRIVACY

[5] Chandramouli, R., Kharrazi, M. &Memon, N., "Image Steganography and teganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003

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

[7] Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999