Volume 7, Issue 1, January 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review in Using Steganography Applications in Hiding Text Inside Digital Image (BMP)

Nafisa Ahmed Hussein. Rustom
National Ribat University
Khartoum, Sudan

Nadir Abdelrahman Ahmed Farah
Information Systems Department, University of Bisha
Bisha, Saudi Arabia

DOI: 10.23956/ijarcsse/V7I1/01108

Abstract- Steganography refers to the methods that using to hide information inside objects known as "Cover Objects". These objects include image, audio, and video. Inside objects the information remains concealed to any unauthorized recipient. digital images are the most popular because of their repetition on the Internet. the information progressed and data become more and more valuable. This paper intends to give an review of image Steganography, its uses and applications, Specifically BMP Format.

Keywords- Steganography, Digital Image, Data hiding, BMP Image, Applications, Stego Image.

I. INTRODUCTION

The purpose from Information security means protecting information from unauthorized access, use , modification or erase. so, many studies focus on the hidden of data to guarantee not vulnerable the data to any dangerous affect them.

Steganography is the art and science of concealing a message within a carrier medium. The first recorded instance of this practice dates back to 440 BC, when Demaratus passed a message hidden beneath the wax surface of a writing tablet, in order to warn Greece about an impending attack[1]. The main destination of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is also to keep others from thinking that the information even exists. If a steganography method causes someone to suspect the carrier medium, then the method has failed[2].

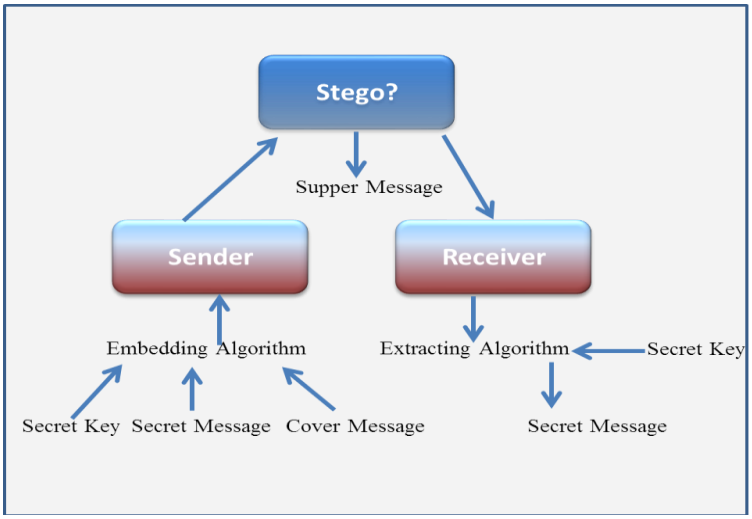

Fig. (1) General Model for Steganography

The main terminologies used in the Steganography systems are: the cover message, secret message, secret key and embedding algorithm. The cover message is the carrier of the message such as image, video, audio, text, or some other digital media. The secret message is the information which is needed to be hidden in the suitable digital media. The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is the way or the idea that usually use to embed the secret information in the cover message[10].

II. RELATED WORK

A. Digital Image

A digital image is intrinsically a multivariate system, which is a collection of data stored in pixels, each usually highly correlated to its neighbors[3].

B. Data Hiding

Data hiding techniques could play a major role to embed important data into multimedia files such as images, videos or sounds. Because digital images are insensitive to human visual system, therefore images could be good cover carriers. Data hiding has two major applications watermarking and steganography. Watermarking merely extends the cover source with extra information. Steganography techniques are used to store watermarks in data [4].

C. BMP Image

The BMP file format, also known as bitmap image file or device independent bitmap (DIB) file format or simply a bitmap, is a raster graphics image file format used to store bitmap digital images, independently of the display device (such as a graphics adapter), especially on Microsoft Windows and OS/2 operating systems [5]. The typical size of a bitmap file is quite large due to the amount of information stored within it .

D. Stego Image

The cover image with a secret message concealed within it is known as the Stego image. It is used at the recipient site for extracting the hidden message[13].

E. Applications

An application is any program, or group of programs, that is designed for the end user. Application software can be divided into two general classes: systems software and *applications software*. Applications software (also called *end-user programs*) include such things as database programs, word processors, Web browsers and spreadsheets[11]. System software is a type of computer program that is designed to run a computer's hardware and application programs. If we think of the computer system as a layered model, the system software is the interface between the hardware and user applications[12].

III. CATEGORIES OF IMAGE STEGANOGRAPHY

Steganography can be applied to images, text, videos, digital signals as well as continuous signals and other information formats, but the preferred formats are those which repeat the data. Repeated bits of an object are those bits that can be altered without the alteration being detected easily[6].

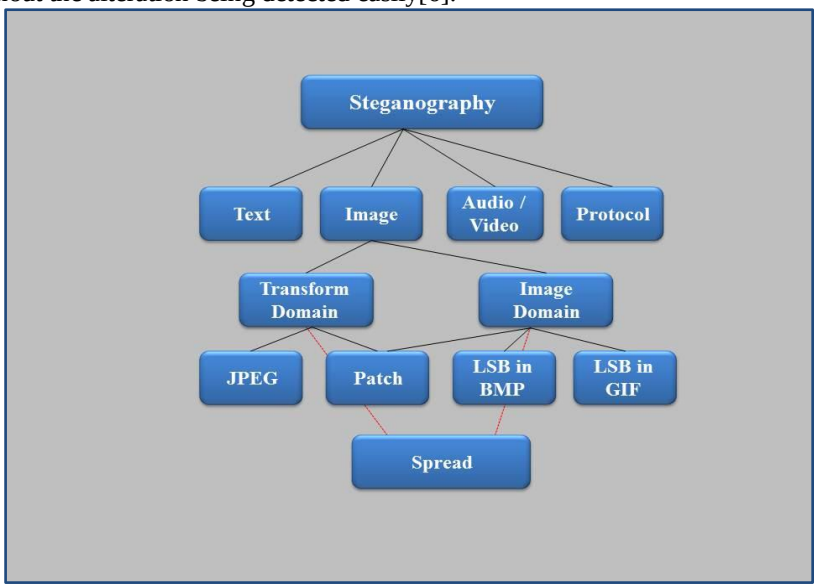

Fig. (2) Categories of Image Steganography.

IV. TYPES OF STEGANOGRAPHY TECHNIQUES

A. Pure Steganography

Pure steganography is a steganography system that doesn't require prior exchange of some secret information before sending message. Therefore, no information is required to start the communication process.

B. Secret Key Steganography

A secret key steganography system is similar to a symmetric cipher, where a sender chooses a cover and embeds the secret message into the cover using a secret key. If the secrete key used the embedding process is known to the receiver, he can reverse the process and extract the secret message.

C. Public Key Steganography

Public key steganography does not depend on the exchange of a secrete key. It requires two keys, one of them private (secrete) and the other public, the public key is stored in a public database [7].

V. IMAGE STEGANOGRAPHY

Image steganography is about exploiting the limited powers of the human visual system (HVS).Within reason, any plain text, cipher text, other mages, or anything that can be embedded in a bit stream can be hidden in an image.Digital image is the most common type of carrier used for steganography[9].

VI. BENEFITS OF IMAGE STEGANOGRAPHY

Data used to hide data in stegnography can be text or image. image stegnography can be helpful in a number of ways such as: [8]

- hiding the secret data.
- data authentication.
- ensuring authenticated data availability for academic usage.
- monitoring of data piracy.
- labelling electronic data/contents.
- copyright protection.
- ownership identification.
- providing confidentiality and integrity enhancement control of electronic data piracy.

VII. STEGANOGRAPHY EVALUATION

In order to examine steganography programs which were already available, it was necessary to first decide the criterion against which they would be graded. Various features characterize the strengths and weaknesses of the methods[13][14].

The criteria were decided to be as follows:

- **Accessibility:** The product must be easily obtainable and easy to install on different platforms.
- **Usability:** The product must be easy to use.
- **Robustness:** Robustness refers to the ability of embedded data to remain intact if the stego-image undergoes transformations, such as linear and non-linear filtering, addition of random noise, sharpening or blurring, scaling and rotations, cropping or decimation, lossy compression, and conversion from digital to analog form and then re-conversion back to digital form.
- **Hiding Capacity :**Capacity of a steganography system implies the amount of data that can be effectively hidden within a selected cover medium by a steganography algorithm without causing visual impairment to the image. The embedding rate is mostly expressed in absolute measurement (*such as the size of the secret message*) or in relative measurement called the data embedding rate (*given mostly in bits per pixel*).
- **Distortion of the cover image:** It is important that the embedding occur without significant degradation or loss of perceptual quality of the cover. In a secret communications application, if an attacker notices some distortion that arouses suspicion of the presence of hidden data in a stego-image, the steganography encoding has failed even if the attacker is unable to extract the message.
- **Perceptual Transparency:** The act of hiding the message in the cover necessitates some noise modulation.
- **Tamper Resistance:** Beyond robustness to destruction, tamper-resistance refers to the difficulty for an attacker to alter or forge a message once it has been embedded in a stego-image**.**

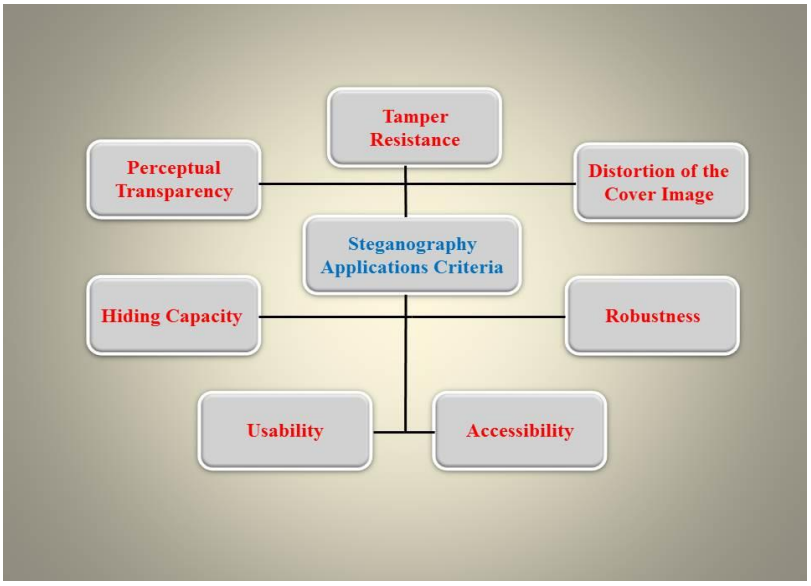

Fig. (3) Steganography Applications Criteria

VIII. STEGANOGRAPHY APPLICATIONS

Some of the popular applications are given below:

A. QuickStego:

It is a freeware application. QuickStego lets you hide text in pictures so that only other users of QuickStego can retrieve and read the hidden secret messages. Once text is hidden in an image the saved picture is still a 'picture', it will load just like any other image and appear as it did before[15].

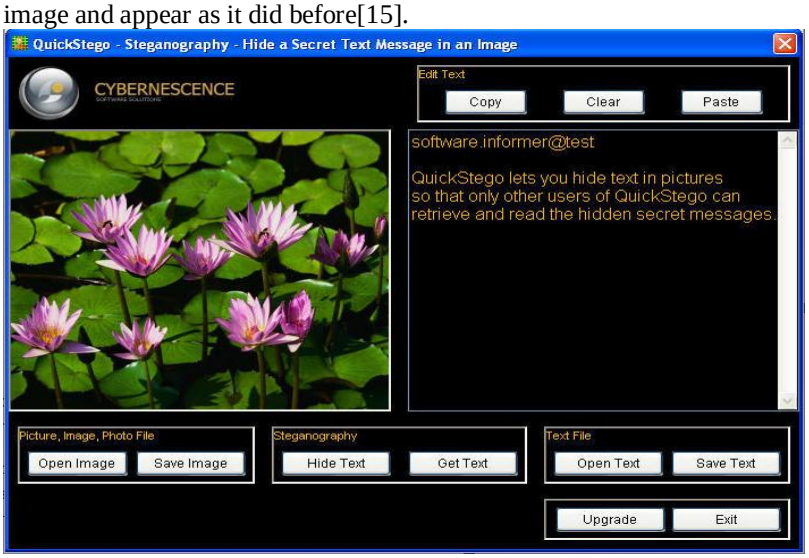

Fig. (4) Quickstego Screenshot

B. Xiao Steganography:

Is a lightweight cross-platform utility that comes packed with encryption capabilities for helping you hide text messages or other files within images or audio. Xiao Steganography enables users to choose between different encryption algorithms (e.g. RC2, DES, Triple DES, MD5), and set up passwords. You need to pick a saving directory and specify the filename. It also offers time estimation for completing the job[16].

Fig. (5) Xiao Steganography Screenshot

C. OpenStego:

Is just 203 KB in size and is easy to use steganography application. You can attach any type of secret message file to cover files. It is a java based, open source steganography software. You can run either BAT file or JAR file from the installed directory[17].

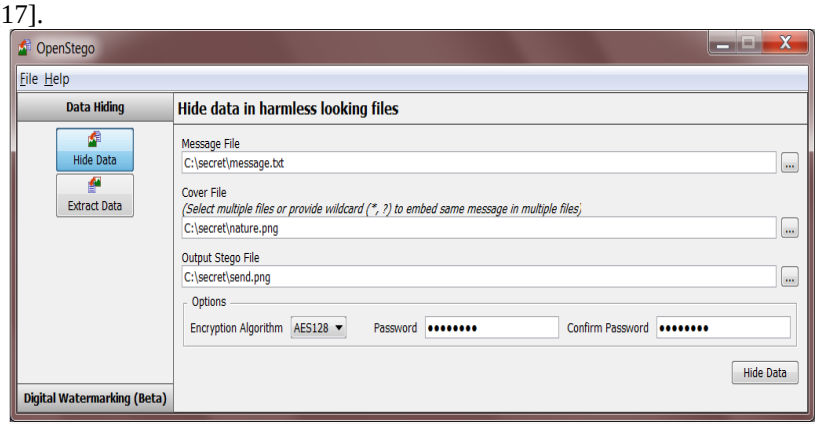

Fig. (6) OpenStego Screenshot

D. SilentEye:

Is a cross-platform application design for an easy use of steganography, in this case hiding messages into pictures or sounds. It provides a pretty nice interface and an easy integration of new steganography algorithm and cryptography process by using a plug-ins system[18].

Fig. (7) SilentEye

IX. CONCLUSIONS

Steganography is an effective way to hide sensitive information. It allows an individual to hide data inside other object such as text, audio, image, and video with hopes that no one can discover the hiden data. Steganography is very famous and important technique for data hiding as compared to other data hiding techniques. Digital image is the most common type of carrier used for steganography. This paper presented a background of Steganography and a review of some Steganography applications.

REFERENCES

[1] C. Gibbs, N. Shashidhar, "Steganography in Two - Dimensional Video Game Maps" , *ACSIJ Advances in Computer Science: an International Journal*, Vol. 4, Issue 3, No.15 , May 2015.

[2] Y. Perwej, F. Parwej, A. Perwej, " An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection" , *The International Journal of Multimedia & Its Applications (IJMA)* Vol.4, No.2, April 2012.

[3] P. Facco, F. Bezzo, M. Barolo, R. Mukherjee, J.A. Romagnoli. " Monitoring roughness and edge shape on semiconductors through multiresolution and multivariate image analysis",*AICHE Journal*,Volume 55, Issue 5 Pages 1082–1302, 2009.

[4] C. Maiti , D. Baksi, I. Zamider, P. Gorai, D. Ranjan Kisku, " Data Hiding in Images Using Some Efficient Steganography Techniques ", *Springer-Verlag Berlin Heidelber*, pp. 195–203, 2011.

[5] BMP (2017). [online].https://en.wikipedia.org/wiki/BMP_file_format

[6] A. Palimkar, S.H.Patil, " Using SBR Algorithm To Hid The Data Into The JPEG Image", *International Journal of Security(IJS)*, Volume (8) Issue (2) ,2014

[7] Computer Network and Information Security. (2015). [online].http://www.slideshare.net/BSheghembe/steganography-document.

[8] Navdeep, N. Goyal, " Hide Text in Images Using Steganography and a Review of Methods and Approach for Secure Stegnography", *International Journal of Research in IT & Management*, Volume 6, Issue 5, 2016

[9] N. Tiwari , M. Shandilya, " Evaluation of Various LSB based Methods of Image Steganography on GIF File Format" , *International Journal of Computer Applications* (0975 – 8887) ,Volume 6– No.2, September 2010.

[10] A. M. Al-Shatnawi, " A New Method in Image Steganography with Improved Image Quality" , *Applied Mathematical Sciences*, no. 79, 3907 – 3915, Vol. 6, 2012

[11] Application. (2017). [online]. www.webopedia.com/TERM/application.html

[12] System Software.(20115). [online].http://www.whatis.techtarget.com/definition/system-software

[13] R. Roy, S. Changder, " Quality Evaluation of Image Steganography Techniques: A Heuristics based Approach",*International Journal of Security and Its Applications* Vol. 10, No. 4, pp.179-196, 2016

[14] M. Juneja, " Data hiding Algorithm for Bitmap Images using Steganography",*Multidisciplinary Academic Journal Publisher*, 2(12):67-73]. (ISSN: 1553-9865), 2010

[15] Quickstego (2015). [online].http://www.quickcrypto.com/free-steganography-software.html

[16] Xiaosteganography (2017).[online].http://www.softpedia.com/get/Security /Encrypting/Xiao-Steganography.shtml

[17] OpenStego (2017). [online].http://listoffreeware.com/list-of-best-free-steganography-software-for-windows

[18] SilentEye (2010). [online]. http://silenteye.v1kings.io

