Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 11, November 2015, pg.187 – 193

RESEARCH ARTICLE

Proposed System for Hiding Information (Sunflower)

Baydaa Jaffer AL-Khafaji
Dr. Areej khuder Hassan
Nadia Mohammed Abdullamajed
Dr. Mejbel hammad awad
Dr. Wisam abed shukur
Omar Mejbel hammad
Computer Science; College of Education for Pure Science; Ibn-AL-Haitham

Abstract

Steganography is destined to become increasingly important as more citizens are looking at steganography to thwart policies of regulating or prohibiting the use of cryptography for personal privacy purposes and pass messages covertly. One should think of steganography, not as a replacement to cryptography but as a vital supplement to it.

Most of the existing steganographic algorithms are performed in pixel domain as it provides more embedding space (capacity), reliability and controllability in encoding/decoding of the hidden message.

The 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 both cover-image and stego-image to verify if there is any different between them.

To make the proposed system familiar and easier to the users, we used a Graphical User Interface (GUI).

Keywords

Cryptography, Steganography, Stego- image, GIF, JPG, BMP, GUI

Introduction

{Steganography, which is Greek for "covered writing," is a subset of the emerging discipline of information hiding. It is the science of transmitting a message between two parties in such a manner that an eavesdropper will not be aware that the message exists. Unlike cryptography, which seeks to hide the content of the message, with steganography we seek to hide the existence of the message. Of course, steganography and cryptography can be used in conjunction, so that message content may be protected cryptographically, even if the steganographic "shield" fails and the existence of the message is discovered} [1].

{Today digital data can be easily copied and multiplied without information loss. It has become imperative to verify the owner of a digital data, to identify illegal copies of the multimedia content and to prevent unauthorized distribution. Information hiding techniques have thus recently received great attention from the research community}[2].

{So, in our modern times, digital images, audio files, and streaming video have become carriers for hidden information, while our networks are the high-speed delivery channels. Unfortunately, these modern delivery channels are still guarded by unsuspecting sentries, in the form of firewalls and sensors that are unable to detect the messages that may be hidden inside of digital images and audio files.}[3]

{Early steganography was messy. Before phones, before mail, before horses, messages were sent on foot. If you wanted to hide a message, you had two choices: have the messenger memorize it, or hide it on the messenger.}[12]

{Steganography use can be traced back at least 2,500 years, when Demaratus smuggled a secret message under the cover of wax in order to warn Sparta of an impending attack on Greece.}[3]. {Herodotus, the ancient Greek historian, relates how a messenger had his head shaved and then had a secret message written on his scalp. With newly grown hair, he traveled to the targeted destination where his head again shaved revealed the message .There are a large number of steganographic methods that most of us are familiar with (especially if you watch a lot of spy movies!), ranging from invisible ink and microdots to secreting a hidden message in the second letter of each word of a large body of text and spread spectrum radio communication.As a familiar example, consider an acrostic, in which the first letter of each word of a text can be interpreted to reveal a hidden message

{To use another childhood example, the writing of a message using invisible ink would constitute steganography. If you knew that a piece of paper had an invisible message on it, you could uncover the message using specific tools; otherwise, you would think you were looking at a blank piece of paper.}[11]

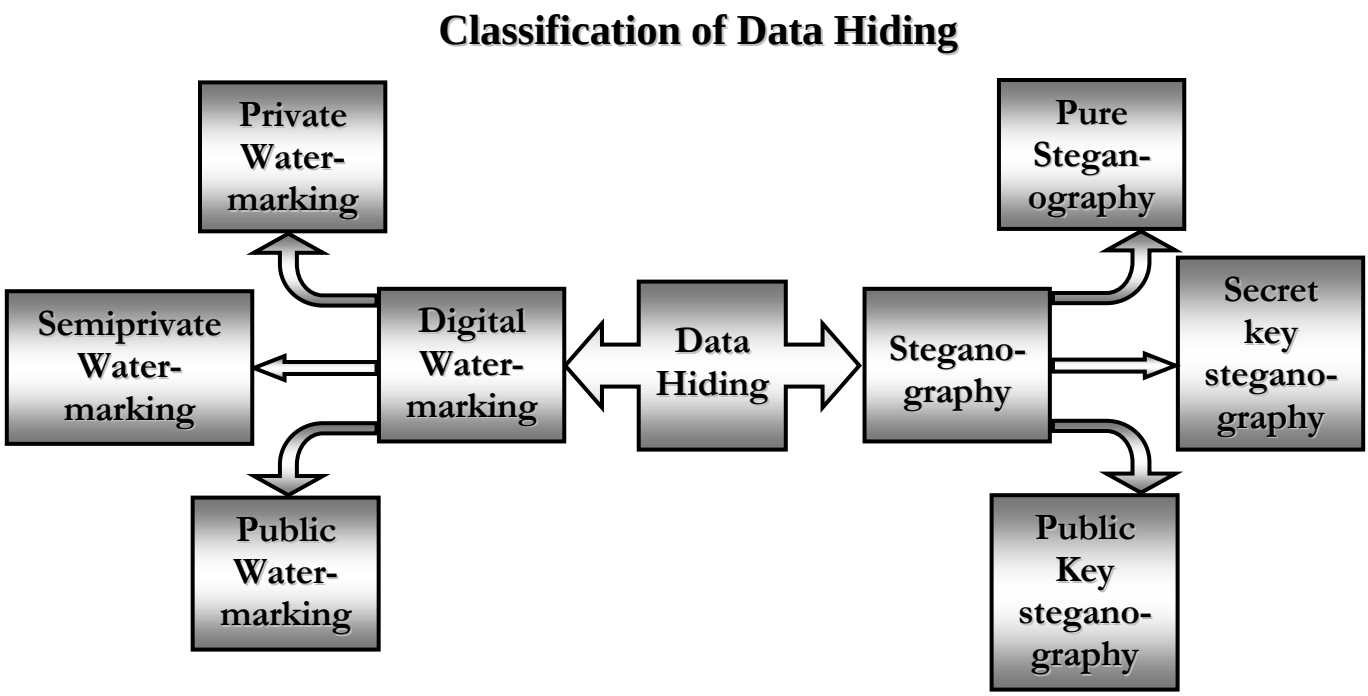
{Steganography today, however, is significantly more sophisticated than the examples above suggest, allowing a user to hide large amounts of information within image and audio files. With computers and networks, there are many other ways of hiding information

{The data to be concealed is compressed and hidden within another file. The hidden message may be placed inside the white space of text messages, the dark areas of a photographic image, or within the unused portions of a digital file format. The first item needed for steganography is called a carrier or a container. This can be a text file, graphic file or sound file, which will host the message that is desired to be hidden. The carrier or container is innocent looking so that it does not arouse the suspicion of anyone viewing it. The next step is to embed the message one wants to hide within the carrier using a steganographic technique.}[11

The Task Of Hiding Information:

{Steganography now is accomplished in the digital world using mathematical algorithms to encrypt data. First, one scrambles the information using an algorithm. This algorithm creates a key later used to transform the encrypted data back to its original form so that the receiver can understand it.

One may hide information in a variety of files. Steganography replaces unused parts of data with the secret information. It is possible to hide information in text, for example, in the spaces between words. This type of information hiding is more successful than steganography that consists of hidden information in infrequent spelling errors and in words replaced by synonyms. }[6] {In the present day, digital images, (as well as audio and video files) offer a rich environment for hiding virtually unlimited types of data.}[4] {One should also choose a cover image that does not contain a large area of solid colors because any slight change caused from the embedded information will be more apparent).}[6]



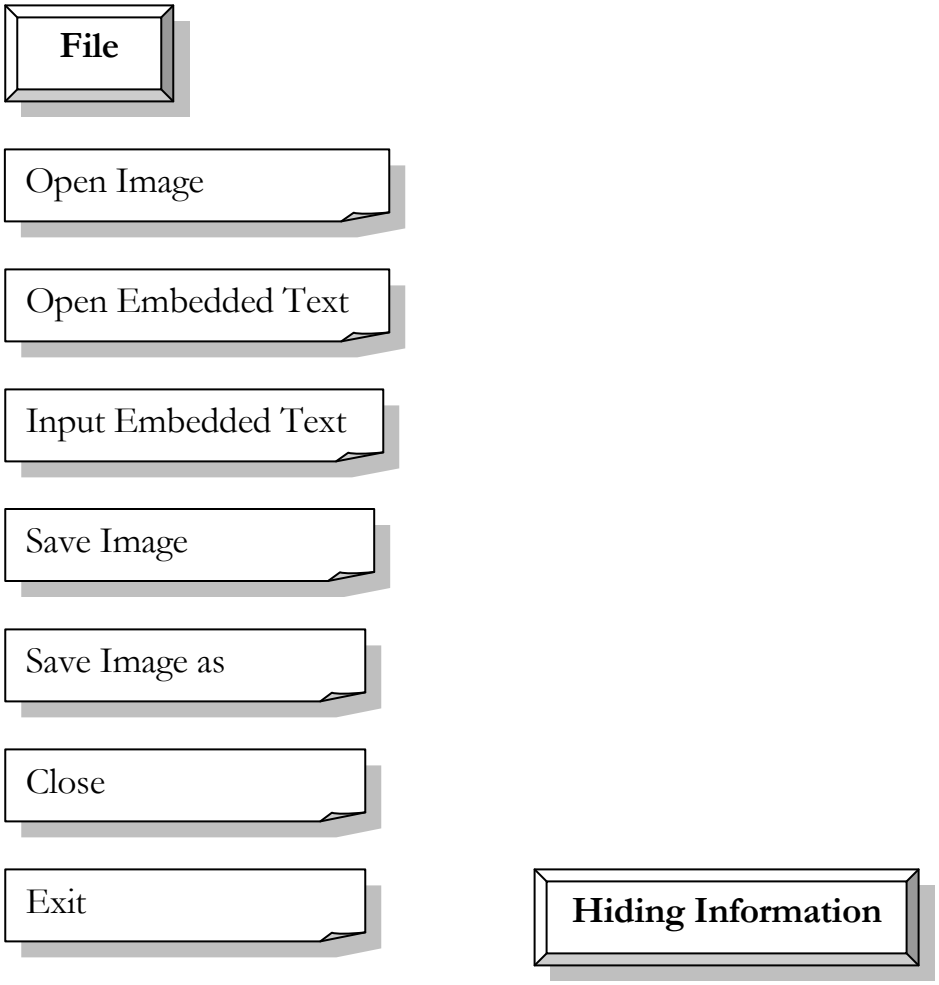
A Proposed Technique

The original aims of the paper are to introduce a technique for hiding a text file, which techniques hide a secret text file inside an image file, and the modified image must be similar to the original image, in other words the changes that happen on the modified image mustn't be visible, or the human eye would be unable to notice it,

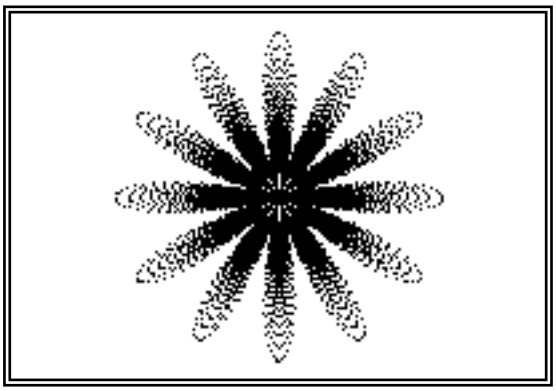
The project application loads 24-bit BMP, GIF, and JPG image format, embed data into them using Sunflower system and saves the images. Encryption can be used before embedding the data to provide robustness. Finally the application can also extract data that was previously embedded. The application runs in a user friend Windows environment where the user can view the image, before and after the embedding.

The Proposed Structure of Sunflower System

structure of the proposed system is shown below:



The basic idea of the proposed system is shown below:



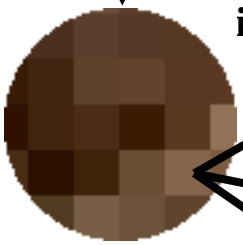
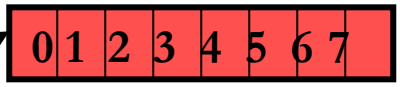
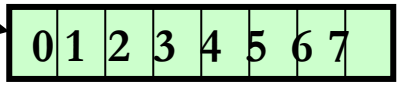


image file.

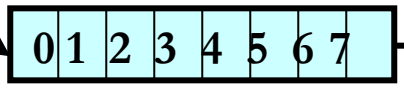
Pixels which is used.



Red color



Green color



Blue color

Layer 1 from Blue color

Layer 2 from Blue color

Layer 7 from Blue color

Layer 8 from Blue color

Pixel Layering

Conclusions

The following are some points concluded from this study:

- **Encryption is the process of passing data or plaintext through a series of mathematical operations that generate an alternate form of the original data known as ciphertext. The encrypted data can only be read by parties who have been given the necessary key to decrypt the ciphertext back into its original plaintext form. Encryption doesn't hide data, but it does make it hard to read!**
- **Hidden directories (Windows) - Windows offers this feature, which allows users to hide files. Using this feature is as easy as changing the properties of a directory to "hidden", and hoping that no one displays all types of files in their**
  - **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 hide 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 if a hidden message is encrypted, it must also be decrypted if discovered.**
- **We change only 2 bits in the pixel, "that will have a minimal effect because the human eye can only detect a round 6 bits of color". In other words, the human eye could not tell the difference of the last 2 bits being changed**

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

[8]Stefan Katznbeisser, Fabien.A., P.Petitcolas editors, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Boston. London, 2000.

[9] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004

[10] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999

[11] Dunbar, B., "Steganography techniques and their use in an Open-Systems environment", SANS Institute, January 2002

[12]Bender, W., Gruhl, D., Morimoto, N. & Lu, A., "Techniques for data hiding", IBM Systems Journal, Vol 35, 1996

