DESIGN AND IMPLEMENTATION OF ALGORITHM FOR HIDING INFORMATION INSIDE THE IMAGE USING STEGANOGRAPHY

S.S. Kale and V.M. Deshmukh
Department Of Computer Science and Engineering, Prof. Ram Meghe Institute of Technology and Research, Badnera, Dist. Amravati, MS, India

ABSTRACT

Steganography is the technique of invisible communication; it is achieved by hiding secret data inside a carrier file such as an image. The basic relationship between steganography and encryption is that while the encryption encrypts the plaintext to cipher text, steganography allows us to hide the cipher text itself. Therefore the combination of steganography and encryption increase the confidentiality, authenticity, non-repudiation, data security and integrity
The Internet as a whole does not use secure links, thus information transmission is mostly prone to malicious use. Cryptography "the science of writing in secret codes" addresses all of the elements necessary for secure communication over an insecure. But cryptography does not always provide safe communication. The protection process is known as encryption and goes through a certain process of encryption. The process requires the original plaintext, the key needed for encryption, the algorithm; containing the blueprint of encryption process and finally it produces the ciphertext i.e. the material from the plaintext, unable to read by the unauthorized user. Original message is called as the plaintext. The disguised message is called as the ciphertext. The strategy of implementing steganography techniques is to improve the security of data in the growing use of digital media. Most often, the strength of data security in cyberspace remains vulnerable due to intruders who are constantly improving their systems/algorithms for stealing organizations'/ individuals' sensitive information.

Keywords: *Steganography, ciphertext, cryptography, carrier file.*

1. Introduction

Steganography refers to the technique of concealing secret information into another cover-media, such as audio, video, image and text in such a manner that the very existence of the information is camouflaged while secret is kept from the knowing of attacker. Steganography is derived from the Greek word steganographic which means covered writing. It is the science of secret communication. The goal of steganography is to hide the existence of the message from unauthorized party. The modern secure image steganography presents a task of transferring the embedded information to the destination without being detected by the attacker. 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 exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. In this paper I purposed an image based steganography that Random bit substitution technique using intgrated key

2. Literature Review

Recently, several methods are developed to protect important information. The developed methods may be classified into two categories: steganography and watermarking. Both steganography and watermarking are data embedding methods. Steganography aims to embedding huge amount of secret data in multimedia carrier such as text, image, audio, and video. On the other hand, watermarking, that may be mainly used for proving copyright, aims to hiding small amount of secret data in multimedia carrier. Although steganography and cryptography have a common goal and are related concepts, the usage and the way of both are somewhat different. Steganography is hiding the message existence completely whereas cryptography is securing the sent message. Steganography's main factors are undetectability, robustness, and capacity. These factors separate steganography from other related techniques e.g. cryptography and watermarking. Figure 1 presents different branches of information hiding. Here we concerns with steganography based information hiding. Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g.,

image, audio, and video files. In other words, steganography is the process of embedding a file, message, image, or video with in another file, message, image, or video.

Past

The word Steganography technically means covered or hidden writing. Its ancient origins can be traced back to 440 BC. Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries for fun by children and students and for serious undercover work by spies and terrorists

Present

The majority of todays steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication. Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level
Hiding information into a medium requires following elements

1. The cover medium(C) that will hold the secrat message.
2. The secret message (M), may be plain text, digital image file or any type of data.
3. The stegonographic techniques
4. A stego-key (K) may be used to hide and unhide the message.

In modern approach, depending on the cover medium, steganography can be divided into five types:

1. Text Steganography
2. Image Steganography
3. Audio Steganography
4. Video Steganography
5. Protocol Steganography

- **Text steganography:** Hiding information in text file is the most common method of steganography. The method was to hide a secret message into a text message. After coming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of excess data.
- **Image steganography:** Images are used as the popular cover medium for steganography. A message is embedded in a digital image using an embedding algorithm, using the secret key. The resulting stego-image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego-image unauthenticated persons can only notice the transmission of an image but can't see the existence of the hidden message.
- **Audio steganography:** Audio steganography is concerned with embedding information in an innocuous cover speech in a secure and robust manner. Communication and transmission security and robustness are essential for transmitting vital information to intended sources while denying access to unauthorized persons. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information. Existing audio steganography software can embed messages in WAV and MP3 sound files.
- **Video steganography:** Video Steganography is a technique to hide any kind of files in any extension into a carrrying Video file.
- **Protocol steganography:** The term protocol steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used.

Following figure 1 shows the steganography with other information security system.

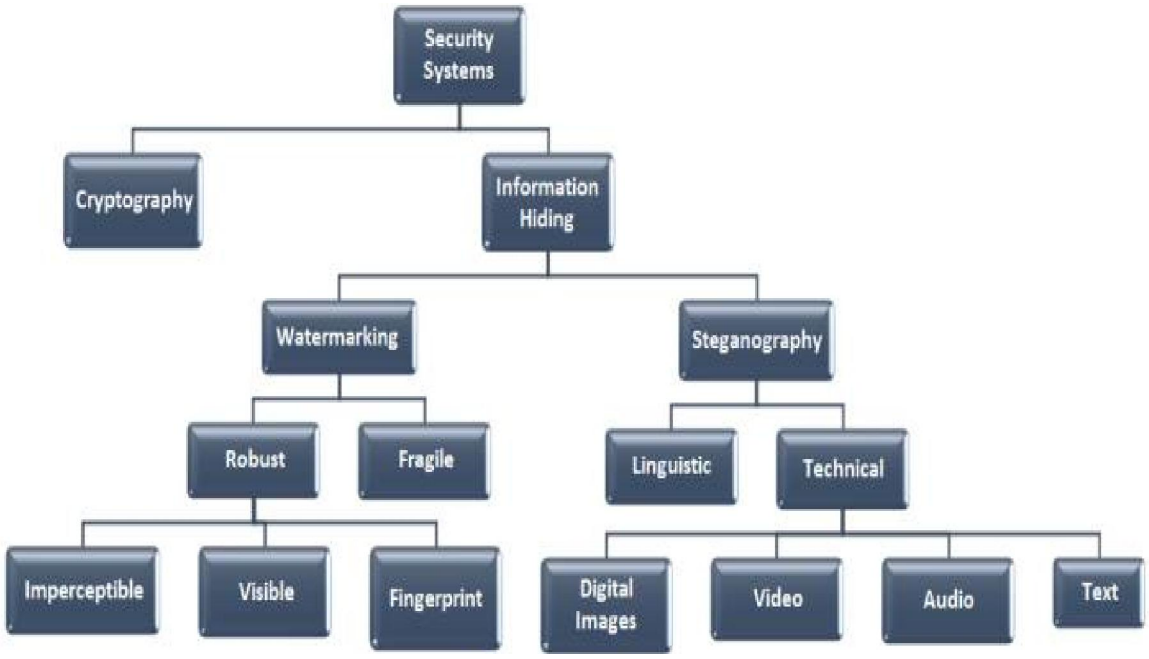

Figure 1: Steganography information security system

3. Steganograpy

The secret image is concealed inside a common image through algorithm and the resultant stegno-image is then hidden again as a visible image or watermark inside another image by algorithm. To provide more than one level of protection for the hidden message, we will require additional security level to protect the secret image, which leads to increased complexity of retrieving the secrete image. The results prove the success of system after the secret image is retrieved successfully. Steganography is derived from the Greek word steganographic which means covered writing. It is the science of secret communication. The goal of steganography is to hide the existence of the message from unauthorized party. The modern secure image steganography presents a task of transferring the embedded information to the destination without being detected by the attacker. 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 exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. In this paper I purposed an image based steganography that Random bit substitution technique using intgrated key technique on images to enhance the security of the communication. In the Random bit substitution approach, the basic idea is to replace the Least Significant Bits of the cover image with the Bits of the messages to be hidden without destroying the property of the cover image significantly. Random bit substitution technique using intgrated key is the most challenging one as it is difficult to differentiate between the cover-object and stego-object if few bits of the cover object are replaced.

4. Applications of Steganography

(i) Secret Communications

The use steganography does not advertise secret communication and therefore avoids scrutiny of the sender, message and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers.

(ii) Feature Tagging

Elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.

(iii) Copyright Protection

Copy protection mechanisms that prevent data, usually digital data, from being copied.The insertion and analysis of watermarks to protect copyrighted material is responsible for the recent rise of interest in digital steganography and data embed.

5. System Analysis

The algorithm used for Encryption and Decryption in this application provides using random bit of image. Writing data starts from last` layer; because the significance of this layer is least and every upper layer has double significance than its down layer. So every step we go to upper layer, the image quality decreases and image retouching transpires. This project has two methods – Encrypt and Decrypt. In encryption the secret information is hidden in any type of image file. Decryption is getting the secret information from image file. The data hiding patterns using the steganographic technique in this project can be explained using three phases:

a. Encryption phase
b. Transmission phase
c. Decryption phase

a. Encryption phase

The "Encryption phase" uses two types of files for encryption purpose. One is the secret file which is to be transmitted securely, and the other is a carrier file such as image. In the encryption phase the data is embedded into the image using Random bit substitution technique by which the least significant bits of the secret document is arranged with the bits of carrier file such as image, Such that the message bits will merge with the bits of carrier file. In this research, the symmetric key encryption with a single key is used.

b. Transmission phase

The transmission phase is one of the important sections for sending the data to destination securely. Usually email or web is used for transferring the data. If the person hacks the e-mail or web and obtains the image, the secret key helps to protect it from unauthorized modification.

c. Decryption phase

The Decryption phase is the reverse of encryption phase. In decryption phase, the carrier image in which the data is hidden is given as an input file. The decryption phase uses the same password which was used for the encryption. After giving the correct password the decryption section uses the Random bit substitution technique using intgrated key by which the encoded bits in the image is decoded and turns to its original state thereby giving the output of a text document as well as an image.

Random Bit Substitution Technique

The Bytes inside an image is changed to a bit of the secret message. Digital images are mainly of two types (i) 24 bit images and (ii) 8 bit images. In 24 bit images we can embed three bits of information in each pixel, one in each last bit position of the three eight bit values. Increasing or decreasing the value by changing the last bit does not change the appearance of the image; much so the resultant stego image looks almost same as the cover image. In 8 bit images, one bit of information can be hidden.

The stego-image is obtained by applying Random bit substitution technique on both the cover and hidden images. The hidden image is extracted from the stego-image by applying the reverse process. If the bit of the pixel value of cover image C(i,j) is equal to the message bit m of secret massage to be embedded, C(i,j) remain unchanged; if not, set the bit of C(i, j) to m. The message embedding procedure is given below

$S(i,j) = C(i,j) - 1$, if $(C(i,j)) = 1$ and $m = 0$
$S(i.j) = C(i,j)$, if $(C(i,j)) = m$
$S(i,j) = C(i,j) + 1$, if $(C(i,j)) = 0$ and $m = 1$

where C(i, j) stands for the last bit of cover image C(i,j) and m is the next message bit to be embedded.
S(i,j) is the stego image

As we already know each pixel is made up of three bytes consisting of either a 1 or a 0.
For example, suppose one can hide a message in three pixels of an image (24-bit colors).

Suppose the original 3 pixels are:

(11101010 11101000 11001011)
(01100110 11001010 11101000)
(11001001 00100101 11101001)

A steganographic program could hide the letter ”J” which has a position 74 into ASCII character set and have a binary representation ”01001010”, by altering the channel bits of pixels.

(11101010 11101001 11001010)
(01100110 11001011 11101000)
(11001001 00100100 11101001)

In this case, only four bits needed to be changed to insert the character succesfully. The resulting changes that are made to the last bits are too small to be recognised by the human eye, so the message is effectively hidden. The advantage of random bit embedding is its simplicity and many techniques use these methods . Random bit embedding also allows high perceptual transparency.

Data Embedding

The embedding process is as follows.
Inputs: Cover image, stego-key and the text file
Output: stego image

Procedure

Step 1: Extract the pixels of the cover image.
Step 2: Extract the characters of the text file.
Step 3: Extract the characters from the Stego key.
Step 4: Choose first pixel and pick characters of the Stego key and place it in first component of pixel.
Step 5: Place some terminating symbol to indicate end of the key. 0 has been used as a terminating symbol in this algorithm.
Step 6: Insert characters of text file in each first component of next pixels by replacing it.
Step 7: Repeat step 6 till all the characters has been embedded.
Step 8: Again place some terminating symbol to indicate end of data.
Step 9: Obtained stego image.

Data Extraction

The extraction process is as follows.
Inputs :Stego-image file, stego-key
Output :Secret text message.

Procedure:

Step 1: Extract the pixels of the stego image.
Step 2: Now, start from first pixel and extract stego key characters from first component of the pixels. Follow Step3 up to terminating symbol, otherwise follow step 4.
Step 3: Extract the characters from the Stego key.
Step 4: If this extracted key matches with the key entered by the receiver, then follow Step 5, otherwise terminate the program.
Step 5: If the key is correct, then go to next pixels and extract secret message characters from first component of next pixels. Follow Step 5 till up to terminating symbol, otherwise follow step 6.
Step 6: Extract secret message.

Image Encoding Algorithm

Inputs : Image file, stego key and image file
Output: Stego image.

a. The cover and secret images are read and converted into the unit8 type.
b. 2. The numbers in secret image matrix are conveyed to 8-bit binary. Then the matrix is reshaped to a new matrix a.
c. The matrix of the cover image is also reshaped to matrix b
d. Perform the bit technique described above
e. The stego-image, which is very similar to the original cover image, is achieved by reshaping matrix b.
f. While extracting the data, the bits of the stego image is collected and they are reconstructed into the decimal numbers. The decimal numbers are reshaped to the secret image.

6. Conclusion

The design and implementation of a steganographic application software will devolve for the purpose of hiding information onto the image using random bit subtitution technique. This will ensure secure information delivery is increased with the system. Future research work on steganography can be done that will help law enforcement agencies to better detect illicit materials transmitted through the Internet.
Today Steganography is mostly used on computers with digital data being the carriers

and networks being the high speed delivery channels. This project intends to offer a state of the art overview of the random bit algorithms used for image Steganography to illustrate the security potential of Steganography for business and personal use.

References

1. **Lyu S. and Farid H. (2006)**. Steganalysis using higher-order image statistics, IEEE Transactions on Information Forensics and Security.
2. **Kahn D. (1996).** The Codebreakers: The comprehensive history of secret communication from ancient time to the Internet Scribner.
3. **Delahaye J.P. (1996)** 'Information noyée, information cache', Pour la Science, www.apprendre-en-ligne.net/crypto/stegano/229_142_146.pdf.
4. **Simmons G.J. (1984)** The prisoners' problem and the subliminal channel, in: Proceedings of International conference on Advances in Cryptology, CRYPTO83, pp. 51-67.
5. **Kurak C. and McHugh J. (1992).** A cautionary note on image downgrading, in: Proceedings of the IEEE 8th Annual Computer Security Applications Conference, pp. 153-159.
6. **Thomas T.L. and Qaeda Al (2003)**. The danger of "cyberplanning", Parameters, US Army War College Quarterly-Spring. Available from: www.carlisle.army.mil /usawc/Parameters/03spring/thomas.pdf.
7. **Hosmer C. (2006)**Discovering hidden evidence, Journal of Digital Forensic Practice47-56.
8. **Hernandez-Castro J.C., Blasco-Lopez I. and Estevez J.M. (2006)**. Tapiador, Steganography in games: A general methodology and its application to the game of Go, Computers and Security, Elsevier Science, 64-71.
9. **Hayati P., Potdar V. and Chang E. (2007).** A survey of steganographic and steganalytic tools for the digital forensic investigator, available from: http://debii.curtin.edu.au/~pedram/images/docs/survey_of_steganography_and_steganalytic_tools.pdf
10. **Bender W., Butera W., Gruhl D., Hwang R., Paiz F.J. and Pogreb S. (2000).** Applications for data hiding, IBM Systems Journal 547-568.
11. **Miaou S., Hsu C., Tsai Y. and Chao H., (2000).** A secure data hiding technique with heterogeneous data-combining capability for electronic patient records, in: Proceedings of the IEEE 22nd Annual EMBS International Conference, Chicago, USA, pp. 280-283.
12. **Nirinjan U.C. and Anand D., (1998).** Watermarking medical images with patient information, in: Proceedings of the20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, HongKong, China,, pp. 703-706.
13. **Li Y., Li C. and Wei C. (2007)**. Protection of mammograms using blind steganography and watermarking, in:Proceedings of the IEEE International Symposium on Information Assurance and Security, pp. 496-499.
14. **Frith D. (2007):** Steganography approaches, options, and implications, Network Security, 4-7.
15. **Farid H. (2009)**:A Survey of image forgery detection, IEEE Signal Processing Magazine.
16. **Cheddad A., Condell J., Curran K. and Kevitt P.M. (2010).** Digital image steganography: survey and analysis of current methods. Signal Processing Journal.
17. **Jambhekar N.D., Dhawale C.A. and R. Hegadi (2015).** Performance analysis of digital image steganographic algorithm, ACM Digital Library, ICTCS'14, Proceedings of the International Conference on Information and Communication Technology for Competitive Strategies, Nov.2014 pp. 1-7