International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 12 (2014), pp. 1221-1227

http://www. irphouse.com

Evolution in Image Steganography

Nancy Sehgal [1] and Dr. Ajay Goel[2]

[1] Baddi University of Emerging Sciences and Technology, Baddi. Himachal Pradesh
[2] Baddi University of Emerging Sciences and Technology, Baddi. Himachal Pradesh
[1] nancysehgal128@gmail. com, [2] goelajay1@gmail. com

Abstract

Steganography is an important area of research, now days. It is the science of hiding information. It centers on the concept of hiding a message in plain sight. In this we embed the information into the cover media. The cover media may be a text, video, audio, image (Payload) and the network packet. We prefer Digital images as a media for hiding information due to their low impact on visibility and high capacity. In this paper we have discussed the general methodology to hide the data and the evaluation tools. The method consists of three phases: secret sharing phase, steganography phase and data extraction phase. The secret sharing and steganography phases are used for encoding the secret message, and the data extraction phase is used for decoding and revealing the secret image. In the current paper we are going present the different aspects of steganography.

Introduction

Steganography is derived from a Greek word meaning secret drawing and it centers on the concept of hiding a message in plain sight. It is the science of embedding information into cover objects such as videos, images that will escape detection and retrieved with minimum distortion at the destination. Now a days the objective of steganography is to keep the payload (embedded information) undetected, but the steganographic methods, because of their intrusive nature, leave behind the vestige in the cover image. Steganography finds applications in finger printing, the modem mms service and in watermarking. The final image obtained after embedding the information into cover image is called as stego Object.

Some examples of Steganography in the past are:

- Tattoos on shaved heads
- Microdots – shrunken pictures

- Invisible Inks - milk, fruit juice, urine
- Null ciphers (unencrypted message) were used to hide secret messages

Steganalysis is classified into two fields: passive and active steganalysis. Passive steganalysis detects the absence or presence of a secret message in an cover image or identify the embedding algorithm. The active staganalysis finds some properties of the information of the embedding algorithm. To achieve the information security and confidentiality, the secret information that gets embedded in a carrier through random permutation with the verification code. The permuted verification code is used to check or verify the integrity of the secret information to that is extracted from the received stego image.

There is a requirements model which is called magic triangle [1] in the fields of information hiding, given in Figure 1. The three corners of the triangle are Imperceptibility, robustness, and the insertion capacity. This model is used for a representation of the trade-offs between the insertion capacity and the robustness to attacks, while keeping the quality of the image at an acceptable level. Steganography is the art of hiding and transmitting data through carriers to conceal the existence of the secret information [2]. It pays more attention on insertion capacity rather than robustness.

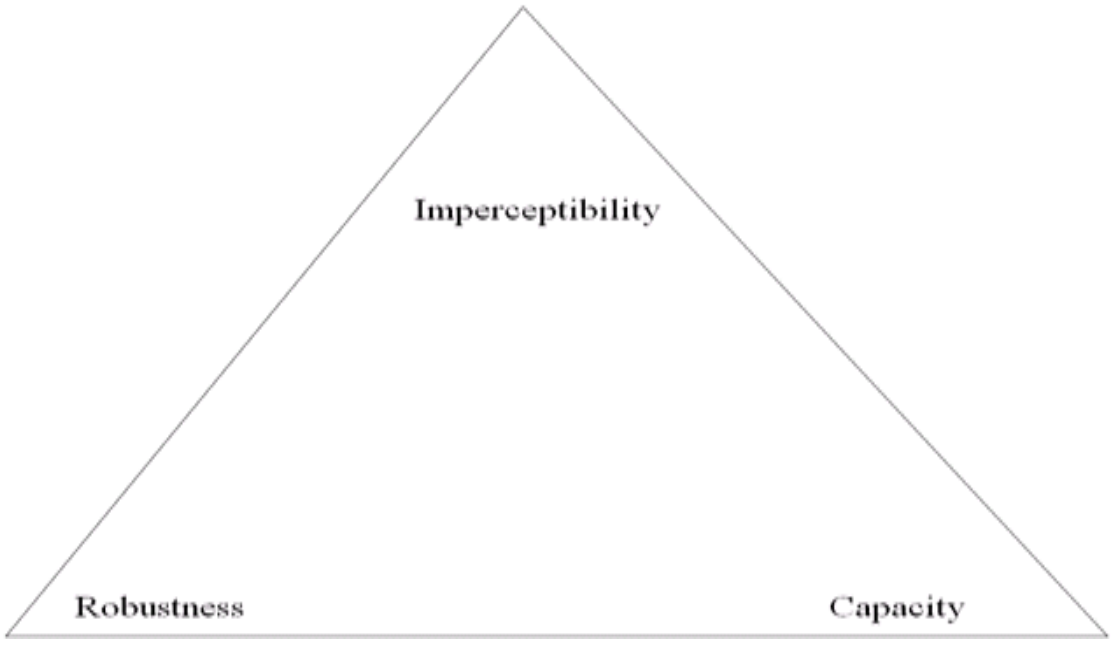

Figure 1. Magic triangle-three Requirements of information hiding

Related Work:

K. B. RAJA[3] have used the combination of LSB algorithms, DCT transformation, and compression using quantization and runlength coding on raw images to obtain secure stego-image. The LSB technique has been used to accommodate maximum

payload. The entire payload is embedded into the cover image to obtain the stego-object. The stego-object in the spatial domain is transformed into frequency domain by applying DCT. The stego-object is further compressed using quantization and runlength coding to derive a secure stego-object. An exactly reverse procedure is followed to retrieve the payload at the receiver. The integrated approach of combining LSB, DCT and compression techniques enable secure transfer of payload with low BER and MSE compared to earlier techniques.

MOHAMMAD JAVAD KHOSRAVI [4]introduced a new method to improve the security of steganography using secret sharing and integer wavelet.

This method has three phases: (1) cryptography phase using a secret sharing method, (2) data hiding phase using a novel Integer-Wavelet based steganography method, and (3) date extraction phase. This Algorithm assumes that the secret message—in the form of images— is made in bitmap grayscale (8 bits) format. First in cryptography phase, n shares are generated from the secret image by inputting the share number from 1 to n into the polynomial functions obtained from the secret image. Next, using a new integer wavelet based steganography method to hide the produced shares into n cover images to produce n stego images. They used a certain arrangement of the coefficients of Integer-Wavelet transform, which also took into account the human visual system (HVS) considerations to hide the share images into the cover images. In the decoding and data extraction phase of the proposed method, two steps are taken. First, the steganography phase is reversed to extract the shares from the stego images. Then, the original secret image is rebuilt from the extracted shares.

PSNR and SSIM criteria are measured, and for steganalysis, RS general attacks, and three supervisory training FLD neural network based steganalysis are employed.

The experimental results show that, considering all aspects, including the visual image quality and all different steganalysis, the proposed method facilitates a very effective system and work well under almost all different attack cases and scenarios.

HONG-JUAN ZHANG, HONG-JUN TANG [5] had proposed a novel LSB image steganography algorithm. It avoids the weak point of classic LSB steganography algorithm, but preserves high insertion capacity and low computational complexity. It can effectively resist RS analysis, Chi-square test and other steganalysis aim at sequential steganography.

In order to increase the embedding capacity further ahead, human perceptive model should be studied and exploited.

MAMTA JUNEJA, PARVINDER SINGH SANDHU[6] introduced the concept of steganography and steganalysis as well as the methods for carrying these out. It also presented the authors' application which was demonstrated to be more secure than current applications against statistical attacks commonly used in steganalysis. According to them steganography when combined with encryption provides a secure means of secret communication between two parties. There application, with its image analysis and ranking capability is a significant improvement on current steganography tools.

JOSHUA R. SMITH AND CHRIS DODGE [7], this paper presents two main results. The first is a new approach to steganography in which data is encoded in

correlations among the pixels in an image. Almost all previous steganographic methods encode data in correlations between the pixels and a known external reference signal. This method hints at the existence of public key watermarking techniques, which will be defined. The other result is a method for greatly increasing the capacity of a printed steganographic channel. Because it is specific to printed images, this method is useful for steganographic problems such as stealth bar coding, but not for digital watermarking. The two results are complementary in that higher noise levels are encountered in the intra-image correlation encoding method, but the second method works by eliminating image-induced noise.

NIELS PROVO AND PETER HONEYMAN UNIVERSITY OF MICHIGAN [8], introduced that Today, computer and network technologies provide easy-to-use communication channels for steganography. Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity). The embedding process creates a *stego medium* by replacing these redundant bits with data from the hidden message. Modern steganography's goal is to keep its mere presence undetectable, but steganographic systems— because of their invasive nature—leave behind detectable traces in the cover medium. Even if secret content is not revealed, the existence of it is: modifying the cover medium changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium's statistical properties. The process of finding these distortions is called *statistical steganalysis*. They discusses existing steganographic systems and presents recent research in detecting them via statistical steganalysis. Other surveys focus on the general usage of information hiding and watermarking or else provide an overview of detection algorithms. They present recent research and discuss the practical application of detection algorithms and the mechanisms for getting around them.

EVALUATION TOOLS

In an effort to propose a more secure technique, we examined the image steganography techniques and tools against a set of criteria. We considered 6 tools.

- Level of Visibility (Perceptible or Imperceptible): Steganography techniques should embed information in such a way that embedded data leave no traces or signs of steganography use. The visibility is directly influenced by the size of the secret message, the format and the content of the carrier image.
- Detectability (DET): This is a crucial criterion. The success of a technique may be viewed by the complexity involved in detecting the hidden data in the carrier. It ranges from High (H) to Low (L).
- Robustness (ROB): The embedded data should survive any reprocessing operation for the cover which may go through and still preserve its fidelity.
- Capacity (CAP): This concerns the amount of information that can be carried in a cover image. There is a trade-off between the capacity (message size) and robustness. For example the LSB techniques have the capacity to hide larger amount of information in a cover image but a little reprocessing to the resulted image will destroy information completely.

- Domain Type (DOM): DOM is either Spatial(S) or Transform (T). The techniques that use transform domain hide information in significant areas of the cover images and may be more complex for attackers. However, such techniques are restricted to lossy format with different quality factors.
- File Format Dependency (DEP): Some techniques are dependent on specific format of a carrier type while others allow for more freedom.

General Methodology

General method consists of three phases: secret sharing phase, steganography phase and data extraction phase. The secret sharing and steganography phases are used for encoding the secret message, and the data extraction phase is used for decoding and revealing the secret image. In secret sharing phase, the secret image is distributed among the shares. In steganography, the shares are hidden in the cover images. Then, the obtained stego images are given to the participants.

In the embedding process, sequences of distance differences and binary values that are generated in the preprocessing are utilized. Each distance between two random pixel channels will embed one message bit by adjusting the distance to the closest value in the distance difference sequence whose binary value is identical to the message bit.

In the deembedding phase, the stego-key is used to generate the same distance differences and binary sequences as those used in the embedding process. For each random selected pixel channels, the closest distance between them is computed to find the hidden message from the corresponding binary value.

The algorithm

Encoding:

1. Read image files
2. Compress secret file
3. Encrypt secret file
4. Calculate Capacity of covert file
5. If the cover capacity is not sufficient goto 1
6. else repeat

i. Generate binary sequence based on the key
ii. Generate random distances sequence based on the key
iii. Get random pixel
iv. Get 2 random channels for this pixel
v. Compute distance between those channels
vi. Match with distance with minimum error and has the same message bit.

Until the Covert file is completed

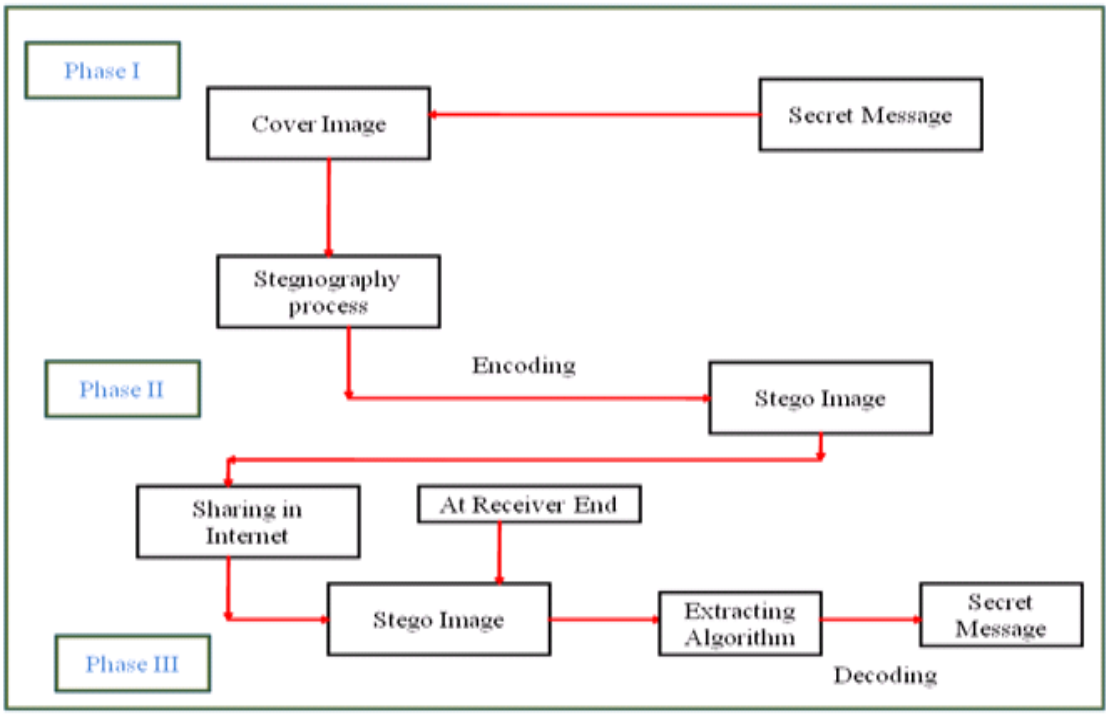

Figure 2. steganography process

Conclusion and Future Work

Steganographic techniques can be used to hide data within digital images with little or no visible change in the perceived appearance of the image and can be exploited to export sensitive information. In the current paper we have described the process of stegnography and various pros and cons done by different researchers. These ideas lead to further work in the field of stegnography. In future we are going to implement multiscale resolution wavelet transform for image stegnography and compare the results with earlier techniques.

References

[1] Johnson N, Duric Z & Jajodia S, "*Information Hiding: Steganography and Watermarking-Attacks and Countermeasures*", Kluwer Academic Publishers, Boston, MA, 2001.

[2] Peticolas FAP, Anderson RJ, and Kuhn MG, "*Information hiding-A survey*", Proc. of the IEEE, Vol 87, No. 7, pp. 1062-1078, 1999.

[3] K. B. Raja, C. R. Chowdary, Venugopal, L. M. Patnaik "*A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images*", Department ofComputer Science Engineering, Bangalore University, 0-7803-9588-3/05/$20. 00 ©2005 IEEE.

[4] Mohammad Javad Khosravi • Ahmad Reza Naghsh-Nilchi "*A novel joint*

secret image sharing and robust steganography method using wavelet", Springer-Verlag Berlin Heidelberg 2013

[5] HONG-JUAN ZHANG, HONG-JUN TANG" *A NOVEL IMAGE STEGANOGRAPHY ALGORITHM AGAINST STATISTICAL ANALYSIS*", Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, 19-22 August 2007.

[6] Mamta Juneja, Parvinder Singh Sandhu "*Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption*", 2009 International Conference on Advances in Recent Technologies in Communication and Computing.

[7] Joshua R. Smith and Chris Dodge, "Developments in Steganography".

[8] Niels Provo and Peter honeyman university of Michigan, "Hide and seek – An introduction to steganography".

[9] Farid, H. : *Detecting hidden messages using higher-order statistics models*, In: Proc. EEE Int. Conf. Image Processing, September 22–25, pp. 905–908, IEEE New York (2002).

[10] M. Kwan, The Snow Home Page, http://www. darkside. com. au/snow/index. html, March 2001

[11] Compris Intelligence, TextHide, Compris Intelligence, http://www. compris. com/TextHide/en

[12] P. Wayner, SpamMimic, http://www. spammimic. com, 2003

[13] S. Inoue, K. Makino, I. Murase, O. Takizawa, T. Matsumoto and H. Nakagawa, A Proposal on Information Hiding Methods using XML, http://takizawa. gr. jp/lab/nlp_xml. pdf

[14] National Academy of Sciences, How do Wavelets work?, National Academy of Sciences, http://www. beyonddiscovery. org/content/view. page. asp?I=1956, 2003

[15] J. Glatt, MIDI is the language of gods, http://www. borg. com/~jglatt/