Punch Holes, Invented Steganography Method Researchers:

Nadia Mohammed
Instructor, Collage of Education for Pure of Law and Political Science
Baghdad University
Msc of Computer Science

Shahbaa Mohammed
Asst.Instructor ,Collage of Science /Ibn-Alhaitham,, Al-Iraqia University
Msc of Computer Science

Abstract

A coin has two sides. Steganography although conceals the existence of a message but is not completely secure. It is not meant to supersede cryptography but to supplement it.

The main goal of this method is to minimize the number of LSBs that are changed when substituting them with the bits of characters in the secret message. This will lead to decrease the distortion (noise) that is occurred in the pixels of the stego-image and as a result increase the immunity of the stego-image against the visual attack.

The experiment shows that the proposed method gives good enhancement to the steganoraphy technique and there is no difference between the cover-image and the stego-image that can be seen by the human vision system (HVS), so this method can be considered a success and can be adopted in the field of steganography.

Keywords: steganography, embedding, extracting, punch holes.

1. Introduction

Image steganography is the science of concealing information and messages within an image using some embedding algorithm. In modern days communication security is the fundamental requirement even though accomplishment of comprehensive security is a superlative state of affairs. The concept of "What You See Is What You Get (WYSIWYG)" associated with printing capabilities of a printing machine for an image, is now a fallacy [1]. Ordinary image is no longer a regular image. It could be a mask over a secret message. In image Steganography, the mask used to hide any message is a color or grayscale image.

Motivation for modern day's image steganography techniques comes from the fact that no existing method is self-sufficient. Increasing the embedded information could cause easy detection by an attacker, whereas enhancing the security could increase the computation and communication overhead due to the fact that one secret message will take several transmissions. A trade-off between embedding capacity and the level of

security needs a strong base for a security measure. The proposed method tries to achieve greater level of security with minimum computation time.

The failure to cease the suspicion of any hidden data in an image is the reason for breakdown of any steganography system. The fundamental requirement for any secure steganography scheme is the ability to cover the hidden message in the cover image. A system is considered to be secure if a snooper cannot be distinguished between cover image and the stego image. There are different measures for steganographic security. The most common measure is called detectability of a stego system. Detectability is defined as the relative entropy between the probability distribution of cover image and the stego image. Any steganography system is called $\mathcal{E}$-secure if the relative entropy of the system is at most $\mathcal{E}$[1]. A steganography scheme is said to be perfectly secure if detectability is zero. Reduction in detectability means reduced embedding capacity. Any image steganography scheme should optimize the embedding capacity to achieve minimum possible detectability taking into account the computational overhead. The maximum number of bits that can be embedded in a cover image and recovered from the stego image without violating the undetectability constraints is known as the steganographic capacity. The maximum steganographic capacity that an existent reversible steganographic scheme can achieve is approximately 3 bpp [2]. Perceptual consistency and robustness are the most desirable attributes of any steganographic system. Peak signal to noise ratio (PSNR) can be used as a measure of steganographic security where the embedding capacity of a model is outsized. Increasing secret information embedding capacity would mean straightforward steganalysis and detection of the hidden information. State of art steganalysis attempt to overpower any steganography scheme. Biggest challenge of a steganography scheme is to outsmart all steganalysis schemes [1]. The science of detecting the concealed message in a cover image is steganalysis. The battle between steganography and steganalysis is getting on since the evolution of the science of steganography. There are several ways in which steganalysis can wreck the structure of steganography. The most common methods are inspection of the inner structure of LSBs, Histogram analysis, feature vector analysis et cetera [1]. Primary goal of any image steganography scheme is to achieve high level of security with high capacity embedding, reduced noise, and minimum computation time.

1.1 Information Hiding: A Brief History

Information hiding is a general term encompassing many subdisciplines. One of the most important subdisciplines is steganography [3] as shown in Figure 1.

Steganography, is derived from a finding by Johannes Trithemus (1462-1516) entitled "Steganographia" and comes from the Greek defined as "covered writing" [4][5]. It is an ancient art of hiding information in ways a message is hidden in an innocent-looking cover media so that will not arouse an eavesdropper's suspicion.

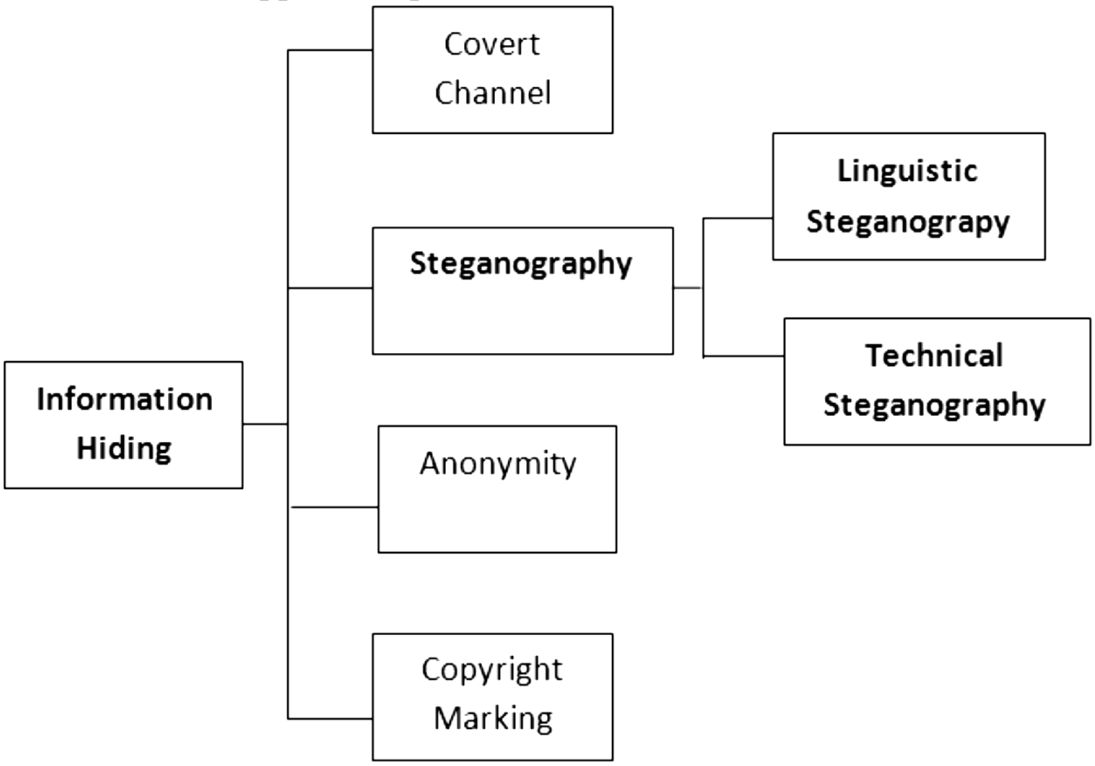


Fig.1: A Classification of Information Hiding Techniques

The goal of steganography is to transmit a message through some innocuous carrier i.e. text, image, audio and video over a communication channel where the existence of the message is concealed. Based on Figure 1, steganography is one of the information hiding techniques which can be classified into linguistic steganography and technical steganography. Linguistic steganography is defined by Chapman et al.[6] as "the art of using written natural language to conceal secret messages". The main component of the linguistic steganography consists of a medium which required the steganographic cover that is composed of natural language text and the text itself which can be generated to have a cohesive linguistic structure [5]. Conversely, technical steganography is explained as a carrier

rather than a text which can be presented, as any other physical medium such as microdots and invisible inks.

During World War II, invisible inks offered a common form of invisible writing. With the invisible ink, a seemingly innocent letter could contain a very different message written between the lines. Therefore, the text document can conceal a hidden message through using null ciphers (unencrypted message), which perfectly camouflage the real message in an ordinary letter. In [7], there is an example on one of the most significant null cipher messages sent by a Nazi spy:

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils [7].

By extracting the second letter from each word, this hidden message can be decoded as:

Pershing sails from NY June 1. [7]

The development of new digital technologies has opened an opportunity to improve message detection that more information can be transferred and even be less conspicuous in transmission such as the microdots technology developed by the Germans. Microdots [8] uses microscopic shrink technique to hide text pictures which can only be read using a microscope. German spies used them in many different ways for instance like messages hidden in letters, on the face of watches and even on spotted ties as shown in [8].

The principle of information hiding was first documented in On the Criteria to be Used in Decomposing Systems Into Modules in 1972 [9] whereby Parnas designed a software system and each module's "interface of definition was chosen to reveal as little as possible about its inner workings". Many researchers are trying to carry out research by applying this concept in information hiding. There are three aspects in information hiding systems which contend with each other: capacity, security and robustness [10]. Capacity refers to the amount of information that is able to be hidden in the medium. However, security is important when a secret communication is kept to be secret and undetectable by eavesdroppers. Robustness can be explained as the amount of modification the stego-medium can withstand before an adversary can destroy the hidden information.

2. Proposed method

The proposed method is suggested here to enhance the performance of the Classic-LSB technique by supporting it through three strong points:

- Decrease the distortion/noise that will be appearing in the pixels of the stego-image.
- Increase the capability of hiding very long secret message in a small stego-image.
- Increase the immunity of the stego-image against the attacks of Human Visual System (HVS) and stego analysis.

In the following paragraphs, the detail explanation of the operations that are doing in the proposed method will be given.

In this method multiple patterns are generated as 2-dimensional matrices (3*3), and hole sites are located randomly for each matrix, then those patterns will be projection on the cover-image, then choosing the pixels that correspond holes and neglecting the rest as shown in figure (2).

After selecting the pixels, they will be dismantled to the main colors (Red Green Blue) and converted to the binary system, and the secret text is also converted to the binary system and encrypted in a way to increase the security, then it is replaced by the LSB data between the pixel and secret text.

A stego-image will be generated, containing the hidden cipher text. You can use the same pattern on whole image or use a different pattern, this depends on the arrangement between the two parties the sender and recipient, as they both must have the patterns used in embedding.

123	121	131
121	131	123
121	123	121

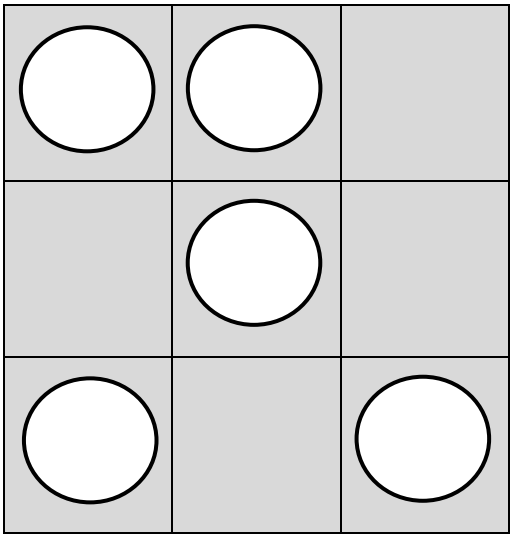
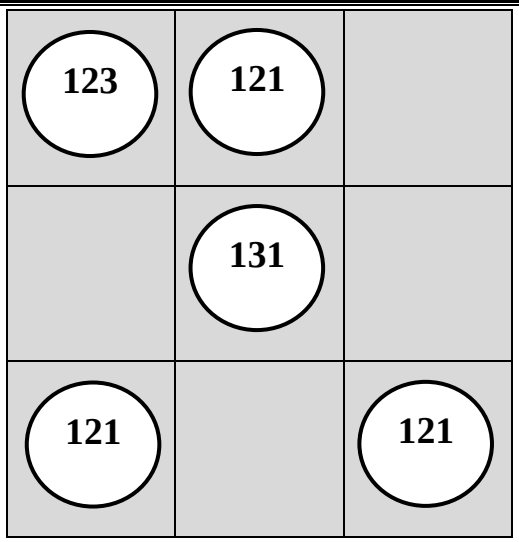


Figure (2): a) cover-image. b) Pattern of the punch hole.



c) stego-image

3. <u>Embedding algorithm</u>

Input: cover-image, encrypted text.
Output: stego-image.
Begin
Step1: check the size of the image and the secret text.
Step2: choose one or more of punch holes pattern.
Step3: convert the encrypted text into binary.
Step4: start sub-iteration1:
Choose one pixel that corresponding to the 1^{ST} hole in the pattern and divided it into red, green, blue.
Hide two bits of the secret text in each 2 LSB in each part of the pixel.
End sub-iteration1.
Step5: set the image with new values and save it.
End

<u>Extracting algorithm</u>

Input: stego-image.
Output: encrypted text.
Begin
Step1: choose the same punch holes patterns that used in embedding algorithm.
Step2: start sub-iteration1:
Choose the same pixel that corresponding to the holes in the pattern and divided it into red, green, blue.
Extract two LSB from each part of the pixel.
Save the binary value.
End sub-iteration1.

Step3: reconstruct the encrypted text.

End

4. Results and Discussion

This section presents the performance of the proposed method. To evaluate the effectiveness of the proposed steganography method, the stego-image quality is considered from two viewpoints. First, we utilized the peak-signal- to-noise ratio (PSNR) metric between the stego-image and the cover-image which is defined as follows. Second, we compare the quality of the stego-image to that of the cover-image as seen by the human visual system (HVS).

$$\mathrm{PSNR} = 10 \times \log_{10} \frac{(255)^2}{\mathrm{MSE}}$$

Where, MSE is the mean-square error between the cover and the stego-images. For a cover- image whose dimensions are W and H, MSE is defined as:

$$\mathrm{MSE} = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} (X_{i,j} - Y_{i,j})^2$$

Where, Xi,j and Yi,j denote the pixel values of the cover and the stego-images, respectively.

To conduct our experiments, we used ‘‘Lena’’ with sizes of 256 × 256 as a and ‘‘Baboon’’ with sizes of 256 × 256 as cover-image see figure (3), we report the average value of all PSNRs as the result of the proposed method in table (1), we can be observed from it that the obtained results of the proposed method are satisfactory from the aspect of PSNR, and the PSNR value of the stego-image is almost acceptable. In figure (4) we can see the experimental results of the proposed method which are stego-images

Figure (3): a) Lena cover-image b) Baboon cover-image


Figure (4): a) Lena stego-image b) Baboon stego-image

Table (1): Experimental results of the proposed method.

Image name	Lena.jpg 24 true color	Baboon.jpg 24 true color
Image size	226 x 256	256 x 256
Message (no. of char.)	100	100
PSNR of stego-image	34.93	35.42
MSE of stego-image	60.296	71.573

5. Conclusion

The experiment shows that the proposed method gives good enhancement to the steganoraphy technique and there is no difference between the cover-image and the stego-image can be seen by the human vision system (HVS), so this method can be considered as a success and can be adopted in the field of steganography.

The Implementation of this method for Audio and Video Steganography will considered as a future work.

References

[1]. A. Cheddad, J. Condell, K. Curran, P. McKevitt, Digital image Steganography: Survey and analysis of current methods, Elsevier, Signal Processing 90 (2010) pp. 727–752.

[2]. Y.H. Yu, C.C. Chang, Y.C. Hu, Hiding secret data in images via predictive coding, Pattern Recognition 38 (2005) pp. 691–705.

[3] M. Hassan Shirali-Shahreza, Mohammad Shirali-Shahreza. "Text Steganography in Chat", IEEE, 2007.

[4] B. Pfiztzmann, "Information Hiding Terminology." pp. 347-350, ISBN 3-540-61996-8, results of an informal plenary meeting and additional proposals, 1996.

[5] K. Bennett, "Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text", Purdue University, CERIAS Tech. Report, 2004.

[6] M. Chapman, G. Davida, and M. Rennhard, "A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography", Proceedings of the Information Security Conference, October 2001, pp. 156-165.

[7] N. F. Johnson, S. Jajodia, "Exploring Steganography: Seeing the Unseen," IEEE Computer, February 1998, pp.26−34.

[8] "Spy Gadgets in World War II: Microdots", 2007. [Online]. Available: http://www.mi5.gov.uk/output/Page303.html [Accessed: Feb. 15, 2008].

[9] D. Parnas, "On the Criteria to Be Used in Decomposing Systems Into Modules", Communication of the ACM, vol. 15, no. 12, December 1972, pp. 1053-1058.

[10] N. Provos, P. Honeyman, "Hide and Seek: An Introduction to Steganography", The IEEE Computer Security, 2003.

ثقوب مثقية ،طريقة تعمية مخترعة

م. نادية محمد عبد المجيد
كلية الـــتربية للعلوم الصرفة
ابن الهيثم /جامعة بغداد

م. م. شهباء محمد عبد المجيد
كلية القانون والعلوم السياسية
الجامعة العراقية

الخلاصة

العملة لها وجهان. إخفاء المعلومات على الرغم انها تخفي وجود الرسالة ولكنها ليست آمنة تماما. وليس المقصود أن تحل محل التشفير ولكن لاستكماله.

الهدف الرئيسي من هذه الطريقة لتقليل عدد LSBs التي تم تغييرها عند استبدالها مع بت الأحرف من الرسالة السرية. وسيؤدي ذلك إلى تقليل التشوه (الضوضاء) التي وقعت في نقطة الشاشة من الصورة الناتجة ونتيجة لزيادة مناعة الصورة لناتجة ضد الهجوم البصري.

تبين التجربة أن الطريقة المقترحة تعطي تعزيزا" جيدا" لتقنية إخفاء المعلومات وليس هناك فرق بين الصورة الأصلية والصورة الناتجة والتي يمكن أن ترى من قبل نظام رؤية الإنسان (HVS)، لذلك هذه الطريقة يمكن اعتبارها ناجحة ويمكن اعتمادها في مجال إخفاء المعلومات.