International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June 2013
ISSN 2229-5518

Multi level De-noise Steganography

Jithesh K, Thavavel.V

Abstract— An innovation that blends both brilliance and craft can only survive. A multi level security mechanism through psychological approach is proposed here. Hiding encrypted data inside an image is introduced. Encryption is done through Visual cryptography and hiding is done through Steganography. This technique provides the features of both encryption and hiding. Hence it gives multi levels of security. Usually, while hiding data inside an image make distortion to the image and leads to unauthorized access. But in lieu of that, this technique tries to remove disturbances or noise that is already present as part of the image, through replacing noise bits with secret data. Since we replace the noise bits with the secret data bits, it improves the quality of the cover medium and hence it is not that easy for a steg-analyst to find the presence of the confidential data. For which the steganography algorithm used is Selected Noise Bits [SNB], because, noise bits need to be replaced to avoid disturbances.

Index Terms— Cover medium, Steganography, , Steg-analyst, Selected Noise Bit, Stego-key, shares, visual cryptography.

1 INTRODUCTION

An important sub division of information hiding is steganography [3]. While cryptography is about protecting the content of messages, steganography is about concealing their very existence. Networking and digitization have become more and more evident features in the rapid development of the economic society. The convenient and timely acquisition of on-line services through accessing the Internet is a tidal current for individuals and organizations. However, the relay of sensitive information via an open Internet channel increases the risk of attacks. Thus many techniques have been proposed to deal with this issue. Data hiding, known as information hiding, plays an important role in information security. For content authentication and perceptual transparency, the main idea of data hiding is to conceal the secret data into the cover medium, such as an image, audio, video or text, and thereby to avoid attracting the attention of attackers in the Internet channel. The growing number of internet-based applications has made digital communication nowadays an essential part of infrastructure. Confidentiality in some digital communication is necessary when sensitive information is being shared between two communicating parties over a public channel. Cryptography and steganography are two sides of a coin for providing confidentiality and protecting sensitive information. The former is the art and science of writing sensitive information is such a way that no one but the intended recipient can recover it. The latter is the art and science of hiding sensitive information within innocuous documents in an undetectable way. The information to be hidden can be of any kind such as text, image, sound and video files. The innocent documents (also known as hosts/covers/carriers) can also be of any kind as long as they do not seem suspicious. However, with the advent of the digital technology, digital hosts such as image, audio and video files have become nowadays the most commonly used host files. Due to their insensitivity for the human visual system, digital images can be regarded as an excellent choice for hiding sensitive information. One of the most commonly used data hiding approaches is the substitution technique. This approach is based on the fact that parts of the image which are regarded as redundant or noisy are replaced by the sensitive information bits. After embedding this information into the host, the resulting image is referred to as a stego-image and the file is referred to as a stego-file. The embedding algorithm may require a secret key, referred to as a stego-key.

- *Research Scholar, Department of Computer Applications, Karunya University, Coimbatore.* jithukotheri@gmail.com
- *HOD i/c, Department of Computer Applications, Karunya University, Coimbatore*

2 PROPOSED STEGANOGRAPHY ALGORITHM

In the following section we describe the proposed algorithm as well as algorithms used for achieving multilevel security for the proposed method.

2.1 Selected noise bit steganography [SNBS]

One popular method of encoding secret information in the spatial domain is LSB. Least-significant bit is the substitution method of steganography where the rightmost bit in a binary notation is replaced with a bit from the embedded message. In lieu of this, here we suggest to select only noise bits from the binary of the image. Selection is done through image filtering [5] or statistical features [4], [8]. The cover image first of all must seem casual, so it must be chosen between a set of subjects that can have a reason to be exchanged between the sender and the receiver. The image should have more or less numbers of noise; it must be "noisy," so that the added data at noise bits will de-noise the image and hence accomplish the task. Selection [9], [10] of a suitable Image with noise is done carefully. That is replacing the noise bits with secret data should enhance [11] the Image. Hence

2.2 Creating shares using visual cryptography

The secret data is made into shares using any of the visual cryptography [12] method. Using advanced algorithm will increase the security. This is the first level of hiding in this ap-

proach.

2.3 Embedding process: noise significant bit substitution:

for $i = 1, \ldots, \ell(i)$**do**
$s^i \leftarrow c^i$
end for
for $i = 1, \ldots, \ell(m)$ **do**
Compute index j_i where to store ith message bit.
$snb_{ji} \leftarrow c_{ji}$?? m_i
end for

2.4 Extraction process:

for $i = 1, \ldots, \ell(M)$ **do**
compute index j_i where the ith messge bit is stored
$m_i \leftarrow \text{snb}(c_{ij})$
end for

First of all, the secret data will be divided into shares using visual cryptography. These shares will be treated as information to be embedded inside an Image. The embedding process consists of choosing a subset $\{j_{1,..}, j_{\ell(m)}\}$ of cover-elements and performing the substitution operation $c_{ji} \rightharpoonup m_i$ on them, which exchanges the SNB of c_{ji} by m_i (m_i can either be 1 or 0). The position of noise bits should be kept as stego-key for extracting the hidden data from the cover medium. In the extraction process, the data that replaced the Selected Noise Bits of the cover-elements are extracted with the help of kept key and lined up to reconstruct the secret message. Here symmetric key cipher is used.

3 PSUEDOCODE FOR THE PROPOSED SYSTEM

3.1 Psuedocode for Encoding Process

- Choose Information to be encrypted, say Mi.
- Create shares of the secret data. [first level of hiding]
- Select an appropriate image or images so that shares of the original message can be embedded in to a single image or more.
- The Image should consist of enough noises to be replaced.
- The selection of a suitable Image is done carefully.
- Shares will be embedded in place of noises in the image.
- Embedding is done using the SNB steganography technique. (Here we get second level of hiding).
- Keep the position of the noise bits as the stego-key for exactly extracting the hidden data.

3.2 Psuedocode for Decoding Process

- Use the stego-key and SNB-Steg decoding process to decrypt the secret from the image.
- Here we use symmetric key ciphers.
- After decoding the message from the cover medium [here the image] the receiver will get shares of the original message.
- These shares can then be super imposed and create the original message.

4 EXPERIMENTAL RESULT AND DISCUSSION

In this section, we present the results from the experiments we conducted in order to evaluate the performance of our proposed method. The proposed method begins with encrypting the secret using visual cryptography. Which itself gives good security. Subsequently, it embeds the secret shares using the proposed steganography. Experiment has done with plenty of images and a single case in point is shown in the following part.

Fig. 1. Secret Data

Fig. 2. Visual Cryptography shares

Fig. 3. Original Image With noises

Fig. 4.Shares embedded Image

In order to improve the security of the secret data communication, here we propose a new technique which gives better safety and security to secret communications. First create shares of the information to be transmitted. Here we get first level of hiding. Then these shares will be inserted into an image using steganography. Here we get second level of hiding. The steganography algorithm used is a new one of its kind. That is selecting an image with noises and these noise bits will be replaced with secret shares. [The original secret data]

Figure.1 is the secret; figure.2 is its visual cryptographic shares: Here we get the first level of hiding. Figure.3 is the cover medium in which some noises are seen. Figure.4 is where data (shares) are stored. Here achieves the second level of hiding. From the view of figures and the histogram analysis before and after steganography, shows it has significantly improved the cover medium, and noises present in the original image are cleared. In addition to this, as aforementioned a two level hiding is also obtained with this approach.

5 CONCLUSION

This project implemented the SNB steganography. It allows the authorized users to work. The algorithm developed can be used depending on the situation and application. The system is being developed as an attempt to overcome the difficulties of the existing system with enhanced features. Because of the complication of the steganography problem and progressive power of steganalysis algorithms, it is a hard problem to build up techniques with considerable better performance. To improve the security of the existing steganography methods, in this paper, we proposed a two-stage visual steganography scheme.

The psychological aspect of this proposed method is that it enhances the cover medium instead of disturbing its original view. Usually, it is easy to verify the presence of secret visually and psychologically by comparing the original image with its secret embedded version. Steganography makes disturbance to the cover image and hence steg-analyst can easily recognize the very presence of the secret. Here authors tried to enhance the image by removing noises already present through embedding secret at places where noise bits are present. So it reduces the chance of steg-analyst.

The following are the merits of the proposed system.

- This system reduces the distortion causing while hiding data inside images.
- Multilevel hiding is achieved
- Since SNB algorithm hides data only on selected bits, it tries to reduce the noise and enhances the clarity of the original image.

REFERENCES

1. Carlo blundo and clemente galdi, "Hiding Information in Image Mosaics", British Computer Society, Cryptography and Network Security Group, University of the Salerno, 84081 Baronissi (SA), Italy, 2003.
2. Karen Bailey & Kevin Curran," Evaluation of image based steganography methods using visual inspection and automated detection techniques", Springer Science, 2006
3. Fabien A. P. Petitcolas, Stefan Katzenbeisser "Information Hiding Techniques for Steganography and Digital Watermarking ",artech house, inc. 685, Canton Street Norwood.
4. Juan Jose Roque, Jesus Maria Minguet, "SLSB: Improving Steganographic Algorithm LSB, Proceedings, the Ibero-American Congress, 2009.
5. Pratt, W. K, "Digital Image Processing", New York: Wiley, 1991.(Book)
6. William Stalling, "Cryptography and Network Security-Principles and Practices", fourth edition, Pearson Prentice Hall pf India P.Ltd.(Book).
7. Chang D. C., & Wu, W. R, "image contrast enhancement based on a histogram transformation of local standard

deviation", IEEE Transactions on Medical Imaging, 17(4), 518–531, 1998.

8. Chen C., Shi Y. Q., Chen W., & Xuan G. "Statistical moments based universal steganalysis using JPEG-2D array and 2-D characteristic function". In Proceeding of CIP,Atlanta, GA, USA (pp. 105–108).2006.
9. Kharrazi M., Sencar H., & Memon, N. "Cover selection for steganograpic embedding". In Proceeding of ICIP (pp. 117–121).2006.
10. Hedieh Sajedi, Mansour Jamzad, "BSS: Boosted steganography scheme with cover image preprocessing", Computer Engineering Department, Sharif University of Technology, Iran.
11. Nilsson M., Dahl M., & Claesson. I. "Gray-scale image enhancement using the SMQT". In Proceeding of international conference on image processing.2005.
12. F. Liu, C.K. Wu1 X.J. Lin, "Colour visual cryptography scheme". IET Information Security, 2009.
13. Piyush Marwaha1, Paresh Marwaha,"Visual Cryptographic Steganography In Images", Second International conference on Computing, Communication and Networking Technologies,2010.
14. V. Potdar, E. Chang, "Visibly Invisible: Ciphertext as a Steganographic Carrier", Proceedings of the 4th International Network Conference, 385-391, 2004.
15. Potdar V.M, Chang E, "Grey level modification steganography for secret communication", Industrial Informatics, 2nd IEEE International, 2004.