Survey on Different Techniques of Image Steganography

Omkar Shetye
Student, Department of Information Technology Fr.Conceicao Rodrigues College of Engineering Mumbai, India

Chinmay Vanmali
Student, Department of Information Technology Fr.Conceicao Rodrigues College of Engineering Mumbai, India

Moses Fernandes
Student, Department of Information Technology Fr.Conceicao Rodrigues College of Engineering Mumbai, India

Prachi Patil
Assistant professor, Fr. Conceicao Rodrigues College of Engineering Mumbai, India

ABSTRACT
Steganography is the technique that hides any data behind other data. Many different carrier file formats can be used but digital images are the most popular ones because of their frequency on the Internet. Steganography are of four types – text, image, audio and video. There are many Steganography techniques for hiding secret information in images. A survey of image steganography is done here and all the techniques to hide a secret image behind an cover image are described.

Keywords
LSB method, DNA sequence method, Reversibility method and (n, n) secret sharing scheme method.

1. INTRODUCTION
Secured data has become an important factor in communication because of various hacking technologies. Messages need to be conveyed safely without any problem between sender and receiver. Due to which an idea of encoding information using redundant characters was made to prevent it from any third party person. Data which should be prevented from such attacks by the attacker can be encoded using different methods and with the use of Steganography. Steganography literally means covering any data, which was practiced during ancient times. In which impressions were created in wooden tablets and covered with wax so that the message will be hidden from any person. Though the methods in that era were physical, they served the purpose. And then more methodical practices were followed which helped in prevention of data from any attack. This marked the era of digital Steganography [6]. Steganography is the art of invisible communication of messages which is done by hiding information in other information. The word steganography is also said as covered writing. There is much difference between Steganography and Cryptography as cryptography keeps the contents of a message secret whereas steganography keeps the existence of a message secret. Steganography and cryptography are the two ways for protecting information from unwanted parties and one more technology that is closely related to steganography is watermarking [7]. The messages are hidden behind an image, text, audio and video. For example, use of invisible ink on any paper can be said as a hidden message. In some methods there is secret key shared between the sender and receiver which helps in proper transfer of messages. There is more security in steganography then in cryptography so steganography is better than the cryptography. In digital steganography, watermarking is used which provides evidence of authenticity. Best example for it is Gandhiji's photo on Indian note which can be seen only under the light. Digital watermarking can protect its content even after its decryption [8]. There are four types of file formats that are used for Steganography which are image, text, audio/video and portal. Images are mainly used for information hiding because images are most popular carrier objects. In the domain of digital images different image file formats exist most of them are available for specific applications. To hide text messages behind an image we can use image steganography and various techniques of it like DCT, DWT, LSB, Hash LSB and Spread Spectrum [9]. Image Steganography has many advantages and is most popular among the others. There are various methods available for implementing Image Steganography such as image domain and transformation domain algorithms [4].

2. TECHNIQUES OF STEGANOGRAPHY
There are mainly four techniques to perform steganography (to hide image into an image) which are as follows:

2.1 LSB method
The author has used an improved LSB method for 24 bit color image and 8 bit color image which are capable of producing secret embedded image. LSB method for both 8 bit and 24 bit are described and there comparison in terms of PSNR and MSE has been mentioned. This Algorithm embeds MSB of secret image into LSB of cover image. In 24 bit color image two methods are used with LSB method. In first method, last 2 LSB of each plane i.e red, green and blue of cover image is getting replace by 2 MSB of secret image and in other method, last LSB of each red plane is replaced by first MSB of secret image along with that last 2 LSB of each green plane is replaced by next 2 MSB of secret image and then also the last 3 LSB of blue plane is been replaced by next 3 MSB of secret image [5].

2.2 DNA sequence method
The author has presented a lossless steganography approach. In sender part, secret image is converted to DNA sequence using four nucleotides A, C, G & T then DNA sequence compression is done using 2-bits encoding method and converted to digital form then bit stream is segmented with 4 bits then by using (t, n) solution F(x) is calculated. Key values (x) from f(x) along with Sudoku solution matrix which is equal to the size of cover image is sent to the receiver. At the receiver end it will reconstruct F(x) using Lagrange's interpolation formula and will obtain the secret digits by extracting the last (t-1) coefficients of F(x). Again convert it in digital form and reconstruct DNA sequence and atlast secret image will be retrieved [2].

2.3 Reversibility method
The author has used (t, n) threshold sharing scheme to losslessly reveal the secret image. It takes use of Sudoku solution matrix. Here the original host image is recovered by embedded shadow images. Thus embedding 4x(t-1) secret bits into each pixel pair of the host image. It has large capacity for embedded secret data. sender sends all the shadows created of cover image to hide secret image and the receiver will recover the secret image by using sufficient shadow images [3].

2.4 (n, n) secret sharing scheme method

The author has used n cover images and n shadow images for sending Secret image to the receiver. Secret image is shared among n different cover images to generate n shadow images and reconstruction of secret image can be done using those n shadow images. Firstly in sender side, author has used Sudoku solution matrix then took secret image and scanned all the pixel values. For each pixel of the secret image he obtained two secret values. Then he took a cover image, taken any random pixel position and mapped the same position in Sudoku solution matrix. By Euclidean distance he mapped the secret value in Sudoku matrix. Altered pixels will be recovered in shadow images generated. Receiver side will reconstruct the secret image by (n, n) secret image sharing scheme. By comparing cover image with shadow image all the altered pixels are noted. Then by mapping the altered pixels position in Sudoku solution matrix secret values will be retrieved. From those secret values, original or secret image will be recovered. Judging from the visual perception of two shadow images and the cover images, this scheme can successfully camouflage [1].

3. COMPARATIVE ANALYSIS

parameters	Capacity	Robustness	Advantage	Disadvantage
LSB method	Yes	No	It is simple to implement , integrity to secret hidden info with high capacity and there are different LSB methods	It has low robustness and problems like low pass filtering and compression
DNA sequence method	Yes	Yes	DNA sequencing is used to represent secret image in min no of bits	Its capacity has low modification rate
Reversibility method	Yes	Yes	The reversibility of new sharing scheme is practically essential to preserve host images such as military and medical images	The participation in secret sharing approach may provide a fake shadowing and cheat other participants during secret revealing procedure
(n,n) secret sharing scheme method	Yes	Yes	Here (t, n) is replaced by (n, n) which makes it easy than the reversibility	The participation in secret sharing approach may provide a fake shadowing and cheat other participants during secret revealing procedure

4. APPLICATIONS OF IMAGE STEGANOGRAPHY

There are various applications in steganography some of which are as follows:

Copyright Control

Copyright is made with the help of watermarking. This copyright is mostly seen in images, videos and audios. In many games we can see the copyright information written so that anyone can see message or any type of information and no one can replace that message or information [10].

Covert Communication

The communication is made from sender to receiver and message is sent with the help of steganography without any error and the main feature of it is that the attacker doesn't come to know that communication was happening between anyone [12].

Smart Id´s

Information is hidden behind the image of a person so that the confidential info of that person is safe. This smart ID's helps in prevention of crimes by identifying the theft [11].

Printers

There are special printers which are used by Steganography for hiding the confidential data. Small yellow dots are created in papers which stores important data like serial no, date and time stamp [13].

5. CONCLUSION

Comparative analysis of different methods of steganography was made and from this analytical survey we have concluded that all method have some advantages and limitations. The strong and weak points of these techniques are mentioned briefly so that researches who work on steganography will gain prior knowledge in designing these techniques and their variants.

6. ACKNOWLEDGEMENT

7. REFERENCES

[1] C. G. Zhi-Hui Wang and C.-C. Chang, "A novel (n, n) secret image sharing scheme based on sudoku," JOURNAL OF ELECTRONIC SCIENCE AND TECHNOLOGY, vol. 11, March 2013.

[2] S. K. B. SumanChakraborty, Sudipta Roy, "Image steganography using dna sequence and sudoku solution matrix," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, February 2012.

[3] C.-C. Chang, "A sudoku-based secret image sharing scheme with reversibility," JOURNAL OF COMMUNICATIONS, vol. 5, January 2010.

[4] R.Poornima and R.J.Iswarya, "An overview of digital image steganography," International Journal of Computer Science and Engineering Survey, vol. 4, 2013.

[5] DeepeshRawat and VijayaBhandari, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image,"International Journal of Computer Applications (0975 – 8887),Volume 64– No.20, February 2013.

[6] R. S. AnkitChadha, NehaSatam and D. Bade, "An efficient method for image and audio steganography using least significant bit (lsb) substitution," International Journal of Computer Applications (0975 – 8887), vol. 77, September 2013.

[7] A. K. Mrs. Kavitha, KavitaKadam and P. Dunghav, "Steganography using least signicantbit algorithm," International Journal of Engineering Research and Applications(IJERA), vol. 2, pp. 338–341, May-June 2012.

[8] JagvinderKaur and Sanjeev Kumar, " Study and Analysis of Various Image Steganography Techniques" IJCST Vol.2, Issue 3, September 2011.

[9] Palak R Patel and Yask Patel, "Survey on Different Methods of Image Steganography, "International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 12, December 2014.

[10] Kambe et al., "COPYRIGHT CONTROL SYSTEM," United States Patent, 5,818,933, Oct. 6, 1998.

[11] S.Brindha Senior Lecturer, Computer Networking, PSG Polytechnic College, Coimbatore, India "Hiding Fingerprint in Face using Scattered LSB Embedding Steganographic Technique for Smart card based Authentication system," International Journal of Computer Applications (0975–8887) Volume 26–No.10, July 2011.

[12] Robert Rosenthal,Department of Psychology, University of California, Riverside, Riverside, California "Covert Communication in Laboratories, Classrooms, and the Truly Real World," CURRENT DIRECTIONS IN PSYCHOLOGICAL SCIENCE,2003.

[13] Seung-Jin Ryu, Hae-Yeoun Lee, Dong-HyuckIm, Jung-HoChoi, Heung-KyuLee,"ELECTROPHOTOGRAPHIC PRINTER IDENTIFICATION BY HALFTONE TEXTURE ANALYSIS," Korea Advanced Institute of Science and Technology, Republic of Korea Kumoh National Institute of Technology, Republic of Korea,2010.