Ravi saini al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 5, Issue 1, March 2018, pp. 308-310

Comparative Study of Current Image Steganography Techniques

Ravi Saini

Lecturer, CMRA Govt. Polytechnic Sanghi
Ravisaini1988@rediffmail.com

Abstract- **Today is world of communication. We transfer the various types of data using Internet and various types of mobile applications. With this communication, the risk of data privacy also increases. Today there are many techniques that are used for the purpose of data privacy like cryptography, steganography etc. Steganography is also of many types like text, image, video, protocol etc. In this paper, we will compare the various image steganography techniques.**

Keywords— Steganography, Image, Cryptography, Security.

I. Introduction

All The field of Steganography is very old. Throughout history, many steganography techniques have been documented, including the use of cleverly-chosen words, invisible ink written between lines, modulation of line or word spacing and microdots [1,2,3]. Usually the secret information is concealed by the use of an innocuous cover as to not arouse suspicion if hostile agents discover the cover. The most popular stegnographic methods used by spies include invisible ink and microdots. People used etching messages in wooden tablets and covered with wax. They used tattooing a shaved messenger's head, letting his hair grew back and then saving it again when he arrived at his contact point to reveal the message. [4].

Digital Steganography uses the digital objects such as image, music, video or any other computer file for hiding the data. Steganography can be classified into different categories based upon the cover media like image steganography, audio steganography, video steganography, text steganography etc. The popular and oldest of hiding the message in a digital image is the LSB method. In LSB method, we hide the message in least significant bit (LSB's) of pixel values of an image. [3].

There are three major disadvantages of LSB insertion method:-

1. Message can be easily recovered by the unauthorized person as message is in LSB.
2. As message is hidden in LSB, so intruder can modify the LSB of all the image pixels in the way the hidden message can be destroyed.
3. LSB is most vulnerable to hardware imperfections or quantization of noise.

Parvinder et al [5] proposed a technique, which uses 6th & 7th bit of pixels to overcome these drawbacks. But this itself has a drawback that the chances of message insertion at any location are reduced to 49%. Recently, Rajkumar et al [6] proposed a technique, which uses 6th, 7th & 8th bits of pixels to increase the chances of message insertion up to 85.93% In this method if the intruder changes the LSB of all the pixels then also we can retrieve the message.

Another technique for hiding data in digital image is Gray Level Modification technique (GLM). In this technique, Potdar et al [7] uses the concept of even and odd numbers. This technique provides 100% chances of message insertion. But, this technique also has two same disadvantages associated with it that are associated with LSB technique.

Those disadvantages are:-

1. Intruder can modify the LSB's of all pixel values such that the hidden message can be destroyed without so much change in image quality.
2. Due to hardware imperfections and quantization of noise, LSB of the pixel value can be changed due to which the message bit 0 becomes 1 and vice-versa.

II. Applications of Steganography

Steganography, in general, have many applications including copyright protection, Feature Tagging and secret communications etc. [3,8].

1. Copyright Protection

A secret copyright notice or watermark can be embedded inside an image to identify it as intellectual property. This is the watermarking scenario where the message is the watermark. A watermark can also serve to detect whether the image has been subsequently modified.

2. Feature Tagging

Captions, annotations, time stamps and other descriptive elements can be embedded inside an image, such as the name of the individuals in a photo or location 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.

3. Secret Communication

In many situations, transmitting a cryptographic message draws unwanted attention. The use of cryptographic technology may be restricted or forbidden by law. However, the used steganography does not advertise covert communication and therefore, avoid scrutiny of the sender, message and recipient.

4. Digital Watermark

The objective of a digital watermark is to place an indelible mark on an image. Usually, this means encoding only a handful of bits, sometimes as few as one. This "signature"

could be used as a means of tracing the distribution of images for an on-line news service and for photographers who are selling their work for digital publication. One could build a digital camera that places a watermark on every photograph it takes. Theoretically, this would allow photographers to employ a "web-searching agent" to locate sites where their photographs appear [8].

5. Tamper Proofing

The objective of tamper-proofing is to answer the question, "Has this image been modified?" Tamper-proofing techniques are related, but distinct from the other data-hiding technologies. What differentiates them is the degree to which information is secured from the host signal. Most data-hiding techniques attempt to secure data in the face of all modifications. Tamper-proofing techniques must be resilient to small modifications (e.g., cropping, tone scale or gamma correction for images or balance or equalization for sounds) but not to large modifications (e.g., removing or inserting people from an image or taking words out of context in an audio recording [8].

III. TYPES OF STEGANOGRAPHY

We can classify steganography into mainly four parts depending upon the cover media i.e.

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography

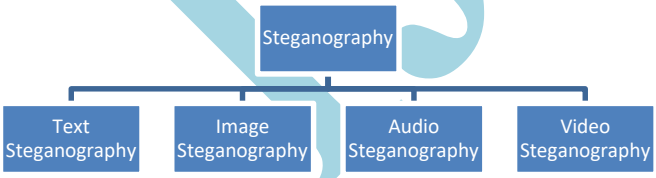

Fig. 1 Classification of Steganography

IV. COMPARATIVE STUDY

Technique Name	Featues	*Advantages*	*Disadvantages*
LSB[3]	LSB of Image pixel is used for insertion of message	Simple	Effected by Noise
6^{th},7^{th}& 8^{th} Bit Method[6]	6^{th},$7^{th}$and 8^{th} bit of image pixel is used for insertion of message	Message Insertion Chances Increases	Not provide 100% chances of message insertion
Partity Checker Method [6]	Parity of image pixel is used for insertion of message	Simple and Provide 100% chances of message insertion	Not Robust
GLM Method[7]	Grey Level Value of pixel is used for insertion of message	Simple and easy to implement	Also Affected by noise
PVD Method[9]	Difference of adjacent pixel is used for insertion of message	High Hiding Capacity and outstanding imperceptibility to stego image	Not Provide optimal hiding capacity
LSB-SM[10]	Magic Matrix is used for insertion of message	Data hiding capacity is high	Highly Complex
LSB-S[11]	Logical Shift Operation is used for insertion of message	Easy to implement and imperceptibility is high	Easy to break
Chaotic Method[12]	Uses Chaotic based equation	Robust Technic	Data capacity and PSNR is less
XOR Based Method[13]	Uses Bit Wise XOR Operation	Imperceptibility is high	Robustness is less
Pixel Interpolation Based Method[14]	Image is enlarged using different interpolation techniques to enhance the capacity of data	Hiding Capacity is increased	Image Structure is disturbed during enlargement of image

V. CONCLUSION

In this Paper, we have studied various image Steganography techniques like LSB Method,GLM, Parity Checker Method, LSB-S, LSB-SM ,Data Hiding Using XOR for Image Steganography etc. In the future, we will try to develop some new image Steganography Techniques.

REFERENCES

[1]. Rodrigues, J. M., Rios, J. R. and Puech, W. (2006), "SSB-4 System of Steganography using bit-4".

[2]. Gutub, A. and Fattani, M. (2007), "A Novel Arabic Text Steganography Method Using Letter Points and Extensions", World Academy of Science, Engineering and Technology, 27.

[3]. Johnson, N. and Jajodia, S. (1998), "Exploring steganography: seeing the unseen," *IEEE Computer*, pp. 26-34.
[4]. Anderson, R. J. (1996), "Stretching the Limit of Steganography", In Information Hiding, Springer Lecture Notes in Computer Science, Vol. 1174, pp 39-48.
[5]. Singh, P., Batra, S. and Sharma, H.R. (2005), ""Evaluating the Performance of Message Hidden in First and Second Bit Plane", WSEAS Transaction on Information Science and Technology, vol. 2, no 8, pp 1220-1222.
[6]. Yadav, R., Rishi, R. and Batra, S.(2010), "A new Steganography Method for Gray Level Images using Parity Checker", International Journal of Computer Applications (0975-8887) Volume 11-No. 11.
[7]. Potdar, V. and Chang, E. (2004), "Gray Level Modification Steganography for Secret Communication", IEEE International Conference on Industrial Informatics, Berlin, Germany.
[8]. Bender, W. and Gruhl, D. (1996), "Techniques for data hiding", Ibm Systems Journal, Vol 35, Nos 3&4.
[9]. D.C. Wu and W.H. Tsai,A steganographic method for images by pixel value differencing‖,Pattern Recognization Letters, Vol. 24, pp 1613,2003
[10]. Khan M, Muhammad S, Irfan M, Seungmin R, Sung B W, A novel magic LSB substitution method (M-LSB-SM) using multilevel encryption and achromatic component of an image. Springer, May 2015, DOI: 10.1007/s11042-015-2671-9
[11]. Joshi K, Yadav R, "A new LSB-S image steganography method blend with Cryptography for secret communication", in Proceedings of Third International Conference on Image Information Processing (ICIIP), Pages: 86 – 90, 2015.
[12]. Atawneh S, Sumari P, "Hybrid and blind steganographic method for digital images based on DWT and chaotic map". Journal of Communications, 8(11), 690–699. (2013). DOI: 10.12720/jcm.8.11.690-699
[13]. Joshi K, Dhankhar P, Yadav R, "A new image steganography method in spatial domain using XOR", in Proceedings of Annual IEEE India Conference (INDICON), IEEE, Pages: 1 – 6, 2015
[14]. Ki-Hyun Jung & Kee-Young Yoo, "Steganographic method based on interpolation and LSB substitution of digital images" Springer Science+Business Media New York, 5 jan., (2014)
[15]. Hartung, F. and Kutter, M. (1999), "Multimedia Watermarking Techniques," Proc, IEEE, vol. 87, no. 7, pp. 1079-1107.
[16]. Hassan, M. and Shahreza, M. (2006) "A New Approach to Persian/Arabic Text Steganography," 5th IEEE/ACIS International Conference on Computer and Information Science (ICISCOMSAR 06), pp. 310- 315.
[17]. Jacokes, B., Kodysh, Y. and Lisy, A. (2005), " Audio Steganography".
[18]. Judge, J.C. (2001),"Steganography: Past, Present and Future", Sans Institute.
[19]. Kahn, D.(1996), "The History of Steganography", Proc. of First Int. Workshop on Information Hiding, Cambridge,UK, Lecture notes in Computer Science, Vol.1174, Ross Anderson (Ed.), pp.1-7.
[20]. Kejariwal, A. (2003), "Watermarking", IEEE Potentials, Vol. 22, No. 4, pp: 37 – 40.
[21]. Krenn, R. (2006)," Steganography and steganalysis".
[22]. Kutter, M., and Hartung, F. (2000), "Introduction to watermarking techniques – Information technology for steganography and digital watermarking", Artec House.
[23]. Lee, Y.K. and Chen, L.H. (2000), "A Secure Robust Image Stegnography Model", 10th National Conference on Information Security, Hualien, Taiwan, pp 275-284.

