A Review of Video Steganography Techniques

Ravi Saini

Lecturer, CMRA Govt. Polytechnic Sanghi

Ravisaini1988@rediffmail.com

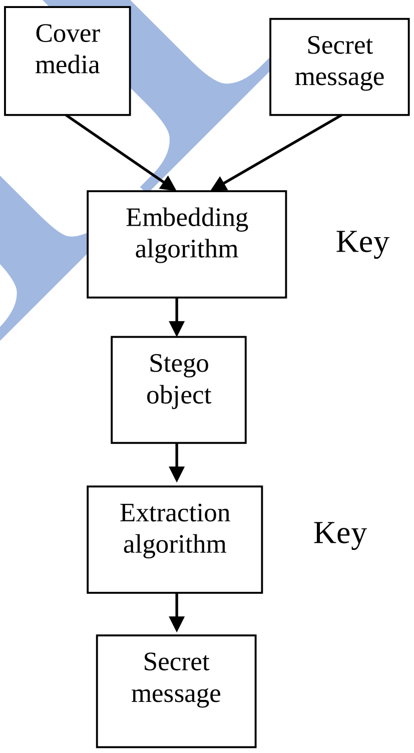
Abstract- **As the internet is growing day by day, Secure communication is the major concern. People do secret communication with various modes like Cryptography, Steganography etc. Steganography is one of the basic technique of secret communication. It uses the image, text, audio file, video file etc. as cover media. A single image frame can only contain limited data. To avoid this limitation, video steganography came into existence. A video steganography uses video file as a cover media. In this paper, different video steganography methods have been reviewed.**

Keywords— Video Steganography, Cryptography, Security, Data Hiding.

1. Introduction

Steganography is a process of hiding information in a cover media. Steganographic techniques hide the very existence of the message. The term Steganography is formed by two Greek words 'stegno means' covert and graphy means 'writing', which means covert writing[1]. However, in hiding information, the meaning of steganography is hiding text or secret messages into another media file such as image, text, sound or video. The word "steganography" is generally considered similar to "cryptography" and "watermarking". But watermarking ensures message integrity. Digital watermarking is the method of embedding data into digital multimedia content. This is used to verify the credibility of the content or to recognize the identity of the digital content's owner. Digital watermarking can be employed for multiple purposes, such as,Copyright protection, Source tracking, broadcast tracking, such as watermarked videos from global news organizations Hidden communication[2], Cryptography is the process of hiding the meaning of secret information so that only those for whom it is intended can read and process it[3]. The word is derived from the Greek kryptos, meaning hidden. Whereas steganography hides the message. The primary objective of steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raised, then this objective that has been planned to achieve the security of the secret message because if the hackers noted any change in the sent message then this observer will try to know the hidden information inside the message[4].

For the steganographic purpose the following terminology were used
Secret message: Message to be hidden.
Cover media: Medium in which message is to be hidden.
Embedding algorithm: Algorithm to insert stego-object
Stego object: Object having hidden message
Extraction algorithm: Algorithm to extract message from stego-object.
Sectete Key: Key for insertion and extraction.



Process of steganography

2. Type style and fonts

On the bases of cover media the steganography is classified in the following sub domain

- Steganography in text
- Steganography in audio
- Steganography in video
- Steganography in images

Text steganography

Text steganography can be achieved by altering the text formatting, or by changing characters. The aim in the design of coding techniques is to develop alterations that are reliably decodable (even in the presence of noise) yet largely indiscernible to the reader[5]. These criteria, reliable decoding and minimum visible change, are somewhat conflicting; herein lies the challenge in designing document marking techniques.

Audio steganography

Audio steganography is the technique of hiding information inside an audio signal. In this type of steganography audio acts as a cover medium and information is embedded in it. The modification done in audio must be made imperceptible to the human ear so that on could not detects the presence of information[6].

Video steganography

Video Steganography is a technique to hide any kind of files into a carrying Video file. The use of the video based Steganography can be more eligible than other multimedia files, because of its size and memory requirements[7]. The least significant bit (LSB) insertion is an important approach for embedding information in a carrier file. Least significant bit (LSB) insertion technique operates on LSB bit of the media file to hide the information bit.

Image steganography

In case of image steganography secret information is hidden into a cover image. Pixel bits of cover image are replaced by bits of message. The most common methods of image steganography are the least-significant bit or LSB, masking, filtering and transformations on the cover image[8]. These techniques can be used on different types of image files.

3. Different Techniques of video steganography

1. Johnson N. and Jajodia S proposed "Exploring steganography: seeing the unseen,"[13]

N Johnson and S Jajodia introduced LSB method.In this method, we hide the message in least significant bit (LSB's) of pixel values of an image. In this method binary values of the secret message is placed in the LSBs of each pixel of a cover image.

The oldest technique of concealing the message in an image is the LSB method. In this method, we hide the message in least significant bit (LSB's) of pixel values of an image. In this method binary values of the secret message is placed in the LSBs of each pixel of a cover image.

For example, considered 8 pixels of a 8-bit image, using 9 bytes of memory:

00100111 11101001 11001000 00100111 11001000 11101001 11001000 00100111

When the character A, which binary value equals 10000001, is inserted, the following pixel results:

00100111 11101000 11001000 00100110 11001000 11101000 11001000 00100111

In this case, only three bits needed to be changed to insert the character. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximal cover size. The result changes that are made to the least significant bits are too small to be recognized by the human eye, so the message is effectively hidden.

Advantages of spatial domain LSB technique are:

1. There is less chance for degradation of the original image.
2. More information can be stored in an image.

Disadvantages of LSB technique are:

1. Less robust, the hidden data can be lost with image manipulation.
2. Hidden data can be easily destroyed by simple attacks.
3. LSB is most vulnerable to hardware imperfections or quantization of noise.

2. D.C. Wu and W.H. Tsai proposed "A steganographic method for images by pixel value differencing,"[14]

D.C. Wu and W.H. Tsai introduced pixel value differencing. The pixel value differencing (PVD) technique provides not only good embedding capacity but also good imperceptibility for the stego image. In this technique cover image is divided into non overlapping blocks having two connecting pixels and changes the pixel difference in each block for data embedding. Larger difference in the real pixel values provides greater modification.

3. Muhammad Bilal, Sana Imtiaz,Wadood Abdul Sanaa Ghouzali • Shahzad Asif proposed proposed " Chaos based Zero-steganography algorithm" [15]

Muhammad Bilal et al introduced a new data hiding method. This technique hides the message on the basis of a relationship of the cover image, chaotic sequence and the message. Also by using the chaotic map while hiding data security is increased This method is analysed using various parameters such as noise, JPEG compression, low pass filtering attacks. Imperceptibility analysis shows that this method is completely imperceptible independent of the length of message. This technique is also analysed for security and is found to be very secure.

4. Wafaa hasan alwan,"Dynamic Least Significant Bit Technique For Video Steganography, 2013[16]

By adding 4 LSB of cover and 4 MSB of hidden frame the position of embedding data is generated. Security is high as compared to LSB method. Complexity of this method is high.

5. Kousik Dasgupta et al. Hash Based Least Significant Bit Technique For Video Steganography, 2012[17]

It Uses 4 LSB of cover frame and then hash function for find the position of embedding the data. It can be applied on different format files with minor changes. PSNR value is low as compared to LSB which decreases the quality

6. Vipula Madhukar Wajgade and Suresh Kumar, Enhancing Data Security Using Video Steganography 2013[18]

It Uses 4 LSB of cover frame and then hash function for find the position of embedding the data. It can be applied on different format files with minor changes. PSNR value is low as compared to LSB which decreases the quality

7. Shivani Khosla and Paramjeet Kaur, Secure Data Hiding Technique Using Video Steganography and Watermarking 2014[19]

It Uses a graphical password and then convert that in binary form apply LSB and after that DCT and DWT is applied for getting watermarked video. Security level increases because of using three combinations of techniques. In this method, Encryption is more complex

4. Conclusion

In this Paper, we have studied various video Steganography techniques like LSB, PVD , Hash Based LSB Technique , Dynamic LSB Technique etc. In the future, we will try to develop some new video Steganography Techniques and try to embed it with encryption technique to make more secure and robust technique.

REFERENCES

1. V. O. Waziri and A. Ochoche, “Steganography and Its Applications in Information Dessimilation on the Web Using Images as SecurityEmbeddment : A Wavelet Approach,” vol. 01, no. 02, pp. 194–202, 2012.
2. Yadav and R. Saini, “Biometric Template Security Using Invisible Watermarking With Minimum Degradation in Quality of Template,” vol. 3, no. 1, pp. 3656–3668, 2011.
3. V. Pascal, “Code Based Cryptography and Steganography,” pp. 9–46, 2013.
4. A. S. Hameed, “Hiding of Speech based on Chaotic Steganography and Cryptography Techniques,” vol. 6890, no. 4, pp. 165–172, 2015.
5. Y. K. Lee and L. H. Chen, “High capacity image steganographic model,” IEE Proc. - Vision, Image, Signal Process., vol. 147, no. 3, p. 288, 2000.
6. M. H. Rajyaguru, “CRYSTOGRAPHY-Combination of Cryptography and Steganography With Rapidly Changing Keys,” vol. 2, no. 10, pp. 329–332, 2012.
7. H. Anand, K. Narwal, and K. Mudgal, “Implementation of 16 * 16 Quantization Table Steganography on Gray Scale Images,” vol. 2, no. 7, pp. 2–5, 2013.
8. K. Kaur and E. N. Singh, “International Journal of Advanced Research in,” vol. 3, no. 6, pp. 402–405, 2013.
9. A. Kumar and R. Sharma, “International Journal of Advanced Research in A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique,” vol. 3, no. 7, pp. 363–372, 2013.
10. G. Chawla and R. Saini, “Classification of Watermarking Based upon Various Parameters,” vol. I, no. Ii, pp. 16–19, 2012.
11. R. J. Anderson, “Cryptography,” Secur. Eng. A Guid. to Build. Dependable Distibuted Syst., pp. 73–114, 2010.
12. E. Satir and H. Isik, “A Huffman compression based text steganography method,” Multimed. Tools Appl., vol. 70, no. 3, pp. 2085–2110, 2014.
13. N. F. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen,” Computer (Long. Beach. Calif)., vol. 31, no. 2, 1998.
14. D. C. Wu and W. H. Tsai, “A steganographic method for images by pixel-value differencing,” Pattern Recognit. Lett., vol. 24, no. 9–10, pp. 1613–1626, 2003.
15. M. Bilal, S. Imtiaz, W. Abdul, S. Ghouzali, and S. Asif, “Chaos based Zero-steganography algorithm,” Multimed. Tools Appl., vol. 72, no. 2, pp. 1073–1092, 2014.
16. Wafaa hasan alwan,“Dynamic Least Significant Bit Technique For Video Steganography”, Journal of Kerbala University,Volume-11, No.4, 2013
17. Kousik Dasgupta, J.K. Mandal and Paramartha Dutta, “Hash Based Least Significant Bit Technique For Video Steganography”,International Journal of Security, Privacy and Trust Management,Volume-1,No.-2,April 2012
18. Vipula Madhukar Wajgade and Dr. Suresh Kumar, “Enhancing Data Security Using Video Steganography”, International Journal of Emerging Technology and
19. Shivani Khosla and Paramjeet Kaur,“Secure Data Hiding Technique Using Video Steganography and watermarking”,International Journal of Computer Applications,Voume-95,No.-20,June 2014