Digital Innovations
& Contemporary Research in SCIENCE,
ENGINEERING & TECHNOLOGY
Vol. 10. No. 4, December 2022 – Special Issue on Cryptography & Security Mechanisms

Article Citation Format
Ohipeni, E.A.K (2022): A Survey of Video Steganography Algorithms.
Journal of Digital Innovations & Contemporary Research in Science,
Engineering & Technology.
Vol. 10, No. 2. Pp 61-64
DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V10N4P8

A Survey of Video Steganography Algorithms

Ohipeni Edwin Angmor Kofi
School of Technology
Ghana Institute of Management & Public Administration
GreenHills, Accra, Ghana
E-mail: ohipeniedwinangmor@gmail.com
Phone: +233501430488

ABSTRACT

The need for data encryption has become more important than ever since the appearance of the covid-19 virus which has led to the rate at which cybercrimes are committed to triple. Data is generally in the form of text, audio, video, and image. Over the years researchers have found a way to hide specific information to intended destinations in these data forms. The is called steganography and hiding secret information in video is known as video steganography. In this paper, a survey on some video steganography algorithms have been presented. Recommendations and direction for future works are also discussed in this paper.

Keywords: Steganography, cover image, secret data, steganalysis, least significant bit (LSB), motion picture expart group (MPEG), high embedding efficiency, embedding payload

1. INTRODUCTION

The evolution of the internet in the early 90's has changed the lifestyle of people drastically. Banking, shopping, etc. has become so easy to do with just a click of a button. This has made the lives of humans very comfortable, which also comes with some bad news because now the internet has become a major source of information interchange. Interchanging information on the internet has possessed more threat than carrying a huge amount of money on you and walking on the streets. Interchanging the information on the internet has created the threats of information to be intercepted by some unauthorized group of people otherwise known as hackers. These actions brought the need for some form of techniques which can secure and safeguard the information from unauthorized persons. Steganography is one of the techniques to curb the problem. People have utilized it ever since the beginning of time. Secret knowledge was formerly concealed in ancient artifacts like rabbits, the scalps of slaves, and the backs of wax.

Steganography is a technique used to hide the secret information in a cover file which may be in the form of audio, video, image or even text. In steganography, secret information is hidden in such a way that nobody other than intended person knows the existence of the information within the cover file. Cryptography is distinct from steganography. Cryptography is encrypting data is another method for protecting sensitive information, steganography hides sensitive information in cover files so that it won't raise any red flags. In contrast to cryptography, which encrypts data, steganography does not leave any room for suspicion (Nath Choudry & Wanjari, n.d.).

The two most important aspects of any steganography system are the embedding payload and embedding efficiency. Embedding payload is the amount of data which can be hidden in the cover file. Embedding efficiency is the capacity of steganography system to hide as much data as it can with inducing as least distortion as it can on the cover file. The most important criteria for any steganography system is the high embedding effectiveness. It is quite impossible to think that the cover file may contain any hidden information because high embedding efficiency results in the least amount of distortion. Because of this, using any steganalysis tool to extract information from the cover file is challenging. The link between embedding payload and embedding efficiency is often inversely proportional. The embedding payload will reduce as embedding efficiency increases and vice versa. Below are some of the common terms which is necessary to understand any steganography system (Nath Choudry & Wanjari, n.d.).

1. Cover Media - It is the medium in which secret information is embedded in such a way that it is difficult to detect the presence of data
2. Stego Media - It is medium obtained after embedding the secret information.
3. Secret Data - The data or information to be hidden in cover media.
4. Steganalysis - The process of detecting, presence of secret data in cover media

2. RELATED LITERATURE AND RESEARCH GAPS

Video mostly consists of static images that were captured at various points in time, and when these photos are played back continuously, we may perceive a moving image. "Frames" are the term for these still pictures. As a result, video steganography may be seen as an extension of image steganography, and the majority of research in the subject of video steganography is therefore essentially an extension of image steganography (Nath Choudry & Wanjari, n.d.).

Wang described a steganographic technique in his paper from 2002 that can conceal a lot of data. In his technique, he uses the discrete cosine transform. The main objective of this method is to boost the steganography method's payload capacity while maintaining resilience and simplicity. The secret information is embedded using this technique in one frame of the video (Neeta et al., 2006). In his approach, he first calculated the I-frame DCT coefficient before performing the modulation between the DCT coefficients and the secret data.

The 3-D SPIHT-BPSC steganography and JPEG 2000-BPSC are tested for this approach. The first technique combines the steganography techniques of BPSC and SPIHT coding. On the other hand, the second technique combines the BPSC algorithm and the JPEG 2000 standard, as the name suggests. The performance of the 3-D SPIHT-BPSC method is superior to the counterpart JPEG 2000-BPSC approach, according to experimental findings on both algorithms (Www et al., 2008).

The vector embedding approach was another data concealing technique that Lane introduced in 2007. For the MPEG-I and MPEG-II video standards, this approach is employed. By using this technique, the audio data is embedded within the host frames' pixels (A P & P P, 2010; Dasgupta et al., 2013). R. Kavitha and A. Murugan (Thyagharajan & Ramachandran, 2008) proposed a steganography method in 2007 that was created for the AVI video format. This technique makes advantage of switching.

The steganography methods for JPEG images and AVI file formats were also compared and contrasted in this work. The comparison is done in terms of the payload size and host image quality. The author of this work concluded that using UTF-32 encoding in the swapping technique will increase the key's security and, as a result, increase the security of the steganography method. The only flaw in this system is how little payload it can support (Thyagharajan & Ramachandran, 2008). In 2009, Cheng-Hung Chuang et.al. proposed an optical video crypto system.

This method uses adaptive steganography for video file encryption and decryption (Chuang & Lin, n.d.). Double random phase encoding algorithm is used in this method for encrypting and decrypting the video file. This method, first of all covert the video file in to RGB frames i.e. red, green and blue channel. Each channel is then encrypted by using the two random phase mask. To generate these phase mask, two sessions key are used in this model. Asymmetric key is used to enhance the security even further.

These key are encrypted and then embedded in the encrypted version of the video file. Content dependent data hiding algorithm is used for this purpose which produce low distortion in the cover video. Zero-LSB sorting algorithm is used for hiding the encrypted key in the video stream. Experimental results of this paper shows that performance wise this method outperforms the traditional steganography method (Chuang & Lin, n.d.).

A large capacity video steganography based on integer wavelet transform was provided by Lakshmi Narayanan, Prabakaran G, and Bhavani R in their study from 2012(Narayanan & Reader, 2012). The host picture in this integer wavelet transform is employed to create the stego-image. This approach increases the payload capacity since just the approximate band of the hidden picture is taken into account in the algorithm. The embedding algorithm is exactly what the extraction algorithm is not. The outcome of the simulation demonstrates that this strategy is more capable, resilient, and secure. Since integer wavelet transform produces the least amount of embedding distortion and performs better when utilizing the spatial and temporal correlation within and between the frames, it is employed in this approach (Narayanan & Reader, 2012).

A fresh method of "Video steganography employing 32 x 32 vector quantization of DCT" was proposed by Prajna Vasudev and Kumar Saurabh in 2013(Nath Choudry & Wanjari, n.d.). This approach starts by converting the input video into frames. Following LSB quantization, which leaves some empty space in the frames, 32 x 32 vector quantization of DCT is generated from each frame. The information bit is placed in these empty spaces.

3. CONCLUSION

In the era of fast information interchange using internet and World Wide Web, Steganography has become essential tool for information security. This paper presents a review work in different steganography methods. Pros and cons of different steganography algorithm were also discussed in this paper

REFERENCES

1. A P, S., & P P, A. (2010). A Compressed Video Steganography using TPVD. International Journal of Database Management Systems, 2(3), 67–80. https://doi.org/10.5121/ijdms.2010.2307
2. Chuang, C.-H., & Lin, G.-S. (n.d.). An Optical Video Cryptosystem with Adaptive Steganography.
3. Dasgupta, K., Mondal, J. K., & Dutta, P. (2013). Optimized Video Steganography Using Genetic Algorithm (GA). Procedia Technology, 10, 131–137. https://doi.org/10.1016/j.protcy.2013.12.345
4. Narayanan, L., & Reader, B. R. (2012). Computer Networks. In Journal of Computer Applications (Issue 5).
5. Nath Choudry, K., & Wanjari, A. (n.d.). A Survey Paper on Video Steganography. www.ijcsit.com
6. Neeta, D., Snehal, K., & Jacobs, D. (2006). Implementation of LSB steganography and its evaluation for various bits. 2006 1st International Conference on Digital Information Management, ICDIM, 173–178. https://doi.org/10.1109/ICDIM.2007.369349
7. Thyagharajan, K. K., & Ramachandran, V. (2008). Segmentation analysis for effective usage of network resources in video streaming. Proceedings - International Conference on Computational Intelligence and Multimedia Applications, ICCIMA 2007, 4, 383–387. https://doi.org/10.1109/ICCIMA.2007.380
8. Www, W. :, Wajgade, V. M., & Kumar, S. (2008). International Journal of Emerging Technology and Advanced Engineering Enhancing Data Security Using Video Steganography. In Certified Journal (Vol. 9001, Issue 4). www.ijetae.com