Review of Role of Digital Video in Information Security

Dinesh Goyal [1], Pratima Jha[2]

[1] Vice-Principal, Suresh Gyan Vihar University, Vice Chairman, CSI, Jaipur, India

[2]Suresh Gyan Vihar University, M. Tech (Student), Jaipur, India

Abstract: ***One of the reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of Steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists. In this review paper we will understand what Steganography, Cryptography is and what are the advantages of using them? In last we will discuss our goal of this paper that what types of techniques worked on video Steganography?***

Keywords: Steganography**.** Cryptography, security, gif image, video

1. Introduction

The desire to send a message as safely and as securely as possible has been the point of discussion since time immemorial. Information is the wealth of any organization. This makes security-issues top priority to an organization dealing with confidential data. Whatever is the method we choose for the security purpose, the burning concern is the degree of security. Steganography is the art of covered or hidden writing. The purpose of Steganography is covert communication to hide a message from a third party. [4]

Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Steganography in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. What Steganography essentially does is exploit human perception; human senses are not trained to look for files that have information hidden inside of them. Generally, in Steganography, the actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or audio which in turn is being hidden within another object. This apparent message is sent through the network to the recipient, where the actual message is separated from it.

2. Steganography and Cryptography

2.1 Comparison of Steganography and Cryptography

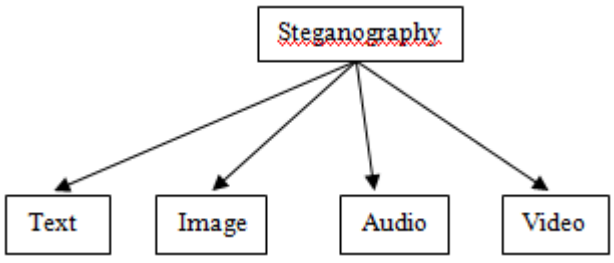
Steganography and cryptography are closely related. Cryptography scrambles messages so it can't be understood. Steganography on the other hand, hide the message so there is no knowledge of the existence of the message. With cryptography, comparison is made between portions of the plaintext and portions of the cipher text. In Steganography, comparisons may be made between the cover-media, the stego-media, and possible portions of the message. The end result in cryptography is the cipher text, while the end result in Steganography is the stego-media. The message in Steganography may or may not be encrypted. If it is encrypted, then a cryptanalysis technique is applied to extract the message.

2.2 Combination of Steganography and Cryptography

Those who seek the ultimate in private communication can combine encryption and Steganography. Encrypted data is more difficult to differentiate from naturally occurring phenomena than plain text is in the carrier medium. There are several tools by which we can encrypt data before hiding it in the chosen medium. In some situations, sending an encrypted message will across suspicion while an invisible message will not do so. Both methods can be combined to produce better protection of the message. In case, when the Steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques.

3. Types of Steganography Methodology

We have four types of Steganography methodology these are showing in this figure

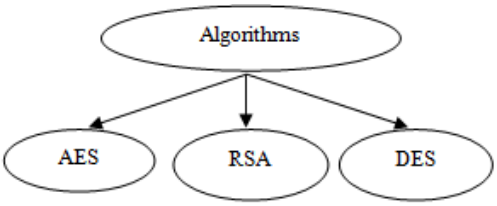


But in this paper we will discuss about video Steganography.

4. Video Secure Message Communication

The use of video as a carrier cover for the secure message is overcame the capacity problem and added small enhancement to the security aspects. The integration of steganography and cryptography techniques provided powerful systems for sharing secure messages. This integration especially within video cover carrier is a good stage of such systems, but the capacity of the produced message from the cryptography technique which is called cipher-text is larger than the original message (plaintext). The cryptography techniques increase the size of message after the encryption to be greater than the size of the original message, on another hand shown that the cipher-text size is much larger than the plaintext size by using the cryptography techniques. While found out the cipher-text size is usually long, at least twice that of the original plaintext. In additional, some specific implementations of cryptography required special hardware at appreciable costs as well as the cryptographic functions require considerable computation and CPU processing time, which might introduces the binding latency. [13]

For solving this problem, researchers have implemented various algorithms for video security to achieve secret communication. Mostly we have used these algorithms for security on video steganography.

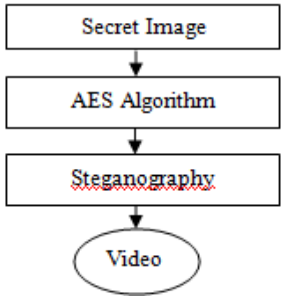


The proposed method for the data hiding is based on video Steganography where we may use the AES algorithm to make the Steganography more secure and robust. The video Steganography is achieved by embedding the video files with the secret data that is to be transmitted with the intention of keeping the secret data unaltered or remains intact at receivers end. [12]

4.1 AES (Advanced Encryption Standard)

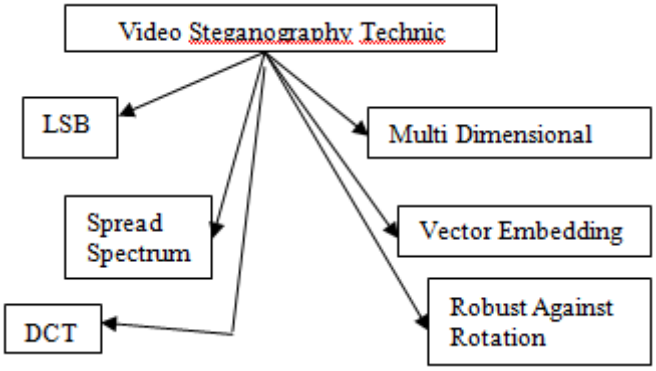
The AES algorithm is most secure and robust cryptographic algorithm against attacks. Unlike the DES which is far slow and is already broken and also produce inefficient software code. Triple DES on the other hand is comparatively slower than DES as it has three more rounds. AES has symmetric block cipher and hence uses same key for encryption and decryption.

The block size of AES varies from 128, 192, and 256 bits the substitution and permutation are performed in AES. The number of rounds depends upon the key length i.e. 10 rounds for 128 bit key,12 for 192 bit key and 14 for 256 bit key. We may also used SHA-1 for providing more restricted approach as it generates the hash function with key which helps to make the secret data secure if it is being identified without key it can never be altered[12]. It will work like this figure



5. Video Steganography Methodology

Several new approaches are studied in video data Steganography literature. In this section, some of the most well-known approaches have been discussed.



First of all, the most common method is Least Significant Bit method (LBS) which hide secret data into the least significant bits of the host video. This method is simple and can hide large data but the hidden data could be lost after some file transformations.

Another well-known method which has been still researching is called Spread Spectrum. This method satisfies the robustness criterion. The amount of hidden data lost after applying some geometric transformations is very little. The amount of hidden lost is also little even though the file is compressed with low bit-rate. This method satisfies another criterion is security.

There are also some introduced methods that base on multi-dimensional lattice structure, enable a high rate of data embedding, and are robust to motion compensated coding or enable high quantity of hidden data and high quantity of host data by varying the number of quantization levels for data embedding.

Wang et. al. presented a technique for high capacity data hiding using the Discrete Cosine Transform (DCT) transformation. Its main objective is to maximize the payload while keeping robustness and simplicity. Here, secret data is embedded in the host signal by modulating the quantized block DCT coefficients of I- frames.

Lane proposed a vector embedding method that uses a robust algorithm with video codec standard (MPEG-I and MPEG-II). This method embeds audio information to pixels of frames in host video.

Moreover, a robust against rotation, scaling and translation (RST) method was also proposed for video watermarking. In this method, secret information is embedded into pixels along the temporal axis within a Watermark Minimum Segment (WMS).Some application are discuss below which using for compressed video.

5.1 Application of BPCS Steganography to WAVELET Compressed Video

A Steganography method is using lossy compressed video which provides a natural way to send a large amount of secret data. The proposed method is based on wavelet compression for video data and bit-plane complexity segmentation (BPCS) Steganography. In wavelet based video compression methods such as 3- D set partitioning in hierarchical trees (SPIHT) algorithm and Motion-JPEG2000, wavelet coefficients in discrete wavelet transformed video are quantized into a bit-plane structure and therefore BPCS Steganography can be applied in the wavelet domain. 3-D SPIHT-BPCS Steganography and Motion- JPEG2000-BPCS Steganography are presented and tested, which are the integration of 3- D SPIHT video coding and BPCS Steganography, and that of Motion-JPEG2000 and BPCS, respectively. Experimental results show that 3-D SPIHT-BPCS is superior to Motion- JPEG2000-BPCS with regard to embedding performance. [2][3][1]

5.2 An Optical Video Cryptosystem with Adaptive Steganography

An optical cryptosystem with adaptive Steganography is proposed for video sequence encryption and decryption. The optical crypto system employs a double random phase encoding algorithm to encrypt and decrypt video sequences. The video signal is first transferred to RGB model and then separated into three channels: red, green, and blue. Each channel is encrypted by two random phase masks generated from session keys. For higher security, an asymmetric method is applied to cipher session keys. The ciphered keys are then embedded into the encrypted video frame by a content- dependent and low distortion data embedding technique. The key delivery is accomplished by hiding ciphered data into the encrypted video frame with a specific hiding sequence generated by the zero-LSB sorting technique. Experimental results show that the adaptive Steganography has a better performance than the traditional Steganography in the video cryptosystem. [1]

5.3 A Secure Covert Communication Model based on Video Steganography

A Steganography model is which utilizes cover video files to conceal the presence of other sensitive data regardless of its format. The model presented is based on pixel-wise manipulation of colour raw video files to embed the secret data. The secret message is segmented into blocks prior to being embedded in the cover video. These blocks are then embedded in pseudo random locations. The locations are derived from a re-orderings of a mutually agreed upon secret key. Furthermore, the re-ordering is dynamically changed with each video frame to reduce the possibility of statistically identifying the locations of the secret message blocks, even if the original cover video is made available to the interceptor. A quantitative evaluation of the model is using four types of secret data. The model is evaluated in terms of both the average reduction in Peak Signal to Noise Ratio (PSNR) compared to the original cover video; as well as the Mean Square Error (MSE) measured between the original and Steganography files averaged over all video frames. Results show minimal degradation of the Steganography video file for all types of data, and for various sizes of the secret messages. Finally, an estimate of the embedding capacity of a video file is presented based on file format and size. [1]

5.4 Lossless Steganography on AVI File using Swapping Algorithm

A comparative analysis between Joint Picture Expert Group (JPEG) image stego and Audio Video Inter- leaved (AVI) video stego by quality and size was performed. The purpose for this method is to increase the strength of the key by using UTF-32 encoding in the swapping algorithm and lossless stego technique in the AVI file. However, payload capacity is low.

5.5 A New Invertible Data Hiding in Compressed Videos or Images

An adaptive invertible information hiding method for Moving Picture Expert Group (MPEG) video is proposed. Hidden data can be recovered without requiring the destination to have a prior copy of the covert video and the original MPEG video data can be recovered if needed. This technique works in frequency domain only. It has the advantages of low complexity and low visual distortion for covert communication applications. However, it suffers from low payload capacity.

6. Previous Work on Video Steganography

“Amr A. Hanafy, Gouda I. Salama and Yahya Z. Mohasseb” author describes in this paper presents a steganography model which utilizes cover video files to conceal the presence of other sensitive data regardless of its format. [5]

“Mrs.Archana S. Vaidya, Pooja N. More., Rita K. Fegade, MadhuriA.Bhavsar, Pooja V. Raut, R. H. ”author describe in this paper presents a Steganography technic. Unlike the space domain approaches, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform[6].

“ChangyongXu, Zhengzhou,Xijian Ping, Zhengzhou,Tao Zhang”author describe in this paper, a steganographic algorithm in MPEG compressed video stream was proposed. [7]

“S. Suma Christal Mary”author describein this paper propose a new method for thereal-time hiding of information used in compressed videoBitstreams. The method is based on the real-time hiding of information in audio Steganography.[8]

“Poonam V Bodhak, Baisa L Gunjal” author describein this paper designs software to develop a steganographic

application to hide data containing text in a computer video file and to retrieve the hidden information. This can be designed by embedding the text file in a video file in such a way that the video does not lose its functionality using DCT & LSB Modification method. [9]

"P.Paulpandi1, Dr.T.Meyyappan,Karaikud" author describe in this paper, we proposed a new technique using the motion vector, to hide the data in the moving objects.[10]

"Dipesh G. Kamdar1, Dolly Patira, Dr. C. H. Vithalani"author said in order to make faithful and secure communication, a dual layer hiding technique is proposed in this paper.[11]

7. Conclusion

While studying video Steganography it was found that lot of work already done on this technique. Text, Audio, Image, Video can hide inside the video and we can use video as a cover file and also as a secret message but did not get anything done on moving images. So it is proposed that one can work on video file as a cover file and we will try to moving images inside it as a secret message. We may try this with the help of cryptography and video Steganography methodology LSB or DCT.

References

[1] "Amr A. Hanafy, Gouda I. Salama And Yahya Z. Mohasseb The Military Technical College, Cairo, Egypt" A Secure Covert Communication Model Based On Video Steganography.

[2] "Mrs.Archana S. Vaidya, Pooja N. More., Rita K. Fegade., Madhuria. Bhavsar., Pooja V. Raut. Asst. Prof. Department of Computer Engg. GES's R. H. Sapat College of Engineering, Management Studies And Research, Nashik (M.S.), INDIA "Image Steganography Using DWT And Blowfish Algorithms.

[3] "Changyong Xu Department Of Information Science, Zhengzhou Information Science And Technology Institute ,Xijian Ping Department of Information Science, Zhengzhou

[4] Information Science And Technology Institute, ,Tao Zhang National Laboratory Of Pattern Recognition, Institute Of Automation, Chinese Academy Of Sciences, Beijing", Steganography In Compressed Video Stream.

[5] "S. Suma Christal Mary M.E (Ph.D.), Lecturer Department of CSE PSN College of Engg. & Technology Tamilnadu, India "Improved Protection In Video Steganography Used Compressed Video Bit streams.

[6] "Poonam V Bodhak, Baisa L Gunjal" Improved Protection In Video Steganography Using DCT & LSB.

[7] "P.Paulpandi1, Dr. T.Meyyappan , M.Sc., M.Phil., M.BA., Ph.D2 Research Scholar1, Associate Professor2 Department Of Computer Science & Engineering, Alagappa University, Karaikud Tamil Nadu, India."Hiding Messages Using Motion Vector Technique In Video Steganography.

[8] "Dipesh G. Kamdar1, Dolly Patira2, Dr. C. H. Vithalani", Dual Layer Data Hiding Using Cryptography and Steganography.

[9] "Vipula Madhukar Wajgade1, Dr. Suresh Kumar", Enhancing Data Security Using Video Steganography.