Secure Video Transmission

Manveen Kaur
Asst. Professor
Dept. of Computer Science & Engineering
Galgotias College of Engineering and Technology
Greater Noida, India

Anchal Maheshwari
Dept. of Computer Science & Engineering
Galgotias College of Engineering and Technology
Greater Noida, India

Nidhi Anand
Dept. of Computer Science & Engineering
Galgotias College of Engineering and Technology
Greater Noida, India

ABSTRACT

Nowadays, as the technology has developed, methods need to be found out that not only hide the information but also hide the existence of that information. The art of hiding information is known as steganography. Till now many algorithms have been proposed for steganography but they suffer few or more drawbacks. This paper uses F5 algorithm for information hiding. F5 offers huge capacity for steganography. F5 is based on matrix encoding. The proposed system is evaluated on the basis of its ability to hide and retrieve the information correctly. In recent days video steganography is considered as a boon for secure and secret transmission of data. The main aim of this paper is to provide new ways of improving the existing methodologies to hide information. In continuation with this, we start by first describing the previously used algorithms and then enhancing them by describing the use of F5.

General Terms

Digital image processing, Network security, Algorithms.

Keywords

Steganography, Cryptography, F5 algorithm.

1. INTRODUCTION

The word 'Steganography' is derived from two Greek words named 'steganos' and 'graphein'.[9] The word steganos means 'covered' and graphein means 'writing'. Steganography is defined as the art of hiding an information or message inside another file under cover medium.[1]

The literal meaning of steganography is covered writing. This refers to hiding information into another.[2] Steganography is advantageous over cryptography taken alone as the secret message never attains direct attention on itself. Whereas in cryptography, it is known that a secret message is present as there is no concealment of that information. For steganographic transmission, the best considered files are audio or video files due to their size. We can hide both text or audio data inside audio or video files. In steganography the unused bits are replaced from the original video or audio to perform hiding activities on the required information. Steganography can be applied on image, audio or video file.[8]

The algorithms used for steganography are responsible for hiding confidential data in carrier file, here it is media. The hidden message should not come in notice of the attacker. Hiding of carrier video into host video based on non uniform rectangular partition is done by ShengDun Hu.[10] The message is scattered more uniformly in comparison to parity block schemes and key-driven distance schemes. Another advantage of F5 is that it does not depend on the length of message.

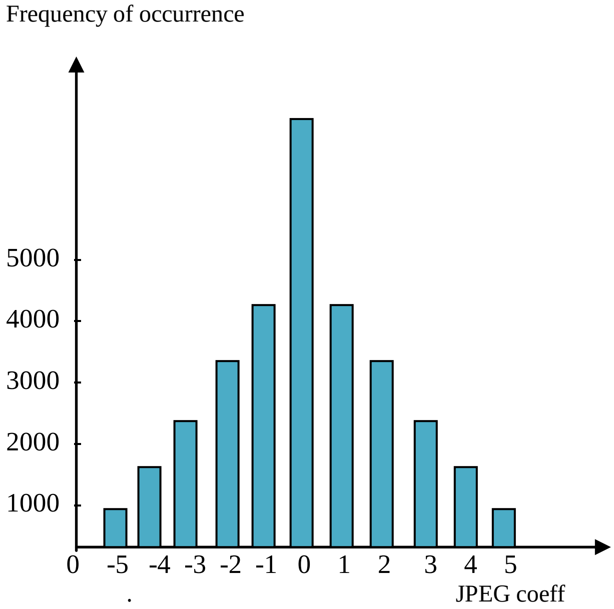

Fig 1: Histogram

The above figure shows high efficiency and capacity of F5 algorithm of steganography. It also shows that it is resistant against attacks. Also, the carrier medium used is JPEG. For maximum embedded message (size is 16KB), the efficiency is 1.5 bits whereas for short message (size is 0.2KB), it is 3.7 bits. Capacity, Security and robustness are the aspects of information hiding.[3]

Characteristics of steganography-

- The data is transmitted such that only receiver can read it.
- Steganography requires cover objects for its implementation.
- It is robust but time consuming.

Methods of steganography- There are three methods used for steganography namely Pure, Secret Key and Public Key steganography. In pure steganography, the data is embedded without using any private key. In secret key steganography, individual key is used for embedding. In public key steganography, there are two keys that has to be used- one for encryption and another for decryption.

2. RELATED WORK

To give more description about the implementation, this section shows some other works.

Initially TEA (Tiny Encryption Algorithm) was used for Video Steganography. It maximizes the speed of the algorithm and consumes less time. But it increases the size of the output file after embedding. In this, the round function uses addition modulo 2^{32} instead of X-OR.[4]The Tiny Encryption Algorithm uses algebraic operations. There is a 128 bit key.

There are four 32 bit blocks in which this 128 bit key is splitted. The sender enters the plain text in block cipher form and round function is applied to change it into cipher text. The function is split into two halves and they are swapped at each step. This has to be done till 64 rounds. Since this is a very lengthy process, the size of output file becomes very large.

To overcome the drawbacks of Tiny Encryption Algorithm, authors went for a new algorithm which is F5. Unlike videos, images provide very limited capacity. Thus most of the part of file is not used. In order to prevent attacks the embedding density should be same.

2.1 Permutative Straddling

For straddling to be easy, the carrier capacity should be known exactly. The well known algorithms used in steganography cover the entire medium for transmission of message. Thus they get slower. In F5, permutation is applied and all coefficients are shuffled using straddling. Then the data is embedded in the sequence. A password is there that decides the permutation by providing a key. The coefficients are delivered to the Huffman coder in original sequence by operating F5 on it.

2.2 Matrix Encoding

Matrix Encoding was introduced by Ron Crandall. This was a new technique for the enhancement in the efficiency of embedding. And F5 algorithm is its first implementation. By using matrix encoding, the number of changes could be decreased if the capacity of the steganogram is not used. Suppose there is a message which is uniformly distributed and also has values that are uniform at the point of changing. If half of the message changes and the other does not than in the absence of matrix encoding, efficiency is two bits per change.

If there is a message of 217 bytes then using matrix encoding causes 459 changes that is efficiency of 3.8 bits per change.

3. DESIGN AND IMPLEMENTATION

The detailed description of working of F5 could be explain by the help of an example. Suppose there are two bits y1, y2 that need to be embed in new bit places c1, c2, c3 changing one place at most. The four cases that could be observed are:

$y1=c1 \oplus c3, y2=c2 \oplus c3$ => No Change

$y1\neq c1 \oplus c3, y2=c2 \oplus c3$ => Change c1

$y1=c1 \oplus c3, y2\neq c2 \oplus c3$ => Change c2

$y1\neq c1 \oplus c3, y2\neq c2 \oplus c3$ => Change c3

The structure of F5 algorithm is as follows:

- Compression of JPEG and halt after quantization.
- A random number is to be initialized from the password by the help of key.
- Start permutation.
- Find k from the capacity of medium and hidden message length.
- Determine word length $n=2^k-1$.
- Apply (1,n,k) matrix encoding to embed the message.

(a) Create a buffer comprising of n coefficients that are not zero

(b) Hash buffer

(c) Sum the next k bits to the above generated value

(d) If sum=0 implies buffer unchanged else sum=buffer's index 1…..n

(e) Test for occurrence of zero. If zero comes, eliminate it by another coefficient, if not check for new coefficients in the buffer.

- Continue compression.

The technique of steganography that is to be used lies under that of secret key. Here a key is required for the retrieval of hidden message.

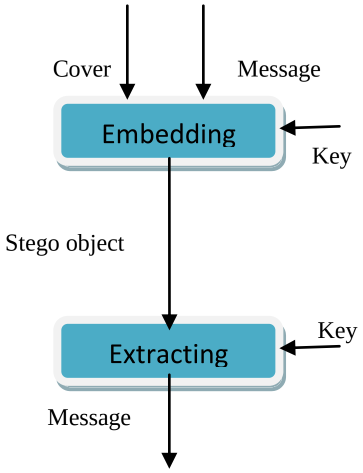

Fig 2: Secret Key Steganography

4. WORK FLOW

Secure Video Transmission mainly comprise of four basic modules namely encryption, hiding of message, retrieval of hidden message and then its decryption.

Encryption: It involves converting plain text of the message to be hidden into a cipher text to provide security. Secret key can be used for encryption.

Hiding of message: The pixels are divided into as per their intensities into red, green and blue respectively.

Retrieving the message: The output file is different from the one where the hiding of messages is performed. This output file comprises of the message that has to be retrieved.

Decryption: It means converting the cipher text into decrypted format. It is also done by passing a secret key.

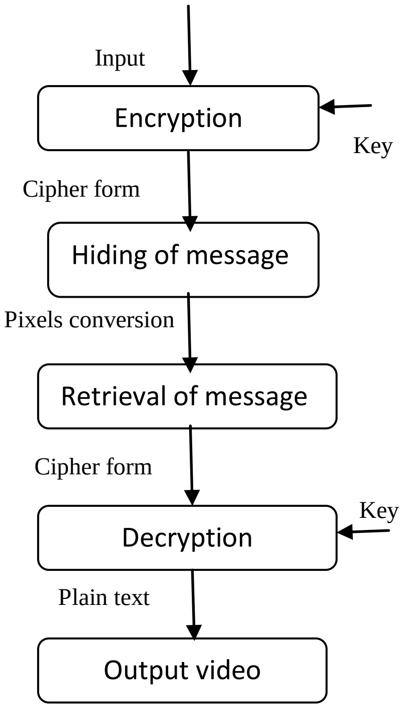

Fig 3: Workflow

5. CONCLUSION

The combination of many still images one after the another arranged in a sequence is termed as a Video. A novel steganography technique that enhances security and preserves the integrity of the sent message is achieved by the usage of algorithm named F5. The main advantage of using F5 algorithm is that the size of the output file is comparatively smaller than the other steganographic algorithms. F5 is a high capacity algorithm that intends to hide one video inside another video. There is no visual distortion by the usage of F5 in the actual videos. The output video comprising of embed message is also of fine quality that has practical acceptance in the outside world. Also it is more secure and beneficial algorithms as compared to previously proposed algorithms in previous time

JPEG is the only available medium on which compression is performed and it is also publicly available. The capacity of steganography increase is also possible. Also resistancy and efficiency is also maintained.

The future work corresponding to this study can be mentioned in a way as this research paper could provide us with more security for more secure transmission. Since the steganography capacity is high in this technique so are the chances of attack possible. The embedding of message using matrix embedding is very complex thus the system may become slow. More historical notes can be referred[5] for exchanging hidden messages. More detailed information can be found in[6,7].

6. REFERENCES

[1] Ross J. Anderson and Fabien A.P. Petit colas, “On the limits of steganography,” IEEE Journal on Selected Areas in Communications(J-SAC), Special Issue on Copyright & Privacy Protection, vol. 16 no.4, pp 474-481, May 1998.

[2] T Mrkel,JHP Eloff and MS Olivier. “An Overview Of Image Steganography,” in Proceedings of the fifth annual Information Security South Africa Conference, 2005.

[3] B. Chen and G.W.Wornell. Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding. In *IEEE Trans. Information Theory*, volume 47, no. 4, pages 1423–1443, 2001.

[4] Johnson N. and Jajodia S., “Steganography: Seeing the Unseen,” IEEE Computer Magazine, vol. 25 , no. 4, pp. 26-34,1998.

[5] Simon Singh. The code book. In *Fourth Estate, London*, 1999.

[6] Bruce Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C. In *Wiley, 2nd Edition*, 1994.

[7] Wenbo Mao. Modern cryptography: Theory and practice. *Prentic Hall, 1st edition*, 2003.

[8] C. Xu, X. Ping, and T. Zhang. Steganography in compressed video stream. In Innovative Computing, Information and Control, 2006. ICICIC’06. First International Conference on, volume 1, pages 269–272. IEEE, 2006.

[9] N. Johnson. Steganography, George Mason University. Information System and Software Engineering, www. jjtc. com/stegdoc/steg1995. html, 1995.

[10] ShengDun Hu,“Novel Video Steganography based on Non-uniform Rectangular Partition” Proceedings of International Conference on Computational Science and Engineering, pp.57-61, 2011.