Shielded Data Sneaking in Video (Steganography) using TEA

Assoc. Prof. Emad S. Othman
Senior Member IEEE - Region 8, Higher Institute for
Computers and Information Systems, AL-Shorouk Academy,
Cairo – Egypt, PH- 0020-010-25830256. E-mail: dr.emad.othman@sha.edu.eg

Abstract- Video steganography is becoming an important research area in various data hiding technologies, which has become a promising tool because not only the security requirement of secret message transmission is becoming stricter but also video is more favoured. This paper presents a solution by using cryptography to protect sensitive information. The message is encrypted using custom algorithm and the TEA (Tiny Encryption Algorithm) to make it even more secure. Then, the encrypted message is hidden within a video using steganography.

Steganography is a method of hiding information in a way that it appears to be just a normal file or data. This makes the transfer of sensitive information secure, as only the sender and the recipient know about the hidden message.

Overall, this paper offers a promising solution for protecting sensitive information by using cryptography and steganography as two stratums.

Keywords: cryptography, steganography, and Security Assessment Algorithm.

1. Introduction

Video steganography is a branch of data hiding, which is a technique that embeds message into cover contents and is used in many fields such as medical systems, law enforcement, copyright protection and access control, etc. [1]. Since human visual system are less sensitive to the small changes of digital medias, especially for digital video, video steganography is a technique which hides message into a video and conceals the fact of the transmission. And it has become more popular recently because of two main reasons: Along with the fast development of computer applications, the security problem in information field is becoming more and more serious. Video is an electronic medium which can be more eligible than other multimedia because of the booming of powerful sharing/transmission tools of digital video contents and its size.

The main goal of video steganography is to conceal the secret message into the digital video, so the visual quality of the embedded video would be changed ranging from a slight distortion to a severe distortion.

2. Methodology

Three main important factors should be considered in the presented steganography system: imperceptibility, robustness and embedding capacity.

a) Imperceptibility is closely related to the safety of steganography methods concealing the secret message into the embedded video. The high imperceptibility means a low modification rate and good visual quality of the embedded video. And the steganography algorithm that contains a high imperceptibility will reduce attacker suspicion of finding hidden message and will be quite difficult to detect by steganalysis tools, and any distortion to the cover data after the embedding process occurs will increase the attention of attackers. In video steganography, imperceptibility is the perceptual similarity between the original and embedding video, and evaluated as a visual distortion caused by embedding modifications. To improve the imperceptibility, many video steganography methods have used lots of methods such as quantization transform coefficients predictions modes and motion vectors, etc. to enhance the performance of imperceptibility.

b) Robustness is the second prerequisite which measures the steganography method's strength against attacks in video steganography. The reason of the consideration of robustness is that the embedded message sometimes cannot survive from various intentional or unintentional attacks, such as network transmission, packet loss, video clipping and scaling operations. The algorithm is robust when the receiver can extract

the secret message correctly without any errors. To improve the evaluation precisely, the survival rate is that all the embedded bits are divided by the embedded bits retrieved without error is used to measure robustness [2].

c) Embedding capacity is the third fundamental prerequisite and is defined as the sum of secret message that can be embedded into the digital video. The higher embedding capacity means the more secret message can be embedded. However, higher embedding capacity could lead to the higher risk for the decrease of visual quality and increment of bit-rate for the embedded video. In traditional steganography methods, embedding capacity and imperceptibility of embedded video are inter conditioned, and the imperceptibility is affected by embedding capacity. So the imperceptibility of video steganography should be taken into account when the method has higher embedding capacity. During the evaluation of steganography methods, the imperceptibility should be considered prior to embedding capacity because we can get the embedding video that the message needed because of the infinite video sequences [3].

There is an exchange-off in the imperceptibility, robustness and embedding capacity. In the video steganography method, if either the robustness or embedding capacity increases, the imperceptibility will reduce.

3. System Design and Implementation

In today's digital world, it's crucial to keep information secure, and it became one of the most valuable assets for individuals and organizations. From personal data to financial records and intellectual property, the amount of sensitive information that is stored and shared online is constantly increasing. However, this convenience also comes with a risk the potential for unauthorized access to confidential information. It is crucial to protect this information. Video Steganography an application that works on the desktop that encrypt information and hide it in video to make it more secure.

Use cryptography science to encrypt information by custom algorithm and Tiny Encryption Algorithm (TEA) as shown in Figure 1 to protect the information. Hiding the encrypted information within a video using steganography LSB1 (Least Significant Bit) technique. Added more security by making it difficult for unwanted parties to access the information. The existence of the hidden information is not easily detected. The combination of cryptography and steganography provides a powerful solution for secure information transfer.

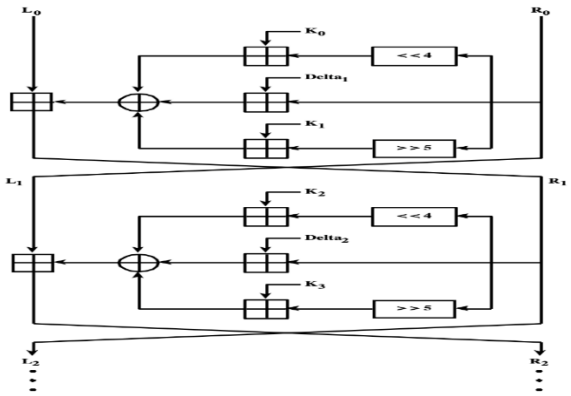

Figure 1: Tiny Encryption Algorithm (TEA)

Use cryptography science to encrypt information by custom algorithm and Tiny Encryption Algorithm (TEA) to protect the information [4].

The purpose of using the TEA algorithm because it has several advantages that make it a great choice for us as undergraduate students. TEA is easy to understand and implement, which is helpful for us as we're still learning about encryption. Additionally, TEA is effective in terms of security and has proven to be resistant to attacks. It provides a good level of protection for our data and is not easily broken by unauthorized individuals. So, overall, TEA offers a combination of simplicity, effectiveness, and strong security, making it a suitable choice for our needs.

Hiding the encrypted information within a video using steganography LSB1 (Least Significant Bit) technique as shown in Figure 2. The video format is MP4 work on any size with high resolution.
If the message to be hidden is very large compared to the video in question, we can divide the message into parts and hide each part in different videos. This way,

we can spread the message across multiple videos to fit its size. Another option is to use the LSB2 technique. Instead of changing just the last bit of each pixel, we can change the Least two bits. This allows us to hide more information in each pixel and accommodate larger messages.

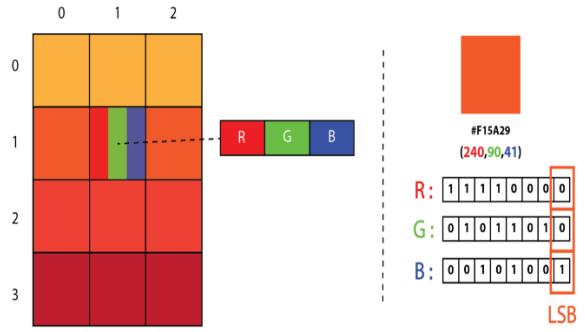

Figure 2 Least Significant Bit

4. CONCLUSION and Future Developments

Protecting important information and hide it from unwanted parties. Using cryptography and steganography to protect data from unwanted party. Send information and messages in a safe and hidden manner by decrypting and hiding the information in video. Decrypt the encrypted messages and turn them into the original message that can be understood. By presenting the results, we aim to make it clear and easy for everyone to understand the outcomes of our paper and see why our approaches are effective.

Most modern security standards and security applications are defined to be algorithm independent; that is, they allow a choice from a set of cryptographic algorithms for the same function. Field Programmable Gates Array (FPGA) are reconfigurable hardware devices. They can switch algorithms on-the-fly. Thus, cryptographic algorithms, which are implemented on FPGAs, provide an ideal match for algorithm independent security applications. On FPGAs, cryptographic algorithms can run much faster than on software applied to improve the high speed in networking protocols (LAN & WAN), and other domains. Consequently, the Integrated KBSA could be implemented into a single hardware chip like FPGA and the encryption and decryption processing will be faster and robust but unfortunately costly.

With the rapidly changing world, Steganography is continuously improving and being utilized. With increasing attention being given to its many uses, Steganography poses a valid security threat. The internet is providing a new outlet for hiding messages. Development in the area of covert communications and Steganography is predicted to continue to grow through the coming years. Steganography today is just the "ice cap" of what Steganography will be in the future.

REFERENCES

1. https://larsenclose.com/recounting-recent-tiny-encryption-algorithm/
2. https://www.ic.unicamp.br/~rdahab/cursos/mo421mc889/Welcome_files/Stinson-Paterson_CryptographyTheoryAndPracticeCRC%20Press%20%282019%29.pdf
3. https://eclass.uniwa.gr/modules/document/file.php/CSCYB105/Reading%20Material/%5BJonathan_Katz%2C_Yehuda_Lindell%5D_Introduction_to_Mo%282nd%29.pdf
4. https://www.researchgate.net/publication/45949372_SteganographyThe_Art_of_Hiding_Data.