EasyChair Preprint

№ 4722

Multi-level Data Security Using Video Steganography

Malaz Rabeea

December 9, 2020

Multi-level Data Security Using Video Steganography

Malaz Rabea Abdallah Adam

Department of Computer Science,

Karary University

Omdurman, Sudan

Email:

Faisal Mohammed Abdallah Ali

Department of Computer Science,

Karary University

Omdurman, Sudan

This study introduces multi-level concealment of information, which describes a new paradigm for covert communication in covert communication technology. The masking algorithm was used more than once in which an encrypted message was hidden inside a vector medium (image) and the transporter was hidden inside another medium (video) by using two masking functions in the first level. The LSB function in the second level was used as the DCT function. The proposed method has several benefits in stealth communications. Including increasing the level of security during the transmission of confidential information through public channels or the Internet, and has also been used to increase reliability. The performance of the proposed algorithm is measured in terms of capacity and security through different experiments using two PNSR and MSR functions.

Keywords- Steganography, Least significant bit, RC4, hidden frames, Matlab, DCT function.

I. INTRODUCTION

With the development of means of communication computer science and electronic revolution I find that we have become in an electronic village unit connects the world with each other became all communication methods such as telephone communications, social media, websites and other components of the network , collected clear and visible to all anonymous users and you must be secured These methods in order to transfer information safely and reliably from the source and validity in this study we will deal with a small part in the insurance is the task of securing the message before sending, using more than an algorithm in the insurance to increase security and complexity to assure the safety A failure in an attempt to break.

"Steganography" originates from "Greek". The word stego implies cover and grafia implies writing which signifies Covered writing" [3]. Steganography aims at hiding the existence of the authentic communication. Steganography has developed into one of the most robust and efficient methods to send secret or sensitive data to another party without the knowledge of any interceptor. In steganography, the sender uses usual file like video, image, audio and text known as cover file which would appear to be of no importance to any interceptor. Video Steganography is defined as the art and science of embedding secret data into videos. A video file is a set of frames (still-images) [4]. Some techniques hide data in the individual frames of the video which is known as video steganography as the extension of image steganography.

Video Steganography as a video container file has numerous advantages not exhibited by other container formats; video steganography is now a growing area of research. Video Steganography is a technique to hide any kind of files into a video file. The Alteration in the video file is significantly more difficult to detect by the human visual system, as frames are displayed on screen in an extremely faster rate. Furthermore, since video frames are not sharply focused images or crisp, variations in pixel color induced by steganography will blend

into the frame very easily. Use of the video based steganography can be more eligible than other multimedia files, because of its size and memory requirements. The video has 2 components and they are an audio stream and a picture stream. Therefore, most of the existing techniques on images and audio can be applied to video files too. Similar limitations as any other kind of steganography: You need to have "free" space in the carrier media. This means usually deleting part of the data that is invisible such as the alpha channel in a picture and replacing it with the hidden data. Sometimes it is only possible to compress this "useless" data, not delete it.

In this study, both video components were used

In a highly compressed video it might be close to impossible to embed additional, hidden information. As steganography on itself is easy to detect, the embedded data has to be encrypted, reducing the information content roughly by half. Encrypted data looks like random noise; a statistical analysis program will not be able to detect it.

In an uncompressed image, the maximum amount of embeddable information is usually at most 30%. In practice however it will be in the single digit range.

II. RELATED WORKKS

Kamred Udham Singh[1].The video is divided into frames and the histogram value of each frame is calculated. These values are compared with threshold value. Based on this, secret data is hidden into the frames by dividing each pixel in two parts, the number of bits embedded in the right part are counted in the left part. This algorithm provides ability to hide large amount of data and extraction of written text without errors.

Using improved LSB (Least significant bit) method the secret image is hidden in the cover image.[2]. BITMAP images are used as they are lossless. Then by using bit plane slicing the cover image is divided into three planes namely Red, Green and Blue. Then, the bits of the secret data are replaced by least significant bits Red, Green and Blue in the order 2, 2 and 4 i.e., 2 bits in Red, 2 bits in Green and 4 bits in Blue. More data hiding is provided.

M. Mennatallah. Sadek,ect …[3]. The cover video is divided into frames and the secret data is extracted from the cover video. The complexity and security is increased by embedding the data in multiple frames of the video. The frames of the video are divided and are converted as .bmp images. The pixel values of the cover video are converted to binary values and the secret data is also converted into binary values. Then the bits of secret data are replaced by the order 2, 3, 3 into Red, Green and Blue respectively, 2 Least Significant Bits of Red, 3 Least Significant Bits of Green and 3 Least Significant Bits of Blue.

DeepaliSinglaand etc.… [4]. they used a sequence of nine uncompressed video sequence as cover data. The secret message was a binary image. First the pixel position of both cover video and a secret image was reordered using a private key. Even the secret message was encoded using Hamming code (7, 4) to make the message more secure before embedding.

"Sim hiewmoi" [5], this paper presents an approach to generate a unique and more secure cryptographic key from iris template. The iris images are processed to produce iris template or code to be utilized for the encryption and decryption tasks. AES 12 Journal of Embedded Systems cryptography algorithm is employed to encrypt and decrypt the identity data.

Sujay narayana1and gauravprasad" [6] This paper give information about Cryptography & Steganography, this paper introduces two new methods wherein cryptography and Steganography are combined to encrypt the data as well as to hide the encrypted data in another medium so the fact that a message being sent is concealed [6].

III. PROPOSED SYSTEM

The other hand there is the so-called TYPE-I approach, a message is hidden in a cover object and that stego-cover object is hidden in another cover object, and so on. This approach increases the level of security of the system. Again, the number of levels is used during the embedding process in multilevel steganography is very important information at the receiving end. That means, security may be increased by varying the number of levels during embedding process. Along with this, any of the encryption algorithms may be used at a transformation phase of the system to increase the security of the system.

IV. OVERVIEW

The aims of this study proposing a data hiding and extraction procedure to embed secret message bits in videos. The secret information taken here is gray scale image pixel values. These pixel values are converted into binary and embedded into bits of images in a video frame, by increasing security due to use random data are also placed in unused frames in the video, the attacker is left clueless to know the real secret data hidden in the video. Hence highly confidential data like military secrets and bank account details can be easily steganography in ordinary video and can be transmitted over internet even in unsecured connection.

The ability to Capacity Text based steganography has limited capacity and Image steganography tried to improve the capacity where 50% of original image size can be used to hide the secret message. But there is limitation on how much information can be hidden into an image. Video Steganography has been found to overcome this problem. That will increase the reliability.

A. Methodology Scenario

To implement video Steganography in Matlab for hiding secret message in a carrier image in the cover frames of a carrier video using LSB (Least Significant Bit) and DCT modification technique and retrieving the hidden image from the video at the receiver end.
The full purpose of hiding information is to ensure that the message is hidden. So if the container media is too broken (loud sound / image) it might reveal the message.
You can use any method of distortion rate technology, but for hiding information, it is necessary to determine the tolerance for the image / sound allowed before concealing

- Encrypt text using RC4.
- Hide encoded text inside an image and measure the quality of the image after the disappearance.
- Read a video and convert it into frames.
- Split and hide the loaded image into video frames and measure the image quality after hiding.
- Hide text (key) inside a sound and measure the sound quality after the disappearance
- Create a video with hidden pictures and hidden sound in it.
- Read the videos Steganography.
- Read the audio file and extract the text to find out which key is used for hiding operations.
- Select hidden frames with the key.
- After the image is retrieved, the encrypted text is retrieved

B. The three level of encryption

1) level 1

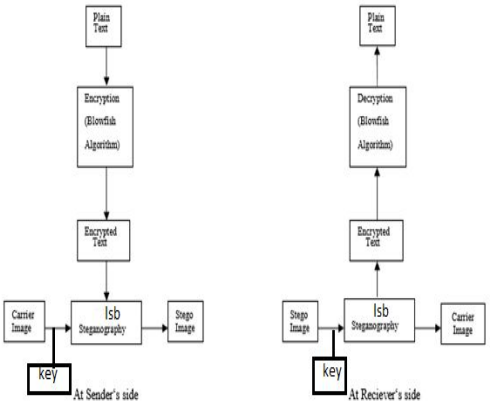

Fig.1. The basic block diagram of level 1 encrypted text and hiding.

In order to increase security, two information security sections were used: (encryption and hide) as previously mentioned, at the first level the message is determined by the user or the programmer and then the message is encrypted using the algorithm of RC4, Then select the carrier image so that the encoded text is hiding inside it using an algorithm LSB. Using the second model of hide, this is concealing with a key, the standardization of the key in encryption and hide.

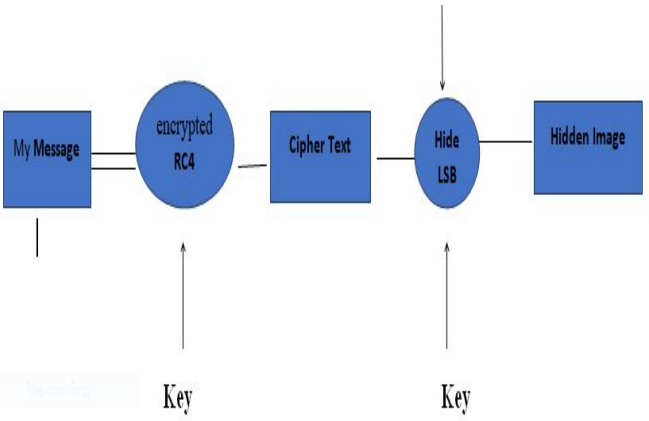

Fig.2. encrypted using the algorithm of RC4 hide the chipper text LSB

2) level 2

In the second level, the video is specified with an extension of pm4, and then the video is converted and divided into two parts. The first is the frames and the second is the extracted sound, and then 8 frames are randomly selected using the same previous key. The process of hiding the image to the encrypted text is divided between the eight frames chosen using the DCT algorithm.

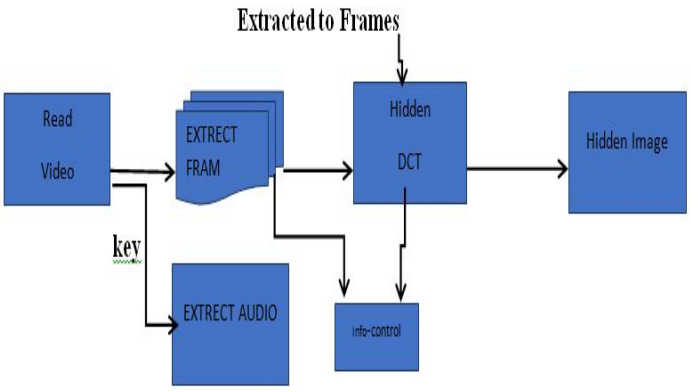

Fig.3. Extract frames from video and hide cover image

3) level 3

In the third level of concealment, the second part of the video data is used, which is the sound, in which the key used in both the encryption and concealment process is hidden and the key is placed in the form of text with an extension. txt is then hidden in the audio file using the optimized LSB algorithm by specifying the first bit to hide and setting the jump level between bytes. Then merge the brain image steganography file and audio steganography file to create a sent video steganography.

Then the first image containing control information is selected for the purpose of Authentication and verification that the video has not been modified by adding clear information about the video from the length, size, number of frames and sound time.... etc., all of this information is included in the form of a text file and hidden using DCT The recipient is notified in advance.

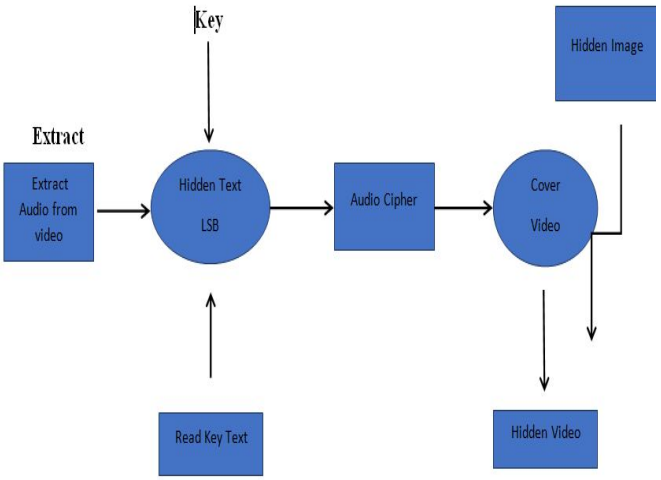

Fig.3. Extract audio and hide text in audio and create video

V. CONCLUSION AND FUTURE WORKS

In conclusion, the objectives of the study were achieved through research and obtaining the highest high quality. In an attempt to achieve the aims of the study, it shows the weaknesses of this methodology followed and decorated, attributed to me the acceleration of the discovery of new and modern technologies that define and destroy every attempt at high insurance, not absolute insurance, which does not exist .This study was disturbed by focusing on some weaknesses of the two masking algorithms: dct, lsb, and dct. An important weakness point is striking and revealing to me. The masking in the video is changing the color of the image or the frame to gray, and this means that the video that is hidden using DCT By using dct when analyzing its tires, the evidence of these frames will be interesting, and this bite has been addressed in the study, as well as improved by the lsb algorithm, by concealing it randomly, irregularly, according to the key used, in addition to that. On the image level, for me, the masking at the sound level was used for lsb, and the masking is determined by the bit number to hide and the jump rate is with a fixed value agreed upon by both the sender and the recipient. This is what the study covered, we ask God Almighty to benefit others. But in particular the following facilities can be added:

- The compression algorithm can be used in the future to reduce the size of hidden data to hide the largest

number of data and reduce interference in the case of large capacity data use.

- The method used in the LSB algorithm used can be modified and replaced with another technology, for example (2 LSB, 3LSB(.
- Try to discover and cover the spots in the algorithm by putting yourself in the third party's place and seeing the weak points and making them stronger.
- An attempt to use encryption is permissible to use encrypted text for confidentiality and making discovery difficult.
- Broader and more comprehensive measurement functions can be used to make sure noise is more accurate and clear.
- An attempt to improve the look of the search by using user interfaces via Matlab (GUI).
- The number of levels can be increased, it can be reduced and other algorithms such as dwt ...
- Compressing the video file obtained by the stream of images with modified cover frames lossless so as to increase the speed of transmission.
- Implement other higher order security measures so as to protect messages from steganalysis, cryptanalysis and various other types of sophisticated attacks.

REFERENCES

[1] KamredUdhamSingh ,"An algorithm based on color histogram was proposed for video steganography",Singh Int. Journal of Engineering Research and Applications , Vol. 4, Issue 5(Version 1), May 2014, pp.105-108 ,

[2] M.MaryShanthi Rani, G. Germine Mary and K. Rosemary Euphrasia, "Using improved LSB (Least significant bit) method the secret image is hidden in the cover image ", International Journal of Innovations &Advancement in Computer Science IJIACS - ISSN 2347 – 8616 Vol.4, Special Issue September 2015.

[3] Mennatallah. Sadek, Amal S. Khalifa Mostafa and G. M. Mostafa "Using LSB technique the secret data is embedded in the cover video", Springer Multimed Tools Applications, Vol.76, Issue.2, pp.3065-3085, 2017.

[4] DeepaliSingla and MamtaJuneja, "An algorithm was proposed based on the principle of linear block code", 2014 Recent Advances in Engineering and Computational Sciences (RAECS), Chandigarh,India, pp.1-5 March, 2014.

[5] Sim hiewmoi, nazeemabintiabdulrahim,putehsaad, pang li sim, zalmiyahzakaria, subariahibrahim, "iris biometric cryptography for identity document", 2009 international conference of soft .

[6] Sujay narayana1and gauravprasad" Image Steganography Using Cryptographic Techniques and Type Conversions" signal & image processing: an international.

[7] Mamtajuneja 1, parvindersingh sandhu2 "A New Image Steganography Technique" 2009 international conference on advances in recent technologies in communication and computing.

[8] B. Schneier, applied cryptography, john wiley& sons, new york,

[9] "Video Steganography implemented by changing the least significant bit of the visual file bite stream into a message file"2015.

[10] A. J. Al-Najjar, The decoy: multi-level digital multimedia steganography model, International Conference on Mathematics and Computers in Science and Engineering, pp.445–450. World Scientific and Engineering Academy and Society, USA, 2008.

[11] W. Frkaczek, W. Mazurczyk, and. Szczypiorski, Multi-level steganography: Improving hidden communication in networks, Journal of Universal Computer Science (J. UCS), vol.18, no.14, pp.1967–1986, 2012.

[12] [11] Samir extended, Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol.1, no.2, pp.71–74, 2012.