CASE STUDY OF HIDING A TEXT USING VIDEO STEGANOGRAPHY

Er. Gursukhmani
Computer Science Engineering
University Institute of Engineering & Technology
Chandigarh University, India
gursukhmanikaur.1328@gmail.com

Er. Sugandha Sharma
Computer Science Engineering
University College of Engineering & Technology
Chandigarh University, India
Sugandha.ss1@gmail.com

***Abstract*— The internet plays a key role in transferring information or data from one organization to another organization. But anyone can modify and misuse the valuable information through hacking at the time. Steganography plays a very important role in hiding the secret data or information inside the digitally covered information. The hidden message can be text, image, speech or even video .Steganography is a type of cryptography in which the secret message is hidden in a digital picture but here the message, as well as the fact that a secret communication is taking place, is hidden. The hided data can embedded in a video file and it can be extracted in a proper way. In this review paper hiding a Text in Image Using S-Tool has been described.**

Keywords*— *Video Steganography, Cryptography, S – Tool

I. INTRODUCTION

The pointed edge of expert technology and the Internet have made a milestone in the existence of data communication. Communication is the vital spark of any organization and is one of the most important needs of human beings. The concept of secret communication is as old as communication itself. Data security means to protect a database from harmful forces and the discarded actions of unauthorized users. Steganography is the art or exercise of concealing a file, image, or message within another a file, image, or message. The word steganography is of Greek origin and means "covered writing" or "concealed writing". Steganography is ever-changing the digital media in such a way that only the sender and the intended receiver are able to reveal the sent message through it. On the other side steganoalysis is the science of detecting or finding hidden message. Steganography is defined as the hiding of an information within another source so that the presence of the hidden message remains are very much effective as they can carry a large amount of data and can keep that data which not easily be noticed. Steganography conceals actuality of message in some another medium such as text, audio, image, video.

Characteristics of Steganography

Steganography techniques embed a message inside a cover. Various features characterized the strength and weakness of the method. And the following characteristics are:

1. Capacity

The idea of scope in data hiding depicts the whole amount of bits, which masked and effectively rediscovered by the Stego scheme.

2. Robustness

Robustness refers to the ability of the embedded data to remain in one piece if the stego-system undergoes complete change, such as linear and non-linear filtering; adding of random noise; and scaling, rotation, and loose compression.

3. Undetectable

The embedding algorithm is untraceable if the image with the planted message is logical with a model of the source from which images are drawn.

4. Invisibility

The thought is based on the properties of the Human Visual System (HVS) or the Human Audio System (HAS). The planted data is invisible if an average of human subject is unable to figure out between carriers that do contain hidden data and those do not. It is necessary that the planted occurs without a noteworthy degradation or loss of noncognitive high quality of the cover.

5. Security

The embedded process is secure if the embedded information is not point to eliminate after being exposed by the attacker and it depends on the total data about the embedded algorithm and secret key.

Comparison Between Cryptography And Steganography

Cryptography is the study of hiding information, while Steganography deals with manufacturing hidden messages so that only the sender and the receiver know that the message still exists. In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is seeable to the world.

Look alike to this Steganography discard the nonessential/unauthorized interest coming towards the hidden message. A cryptographic mode tries to look after the content of a message/text, while Steganography uses other methods that would hide jointly the message as well as the content. By bringing together Steganography and Cryptography one can bringing out superior security.

Comparison between Cryptography & Steganography		
	Cryptography	**Steganography**
Objectives	Keeping the content of the message secret.	Keeping the existence of the message secret.
Applications	Used for information security.	Used for information security.
Security services	Confidentiality Integrity Non-repudiations Authentication	Confidentiality Authentication
Concealment	Only the secret message is hidden.	The message, as well as the fact that a secret communication is taking place, is hidden.

Table 1. Comparison between Cryptography & Steganography

The rest the paper is organized as follows: In section II, Literature review has been described. In section III, Block diagram of Steganography has been explained. In section IV, Hiding a Text in Image Using S-Tool has been described. V, Conclusion & Future has been described.

II. LITERATURE REVIEW

Kolakalur, et al. [2016] In this paper, the set of rules point by pint with the goal to hide a "secret" color video sequence within another color video cycle with the help of wavelet transform in order to splitting up the cover video series and then substitute the less perceptible wavelet band with "secret" video frames has been implemented and verified. On the receiver side, to recover the hidden color video from stego color video the procedure is turned back. Planned algorithm has been implemented using MATLAB and PSNR and MSE error parameters are used to calculate the quality of both video sequences.

Mustafa, et al. [2015] In view its considered a novel video steganography algorithm based on the KLT tracking algorithm and BCH codes in the wavelet domain. The proposed algorithm encompasses four distinct steps. First, in the encryption process the secret message is preprocessed, and secret message is encoded by applying BCH codes (n, k, t). Second, to identify the facial regions of interest, face detection and face tracking algorithms are applied on the cover videos. Third, In the Embedding process embeds the encoded secret message into the high and middle frequency wavelet coefficients of all facial regions are achieved. Forth, In the extraction process, extracting the secret message from the high and middle frequency wavelet coefficients for each RGB components of all facial regions is accomplished. Experimental results of the proposed video steganography algorithm have demonstrated a more embedding efficiency and a more embedding payload.

Vidhya, et al. [2015] In this paper, it regularly focused on Linguistic steganography. This paper proposed a new stenographic process with an Indian local language, Malayalam. The proposed way is based on custom Unicode technique with embedding based on indexing, i.e. firstly the original message is encoded to Malayalam text with custom UNICODE values produced for the Malayalam text. The comparison of the proposed method against an existing method depicts that, the proposed steganography methods is greater part exact in the encoding as well as in decoding process.

Mstafa,et al. [2015] In this paper, the co-write suggest an efficient video steganography algorithm based on the binary BCH codes to rise up the security and efficiency. With the help of private key, first the pixels positions of the video frames components are arbitrary permuted. Furthermore, the bits positions of the secret message are also permuted by using the same private key. The secret message is encoded by applying BCH codes (n, k, t), and XORed with random numbers before the embedding process. The preferred embedding area in each Y, U, and V frame components is randomly chosen, and will vary from frame to frame. After that the embedding process is accomplished by hiding each of the encoded blocks into the 3-2-2 least significant bit (LSB) of the YUV pixels that was selected. Experimental results indicates that the proposed algorithm have a high embedding efficiency, high embedding payload, and resistant against hackers.

Satpute, et al. [2015] developed a system to embed any kind of file in another file, which is called carrier file or carrier media. The carrier media must be a video file for video steganography. Along with steganography author use Cryptography to make the files more secure. This technique is used for secure transferring of data. In Cryptography the data is

encrypted into unreadable form and is hidden but more securely. Without any modification required in the host signal range while hiding data the algorithm that is used is called Forbidden Zone Data Hiding algorithm .The secret data should not be extremely degraded and should be as imperceptible as possible. The embedded data should be as unaffected to modifications from attacks.

Jenifer, et al. [2014] In this paper a method for hiding of information on the poster or advertising board is presented. It is generally known that encryption give secure channels for communicating entities. Here, an author proposes a new form of steganography, on-line hiding of information on the output screens of the instrument. This method can be used for notify a secret message in public place. It can be extended to other means such as electronic billboard around sports stadium, railway station or airport. This steganographic method is very close to image steganography and video steganography. Here, symmetric key steganography technique and LSB technique is used for hiding the secret information for Private marking system.

Dasgupta, et al. [2013] In this paper, the author proposes a novel video steganography technique for efficient and effective information hiding. Today, video is considered to be an effective and important tool for communication. Video steganography uses video that act as a container for embedding secret information. In this paper, A 3-3-2 LSB based scheme has been used as a base technique for video steganography. To decide the goodness of any steganographic scheme two key parameters i.e. Imperceptibility and video quality is used. Thus the base technique is raised or increased using Genetic Algorithm (GA) which succeeds to get best imperceptibility of hidden information. An anti-steganalysis test is used to check for the quality of the frame with respect to original frame. Experimental results show a significant improvement in the Peak Signal Noise Ratio (PSNR) and Image Fidelity (IF) values after optimization over the base technique. Complexity analysis of the proposed technique is also described in this paper.

Dasgupta, et al. [2012] A spatial domain hash based least significant bit (LSB) technique has been presented in which the secret information is embedded in the LSB of the cover frames. A hash function is used to find out the position of insertion in LSB bits and that LSB positions are used to hide data. 8 bits of the secret information is divided into 3, 3, 2 and embedded into the RGB pixel values of the cover frames correspondingly. The performance of the proposed method is analyzed in terms some metrics i.e Peak Signal to Noise Ratio (PSNR) as well as the Mean Square Error (MSE) and estimation of embedding capacity is measured between the original and steganographic files. Image Fidelity (IF) is also measured and the results represent least reduction of the steganographic video file. The proposed technique is compared with existing LSB based steganography technique and the results are found to be promising. Swathi, et al. [2012] Video Steganography is a method to hide any kind of secret files into a Video file. The use of video as a carrier cover for the secure message overcame the capacity problem. Information can be hidden in any frame of video. The least significant bit (LSB) insertion is an essential approach for embedding information in a cover file. In this literature, a data hiding scheme will be presented to hide the secret data in particular frames of the video and in particular location of the frame by LSB substitution using polynomial equation.

III. Block Diagram of Steganography

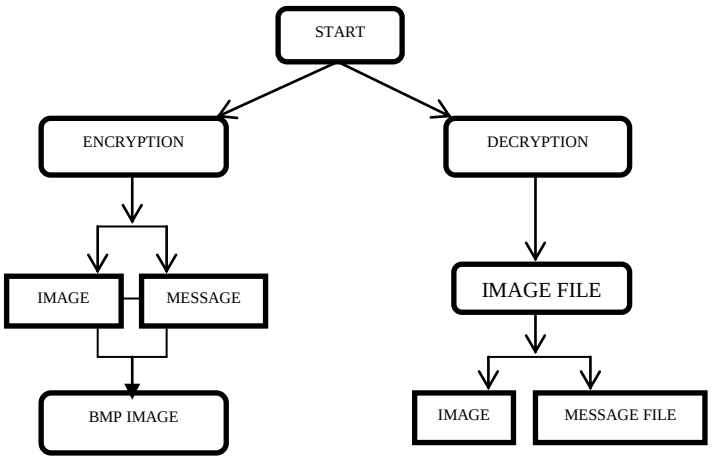


Fig. 3.1. Block Diagram of Stenography

This block diagram explains that how the steganography process takes place by the following points:

Encryption Phase

The "Encryption Phase" uses two types of files for encryption purpose. One is the secret file which is to be transmitted steadily, and the other is a carrier file such as image. In the encryption phase the data is planted into the image.

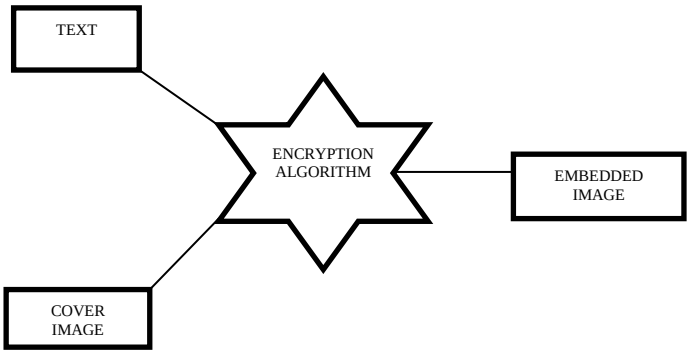


Fig. 3.2. Encryption Phase Process

Decryption Phase

The Decryption phase is overturn to encryption phase. In decryption phase, the carrier image in which the data is hided is given as an input file. Decryption section uses the "Least Significant bit Algorithm" (LSB) by which the encoded bits in

the image is partition and rolls to its original position and gives the output as a text form.

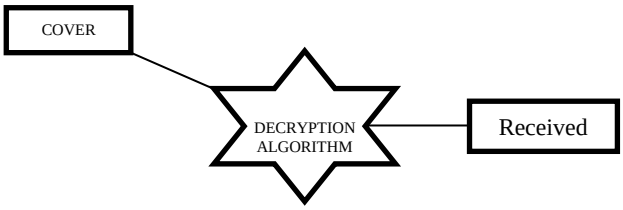


Fig. 3.3. Decryption Phase Process

Advantages

1. It can be used for on-guard data, such as in the field of media where copy write ensures authenticity.
2. It can be used by intelligence agencies for sending their secret message.

Disadvantage

1. Some of the ill minded people performed anti humanities techniques with this steganography.

IV. HIDING A TEXT IN IMAGE USING S-TOOL

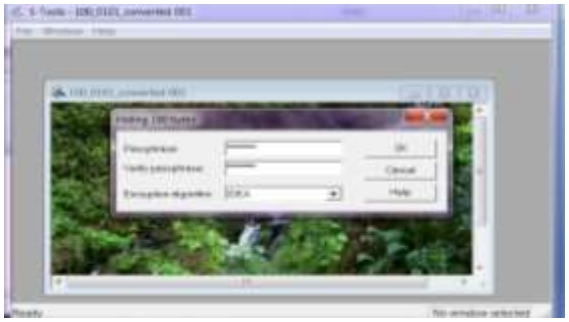
S-Tools is a steganography application which can hide

- Word Files
- Text Files
- PDF Documents
- Excel Sheets

Inside an image or a sound file. The image file has to be either a "**.**gif" or a "**.**bmp" and the sound file has to be a "**.**wav" file.

II. By using following steps S-Tool takes place:

1. Open the S-tools folder and double click on S-Tools.exe.
2. This is the area where either a .gif or .bmp or .wav file must be dragged and dropped to hide data in these files.
3. Drag and Drop the image file in which you want to hide the data.
4. In this example "Bank-Details.txt" is the file to be hidden in the "100_0001_converted 001.gif" file.
5. A dialog box which will prompt you to enter a passphrase will pop up. Now select the algorithm you wish to use to encrypt the data.



6. A new file will be generated. This holds the hidden information. To save the stego-file right clicks on the file and select save as… Assign a destination to the "steganographed" file, then clik on the option "OK".
7. Compare the "Original file" with the "Stego-file" .Visual appearance of both the files is the same.

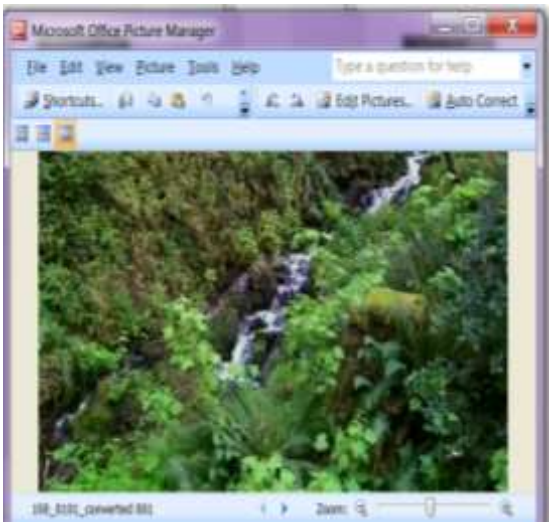
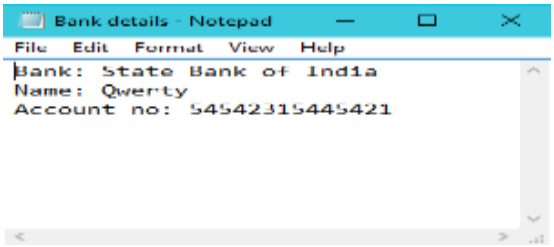


Fig. 4.1 Original File

Fig. 4.2 Stego-File

8. To reveal the hidden information Drag and Drop the Stego-file in S-tools. Then right click on the file and click on the option "*Reveal*".
9. Dialog box will appear which will prompt you to enter a passphrase. "Bank-details.txt" file which was hidden in "hidden.gif" will be displayed in the "Revealed files" list.
10. To retrieve the file right click on the Bank-details.txt and select the option Save as…
11. Double click on the file retrieved to see the contents.



V. CONCLUSION & FUTURE SCOPE

In the generation of in advance information swapping by means of internet and World Wide Web, steganography has developed lifeblood tool for information security. Steganography can be ranked based on many ethics and one among them is positioned on the type of cover media. This paper granted a review work in video steganography and this work is further extended by using DWT (Discrete Wavelet Transform), BCH codes and Haar Wavelet Transform techniques are applicable to hide a data for security purpose.

ACKNOWLEDGMENT

Ms. Gursukhmani Author wishes to express her sincere gratitude to Mrs. Sugandha Sharma, Assistant Professor, University College of Engineering, Chandigarh University, for guiding her throughout the current research work.

REFERENCES

[1] Kolakalur, Anush, Ioannis Kagalidis, and Branislav Vuksanovic. "Wavelet Based Color Video Steganography." International Journal of Engineering and Technology 2016.
[2] Mstafa, Ramadhan J., and Khaled M. Elleithy. "A novel video steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes." Systems, Applications and Technology Conference (LISAT), 2015.
[3] Vidhya, P. M., and Varghese Paul. "A Method for Text Steganography Using Malayalam Text." Procedia Computer Science 46 , pp 524-531, 2015.
[4] Mstafa, Ramadhan J., and Khaled M. Elleithy. "An Efficient Video Steganography Algorithm Based on BCH Codes." 2015.
[5] Satpute, Snehal, et al. "An Approach towards Video Steganography Using FZDH (Forbidden Zone Data Hiding)." 2015.
[6] Jenifer, K. Steffy, G. Yogaraj, and K. Rajalakshmi. "LSB Approach for Video Steganography to Embed Images." International Journal of Computer Science and Information Technologies 2014.
[7] Dasgupta, Kousik, Jyotsna Kumar Mondal, and Paramartha Dutta. "Optimized Video Steganography Using Genetic Algorithm (GA)." Procedia Technology 10, 131-137, 2013.
[8] Dasgupta, Kousik, J. K. Mandal, and Paramartha Dutta. "Hash based least significant bit technique for video steganography (HLSB)." International Journal of Security, Privacy and Trust Management (IJSPTM) 1-11, 2012.
[9] Swathi, A., and Dr SAK Jilani. "Video Steganography by LSB Substitution Using Different Polynomial Equations." MadanapalliInstitude of Technology and science , 2012.