iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: TPAM-2018 Issue: onference Month of publication: March 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

A Review of Video Steganography Using LSB Methodology

Arockia Valan Rani B[1]
[1]Assistant Professor, Department of Computer Science, St. Joseph's College of Arts and Science for women - Hosur

Abstract: ***Computer technology and the Internet have made a breakthrough in the existence of data communication. This has opened a whole new way of implementing steganography to ensure secure data transfer. Steganography is the fine art of hiding the information. Hiding the message in the carrier file enables the deniability of the existence of any message at all. This paper designs a stego machine to develop a steganographic application to hide data containing text in a computer video file and to retrieve the hidden information. This can be done by embedding a text file into a video file in such a way that the video does not lose its functionality using Least Significant Bit (LSB) modification method. This method applies imperceptible modification. This proposed method strives for high security to an eavesdropper's inability to detect hidden information.***
Keywords: Data hiding, LSB, Stego machine, Video Steganography.

I. INTRODUCTION

The revolution in digital information has created new challenges for sending a messages in safe and secure way. Whatever technique we choose, the most important question is its degree of security. Numerous approaches have been developed for addressing the issues of information security such as cryptography and steganography. Cryptography provides move in securing information. It scrambles the secret message, such that it become meaningless to eavesdroppers. In such cases, steganography was the answers.

Steganography is hiding private or secret data within a carrier in hidden manner. The origin of the word steganography comes from the Greek language. It is derived from two Greek words "stegos" which means "cover" and "grafia" which means "writing". Steganography evolved driven by the need to hiding the existence of a secret communication.

Cryptography and steganography try to protect data, but technology alone is perfect. Therefore, sometimes it is better to combine both approaches together to increase the security level of the system. In this case, even if the communications existence was detected and the steganography was overpowered, the attacker still has to break the encryption to know the message.

Watermarking is another technology that is closely related to steganography. But it lies on different philosophies and goals. Both technologies implant information in the cover in order to send this information imperceptibly. However, in steganography, the communication is carried out between two parties. Hence, steganography is mainly concerned with concealing the existence of the communication and protecting the embedded data against any modifications that happens during transmission such as format change or compression.

	Cryptograpy	Steganograpy	Water Marking
Goal	Hide the contents of the communications	Conceal the existence of the communication	Protect the embedded content against intentional attacks for destruction or removal
Perceptual invisibility	Doesn't Exist	Must Exist	Application dependent
Signature size	Large	Large	Application dependent
Signature structure	Must Change	May Change	Doesn't Change
Use of key	Necessary	Optional	Optional
Output	Cipher text	Stego-file	Watermarked file
Goal fails when	Cipher text decrypted	Secret message existence is detected	Watermark is changed or removed
Challenges	Robustness	Perceptual transparency, Hiding Capacity and robustness	Robustness

Comparison between Cryptography, Steganography and Watermarking

Table 1 shows a comparison between cryptography, steganography and watermarking. It highlights the similarities and dissimilarity between these three technologies.

Table1: comparison between cryptography, steganography and watermarking.

Application of steganography varies from military, industrial application to copyright and Intellectual Property Rights (IPR). By using lossless steganography techniques messages can be sent and received security.

II. TYPES OF STEGANOGRAPHY METHODOLOGY

Steganography and cryptography are very much related. Cryptography scrambles messages so it can't be understood. Steganography on the other hand, hide the message so there is no information of the existence of the message. Comparison is made between portions of the plaintext and portions of the cipher text by cryptography method. In Steganography Comparison may perhaps be made between the cover-media, the stego-media, and possible portions of 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. Crypto analysis technique is applied to extract the message, if it is encrypted.

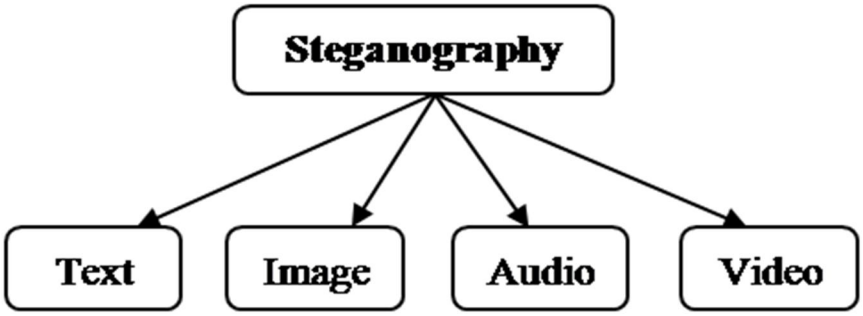


Figure 1: Types of Steganography

The use of video as a carrier cover for the secure message overcame the capacity problem and added small enhancement to the security aspects. The integration of Steganography and Cryptography techniques provided powerful system for sharing secure messages. This integration within video cover carrier is a good stage of such system, but the capacity of the produced message from the cryptography technique which is called ciper-text is large than the original massage (plain text).

Figure.2 Shows two video images, one-carrier image of the message and the other - the image labeled Stego'd image contain the hidden message. It is not viable to recognize the different between the original video and the Stego'd video image.

Figure 2 Steganography using video image

A. Steganography Terms

1) Cover-Medium: The medium in which information is to be hidden, also sometimes called as Cover-image or carrier.

2) Stego-Medium: A medium in which information is hidden.

3) Message: The data to be hidden or extracted.

4) In summary: Stego-medium =hidden-message+carrier+stego-key

III. VIDEO STEGANOGRAPHY TECHNIQUES:

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

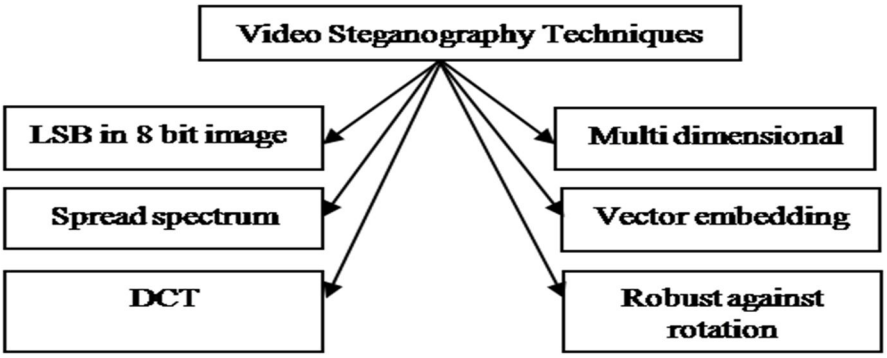


Figure 3: Techniques of video steganography

First of all, the most common method is Least Significant Bit method (LSB) which hide secret data into the least significant bits of the host video. This method is simple and can hide huge data.

Another well-known method which has been still researching is called Spread Spectrum. This method satisfies the robustness criterion. A very little amount of hidden data is lost after applying some geometric transformations . 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.

A technique for high capacity data hiding using the Discrete Cosine Transform (DCT) transformation. Its main intention is to maximize the payload while keeping robustness. In this, secret data is embedded in the host signal by modulating the quantized block DCT coefficients of frames.

A vector embedding method that uses robust algorithm with codec standard(MPEG -1 and MPEG-2). This method embeds audio information to pixels of frames in host video.

IV. MODULES OF STEGO MACHINE

The video Stegomachine performs the process of conceal and reveal in subsequent modules of video stego machine are:

Video Header Information
File Handling
Encryption
Steganography - Conceal data
De Steganography - Reveal Original data
Decryption
Graphical User Interface

A. Video Header Information

The video header module collects the header information of an AVI (Audio/visual interleaved) file which is based on the RIFF (resource interchange file format) document format .This is used to verify the AVI format of the carrier file. This module is used to store the information on the subject of AVI Main Header, AVI Stream Header, Audio, and BITMAP. This information is used to verify whether the carrier file is in AVI format and to check whether it is a video, Audio, or any other format.

B. File Handling

In file handling , the AVI (Audio/Visual interleaved) file header is kipped and its contents are opened in an ASCII format for processing. This reads the AVI file in terms of byte corresponding to the header and creates a key file. The text file to be embedded is converted into binary value. Then each bit in the binary value is converted to 8 bit value. This is done by appending zeros in front of the bit.

C. Encryption

The message to be hidden inside the carrier file is encrypted along with a key to dissatisfy the praying eyes of nosy people. This enhances the security during data transmission. This strong encryption method provides robustness to the Stego machine. In this module, the input message is first converted to byte value. The key is obtained from the user which is added to the respective byte and stored in separate byte array which is then converted to character to get the encrypted form of message. The input to this function is the plain text message and a key value to encrypt the message.

D. Steganography - Conceal data

This module performs the process of steganography. Here the carrier file (AVI file) length is obtained and checked for whether it is eight times greater than that of the text file. Then, find the starting point of the data in the AVI file and create a key file by writing the content of the AVI file starting from the data to the end. The carrier file is changed into binary. The result is overwritten to the data part of the AVI file and as well as written into the newly created text file. The output obtained for this system is a stego'd video file, and a key file which is to be shared by a secure channel. Figure.4 depicts the clear picture of concealing the data.

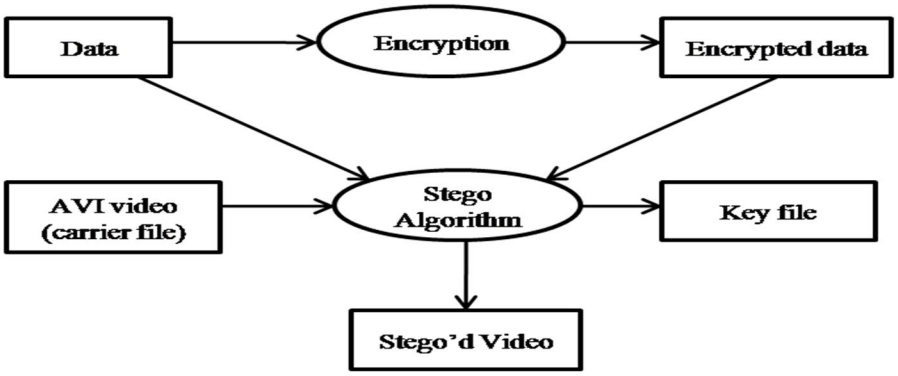


Figure 4: Steganography of Stegomachine

E. DeSteganography - Reveal Original data

This DeSteganography module decodes the video file to receive the hidden data from video. Here, the carrier file (AVI file) and the key file are given as input. Using a Random Access Mode the AVI file and the key file is opened to find the starting point of the data in the AVI file. This reads the AVI file and key file Byte by Byte and finds the difference between them. The output obtained is an original AVI video file, and a data file that is the message which is hidden inside the AVI video file. Figure.5 illustrates the process of revealing the original data from Stego'd video file.

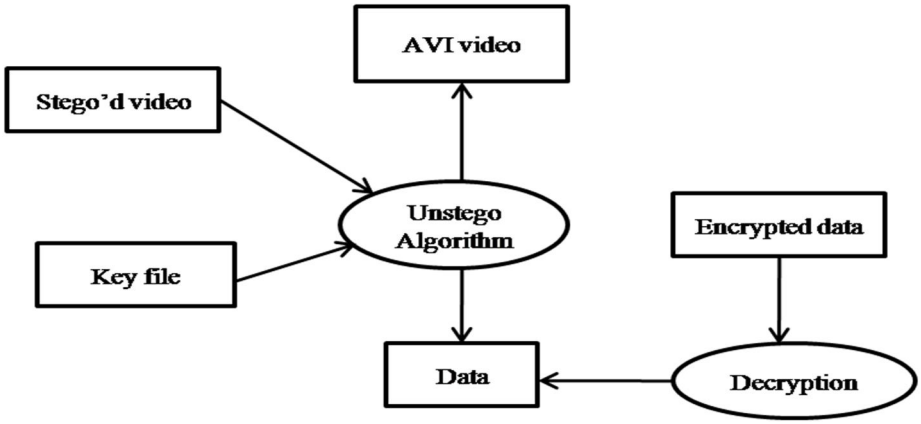


Figure 5: Desteganography

F. Decryption

The hidden message is decrypted using the key. As once the algorithm gets revealed, all encrypted data with the algorithm could be decrypted. First, this module converts the input message to byte value. The key is obtained from the user which is subtracted from the respective byte and stored in a separate byte array ,it is then converted to character to get the decrypted form of message. The input to this function is the encrypted message file and a key value to decrypt the message.

G. Graphical User Interface (GUI)

This GUI is created as a user friendly Wizard and does not need any previous training to operate it. It helps user to do steganography without encryption and encryption without steganography. This will help user with a wizard to

Hide a message in a video file

Retrieve the hidden message in a stego'd video

Encrypt a text file

Decrypt an encrypted file

V. METHOD OF CONCEALING DATA IN VIDEO:

A. Least Significant Bit (LSB)

LSB is the lowest bit in a series of numbers in binary. E.g. in the binary number: 10110001, the least significant bit is far right. The LSB based steganography is one of the steganographic methods, used to embed the secret data in to the least significant bits of the pixel values in a cove image. E.g. 420 can be hidden in the first eight bytes of three pixels in a 24 bit image.

B. Pixels

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
420 : 110100100

C. Result

(00100111 11101001 11001000)
(00100111 11001000 11101000)
(11001001 00100110 11101000)
Here number 420 is embedded into first eight bytes of the grid and only 4 bits are changed.

VI. VIDEO STEGANOGRAPHY BASED ON IMAGE STEGANOGRAPHY

Due to the high encoding speed of the image steganography algorithm, We widen the image hidden technique to video one . Here we simply consider the steganography in the uncompressed video. That means we try to hide a video stream in another video stream with almost the same size. The main idea is that we treat each frame of both videos as the images and apply the image steganography for each frame with some required mechanism. Suppose the host video stream is *F*, hidden video stream is *H*. The frame length of *F* is longer than or equal to that of *H*.
The encoding and decoding process can be described as follows.

A. Encoding of the video steganograph

1) Extract each frame from video stream F and H to R_F,G_F,B_F and R_H,G_H,B_H correspondingly as some static images.
2) For each group of { R_F, R_H},{G_F,G_H} and {B_F,B_H}, apply the above image steganography algorithm to hide {R_H,G_H,B_H} into {R_F,G_F,B_F} to form {$R2_F,G2_F$, $B2_F$}. Here we should choose a suitable control error so that the length of the partitioning codes do not excess the embedding space of the host. Usually, the control error of 6 is chosen and then the non-uniform rectangular partition is performed, if the embedding- length requirement is not satisfactory, increase the control error by 0.5 and try the coding again the requirement is reached although this may further reduce the reconstruction quality.
3) Reform each set of {$R2_F,G2_F,B2_F$} to the whole video stream F2 with the codes of the hidden video stream.

B. Decoding of the video steganograph

When receiving the video stream **F2**, the hidden video can be reconstructed by following the decoding process below:

1) Divide each frame of the video stream F2 and F into static-image group {$R2_F,G2_F,B2_F$} and {R_F,G_F,B_F}.
2) Apply the decoding process of image steganography algorithm to extract each hidden frame from {$R2_F$, $G2_F,B2_F$} and {R_F,G_F,B_F} to {$R2_H$, $G2_H$, $B2_H$}.
3) Reform each set of {$R2_H$, $G2_H$, $B2_H$} to the whole reconstructed hidden video stream H2.

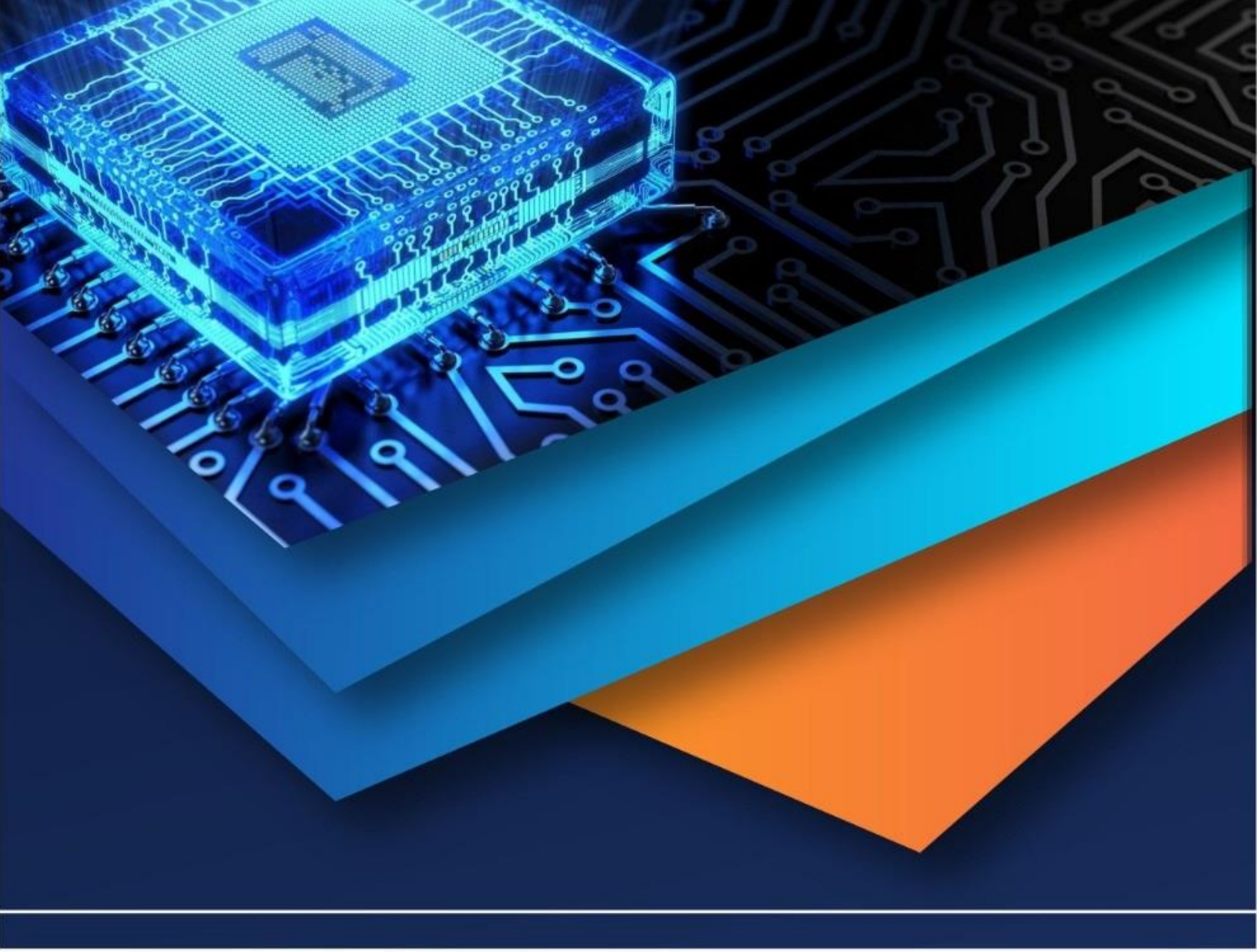
VII. CONCLUSION

A secured based LSB technique for video steganography has been presented in this paper. This technique utilizes cover video files in spatial domain to conceal the presence of sensitive data regardless of its format. This video steganography provides a robust and secure way of data transmission. This system is a Platform-independent application with high portability and high Consistency. This paper hide text file in AVI video file using LSB methodology. In future we extend this hiding process in other video files like MPEG, FLV, MP4, etc.

REFERENCES

[1] Sutaone, M.S.; Khandare, "Image based steganography using LSB insertion technique" IET, 2008.
[2] Niels Provos and Peter Honeyman, "Hide and Seek: An Introduction to Steganography", University of Michigan, IEEE 2003.

[3] Gupta s. and Gujral G., "Enhanced least bit algorithm for image Steganography" IJCEM international journal of computational engineering & management. vol.15 issue4, July 2012.
[4] Bodhak V. and Gunjal L., "Improved protection in video Steganography using DCT & LSB" international journal of engineering and innovative technology (IJEIT) vol.1, issue4, April 2012.
[5] Gupta H. and Dr. Chaturvedi D., "Video Data Hiding Through LSB Substitution Technique" Research Inventy: international Journal Of Engineering and Science. vol.2 Issue 10 2013.
[6] Mr tyagi V., "Data hiding in image using LSB with cryptography" International journal advanced research in computer science and software engineering. vol.2, issue4, april 2012.
[7] K. Steffy Jenifer, G. Yogaraj, K. Rajalakshmi, "LSB Approach for Video Steganography to Embed Images", IJCSIT, Vol.5 (1), 2014, 391-322, ISSN:0975-9646.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY