International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 3, Issue 4, April 2014

SECRET LAYER

Pooja Sontakke, Shweta Tambe, Sonal Sangani, Surbhi Khandelwal

[1]Pune University, Sinhgad College Of Engineering,

Sinhgad Institute, Vadgaon (BK) Pune, India

[2]Pune University, Sinhgad College Of Engineering,

Sinhgad Institute, Vadgaon (BK) Pune, India

[3]Pune University, Sinhgad College Of Engineering,

Sinhgad Institute, Vadgaon (BK) Pune, India

[4]Pune University, Sinhgad College Of Engineering,

Sinhgad Institute, Vadgaon (BK) Pune, India

Abstract: **The growth of high speed computer networks and that of the Internet, in particular, has increased the ease of Information Communication. In comparison with Analog media, Digital media offers several distinct advantages such as high quality, easy editing, high fidelity copying, compression etc. So, Information Security is becoming an inseparable part of Data Communication. In order to address this Information Security, Steganography plays an important role. In present times, confidential information such as medical records and banking or financial data and military information is at a risk because of malicious security threats. The kind of information especially targeted is the one where the issue of authentication and authorization is a critical factor. Steganography is the art and science of information within a video. In this paper, a hash based least significant bit (LSB) technique has been proposed. A spatial domain technique where the secret information is embedded in the LSB of the cover frames. Eight bits of the secret information is divided into 3,3,2 and embedded into the RGB pixel values of the cover frames respectively. A hash function is used to select the position of insertion in LSB bits. The proposed method is analyzed in terms of both Peak Signal to Noise Ratio (PSNR) compared to the original cover video as well as the Mean Square Error (MSE) measured between the original and steganographic files averaged over all video frames. Video Steganography is one proposed system which is based on video Steganography, cryptography and compression, ensures secure and large amount of data transfer between the source and destination.**

Index terms: **Steganography, Video Steganography, cover video, cover frame, secret message, LSB, Cryptography, Decomposition, HLSB algorithm, AES algorithm**

1. INTRODUCTION

One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual

ISSN: 2278 – 909X

or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography become more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevents the detection of hidden messages. Steganography include an array of secret communication methods that hide the message from being seen or discovered. This technique relies on a message being encoded and hidden in a transport layer in such a way as to make the existence of the message unknown to an observer. Importantly, the transport layer – the carrier file - is not secret and can therefore be viewed by observers from whom the secret message itself should be concealed. The power of steganography is in hiding the secret message by obscurity, hiding its existence in a non-secret file. In that sense, steganography is different from cryptography, which involves making the content of the secret message unreadable while not preventing non-intended observers from learning about its existence. Because the success of the technique depends entirely on the ability to hide the message such that an observer would not suspect it is there at all, the greatest effort must go into ensuring that the message is invisible unless one knows what to look for. The way in which this is done will differ for the specific media that are used to hide the information. In each case, the value of a steganographic approach can be measured by how much information can be concealed in a carrier before it becomes detectable, each technique can thus be thought of in terms of its capacity for information hiding. There are numerous methods used to hide information inside of Picture, Audio and Video files.[1],[2],[4] The desire to send a message as safely and as securely as possible has been the point of discussion since time immemorial. In this paper a hash based LSB Techniques is proposed in spatial domain. An application of the algorithm is illustrated with AVI (Audio Video Interleave) file as a cover medium. The results obtained are significant and encouraging. Effort has also been taken to study the steganalysis of the proposed scheme.[5]

2. PROPOSED TECHNIQUE

At the sender's side, take an input file which is the message file that is either a text file(.txt) or an image(.bmp) and a video file(.avi) which is the target file and encrypt the plain text. After that perform steganography on it using the hash based least significant algorithm. Hence, getting the video file stego.

At the receiver's side, there is an extractor for extracting the ciphered message from the video stego file. After extracting the cipher text perform decryption to get the plain text. Thus, getting the desired message file.

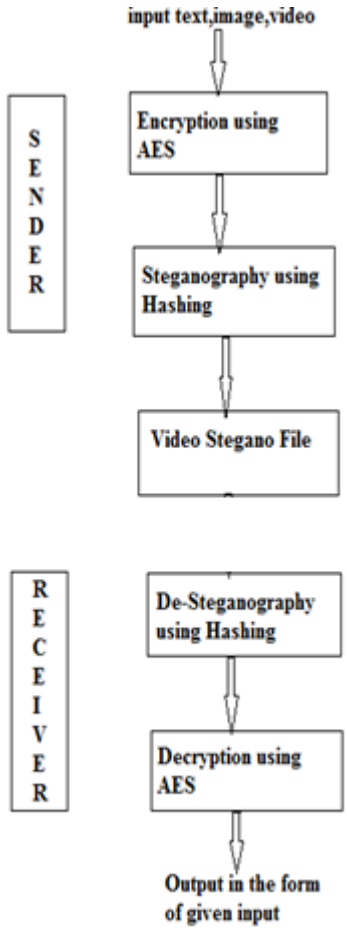

Figure 2.1: Advanced Steganography and Cryptography Technique

3. PROPOSED ALGORITHMS

3.1 Advanced Encryption Algorithm(AES)

AES algorithm is used for the encryption & decryption of data blocks. It uses 10, 12 or 14 rounds. The key size can be 128,192 or 256 bits depending on the round. This technique uses 192 bits.[3]

3.2 Hash Based Least Significant Bit (HLSB) Technique

The proposed technique we will be binding eight bits of secret data at a time and hide them in LSB of RGB (Red, Green and Blue) pixel value of the carrier frames in 3, 3, 2 order respectively. Out of the eight bits of message 6 bits are placed in R & G pixel and the remaining 2 bits are placed in B pixel.

ISSN: 2278 – 909X

As blue is more sensitive and the chromatic influence of blue is more to The human eye that red and green pixel the following pattern of 3,3,2 is taken. According to this pattern small colour change would be very difficult for the human eye to detect.[5] The embedding positions of the eight bits out of the four 4 available bits of LSB is obtained using a hash function of the form,

$$k = p \,\%\, n \qquad (1)$$

where, k is LSB bit position within the pixel, p represents the position of each hidden image pixel and n is number of bits of LSB which is 4 for the present case.[5]

LSB bits mostly consists of the parity and the error checking bits. Thus, changing the LSB bits would not have much effect as compared to the MSB. Change in the MSB bits leads to a drastic change in the image of the video which would be noticeable. Hence, 4 bits LSB technique is used. Robustness of the technique is increased due the distribution of random bits as compared to other LSB techniques. After hiding the data the frames are grouped together and the final stego output video file is formed. [5]

The reverse technique is used to decode the secret data. The video file received is broken into frames and using the same hash function the data of the secret message is regenerated.

The (HLSB) algorithm works as:

Algorithm at Sender:

1. Select the cover video file.
2. Read the video file format.
3. Break the video in frames
4. Use the hash function function for finding the positions shown in equation(1).
5. Embed the data in 3,3,2 format in the RGB pixels.
6. Regenerate the video.

Algorithm at Receiver:

1. Select the stego video file.
2. Read the video file format.
3. Break the video in frames
4. Use the hash function function for position the positions shown in equation(1).
5. Retreive the data from 3,3,2 bits of the RGB pixel.
6. Reconstruct the secret information

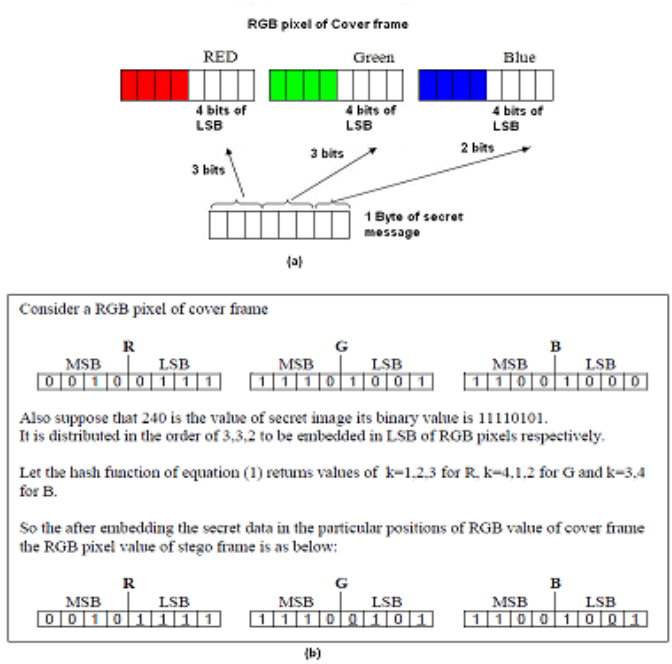

Figure 3.1: Proposed hash based LSB embedding technique[5]

4. CONCLUSION:

Steganography has its place in the security. On its own, it won't serve much but when used as a layer of cryptography, it would lead to a greater security. A secured hash based LSB technique for video steganography has been presented in this paper. This technique utilizes cover video files to conceal the presence of sensitive data. Performance analysis of the proposed technique after comparison with LSB technique is quite encouraging. The proposed technique is applied to AVI files, however it can work with any other formats with minor procedural modification. A software based Steganographic Engine for video steganography is the future scope of the technique.

REFERENCES:

1) Ritej Gaba, Gaurav Deep" Comparison of Various Video SteganographyTechniques" Ritej et al./ IJAIR Vol. 2 Issue 6 ISSN: 2278-7844.

2) Zenon Hrytskiv, Sviatoslav Voloshynovskiy and Yuriy Rytsar "Cryptography and Steganography of video information in modern communication" Series: Electronics and Energetics vol. 11, No.1 (1998), 115-125.

3) Daniel Socek, Hari Kalva, Spyros S. Magliveras, Oge Marques, Dubravko Culibrk, Borko Furht "New approaches to encryption and steganography for digital videos" Springer-Verlag 2007

4) Ms. Monika S. Shirbhate, Prof. S.S. Kulkarni "Hiding and Extracting Secrete Data in Video File with Noise Compression"

ISSN: 2278 – 909X

International Journal Of Computer Science And Applications Vol. 6, No.2, Apr 2013 ISSN: 0974-1011

5) Kousik Dasgupta, 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), Vol. 1, No 2, April 2012

6) Namita Tiwari Dr.Madhu Shandilya " Evaluation of Various LSB based Methods of Image Steganography on GIF File Format" International Journal of Computer Applications (0975 – 8887) Volume 6– No.2, September 2010

7) Shery Elizabeth Thomas, Sumod Tom Philip, Sumaya Nazar, Ashams Mathew & Niya Joseph : "Advanced Cryptographic Steganography Using Multimedia Files"

8) Dipti Kapoor Sarmah, Neha Bajpai: "Proposed System for data hiding using Cryptography and Steganography".

9) Namita Tiwari, Madhu Shandilya "Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth" International Journal of Security and Its Applications Vol. 4, No. 4, October, 2010

10) Parveen Mor, Tanupriya Choudhury, Vasudha Vashisht "A Novel Steganographic Approach to enhance the Performance of Security System in a Smarter Way" IJCSMC, Vol. 2, Issue. 6, June 2013, pg.163 – 169

11) Neil F. Johnson**,** Sushil Jajodia "Exploring Steganography: Seeing the Unseen" IEEE , 1998

ISSN: 2278 – 909X