Securing Video Files using Steganography Method in Android Mobile

S.Jothimani , H.Shaheen

Abstract— The development of smart phone technology has lead to denigrate of the phone prepared with many sophisticated features such as sensors. Camera is one of the most extensively used sensors. Although the photographs capture by camera can be shared via Multimedia Message Service (MMS) which allows broadcast of files like photographs, audio and video. A major problem of MMS is, it doesn't provide adequate safety mechanism. Because of this, the data of the people who wants to conceal confidential information from state-controlled systems that can be easily monitored. Video Steganography is a technique to hide any type of files in any extension into a Video file. The idea proposed in this paper is to embed any kind of data in another file, which is called carrier file. The carrier file must be image video file. Steganography is the art of hiding messages inside other messages such that the very existence of the message is unknown to third party. In this paper, a steganography-based android mobile application that can insert the confidential information into an image, then into a video that can be send it to receiver. Finally we can extract the confidential information from the image in the receiver side.

Index Terms— Steganography, Carrier file, video, android , mobile, confidential , Multimedia Message Service

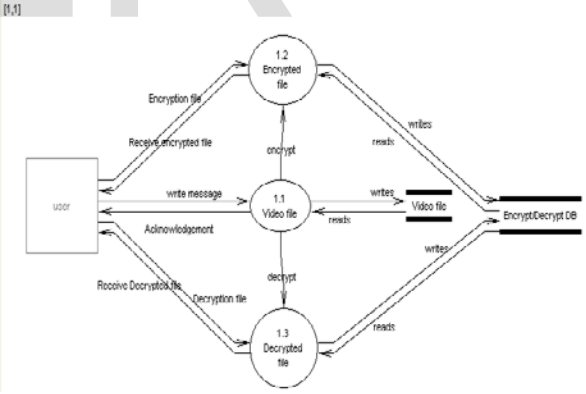
1 INTRODUCTION

Steganography derive from the Greek word steganos, meaning covered or secret. On the simplest level, Steganography is hidden writing, whether it consists of invisible ink on paper or copyright information hidden in an video file. Where cryptography scrambles a message into a code to incomprehensible its meaning, Steganography hides the message completely. These two secret communication technologies can be used separately or together—for example, by first encrypting a message, then thrashing it in another file for transmission. As the world becomes more concerned about the use of any secret communication, and as regulations are created by governments to limit uses of encryption, steganography's role is gaining eminence.

What Steganography fundamentally does is it exploit human perception, human senses are not trained to look for files that have information hidden inside of them, although there are programs available that can do what is called Steganalysis (Detecting use of Steganography.) The most common use of Steganography is to hide a file inside another file. When information or a file is concealed inside a carrier file, the data is typically encrypted with a password.

When information is hidden inside video in program or person hiding the information will usually use the discrete cosine transform (DCT) method. DCT works by slightly changing the each of the images in the video, only so much though so it is not noticeable by the human eye. To be more precise about how DCT works, DCT alters values of certain parts of the images, it is usually rounds them up.

For example if part of an image has a value of 6.667 it will round up to 7. Steganography in videos is comparable to that of steganography in images, apart from information is hidden in each frame of video. White space and tabs occur obviously in documents, so there is not really any possible way using method of steganography would cause someone to be apprehensive.



It is possible to alter graphic or video files slightly without losing their overall capability for the viewer and listener. With video, you can use bits of file that contain sound not audible to the human ear. With graphic images, you can remove superfluous bits of color from the image and still produce a video that looks intact to human eye and is difficult to discern from its original. It is in those bits that stego hides its data. A stego program uses an algorithm, to entrench data in an image or sound file, and a password scheme to allow you to recover information.

2 WORKING OF STEGANOGRAPHY

- *S.Jothimani Assistant Professor, Department of Computer Science and Engineering, Nehru Institute of Engineering and Technology, India. E-mail: jothimanicse@gmail.com*
- *H.Shaheen Assistant Professor, Department of Computer Science and Engineering, Nehru Institute of Engineering and Technology, India. E-mail: shaheen66@gmail.com*

Steganography strips less important information from digital content and injects hidden data in its place. This is done over the spectrum of the entire image. Here's one way it could be implemented:

The following sequence of 24 bits represents a single pixel in an image. Its 3 bytes of color information provide a total of 256 different values for each color (red, green and blue) and thus can represent a total of 16.7 million colors. This particular value displays as a dark green:

Bytewise insertion of data

Byte 1 - Red	Bytc2-Grcci	Byte 3 - Blue
O D O D O mo	onnnnonn	o o onnnno

Now, let's take 11 of these pixels that represent, say, part of a solid-color background. In the following sequence, the least significant (rightmost) bit of each 8-bit byte has been co-opted to hide a text message—the four characters Aha!—in ASCII binary.The hidden message occupies 32 of those 264 bits (about 12%) and contains four 8-bit bytes. In the diagram, each maroon or gold box represents a bit that had to be changed to include the hidden message. Notice that only 15 of 264 bits (less than 6%) had to be changed and only eight of the 11 pixels were altered.

transforms and non-linear substitutions.

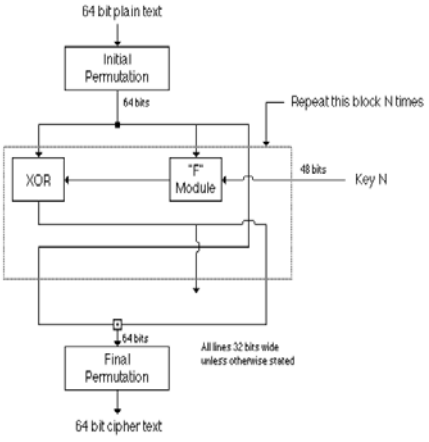


Fig. 5.1: DES

The word 'Steganography' provides means for secure data transmission and secure data storage network. Hereby, important files carrying confidential information can be stored in the server in an encrypted form. Access to these files is restricted to certain authorized people only. Transmission also takes place in an encrypted form so that no impostor can get any useful information from the original file during transit. Further, before trying to access important files, the user has to login to the system using a valid username and password, which is allotted to him by the system administrator

3 STEGANOGRAPHY TECHNIQUES

The effective steganography should have property of remaining intact irrespective of the tampering, the secret message should be invisible and it should go undetected. The capacity of the technique to hide the data should be well achieved.

A. Image Steganography

According to computer system an image can be said as array of numbers which represents light intensities at pixels, which results in data. Image is composed of 8 bits per pixel i.e.256 colors. The colors are generated from three primary colors as red, green and blue (RGB). various approaches has been designed for image steganography some of common approaches are LSB(Least Significant Bit) substitution which is the easy and most common approach of hiding data inside images. Masking is another technique of embedding messages in significant areas. The DCT based on image transformation involve the mathematical function for hiding data inside the images.

B. Audio Steganography

Audio steganography works by slightly changing the binary sequence and concealing with the secret message. Several methods are proposed such as Least Significant Bit (LSB) replacing last digit of carrier file. Parity coding involves breaking down of signal and then hiding the message in parity bits of each sample. Phase coding involves encoding of secret data to phase shifts. Spread spectrum distributes secret data into frequency spectrum, in which direct sequence and frequency hopping is used. The Echo method generates echo for insertion of secret data into signal.

C. Video Steganography

The separation of video into audio and images or frames results in the efficient method for data hiding. The use of video files as a carrier medium for steganography is more eligible as compared to other techniques. As a result of this technique is discussed and proposed in this paper.

D. Network Steganography

The approach for hiding data is to use network steganography by sending data with the help of network protocol. Network or transport layer such as IP/TCP or ICMP and UDP protocols are used for sending messages.

E. Video Steganography

The separation of video into audio and images or frames results in the efficient method for data hiding. The use of video files as a carrier medium for steganography is more eligible as compared to other techniques. As a result of this technique is discussed and proposed in this paper.

4 THE PROPOSED METHOD

proposed method for the data hiding is based on image and video

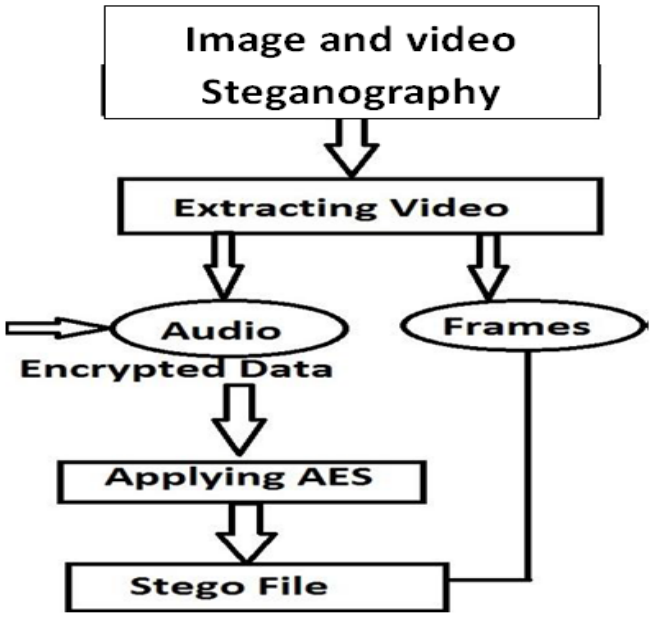
hybrid steganography that we have used the AES algorithm to make the steganography more secure and robust. The image and video hybrid steganography is achieved by embedding the image files with the secret data and it is embedded with video files that are to be transmitted with the intention of keeping the secret data unaltered or remains intact at receivers end.

1. AES (Advanced Encryption Standard)

The AES algorithm is most secure and robust cryptographic algorithm against attacks.Unlike the DES which is far slow and is already broken and also produce inefficient software code. Triple DES on the other hand is comparatively slower than DES as it has three more rounds.

AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. (Rijndael was designed to handle additional block sizes and key lengths, but the functionality was not adopted in AES.) Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of cipher text.

AES has symmetric block cipher and hence uses same key for encryption and decryption. The block size of AES varies from 128, 192, and 256 bits, the substitution and permutation are performed in AES.



The number of rounds depends upon the key length i.e. 10 rounds for 128 bit key,12 for 192 bit key and 14 for 256 bit key.We have also used SHA-1 for providing more restricted approach as it generates the hash function with key which helps to make the secret data secure if it is being identified without key it can never be altered. The next stage is to perform actual steganography where this secret data is given to hide inside the video and image carrier the stego video is generated as a result of video steganography We then tested the algorithm using the PSNR (Peak signal-to-noise ratio). PSNR is a standard measurement used in steganograpy technique in order to test the quality of the stego images. The higher the value of PSNR, the more quality the stego image will have.

If the cover image is C of size M × M and the stego image is S of size N × N, then each cover image C and stego image S will have pixel value (x, y) from 0 to M-1 and 0 to N-1 respectively. The PSNR is then calculated as follows:

$$PSNR = 10.\log_{10}$$

Note that MAP is the maximum possible pixel value of the images. For example, if the pixels are represented using 8 bits per sample, then the MAP value is 255. If the stego image has a higher PSNR value, then the stego image has more quality image.

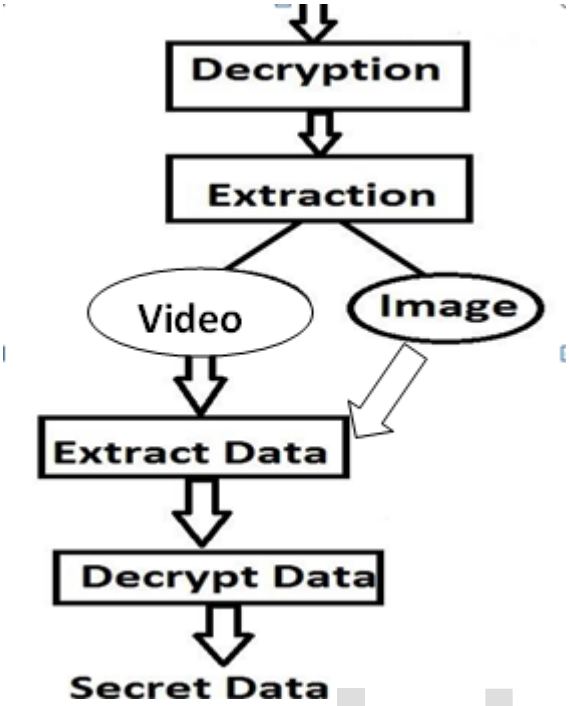
B. Extraction Of image and video File (at Sender Side)

The video steganography composed of two main phases namely extraction of video files and embedding of secret message, as the secret message is already encrypted using AES and SHA-1 it can be easily embedded into carrier video. The extraction of video results in frames as video generally composed of still images and audio, the audio and image frames from the file video is extracted. From this extracted audio the stego file is generated as a secret data is hided in the audio not in the image frames. Audio contains unused bits or free bits of information in which secret data can be very easily hided. For making this file more robust against attack or identification stego file is again encrypted using the Advanced Encryption Standard. The stego filegenerated is then transmitted over the communication channel which remains intact as a result of this complex data hiding method.

C. Extraction Of Stego File(at Receiver Side)

The stego file can be extracted at receiver's side by performing decryption of stego file and then by extracting the carrier video which is nothing but a collection of audio and image frames

The resultant data is the encrypted secret data which is again decrypted to obtain original data.



Thus the proposed system provides the most secure approach using two layer of encryption the first is performed on the secret data itself and another on the audio file.

5 Conclusion

In this paper we presented several ways of hiding the secret data inside the cover medium such as image, audio, video. The proposed system for data hiding uses AES for encryption and SHA-1 for generating secret hash function or key which results in more secure technique for data hiding. We can conclude that the proposed system is more effective for secret communication over the network channel.

.

References

[1] Ahsan K., and Kundur D., "Practical Internet Steganography: Data Hiding in IP" found online at http://www.ece.tamu.edu/~deepa/pdf/txsecwrksh03.pdf.

[2] Digital Watermarking for Digital Media, Information Science Publishing.

[3] Hiding in Plain Sight: Steganography and the Art of Covert Communication Cole, Eric.

[4] M. M Amin, M. Salleh, S. Ibrahim, M .R. Katmin, and M. Z. I. Shamsuddin," Information Hiding using Steganography", IEEE 0-7803- 7773-March 7,2003

[5] Advanced Steganography Algorithm usingencrypted secret message, Joyshree Nath and Asoke Nath, International Journal of Advanced Computer Science and Application (IJACSA) Vol-2 No.3, Page19-24,March 2011

[6] Manpreet Kaur, Er. Amandeep Kaur, "Improved Security Mechanisam of text in Video by using Steganographic Technique: A Review" , International Journal of Advanced Research in Computer Science and Software Engineering , May 2014 ,Volume 4, Issue 5, ISSN: 2277 128X

[7] M. Suresh Kumar, G. MadhaviLatha, "DCT Based Secret Image Hiding In Video Sequence", Int. Journal of Engineering Research and Applications, August 2014, Vol. 4, Issue 8(Version 1), ISSN: 2248-9622

[8] A. Giannoula, D. Hatzinakos, "Compressive Data Hiding for Video Signals", Proceedings of International Conference on Image Processing, 2003, pp. I529- I532.

[9] Giuseppe Caccia, Rosa Lancini, "Data Hiding in MPEG2 Bit Stream Domain", Proceedings of International Conference on Trends in Communications, 2001, pp.363-364

[10] F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn, "Information Hiding-A Survey", Proceeding of the IEEE, vol. 87, no. 7, June 1999, pp.1062-1078.