ISSN (Online) : 2454-4159

International Journal of Advanced Research in Science Management and Technology

IJARSMT

Volume 2, Issue 1, January 2016

Text Hiding In Multimedia By Huffman Encoding Algorithm Using Steganography

Madhavi V.Kale [1], Prof. Swati A.Patil [2]

PG Student, Dept. Of CSE., G.H.Raisoni Institute Of Engineering And Management,Jalgaon (Ms), India[1]

Assistant Professor, Dept. Of CSE., G.H.Raisoni Institute Of Engineering And Management,Jalgaon (Ms), India[2]

ABSTRACT**—** Information hiding is a part of information Security. Steganography is a technique of information hiding that focuses on hiding the existence of secret messages. Image steganography is a process that hides the message into cover-image and generates a stego-image. That stego-image then sent to the receiver without anyone else knowing that it contain the hidden message. The receiver can extract the message with or without stego-key that depends on the hidden scheme Audio steganography is one of the popular data hiding techniques that embeds secret data in audio signals. The secret data is hidden in a way that unauthorized persons are not aware of the existence of the embedded data and without altering the quality of the cover audio. Data hiding in audio signals has numerous applications such as protection of copyrighted audio signals, covert communication, hiding data that may influence the security and safety of governments and personnel Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. Embedding secret messages into digital sound is known as audio Steganography. Audio Steganography methods can embed messages in WAV, AU, and even MP3 sound files. For hiding secret information in Videos, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Digital video sometimes needs to be stored and processed in an encrypted format to maintain security and privacy. For the purpose of content notation and/or tampering detection, it is necessary to perform data hiding in these encrypted videos.

After that, PSNR and SNR ratio are calculated. As well as In Image Steganography, JPEG Image and BMP or PNG image comprise. In Audio Steganography, WAV File and AU sound file comprise. In Video avi file is use.

.

KEYWORDS – Steganography, cover-image, generates a stego-image, WAV, AU, and even MP3 sound files, PSNR and SNR ratio, Image and BMP or PNG image.

I. INTRODUCTION

Steganography entails the art of writing concealed messages in such a manner that only the sender and the intended receiver are aware of the presence of the message. After the unprecedented technological advancement that has taken place over the years and in particular with the era of internet technology that is now commonly used for communication, it can be explained that there is a need to ensure that measures are put in place so that in-formation that is sent from one party to another is secure. Indeed, such an approach would entail encryption and concealing of messages inside an image file, audio file or both types offiles. There are Four Types of Steganography: Text

Steganography, Image Steganography, Audio Steganography and Video Steganography. Hiding information in text is the most important and basic method of Steganography.

II. PREVIOUS WORK FOR TEXT HIDING IN MULTIMEDIA

Information security is becoming very important part of our life now-a-days. Information hiding is the fundamental of information security. Information hiding can be achieved by steganography as well. LSB modification and phase encoding technique are very primitive in steganography. An effective audio steganographic scheme should possess the following three characteristics: Inaudibility of distortion (Perceptual Transparency), Data Rate (Capacity) and Robustness. These characteristics (requirements) are called the magic triangle for data hiding. This method of LSB modification of Steganography is the least secure. That methods security lies on the presumption that no other parties are aware of this secret message [1].

These techniques are more useful for detecting the stego images as well as the image media relating to security of of images and embed the data for complex image area and easily estimate the high embedding rate by using the quantitative steganalytic technique.Steganography is a technique that allows the one to hide the data within an image while adding few noticeable changes.and also explores the steganography methods Image steganography,audio steganography, video steganography, text steganography that are used to embed the information in digital carriers[2].

the text message is encoded using Huffman coding method and entrenched into audio file using LSB algorithm.after that The result is then put into a new audio file and thereafter contrasted through the use of various values that include; PSNR (peak signal to noise ratio), and SNR (signal to noise ratio). The frequency of audio file prior and after entrenched text message is schemed[3].

the capacity and complexity of steganography properties are satisfied.In addition to that, the suggested method for hiding is robust against noise. It is also considered highly secure since data is encrypted using RSA algorithm before embedding data which makes the system secure especially against passive attack. Hiding information inside audio files becomes a challenging discipline, since the Human Auditory System (HAS) is highly sensitive.The bits of information was hidden between frames (BF) in MP3 File[4].

each audio sample is converted into bits and then the textual information is embedded in it. In embedding process, First the message character is converted into its equivalent binary. The last 4 bits of this binary is taken into consideration and applying redundancy of the binary code the prefix either 0 or 1 is used. To identify the uppercase, lower case, space,and number the control symbols in the form of binary is used. and also 16bitWAV and 8bit WAV audio File are supported and the secret message can be hidden in the audio File with less storage capacity[5].

MKA Modified Kekre’s Algorithm improves the capacity as well as PSNR value of the image by a great value and is much better than the LSB technique. MKA is applied to color images. PVD is also a good steganography technique and improves the capacity and quality in case of grey scale images. Limitation of the PVD is that it cannot be applied to color images. Before embedding the secret bits and can preprocess them in such a way that their numbers are reduced. The reduced bits of the secret data can give the actual secret data by performing reverse operation of the preprocessing. By doing this the data hiding capacity is increased without degrading the quality of the stego image[6].

Steganography might also become limited under laws, since governments already claimed that criminals use these techniques to communicate.

III. PROBLEM STATEMENT

Information hiding is a part of information Security. Steganography is a technique of information hiding that focuses on hiding the existence of secret messages. Multimedia data, especially images have been increasing every day. Because of their large capacity, storing and transmitting are not easy. Data hiding in encrypted videos is important to conquer the aim of content annotation, copy right protection, access control and/or tapering detection.

IV. PROPOSED SOLUTION

Hiding Text in multimedia by Huffman Encoding Algorithm using Steganography:

A. Hiding Text in Image

- Loop through the pixels of the image. In each iteration to get the RGB values separated each in a separate integer.
- For each of R, G, and B, makes the LSB equals to 0. These bits will be used in hiding characters.
- Encrypt the compressed data using AES algorithm.
- Get the current character of encrypted data and convert it to integer. Then hide its 8 bits in R1, G1, B1, R2, G2, B2, R3, G3, where the numbers refer to the numbers of the pixels. In each LSB of these elements (from R1 to G3), hide the bits of the character consecutively.
- When the 8 bits of the character are processed, jump to the next character, and repeat the process until the whole text is processed.
- The text can be hidden in a small part of the image according to the length of that text. So, there must be something to indicate that here we reached the end of the text. The indicator is simply 8 consecutive zeros. This will be needed when extracting the text from the image.

B. Hiding Text in Audio

Least significant bit (LSB) coding is the way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. Among many different data hiding techniques proposed to embed secret message within audio file, the LSB data hiding technique is one of the safest methods for inserting data into digital signals in noise free environments, which merely embeds secret message-bits in a subset of the LSB planes of the audio stream.

The following steps are:

a) Receives the audio file in the form of bytes and converted in to bit pattern.
b) Encrypt the compressed data using AES algorithm
c) Each character in the encrypted message is converted in bit pattern.
d) Replaces the LSB bit from audio with LSB bit from character in the message.

This proposed system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. This proposed system will not change the size of the file even after encoding and also suitable for any type of audio file format. Encryption and Decryption techniques have been used to make the security system robust. Low-bit encoding embeds secret data into the least significant bit (LSB) of the audio file. The channel capacity is 1KB per second per kilohertz (44 kbps for a 44 KHz sampled sequence). This method is easy to incorporate.

C.Hiding Text in Video

The main high resolution AVI fie is nothing but a sequence of high resolution image called frames. Initially system will stream the video and collect all the frames in bitmap format and also collect the following information:

a. Starting frame: It indicates the frame from which the algorithm starts message embedding.

b. Starting macro block: It indicates the macro block within the chosen frame from which the algorithm starts message embedding.

c. Number of macro blocks: It indicates how many macro blocks within a frame are going to be used for data hiding. These macro blocks may be consecutive frame according to a predefined pattern. Apparently, the more the macro blocks we use, the higher the embedding capacity we get. Moreover, if the size of the message is fixed, this number will be fixed, too. Otherwise it can be dynamically changed.

d. Frame period: It indicates the number of the inter frames, which must pass, before the algorithm repeats the embedding. However, if the frame period is too small and the algorithm repeats the message very often, that might have an impact onto the coding efficiency of the encoder. Apparently, if the video sequence is large enough, the frame period can be accordingly large. The encoder reads these parameters from a file. The same file is read by the software that extracts the message, so as both of the two codes to be synchronized.

After streaming the AVI video file into AVI frames system will use the conventional LSB replacement method. LSB replacement technique has been extended to multiple bit planes as well. LSB replacement involving more than one least significant bit planes is less detectable than single bit plane LSB replacement. Hence the use of multiple bit planes for embedding has been encouraged. But the direct use of 3 or more bit planes leads to addition of considerable amount of noise in the cover image. Still proposed systems works on high resolution video system will get the RGB combination of each pixel.

V. CONCLUSION

In the Proposes steganographic system, Compress ratio is calculated by Huffman Encoding Algorithm. after that Text is hide in image, audio and Video by Least Substitution Method (LSB) and Encrypt by Using Advanced Encryption Standard Algorithm. On the another Hand Receiver receive that that hiding image, audio as well as Video as appear Original Image. After that Receiver Decrypt that Text by using Advanced Encryption Standard Algorithm (AES) and getting Text which is hide by Sender in image, audio as well as video.

REFERENCES

[1] Prof.Samir Kumar and BandyopadhyayBarnali and Gupta Banik,“LSB Modification and Phase Encoding Technique of Audio Steganography Revisited”,International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 4,June 2012.

[2] Shaveta Mahajan and Arpinder Singh,“A Review of Methods and Approach for Secure Stegnography”,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10,October 2012.

[3] Adel A. Sewisy and Romany F. Mansour and S. Z. Rida and Amal A. Mohammed,Hidden Text into Audio Files,International Journal of Research Studies in Science, Engineering and Technology Volume 2, Issue 5,May 2015.

[4] Mohammed Salem Atoum and Osamah Abdulgader Al- Rababah,Alaa Ismat Al-Attili,“New Technique for Hiding Data in Audio File”,IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.4,April 2011.

[5] K.P.Adhiya and Swati. A. Patil,”Hiding Text in Audio Using LSB Based Steganography”,Information and Knowledge Management www.iiste.org ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol 2, No.3,2012.

[6] Mukesh Garg and A.P. Gurudev Jangra,“An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques”,International Journal of Advanced Research in Computer Science and Software Engineering,January 2014.