www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume -5 Issue - 3 March, 2016 Page No. 15996-16000

Secure Data Hiding in Audio-Video Steganalysis by Anti-Forensic Technique

Dimple Lalwani[1], Manasi Sawant[2], Mitali Rane[3], Vandana Jogdande[4] , S.B.Ware[5]

Sinhgad Institute of Technology, Lonavala
dimple.lalwani123@gmail.com
[2]Sinhgad Institute Of Technology, Lonavala
Manasisis1000@gmail.com
Guided By: Miss. S.B.Ware (SIT IT, Lonavala)

Abstract: Steganography is used to encrypt any secret information like password, text and picture, audio behind original cover file. Original message is converted into cipher text by using mystery key and then hidden into the LSB of original image. The current work signifies cryptostegnography of audio and video which is the combination of image steganography, audio and video steganography by making use of Forensics Technique as a tool for authentication. The main aim is to hide secret data behind image and audio of video file. As video is the utilization of many still frames of images and audio, thus for hiding secret information any frames can be selected for audio and video. Suitable algorithm such as AES for security and authentication image processing is used, hence data security can be increased. And for data embedding, use 4LSB algorithm

1. Introduction

Pure Steganography is defined as a stenographic system the exchange of a cipher is not needed such as a stego key. There is two input, carrier object and message object. The steganographic calculation is utilized to implant message object onto transporter object [3]. The primary criteria for this embedding is no outsider spectator can see, listen or suspect about the message. It ought to be lie in mystery. Distinctive sort of item can be utilized as transporter and message object. It can be Image, Text, sound and and video. But it cannot send large data through this method [2]

Steganography is the method of hiding any secret information such as text and image, and passwords audio behind original cover file. Cipher text by using secret key and then hidden into the LSB of original image is converted into Original Message [6]. The audio-video cryptostegnography is present in proposed system which is the combination of image steganography and audio steganography using Forensics Technique as a tool to authentication [1]. The main aim is to hide secret information behind image and audio of video file. As many still frames of images and audio are applications of video file, it can select any frame of video and audio for hiding our secret data. Suitable [5] algorithm such as AES is used for image steganography suitable parameter of security and authentication hence data security can be increased. And for data embedding, use 4LSB algorithm [4].

This paper focuses the idea sending large data.

I. Related work

Previously, cryptography was used for encryption of data and provides data security. But actually term cryptography provides privacy. Security is the thing that you require when you utilize your charge card on the Internet — you don't need your number uncovered to general society. For this, you utilize cryptography, and send a coded heap of hogwash that just the site can decode. In spite of the fact that your code might be unbreakable, any programmer can look and see you've communicated something specific. To conquer this disadvantage steganography is utilized for sending information like picture and sound and make covered up. Steganography is proposed to give mystery. Steganography approach that makes utilization of Least Significant Bit (LSB) calculation for inserting the information into the bit map picture (.bmp). This methodology is to supplant the information of loiter piece in a spread sound information by a mystery information.

Our framework is composed by utilizing 32-bit ARM controllers for outlining prescient model for picture and sound steganography system. The proposed technique will secure the substance with in the picture and encryption of sound record with in the picture will make the report much securer in light of the fact that despite the fact that if the unapproved individual succeeds in having the capacity to hack the picture, the individual won't ready to peruse the message also gain the data in the sound document. Mystery information like picture and sound is scrambled by spread information included with LSB calculation on ARM architecture device by adding to application [5].

I. EXISTING SYSTEM

Paper Name: Visual Cryptographic Steganography in Images.

In existing system investigated adaptive mechanisms for transform-domain of high-volume data hiding in MPEG-2 video which can be tuned to sustain varying levels of compression attacks. Uncompressed domain by scalar quantization index modulation (QIM) on a selected set of low-frequency DCT coefficients the data is encrypted (hidden). It propose an hiding scheme that is adaptive where the embedding rate changes according to the type of frames and the reference quantization parameter (decided according to MPEG-2 rate control scheme) for that frame. For a 1.5 Mbps video and a frame-rate of 25 frames/sec, It is to embed almost 7500 bits/sec. Also, 20% more data is hidden in adaptive schemes and incurs significantly less frame errors than the non-adaptive scheme [8].

A Steganography technique that is used to hide messages in multimedia objects has been proposed. This is largely due to the fact of significantly large amounts of stego-data by means of simple and subtle modifications that preserve the perceptual content of the underlying cover object. Hence they have been found to be perfect candidates for use as cover messages. A message, either encrypted (hidden) or decrypted, can be hidden in a computer video file (containing the picture of, for instance, an innocent 2 year old baby) and transmitted over the Internet, a CD or DVD, or any other medium. the file can contain images on receipt, which can be used for extracting hidden messages.

Stegnographic Techniques:

1) Steganography that is physical has been widely used. In ancient time people used to write the messages that also on woods and cover it with wax. Message was written on the back of postage stamps. Message was written on paper by inks that are invisible or secret.

2) Digital Steganography is the art of invisibly hiding data within data. It conceals the fact that actual messages are hidden. In this, secret data can be hidden inside the image, text, sound clip which can be represented in binary.

3) Printed Steganography Digital Steganography output can be in the form of documents that could be printed. The letter size, spacing and other characteristics of a cover text can be manipulated for the hidden message to be carried. A receiver who knows the technique used can recover the message and then decrypt

MODULES:

INPUT MODULE:

Input Module is designed such a way that the proposed system handles any type of data formats, such as if the user wants to hide any image format then it must be easily adjusted with all usual image formats such as jpg, gif ,bmp, it is compatible with video formats such as .avi, .flv, .wmf etc. And also it must be also contain various document formats, so that the user can be able to user any formats to hide the secret data.

ENCRYPTION MODULE:

In Encryption module, it consists of file part that is Key, Where key file can be is given with the password with security in it. Then the User can enter data or else it can upload the data also Through the browse button, when it clicks the open file dialog box is Opened and where the user can select the secret message. Then The user selects the video through another. When the cover file button is clicked or image the open file dialog box is opened. Where the user has to first select the cover file and then click hide button so that the secret data or Using Forbidden Zone Data Hiding Technique the message is Hidden in cover file.

DECRYPTION MODULE:

This module is the opposite of Encryption module where same as that of encryption part the key file also should be specified. Then the user should select the encrypted the original file(cover file) and then extract button is to be selected so that the hidden message is displayed in the text area it is extracted to the place where the user specifies it or else it is specified in application.

DES:

DES module by using DES algorithm it contains similar Encryption and Decryption part. The Data Encryption Standard (DES) is a block cipher that uses shared secret encryption.

TRIPLE DES:

The module consists of same as Encryption and Decryption part using Triple DES algorithm. Triple DES is the name that is common for the Triple Data Encryption Algorithm block cipher, which is used to apply the Data Encryption Standard (DES) cipher algorithm three times to each data block.

RSA:

RSA module it consists of same as Encryption and Decryption part using RSA algorithm. RSA it is the first algorithm suitable for (hiding) that is encryption of data and signing as well, and it has great advances in public key cryptography. RSA is frequently used in electronic commerce protocols, and is believed to be sufficiently secure given sufficiently long keys and the use of up-to-date implementations.

I. System architecture with explanation

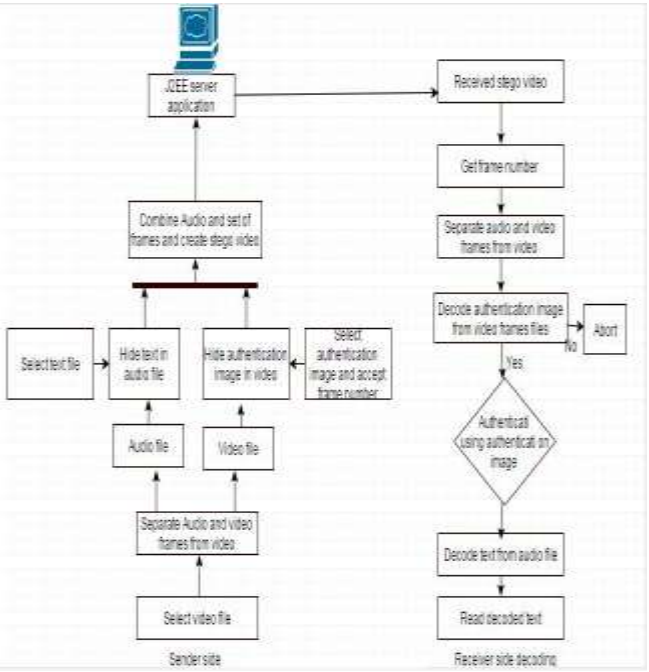


Fig shows the System architecture of the proposed method. The paper discusses the cryptography's combination with steganography that is adaptive for video and audio sequence with algorithm that is chaotic as the algorithm used for encryption. As there is an increase in encryption the PSNR value also gets increased. The author discusses different methods for audio steganography and LSB is found to be a secured method. The paper explains the advanced chaotic algorithm for the encryption and decryption purpose and it consumes minimum time and fewer complexes. The paper discusses the different methods are there for audio and video steganography such as echo hiding, parity hiding, phase coding and their comparison. Author explains how to encrypt an image in AVI video using 4LSB method. Security techniques find parameters such as frame no, width and height of the image, before and after hiding PSNR and Image histogram. If all the Verification of parameters is correct then the data is send to receiver.

I. Mathematical Model

S is the Whole System Consist of

S= {I, P, O}

I = Input.

I = {AF, VF,}

AF = Audio File.

VF = Video File.

P = Process

P = { 4LSB, phase coding algo., LSB}

4LSB = Is used for image steganography.

Phase coding: Is used for audio steganography.

LSB = Least Significant Bit: use of (LSB)algorithm for embedding the data into the bit map image (.bmp).

Step1:selecting audio-video file.

Step2:video steganography.

Step3: Creating stego audio file.

Step4:Authentication (at receiver side). Step5: Audio recovery.

Step6:computer forensics and authentication.

I. Enhanced Proposed Algorithm

A. Phase Encoding:

Step1: The original sound signal (C) is segmented to extract the header.

Step2: The rest portion to is broken up into smaller segments whose lengths equal the size of the message to be encrypted.

Step3: For creating matrix of phase it is applied to each segment using DFT.

Step4: The vector phase of the first signal segment in this the secret message is inserted as follows:

Step5: By using the segment which is first of the new phase and the original phase matrix the new phase matrix is created.

Step6: The inverse DFT is applied to reconstruct the sound signal by using new phase matrix and then the sound segments with original header is concatenated.

B. LSB Modification:

Step1: Select a.warfile (Input file) as a Carrier and a text as message.

Step2: Open Carrier file.

Step3: Prepare message text as a binary column vector of 8.

Step4: Skip first 44 bytes of carrier which is address part of wav file.

Step5: Prepare rest bytes of carrier as a matrix of 8 columns.

Step6: Replace least significant bit of carrier matrix with corresponding element of message vector.

Step7: Get the Stego file as output.

C. Data Hiding using 4LSB Algorithm:

LSB inserts bits of embedded message into Least Significant bits of pixel. LSB (Least Significant Bit) substitution is used in the carrier image for adjusting Least Significant Bit Pixel. It is easy approach for hiding message into the image. The LSB insertion changes according to number of bits in an image. By taking the advantage of human vision system Video displays sequence of images at a faster rate .An extremely simple steganography method is to hide the information at pixel level.

1)Each image or frames is made up of no.of individual pixels. In an image each pixels are made up of a string of bits the 4 least significant bit of 8-bit true color image is used to holds our secret message image of 4 bit by overwriting the data that was already there.

2) In hiding process, the last 4 bits of frame or image pixel is replaced with secret data of 4 bit.

3) Sequence of bytes is broken down into set of 4 bits for Secret Data. To hide each character of secret message it needs two pixels. So it can hide in (mx m) image in number of characters is given by the following equation.

Total size of 1 equation /8 ---------- (1)

4)Suppose size of a one frame is 160KB,For 1 LSB, the Max data that it can hide is 1×20KB = 20 KB. For 2 LSB it can be 2×20KB=40KB. For 3LSB it can be 3x20=60KB. For 4 LSB it can be 4×20KB =80KB. If process of steganography go beyond 4LSB, i.e. for 5 LSB it can be 5×20KB=100 KB, That means it can hide more than 50% of data, hence it is look like visible watermarking.

5) Proposed method is using 4LSB algorithm for implementing steganography. In LSB for any data change it does not change the value of data significantly.

D.AES Algorithm

The AES-256 algorithm is composed of three main parts: Cipher, Inverse Cipher and Key Expansion. Data is converted to an unintelligible form by using Cipher called cipher text while Inverse, data is converted back into its original form called plaintext by Cipher. Key Schedule is generated by key Expansion that is used in Cipher and Inverse Cipher procedure. Specific number of rounds is composed in Cipher and Inverse Cipher For both its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four different byte-oriented transformations:

1) Substitution table (S-box) used in Byte Substitution
2) Rows of the State array are shifted by different offsets
3) Each column of the State array within which data is mixed
4) In State Round Key is added

The Cipher transformations can be inverted and to produce a straightforward Inverse Cipher it is implemented in reverse order for the AES algorithm. The individual transformations used in the Inverse Cipher.

1) Shift Rows are Inversed
2) Sub Bytes are Inversed
3) Mix Columns are Inversed
4) Round Key is added

Key expansion module is present in AES Inverse Cipher, a key reversal buffer, an initial permutation module, a round permutation module and a final permutation module. The key reversal buffer first store keys for all rounds and shows them in reverse order to the rounds. The round permutation module will loop maternally to perform 14 iterations (for 256 bit keys).

E. Forbidden Zone Data Hiding

Here each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. To transform cipher text back into the original plaintext using the same encryption key a set of reverse rounds are applied.

1. Video sequences in data hiding are performed in two major ways: bit stream-level and data-level.

2.It proposes a new selective embedding type block based data hiding framework that encapsulates Forbidden Zone Data Hiding (FZDH)

By Applying simple rules to the frame markers, we provide certain level of robustness against frame drop, repeat and insert attacks

I. IMPLEMENTATION AND RESULT

A. Input:-

Here, Whole System taken many more attribute for the input purpose but here author mainly focuses on the Time and performance of system.

B. Expected Result:-

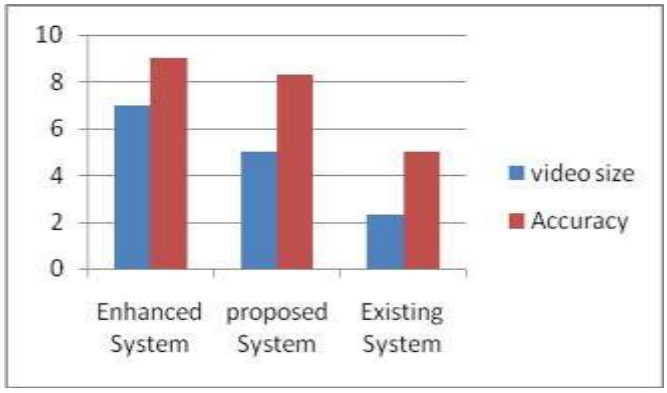
1. Compare Existing Vs Proposed w.r.t Performance

a. Tabular Representation:

Methodology	Video size	Accuracy
Enhanced proposed System	7	9

Enhanced proposed System	7	9
Proposed System	5	8.3
Existing	2.3	5

b. Graphical Representation:

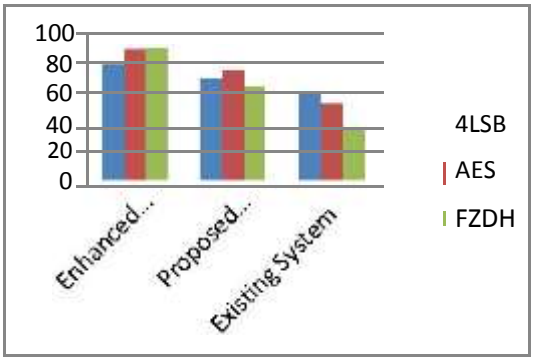


1. Compare Existing Vs Proposed w.r.t. Algorithm

a. Tabular Representation:

Methodology	4LSB	AES	FZDH
Enhanced proposed System	80%	90%	90.6%
Proposed System	70%	76%	65%
Existing System	60.5%	52.5%	35%

b. Graphical Representation:



CONCLUSION

It is hiding an encrypted secret image and data behind a video frame using 4LSB method and in audio file using LSB method with location identification. It obtained satisfactory result in both audio and video steganography. It embedded encrypted image successfully into a selected frame and the PSNR value bitten original and encrypted image also found out which is found to be in the range of 10 to 40 dB according to the size of image and size of video. This proposed method can also withstand different attacks and thus a very strong and secure method of data hiding can be obtained. The histogram and spectrograph of both image steganography and audio steganography are also obtained which looks identical before and after hiding.as the PSNR value increases the data security also increases.

ACKNOWLEDGEMENT

I might want to thank the analysts and also distributers for making their assets accessible. It additionally appreciative to commentator for their significant recommendations furthermore thanks the school poitrs for giving the obliged base and back.

AUTHOR PROFILE

Dimple Lalwani
Pursuing B.E in field of I.T from Sinhgad Institute of Technology, Lonavala.

Manasi Sawant
Pursuing B.E in field of I.T from Sinhgad Institute of Technology, Lonavala.

Mitali Rane
Pursuing B.E in field of I.T from Sinhgad Institute of Technology, Lonavala.

Vandana Jogdande
Pursuing B.E in field of I.T from Sinhgad Institute of Technology, Lonavala.

REFERENCES

[1] N. Provos and P. Honeyman, "Hide and seek: An introduction to Steganography", *IEEE Conference on Security and Privacy*, pp. 32-44, 2003.

[2] Fangjun Huang, Jiwu Huang, and Yun-Qing Shi, ―New Channel Selection Rule for JPEG Steganography‖, *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 4, pp. 1181-1191 August 2012.

[3] Avinash Srinivasan, Srinath Thirthahalli Nagaraj, and Angelos Stavrou, ―HIDEINSIDE – A Novel Randomized & Encrypted Antiforensic Information Hiding‖, *International Conference on Computing, Networking and Communications, Communications and Information Security*, 2013.

[4] Hung-Min Sun, Chi-Yao Weng, Chin-Feng Lee, and Cheng-Hsing Yang, " Anti-Forensics with Steganographic Data Embedding in Digital Images ", *IEEE Journal on selected areas in Communications*, Vol. 29, No. 7, pp. 1392-1403, 2011.

[5] C.C. Chang, P. Tsai, and M.H. Lin, ―An Adaptive Steganography for Index- based images using Codeword Grouping‖, *Advances in Multimedia Information Processing-PCM, Springer*, Vol. 3333, pp. 731–738, 2004.

[6] ―Peak Signal to Noise Ratio (PSNR)‖ from Wikipedia http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio.

[7] Moh Zan and Nyein Aye," A Modified High Capacity Image Steganography using Discrete Wavelet Transform", *International Journal of Engineering Research & Technology* (IJERT), Vol. 2,No. 8, pp. 2712-2715, August - 2013.

[8] Piyush Marwaha and Paresh Marwaha," Visual Cryptographic Steganography in Images", *Second International conference on Computing, Communication and Networking Technologies*,2010.