Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 5, May -2017

Application of data hiding in Audio-Video images Using Anti Forensic Technique for authentication and Data Security .

Aakash Deogaonkar[1], Anali Inamke[2], Aishwarya Kadam[3], Diksha Marathe[4], Prof A.S.Narote[5]

[1,2,3,4,5] Dept.Of IT, Smt. kashibai Navale College Of Engineering,Pune,Maharashtra,India

Abstract — *Steganography is the method of hiding any secret information like password, text and image, audio behind original cover file. Original message is converted into cipher text by using secret key and then hidden into the LSB of original image. The proposed system provides audio-video cryptostegnography which is the combination of image steganography and audio steganography using Forensics Technique as a tool to authentication. The main aim is to hide secret information behind image and audio of video file. As video is the application of many still frames of images and audio, we can select any frame of video and audio for hiding our secret data. Suitable 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 we use 4LSB algorithm.*

Keywords: 4LSB,Hidding,stegnography,cryptography,AES.

I. INTRODUCTION

Pure Steganography is defined as a steganographic system that does not require the exchange of a cipher such as a stegokey. There is two input, carrier object and message object. The steganographic algorithm is used to embed message object onto carrier object. The main criteria for this embedding is no third party observer can see, listen or suspect about the message. It should be lie in secret. Different type of object can be used as carrier and message object. It can be Image, Text, audio and video. But we can not send large data through this method. Stegnography is the method of hiding any secret information like password, text and image, audio behind original cover file. Original message is converted into cipher text by using secret key and then hidden into the LSB of original image. The proposed system provides audio-video cryptostegnography which is the combination of image steganography and audio steganography using Forensics Technique as a tool to authentication. The main aim is to hide secret information behind image and audio of video file. As video is the application of many still frames of images and audio, we can select any frame of video and audio for hiding our secret data. Suitable 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 we use 4LSB algorithm. This paper focus the idea sending large data .

II. LITERATURE SURVEY

Sr. No.	Paper Name	Author Name	Publishing year	Description	Drawback
1	Data Hiding in H- 264 Encoded Video Sequences	S. K. Kapotas, E. E. Varsaks	**2010**	A new method for high capacity data hiding in H.264 streams is presented. The proposed method takes advantage of the different block sizes used by the H.264 encoder during the inter prediction stage in order to hide the desirable data. It is a blind data hiding scheme	Building such type of architecture is very time consuming.
2	Adaptive MPEG-2 Video Data Hiding Scheme	A. Sarkar, U. Madhow	**2005**	. We propose an adaptive hiding scheme where the embedding rate is varied according to the type of frame and the reference quantization parameter (decided according to MPEG-2 rate control scheme) forthat frame..	This project gives a less performance.
3	Robust image-adaptive data hiding using erasure and error correction	Solanki, N. Jacobsen	**1997**	we propose practical realizations of this prescription for data hiding in images, with a view to hiding large volumes of data with low perceptual degradation. The hidden data can be recovered reliably under attacks, such as compression and limited amounts of image tampering and image resizing	Accuracy of is not up to the mark.
4	Correction of Insertions and Deletions in Selective Watermarking	M. Schlauweg, D. Profrock,	**2010**	We analyze these techniques, which can be separated into three approaches, namely concatenated coding, dynamic gramming, and punctured channel coding. As demonstrated, the latter one fails to correct de-synchronization in second generation watermarking schemes, if the number of selected embedding locations is much smaller than the number of host signal samples. In this paper, we propose a new method that outperforms all other methods presented so far concerning insertion/deletion error correction in second generation watermarking schemes.	Computation cost is high

III. PROPOSED SYSTEM

In this paper, proposed Information security using data hiding audio video stegnography with the help of computer forensic techniques provides better hiding capacity we have worked on hiding image and text behind video and audio file

and extracted from an AVI file using 4 least significant bit insertion method for video steganography and phase coding audio stegnography. Stegnography is the method of hiding any secret information like password, text and image, audio behind original cover file. Original message is converted into cipher text by using secret key and then hidden into the LSB of original image. The proposed system provides audio-video cryptostegnography which is the combination of image steganography and audio steganography using Forensics Technique as a tool to authentication. The main aim is to hide secret information behind image and audio of video file. As video is the application of many still frames of images and audio, we can select any frame of video and audio for hiding our secret data. Suitable 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 we use 4LSB algorithm.

IV. SYSTEM ARCHITECTURE

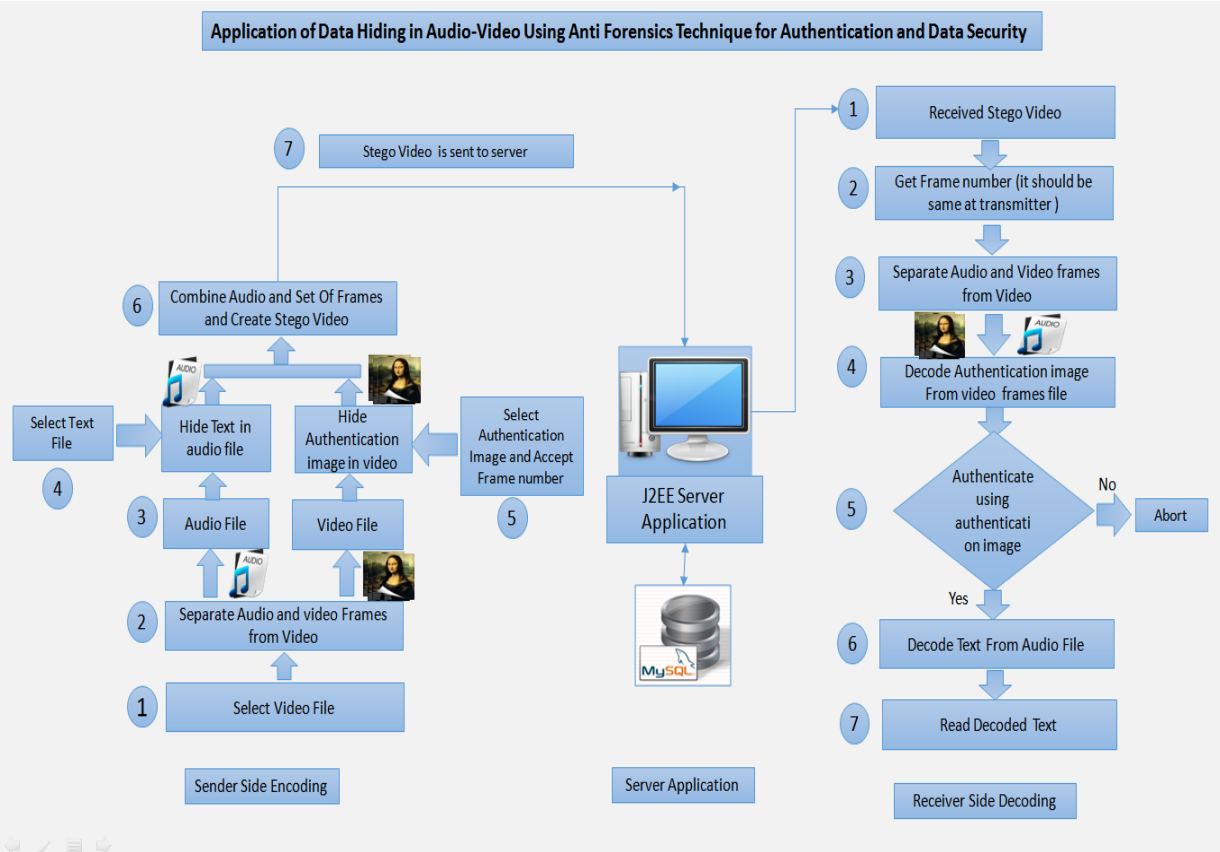

Fig. 1 System Architecture

V. ENHANCED PROPOSED ALGORITHM.

Data Hiding using 4LSB Algorithm:

The idea of the LSB algorithm is to insert the bits of the hidden message into the least significant bits of pixels. LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. The Least Significant Bit insertion varies according to number of bits in an image. Video is a sequence of images displayed at faster rates taking the advantage of human vision system .An extremely simple steganographic method is to hide the information at pixel level.

1) Each frame or image is made up of no.of individual pixels .Each of these pixels in an image is made up of a string of bits the 4least significant bit of 8-bit true color image is used to hold 4-bit of our secret message image by simply overwriting the data that was already there.
2) In hiding process, the last 4 bits of image or frame pixel is replaced with 4 bits of our secret data.

3) For this secret data which is also sequence of bytes are broken down into set of 4 bits. To hide each character of secret message we need two pixels. So the number of characters that we can hide in (mx m) image is given by the following equation.
Total size of one frame ÷ 8 ---------- (1)

4) Suppose size of a single frame is 160KB, then for 1LSB, maximum data that can be hidden is 1×20KB = 20KB. For 2LSB it is 2×20KB = 40KB. For 3LSB it is 3x20=60KB. For 4LSB it is 4×20KB =80KB. If steganographic process go beyond 4LSB, i.e. for 5LSB it is 5×20KB=100 KB, means that size of the data can be hide is more than 50%, hence it is look like visible watermarking.
5) For implementing steganography proposed method is using 4LSB algorithm. Any data change in least significant bit does not change the value of data significantly.

THE AES ALGORITHM .

The AES-256 algorithm is composed of three main parts: Cipher, Inverse Cipher and Key Expansion. Cipher converts data to an unintelligible form called cipher text while Inverse Cipher converts data back into its original form called plaintext. Key Expansion generates a Key Schedule that is used in Cipher and Inverse Cipher procedure. Cipher and Inverse Cipher are composed of specific number of rounds For both its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four different byte-oriented transformations:
1) Byte substitution using a substitution table (S-box)
2) Shifting rows of the State array by different offsets
3) Mixing the data within each column of the State array
4) Adding a Round Key to the State

The Cipher transformations can be inverted and then implemented in reverse order to produce a straightforward Inverse Cipher for the AES algorithm. The individual transformations used in the Inverse Cipher.
1) Inverse Shift Rows
2) Inverse Sub Bytes
3) Inverse Mix Columns
4) Add Round Key

The AES inverse cipher core consists of a key expansion module, 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 the presents them in reverse order to the rounds. The round permutation module will loop maternally to perform 14 iterations (for 256 bit keys).

VI. MATHEMATICAL MODEL

Let 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 codingalgo., 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.

VII. CONCLUSION

In this paper, proposed Information security using data hiding audio video stegnography with the help of computer forensic techniques provides better hiding capacity we have worked on hiding image and text behind video and audio file and extracted from an AVI file using 4 least significant bit insertion method for video steganography and phase coding audio stegnography. We are hiding encrypted data using stegnography and cryptography behind selected frame of video using 4LSB insertion method.

VIII. RESULT ANALYSIS

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

   a. Tabular Representation:

Methodology	Video size	Accuracy
Enhanced proposed System	7	9
Proposed System	5	8.3
Existing	2.3	5

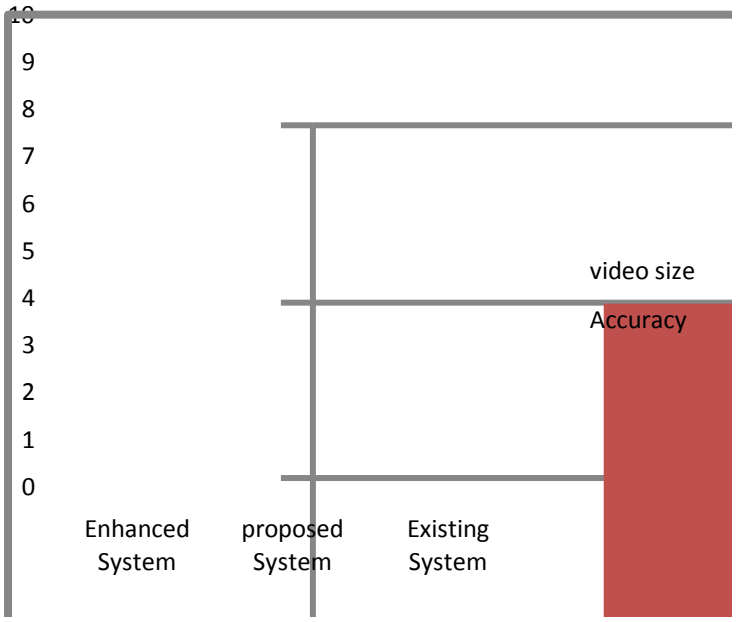

Table 1 Existing Vs Proposed System

Acknowledgment

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

REFRENCES

[1] Shoji Sakurai, Shinobu Ushirozawa, "Input Method against Trojan Horse and Replay Attack "Information Theory and Information Security (ICmS), pp.3S4-3S9, Jan 2010.

[2]Ken Birman. "In Computers We Trust" Distributed Systems Online, Dec200S.

[3]MicroSoft Security Intelligence Report http://www.microsoft.comlsecurity/sir/keyfindings/default.aspx

[4] J.Hursti, "Single Sign-On", in Proceeding of Helsinke Univ of Technology, Seminar on Netwokr Security, 1997.

[S]Aloul.F, Zahidi.S, EI-Hajj.W "Two factor authentication using mobile phones" Computer Systems and Applications(AICCSA 2009), pp. 641644,May 2010

[6] A. Vapen, D. Byers, and N. Shahmehri, "2-c1ickAuth – optical challenge-response authentication," in Proc. Conference on Availability,Reliability and Security (ARES), 2010.

