ISSN(Online) : 2319 -8753
ISSN (Print) : 2347 -6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

Video Steganography by Using Statistical Key Frame Extraction Method and LSB Technique

Nishi Khan[1], Kanchan S. Gorde[2]

P.G. Student, Department of Electronics Engineering, Terna Engineering College, Nerul, Navi Mumbai, India[1]

Professor, Department of Electronics Engineering, Terna Engineering College, Nerul, Navi Mumbai, India[2]

ABSTRACT:Steganography is the fine art and science of sending concealed messages such that the presence and nature of such a message is only known by the sender and anticipated recipient. Security of documents through digital media is of great concern today because of attacks, exploitation or unauthorized access of information. Steganography is the skill of hiding message inside a multimedia block. Use of DCT coefficients, DWT ,LSB, etc., are some of the known techniques for this, but they have some or the other drawback of losing crucial information. Video Steganography deals with hiding secret information within a video. In this paper we have proposed an advanced approach for dynamic data protection in which we have used key frame extraction technique. In this the cover-video is divided into frames. From these frames, key frames are extracted using statistical features such as standard deviation, skewness and kurtosis. Secret message in binary form is embedded into key frames of stego video using LSB technique and hybrid approach in such a manner that the video does not lose its functionality. Text message is encrypted by means ofAES algorithm. As key frame extraction technique is completely new in video steganography so it becomes impossible for interloper to estimate that a text message is hidden in the video. The proposed system is simple and new and therefore can be used to transfer extremely confidential data like military secrets, hospital reports and other data.

KEYWORDS:Data Hiding, Key frame extraction, Video Steganography, LSB, AES

I. INTRODUCTION

Steganography is a Greek word which means the covered writing. Mainly Steganography is known as “invisible” communication as it hides the mere presence of the secret data. This paper provides some important information about steganography which will help us in data hiding field. Application of Steganography varies from military, industrial applications to copyright and Intellectual Property Rights (IPR). By means of lossless steganography techniques messages can be sent and received securely. Steganography helps in embedding of messages in the cover media, authentication, and copyright protection. This paper is divided into different section in which we explain steganography in digital mediums, its characteristics, related work, proposed mechanism, some related methodology and conclusion.

II. STEGANOGRAPHY IN DIGITAL MEANS

Depending on the type of the cover object, there are many suitable steganography techniques which are followed in order to obtain security.

A. *Image Steganography*: Considering the cover object as image in steganography, it is known as image steganography. Generally, in this technique pixel intensities are used to hide the information.

B. *Network Steganography*: When taking cover object as network protocol, such as UDP, TCP, ICMP, IP etc, where protocol is used as carrier, is known as network protocol steganography. In the OSI network layer model, there exist secret channels where steganography can be achieved in unused header bits of TCP/IP fields.

C. *Video Steganography*: Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of images) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (e.g. 7.667 to 8) which is used to hide the information in each of the images in the video, which is not visible by the human eye. Video steganography uses such as H.264, Mp4, MPEG, AVI or other video formats.

ISSN(Online) : 2319 -8753
ISSN (Print) : 2347 -6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

D. *Audio Steganography*: When taking audio as a carrier for information hiding it is called audio steganography. It has become significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI, and MPEG for steganography.
E. *Text Steganography*: General technique in text steganography, such as number of tabs, capital letters,white spaces, just like Morse code is used to achieve information hiding.
F. *Steganography using puzzles:* This is the ability of concealing data in a puzzle can take advantage of the degrees of freedom in maintaining the puzzle, using the starting information to encode a key within the puzzle / puzzle image. For instance, steganography using Sudoku puzzles has as numerous keys as there are possible solutions of a Sudoku puzzle, which is 6.71×1021. This is equivalent to about 70 bits, making it much stronger than the DES method which uses a 56 bit key.

III. CHARACTERISTICS OF STRONG STEGANOGRAPHY

Though steganography's most obvious goal is to hide data, there are several other related goals used to judge a method's steganographic strength. These include:

- Capacity (how much data can be hidden)
- Invisibility (inability for humans to detect a distortion in the stego-object)
- Undetectability (inability for a computer to use statistics or other computational methods to differentiate between covers and stego-objects)
- Robustness (message's ability to persist despite compression or other common modifications),
- Tamper resistance (message's ability to persist despite active measures to destroy it), and
- Signal to noise ratio (how much data is encoded versus how much unrelated data is encoded).

Steganography would be strongest if the algorithms used to hide data were known and attackers still could not tell whether or not hidden data was present.

IV. STEGANOGRAPHY IN VIDEOS

Videos may use individual frames that flash by too quickly to be noticed, but contain secret information when viewed as still images. Video images may perhaps also be modified in essentially the same ways as still images, and since video files are bigger than single image files, more data could be hidden. Audio recordings may contain background "noise" that really contains a message, or could be altered in a way that, like the alteration of images discussed above, leaves the sound unchanged, but discloses a message when compared against the original audio file.

V. RELATED WORK

The most rudimentary way to hide data within a video file is in changing low order bits, which adaptscolor data slightly, but not in amanner visible to the human eye for some visual examples. This is called a least significant bit (LSB) alteration or modification.

In Hash based least significant bit technique [1], a spatial domain technique is used where the secret information is embedded in the LSB of the cover frames. A hash function is used to select the position of insertion in LSB bits. The proposed method is analysed 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. Image Fidelity (IF) is also measured and the results show minimal degradation of the steganographic video file.

In LSB based hybrid approach for video steganography [2], one or two or three LSB of each pixel in video frame are replaced and Advance encryption standard (AES) is applied.

In Video Steganography based on Integer Haar Wavelet Transforms for Secured Data Transfer [3], paper proposes a video steganography algorithm based on Haar Integer Wavelet Transforms (IWT) and Least Significant Bits (LSB) substitution for data hiding and extraction in Red Green Blue (RGB) components of the video files. In this approach, the cover-video is divided into RGB frames and the text in binary form is embedded into the LSBs of IWT coefficients.

ISSN(Online) : 2319 -8753
ISSN (Print) : 2347 -6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

The embedded text is extracted from stego-video using the reverse process of data hiding. The proposed system was implemented using Audio Video Interleave (AVI) files

In [4] Author is mainly concerned with how to embed data in a video file in from of bmp images and how we can make use of the internal structure of the video to hide data to be secured.

In [5] Based on similar concept with stenography, it is desired to maximize the amount of hidden information while preserving security against detection by unauthorized parties. The image based stenography issues has been illustrated to hide secret information in images and the possibility of using the image as a cover carrier for hiding secure data.

In [6] an image encryption algorithm combining the image encryption based on S-boxes scrambling with error correcting code was developed. The error correcting code could effectively improve the security of image encryption algorithm based on S-boxes scrambling. The basic concept of this author which we have used in my work focuses on maximizing security, and secures the data through AES.

In [7] author uses an algorithm based on AES expansion in which the encryption process is a bit wise exclusive or operation of a set of image pixels along with the 128 bit key, which changes for every set of pixel. The keys to be used are generated independently at the sender and receiver side based on AES key expansion process. Hence the initial key is shared rather than scaring the whole set of keys. The author gives the information about AES.

In [8] the author has proposed an AES technique which presents fundamental mathematics behind the algorithm along with a brief description of some cryptographic primitives that are commonly used in the field of communication security. AES provides better security and has less implementation complexity. It has emerged as one of the strongest and the most efficient algorithm.

In [9] author gave a different concept from above the authors using a new approach of hiding image in video. The algorithm is replacing 1 LSB of each pixel in video frame. It becomes very difficult for an intruder to guess that an image is hidden in the video as individual frame are difficult to analyze in a video running at 30 frames per second. We have seen that the author has used only 1 LSB substitution technique here. This is the basic concept of the author which is implemented in my research work.

In [10] Author has dealt with three main stenography challenges capacity, imperceptibility and security. This is achieved by hybrid data hiding scheme in corporate LSB technique with a key permutation method. In my work I have implemented this basic concept of using LSB substitution and the ways to increase the system performance as well as its security.

VI. THE PROPOSED MECHANISM

A. Proposed Algorithm

1) Embedding Algorithm:

- Input Video.
- Extract the frames of the given video.
- Using statistical features extract the key frames(K).
- Insert secret data in K-1 frame.
- The LSB position of each K-1 frame will be used to store the secret data.
- Store key frame index number in the LSB of the last frame of the video.
- Combine all the K-1 frames and key frames to generate the video sequence this is the Stego video i.e. encrypted video.

*secret data is the data from text file in binary format.

2) Extracting Algorithm:

- Input the Stego video.
- Extract the frames from the Stego video.
- Get the last frame and read the LSB to get the key frame index.
- Extract the K-1 frames based on the index of the key frame.
- Read the secret data from LSB of each K-1 frame.
- Combine the data read from each K-1 frame to get the secret message.

ISSN(Online) : 2319 -8753
ISSN (Print) : 2347 -6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

VII. METHODOLOGY

A. Algorithm of shot boundary detection

Many approaches used different types of features to detect shot boundary, including histogram, shape information, motion activity. Among these methods, histogram is the widely held approach. However, in these histogram-based approaches, pixels' space distribution was ignored. Different frames may have the same histogram. divided each frame into r blocks, and the difference of the corresponding blocks of sequential frames was computed by color histogram. The color histogram contains only the frequency of a color value, but loses the pace information of the pixels. Therefore, in order to get the spatial distribution information of the color, the image is usually divided into appropriate blocks. If the blocks of the image are too small, it cannot be partitioned. More image blocks can improve the spatial resolution of the image, but it also increases the storage space of the image characteristics..

Algorithm steps are as follows.

Step 1: Partition the frame into m*n blocks .B(i,j,k) stands for the block of i, j at the k^{th}frame.
Step 2: Computing x2 histogram matching difference between all blocks of single frame.
Step 3: Compute mean (MD), standard variance (STD), skewness (S) and kurtosis (k) for a single frame.
Step 4: Compute difference of these four values from two consecutive frames
MD=MDi-MD(i+1)
STD=STDi-STD(i+1)
S=Si-S(i+1)
K=Ki-K (i+1)
Where i and i+1 are two consecutive frames.
Step 5: Add all four differences to and out total difference Td
Td=MD+STD+S+K
Step 6: Calculate threshold
T = Md + _STD
Step 7: Compare Td with threshold.
Step 8: If Td(i; i+1) _ T then i is the end of previous shot and i+1 is start of next shot.

B. Key Frame Extraction

A key frame is a frame that best represents the video content in an abstract manner. In proposed system to extract key frames above algorithm of shot boundary detection is applied over video sequence.Then from each shot a frame with highest mean and standard deviance is extracted. So, from every shot one key frame is extracted to form static video summarization.

Algorithm of key frame extraction
Step 1: Divide the whole video sequence into shots using above algorithm.
Step 2: Find frame with maximum mean and standard variance from each shot.
Step 3: These frames form static summarization.

C. Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption.

In December 2001, the National Institute of Standards (NIST) sanctioned the AES as Federal Information Processing Standards Publication (FIPS PUB) 197, which specifies application of the Rijndael algorithm to all sensitive classified data.

The AES has three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits. Key size is unlimited, whereas the block size maximum is 256 bits. The AES design is created on a substitution-permutation network (SPN) and does not use the Data Encryption Standard (DES) Feistelnetwork.

The AES replaced the DES with new and updated features:

- Block encryption implementation
- 128-bit group encryption with 128, 192 and 256-bit key lengths
- Symmetric algorithm demanding only one encryption and decryption key

ISSN(Online) : 2319 -8753
ISSN (Print) : 2347 -6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

- Data security for 20-30 years
- Worldwide access
- No royalties
- Easy overall implementation

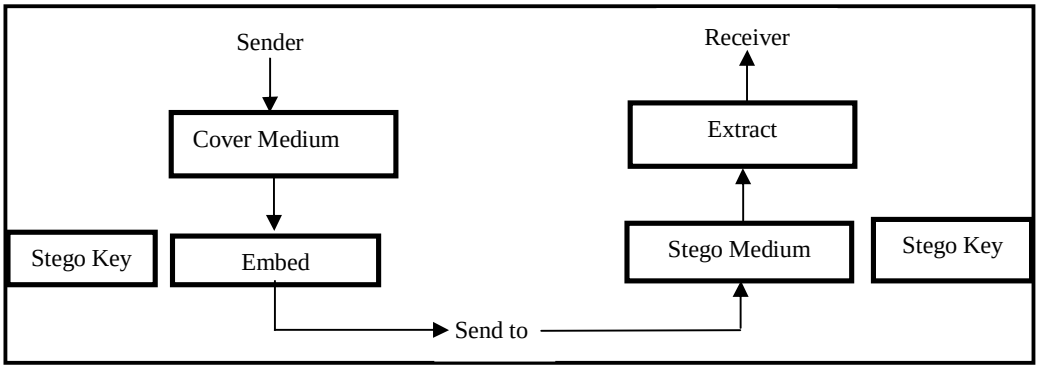

Fig.1. Block diagram of Steganography mechanism

D. Parameters

- MSE
- PSNR
- PAYLOAD

1. Mean Squared Error (MSE)

$$MSE = \frac{1}{H * W} \sum_{i=1}^{H} (P(i,j) - S(i,j))^2 \qquad (1)$$

where, MSE is Mean Square error, H and W are height width and P(i, j) represents original frame and S(i, j) represents corresponding stego frame.

2. Peak Signal To Noise Ratio (PSNR)

$$PSNR = 10log_{10} \frac{L^2}{MSE} \qquad (2)$$

where, PSNR is peak signal to noise ratio, L is peak signal level for a grey scale image it is taken as 255.

3. PAYLOAD

Payload refers to the amount of information that can be hidden in the cover image. The ability of steganalysis methods depend on the volume of payload of hidden message. Hence, this fact imposes an upper bound limit for embedding data, such that if the hidden data size is less than that upper bound, one may assert that the stego-image is safe and the steganalysis methods cannot detect it

VIII. RESULT

The proposed video steganography algorithm is tested using different AVI files. The performance and robustness of the proposed video steganography system are discussed in this section. The proposed method is implemented using MATLAB and Eclipse. The performance of the proposed system is analyzed based on the parameters as MSE, PSNR and PAYLOAD. In [1], performance of the proposed technique is evaluated using three different video streams (drop.avi, flame.avi &american football.avi) and one secret data (message.png). The perceptual imperceptibility of the embedded data is indicated by comparing the original image or video to its stego counterpart so that their visual differences, if any, can be determined. Additionally, as an objective measure, the Mean squared Error

ISSN(Online) : 2319 -8753
ISSN (Print) : 2347 -6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

(MSE) and Peak Signal to Noise Ratio (PSNR) between the stego frame and its corresponding cover frame are studied. The quantities are given in Table 1.

TABLE 1RESULTS OBTAINED FROM HLSB AND LSB TECHNIQUES[1]

Name Of TheVideo File	No. Of Frames	Results Obtained Using HLSB			Results Obtained Using LSB		
		MSE	*PSNR*	*PAYLOAD*	*MSE*	*PSNR*	*PAYLOAD*
drop.avi	182	0.34	44.34	2.66	0.42	48.56	1
Americanfootball.avi	455	0.34	45.67	2.66	0.52	52.34	1
flame.avi	294	0.34	42.66	2.66	0.38	48.56	1
Average value		0.34	44.23	2.66	0.44	49.82	1

The proposed technique has been applied to different videos of AVI format (flame4.avi, bird.avi, cbw3.avi, and drop.avi) and the result has been shown in Table 2. On Comparison the average value of MSE using HLSB is 0.34 and using LSB is 0.44 while the average value of MSE using proposed technique is 0.1789 which has improved to large extend. Average PSNR value obtained for HLSB is 44.223 dB and for LSB is 49.82dB while for proposed technique, the average PSNR value is 55.6059dB.

TABLE 2 RESULTS OBTAINED FROM PROPOSED TECHNIQUE(KEY FRAME EXTRACTION AND LSB TECHNIQUE)

Name Of TheVideo File	No. Of Frames	*MSE*	*PSNR*	*PAYLOAD*
Flame4.avi	110	0.178141	55.6236	3
bird.avi	355	0.183648	55.49094	3
Cbw3.avi	250	0.183702	55.48967	3
drop.avi	182	0.169575	55.83719	3
Average value		0.1789	55.6059	3

- **SCREEN SHOTS**
- Fig. 2a is the screen shot of original flame4 video and fig. 2b is the screen shot of flame4 stego video with message encrypted in it. While playing both the videos i.e. original video and stego video, no difference has been noticed. This shows the proper encryption of the message in the video.

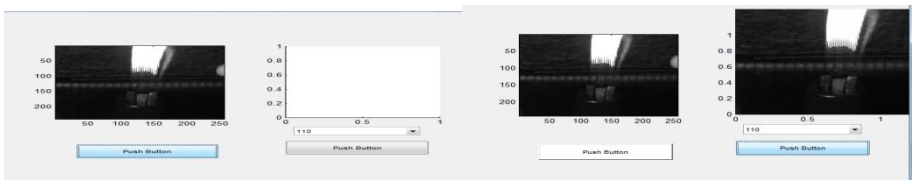

Fig 2a. Screen shot of Original flame4 video

Fig 2 b. Screen shot of original with stego flame4 video

- Fig. 3a is the screen shot of original bird video and fig. 3b is the screen shot of bird stego video with message encrypted in it. While playing both the videos i.e. original video and stego video, no difference has been noticed. This shows the proper encryption of the message in the video.

ISSN(Online) : 2319 -8753
ISSN (Print) : 2347 -6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

Fig 3a. Screen shot of Original bird video Fig 3 b. Screen shot of original with stego bird video

- Fig. 4a is the screen shot of original Cbw video and fig. 4b is the screen shot of Cbw stego video with message encrypted in it. While playing both the videos i.e. original video and stego video, no difference has been noticed. This shows the proper encryption of the message in the video.

Fig 4a. Screen shot of OriginalCbwvideo Fig 4 b. Screen shot of original with stego Cbw video

- Fig. 5a is the screen shot of original drop video and fig. 5b is the screen shot of drop stego video with message encrypted in it. While playing both the videos i.e. original video and stego video, no difference has been noticed. This shows the proper encryption of the message in the video.

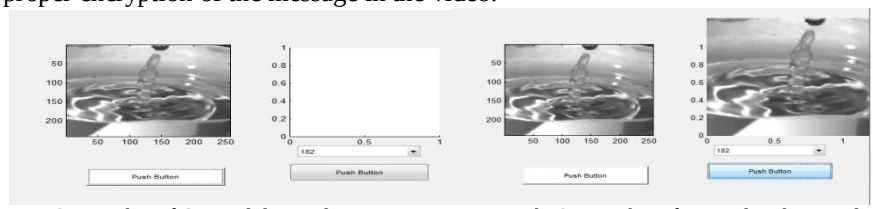

Fig 5 a. Screen shot of Original drop video Fig 5 b. Screen shot of original with stego drop video

IX. CONCLUSION

In this paper we discussed several ways of hiding the secret data inside the cover medium such as image, audio and video. The proposed method for data hiding uses LSB techniques and statistical features for key frame extraction and AES for encryption which results in more secure and robust technique for data hiding as average MSE and PSNR value have been reduced much as compared to HLSB and LSB techniques. We can conclude that the proposed system is more effective for secret communication over the network channel, as key frame extraction method would not be known to hackers as it is completely new technique for video steganography, which is the main strength of my proposed method, so they will not be able to find data hidden frames easily. Hence it is clearly perceived from the result that the distortions occurred in the cover-video by applying the proposed algorithm is highly imperceptible to human eyes. Hence the proposed video steganography method is proved to be apparent to transfer highly confidential data like banking details, medical reports, military data and other important data.

REFERENCES

[1] 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.

[2] Hemant Gupta and Setu Chaturvedi "Video Steganography through LSB based Hybrid approach" IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3, March 2014.

ISSN(Online) : 2319 -8753
ISSN (Print) : 2347 -6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

[3] Mritha Ramalingam and Nor Ashidi Mat Isa "Video Steganography based on Integer Haar Wavelet Transforms for Secured Data Transfer" Indian Journal of Science and Technology, Vol 7(7), 897–904, July 2014.
[4] A.K. Al Frajat, "Hiding data in video file An overview" Journal of applied sciences 10(15):1644-1649, 2010.
[5] Ali K Hmood, "An overview on hiding information technique in images" Journal of applied sciences 10(18)2094-2100, 2010.
[6] Niu Jiping, "Image encryption algorithm based on rijndael S-boxes" in IEEE applied International conference on computational intelligence and security 978-0-7695-3508-1\08, 2008.
[7] B. Subramanan, "Image encryption based on AES key expansion" in IEEE applied second international conference on emerging application of information technology, 978-0-7695-4329-1/11, 2011.
[8] Punita Meelu ,"AES Asymmetric key cryptographic system" in international journal of information technology and knowledge management, volume 4, 113-117, 2011.
[9] Saurabh Singh, "Hiding Image to Video" International Journal of engineering science & technology Vol. 2(12), 6999-7003 ,2010.
[10] Marghny Mohamed, "Data hiding by LSB substitution using genetic optimal key permutation " in International arab journal of e-technology, vol.2,no 1,11-17, January 2011.

BIOGRAPHY

Nishi Khan received her B.E. degree in the field of Electronics Engineering from RTMNU University in 2013 and pursuing M.E. in the field of Electronics Engineering from Terna Engineering College, Navi Mumbai, India. Her research interests include image processing, steganography and cryptography. She has represented research paper in International conference as well as journal.

Kanchan S. Gorde is currently working as an Assistant Professor in Department of Electronics Engineering in Terna Engineering College, Navi Mumbai, India. She has more than 10 years of experience in teaching. She has represented various papers in International journals and in international as well as national conferences.