International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 194-199
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

AN INNOVATIVE APPROACH FOR VIDEO STEGANOGRAPHY USING STATISTICAL FEATURES IN ROUND-LSB

Ajit Danti, G.R.Manjula
Dept. of computer Science and Engg.
Jawaharlal Nehru National College of Engg.
Shimoga, Karnataka, India

Priya K
Dept. of computer Science and Engg.
Jawaharlal Nehru National College of Engg.
Shimoga, Karnataka, India

***Abstract*— Security of records through computerized media is of great concern today in light of attacks, abuse or unapproved access of data. Steganography is the ability of concealing message inside a block of multimedia. Video Steganography manages concealing secret data inside a video. Cover video of various formats are utilized in the proposed technique. In this paper the proposed algorithm for data hiding utilizes Round-LSB technique to conceal the secret information in cover video. Data to be concealed and sent is hidden only in selected frames of the cover video, known as key frames to improve the security of the system. Selecting key frames are done using two methods. First, statistical features like kurtosis, skewness, standard deviation and mean are utilized for key frame extraction. Second, is by using fixed threshold. Concealing secret data in only key frames obtained from these methods enhances the security of the algorithm by creating more confusion to the hackers. Hence the proposed system is more efficient for secret communication, as frames in which data is concealed would not be known to hackers. Experimental results show that key frame extraction with statistical features provides better results in contrast to fixed threshold in terms of PSNR and MSE.**

***Keywords*— Video Steganography, Round-LSB, Key frame extraction, Statistical features, Threshold**

I. INTRODUCTION

In this day and age of innovation in the technology everybody is dependent on the internet for the purpose of communication and also to send and receive the secret information. But this internet is not so safe for communicating because of the intruder attacks to obtain the secret information, which is a very crucial part for any of the organization. Thus the security is of major concern in communication. The advancement in innovation and systems administration has postured genuine dangers to get secured information. Since computerized sight and sound have turned out to be logically best in class in the quickly developing field of web application, information securities, including copyright insurance and information integrity recognition, have turned into a vast concern. Today in this technology world there is a huge demand for digital communication which has created a powerful need for new approach to protect the secret records from illegal usage. In some cases is highly desired to have secret communication. This objective is accomplished utilizing two methods to be specifically called as cryptography and steganography [1]. A sender scrambles the message utilizing an encryption key and recipient will extract the original information from scrambled message utilizing the proper unscrambling key, in cryptography. In any case, in steganography, the message is not mixed; rather the presence of a message is covered up in a transporter typically called as cover medium. Fig.1 shows the complete mechanism of video steganography.

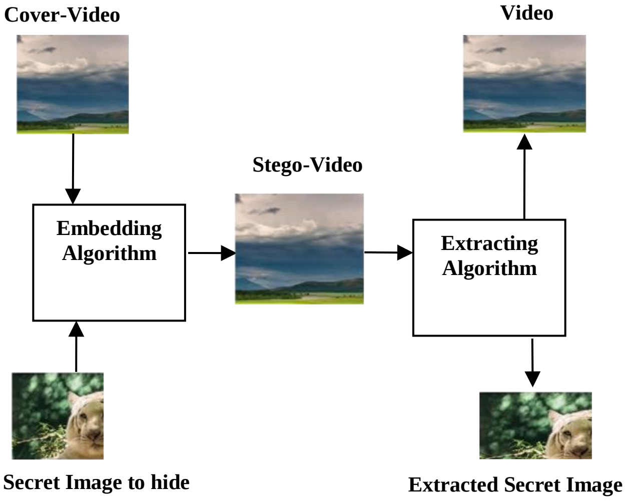


Fig.1: Simple Video Steganography Mechanism

The bearer containing the secret message is called as stego-medium. Video steganography method is best choice to conceal our secret data because it will resolve the difficulties of security and embedding capacity. Advantage of using the carrier file as video is development in security against the attacks from interlopers because of its huge structure.

The rest of the paper is structured as follows. Proposed algorithms of embedding and extraction along with statistical featured, fixed threshold key frame extraction algorithm are explained in the section II. Experimental results are described in section III. Concluding remarks are given in section IV.

II. Proposed Algorithm

A. *Data embedding and extraction algorithm –*

In embedding part secret message is embedded in the video record and initially data is gathered about the cover video that is available in header part of video document [2]. After accumulation of data, video record is changed over into the number of frames which are there in video as form of frames. At the point when all those pictures are appeared in a stream with some speed then it is called to be as frame rate. Select the required frame from the accumulation of frames by using key frame extraction algorithms with statistical feature and fixed threshold then conceal the secret data in the chosen keys by utilizing proposed round-LSB technique of the video steganography [3]. At that point modify the video record with the stego video and now this is prepared to send out to the expected recipient on the network. This overall process of embedding is described in the fig.2 and extraction process is explained in detail in fig.3 below.

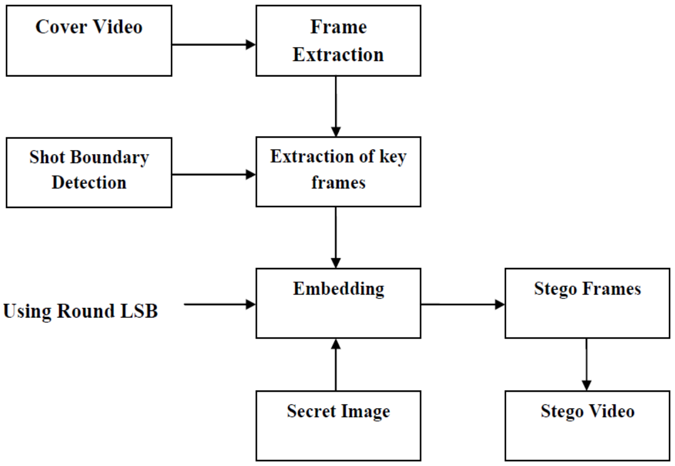


Fig.2: Block Diagram for Data Embedding Process

In extraction part when the indented recipient gets the stego video then initial pace is to gather data about the video record like number of key frames, secret message length etc,. At that point change over the video into frames then concentrate the stego frames from the video and after that take out the secret data from the stego video utilizing and applying desteganography round LSB technique [5]. Once the removal of secret information is taken from stego video the actual video is got then rearrange this with the already existing other frames to get the actual video.

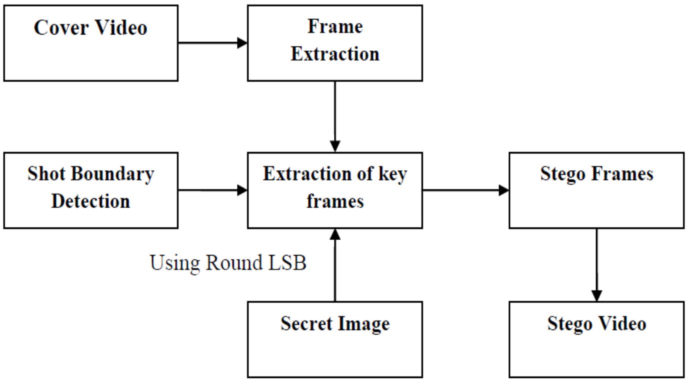
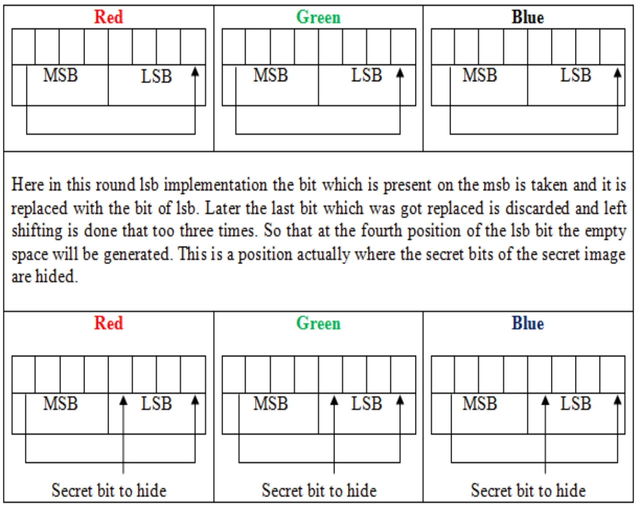


Fig. 3: Block Diagram for Data Extracting Process

B. *Round-LSB(Least Significant Bit) –*

In order to conceal the information inside the carrier file that is video the most common and the simple approach is this LSB which stands for Least Significant Bit. Here in this round lsb implementation the bit which is present on the msb is taken and it is replaced with the bit of lsb. Later the last bit which was got replaced is discarded and left shifting is done that too three times. So that at the fourth position of the lsb bit the empty space will be generated [15]. This is a position actually where the secret bits of the secret images are hided. Here with this round lsb we can also round the lsb bit, by modifying the bit of msb, but this approach gives increased mse and lesser psnr which is not good.

Table 1: Working of Round LSB.



Here in this round lsb implementation the bit which is present on the msb is taken and it is replaced with the bit of lsb. Later the last bit which was got replaced is discarded and left shifting is done that too three times. So that at the fourth position of the lsb bit the empty space will be generated. This is a position actually where the secret bits of the secret image are hided.

C. Key Frame Extraction Algorithm using Statistical Features

The statistical features comprises of the skewness, mean, standard deviation and the mean using these features the keys are extracted by the proposed method. Skewness is defined as the measure of symmetry or more accurately it can also be called as the nonexistence of proportion. The measure that tells whether the information is heavy- tailed or light-tailed in respect to a normal distribution is called as kurtosis. The skewness value will be zero for the ordinary dispersion, and all the symmetric information will have the skewness value closer to zero. The standard deviation (SD) is a measure that is utilized to evaluate the measure of scattering of an arrangement of information values [12]. A low standard deviation tells that the information is inclined towards the mean of the set, on the other hand a higher SD requirement deviation depicts that the information are multiplied out over a wider range of values. Algorithm steps are shown below.

Input: Cover-video
Output: Key-frames

Step 1 : Extract the frames of the video one by one
Step 2 : Change all the colored images to gray scale or black and white images
Step 3 : Calculate the difference of histogram between the two successive frames
Step 4 : Calculate the absolute difference between the frames
Step 5 : Calculate standard variance (STD), mean (MD), and kurtosis (k), skewness (S) for a single frame
Step 6 : Figure out the difference of these four values from two successive frames
S=Si-S (i+1)
STD=STD i-STD (i+1)
MD=MD i-MD (i+1)
K=K i-K (i+1) here i+1 and i are two successive frames
Step 7 : Sum up all these 4 differences and calculate Td- total difference
Step 8 : Calculate threshold, T = mean + standard variance
Step 9 : Compare Td with T
Step 10 : If Td is greater than threshold that is Td (i; i+1) > T, consider it as key-frame, i is the last part of previous shot and i+1 is begin of next shot

D. Key Frame Extraction Algorithm using Fixed Threshold

Intially in this key extraction process with predefined threshold , the value for the threshold will be already set to the three-fourth of the maximum value obtained in the difference. Convert the colored images into an gray-scale image and find the histogram difference between the two consecutive frames of the cover-video.Then it is required to find the absolute differences between the frames.The threshold here it is calculated by using the formula [9].Lastly the differnce of frames is compared aginst the threshold, if it is found greatest select that as the key frame. Algorithm is as below.

Input: Cover-video
Output: Key-frames

Step 1 : Extract the frames of the video one by one

Step 2 : Change all the colored images to gray scale or black and white images

Step 3 : Calculate the difference of histogram between the two successive frames Calculate the absolute difference between the frames and call it as diff (i)

Step 4 : Threshold = max (diff) * 3 / 4, set threshold to 3 / 4th of the maximum value in the array diff

Step 5 : Compute the threshold using the above formula

Step 6 : Compare the difference diff (i) with T and if diff (i) is > T, selects it as a key-frame else repeat

Step 7 : End

III. Experiment and Result

Matlab 2014 is used to implement the proposed method and it is tested with different formats of video and different formats of secret images. MATLAB is utilized as test system or simulator to execute the methods of steganography. Advanced built-in functions and intense computing background for image handling and image processing are provided by MATLAB [14]. The video steganography technique mainly has two elements one is imperceptibility and the other being the embedding capacity. Imperceptibity refers to perceptual invisibility. Apart from this we have objective measures, the MSE-Mean Squared Error and PSNR-Peak Signal to Noise Ratio. The values of these are found using below equations. The distortion in the stego video is measured by Peak Signal to Noise Ratio (PSNR) utilizing equation 1.The perceptual nature of stego video can be measured utilizing the equation 2.

$$\mathrm{PSNR} = 10 * \mathrm{Log}_{10}\left(\frac{\mathrm{MAX_O}^2}{\mathrm{MSE}}\right) \qquad (1)$$

$$\text{MSE} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}[\text{O(i,j)} - \text{S(i,j)}]^{2}}{\text{m}*\text{n}} \qquad (2)$$

Table 2: The MSE, PSNR values of 3 different videos for 5 different secret images Using Key frame algorithm with pre-defined threshold

Video Sequences (.mpg, .avi, .mp4)	**Secret Images (40 X 40)**	**Key Frames**	**MSE**	**PSNR**
Xylophone.mpg	Lena.tif	69	0.567	50.626
Xylophone.mpg	Pepper	69	0.565	50.646
Xylophone.mpg	Building	69	0.568	50.637
Xylophone.mpg	Tiger	69	**0.565**	50.640
Xylophone.mpg	Flower	69	0.567	50.626
Rhinos.avi	Lena	10	0.599	50.390
Rhinos.avi	Pepper	10	0.602	50.368
Rhinos.avi	Building	10	0.637	50.365
Rhinos.avi	Tiger	10	0.640	50.308
Rhinos.avi	Flower	10	0.626	50.262
Container.mp4	Lena	10	6.859	39.801
Container.mp4	Pepper	10	6.866	39.797
Container.mp4	Building	10	6.880	39.788
Container.mp4	Tiger	10	6.854	39.805
Container.mp4	Flower	10	6.885	39.785

Video Sequences (.mpg, .avi, .mp4)	**Secret Images (40 X 40)**	**Key Frames**	**MSE**	**PSNR**
Xylophone.mpg	Lena.tif	83	0.4697	51.4462
Xylophone.mpg	Pepper	83	0.4660	51.4808
Xylophone.mpg	Building	83	0.4677	51.4647
Xylophone.mpg	Tiger	83	0.4683	51.4593
Xylophone.mpg	Flower	83	0.4702	51.4417
Rhinos.avi	Lena	84	1.0010	48.1603
Rhinos.avi	Pepper	84	1.0036	48.1490
Rhinos.avi	Building	84	1.0010	48.1603
Rhinos.avi	Tiger	84	1.0059	48.1390
Rhinos.avi	Flower	84	1.0018	48.1571
Container.mp4	Lena	76	3.9949	42.1497
Container.mp4	Pepper	76	3.9869	42.1584
Container.mp4	Building	76	4.0099	42.1335
Container.mp4	Tiger	76	3.9874	42.1579
Container.mp4	Flower	76	4.0226	42.1197

Table 3: The MSE, PSNR values of 3 different videos for 5 different secret images using Shot boundary Detection algorithm with statistical features

The technique proposed is tested using five various secret images and three different cover videos of varying format (xylophone.mpg, rhinos.avi and conatainer.mp4). The cover video chosen is in AVI format, .mp4 format and mpg (Motion Picture Experts Group) format. The size of the secret picture is 40x40. The experimental results are depicted in Table 5.1 and Table 5.2. Overall, the xylophone video with pepper as secret image has the best visual quality for statistical featured method. The proposed algorithm uses key frame extraction algorithms with pre-defined threshold and with statistical features. The benefit of using this keys concept is to make the intruders difficult to hack the secret content which is been hidden. The PSNR value for fixed threshold algorithm ranges between 39DB to 50DB, and the PSNR value for shot boundary detection algorithm is between 42DB to 52DB. The PSNR value of statistical feature technique is more than PSNR value of fixed threshold technique because of the usage of measures like skewness, kurtosis, mean and the standard deviation. The output samples for cover videos and secret images are shown below.

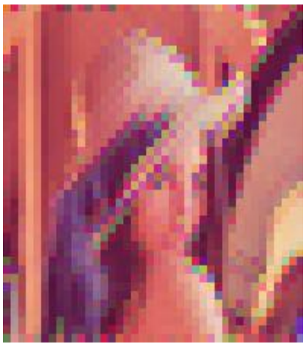
Cover video

Original secret Image

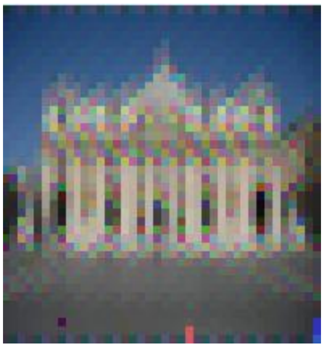
Cover video

Secret Image

Stego Video


Extracted secret Image

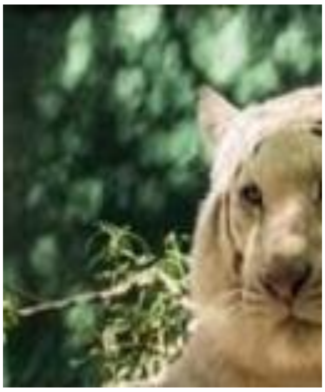
Stego Video


Extracted secret Image

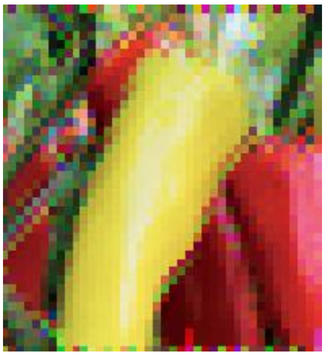
Cover video

Secret Image

Cover video

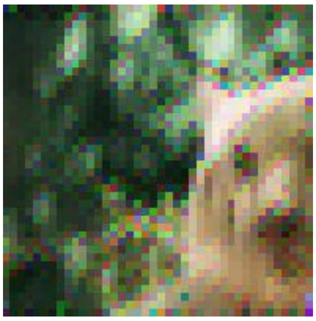

Secret Image

Stego Video


Extracted secret Image

Stego Video

Extracted secret Image



IV. CONCLUSION

The proposed algorithm for data hiding utilizes Round-LSB technique to conceal the secret information in cover video. Data to be concealed and sent is hidden only in selected frames of the cover video, known as key frames to improve the system security. To select the key frames from the set of video frames two methods are used. First, statistical features like kurtosis, skewness, standard deviation and mean are utilized for key frame extraction. Another method used for key frame extraction is by using fixed threshold. Concealing secret data in only key frames obtained from these methods enhances the security of the algorithm by creating more confusion to the hackers. The proposed system is more efficient for secret communication over the network channel, as frames in which data is concealed would not be known to hackers.

For example, utilizing xylophone.mpg as cover video for embedding secret image pepper.jpg gives PSNR estimation using Round LSB with statistical feature as 51.4808 dB. And the PSNR value for Round-LSB technique with fixed threshold method for key frame extraction using xylophone.mpg as cover video for embedding secret image tiger.jpg is observed to be 50.6409 dB. The MSE estimation of Round LSB (statistical features) is 0.4 and that of Round-LSB (fixed threshold) is 0.5. Hence the proposed strategy results in more secure and robust method for hiding information.

V. REFERENCE

[1] Prof. Dr. P. R. Deshmukh, Bhagyashri Rahangdale―Hash based least significant bit technique for video steganography Int. Journal of Engineering Research and Applications ISSN: 2248 - 9622, Vol. 4, Issue 1(Version 3), January 2014, pp.44-49. www.ijera.com.

[2] S.Chitra, Narasimhalu Thoti ―Implementation of video steganography using hash function in LSB technique International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 2 Issue 11, November – 2013. www.ijert.org.

[3] Koushikdasgupta 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.DOI:10.5121/ijsptm.2012.2201.

[4] ShashikalaChannalli and Ajay Jadhav ―Steganography an art of hiding data International Journal on Computer Science and Engineering Vol.1 (3), 2009, 137-141.

[5] Changyong Xu Xijian Ping and Tao Zhang ―Steganography in compressed video stream First IEEE International Conference on Innovative Computing, Information and Control 2006.

[6] ShengDun Hu and KinTak U ―A novel video steganography based on non-uniform rectangular partition. The 14th IEEE International Conference on Computational Science and Engineering 2011 DOI 10.1109/CSE.2011.146.

[7] Tomonori Furuta Hideki Noda, MichiharuNiimi and Eiji Kawaguchi ―Bit-plane decomposition steganography using wavelet compressed video‖ ICICS-PCM IEEE december 2003.

[8] Prof. D P Gaikwad , TruptiJagdale, Swati Dhanokar, AbhijeetMoghe, Akash Pathak ―Hiding the text and image message of variable size using encryption and compression algorithm in video stegnography International Journal of Engineering Research and Applications (IJERA) 2011 ISSN: 2248-9622 Vol. 1, Issue 2, pp.102-108. www.ijera.com.

[9] A.Swathi, Dr. S.A.K Jilani ―Video steganography by key frame extraction algorithm using LSB. International Journal Of Computational Engineering Research (ijcer) Vol. 2 Issue-5, Issn 2250-3005(online) September| 2014.

[10] Saurabh Singh, Gaurav Agarwal ―Hiding image to video: a new approach of LSB replacement‖ International Journal of Engineering Science and Technology Vol. 2(12), 2010, 6999-7003.

[11] K. Steffy Jenifer, G. Yogaraj , K. Rajalakshmi ―LSB approach for video steganography to embed images International Journal of Computer Science and Information Technologies Vol. 5 (1) , 2014,319-322, www.ijcsit.com.

[12] Nishi Khan, Kanchan S.Gorde ―Video Steganography by using statistical key frame extraction & LSB technique. International Journal of Engineering and Innovative Reasearch in science (IJIRS) Volume 4, Issue 10, october 2015.

[13] Rajeev Sobti, G.Geetha ―Cryptographic hash functions: a review. IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2, March 2012, ISSN (Online): 1694-0814 www.IJCSI.org.

[14] G.R.Manjula, AjitDanti ―A novel hash based least significant bit (2-3-3) image steganography in spatial domain. International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015 DOI: 10.5121/ijsptm.2015.4102.

[15] Koumal Kaushik, Suman― An innovative approach for video steganography :International Journal Computer Network and Information Security, 2015 , 11,72-79 DOI:10.5815/ijcnis.2015.11.08.