

An Innovative Approach for Video Steganography

Koumal Kaushik

M.Tech Student, CSE Dept.

Deenbandhu Chhotu Ram University of Science & Technology, Murthal Distt.Sonepat-131039(Haryana) India

Email: koumalkaushik@gmail.com

Suman

Asstt. Professor, Deenbandhu Chhotu Ram University of Science & Technology, Murthal Distt.Sonepat-131039(Haryana) India

Email: Suman2222@yahoo.com

Abstract—In today's world internet is used for data communication which is not secure enough to transfer highly confidential data so information hiding become a emerging research area. Steganography is an art to hiding secret message in a cover and it will also hide the fact that secret information is being sent over the communication network. In this paper a video steganography method is proposed using hash based round Least Significant Bit technique. Video steganography is a more secure than any other steganography technique in hiding information because of its complex structure it disables the intruder to attack. In this paper secret text message is embedded in the video file using proposed hash based round Least Significant Bit technique. This work will improve the information security and embedding capacity. The proposed technique hash based round Least Significant Bit will be compared with the hash based Least Significant Bit. The technique proposed in this paper is analysed in term of Peak Signal to Noise Ratio, Mean Square Error and Embedding capacity.

Index Terms—Video steganography, secret message, hash based round LSB, AVI, secret text message.

I. INTRODUCTION

In today's world of technology everyone is using internet for communication and also for sending and receiving confidential data. Because of intruder internet is not that secure way to communicate because information is the wealth of any organisation so security is the top issue. Steganography is an emerging research area in the field of information hiding. Steganography is an art to hide fact that the secret information is being sent over the communication network and it also hide the content of the message. The word steganography derived from Greek word "steganographia" which means "covered writing".

Information is hide inside the cover file such as text, image, audio, video file. Fig. 1 explains the mechanism

of steganography. Video file is the better option to hide the secret information because it overcame the problem of embedding capacity and security. Steganography is done in two part first one is embedding of information in the cover file and then to extract that information from the video file [1]. There are various application of steganography such as in military, industrial applications to copy right and Intellectual Property Rights (IPR). By using lossless steganography techniques message can be sent and received securely [2]. Video steganography is having mainly to broader areas which are temporal domain and spatial domain. In temporal domain cover file is transformed in the transform coefficient by using various transformation techniques such as discrete cosine transform, discrete wavelet transform etc. and then secret information is then hid in these transform coefficient[3]. In spatial domain bits are inserted in the pixel of the frame of video file by which embedding capacity is increases by using LSB techniques but it is prone to attack [3]. Benefit of video steganography in hiding information is improvement in security against the attack of intruder because of its complex structure [2].

This paper proposes a hash based round LSB Technique is developed in MATLAB. The proposed method is illustrated with AVI (Audio Video Interleave) as a cover medium. Significant and encouraging results are obtained. This paper is organised as follows- Section 2 describe literature survey, section 3 describe proposed work, section 4 describe comparison table, section 5 describe the experimental results and section 6 describes the conclusion and future work.

II. LITERATURE SURVEY

Many kind of steganography method have been proposed. Video steganography is become a wide area of research as it can hide large amount data. To understand the concept of video steganography we have surveyed many paper and we want to discuss some them in brief. We thank these authors for provide us such a use full on video steganography.

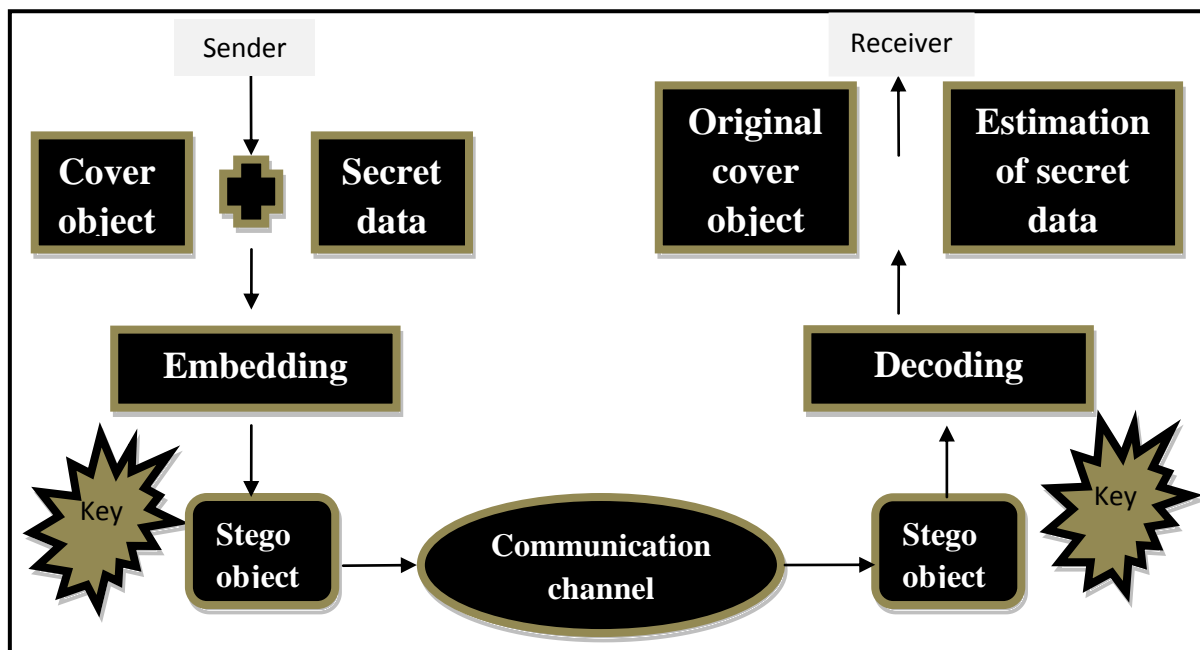


Fig.1. Simple Steganography Mechanism

In [2] hash function was used to generate index values and these values are used to insert message bits in the LSB of RGB pixel this technique was an improvement LSB insertion technique.

In [3] hash function was used to find the position to embed the secret message bit in the LSB of RGB pixels and this technique was used to hide secret message in cover video file.

There are number of requirement which must be satisfied by a steganography technique and a method was proposed using symmetric key steganography technique and LSB technique to hide data in an image which was published on advertisement board [4].

In [5] data hiding was done in the compressed video file in motion vectors which is having larger magnitude using steganography method in MPEG compressed video stream.

An uncompressed secret video file hiding in a video cover file this method was proposed in [6] using non-uniform rectangular partition method along with optimal quadratic approximation principal.

In [7] secret data was embedded into a 3-D wavelet transformed video by using BPCS (bit – plane complexity segmentation) and 3-D (SPIHT) set partitioning in hierarchical trees. In [8] a method was proposed to embed variable size secret data in cover object.

In [9] a method was proposed to improve embedding capacity by using color channels here text was embedded in lossless RGB image.

In [10] an image was embedded in a video using a hybrid technique of DWT (discrete wavelet transform) and SVD(singular value decomposition) to improve security.

In [11] polynomials equations were used to find location in these frame of the video to embed the binary data bit of the secret data in the video here polynomial

coefficient was used as stego key.

In [12] simple LSB technique was used to hide data in video file by hiding message pixel row in first row of cover video file frame. In [13] LSB technique was used along with masking and filtering and transformation technique to embed secret image in cover video file.

In [14] message bit was embedded in cover video file using LSB technique along with DCT compression technique and the secret message bits was embedded in the DCT coefficient. In [15] Deffie Hellman key exchange method was used to generate index and using this index message is embedded in LSB of RGB pixels of audio and video cover file.

In [17] a method was proposed to embed secret message in RGB pixel and embedding was done on basis of color intensity of RGB pixel value. For encryption key exchange method was used and then low intensity RGB pixel are selected to embed secret data using LSB insertion method.

In [18] a method was proposed to embed a secret image in a cover image file using hash based (2-3-3) LSB insertion method which is an improvement over hash based (3-3-2) LSB technique.

In [19] a method was proposed to hide data using 4LSB and phase encoding algorithm in audio and video cover file.

III. PROPOSED WORK

The proposed technique video steganography using hash based round LSB is used to hide secret information in a video file (AVI) the proposed method is discussed in the following part of this section.

A. Diagrammatic Representation of Hash Based Round LSB

Video steganography is a more secure than any other steganography technique in hiding information because of its complex structure it disables an intruder to attack. The technique proposed for video steganography is Hash based Round Least Significant Bit. The block diagram of the proposed technique is given in Fig. 2 and 3. The tool which is used here for embedding and extraction of message is MATLAB.

based round LSB is implemented in two parts (a) encoding and (b) decoding.

In encoding part text message is encoded in the video file and it is done as follows: firstly information is collected about video which is present in header of video file and the file format of the video is AVI which stands for Audio Video Interleave which is suitable in the work. After collection of information video file is converted into the number of frame these frames are images which is present in the video in the form of frames. When these images are shown in a flow with some speed then it's called as video and speed is called as frame speed (frame per sec).

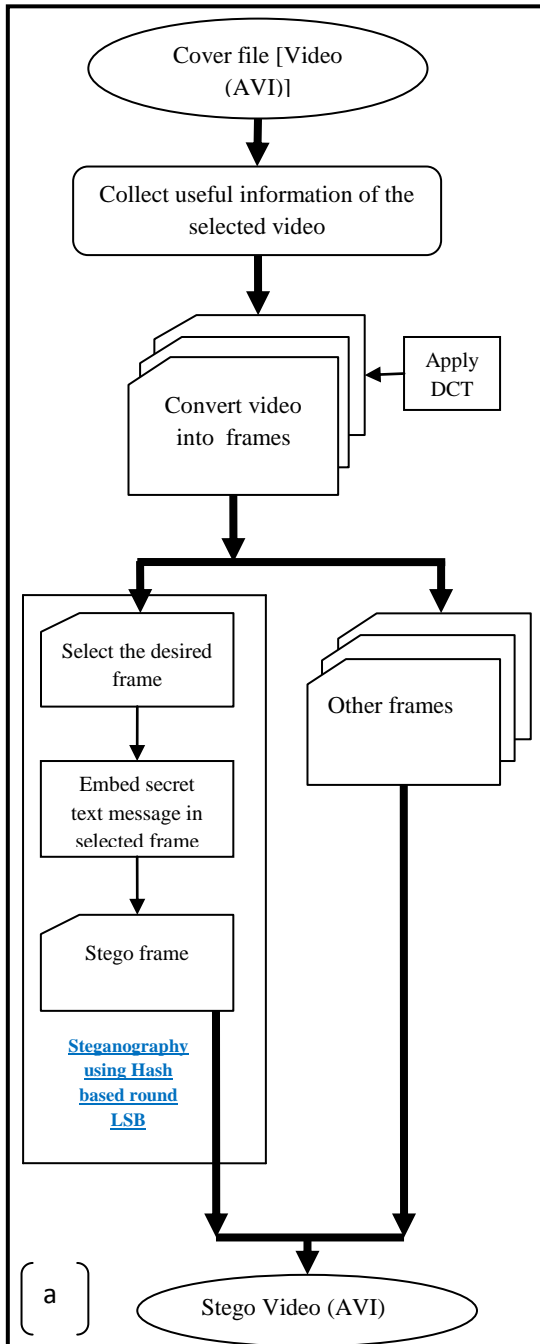


Fig.2. Block diagram of Hash based Round LSB (a) Encoding

A video is collection of number of frames. All the information which we need about video in steganography is present in its header such as number of frame, frame speed (frame per sec), height and width of frame etc [3]. The proposed video steganography method using hash

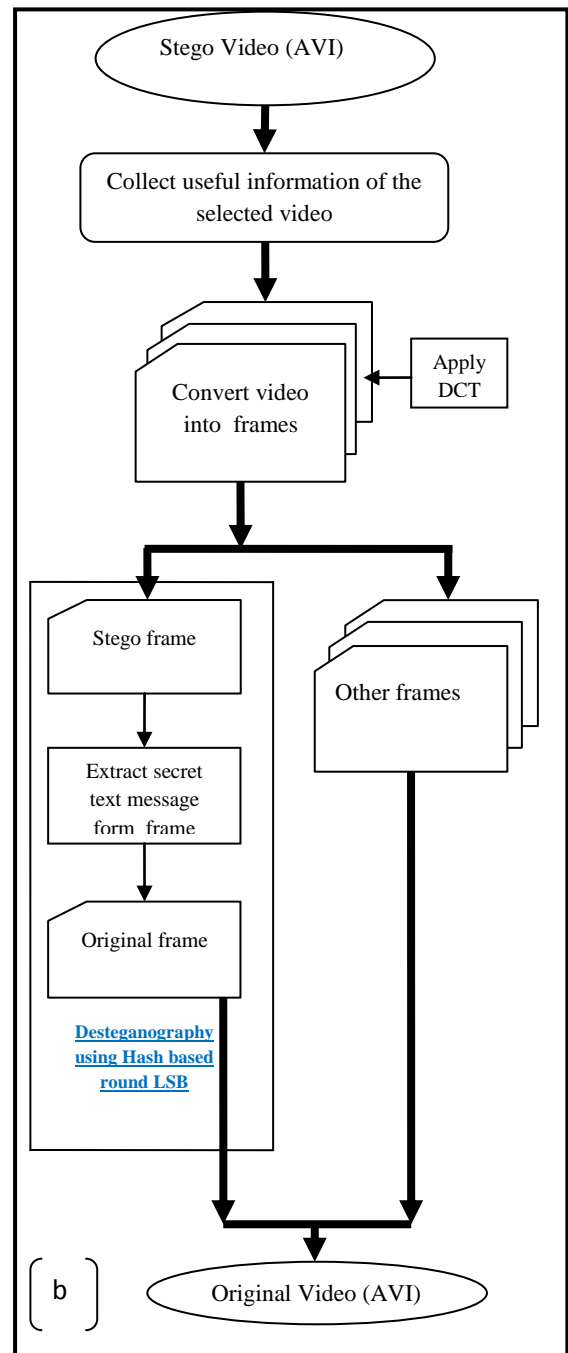


Fig.3. Block diagram of Hash based Round LSB (a) Encoding

After conversion of video into frames then DCT (Discrete Cosine Transform) compression technique is apply on these frames. Select the desired frame from the collection of frame then hide the secret text message in the selected frame by using proposed video steganography hash based round LSB method. Then rearrange the video file with the stego frame and now stego video is ready to transmit to the intended receiver.

In decoding part when stego video is received by the indented receiver then first step is to collect information about the AVI video file. Then convert the video into frames and apply DCT (Discrete Cosine Transform) compression technique. Then extract the stego frame from the video and then extract the secret text message from stego frame using stego key and applying desteganography hash based round LSB. After extraction of secret message from stego frame the original frame is obtained then rearranged the original frame with other frame to get the original video.

B. Hash function

Hash function is a term which is used in the field of computer science in information hiding. It is a process in which it will take an arbitrary amount of data in input and produce a fixed amount of data as output. This fixed output is called as hash code, message digest, and hash index. Formal definition of hash function in [16] is“ A hash function is a function $h: D \rightarrow R$, where the domain $D = \{0, 1\}^*$ and $R = \{0, 1\}^n$ for some $n \geq 1$ ”.Security service provide by hash function are integrity and authenticity, digital signatures, pseudo number generation, digital steganography, digital time stamping [16].

C. Hash based Round - LSB (Least significant bit)

LSB which stands for Least Significant Bit is a most common and simple approach to embed information in

an image file. In hash based round LSB will round the LSB when hash index is generated. In this technique it will bring last bit on MSB by which an array of values is generated so that an extra bit is generated between LSB and MSB. Now we get dynamic values at the time of embedding of data and this improve the embedding accuracy by which security and embedding capacity is improved. A simple example of round LSB is given in Table.1. In table 1 it is discussed with RGB pixels i.e. Red, Green and Blue pixels in which last bit of LSB is rounded by which extra bit is generated in between LSB and MSB.

Consider a RGB pixel value of the cover frame as below:

R: 10110111
G: 10010100
B: 11001001

And a message to be inserted: 10001001.

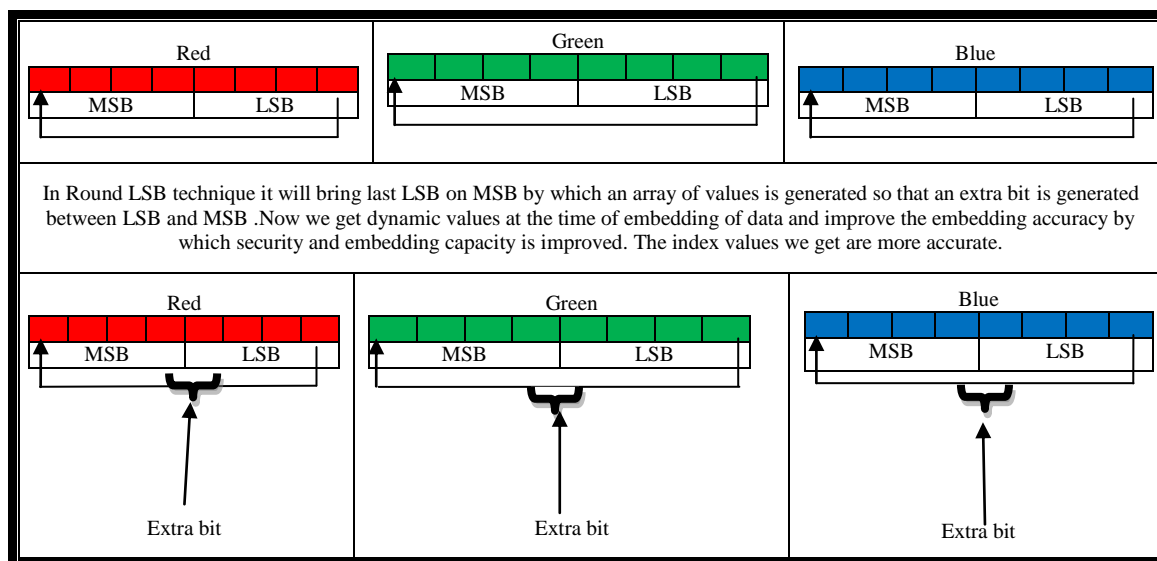
Hash based round LSB technique will round pixel value by which an extra bit is generated in between LSB and MSB:

R: 1011 _ 0111
G: 1001 _ 0100
B: 1100 _ 1001

A secret message is inserted in these extra bits: 10001001. And when extra bits generated in a pixel are filled with secret message bits are left to be filled then rest message bits are embedded in the next pixels.

For extraction of secret message bit hash key is used. Hash key will determine the location of pixels where secret message bits are embedded. Extraction is the reverses process of embedding of secret message bit.

Table 1. Diagrammatical Description of Hash Based Round LSB.



Hash key determine a RGB pixel:
As the intended user having the hash key value so

he/she will calculate the hash key and have same RGB pixel.

R: 1011_0111
 G: 1001_0100
 B: 1100_1001

With round LSB intended user will know the position of extra bit then message bits are generated: 10001001.

The security and embedding capacity is increased because of the generation of extra bit between LSB and MSB. In these extra bits secret information will embed in the form of text message. Simply it can be said that LSB bits are rounded to improve security and embedding capacity

D. Flow chart of Hash based Round LSB

In this paper a method is proposed for information hiding in a video by using hash based round LSB technique. A video consist a number of frame in these frame secret data is embedded as pay load.

Flow chart for the novel video steganography by using hash based round LSB in Fig. 3. In the flow chart first step for the proposed method to select the text message that is required to hide in the cover file. If text message is selected then go to the next step which is to select the video (AVI) file. If video file is selected then convert the video into the frames. A frame is itself an image so we can a video is collection of images.

After conversion apply DCT(Discrete Cosine Transform) compression on the frames. Next step is to select the desired frame for embedding secret data. After selection of frame hash index is generated and this index is used to embed data by using proposed method. Rearrange the video with stego frames and other frames.

Transmit the stego video to intended receiver. When stego video received then extracts the frames and applies DCT (Discrete Cosine Transform) compression. After conversion apply stego key to extract the text message and at last original video is transmitted.

E. Comparison table

The proposed technique is implemented in the MATLAB. Comparison of hash based LSB technique and hash based round LSB technique is given in the table. A steganography method is characterised by imperceptibility and capacity. Imperceptibility means invisibility of hidden data and computer analysis. Here performance is measured using an AVI video "xylophone". The number of frame of video is 141 and width and height of video is 320 and 240 respectively and the speed of video is 30 frames per sec. PSNR and embedding capacity is measured for the proposed technique there mathematical formula is given bellow

$$PSNR = 10\log_{10} \frac{L^2}{MSE} \quad (1)$$

PSNR stands for Peak to Signal Noise Ratio, L is peak signal level and MSE stands for Mean Square Error and it is calculated as

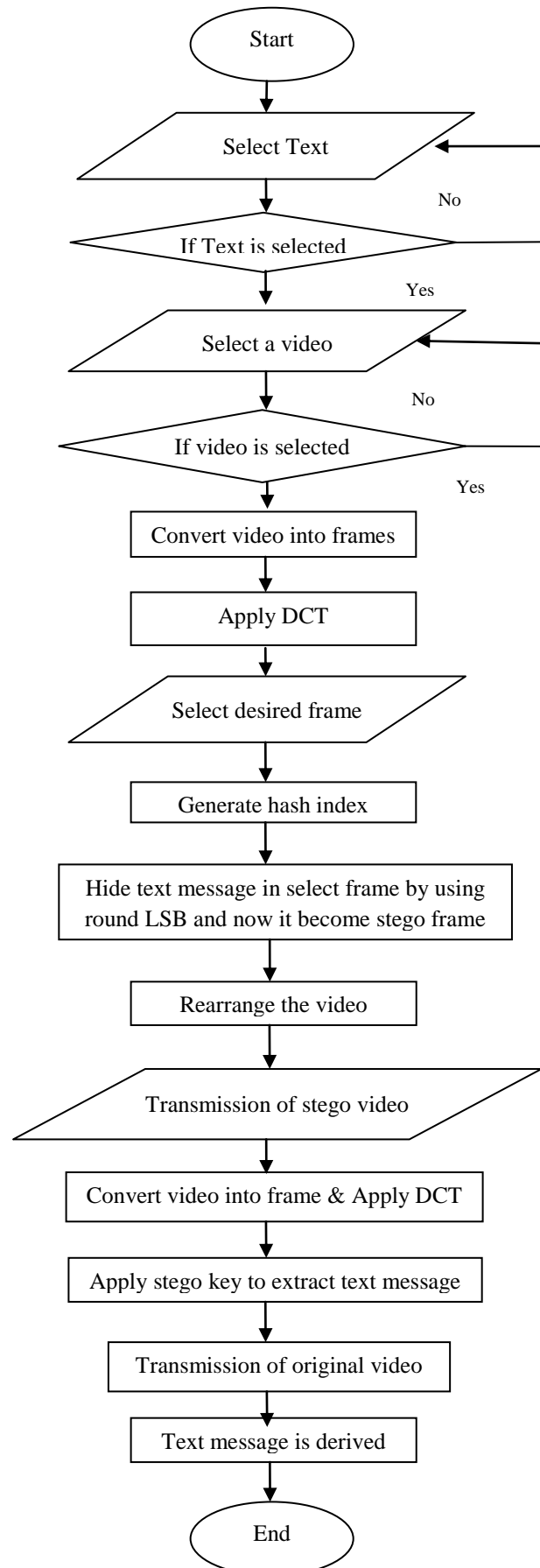


Fig.4. Flow Chart of Hash Based Round LSB Technique for Video Steganography

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

H and W represent height and width and P(i,j) and S(i,j) represent original image and stego image respectively. Embedding capacity means amount of data that can be hidden in the cover file. Details of cover video file and comparison are given in table 2 and table 3.

Table 2. Details of Cover Video File

| Name of video file. | Resolution (W*H) | Frames per sec | Number of frames | Secret message resolution |
|---------------------|------------------|----------------|------------------|---------------------------|
| xylophone | 320*240 | 30 | 141 | Text |

Table 3. Comparison Table Of Hash Based LSB And Hash Based Round LSB.

| | Name of video file | PSNR | MSE | Embedding capacity |
|-------------|--------------------|---------|-----|--------------------|
| H-LSB | Xylophone | 13.4594 | 9.4 | 13 |
| H-Round LSB | Xylophone | 44.7740 | 0.2 | 33 |

IV. EXPERIMENTAL RESULT

The proposed method is implemented in MATLAB 2012 and method is tested with an AVI video (xylophone.avi) and text message.

Fig. 5 shows a snapshot of select video file which is used as a cover file and after embedding of text message when video is transmitted to the intended receiver then reconstruction of video is done after the extraction of secret message Fig. 6 shows a snapshot of reconstructed video.



Fig.5. Original Video



Fig.6. Reconstructed image

Quality of the proposed technique is evaluated in term PSNR which stands for Peak to Signal Noise Ration and embedding capacity which is quite encouraging. PSNR value of hash based round LSB is more than the hash based LSB.

PSNR graph of original image and reconstructed image is shown in Fig 7. In starting PSNR value of frame without extraction of secret message is more than the PSNR value when the hidden data is extracted from frame but from frame 18 PSNR value of frame without extraction is less than the PSNR value when the hidden data is extracted from the frame. Fig. 8 shows the embedding capacity Vs threshold value.

The comparison graph of the proposed technique hash based round LSB and hash based LSB is mentioned in term of MSE which stands for mean square error and embedding capacity Fig. 9 shows embedding capacity performance for H-LSB and H- Round LSB Fig. 10 shows the MSE comparison ratio for H-LSB and H-Round.

Other values of comparison between hash based LSB and hash based round LSB techniques is mentioned already in the comparison table. All the results are improved over hash based LSB.

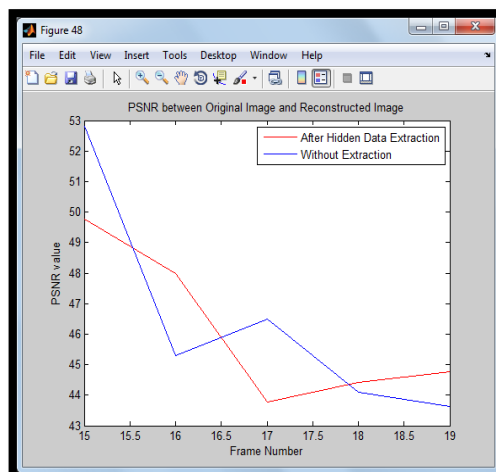


Fig.7. PSNR Graph

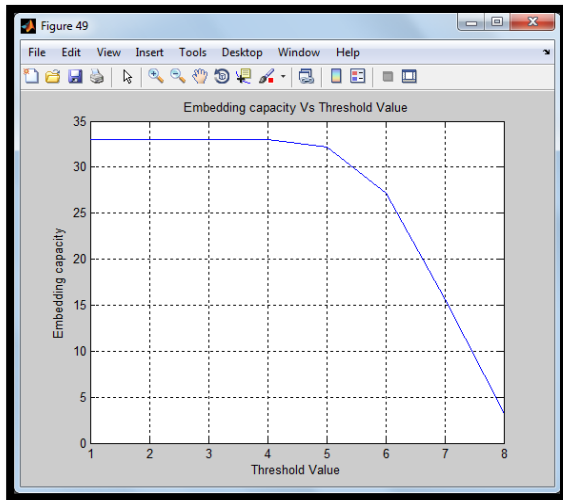


Fig.8. Embedding Capacity Graph

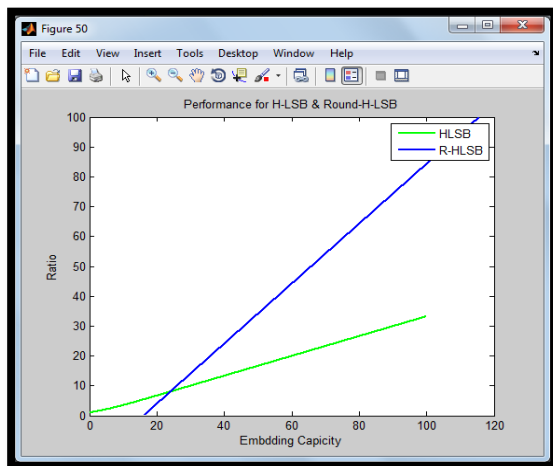


Fig.9. Embedding Capacity Comparison Graph

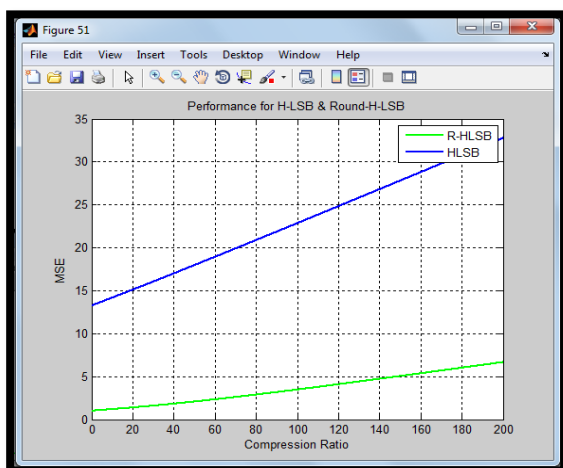


Fig.10. MSE Comparison Graph.

V. CONCLUSION AND FUTURE WORK

In this paper an improved technique for video steganography has been proposed. The technique is based

on hash based round LSB method. The proposed method has considerably improved the security and embedding capacity by hiding text and extracting it again from the video by encoding and decoding method. The security and embedding capacity is increased because of the generation of extra bit between LSB (Least Significant Bit) and MSB (Most Significant Bit). In these extra bits secret information was embed in the form of text message. The results obtain for the proposed technique are quite encouraging as PSNR, MSE and Embedding capacity values are improved in comparison to H-LSB. PSNR value of H- Round LSB is 44.7740 which is improved in comparison H-LSB which is 13.4594, MSE value of H-Round LSB is 0.2 which is improved in comparison H-LSB which is 9.4, Embedding capacity of H- Round LSB is 33 which is improved in comparison H-LSB which is 13. In future proposed method can be applied to other file formats. An image file and an audio file and a video can be hidden in a cover video file by security issue may be fully resolved.

ACKNOWLEDGMENT

The authors wish to thank all facility members of Deenbandhu Chhotu Ram University of Science & Technology, Murthal for their guidance and their support .

REFERENCES

- [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] Koushik 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. DOI: 10.5121/ijstpm.2012.2201.
- [4] Shashikala Channalli 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, Michiharu Niimi and Eiji Kawaguchi "Bit-plane decomposition steganography using wavelet compressed video" ICICS-PCM IEEE december 2003.
- [8] Prof. D P Gaikwad , Trupti Jagdale, Swati Dhanokar, Abhijeet Moghe, Akash Pathak "Hiding the text and image message of variable size using encryption and compression algorithm in video steganography" International Journal of Engineering Research and

- Applications (IJERA) 2011 ISSN: 2248-9622 Vol. 1, Issue 2, pp.102-108. www.ijera.com.
- [9] Ankit Chaudhary, J. Vasavada, J.L. Raheja, Sandeep Kumar, Manmohan Sharma "A hash based approach for secure keyless steganography in lossless RGB images" The 22nd International Conference on Computer Graphics and Vision Russia, Moscow, October 01- 05, 2012.
- [10] A.Hamsathvani "Image hiding in video sequence based on MSE" International Journal of Advanced Research in Computer Science and Software Engineering 2014 ISSN-2277-1956 volume1, Number 3, www.ijecse.org.
- [11] A.Swathi, Dr. S.A.K Jilani "Video steganography by LSB substitution using different polynomial equations" International Journal Of Computational Engineering Research (ijcer) Vol. 2 Issue-5, Issn 2250-3005(online) September| 2012.
- [12] 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.
- [13] 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.
- [14] Poonam V Bodhak, Baisa L Gunjal "Improved protection in video steganography using DCT & LSB" International Journal of Engineering and Innovative Technology (JEIT) Volume 1, Issue 4, April 2012.
- [15] Sateesh Gudla, Suchitra Reyya, Aswini Kotyada, Aditya Sangam "Key based least significant bit (LSB) insertion for audio and video stegnography" International Journal of Computer Science Engineering Research and Development ISSN 2248 - 9363(Print) ISSN 2248 - 9371(Online), Volume 3, Number 1 Jan- March (2013), pp: 60-69 © PRJ Publication, http://www.prjpublication.com/IJCSERD.asp.
- [16] 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.
- [17] Dr.ManishShrivastava, Richa Ranjanand, SushmitaKumari "Video steganography using pixel intensity value and LSB technique" International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 3 Issue: 2 February 2015, Available @ http://www.ijritcc.org.
- [18] 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/ijstpm.2015.4102.
- [19] Vaishali B. Bhagat, Prof. P. N. Kulkarni "Audio and video steganography: using LSB and phase encoding algorithm" International journal of pure and applied research in engineering and technology a path for horizing your innovative work ISSN: 2319-507X 2015; Volume 3 (9): 1640-1648 Research Available Online at www.ijpret.com

Authors' Profiles



Koulmal Kaushik was born in Nasirabad Rajasthan India in January 1, 1991. She received her B.Tech Degree in Information Technology from Bharat Institute of Technology, Sonapat (BITS) in 2012. Now she is doing her M.Tech from Deenbandhu Chhotu Ram University of Science and Technology, Murthal (Haryana) INDIA. Her research intrests are in the area of Information Hiding and Computer Networks. She has published her paper in a conference of repute.



Dr. Suman has been into teaching and research for about 14 years. She did her Ph.D. from Deenbandhu Chhotu Ram University of Science and Technology, Murthal (Haryana) INDIA. Her research areas include Network Security and Heterogeneous Wireless Networks. She received her M.tech. deegree in Computer Science & Engineering from Kurukshetra University, Kurukshetra, INDIA. She has published more than 20 papers in various journals and conferences of repute.

How to cite this paper: Koulmal Kaushik, Suman, "An Innovative Approach for Video Steganography", IJCNIS, vol.7, no.11, pp. 72-79, 2015.DOI: 10.5815/ijcnis.2015.11.08