Implementation of Random Byte Hiding algorithm in Video Steganography

S.Aswath[1], K.Akshara[2], P.Pavithra[2], D.S.Abinaya[2]

Asssisant Professor[1], Student[2] (IV Year)

Department of Electronics and Communication Engineering

TRP Enginnering College,Irungalur,Trichy-621105.

Abstract-

Steganography is an art of hiding secret information inside a cover information. The challenge is how strong the hiding procedure is built. Here a novel algorithm is presented where the secret video is hidden inside a cover video using Random Byte Hiding technique. Additional frame is added after each frame that indicates the secret message pixel value called Map frame. Map frame is hidden in the cover video by LSB technique. Thus the proposed RBH is double secured when compared with other techniques like LSB, DWT, DCT. MATLAB is used to simulate the result.

Keywords: RBH, secret message, cover video, steganalysis, stego-video.

I. INTROCDUCTION

Steganography is the hiding of secret message within an ordinary message and the extraction of it at its destination[1]. Steganography takes cryptography[2]a step father for hiding an encryption message so that no one can suspect it exists. Ideally anyone scanning your data will fail to know, it contains encrypted data.

Cryptography is the practice and study of secure communication. The unauthorized person cannot read the data. "stegano" means covered or protected and „graphia" means writing.

II. VIDEO STEGANOGRAPHY

They are two methods in video steganography,

i. Frame to frame conversion (spatial domain) [3]

ii. Converting frames into frequency domain (frequency domain)[4]

Video steganography is classified into two types as lossy[5]and lossless steganography[6]. Lossless- secret and cover message can be retrieved without any errors or modification. Lossy- secret message can be retrieved absolutely while the cover message may have some errors or distortion.

In lossless steganography technique, the messages can be send and receive safe. Video files cannot be hacked. The original video and message file can be retrieved without any loss after encryption and decryption of steganography.

In lossy steganography, the data can be stored at LSB location or particular pixel value. For example, JPEG (Joint Photographic Experts Group) format files offers high compression, but may not maintain the original image"s integrity hence it is called lossy steganography.

III. TECHNIQUES IN VIDEO STEGANOGRAPHY

1.*DCT:*

The discrete Cosine transform (DCT) transforms [7] the image from spatial domain to frequency domain. DCT separates the image into spatial sub-bands with respect to its visual quality. i.e., high, middle and low frequency components.

In DCT based technique, DCT coefficients are obtained for the given carrier image. The secret data is embedded in the carrier image for DCT coefficients lower than the threshold value. To avoid visual distortion embedding of secret information is avoided for DCT coefficients Value 0.

There is a major disadvantage of DCT. i.e., while the input from preprocessed 8x8 blocks are integer valued, the output values are typically real-valued. Thus there is a need of quantization step to make some decisions about the values in each DCT block and produce output that is integer-valued.

2.*DWT*:

Discrete wavelet transform (DWT)[8], which transforms a discrete time signal to a discrete wavelet representation. The DWT is because of inherent multi-resolution nature, wavelet-coding schemes for applications where scalability and tolerable degradation are important.

Lifting scheme of DWT has been recognized as a faster. The basic principle is to factorize the poly-phase matrix of a wavelet filter into a sequence of alternating upper and lower triangular matrices and diagonal matrix. Applications of DWT can be medial application, signal de-noising, data compression, image processing. It operates at a maximum clock frequency of 99.197 MHZ.

The disadvantage of DWT is that greater complexity and resources required to perform the computation in memory time or signal in the frequency domain. The theory is difficult to understand and more difficult to interpret the results.

3.*LSB:*

Secret information is embedded into the cover image pixel values by spatial domain technique and LSB is one among the spatial domain image steganography[9]. The LSB is the least significant bit in the byte value of the image pixel. It is a simple embedding. Perceivable by average human vision is less when compared with precision level of many image formats. It will create some alterations in the color image. In this LSB technique, one message byte can be held by four bytes of pixel the rest of the bits in the pixels remain same.

The algorithm for encryption in LSB based steganography technique is,

1. Frame size of cover video is identified.
2. Secret video‟s message is rearranged into bit stream.
3. Bit stream is rearranged into small group of row and column size bit groups.
4. Hidden message portion is rearranged with respective hidden pattern.
5. Frames are extracted from cover video.
6. Encrypt the messages in LSB of each frame‟s pixel.
7. Finish encryption then go to step 4
8. Form the rules for the extraction of frames for the receiver and put it on first frame.
9. Video that have hidden message is generated by integrating all frames that contains hidden information into a video.

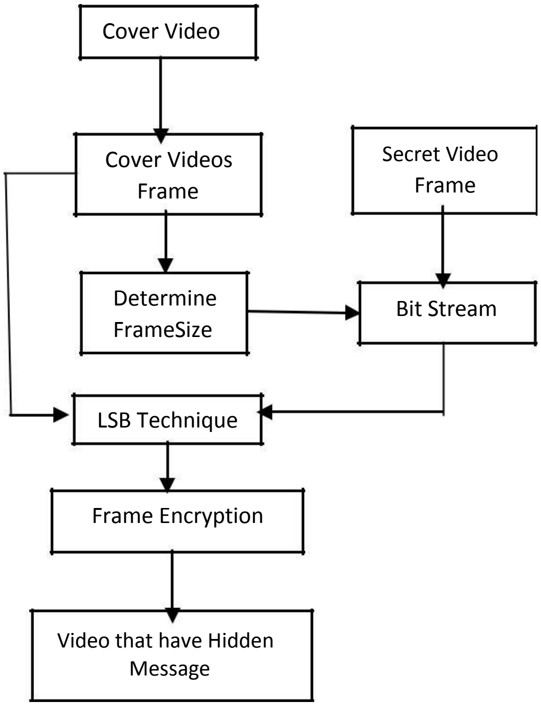


Fig: steganography encoding for LSB technique

Decoding is the reverse process of encoding or encryption process. The algorithm for decryption in LSB based steganography technique is,

1. Read the video that has hidden or secret message
2. Frames are extracted from the video.
3. From the first frames rules is read (for example., frames that contain message, number of message per frames).
4. Eliminate frames that does not have hidden or secret message in the frames.
5. In frame, by extracting the least bit of each pixel decrypt the small messages.
6. If the decryption process is not completed go to step 5.
7. Bit stream is rearranged to byte stream.
8. By specific format integrate the message.
9. Secret message can be generated.

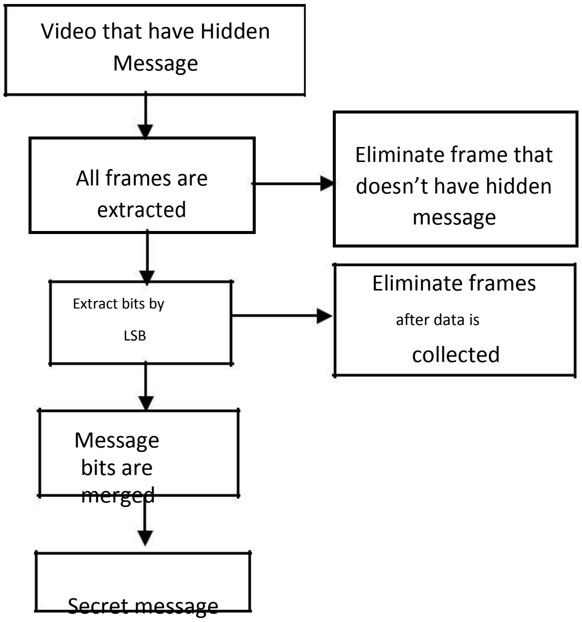

Video that have Hidden Message
All frames are extracted
Eliminate frame that doesn't have hidden message
Extract bits by LSB
Eliminate frames after data is collected
Message bits are merged
Secret message

Fig: steganography for decoding using LSB technique

The major disadvantage of LSB technique is that the decryption can be very easy and there is no high level of security in this technique.

4.RANDOM BYTE HIDING TECHNIQUE:

In random byte hiding technique (RBH)[10], the secret information is hidden in each frames at different pixel value. For example, the secret video frames are retrieved and the secret frame first pixel say „pp‟is added with some „y‟ value and store „y+pp‟ in the cover videos frame value. i.e., storing the „y+pp‟ value in „s‟ pixel value in cover videos frames. (y+pp=s). For example, 260+50=310. The „y‟ value should beabove 255(a bit higher than the logical bit level). This „s‟ pixel value can be stored in some new frame that is added after every frame in the cover video while hiding the secret video frames. This additional frame is called map. Because the map directs the decryption of the secret video from the cover video. The map is then encrypted using LSB technique in the cover video. So that the security level will be double and it will be hard to decrypt the secret message from the video.

In lossless steganography, specific location is needed to store the hidden information or message and it will take some valuable time to run the algorithm. Because of the delay in the run time the real time application is somewhat harder to implement and the system specification is responsible.

In lossy steganography, the information or message is stored in LSB or at some specific location of the pixel. So the implementation of lossy steganography in real time application is feasible in the normal system specification.

Algorithm for the encryption in random byte hiding technique can be written as,

1. Read the cover video.
2. Identify the frame size of cover video.
3. Read the secret video and determine its frame size.
4. Extract each frames from the cover video and read it.
5. Encode the secret message into each frame by random byte hiding technique.
6. A new frame is added after each cover video frame to map the storing pixel value of secret video messages.
7. That the new frame (map) is hidden into the cover video by LSB technique.
8. Then the stego-video (secret video is hidden inside cover video) is generated.

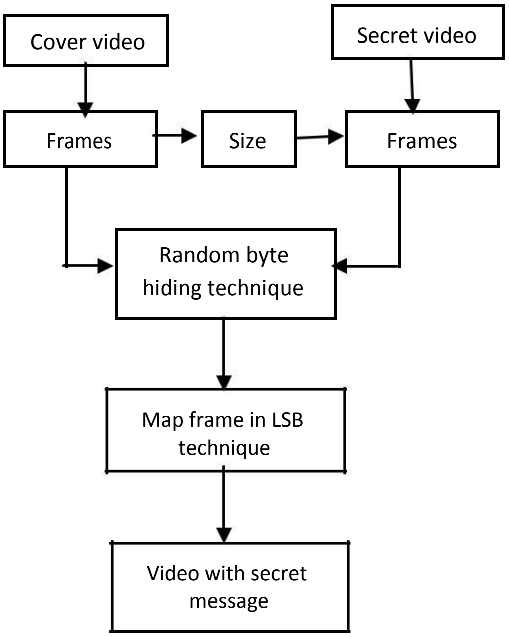

Cover video
Secret video
Frames
Size
Frames
Random byte hiding technique
Map frame in LSB technique
Video with secret message

Fig: Encoding in video steganography with RBH

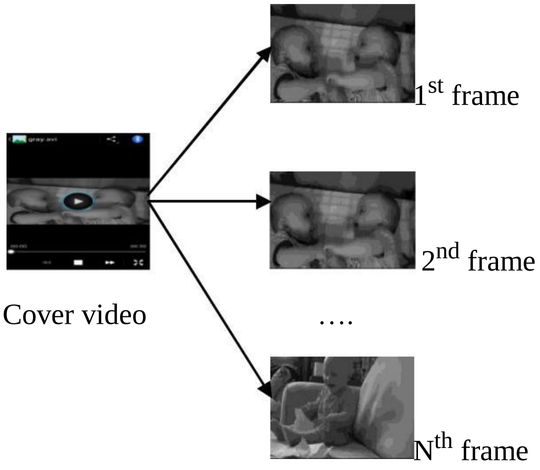


Fig: Separation of frames from cover video

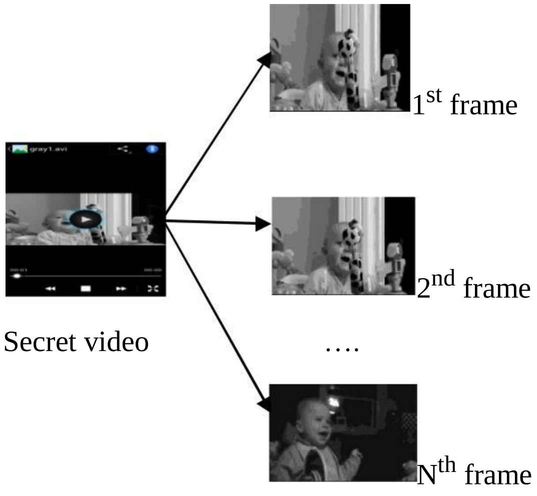


Fig: Separation of frames from the secret video

Algorithm for the decryption in random byte hiding technique can be written as,

1. Stego-video is read.
2. Frames are extracted from the stego-video.
3. Map is decoded with least significant bit method.
4. Decode the frames by random byte hiding technique.
5. Put all the decrypted pixel values and extract the secret information or message as frames.
6. Frame the secret frames as video.
7. Then the cover video and secret video is retrieved.

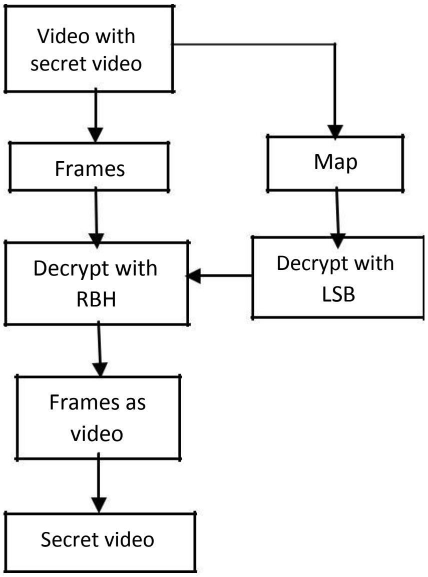


Fig: Decoding in video steganography with RBH

ENCRYPTION AND DECRYPTION TIMING ANALYSIS:

Encryption in RBH is hard to decrypt when comparedwith other steganography techniques and the encryption and decryption time is also less in RBH technique.

Technique	DCT	DWT	LSB	RBH
Encryption timing (in seconds)	116.14	94.87	76.16	88.21
Decryption timing (in seconds)	132.41	102.24	81.25	90.78

Fig: Encryption and decryption timing analysis of various steganography techniques.

First Step Of Encryption:

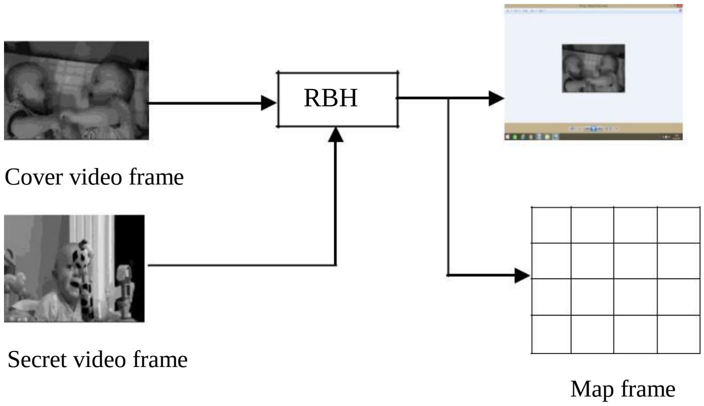
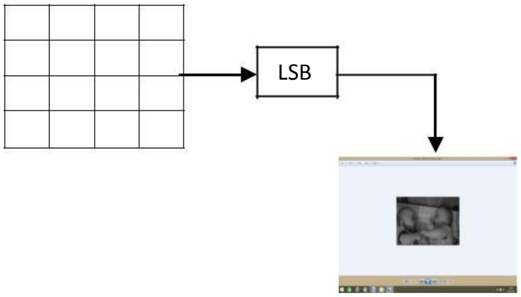


Fig: Encryption process using RBH techniques.

Second Step Of Encryption:



Encrypted frame

Fig: Encrypting the map frame into encrypted frame in LSB technique

Decryption:

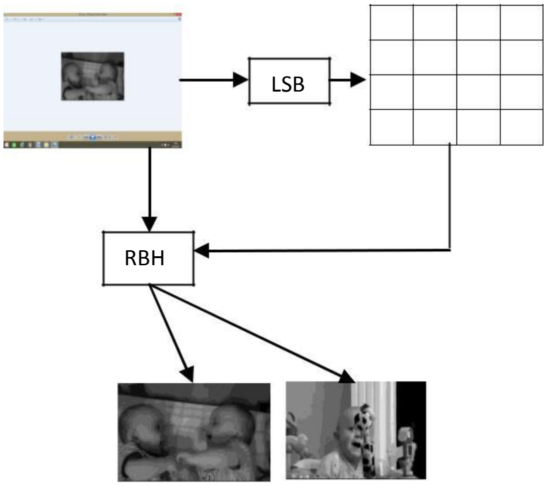


Fig: Decryption process from the encrypted video frames

IV COMPARISON TABLE:

The below table describe the analysis of various steganography techniques like DWT, DCT, LSB and RBH.

TECHNIQUE	VIDEO FILE	PSNR(dB)	MSE(dB)
DWT	Cover video	44.76	1.4741
	Secret video	44.96	1.4405
DCT	Cover video	55.6	0.4208
	Secret video	58.3	0.3047
LSB	Cover video	52.786	0.5850
	Secret video	53.7558	0.5234
RBH	Cover video	57.23	0.5854
	Secret video	59.462	0.4781

Fig: comparison of various steganography technique

.

V. CONCLUSION:

Steganography is the secured way of communication. There are many hiding techniques like DCT, DWT, LSB and random byte hiding technique and it is not necessary to use a technique that is already exist. In this proposed method the encrypted video is doubly secured and the receiver who knows the decryption methodology can only decrypt the secret video from the cover video. No one knows the secret video is inside the cover video. Thus the hybrid system uses the high security and the secret video is retrieved.

VI. REFERENCES

[1] Ramadhan Mstafa, Christian Bach, “Information Hiding in Images Using Steaganography Techniques”, Northeast conference of the American society for Engineering Education (ASEE). DOI:101.13140/RG2.1.1350.9360, March 2013.

[2] Vikas Tyagi, “Data Hiding in image Using least significant bit with cryptography”, International Journal of Advanced in computer science and software Engineering, volume 2,issue 4,April 2012.

[3] Manish Kumar Saini, Deepak Narang, “Review on Image Enhancement in Spatial Domain”, Proc. Of International conference on advanced in signal processing and communication, 2013.

[4] Pedro A.A.Assucao and Mohammed Ghanbari, “A Frequency-Domain Transcoder for Dynamic Bit-Rate Reduction of MPEG-2Bit streams”, IEEE Transactions on Circuits and systems for video technology, vol 8, No.8, December 1998.

[5] Mohmud Hasan, Kamruddin Md.Nur, Tanzeem Bin Noor, “A Novel Compressed Domain Technique for Reversible Steganography”, International Journal of Advanced Research in computer science and software engineering, volume 2, issue 3, March 2012.

[6] R.Vijayarejeswari, A.Rajiv Kannan, J.Santhosh, “A Simple Steganography Algorithm Based on Lossless Compression Technique in WSN”, Circuits and system, 2016.

[7] Juan-juan Gu, Liang ao, “DCT-based Real-valued Discrete Gabor Transforms and its fast”, International colloguium on computing, communication, control and management, 2008.

[8] K.Ayyappa swamy, C.Somasundar Reddy, K.Durga Sreenivas, “Image Compression using Hybrid DCT-DWT transform”, International Journal of Advanced Research in Computer science and software engineering. Volume 5, issue 5. May 2015.

[9] G.S.Sravanthi, B.Sunitha Devi, S.M.Riyazoddin, M.Janga Reddy, “A Spatial Domain Image Steganography Technique Based on Plane Bit substitution Method”, Global Journal of computer science and Technology. Volume 12, issue 15,2012.

[10] Ashish T.Bhole, Rachna patel, “Steganography over Video File using Rnadom Byte Hiding technique and LSB technique”, IEEE International conference on computational Intelligence and computing research, 2012