IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 5, Ver. I (Sep - Oct .2015), PP 14-20
www.iosrjournals.org

Design of Random Scan Algorithm in Video Steganography for Security Purposes

Sahil Gupta[1], Jyoti Saxena[2] and Sukhjinder Singh[3]
[1, 2, 3]Department of ECE, GianiZail SinghPTU campus, Bathinda-151001, Punjab (India)

***Abstract**: Steganography is defined as the process of hiding information in a multimedia carrier. In this paper, video is taken as a carrier to hide information. To achieve Undetectability and robustness of the hidden data, Random Scan approach is used. To make the data more secure encryption is done on the data before hiding. Experimental results show that MSE, PSNR are better forMLSB technique whereas Correlation factor is better for Random scan technique.*

***Keywords:** Modified Least Significant bit (MLSB), Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Correlation.*

I. Introduction

Internet is the fastest medium for communication but it faces many security related problems like hacking, copyright, eavesdropping *etc.*There are various techniques for security of data likecryptography and steganography. Cryptography is a technique which is used to secure the secrecy of communication. There are many different methods to encrypt and decrypt the data in order to keep the message secret. Unfortunately, it is not enough to keep the content of a message secret, at the same time it is also important to keep the existence of message secret. The technique in which the existence of hidden message is kept secret is called as steganography [1].

Steganography (literally meaning *coveredwriting*) dates back to ancient Greece, where common practices consisted of etching messages in wooden tablets and covering them with wax, and tattooing a shared messenger's head, letting his hair grow back , then sharing it again when he arrived at his contact point [2].

Steganography is the art of hiding message into cover objects such as images, text, videos [3].Images had been mostly used media for data hiding. But now a day, video steganography is used for hiding data in a more secure hiding way than in images as data capacity of video is more than images. A Steganography system consists of three elements: cover object (which hides the secret message), the secret message and the stego object (which is the cover object with message embedded inside it) [4].

The paper is organized as follows; section II starts with literature Survey, section III gives the Experimental setup in which block diagram and algorithm with examples is explained. Section IV illustrates the results in which MSE, PSNR and Correlation factor ofRandom scan technique is compared with Modified LSB technique. The conclusion and scope of future work is discussed in section V.

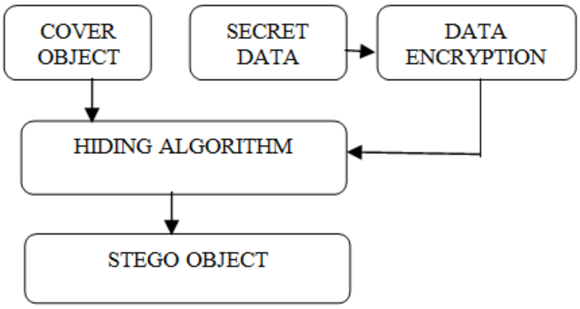

Fig. 1 Block Diagram of Steganography

Figure 1 shows the fundamental block diagram of Steganography. In Steganography cover file and secret data is read. Then encryption algorithm is applied on secret data followed byhiding algorithm applied onencrypted data to hide in cover object. After thatstego object is transmitted.At receiver side recovery algorithm is applied on stego object for extracting secret data.

II. Literature Survey

In the literature, various steganography techniques for digital images have been proposed. However, the digital videos, one of the most suitable cover for data hiding was less considered.

SamidhaS*et.al* [5], discussed various image steganography techniques based on spatial domain. Spatial domaintechniques are based on physical location of pixels in an image. Generally 8 bit gray level or color images can be used as a cover to hide data. Random bits from these bytes are used to replace the secret data bits.

Bhautmage*et.al*[6], presented new technique for data embedding and extraction for AVI (audio video interleave) videos in which instead of changing the LSB of the cover file, the LSB and LSB+3 bits are changed in alternate bytes of the cover file. The secret message is encrypted by using a simple bit exchange method before the actual embedding process starts. An index is created for the secret information and the index is placed in a frame of the video itself. With the help of this index, the secret message can be extracted easily, which also reduce the extraction time.

Dasgupta*et.al* [7],proposed hash based technique for video steganography. Eight bits of the secret information is divided into 3, 3, and 2 bits, and thenembedded into the RGB pixel values of the cover frames respectively. A hash function is used to select the position of insertion in LSB bits.

Kelash*et al.* [8], proposed algorithm to hide message within part of frame or in whole frame based on HCV (histogram constant value). The random selection of frame increases security level and to increase embedding capacity, faded pixel were reduced in each frame.

In this paper motivation is taken from [5, 6, 7 and 8] and proposed a technique for data hiding. In this technique before hiding, the encryption of data is done in which the negative of data is generated by doing complement. After that data is made to hide using Random Scan and MLSB Techniques.

III. Experimental Setup

In this work, Random Scan and MLSB techniques are implemented usingMatlab platform.Figure 2 shows the experimental set up of this process in which the secret message is hidden in anyvideo frame as cover.

- Cover Video: Video consists of images as well as audio. Hence both images and audio are considered for steganography.
- Frame Extraction: Frame extraction is the process of extracting frames from the video. Video is converted into frames. From the frames one frame is selected for embedding.

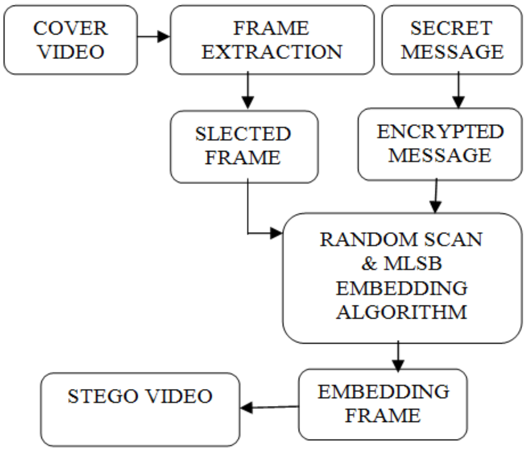

Fig. 2 Experimental setup of Video Steganography

- Secret Message: The secret data is in any form like text, audio, image. In the proposed algorithm the encryption of data is done. For encryption the negative of data is generated.
- Embedding Algorithm: For embedding the encrypted data, Random Scan and MLSB technique is applied. In Random scan technique for hiding bits, 1 to 4 bits are taken from LSB side randomly because as the bit goes from 4th to 5th bit there is large variation in pixels whereas in MLSB technique, data is hidden at 2 LSB positions only.
- Stego Video: After embedding the encrypted data in frame, the reconstruction of video is done and stego video is generated.

3.1 Algorithm

The step by step algorithm for video steganography is explained below:

Step 1: Read the video file.
Step 2: Extract the frame from video file.
Step 3: Read the secret data

Step 4: Encryption Algorithm is applied on secret data.
Step 5: Split the data into 2-2 bits for hiding.
Step 6: The encrypted data is hidden in cover frame using Random Scan and Modified LSB Technique.
Step 7:Compare MSE and PSNR of random scan technique with MLSB technique.

Example

1. Cover Frame Pixels

Table 1 Cover Frame Pixel

Cover data of Ist Row	01011010	01010101	11001100	10111011
Cover data of Second Row	00011100	00111100	11100001	10001000

2. Data value: 10110111
3. After Encryption Data Value: 01001000
4. Stego Frame Pixel values after Modified LSB Technique

Table 2 Stego pixel after MLSB Technique

Cover data of Ist Row	01011010	01010101	11001100	10111011
Encrypted data shifted to 2 LSB	000000**00**	000000**10**	000000**00**	000000**01**
Data Embedding using replacement	**01011000**	**01010110**	**11001100**	**10111001**
Bit Variation	2 bit	1 bit	No	2 bit
Cover data of 2^{nd} Row	00011100	00111100	11100001	10001000

5. Stego Frame Pixel Values after apply Random Scan Technique

Table 3Stego pixel after Random Scan Technique

Cover data of ist Row	01011010	01010101	11001100	10111011
Encrypted data shifted to 2 LSB	0000**00**00	000000**10**	0000**00**00	000000**01**
Data Embedding using EXOR	**01011010**	**01010111**	**11001100**	**10111010**
Bit Variation	No	2 bit	No	1 bit
Cover data of 2^{nd} Row	00011100	00111100	11100001	10001000

3.2 Performance Metrics

To measure the imperceptibility of steganography several metrics are used.The metrics indicate how similar or different the stego image is from cover image.The following metrics are used:

1. **Mean Square Error (MSE)** is computed by performing byte by byte comparison of the cover image and stego image. The Computation formula is expressed as[4]

$$\mathrm{MSE} = \frac{1}{M*N} \sum_{1}^{M} \sum_{1}^{N} (\mathrm{Fij} - \mathrm{Gij})^2 \qquad (1)$$

M: numbers of rows of cover image
N: number of column of Cover Image
Fij: Pixel value from cover image
Gij: Pixel value from Stego Image

Higher value of MSE indicates dissimilarity between Cover image and Stego image.

2. **Peak signal to noise ratio (PSNR)** measures in decibels the quality of the stego image compared with the cover image. The higher the PSNR better the quality. PSNR is computedusing the following equation.

$$\mathrm{PSNR} = 20 \log_{10} 255 - 10 \log_{10} \mathrm{MSE} \qquad (2)$$

3. **Correlation Factor**: Correlation factor is one of the performance parameters. Correlation factor ‘r’ is the measure of extent and direction of linear combination of two random variables. If two variables are closely related, the correlation factor is close to the value 1. On the other hand, if the factor is close to 0, two variables are not related.

$$r = \frac{\sum_i (Xi - Xm)(Yi - Ym)}{\sqrt{\sum_i (Xi - Xm)^2}\sqrt{\sum_i (Yi - Ym)^2}} \qquad (3)$$

Where

Xi - Pixel intensity of original image
Xm- Mean value of original image intensity
Yi- Pixel intensity of encrypted image
Ym - Mean value of encrypted image intensity

IV. Results and Discussion

In this paper, Random Scan and MLSB Techniquesare implemented in MATLAB 2013. The experiment is carried out on two different video files namely (visiontraffic.avi) and (atrium.avi) which is used as a cover file and six images are used as secret data.

Cover media file

In this process visiontraffic.avi and atrium.avi video having resolution of 360*640 has been used as a cover media. Figure 3 shows the frame extraction from visiontraffic.avi and atrium.avi video.

Fig. 3 Frame Extraction from visiontraffic.avi and atrium.avi

The features of these cover file have been shown in table 4.

Table 4 Cover video

S. No	Cover video file information			
	Name of video file	**Resolution (W*H)**	**Frames/sec**	**Total frames**
1.	Visiontraffic.avi	360*640	29	531
2.	atrium.avi	360*640	30	431

4.1 Secret data

In this process image taken from MATLAB data base has been used as secret data which is to be hidden in cover media.

Scene_right **Parkinglot_right** **Vision team1**

Vipstereo_halwayLeft **Stopsigntest** **Yellowstone_right**

Fig.4 Secret data images

The features of these secret images have been shown in table 5

Table 5 Secret Data

S.No	Secret data image information		
	Name of image	Size	Format
1.	Scene_right	284*512	Png
2.	Vipstereo_halwayLeft	300*400	Png
3.	Parkinglot_right	480*640	Png
4.	Yellowstone_right	480*640	Png
5.	Stopsigntest	368*653	Jpg
6.	Vision team1	582*800	Jpg

Stego Video

The secret imageis embedded in cover video with the help of two techniques namely:

- Random Scan method
- Modified LSB method

This is the stego frame generated after hiding parkinglot_right image in visiontraffic.avi video using Random scan technique.

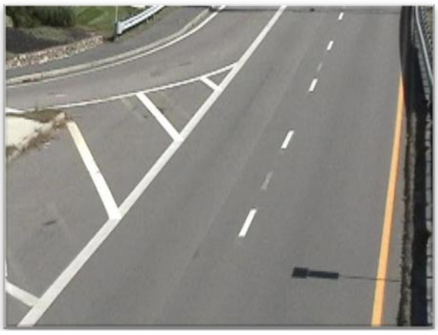

Fig. 5Stego Frame after hiding parkinglot_right image in cover Frame

Similar stego frames can be generated after hiding othersecret images in cover files.

For Steganography, the Correlation factor should be 1 for ideal Case so that there is no dissimilarity in stego image as compared to cover image.

The MSE, PSNR and Correlation factor of Random Scan technique is compared with Modified LSB technique in table 6 and table 7 for visiontraffic and atrium video respectively.

Table 6 Comparison of MSE, PSNR and Correlation values (visiontraffic.avi)

Secret image	Results obtained using Random Scan			Results obtained using MLSB		
	MSE	PSNR	Corre lation	MSE	PSNR	Correl ation
Parkinglot_right	4.87	43.25	.998	.370	47.76	.992
Scene_right	5.63	42.49	.998	.405	47.72	.992
Vision team1	5.53	42.59	.998	.383	47.74	.992
Vipstereo_halwayLeft	5.28	42.85	.998	.365	47.76	.992
Yellowstone_right	5.17	42.95	.998	.390	47.74	.992
Stopsigntest	5.27	42.85	.998	.437	47.69	.992

Table 7 Comparison of MSE, PSNR and Correlation values (atrium.avi)

Secret image	Results obtained using Random Scan			Results obtained using MLSB		
	MSE	PSNR	Corre lation	MSE	PSNR	Corre lation
Parkinglot_right	4.86	43.26	.999	.378	47.76	.987
Scene_right	5.70	42.42	.999	.405	47.72	.987
Vision team1	5.53	42.59	.999	.383	47.74	.987
Vipstereo_halwayLeft	5.38	42.74	.999	.365	47.76	.987
Yellowstone_right	5.17	42.95	.999	.390	47.74	.987
Stopsigntest	5.29	42.83	.999	.437	47.69	.987

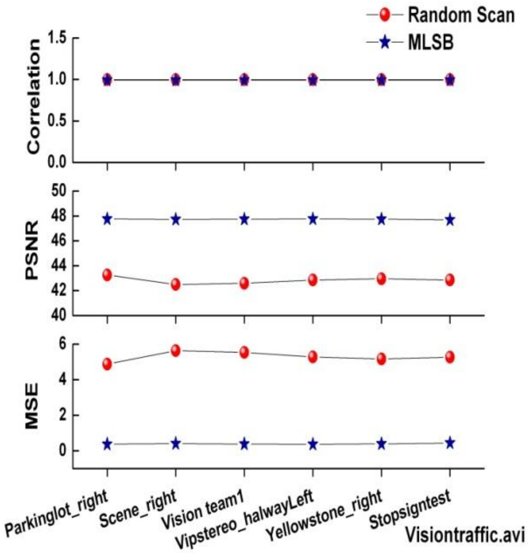

Fig.6Comparison of MSE, PSNR and Correlation factor using Random Scan and MLSB technique for Visiontraffic video

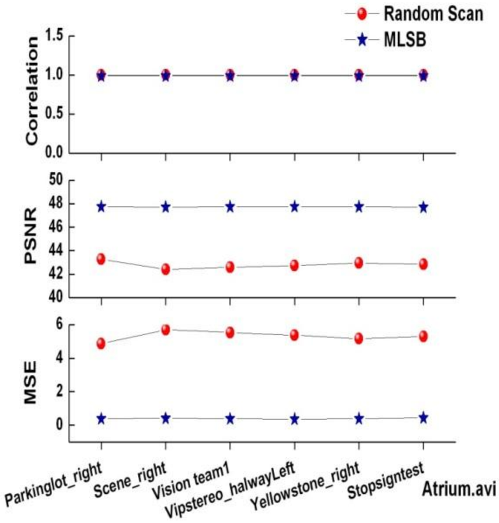

Fig. 7Comparison of MSE, PSNR and Correlation factor using Random Scan and MLSB technique for atrium video

Figure 6 and 7shows thatMSE using MLSB technique has less value as comparison to Random Scan technique. Becausethere is very small change in pixel value using MLSB technique, whereas PSNR using MLSB technique is more than Random scan technique. But Correlation factor using Random Scan Technique is better than MLSB Technique. Therefore Random scan technique is preferable over MLSB technique as per security concern.

V. Conclusion

In this work video is used as a carrier to embed secret message. In this technique the negative of secret image is made to hide in cover frame. So it is difficult to extract the original image from cover frame becausePixels are hidden at Random locations in cover frame pixels.Also even if an unknown person extracts the image from cover frame they get the negative of secret image.The figure 6 and 7 shows that the MLSB technique has better MSE and PSNR as compared to Random scan technique, but Correlation factor is better for Random scan technique. In Futuremore emphasis will be given on frequency domain due to better PSNR and MSE value as compared to spatial domain.

References

[1] S.D. Thepade and S.S. Chavan, Cosine, Walsh and Slant Wavelet Transforms for Robust Image Steganography, Tenth International Conference on Wireless and Optical Communications Networks (WOCN), 2013, 1-5.

[2] K.S.Jenifer, G. Yogaraj and K. Rajalakshmi, 2014, approach for Video Steganography to embed Images, International Journal of Computer Science and Information Technologies, 5(1), 2014, 319-322.

[3] R.G Bal, P.Ezhilarasu,An Efficient Safe and Secured Video Steganography Using Shadow Derivation, International Journal of Innovative Research in Computer and Communication Engineering, 2, 2014, 3251-3258.

[4] I. Premi and S. Kaur,Random Scan Algorithm for image steganography inScilab for security purposes, International Journal of Advanced Research in Computer and Communication Engineering, 3(12), 2014, 8876-8879.

[5] D. Samidha and D. Agrawal, Random Image Steganography in Spatial Domain, International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System, 2013, 1-3.

[6] P. Bhautmage, A.J kumar and A. Dahatonde, Advanced Video Steganography Algorithm, International Journal of Engineering Research, 3(1) 2013, 1641-1644.

[7] K. Dasgupta, J.K Mandal and P. Dutta,Hash Based Least Significant Bit Technique for Video Steganography, International Journal of Security, Privacy and Trust Management, 1(2), 2012, 1-11.

[8] H.M. Kelash, O.F.A Wahab, O.A. Elshakankiry and H. S. El-sayed,Utilization of SteganographicTechniques in Video Sequences, International Journal of Computing and Network Technology, 2(1), 2014,17-24.