First International Conference on Information Technology, Communications and Computing (ICITCC 2017)
24-December-2017, Bhopal, M.P., India | ISBN (Online): 978-81-932623-3-7 | DOI: 10.5281/zenodo.1134255

Comparative Analysis Among Steganographic LSB Variants

Namrata Singh[1]
[1] AKTU Lucknow, India
[1]nam2817210@gmail.com

Jayati Bhardwaj[2]
[2] AKTU Lucknow, India
[2]jayatibhardwaj2@gmail.com

***Abstract*- Combining the best features of steganography and cryptography is the trending concept which is being followed for the purpose of information security. Steganography provides the provision for hiding secret data in some cover file in order to make it undiscovered by the perpetrators. On the complementary, cryptography secures that secret data by manipulating its original form and converting it into an unintelligent form. Hence, making the data more powerful and secure against the prevailing security attacks and breaches. This paper represents the implementation of this combination on the two LSB variants namely sequential LSB and randomized LSB. A comparison among the two approaches is carried out by adding a secret text into a video cover file. The concept of chaotic sequence has been used as the security approach that converts the secret data into random bits pattern. The proposed work uses the traditional LSB approach as basic steganographic model. The inference on the basis of parameters concludes that the randomized LSB shows better results than the sequential LSB scheme.**

Keywords-CVSS, Hash LSB, LSB+3, Least Significant Bit (LSB).

I. INTRODUCTION

With every increase in the quality of work in the field of information security, the need to find out the best possible solutions out of the proposed ones is quite imposing. Finding out the best solutions is a result of comparative analysis being carried out on two or more than two techniques related to a relevant field. Information security concerns with two broad topics: Steganography and Cryptography. In the steganographic approaches the main concern is to find out best cover object that could hide any kind of secret file with high degree of imperceptiblity, security and whose steganalysis detection could be low. In cryptography the main concern is to make the strongest encryption with unbreakable key that could provide security at its best.

A. Metamorphic Concept

The steganography provides only the hiding provision to the secret message in any of the cover file types without being discovered/noticed by the intruder. But this approach needs additional security as the stego-data remains intact in its original form. So, the security of the secret file is achieved by applying the concept of cryptography before embedding procedure. This combination of the two wide fields leads to new concept of Metamorphic Cryptography. This metamorphic combination first secures the data through encryption and then embed the encrypted file in to the cover file. Many of research work proposed the different encryption theories and algorithm. The work hereby presented in this paper uses Chaotic Sequence concept for the encryption purpose.

B. Chaotic Sequence

Chaos is one type of complex dynamic behaviors generated by deterministic nonlinear dynamical systems and motivated by the chaotic properties such as non-periodic, extreme sensitivity to initial conditions, system parameters etc. These system are complex, non-periodic and random in time domain and widely used in encryption algorithms since 1989[16]. Chaotic arrangement has also been used in the field of cryptography for providing randomness to our information .Properties of chaotic series which makes it additional intense are:

- Unpredictability
- In decomposability
- Element of normality.

The random values created by the chaotic sequence lies in the boundary values of [0,1].

Chaotic Sequence=$\begin{cases} 0 \\ 1 \end{cases}$

Determination of the values, collection will be performed by using the following formula[17].

$$X_n+1= \mu^* X_n^*(1-X_n) \qquad (1)$$

C. Video Steganography

The video steganography is the sub branch of the steganography concept. In this methodology, the video is used as the cover medium to hide the secret message by inculcating the message bits into the redundant bits of the cover. The secret could be any of these- text, audio, video, image etc. This method of replacing the redundant least significant bits with the message bits is the well known LSB technique. This technique is quite simple and possess efficiency in meeting the requirements of an imperceptible steganographic technique. The originality is of the cover video is maintained in this technique as compared to the MSB (Most Significant Bit) technique in which the pixel values vary to a large scale after insertion of the secret data bits. Hence, it has poor perceptibility and complexity is also there with the scheme.

The paper represents a comparison among two LSB techniques by using chaotic sequence as the encryption technique. The LSB types being compared here are Sequential LSB and Randomised LSB. The secret data being hidden in the cover video file is a text of 350 bits. Main parameters on the basis of which the comparisons are being done are PSNR, MSE and SNR. Also, histograms and embedded frames are also used for the defining the best LSB approach out of the two. The formulas for the deciding parameters are as follows:

$$SNR = 10\log_{10}(P_{signal}/P_{noise}) \quad . \qquad (2)$$

$$PSNR = \ 10\log_{10}(255/MSE)^2 \, . \qquad (3)$$

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(x_{j.k} - x'_{j,k})^2 \qquad (4)$$

This paper is organized in the following manner: Section 1 contains the introductory part describing the basic concept related to the proposed work. Section 2 contains the literature survey of all the related work concerning same domain. Section 3 contains the proposed work involving all algorithms and flowcharts. Section 4 contains the results and observations while section 5 concludes the paper.

II. LITERATURE REVIEW

Paper [1] defines the scheme of LSB by using a video as cover. Text is embedded into the least significant bit of each video frame. Text message is converted into its subsequent binary format and then replaces the bits of RGB components inside each image. Decoding of the secret message is done by extracting the LSB from the encoded image/frame. Stego key is used in the form of polynomial equation which increases the bits capacity of cover video frames. A modified LSB is proposed by Mritha Ramalingam[2] in the form of stego machine. This stego machine embedded the secret text message into a video file. The work proposed an application that provided a user interface to the existing system and overcome the shortcomings of all other existing systems. The stego machine is platform independent which results in high portability and consistency. In a scheme proposed by Manpreet and Amandeep kaur, the combination of both steganography and cryptography features is used. The scheme derives insertion of text in a video cover with the help of hash LSB algorithm [3][12] with a new encryption algorithm. Hash function is used to evaluate the positions where to hide the data in the cover file. Insertions are being done using LSB. The encryption algorithm implemented here is RSA which converts the original text to the cipher text before the embedding could take place. The embedded video so produced is secure and conforms to the original video in quality terms.

The methodology of hiding acoustic data into a video file by using LSB technique is presented in the paper [4]. The redundant LSBs of the video file are replaced by the audio bits. The random number generator is used to decide the sequence of hiding audio samples into the extracted frames of the video. LSBs of Red component are being opted for the insertion of audio bits. The proposed technique shows remarkable results as minimal changes are observed after insertion i.e. embedded video resembles the original video. The PSNR and MSE values are found to be high and low respectively.

The work presented in paper [5] by Pritish et.al. introduced a new video steganographic technique for high resolution .avi files. The method changes the LSB and LSB+3 bits in the alternate bytes of the cover file (video). In order to reduce the extraction time, an index is created and placed within the frame of video. Encryption of data is done before insertion/embedding by using bit exchange method. The scheme possessed various advantages like high imperceptibility, security, less computational time and increased capacity. Similarly index based more secure video steganography is mentioned in [6]. The technique used index for hiding secret information in the cover video at a selected frame location. This simplifies the decoding and extraction procedure by analyzing only selected frames as defined by the index. This reduces computational time as the extraction is done selectively instead of sequentially frame by frame. The proposed scheme claimed to be more secure with the extraction time. The comparison among LSB and Random byte hiding technique is done by Ashish and Rachna [7]. The work shows the advantage of using video as cover by overcoming the disadvantages of using image as cover. The lossy type technique is implemented as lossless type technique is quite complex and require more run time. The results inferred the random byte hiding technique as the better one as compared to LSB. The encryption and decryption time taken is quite less in random as compared to the LSB.

Another approach of video steganography of hiding a video into another video is proposed in paper [8].The extracted frames are converted into 8-bit binary values and XORed for encryption purpose. The encoding of each encrypted bits of frames is done sequentially by using LSB technique. The insertions are being done in the RGB components of the cover video frames. The results are highly secure resulting in no distortion in the quality of video (both cover and secret). Mohamed Elsadig et.al [9] used LSB technique along with 3-3-2 embedding approach for video steganography. 3-3-2 approach defined the number of bits to be stored at the RGB plains respectively. However, the insertion is being done sequentially using LSB technique. A new video steganographic approach using LSB is proposed in [10] where security is inculcated by generating an indexed based chaotic sequence and arranging the frame pixels in accordance to it. This provides randomization to the pixels. Information is embedded into the video frames where the scene chances abruptly. The results show high quality of imperceptibility amongst the videos. A steganographic technique of hiding text into a video cover is mentioned in the paper by Sunil and Rajshree [11]. The approach used computer forensics for authentication purpose. Comparison among different LSB approaches is done- 1LSB, 2LSB and 4LSB. The paper concludes 4LSB as an effective algorithm for the large amount of secret data hiding purpose. CVSS (Compressed Video Secure Steganography) is the new algorithmic approach defined by Bin Liu et.al. [13]. The variance of each frame decides the embedding payload. Compressed domain is used for both embedding and detection. Steganalysis is done on the basis of collision based video Steganalysis algorithms. Visually no distortion is observed in the cover file after embedding procedure.

Improving the performance of video steganography through Artificial Neural Network (ANN) and Backpropagation Neural Network (BPNN) is defined in paper [14]. Secret message is hidden in the frame by XORing bits through a trained neural network which leads to improved security. The selection of symmetric key and bit position (index) is also performed by the neural network.

LSB implemented on cover image with different image formats is implemented in [15]. Comparison between different image formats namely BMP, GIF and PNG is carried out in the paper. BMP format is found to be more secure with less distortion and low steganalysis detection. Also, amount of data embedded is comparatively high.

III. PROPOSED WORK

A. Algorithm for Sequential LSB Coding

1. Embedding Algorithm.

```
1. User inputs:
   a) videofile.
   b) textfile.

2. Read the Video and Text files.
   a) Read the Video file.
   b) Read the Text file.

3. Convert Text file to Binary data stream.
   a) Convert the text data to binary format.
```

b) Convert the binary data to a binary stream.

c) Find out the required number of LSB's to hide data.

4. Extract all video Frames into variable 'v'.

a) Take the variable K for frame counter.

b) Read the Video file.

c) Keep looping for all frames.

d) Compile all frames in the 4th dimension of variable 'v'.

e) The total number of LSBs available in video file is found.

5. Space check.

a) if (reqspace > availspace), we get the error message.

display('The video file does not have enough pixels/size to hide secret text ');

b) if (reqspace < availspace), we simply embed the text into the video file.

6. Lsb embedding

a) Use ctr is for the text bits.

b) Calculate the each Row pixel number.

c) Calculate the each Column Pixel number.

d) Select the channel (1,2,3) red, green or blue.

e) Calculate the each frame of the video.

f) The original pixel value converted to binary.

g) Apply Chaotic sequence formula to the message bits

XOR chaotic sequence with the LSB of each frame

g) Embed: Change the LSB value to the XORed bits.

h) Convert to decimal.

i) Assign to new pixel value.

j) Put the coded video into this variable.

7. Write coded Video in a New file.

a) Create a VideoWriter object for a new video file. Use the 'Archival' profile to specify a Motion JPEG 2000 file with lossless compression.

b) Open the file/Writer.

c) Loop for all frames.

d) Write all the frames.

e) Get the embedded video.

2. Extraction Algorithm.

1. User inputs.

a) video file: this is the file which has coded video.

b) text size: length of text data to be extracted.

2. Extract all video Frames into variable.

a) Take the variable K for frame counter.

b) Read the Video file.

c) Keep looping for all frames.

d) Compile all frames in the 4th dimension of variable 'v'.

e) The total number of LSBs available in video file is found.

3. Lsb extraction

a)reqspace = textsize.

b) Use ctr is for the text bits.

c) Calculate the each Row pixel number.

d) Calculate the each Column Pixel number.

e) Select the Channel (1,2,3) red, green blue.

f) Calculate the each Frame of the video.

g) The Original Pixel Value converted to binary.

h) Extract: Get the LSB value (i.e the hidden text bits)

Reverse XOR the bits

Get the real message bits and the LSB of original video

i) Convert the LSBs of each frame.

j) Get the original video and text.

B. Algorithm for Random LSB Coding

1. Embedding Algorithm

1. User input:.

a) videofile.

b) text file.

2. Read the Video and text files.

a) Read the Video file.

b) Read text in native integer format.

3. Convert Text file to Binary data stream.

a) Convert the text data to binary format.

b) Convert the binary data to a binary stream.

c) Find out the required number of LSB's to hide data.

4. Extract all video Frames into a variable say 'v'.

a) Take the variable K for frame counter.

b) Read the Video file.

c) Keep looping for all frames.

d) Compile all frames in the 4th dimension of variable 'v'.

e) The total number of LSBs available in video file is found.

5. Check for the space condition for embedding

a) If(reqspace > availspace), we get the error message.

display('The video file does not have enough pixels/size to hide secret text');

b) If(reqspace < availspace), we simply embed the text into the video file.

6. Here we define Random algorithm.

a) Use CryptGenRandom to generate random number for frame selection.

7. Lsb embedding

a) Use Random variable ‘r’ containing the frame number.

b) Find the length of the message.

```
m = length(message) * 8;
```

c) Convert it into the AsciiCode.

```
AsciiCode = uint8(message);
```

d) Transpose (decimal to binary)

```
binary_String = transpose(dec2bin(AsciiCode,8));
binary_String = binary_String(:);
```

e) Find out the length.

```
N = length(binary_String);
I = zeros(N,1);
```

Apply Chaotic Sequence Formula on message bits(For Encryption)

Message bits are converted into random sequences.

XOR the random bits with the LSBs of frame.

f) Find out the height and width of random frame.

```
height = size(im,1);
width = size(im,2);
```

g) Change the LSB value to the message bits resulted by XORing.

```
LSB = mod(double(im(i,j)), 2);
    if (A>m || LSB == I(A))
        s(i,j) = im(i,j);
    else
        if(LSB == 1)
            s(i,j) = im(i,j) - 1;
        else
            s(i,j) = im(i,j) + 1;
        end
```

h) write the Coded video/image into the output folder.

```
imwrite(s, '035.png');
```

8. Write Coded Video in a New file.

a) Construct a VideoWriter object for a new video file.

b) Open the file/Writer.

c) Incrementing loop for all frames.

```
images{count} = imread('frame name');
```

d) Write the frames to the video.

```
for u=1:length(images)
```

e) Convert the image to a frame.

```
frame = im2frame(images{u});
```

f) Get the embedded video

2. *Extraction Algorithm.*

1. User inputs.

a) videofile: this is the file which has coded video.

b) textsize: length of text data to be extracted.

2. Extract all video Frames into a variable.

a) Take the variable K for frame counter.

b) Read the Video file.

c) keep looping for all frames.

d) Compile all frames in the 4th dimension of variable 'v'.

e) The total number of LSBs available in video file is found.

3. Lsb Extraction

a)reqspace = textsize.

b) Use Random=r is for the text bits.

c) Calculate the height and width.

```
height = size(s,1);
width = size(s,2);
```

d) Calculate the each Frame of the video.

e) The original pixel value converted to binary.

f) Extract: Get the LSB value (i.e the hidden text bits).

```
  for i = 1 : height
for j = 1 : width
   if (A <= m)
      b(A) = mod(double(s(i,j)),2);
      A = A + 1;
   end
```

i) Do reverse XOR:

extract the LSBs and the message bits.

j) convert them from binary to decimal.

k) Extract the original video and original message.

B. Working Model

The flowcharts for both the LSB techniques are being represented in the figures below. Figure 1 shows the working model of the sequential algorithm using LSB. Figure 2 shows the working model of the randomized LSB technique using video as cover and text as secret object. The two basic models of cryptography and steganography are defined clearly in the schemes. Both the models use chaotic sequence in the text for encryption before embedding through equation (1) as mentioned in section 1. XORing among the chaotic bits and LSBs is done before insertion/embedding into the LSB place of the frames as per the mentioned table 1 below. In sequential LSB each frame participates in the LSB replacement while in randomized technique, a crypt random generator function selects a random frame for insertion purpose. However, the cryptographic and steganographic approaches remain the same as mentioned above. XORing among the bits is done as follows:

TABLE I. XORING AMONG THE MESSAGE BITS AND LSB BITS

Message bits	**LSB bits**	**New XORed LSB**
0	**0**	0
0	**1**	1
1	**0**	1
1	**1**	0

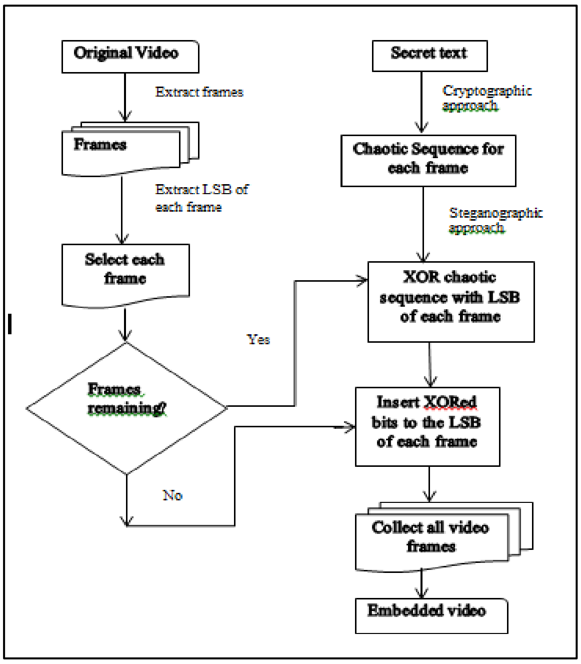


Fig. 1. Flowchart of the Sequential LSB technique.

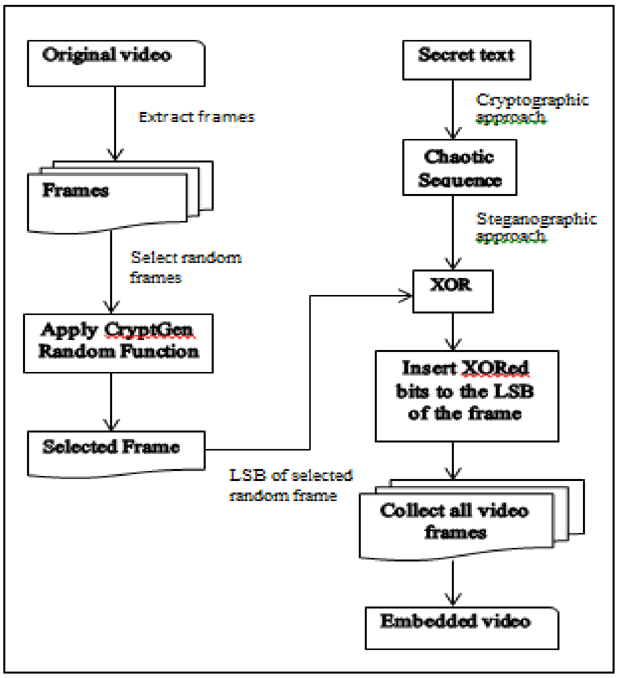


Fig. 2. Flowchart of the Randomised LSB Technique.

IV. RESULTS AND OBSERVATIONS.

The proposed approaches are implemented on MATLAB 2016. The secret message encoded is in the form of text of 350 bits. Four different video are used for the comparison scenario namely nature.avi, shuttle.avi, tower.avi, walk.avi. Each of the four videos have varying sizes as: 28Mb, 7Mb, 12Mb and 60 Mb respectively. The table 2 and 3 represent the Sequential LSB and randomized LSB parameters in which the PSNR values of the random LSB vary greatly as compared to sequential one. Same goes with MSE of random LSB technique, its value is more lesser in the first one than the latter. These variations are symbolizes the effectiveness of random LSB coding as in a good steganographic approach the PSNR values go higher while MSE values go lesser.

The fig 3,4,5 and 6 represent the graphical presentation of the variations in the parameters in of the LSB technique. The tables 4 and 5 represent the comparison among the embedded frames and the original frames along with their histograms in both the approaches scenario.

TABLE II. SEQUENTIAL LSB PARAMETERS

Parameters	Type	nature.avi	shuttle.avi	tower.avi	walk.avi
SNR	Original	19.3901	18.9563	10.4789	15.5013
	Embedded	20.3957	21.9636	11.5257	16.5836
PSNR	Original	20.9306	22.3623	20.6080	22.2204
	Embedded	21.9430	23.3696	20.6413	22.6813
MSE	Original	524.5850	383.7629	561.6528	389.6067
	Embedded	521.3834	381.5445	557.6314	387.5631

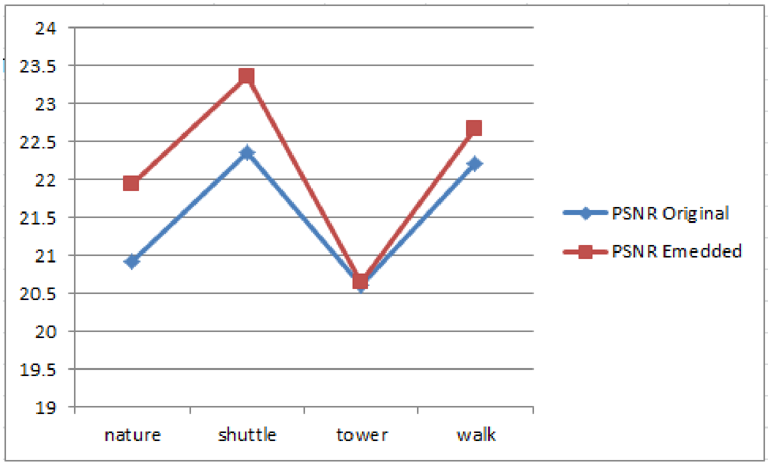


Fig. 3. Representation of PSNR values in Sequential LSB Technique.

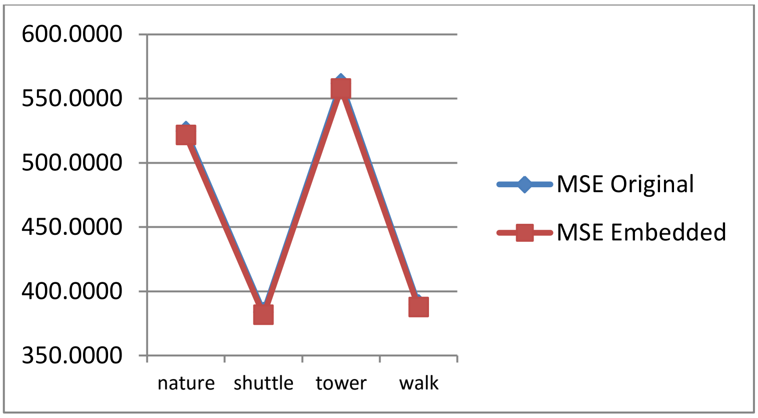


Fig. 4. Representation of MSE values in Sequential LSB Technique

TABLE III. RANDOMISED LSB PARAMETERS

Parameters	Type	nature.avi	shuttle.avi	tower.avi	walk.avi
SNR	Original	20.9707	22.3412	20.5860	22.0057
	Embedded	22.9871	25.3504	26.6816	28.1685
PSNR	Original	19.4321	18.5866	10.4570	15.4386
	Embedded	21.5389	23.9744	15.5657	21.6013
MSE	Original	524.0303	369.3592	556.4750	402.2987
	Embedded	520.5691	363.7040	553.9524	398.4731

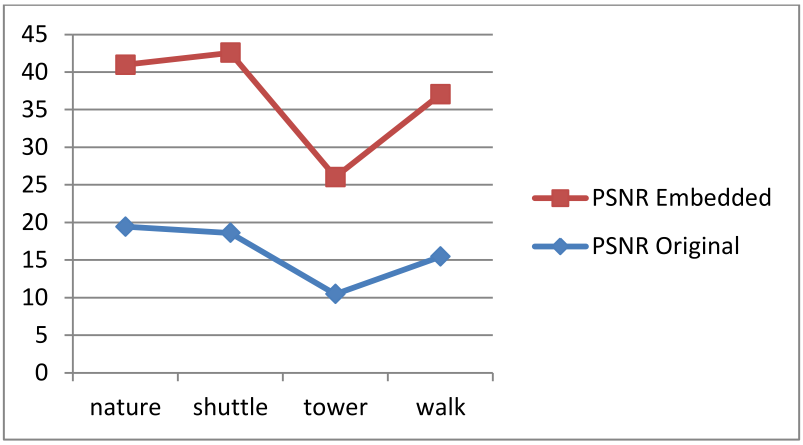


Fig. 5. Representation of PSNR values in Random LSB Technique

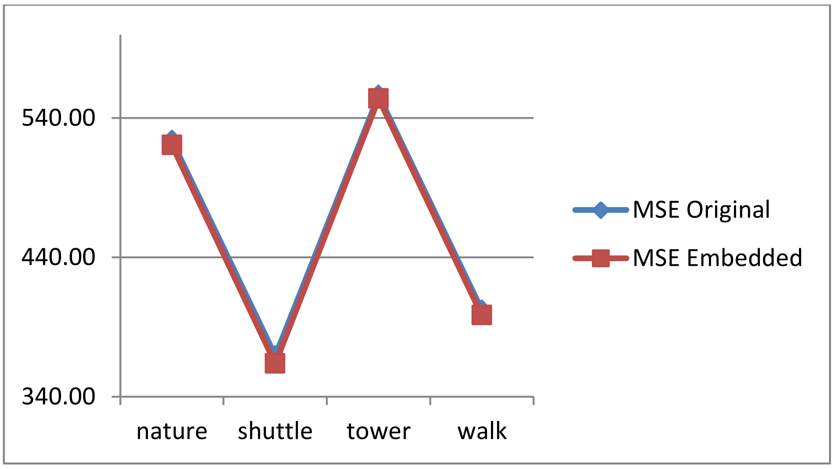
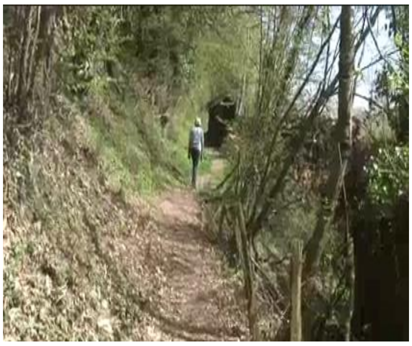
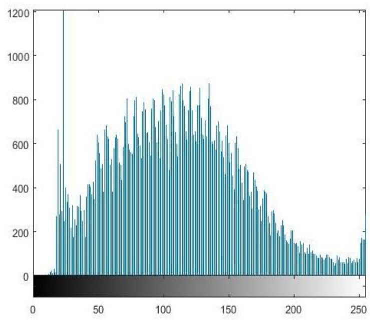
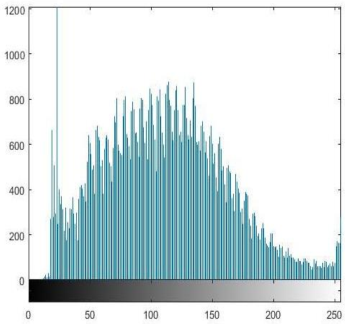
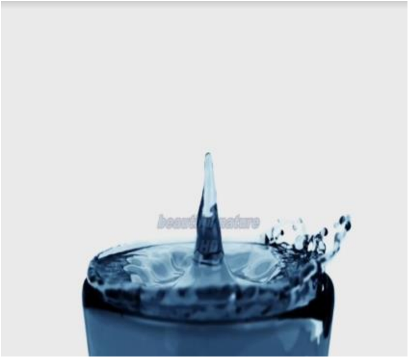
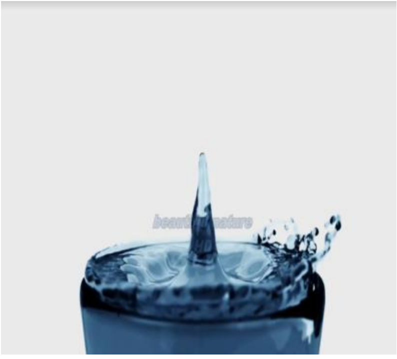
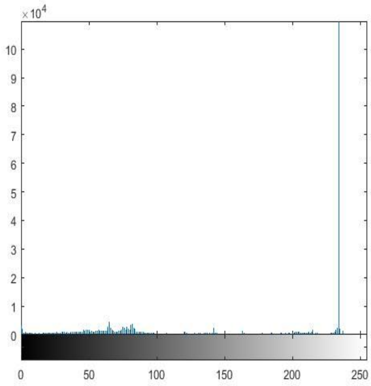
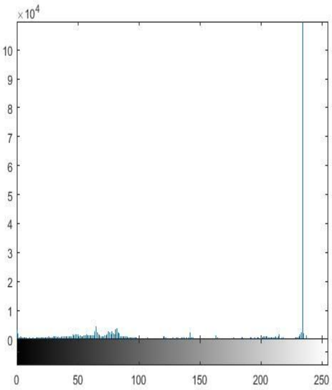


Fig.6. Representation of MSE values in Random LSB Technique.

TABLE 4. COMPARISON AMONG THE ORIGINAL AND EMBEDDED FRAMES OF SEQUENTIAL LSB TECHNIQUE.

Videos	**Original Frames**	**Embedded Frames**
		
	Histogram of original frame	**Histogram of embedded frame**

walk		
	Original Frame	**Embedded Frame**
nature		
	Histogram of original frame	**Histogram of embedded frame**
nature		
	Original frame	**Embedded frame**

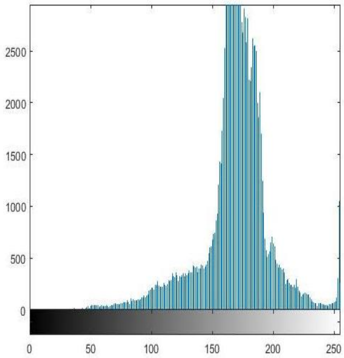
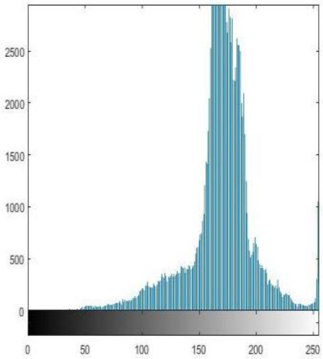
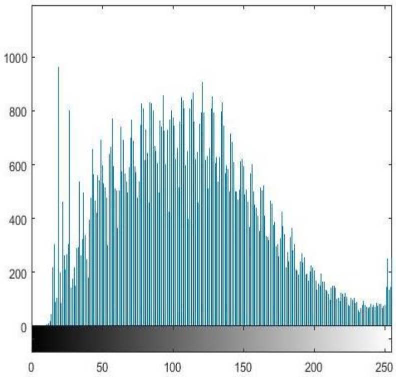
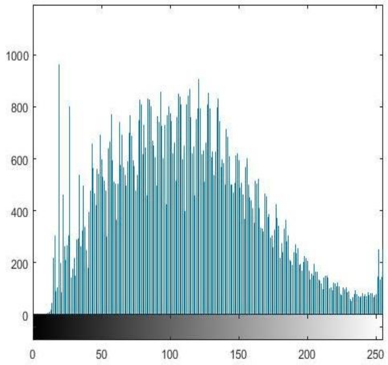
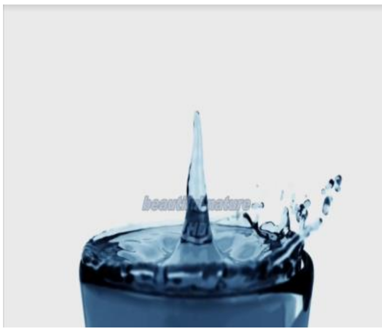
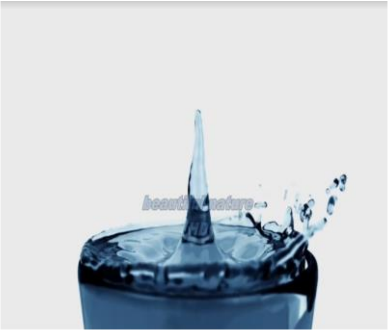
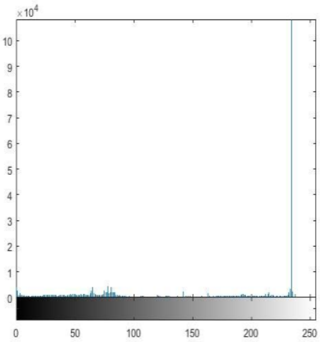
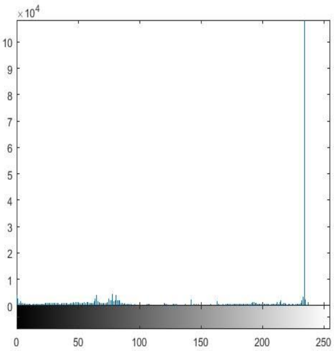
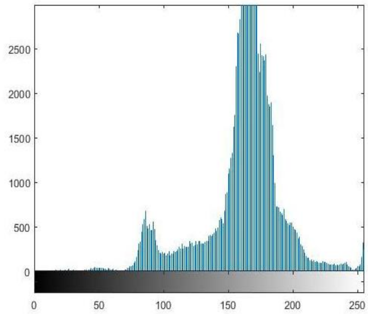
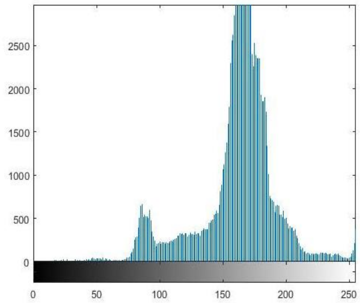
shuttle		
	Histogram of original frame	**Histogram of embedded frame**
shuttle		

TABLE 5. COMPARISON AMONG THE ORIGINAL AND EMBEDDED FRAMES OF RANDOMISED LSB TECHNIQUE.

Videos	**Original Frames**	**Embedded Frames**
walk		
	Histogram of original frame	**Histogram of embedded frame**

walk		
	Original frame	**Embedded frame**
nature		
	Histogram of original frame	**Histogram of embedded frame**
nature		
	Original frame	**Embedded frame**

shuttle		
	Histogram of original frame	**Histogram of embedded frame**
shuttle		

V. CONCLUSION

The comparison of the above two steganographic techniques show that the randomized LSB is better than the sequential LSB technique. The PSNR values in the randomized LSB approach are comparatively higher than the traditional approach. Similarly, the MSE values are going less in more values in random LSB than the sequential (as shown in tables 2 and 3). The Steganalysis of both approaches show Random technique as more imperceptible strong and secure. The time elaspsed in embedding and extraction are also small in the randomized LSB. The video retain more originality in the same approach.

REFERENCES

1. 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, Sep 2012.
2. Mritha Ramalingam,"StegoMachine-Video Steganography using Modified LSB Algorithm", World Academy of Science, Engineering aand Technology 50, 2011.
3. Manpreet Kaur, Er. Amandeep Kaur," Improved Security Mechanism of Text in Video by using Steganographic Technique: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, vol.4 issue 5, May 2015.
4. Siddartha Gosalia et.al. ,"Embedding audio inside a digital video using LSB Steganography", 2016 International Conference on Computing for Sustainable Global Development (INDIAcom), 2016 IEEE.
5. Pritish Bhautnage, Prof. Amutha Jeyakumar, Ashish Dahatonde, " Advanced Video Steganography Algorithm" International Journal of Engineering Research and Applications (IJERA), Jan-Feb, 2013.
6. R.Balaji, G. Naveen," Secure Data Transmission using Video Steganography", 2011 IEEE International Conference on Electro/Information Technology".
7. Ashish T. Bole, Rachna Patel, "Steganography over Video File using Random Byte Hiding and LSB Technique", International Conference on Computational Intelligence and Computing Research, IEEE, 2012.
8. Pooja Yadav, Nishchol Mishra, Sanjeev Sharma," A Secure Video Steganography with Encryption Based on LSB Technique", International Conference on Computational Intelligence and Computing Research", 2013, IEEE.
9. Mohamed Elsadig et.al. ,"High Rate Video Streaming Steganography", Proceedings of 2009 IEEE International Conference on Future Computer and Communications, 2009.
10. Rahul Paul et.al. ,"Hiding Large Amount of Data Using a New Approach of Video Steganography", Confluence 2013:

The Next Generation Information Technology Summit (4th International Conference),2013.

11. Sunil K. Moon, Rajshree D. Raut, "Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhanced Data Security", Proceedings of 2013 IEEE 2nd International Conference on Image Information Processing (ICIIP-2013).
12. Namrata Singh, Virendra Kumar Yadav, " Trends in Digital Steganography: A Survey", International Journal of Computer Applications, July 2017.
13. Bin Liu, Fenlin Liu, Chunfang Yang, Yijeng Sun, "Secure Steganography in Compressed Video Bitstreams", 3rd International Conference on Availability, Reliability and Security, 2008 IEEE.
14. Richa Khare, Rachna Mishra, Indrabhan Arya, " Video Steganography by LSB Technique using Neural Network", 6th International Conference on Computational Intelligence and Communication Networks",2014 IEEE.
15. Deshpande Neeta, Kamalapur Snehal, Daisy Jacobs," Implementation of LSB Steganography and its Evaluation for Various Bits", 1st International Conference on Digital Information Management, 2006 IEEE.
16. H. Ogras, M. Turk," Digital Image Encryption Scheme using Chaotic Sequences with a Nonlinear Function", World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:6, No:7, 2012.
17. M.C. Trivedi et.al. ," Metamorphic Cryptography using Strength of Chaotic Sequence and XORing Method", Journal of Intelligent and Fuzzy Systems 32 (2017) pp-3365-3375.