

# Video Steganography Schemes for Hiding Acoustic Data: A Comparison

Namrata Singh  
AKTU Lucknow

Renu Prasad  
AKTU Lucknow

## ABSTRACT

Steganography allows data secrecy of any form inside any cover type without getting identified by any third person. Not only hiding the data could secure the secret instead applying any security/encryption technique would ensure its full secrecy and security. This paper presents two audio data hiding scheme inside a cover video by using LSB replacement technique for steganography. The acoustic data is encrypted by using XOR method before embedding it inside LSBs of original video. The secret audio data bits are inculcated inside a random frame and also in all sequential frames of cover video. Comparison among the two embedding schemes is done in this paper. Comparative analysis among the approaches is done on the parametric grounds of steganography. The results show that the randomized embedding technique is better than the sequential embedding technique on the security grounds and require less time for embedding and extraction.

## Keywords

Least Significant Bit (LSB), XOR, PSNR, MSE

## 1. INTRODUCTION

The concept of steganography with cryptography is quite a strong and security preserving methodology. The steganography provides the secrecy of the data by inculcating the secret bits inside the cover without being identified by the third party. Cryptography provides the security enhancing scheme by encrypting the secret data into some unintelligent form. The paper focuses on the metamorphic cryptography which is exactly the fusion of two wide fields of steganography and cryptography i.e. hiding encrypted secret data bits inside some cover type. This metamorphic combination of both the concepts provides a wide scope for data security in the communications.

The steganographic approach used here is LSB (Least Significant Bit) Replacement. The traditional LSB concept is quite simple and effective in terms of steganographic quality parameters like imperceptibility, less distortion and hiding large number of bits. In this LSB Replacement approach the original LSB bits are being replaced by the secret data bits. This paper defines an improvised LSB by incorporating the LSB replacement of the original cover bits by the resultant XORed bits. XOR is an encryption technique which is hereby performed among the original LSB bits of cover and the secret data bits. Here, secret audio bits are hidden inside a cover video in two different ways namely randomized and sequential. So, XORing is performed among the encrypted secret audio data bits and the LSBs of the selected frame (random or sequential). This XOR approach efficiency lies in minimizing the distortion effect after insertion of secret bits. In case of sequential embedding the secret audio bits are hidden inside each sequential frame while in randomized approach, random frame for embedding is selected by using CryptGenRandom function. This function ensures security against intruder attacks.

The paper is organized as follows: Section 1 contains introduction to the basic concepts and provides brief insight to the work. Section 2 defines literature survey while section 3 presents working approaches. Section 4 show results and observations with section 5 concluding the paper.

## 2. LITERATURE SURVEY

Siddhartha et.al.[1] proposed a high PSNR and low MSE valued audio hiding approach in carrier video in paper[1]. The work results show that the implemented technique is secure and robust. Also the resultant embedded video with secret audio are highly imperceptible. A new network steganography approach by using PRNGs is being proposed by Amritha et.al. in paper [2]. These Pseudorandom number generators decrease the chances of information leakage and attacks.. Randomization of key generation process is done along with fake key concept. In order to mislead intruder fake keys are introduced. The secret message is encrypted and hidden in cover video by using encryption and compression. Embedding is done into the packet headers. The proposed technique resulted into high quality of embedded cover video.

Pratiksha Sethi and V. Kapoor, proposed an image steganography approach in paper [3] by using genetic algorithm and cryptography. The secret encrypted data is hidden in an image only after compressing and encrypting it by AES. Genetic algorithm usage prevents the discovery of secret data inside the cover image. Genetic algorithm makes the system quite tough to break by using the strength of heuristics. The resultant image shows high imperceptibility with higher PSNR values. A 3-3-2 LSB based steganography technique implemented by Koushik et.al. in [4]. Video is used as carrier file and genetic algorithm is applied in order to get high imperceptibility of secret data. Steganalysis is also performed for comparing the original and embedded frames and the scheme proves out to be effective through high PSNR and Image fidelity (IF) rates. Splitter, embedder, optimizer and decoder were the main components used for information hiding. Lakshmi et.al. [5] performed data hiding technique by contrast enhancement of poor quality videos. This improves the visual quality of video after embedding. The quality of illumination along with the size of video is preserved even after enhancement. V. Satya et.al. in paper [6] shows various methods of audio, video, image steganography where text is hidden inside the carrier files. The methods of parity coding, phase coding, spread spectrum, echo hiding are defined for hiding text in audio. An image steganography model called T-coding is proposed for hiding audio in image. This provides robustness through self-synchronization without changing the file size. Encryption of audio bits is done before embedding. A key based cryptography is shown better results than the non key based cryptography. The papers [7] [8] define scene change detection based data hiding techniques. In [7] DCT is used for finding the changing video sequences. DWT and DCT are used for getting enhanced and secured quality of video steganography. DWT is used for normalizing the cover object with the hidden payload. An effective high resolution

AVI video steganography is proposed by Arup et.al. [9]. The process of hiding and extraction of data is securely done by encryption. The blind scheme is used which results in high quality, security, robustness and embedding capacity. Paper [10] defines some principles of data hiding in audio. Audio hiding methods likely echo hiding, parity coding, phase coding etc. are reviewed. A method of hiding data in LSBs of audio stream is also proposed. For security and robustness encryption and decryption techniques are also applied. The resultant audio file shows no change in size even after embedding.

### 3. PROPOSED METHODS

The acoustic data bits are being hidden inside the cover video in two different ways. The embedding schemes as defined in section 1 above are namely: sequential and randomized. The first approach hides audio data in each frame while latter one hides the audio in a randomly selected frame. LSB steganographic approach is used as an improved form in collaboration with the encryption techniques. The secret audio data is firstly encrypted before performing the XOR operation with the original LSBs. The extraction and embedding of defined schemes are explained in the sections below. Both approaches hide the same audio sequence (as shown in the fig. 1) no matter either in all sequential frames or in the randomly selected frames of the cover video.

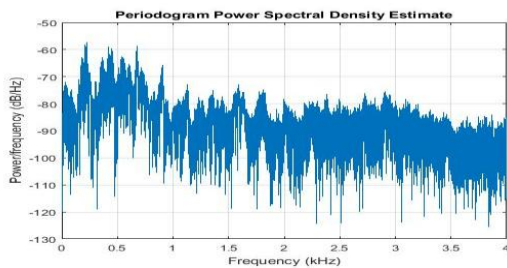


Fig. 1 Frequency diagram of the secret audio used for hiding purpose.

#### A. Sequential Audio Data Hiding Scheme

This approach embeds the encrypted bits of audio inside the LSBs of each frame of cover video by following proper secret data chunking. The algorithms for the embedding and extraction processes are mentioned below.

##### 1 Embedding Algorithm:

- Select a cover video and secret audio file.
- Extract all the video frames.
- Extract LSBs of the each frame. Check for the space requirement –if (Total LSBs available > audio bits).
- If no then throw error else encrypt the secret bits.
- Now, XOR among the LSBs and the encrypted bits.
- Replace the original bits of original cover frame with the XORed bits resultant.
- Repeat this process for all the frames and generate the embedded frames.
- Recollect all embedded frames to get the embedded video.

##### 2. Extraction Algorithm:

- Obtain the embedded video.

- Extract the embedded frames.
- Extract the LSBs of the each embedded frames
- Perform the reverse XOR function to receive the original LSBs and the encrypted bits.
- Perform decryption and obtain the audio message bits.
- Convert the binary audio bits to the audio file format and the similarly for the frames.
- Obtain the original video and secret audio file.

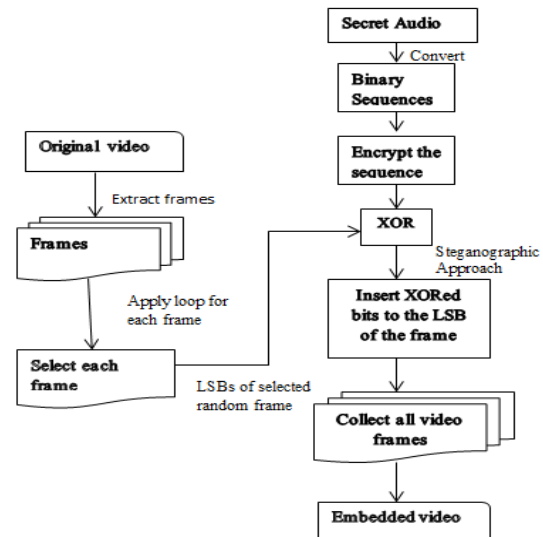


Fig.2 Embedding procedure for sequential algorithm.

#### B. Random Frame Audio Data Hiding Scheme

This approach embeds the encrypted bits of audio inside the LSBs of randomly selected frame of cover video as mentioned in section 1. The algorithms for the embedding and extraction processes are mentioned below.

##### 1. Embedding Algorithm:

- Select a cover video and secret audio file.
- Extract all the video frames.
- Apply CryptGenRandom function to get randomly selected frames.
- Extract LSBs of the each random frame. Check for the space requirement –if (Total LSBs available > audio bits).
- If no then throw error else encrypt the secret bits.
- Now, XOR among the LSBs and the encrypted bits.
- Replace the original bits with the XORed bits resultant.
- Repeat this process for all random frames and generate the embedded frames.
- Collect all frames to get the embedded video.

##### 2. Extraction Algorithm:

- Obtain the embedded video.
- Select the random embedded frames.
- Extract the LSBs of the randomly embedded frames.
- Perform the reverse XOR function to receive the original LSBs and the encrypted bits.
- Perform decryption and obtain the audio message bits.
- Convert the binary audio bits to the audio file format and the similarly for the frames.
- Obtain the original video and secret audio file

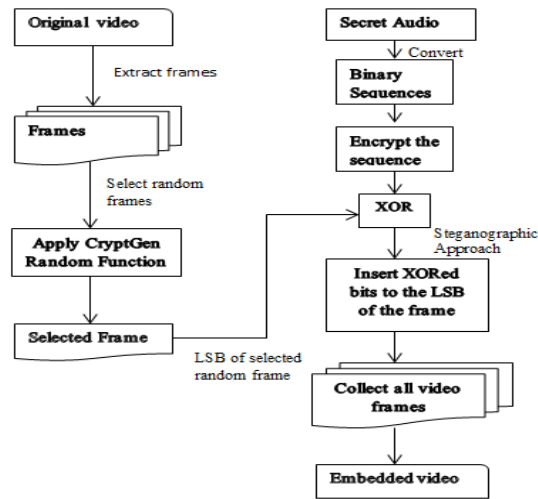


Fig.3 Embedding procedure for random algorithm



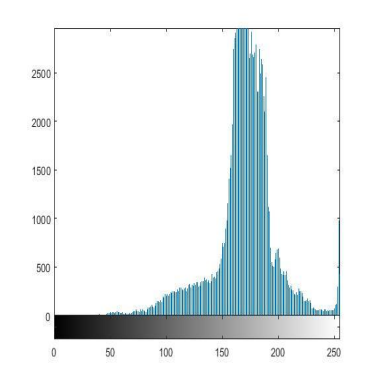
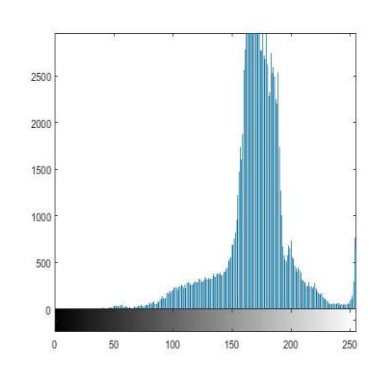
#### 4. RESULTS & OBSERVATIONS

Table 1 Comparing both Sequential and Randomized approaches on parameters basis



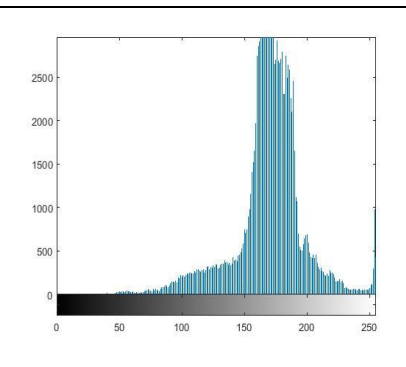
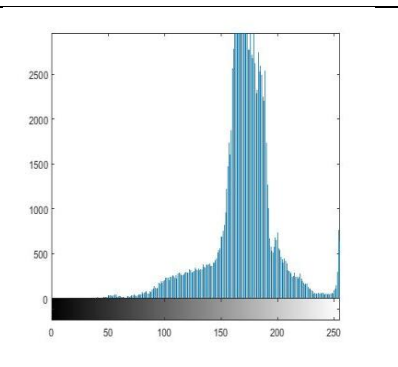


Sequential (On Frames)		PSNR	MSE	SNR	Randomized (On Frames)		PSNR	MSE	SNR
Video 1	Original	23.7710	402.2266	15.3361	Video 1	Original	22.0077	401.1627	15.4407
	Embedded	23.8422	402.0003	15.5948		Embedded	22.1520	392.4034	15.5826
Video 2	Original	22.3929	381.7009	18.1603	Video 2	Original	22.3205	382.7564	18.9445
	Embedded	22.7561	380.1182	18.6048		Embedded	22.3974	380.0496	19.0364
Video 3	Original	20.3853	525.5831	19.8060	Video 3	Original	20.9239	525.2850	19.3852
	Embedded	20.7556	525.3600	19.8894		Embedded	20.9451	522.1039	19.4070

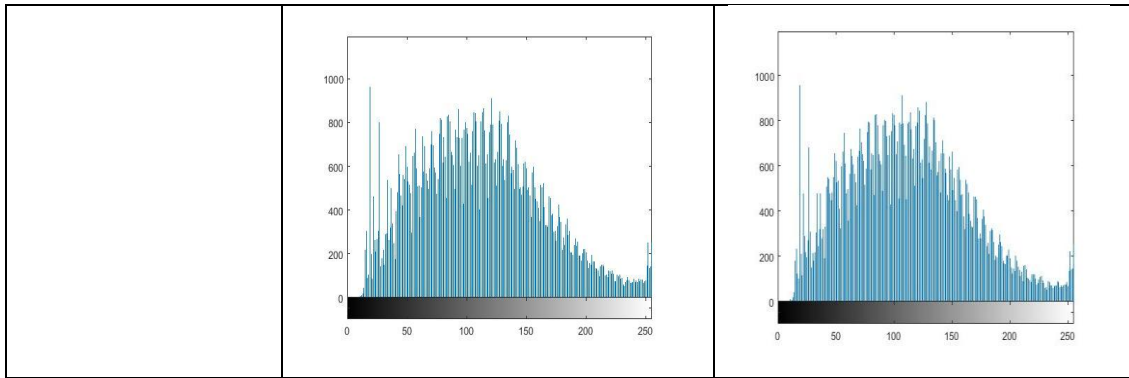
Table 2 Sequential approach results on the basis of frames and histograms.

Sequential Approach	Original Frame	Embedded Frame
Video 1 Frames & Histograms		

<b>Video 2 Frames &amp; Histograms</b>		
		

**Table 3 Randomized approach results on the basis of frames and histograms.**

Random Approach	Original Frame	Embedded frame
<b>Video 1 Frames &amp; Histograms</b>		
		
<b>Video 2 Frames &amp; Histograms</b>		



The implementation of both the schemes is done on the MATLAB 2016 tool. The observations of the implemented approaches are summarized in the tables shown below. The parametric analysis of the approaches is shown in the table 1 where the PSNR, MSE and SNR values are evaluated for both original and embedded frames. The PSNR and SNR values of the embedded frames are going high while the MSE values for the embedded frames are going down. This inverse trend of both approaches shows the strength of the steganography practice being done. The comparative analysis on the basis of visual detection is done in table 2 and 3 where both sequential and randomized frames are compared respectively. Also, the histograms are presented in the same table inferring that there is no difference or distortion among frames even after secret bits insertion. The real comparison among the two approaches is on the basis of total time elapsed. The sequential approach when applied on video 1 takes 18.0733 sec and 20.5822 sec for embedding and extraction respectively. While the randomized approach uses quite a lesser time with 5 sec (approx.) and 3 sec (approx.) for embedding and extraction respectively when applied on same video 1. Importantly from the security purpose the randomized approach offers best advantage but in terms of distortions sequential seems better as the insertions are being done in each frame hence minimizing it.

## 5. CONCLUSION

The paper shows two implementation schemes of hiding secret audio data inside a cover video. Comparison among the sequential and randomized approaches is done on the parametric grounds of steganographic measures namely PSNR, SNR, MSE etc. Pictorial differences among the performance of the two approaches are shown on the basis of frames and histograms. The results and observations conclude about the pros and cons of both the techniques. The both have higher PSNR and lower MSE values for the embedded frames. The embedding and extraction time in randomized technique is lower than the sequential technique. But, the imperceptibility quotient is quite high in the sequential approach.

## 6. REFERENCES

- [1] 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.
- [2] Amritha Shekhar, Manoj Kumar G., M Abdul Rahiman, "Novel Approach for Hiding Data in Videos Using Network Steganography Methods", 4<sup>th</sup> International Conference on Eco-friendly Computing and Communication Systems, 2015 Elsevier.
- [3] Pratiksha Sethi, V. Kapoor, "A Proposed Approach Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography", 2016 International Conference on Computational Science, Elsevier.
- [4] Koushik Dasgupta, Jyotsana Kumar Mondal, Paramartha Dutta, "Optimized Video Steganography Using Genetic Algorithm", International Conference on Computational Intelligence Modelling, Techniques and Applications (CIMTA) 2013, Elsevier.
- [5] Lakshmi M et.al., "Reversible Data Hiding in Video for Better Visibility and Minimal Transfer", Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology (RAEREST), 2016 Elsevier.
- [6] V. Sathya et.al., "Data Hiding in Audio Signal, Video Signal, text and Jpeg Images", IEEE International Conference on Advances in Engineering Science and Management (ICAESM 2012).
- [7] Mriitha Ramalingam, Nor Ashidi Mat Isa, "A Data Hiding Technique Using Scene Change Detection for Video Steganography" Computer and Electrical Engineering 54 Journal, 2016 Elsevier.
- [8] Rahul Paul et.al. "High Rate Video Streaming Steganography" Proceedings of 2009 IEEE International Conference on Future Computer and Communications.
- [9] Arup Kumar Bhaumik et.al., "Data Hiding in Video", International Journal of Database Theory and Applications, June 2009.
- [10] Poulami Dutta, Debnath Bhattacharya, Tai-hoon Kim, "Data Hiding in Audio Signal: A Review" International Journal of Database Theory and Application, Vol.2 No.2, June 2009.