XOR Encryption Based Video Steganography

Ramandeep Kaur[1], Pooja[2]

[1]Research Scholar, CSE, CT Group of Institutions, Shahpur, Jalandhar, Punjab, India

[2]Assistant Professor, CSE, CT Group of Institutions, Shahpur, Jalandhar, Punjab, India

Abstract: ***In this paper, an XOR encryption based video steganography scheme is put forward which encrypts the text secret message (.txt) and hide it using 1LSB substitution method behind the random frames of video file (.avi). The main motive of this methodology is to protect the confidential information from the attackers by hiding its presence from the human visual system (HVS) and secure the text data from cyber criminals. There are several algorithms are proposed in previous works which are not enough capable to secure the hidden data and are not much efficient for embedding high amount data behind career medium. So this work is used for embedding high payload and to provide security to text data. The result values are simulated on the basis of quality metrics such as PSNR, MSE, BER and histogram analysis.***

Keywords: Least Significant Bits (LSB), Encryption, Payload Capacity, Human Visual System (HVS), Embedding, Secret Message, Random and dynamic frame selection, Secret Key.

1. Introduction

Nowadays in a digitized world, security of private information is a major issue over the internet. To protect the private information from being misused by the cyber criminals, various data hiding approaches are used. Steganography is one of them which is an information hiding technique and hides the presence of secret message behind a multimedia file without changing the perceptual quality of media file and provide secure communication between two parties. It is originated from Greek words i.e. Steganós (means Covert/Secret), and Graptos (means Writing) which means conceal the secret message inside the cover. It is a one- to one communication process. Steganography is used for various purposes like for copyright protection in digital marking, feature tagging, and biometrics, in computer forensics as an authentication tool and in military or medical field. From the ancient time, various methods were used to hide information such as invisible inks, microdots, wax, tattoos on the slave's head etc. but nowadays digital media is used to embed the confidential information. On the basis of Digital media steganography is categorized as; text, image, audio, video and protocol based steganography. Here we are dealing with video steganography. [1]

1.1 Video Steganography

Video steganography has become very popular research area to hide secret data. It is a non- tangible masking of confidential information behind the video file. Video is a combination of audio and multiple image frames so can be used to embed large amount of data. The maximum frames required for creating a video file is 16 fps (frame per second). The main goal of video steganography is to embed the secret data behind video in such a manner that it should not be perceptible to HVS and no degradation in the quality of video. A good video steganography must have three parameters i.e. Security, Capacity and imperceptibility. Video steganography works in two phases i.e. embedding process and extraction process. [2]

1.1.1Embedding Process (Sender Side)

This process is carried out at sender side in which, a secret message is embedded inside the cover video using embedding algorithm and generate a stego video.

1.1.2 Extraction Process (Receiver Side)

Extraction process is a reverse process of embedding algorithms in which a secret message is extracted from stego video using stego key at receiver side. Many algorithms are proposed for video steganography on the basis of Spatial Domain and Transform Domain. The most basic algorithm is Least Significant Bits (LSB), which replace the secret bits directly inside the East significant bits of video. Videos are more secure than images as human eye can't predict small color variations in whole video stream.

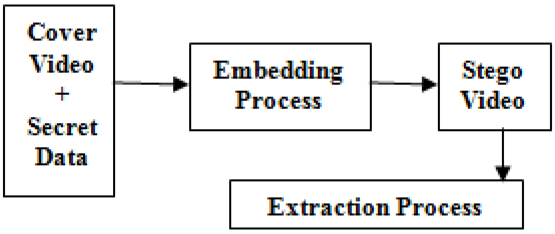

Figure 1: Process of Video steganography

1.2 Video Steganalysis

Detection of the presence of secret message behind video is done using steganalysis. It is basically used for computer forensics to detect cyber criminals.

2. Related Work

The issue regarding security and data protection has become major problem which has to be reduced in order to protect the confidential information from the hackers or cyber criminals. Many methodologies and algorithms have been proposed for minimizing the bad impact of cyber attacks on secret data.

In the year 2014, Hemant Gupta, Setu Chaturvedi [1] has proposed a basic technique for image steganography. An advance approach is applied for hiding data i.e. single bit, 2 bit, 3 bit LSB with AES encryption method to stop hacking. Then calculate PSNR & Correlation Factors. It concludes that the PSNR decreases as number of LSB substitution bit increased. This makes steganography to hide large amount of data but easy to attack and less secure.

Sunil. K. Moon, Rajeshree. D. Raut [2] has proposed a method to hide secret message behind a video file using 4 LSB technique and used computer forensics as an authentication tool and achieve high capacity of data.

Geetha C.R., H. D. Giriprakash [3] has proposed an image Steganographic method by using multiple edge detection operator (Canny Edge detector) and Variable embedding method. The multiple edge detection is limited to three times so as to reduce the distortion from image. 4 bits are embedded in edge pixels and 2 bits in other pixels using LSB substitution process. High data capacity and good quality is achieved by calculating the PSNR values of original image and stego image.

Shivani Khosla, Paramjeet Kaur [6] proposing a hybrid approach of video steganography with watermarking is used to embed the secret message in carrier video. DCT & DWT techniques are used to hide message inside video and generates a stego video. This stego video is again used to embed a watermark using LSB technique to increase the security of stego video.

Youssef Bassil,[9] proposed an Image Steganography method in which Parameterized based Canny Edge Detection Algorithm is used. Secret message is embedded into a digital image within the edge pixels that are detected in image using canny edge detection algorithm and 3LSB substitution. This algorithm used basically three parameters: size of Gaussian filter, low threshold and high threshold values. But has limitation of complex processing as it generates three different outputs corresponding to three parameters.

3. XOR Encryption

XOR Encryption is a symmetric key based encryption technique which helps to encrypt the secret data into another unreadable format to protect it from intruders and from unauthorized users [5]. It provides one- tier protection to private information. Some logical and Boolean operations are formed on secret data for converting it into another form. In this work we are using following function to encrypt the data using XOR Boolean expression. These expressions are more secure than standard operations such as addition, subtraction.

Encypted_Msg = XOR (Secret_Data_Bits, Key) (1)

4. Proposed Methodology

In this work, a text secret message (.txt) is used to hide behind video clip (rhinos.avi). The secret message bits are hidden in places of least significant bits (LSB) by following the pattern BGRRGBGR. Each pixel hides 1 bit of secret message at a time in sequential manner behind the selected random video frames. 10 random frames are selected on the basis of 10 digit secret key. The secret message is encrypted using XOR encryption to make it secure from cyber criminals. The bit level embedding is done in this algorithm. The algorithm shows high imperceptibility, better quality and high embedding capacity of secret data behind video frames [5].

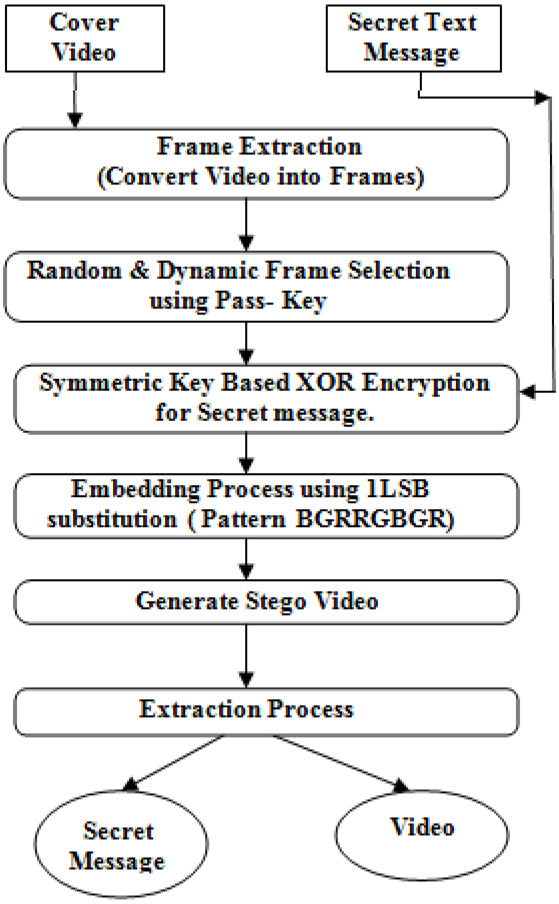
Cover Video
Secret Text Message
Frame Extraction (Convert Video into Frames)
Random & Dynamic Frame Selection using Pass- Key
Symmetric Key Based XOR Encryption for Secret message.
Embedding Process using 1LSB substitution (Pattern BGRRGBGR)
Generate Stego Video
Extraction Process
Secret Message
Video

Figure 2: Flow Chart of Proposed Algorithm

4.1 Embedding Algorithm

The following steps are followed for hiding the text message behind video.

a) Select cover video (.avi) and enter secret message (.txt).
b) Enter10 digit Secret_Key for authorization proposes.
c) Convert video into frames and extract 10 random frames from extracted frames on the basis of secret key (i.e. 1234567890) such as [8]:
frame$_{1=}$ Secret_Key(1) + Secret_Key(2) (2)
frame$_2$= Secret_Key(4) + Secret_Key(10) (3)
…..
frame$_{10=}$ Secret_Key(8) + Secret_Key(2) (4)
Where, frame$_1$ $_{to}$ frame$_{10}$ are ten random functions for extracting 10 random frames for hiding the secret message.
d) Encrypt secret message using XOR encryption formula where EM is encrypted message.
EM = bitxor (Secret_msg_bit, Secret_Key) (5)
e) Hide secret key, selected frame addresses and message length in the first frame of video clip.

f) Embed encrypted secret bits behind selected frames using 1LSB substitution and by following the BGRRGBGR pattern where R, G, B represents the Red, Green & Blue channel respectively in sequentially manner [5]. Generate Stego.avi video file which contains secret message.
g) Compute PSNR, BER, MSE and Histogram for all selected Frames.

4.2 Extraction Algorithm

The extraction process is carried out at receiver side to extract secret message. The following steps are followed for performing extraction process [5].

a) Select Stego video and convert it into frames.
b) Extract secret key, selected frame addresses and message length from the first frame of video.
c) Enter secret key and compare it with originally stored key. If user is unauthorized then video clip will get corrupted after 4 attempts and damaged by leaving no secret data behind it.
d) Now, extract secret message by performing reverse process of embedding algorithm using 1LSB substitution mechanism.
e) Decrypt the extracted message.
f) Display final secret message as output.
g) Exit.

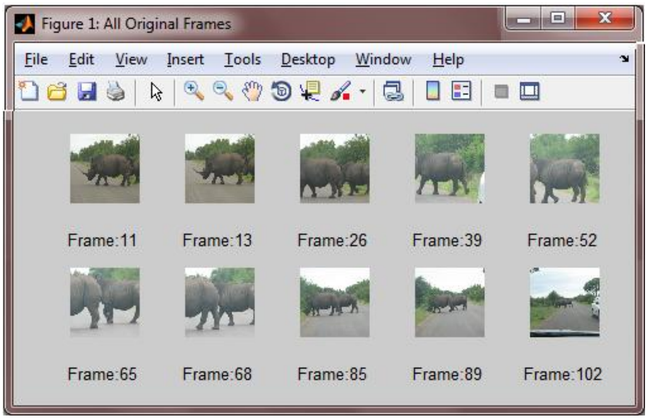

Figure 3: Selected 10 Random Frames

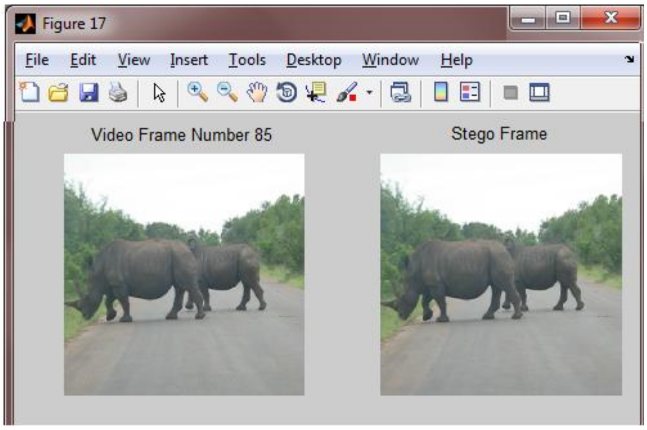

Figure 4: Selected Frame and Corresponding Stego Frames

5. Experimental Results

The proposed work is simulated on Matlab 7.10.0 (R2010a) for hiding 2048 bytes data and the experimental results are simulated on the basis of Quality metrics such as PSNR (Peak Signal to Ratio), MSE (Mean Error Square) and BER (Bit Error Rate). It shows that this algorithm achieving high PSNR and low MSE value and have high embedding capacity with high security which are showed in figure 5,6, & 7 and high imperceptibility as histogram of stego and original is visibly same as shown in figure 8. All the Values of PSNR, BER and MSE for all selected values are tabulated in table1.

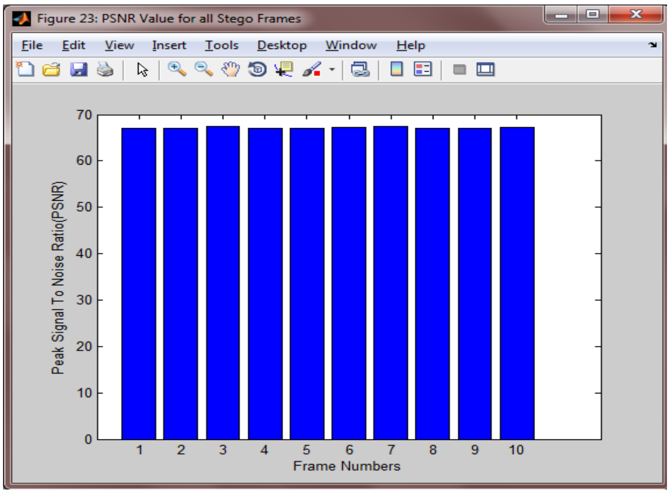

Figure 5: PSNR value of all selected frames (for hiding 2048 bytes data)

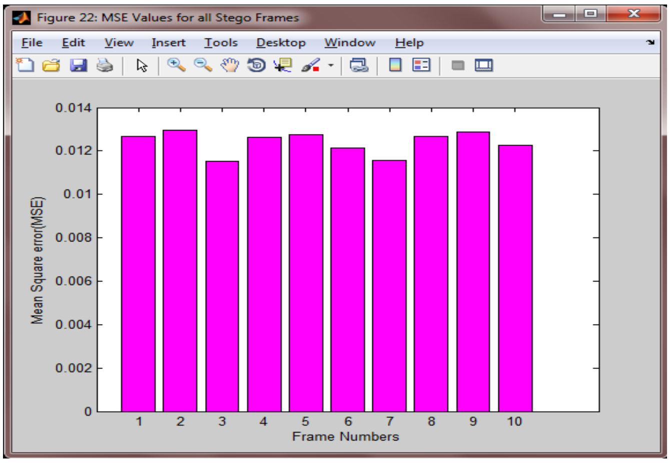

Figure 6: MSE value of all selected frames

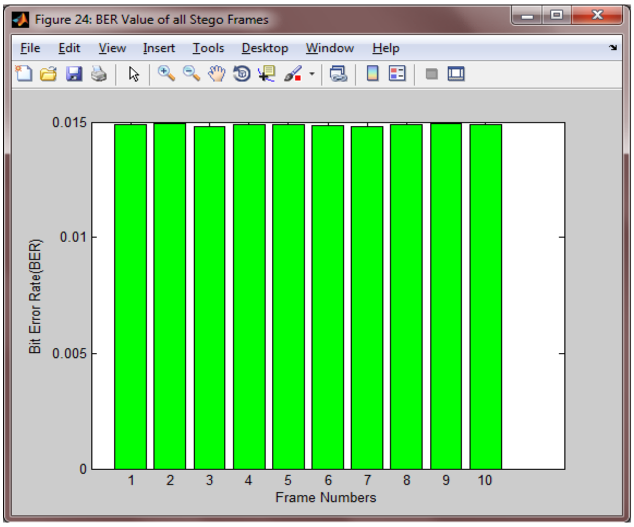

Figure 7: BER value of all selected frames

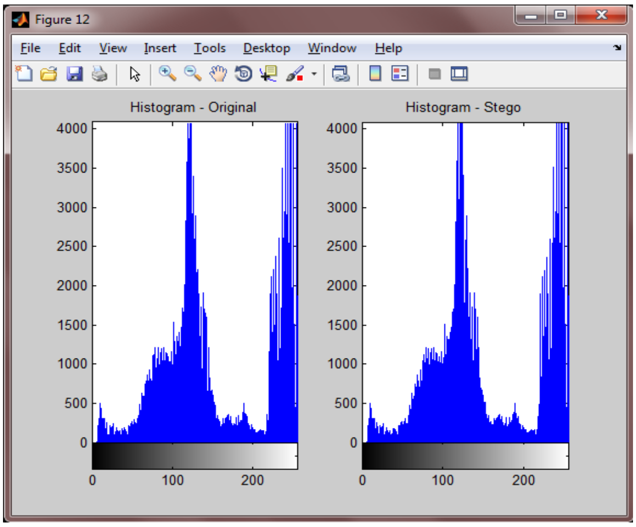

Figure 8: Histogram Analysis

Table 1: PSNR, MSE, BER Values for all Selected Frames for hiding 2048 bytes data

Frame Numbers	PSNR (db)	BER	MSE
1	67.10	0.0149	0.0127
2	67.00	0.0149	0.0130
3	67.52	0.0148	0.0115
4	67.12	0.0149	0.0126
5	67.06	0.0149	0.0128
6	67.28	0.0149	0.0121
7	67.49	0.0148	0.0116
8	67.10	0.0149	0.0127
9	67.03	0.0149	0.0129
10	67.24	0.0149	0.0123
Average Values	67.19	0.0149	0.0124

6. Conclusion & Future Scope

Video steganography is a very active research field with lots of applications. In this paper, a basic implementation of video steganography process is done using 1LSB based substitution and encrypted text message is hide inside random frames of video by following a pattern i.e. BBRGGB in sequential manner. This algorithm provides high embedding capacity of secret data i.e. 32KB and provides high imperceptibility performance and high speed of processing. In future work, we can embed secret data using edge based video steganography and also can use different format of video and media for steganography process.

References

[1] Hemant Gupta, Setu Chaturvedi, "Video Steganography Through LSB Based Hybrid Approach", International Journal of Computer Science and Network Security, Vol.14, No.3, pp 99-106, March 2014.

[2] Sunil. K. Moon, Rajeshree. D. Raut, "Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data Security", IEEE Second International Conference on image information processing (ICIIP- 2013), pp 660-665.

[3] Geetha C.R., H. D. Giriprakash," Image Steganography by Variable Embedding and Multiple Edge Detection using Canny Operator", International Journal of Computer Applications (0975 – 888) ,Volume 48, No.16, June 2012.

[4] Vandana Thakur, Monjul Saikia, "Hiding Secret Image in Video", 2013 IEEE International Conference on Intelligent Systems and Signal Processing (ISSP).

[5] Pooja Yadav, Nishchol Mishra, Sanjeev Sharma," A Secure Video Steganography with Encryption Based on LSB Technique", IEEE International Conference on Computational Intelligence and Computing Research, 2013.

[6] Shivani Khosla, Paramjeet Kaur, "Secure Data Hiding Technique Using Video Steganography and Watermarking", International Journal of Computer Applications (0975 – 8887), Vol. 95, No.20, June 2014.

[7] Ashish T. Bhole, Rachna Patel, "Steganography over Video File using Random Byte Hiding and LSB Technique", IEEE International Conference on Computational Intelligence and Computing Research 2012.

[8] Amrinder Singh, Sukhjit Singh, "A Robust Video Watermark Embedding and Extraction Technique Based on Random Frame Selection", IJRIT International Journal of Research in Information Technology, Vol. 2, Issue 2, February 2014, pp: 28-37.

[9] Youssef Bassil, "Image Steganography based on a Parameterized Canny Edge Detection Algorithm", International Journal of Computer Applications, Vol. 60, Issue no.4, December 2012.

[10] Babloo Saha and Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images", Defense Science Journal, Vol. 62, No. 1, January 2012, pp. 11-18.

[11] K.V.Vinodkumar, V. Lokeswara Reddy, "A Novel Data Embedding Technique for Hiding Text in Video File using Steganography", International Journal of Computer Applications (0975 – 8887), Vol. 77, No.17, September 2013.

[12] Soumyajit Sarkar, Arijit Basu, "Comparison of various Edge Detection Techniques for maximum data hiding using LSB Algorithm", International Journal of Computer Science and Information Technologies, Vol. 5, Issue 3, 2014.

[13] P.Paulpandi, Dr.T.Meyyappan, "Hiding Messages Using Motion Vector Technique in Video Steganography", International Journal of Engineering Trends and Technology, Vol.3, Issue no. 3, 2012.

[14] Vipul Sharma, Sunny Kumar, " A New Approach to Hide Text in Images Using Steganography", International Journal of Advanced Research in Computer Science and Software Engineering , Vol.3, Issue no 4, April 2013, pp. 701-708.

[15] Arijit Basu, Gaurav Kumar, Soumyajit Sarkar, "A Video Steganography Approach using Random Least Significant Bit Algorithm", International Journal of Science and Research (IJSR), Volume 3 Issue 6, June 2014.

[16] Mamta Juneja & Parvinder Singh Sandhu," Improved LSB based Steganography Techniques for Color Images in Spatial Domain", International Journal of Network Security, Vol.16, No.6, pp.452-462, Nov. 2014.

Author Profile

Ramandeep Kaur has completed B-Tech degree in Computer Science & Engineering from College of engineering & Management, Kapurthala in 2012 and pursuing M-Tech in CSE from CT Group of institutions, Shahpur (Jalandhar). Her interest of areas is Digital image processing, multimedia, Networking & information security. She has attended various seminars related to research work.