ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Improved Data Security and Secrecy Using Randomized Video Steganography

Shivali Bansal, Manpreet Kaur, Amit Doegar, Vandna Kumari

M.E Student, Dept. of CSE, National Institute of Technical Teacher's Training & Research, Chandigarh, India

Asst. Professor, Dept. of ECE, Indo Global College of Engineering, Abhipur, Punjab, India

Asst. Professor, Dept. of CSE, National Institute of Technical Teacher's Training & Research, Chandigarh, India

Asst. Professor, Dept. of CSE, Indo Global College of Engineering, Abhipur, Punjab, India

ABSTRACT: Information security has become an area of concern in the recent past due to advancement in technology. Digital media has become main source for communication. To safeguard the data from getting breached during communication various data hiding techniques have been evolved. Steganography is one of promising techniques of data hiding which is being used to provide secrecy to data. In this paper a novel approach to video steganography has been used to embed the information in video frames by randomizing various spatial domain techniques of Steganography. Each frame of video will be selected randomly and data will get embedded by XORing of data bits with cover frame bits according to the randomly selected technique. Qualitative and quantitative analysis of the proposed approach are also reported in this paper.

KEYWORDS-Information hiding, Video steganography, Spatial Domain, Randomization

I. INTRODUCTION

There is a substantial increase in usage of digital information in this modern era. To protect the digital information for getting compromised, Steganography can be used. However, steganography has been used since ancient times in various forms like it was first recorded in 440 BC, when Herodotus passed a message by shaving head of his servant and then scribbling the message on his scalp, then sending him to communicate the message once his hair had regrown[1], another method includes writing the message on wooden piece and then shielding it with wax layer [2], or using microdots for embedding[3]. Modern Steganography uses digital media for hiding viz. Text files, images, audios or videos. Steganography is an art and science of covert writing, the word steganography itself is derived from two words of Greek 'language, "stegos" which means covered and "grafia" which means writing. Steganography contains 3 components for embedding message, **cover media** in which data will get embedded, **message** which is to be hidden and **Stego Media** is cover file with data embedded into it. Steganography is a technique which provides secrecy to data by obscuring its existence during data communication.

It can be classified on the basis of cover media used for embedding i.e. text steganography, image steganography, audio steganography or video steganography. Recently, videos are being used for data hiding on a large scale, video steganography is an extension to image steganography where each frame of video is considered as an individual image, but video is dynamic in nature, so there are little chances of perception or the hiding capacity of video is much higher than in images. [4]. In this paper video has been used for data hiding.

This paper is constituted as follows. Section II contains the related research work in the field of Video Steganography, section III contains proposed work and section IV contains the qualitative and quantitative results of proposed method and section V includes the conclusion part.

II. RELATED WORK

In [5] author proposed an approach that was used to conceal a video stream in another video stream by using a unified approach of cryptography and steganography. Frames were encrypted using XOR operation and then scrambled frames were concealed in Least Significant Bit of frames of cover video by using sequential encoding following a specific pattern. In [6] author proposed an algorithm in which 3-3-2 LSB method was used to hide the data into cover frames of a video, i.e. 8 bits of data are embedded in such a manner that 3 bits of data get embedded into Red pixel, 3 in Green pixel and 2 in Blue pixel of LSB, then after the embedding stego frames went through an Genetic Optimizer, which optimized the stego. In [7] author described a method in which cryptography, steganography and parallelization were used altogether for data hiding, encryption was done using XORing of message bit with some key value and then embedding was done using LSB method in randomly selected frames. In [8] author proposed a method in message string was encrypted using 128 bit AES encryption, and then encrypted message's nibble was encoded in least significant nibble of cover image. Cryptography was proliferation to security of data over steganography. In [9]author proposed a new technique to embed the secret data in LSB of low color intensity value of RGB pixel, as low color intensities are not visible to HVS, so this resulted in less distortion.In[11] author proposed a spatial domain technique in which secret data bits were divided into an order of 3,3,2 and embedded in the LSB of RGB pixels of the cover video frames respectively. The locations to embed data in LSB were decided using a hash function. In [12] author introduced a method in which image cropping and LSB were used to conceal the secret message. A specific no. of portions of the cover image were cropped and also secret message was divided into same no. of parts, then message was embedded into three different color components of cover image crops using LSB method.

III. PROPOSED WORK

A. *RANDOM SCAN TECHNIQUE*

In Random Scan technique, the random locations bits of cover image are replaced with data bits –

Table ICover Video Frame Pixels for Random Scan Technique

10010101	11100011	01110010	01111111

Message bits: 10101100

Table IIStego Video Frame Pixels for Random Scan Technique

10**1**10101	11**0**00011	**1**1110010	0111111**0**

In this technique, detection of data is difficult as compared to LSB technique so highly secure technique. But for Steganalysis, lookup table required to know at which locations data is hidden.

B.*Raster Scan Technique*

In CRT display the electron beam scan the image from left to right, then right to left and come back to original position and so on. In the same way in data can be hidden left to right then right to left or can also take another pattern top to bottom or bottom to top for data hiding.

Table IIICover Image Pixels for Raster Scan Technique

10010101	11100011	01110010	01111111
10001001	01010101	10101110	00011001

Message bits: 10101100

TABLEIV Stego Image Pixels for Random Scan Technique

1001010**0**	1110001**0**	0111001**1**	0111111**1**
1000100**1**	0101010**0**	1010111**1**	0001100**0**

C. *LSB Technique*

This technique is one of the most popular techniques used to hide the information. In this technique the LSB of the 8 bit data series will be replaced in the LSB of the data already stored in the pixel. It goes on until all the bits of the information have been stored in the corresponding pixels:

Table VCover Video Frame Pixels for LSB Technique

10010101	11100011	01110010	01111111

Message bits: 10101100

Table VI Stego Video Frame Pixels for LSB Technique

1001010**0**	1110001**0**	0111001**1**	0111111**1**

D. *XORing Technique*

The XORing of data bits with cover pixels bits is done in LSB side for embedding because of this the probability in variation in pixel value of cover image reduces.

TABLE VII Stego Pixels for XORing Technique

Cover image	10101100	11011011
Data bits	000000**01**	000000**11**
Stego Image	**10101101**	**11011000**

E.*Methodology*

Steps of methodology of proposed work-

1. Input the Cover video and gray scale image to be concealed in the cover video.
2. Gray Scale image is converted into binary format and then data is split into 1-1 bits using BIT AND and BIT SHIFT operations.
3. Frames of cover video are extracted.
4. A frame is chosen at random using uniformly distributed pseudo random number generator to embed data.
5. R, G and B planes of selected frame are extracted.
6. Embedding technique is selected at random by using random number generator among three techniques- Random Scan Algorithm, Raster Scan Algorithm and LSB technique.
7. Data is embedded by XORing of the bits of cover frame and secret image using randomly selected technique
8. Recollect other unused frames and the frame with embedded data, and then make a stego video.

9. Calculate MSE, PSNR and correlation the stego video frames and evaluate the performance of techniques.

F.*Performance Analysis and Parameters*

Imperceptibility and Security are main features of any steganographic algorithm. Imperceptibility depends upon similarity of cover frame and stego frame and security depends upon degree of randomness in embedding. Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR) and correlation can be calculated to find similarity between cover and stego image.

IV.**RESULTS**

A. *Qualitative Analysis*

In Table VIII, videos of .avi format are taken as cover frame, and stego frame is frame with data embedded into the cover frame. Visual quality analysis of proposed approach is shown using different videos and different techniques of steganography selected randomly. Imperceptibility is most important characteristic of Steganography. In Table VIII, Fig a, c, e, g, i, k and m are randomly selected cover frames of different videos, while Fig. b, d, f, h, j, l and n are stego frames with data embedded into them according to randomly selected technique as mentioned in each cell of table. As per comparative analysis, cover frame and stego frame are similar, it's not easy for any opponent to percept the changes. So the proposed algorithm provides high level of imperceptibility, thus making it more secure and proving more secrecy to data

Table VIII Qualitative analysis

Cover Frame	Stego Frame
(a) Attrium.avi **Technique selected: LSB**	(b) **Attrium.avi**
(c) **Attrium.avi** **Technique selected: Raster Scan**	(d) **Attrium.avi**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

(e) **Attrium.avi** **Technique selected: Random Scan**	(f) **Attrium.avi**
(g) vipraffic.avi **Technique selected: Raster Scan**	(h) **vipraffic.avi**
(i) vipraffic.avi **Technique selected: LSB**	(j) **vipraffic.avi**
(k) Cat_video.avi **Technique selected: Random scan**	**(l) Cat_video.avi**

(m) Cat_video.avi	(n) Cat_video.avi
Technique selected: Raster Scan	

.

B. *Quantitative Analysis*

Quantitative analysis provides the results using mathematical calculations. In Table IX, results for 3 different .avi format videos with different steganography techniques selected randomly as per proposed technique are given using MSE, PSNR and Correlation as evaluation parameters. MSE should be least as possible. PSNR of 30 dB and above is acceptable in steganography and correlation should be nearly 1. As per the results given in Table IX, all the parameters are in acceptable limits and even providing better values for PSNR and Correlation thus resulting into more secure and randomized method for data hiding.

Table IX Quantitative analysis

Video	MSE	PSNR (dB)	Correlation
Video: Attrium.avi **Technique Selected:LSB**	0.46	51.49	0.99
Video: Attrium.avi **Technique Selected:Raster Scan**	0.48	51.47	0.99
Video: Attrium.avi **Technique Selected:Random Scan**	9.7	38.24	0.99
Video: Viptraffic.avi **Technique Selected:Raster Scan**	0.49	51.21	0.99
Video: Viptraffic.avi **Technique Selected:LSB**	0.49	51.21	0.99
Video: cat_video.avi **Technique Selected:Random Scan**	11.96	37.35	0.99
Video:cat_video.avi **Technique Selected:Raster Scan**	0.49	51.21	1

V.CONCLUSION

The proposed method provides a more secure approach to conceal confidential data by using three steganographic techniques randomly to make the system more robust against external attacks. Video is used as a cover media, as video provides large hiding capacity and is moving in nature, which makes it more difficult to judge any data inside video. Frames are selected randomly and steganographic techniques were applied randomly to hide data by XORing bits, thus providing more security and complexity for hackers. The proposed method gives Correlation, PSNR and MSE values in acceptable ranges. In future, visual cryptography can also be integrated with Steganography to provide more security. So data can be scrambled using visual cryptography and hence embedded into cover video. Also, more efficient steganographic techniques can be used randomly for hiding data.

REFERENCES

1. A. J. Raphael and V. Sundaram, “Cryptography and Steganography – A survey”, International Journal of Computing Technology and Applications, vol. 2, no. 3, pp. 626–630, 2011.
2. M. Bachrach and F. Y. Shih, “Image Steganography and Steganalysis”, Wiley Interdisciplinary Reviews: Computational Statistics, vol. 3, no. 3, pp. 251–259, 2011.
3. A. Thakur, H. Singh, and S. Sharda, “Different Techniques of Image and Video Steganography: A Review”,Recent Innovations in Electronics, Electrical and Computer Engineering, vol. 2, no. 2, pp. 5–8, 2015.
4. M. M. Sadek, A. S. Khalifa, and M. G. M. Mostafa, “Video Steganography: a comprehensive review”, Springer-Multimedia Tools and Applications, vol. 74, no. 17, pp. 7063-7094, March 2014.
5. P. Yadav, N. Mishra, and S. Sharma, “A secure video steganography with encryption based on LSB technique,” IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-5, 2013.
6. Kousik Dasguptaa, Jyotsna Kumar Mondalb and Paramartha Dutta, “Optimized Video Steganography using Genetic Algorithm (GA),” International Conference on Computational Intelligence: Modeling, Techniques and Applications, vol. Procedia Technology 10, pp. 131 – 137, 2013.
7. S.K.B, R.K, R.K.HS and G.Aithal," A New Approach for Video Steganography based on Randomization and Parallelization," Elsevier, International Conference on Information Security and Privacy, Nagpur, vol 78, pp. 483-490, 2015.
8. U. Sheth and S. Saxena, "Image steganography using AES encryption and least significant nibble," IEEE International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, pp. 0876-0879, 2016.
9. M. Srivastava, R. Ranjanand, “Video Steganography Using Pixel Intensity Value and LSB Technique,” International Journal on Recent and Innovation Trends in Computing and Communication, vol. 3, no. 2, pp. 287–290, 2015.
10. K. Dasgupta, J. K. Mandal and P. Dutta, “Hash Based Least Significant Bit Technique for Video Steganography (Hlsb),” International Journal of Security, Privacy and Trust Management (IJSPTM), vol. 1, no. 2, pp. 1–11, 2012
11. K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E. S. M. El-Rabaie and G. M. El-Banby, "High Security Data Hiding using Image Cropping and LSB Least Significant Bit Steganography," 4th IEEE International Colloquium on Information Science and Technology (CiSt), Tangier, pp. 400-404, 2016.

BIOGRAPHY

Shivali Bansal is a postgraduate student in the Computer Science and Engineering Department, National Institute of Technical Teachers Training and Research Institute, Punjab University, Chandigarh. She has done her thesis work in developing a secure approach for information hiding using Video Steganography. Her research interests are Digital Image Processing, Information Security, Computer Networks, etc.

Manpreet Kauris working as an assistant professor in ECE department at Indo Global College of Engineering. She has published 4 research papers in international journal & conferences. Her research interest is in Microelectronic, Sensors, Image Processing and Soft Computing.

Amit Doegar is working as an Assistant Professor in Department of Computer Science &Engineering ,National Institute of Technical Teachers Training & Research, Chandigarh and is actively engaged in research related to Computer Networks, Image Processing, Virtual Learning, Open Source Technology.

Vandna Kumariis working as an assistant professor in CSE department at Indo Global College of Engineering. Her research interest is in Image Processing and Cloud Computing. She has published research papers in international conferences.