CLEARIJRMST *Volume-05* *Issue-10* *Jul-Dec 2015*
Online -ISSN: 2249 -3506
Print-ISSN: 2249 -3492
www.thaavan.com

A NOVEL VIDEO-BASED STEGANOGRAPHIC MODEL FOR SECURE COVERT COMMUNICATION

[1]Dr.S.Meenakshi Sundaram,.[2]U.Revathy, [3]S.Pradeep
[1]Associate Professor - Department of Computer Science and Engineering, Aringer Anna College of Engineering and Technology, Dindigul,India, E-mail bosemeena@gmail.com
[2]Assistant professor- Department of Computer Science, Government Arts College for women, Sivagangai, India, E-mail urevathymeena@gmail.com
[3]Assistant professor- Department of Computer Science, Pannai College of Engineering and Technology, Sivagangai, India, E-mail csspradeep@gmail.com

ABSTRACT

Steganography is the art and science of hiding secret information by embedding it into multimedia data without leaving any apparent evidence of data alteration. Picture quality and Undetectability are two key factors related to image steganography techniques. The objective is to develop a video steganographic model that provides a secured communication and to send maximum hidden information while preserving security against Steganalysis techniques. This Paper presents an enhancing Steganographic model that uses video files as cover medium so as not to arise an eavesdropper's suspicion. The proposed model can conceal the presence of sensitive data regardless of its format. The secret message is divided into blocks and these blocks are randomized using random number to ensure security against hacker attacks. Data security depends on the robustness of the applied algorithm. We proposed a new algorithm that can select the embedding color channels in cover video based on pseudo random number generation. Then, the randomized message blocks are embedded in pseudo random locations. Embedding capacity is increased without losing the quality and fidelity of the cover video with the proposed algorithm. The Performance of the model is measured in terms of Peak Signal-Noise Ratio between cover and stego video.

INDEX TERMS: *Video Steganography, Steganalysis, LSB Embedding, Imperceptibility*.

I.INTRODUCTION:

Steganography can be considered as a branch of cryptography. But, unlike cryptography, which simply conceals the content or meaning of a message, steganography conceals the existence of a message. The strength of steganography can thus be amplified by combining it with cryptography. In this paper, we are going to implement Dual Steganography which combines the techniques in both cryptography and steganography.

We focused on spatial domain techniques that refer to the aggregate of pixels composing an image. It directly embeds the secret message in Least Significant Bits of pixels in cover file. In frequency domain techniques, the digital data is first transformed to frequency domain by using DCT, DWT or FFT and then the message is embedded in transformed co-efficients. Even though, the frequency domain scheme works better with minimal distortion in cover medium, it can embed only the limited amount of data. Embedding capacity of the cover medium will be increased with the spatial domain scheme and the proposed algorithm.

This paper is organised as follows: Section II presents the Embedding stage with the proposed steganographic algorithm. Section III presents the Extraction stage with performance measurement.

Section IV reports the experimental reports and analysis. Finally, Section V presents the conclusion.

II.EMBEDDING

Assume, we have a cover medium as video file and image as secret message. The Embedding stage includes four phases as follows:

- Cover Video Preprocessing
- Secret Message Preprocessing
- Randomization of secret message
- Embedding(Stego-key & Secret Message)

Here, the Stego-key includes Secret

Message file length, file format and Randomization seed which is used to randomize the secret message. The stego-key will be included in very first frame of cover video.

In first phase, the cover video is splitted into 'S' no. of frames. Each frame dimension is HxW. Each input pixel is encoded with K-byte precision.

In second phase, the secret message is divided into's' no. of blocks where s≤S. Each block is assigned with N^2 bytes.

In third phase, the blocks of secret message are randomized with generation of permuted vectors Q_1 and Q_2 , each of size N to randomize the positions (row, column) of the secret-message blocks of data. To do this, we generate two permuted vectors Q_1 (1: N) and Q_2 (1: N) .Starting with a secret message block P (1: N,1: N), we construct the randomized permuted secret message block U(1: N,1: N) as follows:

$$U\ (i, j) = P\ (Q_1\ (i), Q_2\ (j)),$$

Where i and j are image/video frame row and column coordinates respectively. In effect, we utilize the generated random permuted values of $Q1$ and Q_2 vectors to change the locations of pixels in P matrix in a manner specified by the stego key which is the seed to generate the 1 Q and 2 Q vectors. The locations in each of the two vectors are unique, therefore the mapping $P \rightarrow U$ is one to one. In the LSB based techniques used so far, the algorithm just replaces the two LSB of each color channel in each pixel. By this, the hacker can easily detect the secret message or can change the LSB to destruct the message. Our proposed algorithm ensures more security since it predicts the sequence of color channels, in that sequence only the secret message will be embedded. The algorithm is explained below:

STEP 1: Get a pseudo random generated no. to predict the sequence of color channel.

The following table depicts the sequence of color channels:

Table 1: PROPOSED ALGORITHM

Random Number	Sequence
0	RGB
1	RBG
2	GRB
3	GBR
4	BRG
5	BGR

STEP 2: Depending on the random no. generated, select the sequence of color channels.

STEP 3: Replace the two LSB of color channels in the predicted sequence.

The process of embedding secret message bits in the RGB color channels is explained below:

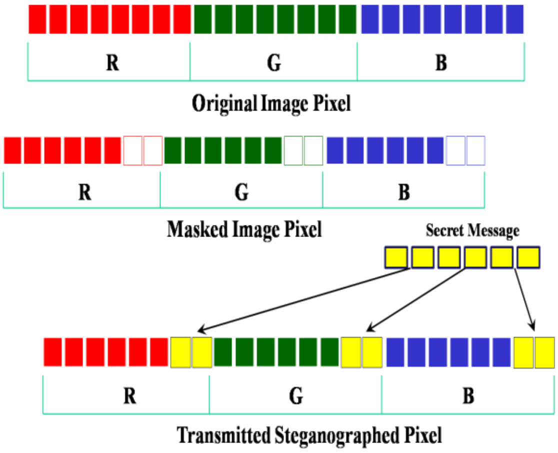


Fig 1: RGB Pixels and secret message bits

In fourth phase, the randomized secret message blocks and the stego-key are converted to binary streams. The stego-key is embedded in very first frame of cover video. Then, the secret message blocks are embedded in cover video frame by using the above algorithm.

The block diagram of embedding stage is explained as follows:

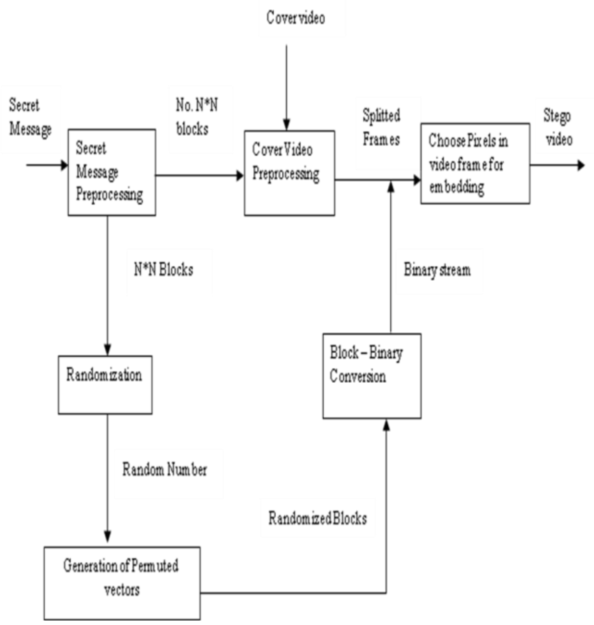


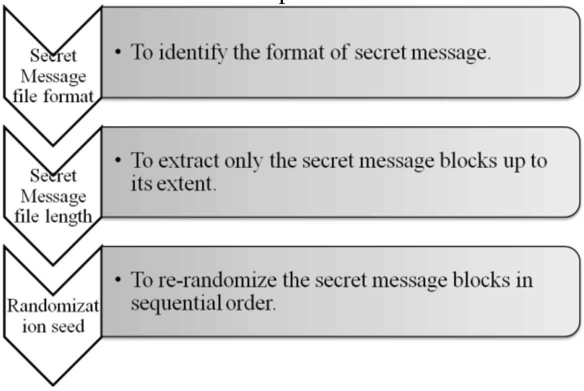
Fig 2: Embedding Stage

III.EXTRACTION

In extraction stage, there are four phases:

- Extraction of Stego-key
- Extraction of randomized secret blocks
- Re-Randomization of secret message
- Performance Measurement

In first phase, the stego-key is extracted from the first frame of stego video. From the stego-key, the secret message file length, file format and randomization seed are separated.



- To identify the format of secret message.
- To extract only the secret message blocks up to its extent.
- To re-randomize the secret message blocks in sequential order.

Fig 3: Stego-key Extraction

In second phase, the randomized blocks of secret message are extracted from the cover video frames by using the proposed algorithm. The two LSB from each pixel is extracted from each stego video frame to get N^2 bytes of data. Based on the sequence of color channels, the randomized blocks are constructed.

In third phase, the randomized secret message blocks are re-randomized with the randomization seed extracted from the stego-key. The secret message is constructed from the re-randomized blocks. The format of the secret message is extracted from the stego-key.

In fourth phase, the performance between the cover video and the stego video can be measured. Steganography is mainly characterized by imperceptibility. The perceptual imperceptibility of the embedded data is indicated by comparing the original image or video to its stego counterpart so that their visual differences, if any, can be determined. Additionally, as an objective measure, the Mean squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) between the cover and stego video may be calculated. These parameters are given by:

$$MSE=1/HW \sum_{(i=1toH)}\sum_{(j=1toW)} (P(i,j)-U(i,j))^2$$

Where *P (i,j)* and *U (i,j)* are the pixel values at row *i* and column *j* of the cover image and stego image respectively.

$$PSNR=10 \log_{10} L^2/MSE$$

Where *L* is the Peak signal level.

The block diagram for extraction stage is explained as follows:

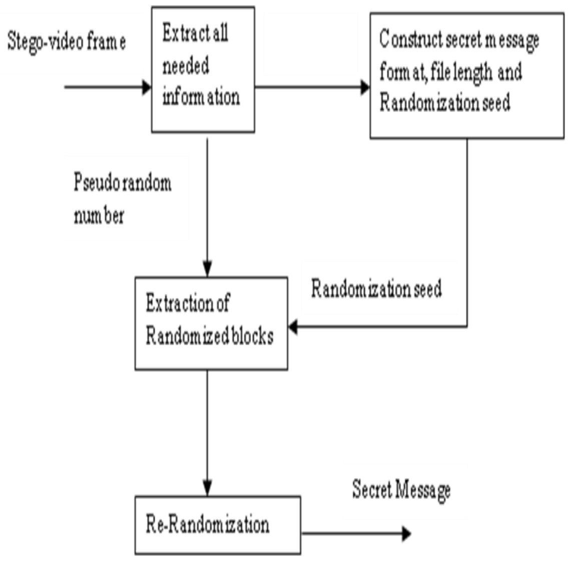
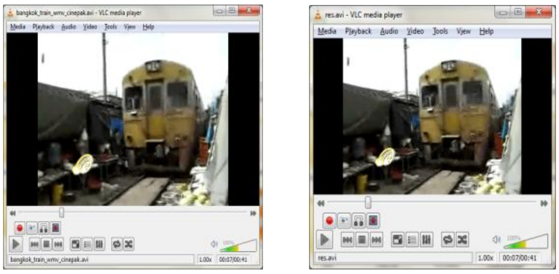
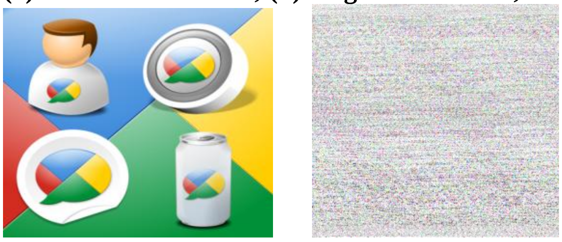

Stego-video frame
Extract all needed information
Construct secret message format, file length and Randomization seed
Pseudo random number
Randomization seed
Extraction of Randomized blocks
Re-Randomization
Secret Message

Fig 3: Extraction Stage

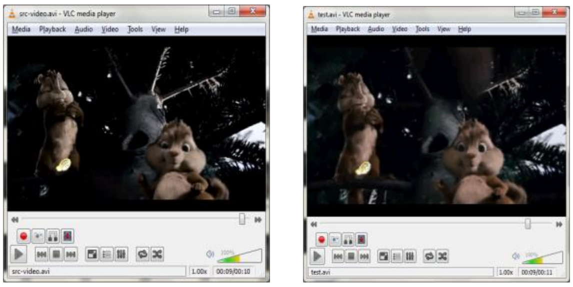
IV. EXPERIMENTAL RESULTS


(a) (b)

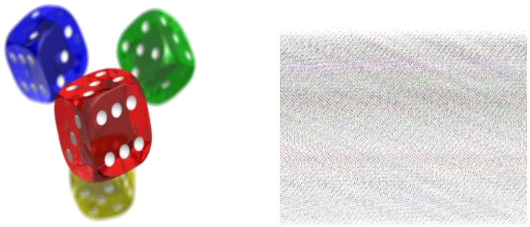
(a) Cover video frame; (b) Stego video frame;


(c) (d)

(c) Secret message (Dimension: 390x390, Size: 103 KB); (d) Secret message after randomization


(a) (b)

(a) Cover video frame; (b) Stego video frame;


(c) (d)

(c) Secret message (Dimension: 600x800, Size: 215 KB); (d) Secret message after randomization

V.PERFORMANCE EVALUATION

1. PSNR and MSE

Steganography is characterized mainly by two aspects; imperceptibility and capacity. Imperceptibility means the embedded data must be imperceptible to the observer (perceptual invisibility) and computer analysis (statistical invisibility). Capacity means maximum payload is required, *i.e.* maximum amount of data that can be embedded into the cover image without losing the fidelity of the original image. The perceptual imperceptibility of the embedded data is indicated by comparing the original image or video to its stego counterpart so that their visual differences, if any, can be determined. Additionally, as an objective measure, the Mean squared Error (MSE), Peak Signal to Noise Ratio (PSNR) and Root Mean Square error (RMS) between the cover and stego images may be calculated. These parameters are given by:

$$\mathbf{MSE=1/HW \sum_{(i=1toH)}\sum_{(j=1toW)} (P(i\,,j)-U(i\,,j))^2}$$

Where *P (i , j)* and *U (i , j)* are the pixel values at row *i* and column *j* of the cover image and stego image respectively.

$$\mathbf{PSNR=10\ log_{10}\ L^2/MSE}$$

Where *L* is the Peak signal level.

2.RUN TIME COMPLEXITY

Run-time analysis is a theoretical classification that estimates and anticipates the increase in running time (or run-time) of an algorithm as its input size (usually denoted as *n*) increases. The specific amount of time to carry out a given instruction will vary depending on which instruction is being executed and which computer is executing it. The run-time complexity is measured for different size of images so that the robustness of the algorithm can be proved.

Table 5.1: Run-time complexity for different size of images

Size of the Secret Image File (bytes)	Time for Embedding (milli secs)	Time for Extracting (milli secs)
30000	130	20
120000	200	70
151875	180	120
494928	340	140
593280	410	150
705600	430	130

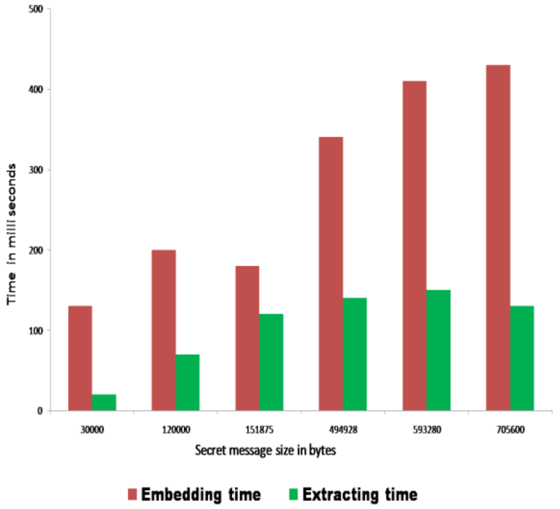


Fig 5.1 Bar chart indicating the Run-time complexity for various size secret message

Table 5.2: Peak Signal to noise Ratio and Mean Squared Error for different size of images

Size of the Secret Image File (bytes)	Mean Squared Error value	Peak Signal to Noise Ratio
30000	0.06436724	60.07815
120000	0.22481166	54.64661
151875	0.27237862	53.81307
494928	0.6389	52.0987
705600	0.68698	51.987

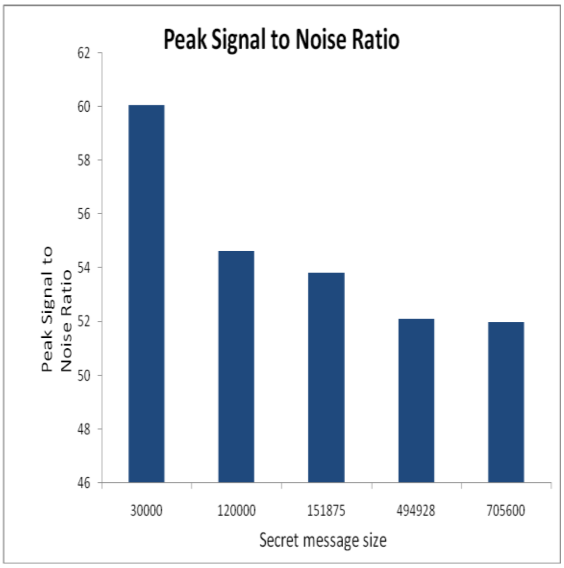


Fig 5.2: Bar chart indicating the Peak Signal – Noise Ratio

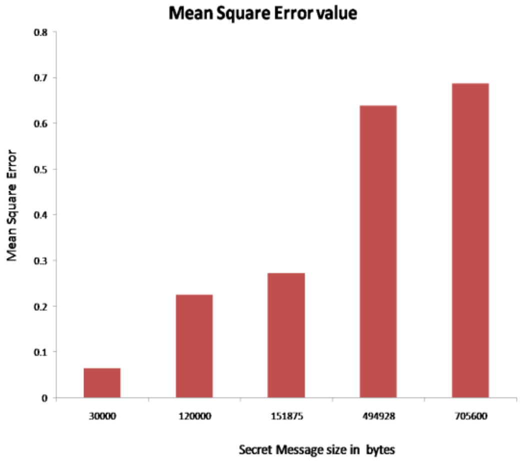


Fig 5.3: Bar chart indicating the Mean Square Error value

VI.CONCLUSION

Steganography is a fascinating and effective method of data hiding that can be used throughout history. There are many good reasons as well to use this type of data hiding, including watermarking for storing such things as passwords and confidential information. Success in steganographic system's secrecy results from selecting proper mechanisms. Our proposed steganographic system implements the LSB replacement algorithm to reduce the difference between original pixel and steganographic pixel. The algorithm cannot provide the way to attackers to reveal the secret information, since it is embedded under two encrypted layers. Secret data detection is much more difficult than previous techniques. The randomization of secret message blocks adds more security especially if an active encryption technique is used. The previous techniques, where one technique lacks in payload capacity, the other lacks in robustness. Since, the video files is used as a cover file, the payload capacity is increased as well the proposed algorithm improves the robustness of the system.

VII.REFERENCES

[1] Daniela Stanescu, Mircea Stratulat, Voicu Groza, Joana Ghergulescu and Daniel Borca, **"Steganography in YUV color space"**, IEEE International Workshop on Robotic and Sensors Environments (ROSE 2007), Ottawa- Canada, pp.1-4, October 2007.

[2] N. Provos and P. Honeyman, **"Hide and Seek: An Introduction to Steganography"**, IEEE Security & Privacy Magazine, Vol. 1, issue 3, pp. 32-44, June 2003.

[3] Stefan Katzenbeisser and Fabien A. P. Petitcolas, **"Information Hiding Techniques for Steganography and Digital Watermarking"**, Artech House Books, December 1999, ISBN 1-58053-035.

[4] R.Kavitha and A. Murugan, **"Lossless Steganography on AVI File using Swapping Algorithm"**, International Conference on Computational Intelligence and Multimedia Applications, pp. 83-88, Sivakasi-TamilNadu, Dec. 2007

[5] Yeunan-Kuen Lee and Ling-Hwei Chen, **“High Capacity Image Steganohraphic Model”**, IEE Proceedings in Vision, Image and Signal Processing, Vol. 147, issue 3, pp. 288-294, June 2000.

[6] Neil F. Johnson, Zoran Duric and Sushil Jajodia, **"Information Hiding: Steganography and Watermarking - Attacks and Countermeasures"**, Kluwer Academic Publishers, 2000, ISBN: 0-79237-204-2.

[7] C. Ming, Z. Ru, N. Xinxin and Y. Yixian, **"Analysis of Current Steganography Tools: Classifications & Features"**, Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06), pp. 384-387, California, Dec. 2006.

[8] Hema Ajetrao, Dr.P.J.Kulkarni and Navanath Gaikwad, **” A Novel Scheme of Data Hiding in Binary Images”**, International Conference on Computational Intelligence and Multimedia Applications,Vol.4, pp. 70-77, Sivakasi-Tamil Nadu, Dec. 2007.

[9] Yueyun Shang, **"A New Invertible Data Hiding in Compressed Videos or Images"**, Third International Conference on Natural Computation (ICNC 2007), Vol. 4, pp. 576-580, Haikou, Aug. 2007.

[10] Venkatraman S., Ajith Abraham and Marcin Paprzycki, “**Significance of Steganography on Data Security”**, International Conference on Information Technology: Coding and Computing (ITCC’04), Vol. 2, April 2004.

[11] Namita Tiwari, Madhu Shandilya, **“Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth”,** International Journal of Security and Its Applications Vol. 4, No. 4, October, 2010.