Password Protected Secure Data Hiding Technique Using Raster Scan Technique

[1]Maninder Pal Singh, [2]Harmandeep Singh
[1]Research Scholar, [2]Assistant Professor
[1]Department of Electronics and Communication Engineering
[1]Global Institute of Management and Emerging Technologies, Amritsar, India

***Abstract* - Video Steganography is an art of hiding any kind of secret data or any type of information inside a video. Therefore, with the help of password protected security it's safer and it also overcomes the capacity issues and increases the space of data hiding because a single video consists of multiple of fames. In this paper, propose video steganography technique which is based on Raster Scan Technique. The main aim of this paper is to provide secure data as well as high capacity as compared to Shadow Derivation Technique. This proposed method also analyzed the Peak Signal to Noise Ratio with the existing results.**

***Index Terms* - Raster Scan Technique, Peak Signal to Noise Ratio (PSNR), Security, Shadow Derivation Technique, Steganography.**

I. INTRODUCTION

Steganography is a technique of hiding a data i.e. audio, video, text and image with changing its perceptual quality. Steganography word comes from Greek which pronounce like steganos means "covered" and graphia means "writing" which is known as cover writing. The main purpose of steganography is to hide the existence of communication from a third party. Thus, in steganography it hides the existence of data in such a way which is very difficult to find out with the help of human eyes [3].

Generally, in data hiding, the actual information is not maintained in its original format. It would be converted into an alternative equivalent multimedia files like video, audio, text and images. With the help of these multimedia files a secret information is being hidden within another object [7].

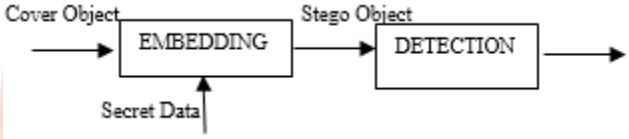

Fig. 1: Block Diagram of Video Steganography

a) ***Cover Object*** - Cover object is an object in which secret data can be hided.
b) ***Secret Data*** - Secret data is a one type of message which hides in the cover object. The Secret data is would be any image, text message, audio and video.
c) ***Embedding*** - The Secret data is embedded in cover object with the help of multiple techniques like Least Significant Bit (LSB) Technique, Modified LSB, Random Scan and Raster Scan Technique.
d) ***Stego Object*** – After hiding the secret data into a cover object the Stego object is generated. Then Stego object is transmitted from the transmitter side to the receiver side.
e) ***Detection*** - At the receiver side, the receiver receives the steganalysis is done on the stego object and further receiver detects original data.

In a Video Steganography, the hidden data can be embedded into two parts i.e. either into image or into audio part of the video stream.

Method of Steganography

The effectiveness of any Steganographic method can be determined by comparing stego-image with the cover image. There are some factors that determine the efficiency of a technique. These factors are [6]

1. ***Mean Square Error (MSE):*** It is defined as the average squared difference between a reference image and a distorted image. The small the MSE, the more efficient the video steganography technique. MSE is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count.

$$MSE=\frac{1}{M*N}\sum_{1}^{M}\sum_{1}^{N}(Fij-Gij)^2 \qquad (1)$$

M: Numbers of rows of cover image

N: Number of column of Cover Image
Fij: Pixel value from cover image
Gij: Pixel value from Stego Image

2. ***Peak Signal to Noise Ratio (PSNR):*** It is defined as the ratio between the signal and corrupting noise. This ratio measures the quality between the original and compressed frame. The higher the value of PSNR represents the better quality of the compressed image.

$$PSNR=10\log_{10}\frac{Imax^2}{MSE}\ dB \qquad (2)$$

Where I*max* is the maximum intensity value.
MSE is the mean square error

3. **Correlation Factor**: It is defined as the measure of extent and direction of linear combination of two random variables. If there are number of two variables are closely related, then the correlation coefficient is close to the value 1.
At the other side, if the coefficient is close to 0, then two variables are not related [6].

$$r=\frac{\sum_i(Xi-Xm)(Yi-Ym)}{\sqrt{\sum_i(Xi-Xm)^2}\sqrt{\sum_i(Yi-Ym)^2}} \qquad (3)$$

Xi - pixel intensity of original image
Xm- mean value of original image intensity
Yi- pixel intensity of encrypted image
Ym - mean value of encrypted image intensity
For Steganography the Correlation factor should be 1 for ideal Case so no dissimilarity in Stego image as compared to cover image.

4. ***Root Mean Square Error (RMSE):*** It is calculated by getting the square root of the mean square error (MSE). The RMSE can be calculated as follows.

$$RMSE=\left[\frac{1}{NM}\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}(g(x,y)-f(x,y))^2\right]^{1/2} \qquad (4)$$

5. ***Total Average Difference****:* This parameter is used to calculate the average difference between the two values.

$$AD=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j)-y(i,j)) \qquad (5)$$

The paper is organized as follow; section II starts with the Proposed Methodology in which proposed block diagram, proposed algorithm with examples. Section III illustrates the results in which proposed work PSNR are compared with Shadow Derivation technique.

II. PROPOSED METHODOLOGY

The Proposed block diagram of video steganography at the transmitter side is explained below:

1. Input Video
2. Frame Extraction
3. Secret Data
4. Password Protected Key
5. Frame Generate in RGB Plane
6. Stego Data
7. Secret Data Generate in RGB Plane in Receiver Side
8. Secret Data Recovered
9. Embedding Frame
10. Output Video

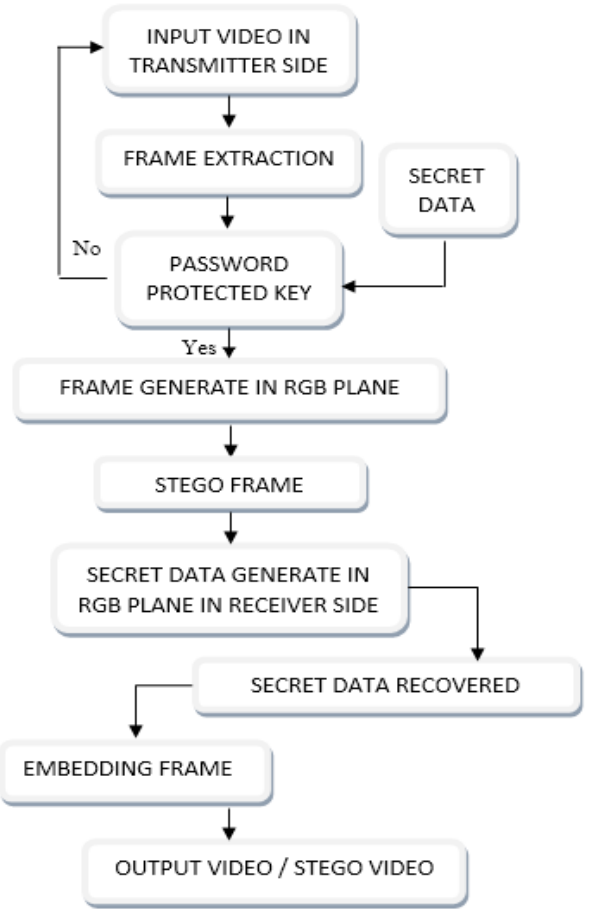

Fig. 2: Proposed Block Diagram of Video Steganography in Transmitter & Receiver Side

1. ***Input Video:*** A video is a mixture of multiple of images as well as audio. Therefore, these both images and audio consider for steganography.
2. ***Frame Extraction****:* Frame extraction is a process of extracting a frame from a video.
3. **Secret Data:** The secret data is in any form like text, audio, image.
4. ***Password Protected Key****:* When right key is entered only then secret data will be hidden in the cover frame otherwise it shows error.
5. ***Frame Generate in RGB Plane****:* At the transmitter side, while hidden process is running then cover fame converted into Red, Green and Blue (RGB) planes.
6. ***Stego Frame****:* After hiding the secret data into a frame the Stego frame is generated.
7. ***Secret Data Generate in RGB Plane****:* At the receiver side, while recovering the original data secret data can be converted into Red, Green and Blue (RGB) planes.
8. ***Secret Data Recovered***: When RGB process is finished, original secret data can be recovered at the receiver side.
9. ***Embedding Frame***: Embedding Frame is a technique to re-attach the stego frame into a video.
10. ***Output Video****:* After embedding the data in frame the reconstruction of video is done. Which is also known Stego Video in the Transmitter side.

Proposed Algorithm

Transmitter Side

1. Read the cover Frame.
2. Read the secret data.
3. Enter the Secret key.
4. Hide the Encrypted data in Random bits of cover image by doing XORing of cover image with data bits.
5. Frame generate in RGB plane
6. After hiding data Stego image is transmitted.

Receiver Side

1. At the Receiver side XORing of cover image and Stego image is done to extract the encrypted data bits from stego image.

2. Then Original message is generated by subtracting the data bits from their class.

III. SIMULATION RESULTS

In this paper, to implement Raster Scan Technique we use MATLAB 2013. This MATLAB, which is commonly known as Matrix Laboratory, it is a state of the art of mathematical software package and it is used in both academia and industry.
The results of this proposed algorithm as follows:

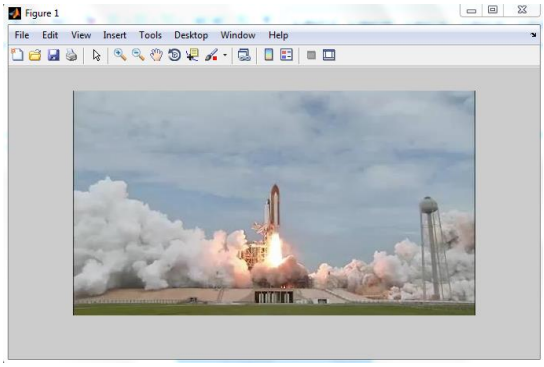

Fig. 2: Cover Frame

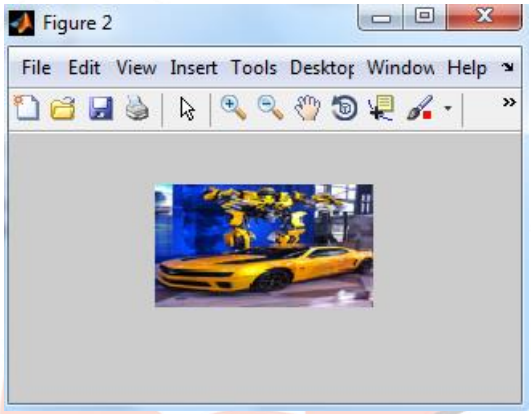

Fig. 3: Secret Data

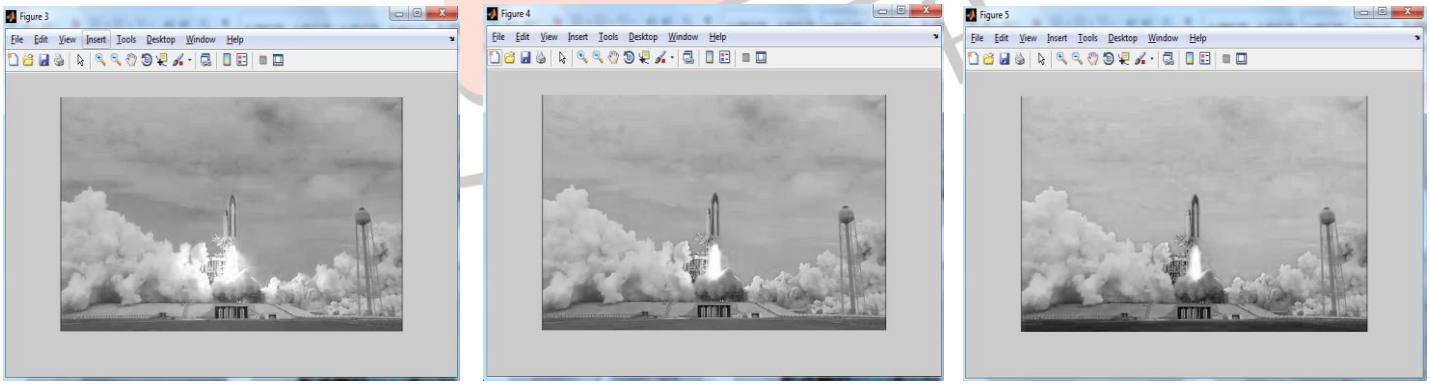

Fig. 4: Cover Frame in Red, Green & Blue (RGB) Plane

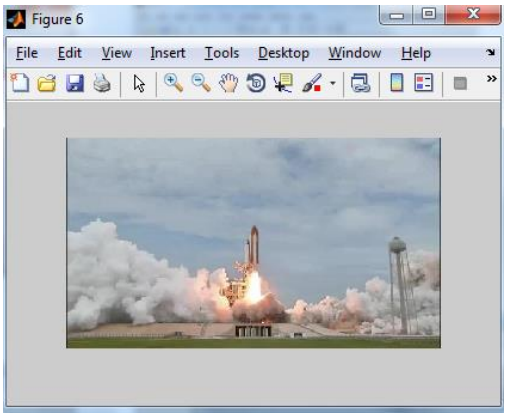

Fig. 5: Stego Frame

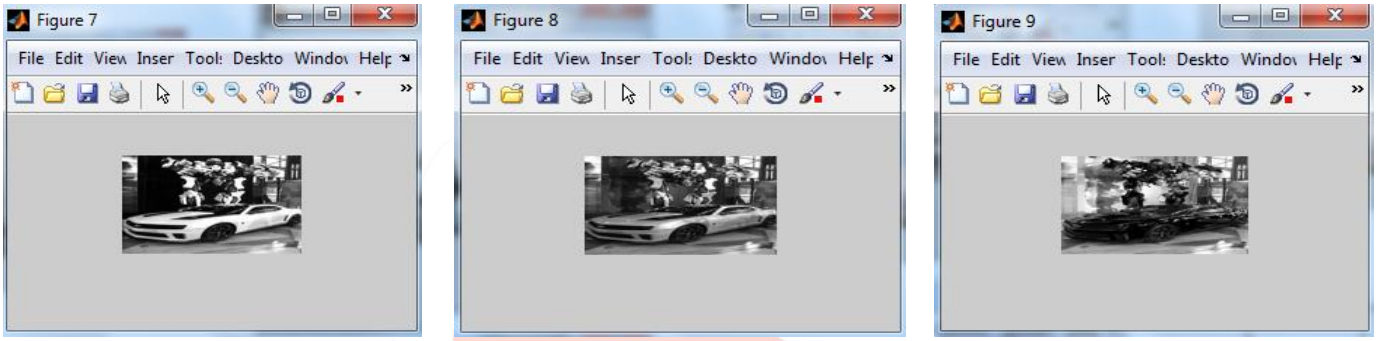

Fig. 6: Secret Data in Red, Green & Blue (RGB) Plane

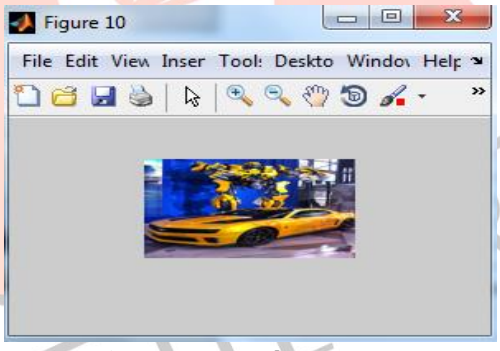

Fig. 7: Recovered Secret Data

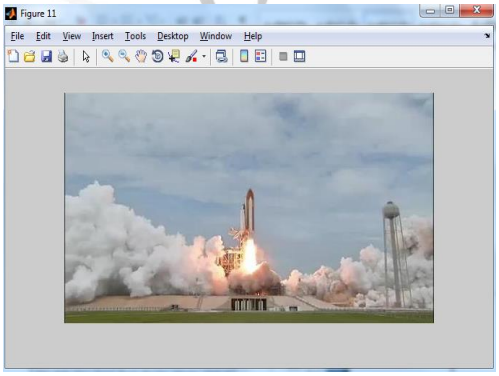

Fig. 8: Original Cover Frame

Comparison table for Proposed and Existing Technique PSNR

Table 1: Comparison table for Proposed and Existing Technique PSNR

Parameter	PSNR for Existing Algorithm (dB)	PSNR for XORing Algorithm (dB)
PSNR	42.50 db	47.8645 db

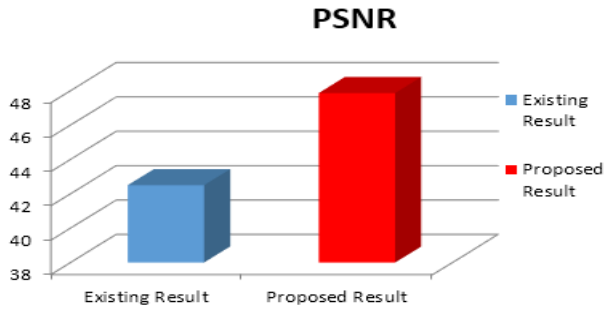

Fig. 9: Comparison Parameter for PSNR

TABLE 2: SOME OTHER PARAMETERS

S. No.	Parameters		Proposed Results
1.	MSE		0.3048
2.	Correlation Factor	R	0.9996
		G	0.9996
		B	0.9999
3.	RMSE		0.5521
4.	Total AD		0.0070

IV. CONCLUSION

In this paper, Raster Scan technique is used. This Raster scan technique is known as proposed and implemented using Shadow Derivation as an existing. The PSNR are compared with existing Shadow Derivation Technique. The Simulation Results shows that proposed technique better PSNR as compared to existing technique and some other Parameters are also mention in this paper which shows better result by using Raster Scan Technique.

V. ACKNOWLEDGEMENT

This research paper is made possible with the help and support of our family members, teachers and friends. We would also like to dedicate this acknowledgment of gratitude toward all those significant advisors.

REFERENCES

[1] Rohit G Bal, Dr P Ezhilarasu "An Efficient Safe and Secured Video Steganography Using Shadow Derivation" International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Online): 2320-9801, ISSN (Print): 2320-9798 Vol. 2, Issue 3, March 2014 PP 3251-3258.

[2] Youssef Bassil "Image Steganography Method based on Brightness Adjustment" Advances in Computer Science and Application (ACSA), ISSN: 2166-2924, Vol. 2, No. 2, 2012.

[3] Ajay Kumar, Manu Bansal, "Hiding Negative of an Image using Steganography Even Odd Algorithm for Security Purposes" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727 Vol. 16, Issue 1, Ver. VI (Feb. 2014), PP 70-75.

[4] Japleen Kour, Deepankar Verma, "Steganography Techniques-A Review Paper", International journal of Emerging Research in Management and Technology, Vol-3, May 2014.

[5] Pritish Bhautmage, Prof. Amutha Jeyakumar, Ashish Dahatonde, "Advanced Video Steganography algorithm", International Journal of Engineering Research and application, Vol.-3,Janurary-February 2013.

[6] S. Thenmozhi and M. Chandrasekaran "A Novel Technique for Image Steganography Using Nonlinear Chaotic Map" 7th International Conference on Intelligent Systems and Control (ISCO), pp. 307-311, 2013.

[7] A. Swathi 1, Dr. S.A.K Jilani "Video Steganography by LSB Substitution Using Different Polynomial Equations" International Journal of Computational Engineering Research (ijceronline.com) Vol. 2 Issue, 5 PP- 1620-1623.