DESIGN AND IMPLEMENTATION OF VIDEO STEGANOGRAPHY SYSTEM USING SINGULAR VALUE DECOMPOSITION

[1]Vivek Kumar Yadav, [2]Sonu Lal
[1]M-Tech scholar, [2]Professor
[1] Department of Electronics & Communication Engineering,
[1,2]IES College of Technology, Bhopal, India

Abstract— Steganography is the art by virtue of which one can hide the very existence of an existing communication. Different steganography methods are used based on suitable types of requirements. In this project, we propose a video steganography methodology using singular value decomposition (SVD) and discrete wavelet transform (DWT). SVD and DWT enhance the quality and performance of video steganography. Results have been taken over the data sets of an embedded standard secret image in a standard video stream. The final results have been plotted and compared between peak signal to noise ratio (PSNR) with embedding strength and mean square error (MSE) with embedding strength. Experimental results indicate that the proposed steganography method based on SVD and DWT provides high level of imperceptibility, robustness against many existing methods.

Index Terms— Video Steganography, Singular Value Decomposition, Discrete Wavelet Transform, Embedding Strength.

I. INTRODUCTION

The very term steganography named after the amalgam of two Greek words namely 'Stegos' and 'Grafia'. Stegos stands for 'Cover' and grafia stands for 'Writing' [1]. Video Steganography simply referring about concealing the secret data into the video stream [2]. It is an extension of image steganography. Since, we already know that a series of consecutive and equally time-spaced static images, exploiting our own visual system i.e. Human Visual System, are called as Video stream [3]. It even consists of audio most of the times now days. This is the reason why many of the image steganographic techniques are applicable for the video steganography too. The best advantage of video steganography over image steganography is that it's better data hiding capacity and the popularity and a frequent data sharing in form of video over the internet especially through the social networking websites [4]. Thanks to the cheaper cost of data rates over the internet. The positive surge in digital communication over the internet arise higher requirements of security to maintain the secrecy of communication. Video steganography is a suitable tool for it [5].

II. RELATED WORKS

In 2016 IEEE, Ramadhan J. Mstafa et al. [6] presented associate article. The article states that, in the past decade, the science of info activity has gained tremendous significance owing to advances in information and communication technology. The performance of any steganographic algorithm depends on the embedding potency, embedding payload, and robustness against attackers. Low hidden ratio, less security, and low quality of stego videos are the key problems with several existing steganographic strategies. In this paper, we propose a novel video steganography technique in DCT domain supported hamming and BCH codes. To improve the safety of the proposed algorithmic program, a secret message is first encrypted and encoded by exploitation BCH codes. Then, it is embedded into the discrete cosine transform (DCT) coefficients of video frames. The hidden message is embedded into DCT coefficients of each Y, U, and V planes excluding DC coefficients. The proposed algorithmic program is tested over two varieties of videos that contain slow and fast-paced objects. The experiential results of the proposed algorithmic program are compared with three existing strategies. The comparison results show that our proposed algorithmic program outperformed alternative algorithms. The hidden ratio of the planned algorithmic program is more or less 27.53%, which is thought of as a high concealing capability with a tokenish exchange of the visual quality. The robustness of the planned algorithmic program was tested over totally different attacks.

In 2016 IEEE Conference, Liyun Qian et al. [7] presented associate article, in which he uses EMD to construct a replacement transformation matrix to enhance the initial matrix cryptography algorithmic program and proposes a replacement video steganography algorithm: Improved Matrix encoding (IME). The proposed algorithmic program retains the benefits of EMD and matrix secret writing that it will greatly scale back the modifications of infix carrier to attain a high embedding potency over the conditions of same embedding capability. At the same time, the proposed algorithmic program solves the drawback that the embedding rate of matrix secret writing is comparatively low. The experiment compared with similar algorithms show that the algorithm has benefits in PSNR, SSIM, and bit rate increase.

In 2016 IEEE Conference, Kasra Rezagholipour et al. [8] presented associate article and expressed that Video steganography may be a data that gives a secure association by concealing the key message within the video sequins. In this paper, we propose a new video steganography algorithmic program supported by object motion that the key info is embedded in motion vectors of moving objects. Therefore by exploitation the mean shift algorithmic program the existed objects in every frame are detected. Based on motion estimation algorithmic program in B and P frames, motion vectors of each object with quarter pixel accuracy are extracted. To ensure that the chosen motion vectors are belong to the article and even have a required balance between capability and video quality, a threshold value is outlined. So the motion vectors whose worth are higher than the edge value are chosen. The secret message is embedded in one-quarter both horizontal and vertical part of every chosen motion vector. The result shows that the proposed algorithmic program will infix a massive quantity of information in motion object and achieved a decent video quality.

III. PROPOSED METHODOLOGY

The proposed method has two primary functions i.e. embedding of secret image into the original video data file at one end and its extraction from the stego video data file at the other end. For embedding of the secret image we have focused on primary color planes i.e. R, G, B planes of each frame using DWT and DCT. Singular Value Decomposition (SVD) is used for realizing Singular values of each frame. For the extraction process, the reverse procedure has been followed using inverse SVD, IDCT and inverse DWT respectively. The following figure shows the overall embedding and extraction process at respective ends:

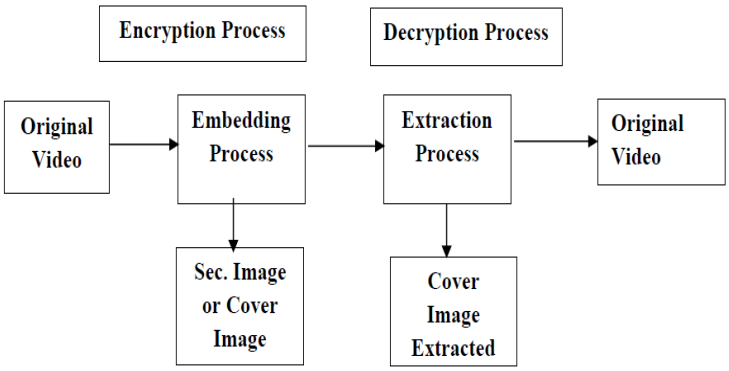

Fig 1 Proposed Methodology overview

The following flowchart indicates the detail procedural steps taken during the embedding process:

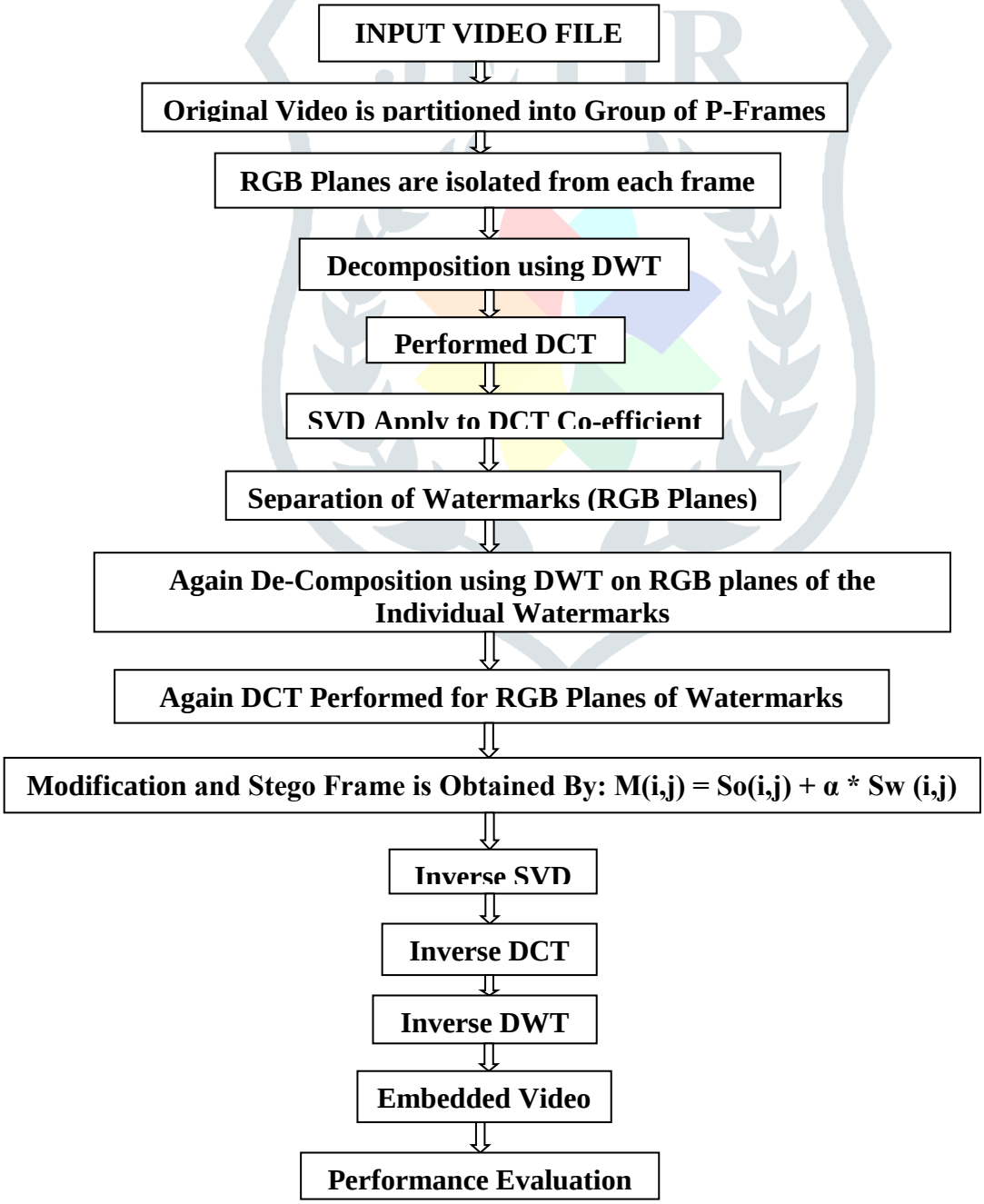

Fig. 2 Embedding Process of Secret Image into the Original Video

In the above flowchart, first the original video file is converted into a group of P number of frames then RGB planes are separated and decomposed in different frequency bands with the help of DWT. For acquiring the transformed coefficient DCT is applied on selected frequency bands then SVD provides the singular values in subsequent step. Same procedure is followed for the individual watermarks too. Now the singular values of each plane of each frame in video is merged with singular values of each planes of individual watermarks at particular scaling factor. The following expression is used for getting the stego frame:

$$M(i, j) = So(i, j) + \alpha * Sw(i, j)$$

M(i, j): Stego Frame;
So(i, j)= Singular values of R, G, B plane of each frame in video;
Sw(i, j)= Singular values of R, G, B plane of individual watermarks;
α= Scaling Factor
Further processing is also shown in the figure given. Now, for the extraction of the cover image reverse procedure is applied. The extracted file can be acquired by following expression:

$$Sw(i, j) = (M(i, j) - S0(i, j)) / \alpha$$

IV. RESULTS AND DISCUSSIONS

The result has been obtained using Matlab R2012b platform. To evaluate the performance, first human vision test has been done with some persons i.e. by visualizing the original and stego video with naked eye, how many of them are able to finding any difference between them. But this test is purely subjective in nature and hence not sufficient. Therefore, some rational methods are needed to check the performance of the method.

To check the performance of the technique we have proposed, a number of experiments, comprising of standard video files and cover image files, have been done.

One of the used video streams (Figure 3) has the following specifications:

File Name: Viptrain
Size (Frame Width × Frame Height): 360× 240
Frame Rate: 25 fps
Total bit rate: 4000 kbps

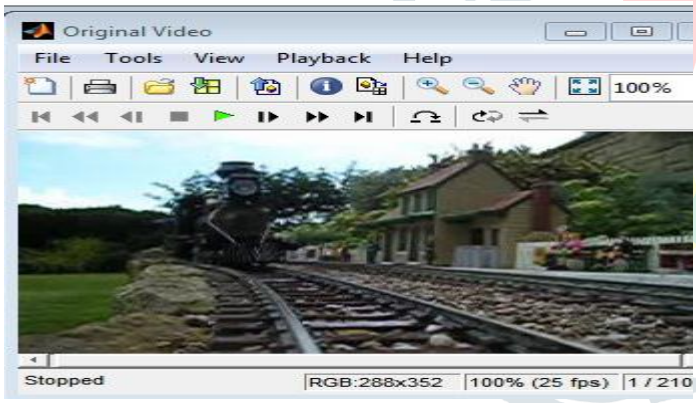

Fig 3 Original Video viptrain

Fig 4 Stego Video viptrain

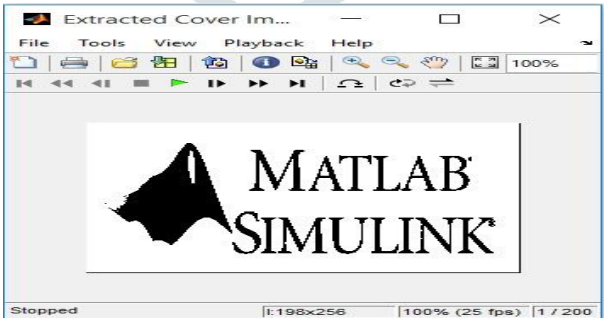

Fig 5 Extracted Cover Image with x =0

Figure 3 shows the standard video streams which we have used for our interest, the specifications have been provided in the paper. Figure 4 shows the stegno video in which we have embedded the secret image. Figure 5 shows the extracted image from the stegno video.

Performance Evaluation

Performance of our proposed system is evaluated with the help of peak signal to noise ratio (PSNR) and the mean squared error. The PSNR attributed to the present work to calculate the extracted image quality in comparison with the original hidden image. The PSNR is given by;

$$PSNR = 10 \log_{10} (255^2/MSE)$$

Where, the Mean Square Error between the original image I of size M × N and the extracted image I_s are evaluated by following expression;

$$MSE = \frac{1}{MN}\left[\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I(i,j) - I_s(i,j)\right)^2\right]$$

Based on our testing, the values of MSE and PSNR with respect to embedding strength are summarized in the following table.

Table 1 MSE and PSNR Values

Embedding Strength	MSE	PSNR
0.1	.0161	152.13
1	0.161	129.10
2	0.3214	122.17
3	0.4821	118.12
4	0.6428	115.24
5	0.8035	113.01
6	0.9643	111.18
7	1.1250	109.6478
8	1.2857	108.3125
9	1.4464	107.1346
10	1.6071	106.0810

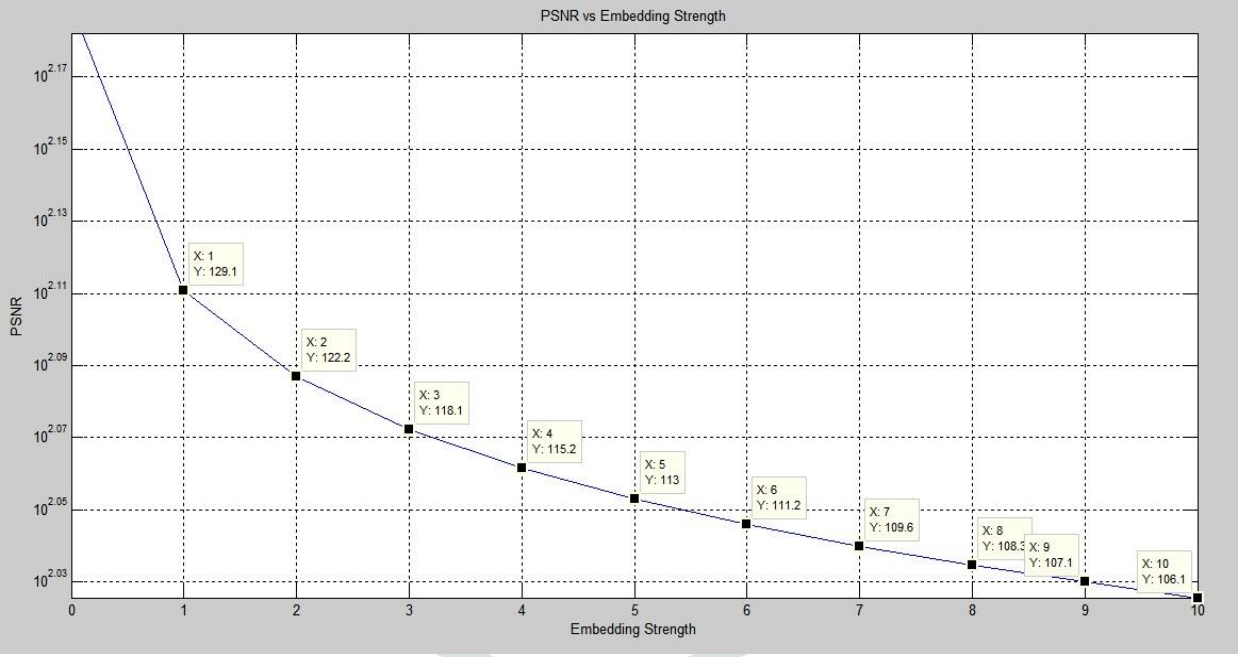

Fig 6 PSNR Vs Embedding Strength

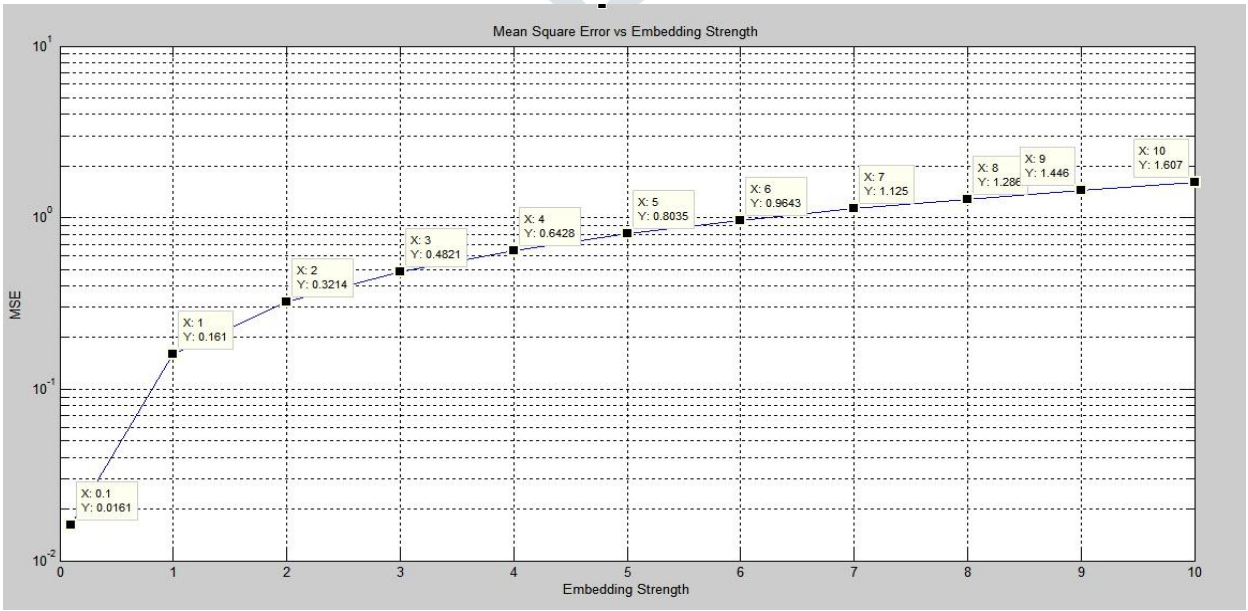

Fig 7 MSE vs Embedding Strength

In figure 6 we have plotted PSNR with respect to embedding strength and in figure 7 it is MSE with respect to embedding strength to check the performance of the system. It shows that as the embedding strength increases the MSE also increases but the PSNR decreases.

V. CONCLUSION

In this paper, we have presented video steganography method based on SVD using DWT and DCT. It is a less complex method as compared to many other existing video steganography methods. Moreover, the application of DWT makes our method computationally feasible. The experimental outcomes indicate that the DWT and SVD based system has more imperceptibility which results in increased level of security as far as communication is concerned.

REFERENCES

[1] Diljeet Singh, Navdeep Kanwal, "Dynamic Video Steganography Using LBP on CIELAB Based K-Means Clustering". IEEE 2016

[2] Dhanya Job, Varghese Paul, "An Efficient Video Steganography Technique for Secured Data Transmission". IEEE 2016

[3] Ramandeep Kaur, Pooja, Varsha, "A Hybrid Approach for Video Steganography using Edge Detection and Identical Match Techniques". IEEE 2016

[4] Diksy M. Firmansyah, Tohari Ahmad, "An Improved Neighbouring Similarity Method for Video Steganography".

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

[6] Ramadhan J. Mstafa, Khaled M. Elleithy, "A Novel Video Steganography Algorithm in DCT Domain Based on Hamming and BCH Codes". IEEE 2016

[7] Liyun Qian, Pei Zhou, Jian Chen, Zhitang Li, "An Improved Matrix Encoding Steganography Algorithm Based on H.264 Video". IEEE 2016

[8] Kasra Rezagholipour, Mohammad Eshghi, "Video Steganography Algorithm based on motion vector of moving object". IEEE 2016.