International Journal of Advanced Trends in Computer Applications
www.ijatca.com

Video steganography based on interpolation and LSB substitution with secret key and DWT

[1]Amandeep kaur, [2]Rupinder kaur
[1]Department of cse,Doaba institute of engineering and technology,kharar, India
[2]Assistant Professor
Department of cse,Doaba institute of engineering and technology,kharar, India
[1]eramandeepkaur91@gmail.com,[2]rupinder8610@gmail.com

Abstract: *The improvement in computer network communications make transmission of data comparatively simple and quick although, there are chances of attacks on them. The hidden information is an imperative problem for transferring video data from one party to third party. In the image processing field of research, steganography determines the legitimate meaning of hiding all the information from introducers and transmit the video data in secure, protected form so that the third party cannot reveal that message. Steganography is a branch of hiding information used for hiding corrective information in digital media such photographs, digital music, or digital video. This approach can be applied on graphics, images, text, audio and video, and so forth. In this paper, approach based on Interpolation and LSB (Least significant bit) technique with secret key and DWT is proposed for video steganography. This technique is applied for replacing the byte into M's bit for transmitting video to the trusted receiver. The video in cover file is inputted and then steganography technique is applied that will converts this cover file into output file which is in the form of stego file.*

Keywords: *Steganography, video steganography, LSB and stego file, embedding capacity.*

I. INTRODUCTION

Steganography is a process in which the data is hiding for transferring information in secure form and for achieving protected communication environment. Earlier, some techniques were employed to write over an invisible standard ink for painting. Usually an application is created by a person and that application is used by many units of persons. Hackers are people who try to alter the authentic application by modifying it or by using that application for making profits without giving any credit to owner. For this reason protection should have the substantial priority for application [1]. The techniques used for protection must be efficient, robust and unprecedented to impede malicious users. Steganography has many applications that involve medical applications, ownership protection to access, validation for authentication in future use, air traffic monitoring system, and many more.

Earlier the schemes that were introduced for stegnography, worked in spatial domain, where stegnography is applied by modifying the values of pixel of the host image. The spatial domain stegnography is easy for implementation from a computational point of view, but too fragile for resisting various attacks. In contemplation of having more encouraging techniques, stegnography in transform domain was the main focus. Here, stegnography is not combined to the image intensities, but with values of its transform coefficients. After this the inverse transform is performed, to get the stegnography image. Some techniques of stegnography based on transform used the Discrete Cosine Transform (DCT). In the transform domain there is another type of transformation namely wavelet transform. In stegnography DWT (Discrete Wavelet Transform) is most commonly used wavelet transform and is most effective, easy to implement. It is more intermittently used because of its excellent spatial localization and multi-resolution characteristics.

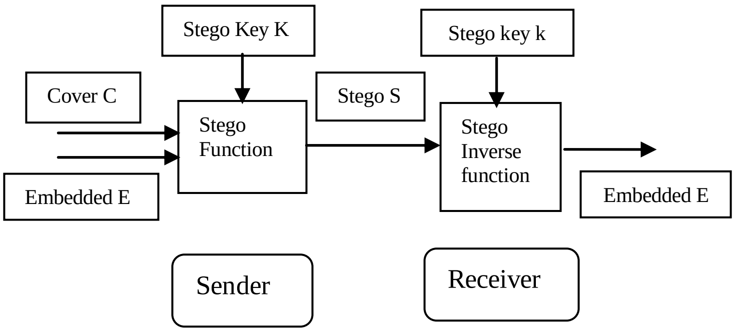


Fig 1: Stegnography

Steganography is the secure transmission of hiding secret messages (hidden text) within object (cover text) which produce a stego text. This stego text can use by recipient to improve his knowledge with help of the particular method of steganography method. This process is employed to recover the hidden text from the stego text. The purpose behind steganography is to consent all parties for communicating easily such that an attacker cannot educate about the location either there is meaning hidden in their conversation for excelling performance. The process of steganography is distinct from the process of cryptography. Even though stegnography provide private communication which based merely on fact that it is being helped to include useful information. The stegnography process has received significant attention from both academia and industry. There are two main branches for security that is digital watermarking and steganography but steganography is a new way to covert communication message. The main purpose of this is used to convert the data information secretly by applying very existence of communication [3]. In the stegnography, carrier can be image, text, audio and video etc.

The main advantage of this system is to provide high security for key information exchanging. This system finds applications in medicine by doctors to combine explanatory information within X-ray images. It is also useful in communications for codes self error correction.

Secret Key Steganography

A secret key or private key is an encryption/decryption key which is only known to the single person or group of person that exchange secret messages. The secret key steganography system is analogous to a symmetric cipher, in which the sender chooses a cover image and the secret message is then embedded into the cover image by using a secret key. If the secret key used for embedding is known to the receiver, then the receiver can reverse the process and extract the secret message. Anyone who doesn't know the secret key should not be able to obtain the information.

Interpolation

It is a process which is used to improve capacity, enhance image quality, and recover a cover video steganography. Here the nearest neighbor method of interpolation is used. This technique can find the close interconnected corresponding pixels of the cover video for each block and set these pixels to a new value for the destination received video by utilizing the neighboring pixels. The Interpolation Neighboring Pixels (INP) method helps to increase the payload in hiding data. The pixels present at near neighboring locations likely to have similar values of intensity. So with this there can be improvement in better quality with less distortion of video. Another interpolation technique is Bilinear Interpolation method. This technique tenacious the new value from the weighted average of four closest pixels. This method is also used to alter the size of video frames for estimating unknown pixels values.

Nearest Neighbor technique for Interpolation

Nearest Neighbour technique is the simplest as well as fastest implementation of video scaling in interpolation. It is very useful when the speed is concerned for the basic form of interpolation. As the actual pixels are copied to their new locations proportionality, so that the position in relation to one another remains the same. The video is enlarged and filler pixels must be placed in between the actual pixels. The most basic nearest neighbor interpolation is just copied the exact same pixel values over to the filler pixel closest to the pixel.

Least significant bit (LSB) techniques

LSB is the type of steganography technique which is common and simple for embed information in an image file. This LSB Method will replace byte into an M’s bit therefore technique works for image, video steganography. Due to widespread and increasing use of the Internet and easy file access, there are many different methods to ensure that a file is not accessible to everyone; steganography is one of them to hide information. By using steganography the file is completely hidden from anyone’s eyes. During hiding one file in another file, there are several techniques for maintain high quality of cover data at same time ensuring high capacity for embedding information of send video, Interpolation technique can be used to obtain the high quality of digital media. Watermarking technique can used for embedding hidden data to attaches copyright protection information with stego media for security. This provides an indication of ownership of the digital data over video steganography.

In 1-LSB insertion usually has a 50 percent chance to change a LSB every 8 bits, thus adding very little noise to the original picture. For 24-bit images the modification can be extended sometimes to the second or even the third LSBs. 8-bit images instead have a much more limited space, so it's possible to change only the LSBs without the modification being detectable. The most basic of LSBs insertion for 24-bit pictures inserts 3 bits/pixel. Since every pixel is 24 bits, we can hide

3 hidden_bits/pixel / 24 data_bits/pixel = 1/8 hidden_bits/data_bits

For this case 1 bit of the embedded message is hided for every 8 bits of the cover image where as insertion to include the second LSBs, the formula used is given below;

6 hidden_bits/pixel / 24 data_bits/pixel = 2/8 hidden_bits/data_bits

In this case 2 bits of the embedded message can be hiding for every 8 bits of the cover image. Data rate for 1-LSB insertion in 24-bit images or in 8-bit images is 8/1*8 = 8 Bytes, whereas for 2-LSBs insertion in 24-bit pictures it becomes 8/2*8 = 4 Bytes.

DWT discrete wavelet transform

DWT is the form of wavelet transform that divides an image into four coefficient segments in single level. Each coefficient segment contains one of low frequency bands and high frequency bands. In DWT, the most useful information in the signal appears in high amplitudes and the less eminent information appears in very low amplitudes. For this, DWT need to improve the security of the videos as it uses the frequency domain information of the cover video frames.

II. LITERATURE SURVEY

This section discussed the research work that has been done in last few years. Stegnohraphy is the most promising field of research in which all researchers are interested. A literature review goes beyond the pursuit for information or knowledge and it involves the recognition and connection of relationships among the literature and our research field.

Ki-Hyun Jung et al. [1] in 2014, proposed steganography method for hiding secret data in order to provide high level data such as video or an image. Therefore, the reversible data hiding method can extract information to cover image in place from a stego-image without distortion or noise after extracting the hidden data.

In this work, Steganography using LSB and DWT are used together hiding the secret message with copyright protection of data to provide high level of security and interpolation technique is used for maintain higher quality of cover video. The proposed work makes the use of video for embedding the secret data. Today video are fast emerging as a next generation steganography medium that offers many advantages over traditional steganography. The great benefits of video are hide large amount of data inside. Therefore, any small but otherwise noticeable distortions might go by unobserved by human’s eyes because of the continuous flow of information.

Semi reversible data hiding method utilizes to interpolation in the video quality and the least significant substitution methodology is proposed to embed information. Interpolation methods are used in scaling up and down the cover information before hiding secret data for a higher capacity and quality. The LSB substitution method is used to categories to embed secret data to the video techniques and experimental results show. The proposed method can embed a huge amount of secret data for the security purpose while keeping very high visual quality.

Bhautmage et al. [2] (2013) introduced the data embedding for the process of embedding information in a data source without changing its attributes perceptual quality of video. Several constraints affect to this process so that the quantity of data is hidden due to need for invariance. These data under the condition consists a host signal which is subject to distortions such as lossy compression. The degree of data must be immune to interception, modification or removal by a third party. A new technique is applied for data embedding and extraction for high resolution AVI videos. For change the LSB of the cover file, the LSB and LSB+3 bits are changed in alternate bytes of the cover file. The secret message is encrypted by using a simple bit exchange method for actual embedding process. The index is created for the secret information and the index is placed in a frame of the video itself. It is easily extract the secret message which can reduce the extraction time.

Sidham Abhilash et al. [3] in 2013 proposed a Novel Lossless Robust Reversible Steganography Method for Copyright Protection of Images for the reversible Steganography (RRS) methods. These methods are popular in multimedia to protect copyright and preserving the host images as well as providing robustness against unintentional attacks. RRS methods are not rapidly applicable in practice because they fail to provide satisfactory results on wide-scale image datasets; they have limited access to robustness in extracting message from the stego images destroyed by different unintentional attacks and some of them suffer from extremely very poor invisibility for stego images. The framework has needed to address problems and further improve its performance.

Yadav Pooja et al. [4] in 2013 introduced the need of hiding information from intruders. It has been seen around ancient times. Therefore, the digital media is getting more advanced research like text, image, audio, video etc. Maintain the secrecy of information which is different methods of hiding steganography deals with true meaning of hiding information under some other information without any noticeable change in cover information. Video Steganography become bone for providing solution of large amount of data to be transferred secretly. Videos are simply a sequence of images where space is available between in range to hiding information. In recent research, video steganography is used to hide a secret video stream in cover video stream. Each frame of secret video has broken into individual set of components then changed into 8-bit binary values. It is encrypted video using XOR with secret key. The encrypted frames hide information in the least significant bit so that each frames using sequential encoding process of Cover video and enhance more security for each bit of secret frames stored in cover frames following a pattern BGRRGBGR.

Tao Zhang et al. [5] in 2010 described the new steganalytic method which is based on statistical distribution of pixel differences. This is designed to detect information to the presence frame of spatial LSB matching steganography strategy in high-resolution of natural images. Therefore, it established an advance statistical model used for the distribution of pixel differences of all natural images based on the Laplacian distribution techniques and estimated the numbers of zero pixel difference values are based on the number of non-zero pixel to find difference values. According to the properties of LSB matching steganography, it also estimated error on basis of distinguishing feature for steganography classification. The steganalytic method provides the better performance analysis for the detection of LSB matching steganography strategy in high-resolution image for future use. It has a low computational complexity as well as fast computational speed for hidden features of video data.

Balaji et al. [6] in 2011 introduced the Video Steganography which is the process of hiding some secret meaningful information inside a video. The addition information to video is not easily recognizable by the human eye perception as the change of a pixel color is negligible to process. This research has provided an efficient, effective and a secure method for video Steganography. This method creates a number of indexes for the secret information and this index is placed in a frame for the video itself with the help of this index and the frames containing the secret information are located in frame.

Moon et al. [7] in 2013 described the video as cover media for hiding the secret message which is used computer forensics as tool for authentication for hide an image and text behind a video file. The algorithm is used such as 1LSB, 2LSB, 4LSB. In this research, 4LSB method has found to be better for hiding more secret information data. It deals with more idea of video steganography, cryptography for computer forensic techniques in both investigative and security manner.

III. METHODOLOGY

In this section, methodology is discussed which is followed in this research. Here, how the stegnography and the secret key are embed into the video frames is described. Because of the human perceptible system the stegnography is applied only in the mid frequency band of the image. Figure 2 represents the flow chart of embedding algorithm to embed the stegnography into color video.

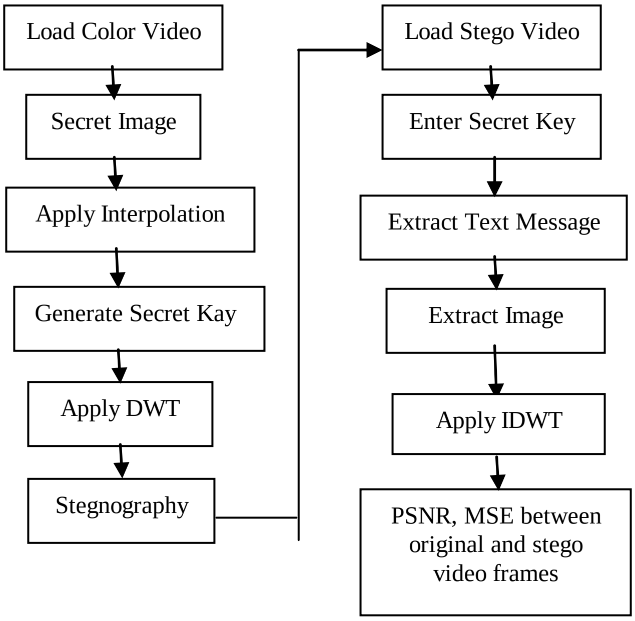


Fig 2: Flowchart of Methodology

Step 1: First of all we load the color video and then convert video into frames and frames into images.
Step 2: In this step, secret image is added to the images (from input video).
Step 3: Interpolation is applied on the images and secret key is generated. This secret key is then used for security purpose.
Step 4: Apply LSB (least significant bit) to hide the text message.
Step 5: In this step DWT is applied. Here each image is decomposed into three color components (R.G.B) and then 5-Level DWT is applied to each component of video frame.
Step 6: Then apply stegnography into LH and HL bands i.e. mid frequency bands of each level so convert each pixel value into binary.
Step 7: We start to embed the stegnography from HL5 (5th level mid frequency band) and then sequence into LH5, HL4, LH4, HL3, LH3, HL2, LH2, HL1 and LH1.
The process of extraction requires secret key (generated during transmission phase) for selecting the frames, the wavelet transform filter and the channel where the stegnography is inserted. Fig. 2 represents the flow chart of methodology that includes extraction algorithm also for extracting the stegnography, hidden message and secret key from the stegnography video. Steps involve in extraction process are;
Step1: Load the stegnographyed video or data stored in array and then separate it into the frames.
Step 2: Convert each pixel of mid frequency band into binary and extract the secret image, secret message.
Step 3: Combine three arrays for three images R.G.B, so that the original video will retrieved.

Step 4: Finally calculate the MSE and PSNR values between the original and stegnographyed (Stego) image.
Step 5: Last stored the stegnography video frame data into array for stegnography extraction before applying inverse DWT.

IV. EXPERIMENTAL RESULTS

Parameters Used:
There are some parameters which were useful in our implementation:

A) PSNR

PSNR is most commonly used to measure the quality of for image. The signal in this case is the original data, and the noise is the error introduced. When comparing, PSNR is a human perception of reconstruction quality. The PSNR is calculated based on color texture based image segmentation. The PSNR range between [0, 1], the higher is better. PSNR calculate by using formula:-

$$PSNR = 20\log10\ (255/\sqrt{MSE})$$

B) MSE

Mean Square Error (MSE) is calculated pixel-by pixel by adding up the squared difference of all the pixels and dividing by the total pixel count. MSE of the segmented image can be calculated by using the Equation given below. The MSE range between [0, 1], the lower is better. The MSE between the signals is given by the following formula:

$$MSE = (1/N)\ \Sigma i|x\ (i) - e\ (i)\ |^2$$

Here x is the stego image and e input image. N is the size of image.

C) Embedded Capacity

For embedding payload, also called embedding capacity, we use ER, being short for embedding rate, to represent the percentage of the embedded secret bits in the whole pixels of the cover image. The ER is defined as in equation written below,

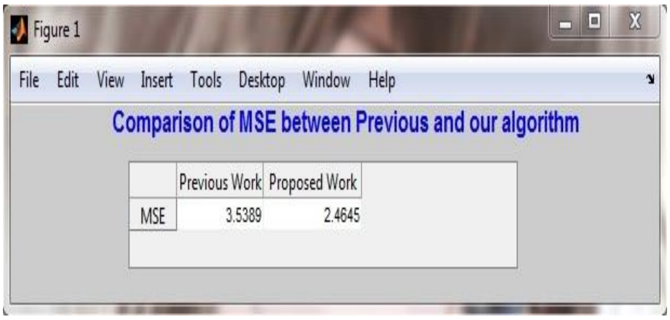
$$ER = \frac{N}{H \times W} bpp$$

Here, N is the total number of the embedded secret bits and $H \times W$ is the size of the carrier. According to the embedding capacity evaluation, a large value of ER represents that the Steganographic scheme has better performance in terms of the embedding capacity, that is, a cover pixel in the cover image can carry more secret bits. On the contrary, a small value of ER represents a worse performance.

D) BER

Bit error rate is the number of bit errors per unit time. BER is a unit less performance measure, often expressed as a percentage. The bit error ratio can be considered as an approximate estimate of the bit error probability. This estimate is accurate for a long time interval and a high number of bit errors.
BER=1/PSNR

Results Obtained:
The main objective of the research was to provide enhanced security by LSB (Least significant bit) technique with secret key and DWT for color video stegnography. Different parameters such as PSNR, MSE, BER and embedded capacity are estimated for validating the proposed technique in comparison with the earlier techniques.



Comparison of MSE between Previous and our algorithm

	Previous Work	Proposed Work
MSE	3.5389	2.4645

Fig 1: Comparison of MSE between Previous and Proposed techniques

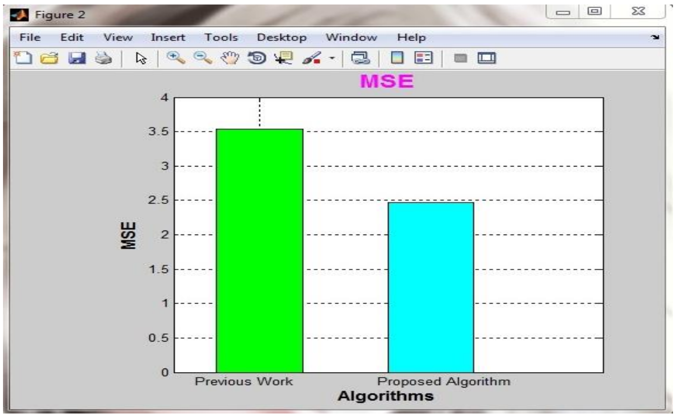
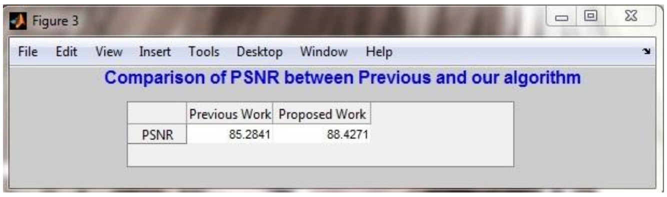


Fig 2: Graph Comparison of MSE between Previous and Proposed techniques

From figure 1 and 2 it is observed that the mean squared error calculated for proposed work is lower in comparison to that of previous. This shows that the proposed method is more efficient that previous method. A lower value for MSE means lesser error and as seen from the inverse relation between the MSE and PSNR, this translates to a higher value of PSNR. Logically a higher value of PSNR is good because it means is that the ratio of signal to noise is higher



Comparison of PSNR between Previous and our algorithm

	Previous Work	Proposed Work
PSNR	85.2841	88.4271

Fig 3: Comparison of PSNR between Previous and Proposed techniques

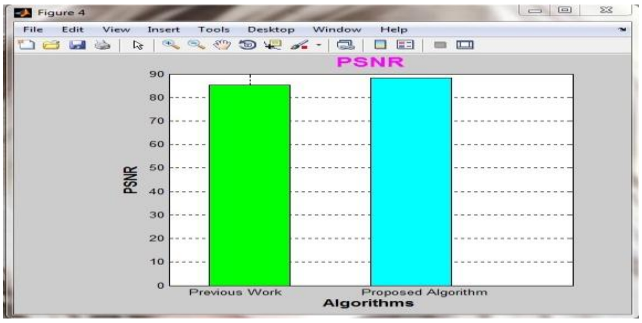
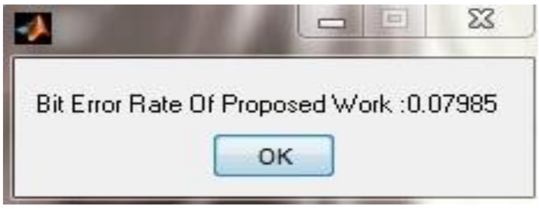


Fig 4: Graph Comparison of PSNR between Previous and Proposed techniques

The figure 3 shown below shows the comparison graph of PSNR (peak signal to noise ratio) between the original and stego video frames. The green color bar shows the values of PSNR obtained by previous technique and the blue color line shows the values of PSNR obtained by using proposed technique. PSNR is the measure of quality of the image. Higher the value of PSNR higher is the strength of the signal and lower is the distortion.

The figure 4 shows the values of PSNR for both previous and proposed work. Here peak signal to noise ratio is calculated for each frame. It is estimated by using previous technique. PSNR is calculated by using
PSNR = 10.log$_{10}$ (MAX^2_I/MSE)

PSNR is the measure of signal strength in comparison to the noise present. After calculating MSE, PSNR is estimated. It is the mean squared errors and lower the value of MSE, more efficient is the system.



Bit Error Rate Of Proposed Work :0.07985

Fig 5: BER of Proposed techniques

The figure shown above shows the value of BER for proposed work. It is the number of bit errors per unit time and is calculated by using the relation
BER= 1/PSNR.

The value obtained of BER is 0.079 with the proposed approach.

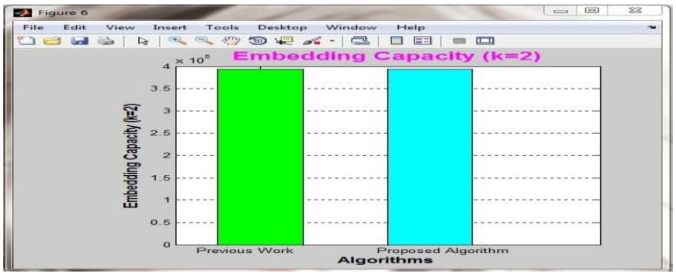
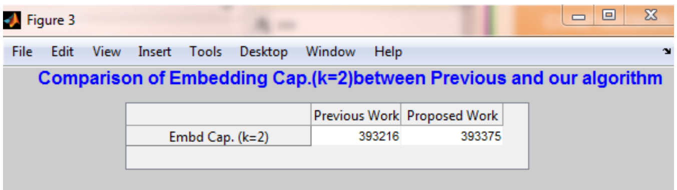


Fig 6: Graphical Comparison of Embedding Capacity (k=2) between Previous and Proposed techniques



Comparison of Embedding Cap.(k=2)between Previous and our algorithm

	Previous Work	Proposed Work
Embd Cap. (k=2)	393216	393375

Fig 7: Comparison of Embedding Capacity (k=2) between Previous and Proposed techniques

The figures shown above (figure 6 and figure 7) shows the comparison of embedding capacity between previous and proposed algorithm when the value of k=2.

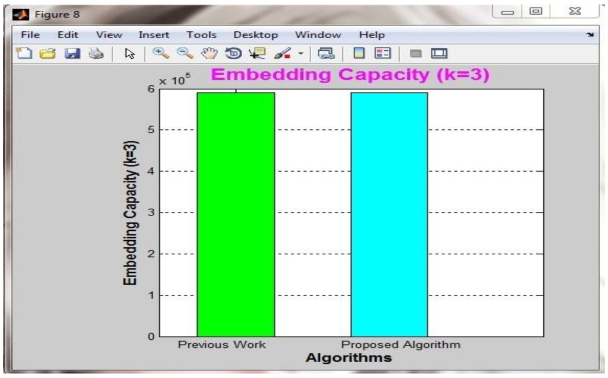
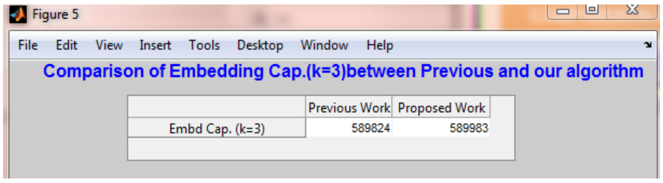


Fig 8: Graphical Comparison of Embedding Capacity (k=3) between Previous and Proposed techniques



Comparison of Embedding Cap.(k=3)between Previous and our algorithm

	Previous Work	Proposed Work
Embd Cap. (k=3)	589824	589983

Fig 9: Comparison of Embedding Capacity (k=3) between Previous and Proposed techniques

The figures shown above (figure 8 and figure 9) shows the comparison of embedding capacity between previous and proposed algorithm when the value of k=3. Higher the value of the embedding capacity, higher is the performance of the approach.

From all the experiments performed and these results obtained are evident that the proposed LSB technique with secret key and DWT is more efficient and competent for color video steganography.

V. CONCLUSION AND FUTURE SCOPE

In this paper, the method proposed is to solve problem in video steganography that is transfer is secure and here least significant bit steganography technique is applied where data is hiding in cover video frames. If video is tampered than hidden message does not get lost and thus purpose of research help in future for security.

The proposed method provides acceptable image quality with very little distortion in the image. It can embed corrective audio or image data in case corruption occurs due to poor connection or transmission. The proposed system is the high secured system using steganography and stegnography is tested by taking message and hiding them in some images of different sizes. The results that are obtained from these experiments are recorded.

Future Work may be further enhancement of results by applying some other algorithm than used in this thesis.

ACKNOWLEDGMENT

Thanks to my Guide and family member who always support, help and guide me during my dissertation. Special thanks to my father who always support my innovative ideas.

REFERENCES

[1] Ki-Hyun Jung & Kee-Young Yoo; “Steganographic method based on interpolation and LSB substitution of digital images”, Multimedia Tools Application: Springer Science Business Media New York 2014.

[2] Bhautmage P, Jayakumar A, Dahatonde A, “Advanced Video Steganography Algorithm” International Journal of Engineering Research, pp.1641-1644, Vol. (1), 2013.

[3] Sidham Abhilash, S M Shamseerdaula; “A Novel Lossless Robust Reversible Watermarking Method for Copyright Protection of Images”; al Int. Journal of Engineering Research and Applications , Vol. 3(6), Nov-Dec 2013.

[4] Yadav Pooja Mishra, Nishchol Sharma, Sanjeev; "A secure video steganography with encryption based on LSB technique”, Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference Dec. 2013. Doi: 10.1109/ICCIC.2013.6724212.

[5] Tao Zhang, Wenxiang Li, Yan Zhang, Xijian Ping; "Detection of LSB matching steganography based on distribution of pixel differences in natural images”, Image Analysis and Signal Processing (IASP), 2010 International Conference on , vol., no., pp.548,552, 9-11 April 2010, Doi: 10.1109/IASP.2010.5476056.

[6] Balaji R., Naveen G.;”Secure data transmission using video Steganography,” Electro/Information technology (EIT), IEEE International conference on, May 2011, and Doi: 10.1109/EIT.2011.5978601

[7] Moon S.K & Raut R.D; "Analysis of secured video steganography using computer forensics technique for enhances data security," Image Information Processing (ICIIP)”, 2013 IEEE Second International Conference on, volume no pp.660, 665, 9-11 Dec. 2013. Doi: 10.1109/ICIIP.2013.6707677.

[8] Jung KH & Yoo KY “Data hiding using edge detector for scalable images”, Multimedia Tools and Applications, 2013, Doi: 10.1007/s11042-012-1293-84.

[9] Lee CF, Huang YL “An efficient image interpolation increasing payload in reversible data hiding”, Expert System Applications 39:6712–6719, 2012.

[10] Lee YP, Lee JC, Chen WK, Chang KC, Su IJ, Chang CP “High-payload image hiding with quality recovery using tri-way pixel-value differencing”, Information Sciences 191:214–225, 2012.

[11] Lehmann TM, Gonner C, Spitzer K “Survey: interpolation methods in medical image processing”, IEEE Trans Med Imaging 18(11):1049–1075, 1999.

[12] Mielikainen J “LSB matching revisited”, IEEE Signal Processing Letters 13:285–287, 2006.

[13] Ni Z, Shi YQ, Ansari N, Su W “Reversible data hiding”, Circ System for Video Technology IEE 16:354–362, 2006.

[14] Swanson M, Kobayashi M, Tewfik A “Multimedia data embedding and watermarking technologies”, Proc IEEE 86(6):1064–1087, 1998.

[15] Thien CC, Lin JC “A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function” Pattern Recognition, 36:2876–2881, 2003.

[16] Vleeschouwer C, Delaigle JF, Macq B “Circular interpretation on histogram for reversible watermarking”, IEEE IMSP Workshop, 345–350, 2001.

[17] Wang XT, Chang CC, Nguyen TS, Li MC “Reversible data hiding for high quality images exploiting interpolation and direction order mechanism”, Digital Signal Process 23:569–577, 2013.

[18] Wang RZ, Lin CF, Lin JC (2001) Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognition 34(3):671–683

[19] Wu NI, Wu KC, Wang CM “Exploring pixel-value differencing and base decomposition for low distortion data embedding”, Applications Software Computer 12:942–960, 2012

[20] Xuan G, Zhu J, Chen J, Shi YQ, Ni Z, Su W “Distortionless data hiding based on integer wavelet transform”, IEEE Electronics Letters 38:1646–1648 , 2002.

[21] Zeng XT, Li Z, Ping LD “Reversible data hiding scheme using reference pixel and multi-layer embedding”, Inter J Electron Communication 66:532–539, 2012