Volume 5, Issue 12, December 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Novel Video Steganography Technique

Pooja Shinde
Student, SRIST
RGPV, Bhopal, India

Tasneem Bano Rehman
Faculty, SRIST
RGPV, Bhopal, India

Abstract: ***This paper describes the method for hiding data in a secure manner. The technique used for this purpose is Steganography. Here Video is used as medium for carrying secret messages. Video Steganography is a method for hiding data in a video file. A Novel Video Steganography technique has been proposed in this paper, which can be used with multiple types of cover format(.mov,.mts,.flv,.mpeg). The secret message also can be of any type like text, audio, video and image. The security is achieved by combining encryption, compression and Embedding technique altogether. The problem with existing video steganography technique is that they have work only on .AVI files and only single data format i.e. text or image. After studying the literature related to steganography it is observed that the techniques/methods available for Video Steganography lack support for versatility with respect to its cover file format and data file format. The amount of data the cover file can carry is also limited and security layers are not added effectively which results in insecure communication.***

Keywords: Huffman encoding, Advanced Encryption Standard (AES), Hash based LSB, RedGreenBlue(RGB), Least significant Bit(LSB)

I. INTRODUCTION

Steganography is an ancient art of conveying messages in a secret way in which only the receiver knows the existence of message. The word steganography derives from the Greek word "steganos", which means covered or secret, and "graphy" which means writing or drawing[1]. The concept of steganography is present from thousands of year. The Greek's used it to pass secret information by writing in wax-covered tablets: wax was first scraped off a tablet, the secret message was written on the tablet, and then the tablet was covered again with the wax. Another technique was to shave a messenger's head, tattoo a message or image on the bald head, and let the hair grow again so that the tattoo could not be seen. Shaving the head again revealed the tattoo[1]. The use of invisible ink was also used extensively during the World War II. The invisible ink method and other traditional steganography methods were extensively used. Then the image files were used to hide messages. Over the past few years, numerous Steganography techniques with hidden messages in multimedia objects have been proposed[1] This is largely due to the fact that multimedia objects often have a highly redundant representation, which usually permits the addition of significantly large amount of data.
The basic framework of the steganography is given in figure1.1:

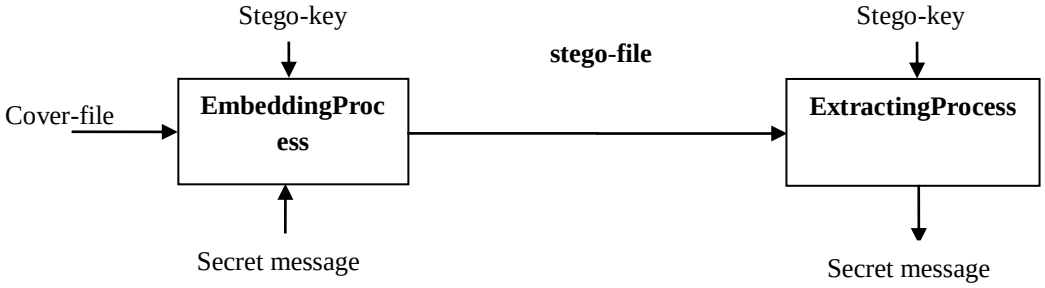

Figure 1.1. Steganographic Model

This model consists of two main processes, namely the *embedding process* and the *extracting process*. The main function of the embedding process is to hide the secret message, called *embedded message*, in a given cover, called *cover-file*. In hidden communication techniques, the cover file is not more than an innocent piece of information that is used to hide the secret information. A secret key, called *stego-key* is used in the embedding process such that it makes the embedded message computationally infeasible to extract without possessing this key. The output of the embedding process is called *stego-file*, which is the original file holding the hidden secret message. This output becomes, at the other end, the input of the extracting process, in which the embedded message is extracted from the stego-file to complete the hidden communication process. Since the stego-key is used in the embedding process, it needs to be used in the extracting process[2].

Features of Steganography
The features of steganography which makes it favorable for data hiding are given below[2]:

a) **Imperceptibility:** The video with data and original data source should be perceptually identical.
b) **Robustness**: The embedded data should survive any processing operation the host signal goes through and preserve its fidelity.
c) **Capacity**: Maximum data embedding rate.
d) **Secrecy**: Extraction of hidden information from the video must not happen without prior permission of intended user having password.
e) **Accuracy**: The extraction of the hidden data from the medium should be accurate and reliable.

The cover for steganography can be image, text, audio and video. Image is the most familiar cover, but the limited size of image will inevitably restrict the capacity of embedding. Whenever it is required to transmit large amount of secret messages, steganography in image will not satisfy the demand. So steganographic method that has higher embedding capacity needs to be applied. Because digital video is composed of series of frames and has greater signal space, steganography in video will have larger capacity for embedding. Furthermore, with the development of multimedia and stream media on the Internet, transmitting video on the Internet will not incur suspicion. Besides this, the degradation of video quality cannot be observed by naked eyes, it may be occur by video compression of lower quality. These reasons make it possible to securely hide data in video.

Higher the quality of video, the more redundant bits are available for hiding. By using lossless steganography techniques, messages can be sent and received securely. Traditionally, steganography was based on hiding secret information in image files. But modern work suggests that there has been growing interest among research fraternity in applying steganographic techniques to video files. The advantage of using video files in hiding information is the added security against the attack of hacker due to the relative complex structure of video compared to image files. Application of Steganography varies from military, industrial applications to copyright and Intellectual Property Rights (IPR), data authentication.

The problem with existing video steganography technique is that they have work only on .AVI files and only single data format i.e. text or image. The challenge is to develop an algorithm which will facilitate the usage of any video format(flv,mts,mpeg,mov) as the cover and versatile data format(text, image, audio, video) as secret message. After studying the literature related to steganography it is observed that the techniques/methods available for Video Steganography lack support for versatility with respect to its cover file format and data file format. The amount of data the cover file can carry is also limited and security layers are not added effectively which results in insecure communication.

II. LITERATURE REVIEW

B.SUNEETHA et. al has proposed in his work Cryptography and Steganography together system based on hiding data in video by encrypting it with ASCII code and provides a additional layer of security to existing system. Cryptography provides privacy whereas Steganography is intended to provide secrecy[2].

Kousik Dasgupta, J.K. Mandal and Paramartha Dutta has proposed a secured hash based LSB technique for video steganography uses cover video files in spatial domain to hide the presence of sensitive data regardless of its format. Performance analysis of the hash based LSB technique after comparison with LSB technique is quite better[3].

A. Swathi , Dr. S.A.K Jilani has proposed in his paper the LSB substitution using polynomial equation is developed to hide the information in specific frames of the video and in specific location of the frame by LSB substitution using polynomial equation. Here the information will be embedded based on the key. Key is in the form of polynomial equations with different coefficients. By using this the capacity of embedding bits into the cover image can be increased[4].

Mritha Ramalingam in his proposed work has given More secured LSB method a way in which video file is used as a host media to hide secret message without affecting the file structure and content of the video file. Because degradation in the video quality leads to visible change in the video which may lead to the failure of the objectives of Steganography[5] .

Ashawq T. Hashim et al has proposed a Hybrid Encryption and Steganography technique where there are two methods of hiding used, the first method is the Least Significant Bit (LSB) and the second is the Haar Wavelet Transform (HWT). This work is based on a combination of steganography and cryptography techniques to increase the level of security and to make the system more complex to be defeated by attackers[6].

R. Shanthakumari and Dr.S. Malliga in their proposed work has stated a LSB Matching Revisited algorithm (LSBMR) selects the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. LSBMR scheme addresses two problems Lack of Security and Low Embedding rate[7].

It is observed that the work done so far has limitation of single cover file format i.e. .avi files are mostly used, other formats are been neglected. The secret message which can be embedded in cover file is generally text or image, there is limitation of size the cover file can carry. Security is also one of the issue which is not taken into consideration while implementing steganography concept. The systems developed for steganography are not user friendly.

III. PROPOSED WORK

Video Steganography is the art of writing hidden messages inside videos, in such a way that no one apart from the sender and intended recipient realizes the existence of a hidden message. Steganography uses repeating portions of the Video files to embed the secret message. There are many techniques for hiding data in Video.

Proposed Algorithm-A Novel Video Steganography using Encryption and Compression[NVS]:

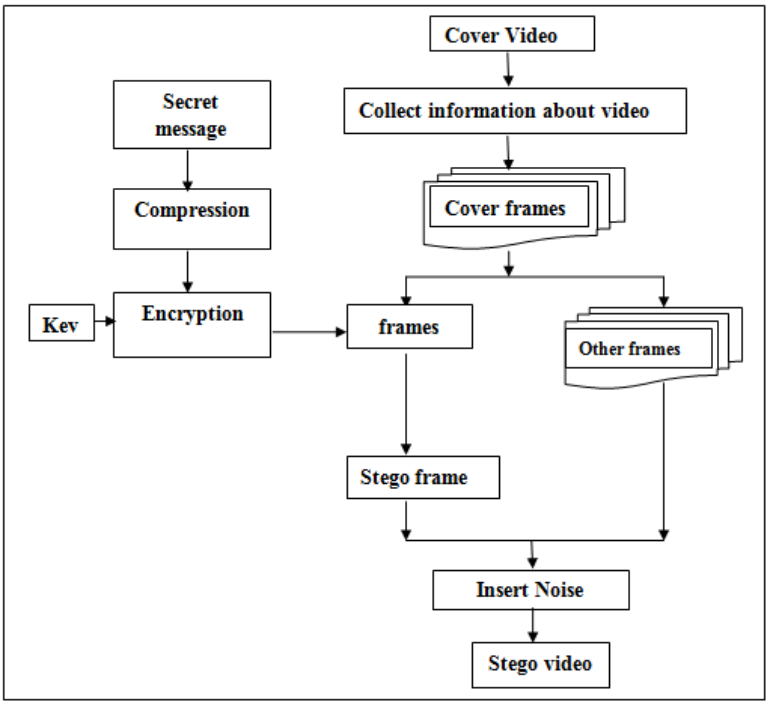

Figure 3.1 Block diagram for Encoding in Video

The NVS technique uses Video as the cover file, this video is divided into frames to find position of data insertion. As there are many frames in a video there is more chance of redundant bits to be found, where secret message can be embedded. This system is three times more secure than the existing system (HLSB) as three levels of security is added. The first is using Compression technique which is Huffman coding for compressing the secret message which can be text, audio, image or video. Compression increases the embedding capacity of data and intruder cannot guess that compression is been used, if he detects compression he may not be able to know which compression technique is been used. Then next level of security is provided by the use of Encryption algorithm which is AES +256 shift. This again is enhanced by using a password as a key for AES. Next level of security is provided by embedding noise in the stego video due to which it would be difficult to recognize message bits and noise bits.

Algorithm for Novel Video Steganography (NVS):

The Algorithm for Novel Video Steganography (NVS) is given below:

a) Input Video file.
b) Read required info from video & break it into frames .
c) Input secret message in the form of text, or audio, or image, or video.
d) If Compression of the secret message is required use Huffman encoding.
e) Encrypt the secret message using AES algorithm+256 bits shift operation.
f) Find position of insertion of bits using HLSB technique.
g) Combine frames and insert some noise.
h) Regenerate video frames.

The process of encoding can be illustrated using figure3.7:

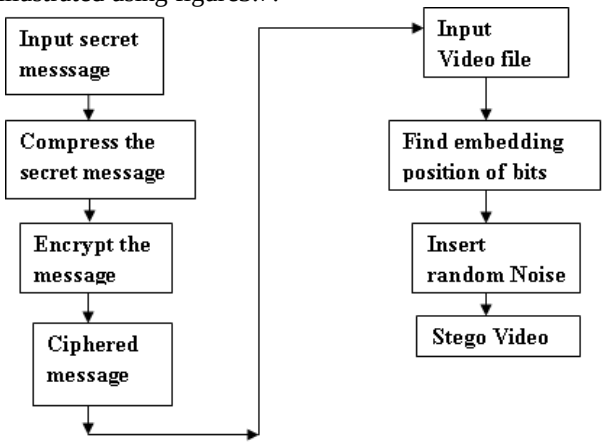

Figure 3.7. Encoding using NVS technique.

Algorithm for Novel Video DeSteganography is given below

a) Input Stego-Video file.
b) Read required info from video.
c) Remove random bits in the form of noise.
d) Break the videos in frames and find the position of inserted bits using HLSB technique.
e) Collect the bits and Decrypt the collected bits using reverse AES algorithm with Key(password).
f) Decompress the secret message if compression is done.
g) Reconstruct the secret message.
h) Display the secret message.

The decoding process can be illustrated using the figure3.8 :

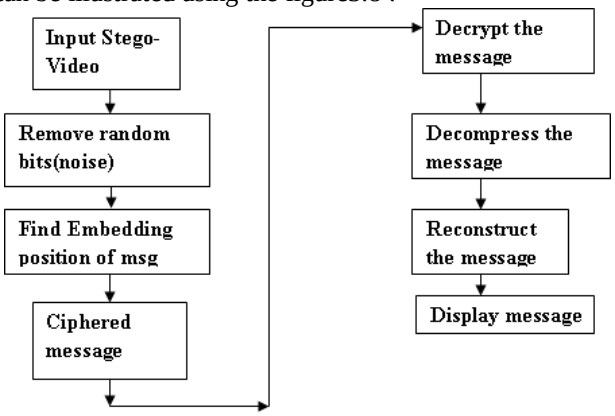

Figure 3.8.Decoding using NVS Technique

Features of Novel Video Steganography (NVS)

The features of NVS are given below:

a) Secure

Since random data are also placed in unused frames in the video, the attacker is left clueless to know the real secret data hidden in the video. Hence highly confidential data like military secrets and bank account details can be easily steganography in ordinary video and can be transmitted over internet even in unsecured connection.

b) Capacity

Text based steganography has limited capacity and Image steganography tried to improve the capacity where 50% of original image size can be used to hide the secret message. But there is limitation on how much information can be hidden into an image. Video Steganography has overcome this problem.

c) Imperceptibility

It is less imperceptible because of quick display of the frames. It becomes harder to be detected by human perception system.

d) Video error correction

Since the transmission of any data is always subject to corruption due to errors, then the video transmission must deal with these errors without retransmission of corrupted data. This is another application for steganography rather than security purpose.

e) Different file format

The NVS can be used with multiple cover file format(.mpeg,.mov,.flv,.mts)and data format(text,image,audio,video).

IV. IMPLEMENTATION AND RESULT ANALYSIS

In video there are frames, these frames are defined by frame rate. Frame rate is the number of still pictures per unit of time of video the ranges from six or eight frames per second (frame/s).The size of a video image is measured in pixels for digital video, horizontal scan lines and vertical lines of resolution for analog video. Aspect ratio describes the dimensions of video screens and video picture elements. All popular video formats are rectilinear, and so can be described by a ratio between width and height. Video quality can be measured with formal metrics like PSNR.

The simulation environment is created using Java7.0 as IDE and the results are calculated using MSU tool. The application of proposed algorithm with test video Sample.avi is given in following table. It is observed that after desteganography secret message is obtained without any loss or noise. The original video and stego video are analyzed using Peak Signal to Noise ratio. The Mean Square Error of two video is equal to Zero which means they are identical.

MSU for Analyzing

The results obtained for NVS are calculated using a tool which is MSU Video Quality Measurement Tool(VQMT). The parameters on which results are compared are calculated using MSU tool. Generally, a video is compared based on certain parameters like the PSNR, MSE, Payload, Blurring effect, etc. The video is large and contains 1000s of frames, so these parameters cannot be calculated manually. Therefore there is a need of readymade tool which can calculate/compare two video on certain criteria. The tool used for NVS as simulator is MSU tool.

In NVS, there is a cover file which is video and message file can be text, image audio, video. Video files are available in different formats like flv, avi, mpeg, mts, etc.. Thus, to calculate the results there is need of some sample files. These sample files with their properties are listed below in Base table. The Base table given below gives the details of cover video files and various secret message file format used while presenting the results. The details of each file is given along with their name, resolution, frames, etc.. the secret message is of the form text(sample.txt), image(peacock.jpg), audio (1elevator.wav), video.

Table 4.1.Base Table

Sr.No.	Name of file	Resolution	Frames/sec	No. of Frames
1	Sample1.avi	360*240	30	45
2	Sample2.flv	360*240	30	78
3	Sample3.mpeg	320*240	25	
4	Drop.avi	256*240	30	182
5	Flame.avi	256*240	30	294
6	Sample.txt	4.54kb		
7	1elevator.wav	121kb		
8	Peacock.jpg	234*300		

Performance Metrics

The performance of NVS is calculated using the following three parameters:

MEAN SQUARE ERROR (MSE)

MSE measures the average of the squares of the "errors". The average squared difference between an original image and resultant (stego) image is called Mean Squared Error[10]

where,

H and W=Height and Width

P (i, j) =Original Frame

S (i, j) =Corresponding Stego frame.

PEAK SIGNAL TO NOISE RATIO (PSNR)

PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise. PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure of quality of reconstruction of lossy compression PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases the reverse may be true. One has to be extremely careful with the range of validity of this metric. It is only conclusively valid when it is used to compare results from the same content. PSNR is most easily defined via the mean squared error (MSE)[10].

Where,

L - Maximum intensity it is taken as 255

MSE - mean squared error

Typical values for the PSNR is 30 to 50 dB, where higher is better.

Payload

Maximum payload is bits per byte [10]i.e. maximum amount of data that can be embedded into the cover file without losing the quality of the original file.

Analysis

The algorithm stated in literature review are compared with NVS based on Steganography features and a table of analysis is given in figure 4.2:

Table 4.2.Steganographic Features Analysis

Features	SDT	HLSB	LSB POLY	MLSB	HES	LSBMR	NVS
1.Imperceptible	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.Robust	Robust	Robust	Less Robust	Robust	Robust	Robust	Robust
3.Capacity	Better	Good	Low	Good	High	High	High
4.Secure	Less Secure	Less Secure	Less Secure	Secure	Secure	Secure	Highly Secure
5.Cover file	AVI	AVI	AVI	AVI	AVI	AVI	.flv, .mts, .avi, .mov, .mpeg
6.Secret message	Image	Image	Text	Text	Text	Text	Text, Image, Audio, Video

In the Secured Data Transmission (SDT) the cover file is Bulb.avi with resolution 256*240 ,15 frames per second, total frames are 80 is taken as input. In HLSB the cover file is Drop.avi with resolution 256*240, 30 frames per second, total frames are 182 is taken as reference video. In LSB Polynomial equation Algorithm, cover file is Drop.avi with resolution 256*240, 30 frames per second, total frames are 182 is taken as reference. In MLSB Algorithm, cover file is Globe.avi with resolution 320*240, 30 frames per second, total frames are 107 is taken as input video. In Hybrid Encryption and Steganography(HES), cover file is Globe.avi with resolution 320*240 , 30 frames per second, total frames are 107 is taken as input. In LSBMR, cover file is Rhinos.avi with resolution 320*240, 15 frames per second, total frames are 105 is taken as reference. For these parameter the PSNR and MSE are calculated.
The Comparison is given based on the results related in each steganography technique.

Table 4.3.Comparison of SDT, HLSB, LSBPoly algorithm based on MSE , PSNR , Payload.

Algorithm	**Video Filename**	**Resolution**	**MSE**	**PSNR**	**Payload (text)**
1.SDT	Bulb.avi	256*240	9.51	38.71	199Kb
2.HLSB	Drop.avi	256*240	0.34	44.34	2.66Kb
3.LSB Poly	Drop.avi	256*240	0.42	48.56	1Kb

Table 4.4.Comparison of MLSB, HES, LSBMR algorithm based on MSE, PSNR, Payload.

Algorithm	**Video Filename**	**Resolution**	**MSE**	**PSNR**	**Payload (image)**
4.MLSB	Globe.avi	320*240	0.295	53.43	13.3Kb
5.HES	Globe.avi	320*240	0.46	51.43	13.3Kb
6.LSBMR	Rhinos.avi	320*240	0.00065	80	136bits

The larger the PSNR dB value, higher is the image quality i.e. there is a little difference in the original image and stego image. Therefore PSNR should be large. Small PSNR means there is distortion between original and stego image. MSE is the average of squares of the errors. If MSE = infinity then, two images are identical. It is required that the PSNR should be high and MSE must be less for an Video Steganography algorithm to be effective. The table4.5 given below states that NVS technique is applicable for any type of cover video file format. Here only three formats are been displayed but it can work with many other formats also like .mts, .mov, etc in table 4.5.

Table 4.5.Results with NVS for different carrier file format.

Carrier Video File	PSNR	MSE
Sample1.avi	100	0
Sample2.flv	100	0
Sample3.mpeg	21.13	0.50
Sample4.mov	100	0
Sample5.mts	100	0

Comparison
The comparison of proposed NVS is done with Least Significant Bit technique proposed in [14] and Hash based Least Significant Bit technique proposed in [13] w.r.t. PSNR and MSE metrics.

Comparison of NVS with LSB:
Here NVS technique is compared with LSB method which is proposed in[14]. The results generated by these two schemes are analyzed using PSNR and MSE parameters. The results are calculated using a "MSU video quality Measurement tool". In this tool the cover video and stego video are given as input to calculate PSNR and MSE. The results generated for Sample2.flv (cover video) with Sample.txt (secret message) is given in table4.6:

Table 4.6.Results obtained with Secret text file embedded in Video (NVS & LSB)

Stego Video with Text secret message	**Results with NVS**		**Results with LSB**	
	PSNR	**MSE**	**PSNR**	**MSE**
Sample2.flv	100	0	48.19	0.32

Comparison of NVS with HLSB:
Similarly, the parameters are calculated using MSU tool with cover video(drop.avi) and secret file(peacock.jpg) is given below. Here comparison of NVS is done with HLSB technique is done w.r.t. PSNR and MSE metric. The table 4.7 shows the results generated.

Table 4.7.Results obtained with Secret image file embedded in Video (NVS and HLSB)

Stego Video secret image message	**Results with NVS**		**Results with HLSB**	
	PSNR	**MSE**	**PSNR**	**MSE**
Drop.avi	100	0	44.34	0.34
Flame.avi	100	0	42.66	0.30

The comparison of NVS with HLSB shows that NVS has outperformed w.r.t. Peak Signal to Noise Ratio(PSNR) and Mean Square Error(MSE). It is expected that PSNR should be High and MSE should be Low. Here for NVS, PSNR is approximately 60% higher than HLSB, MSE is lower by 30%. The added feature of NVS is high embedding capacity.

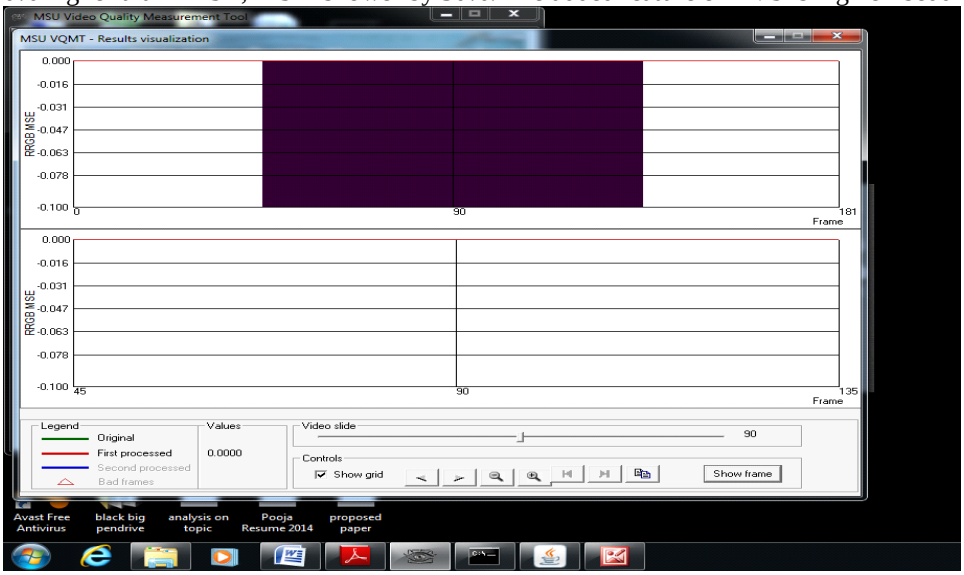

Figure 4.11.Graph for results obtained in NVS with MSE=0

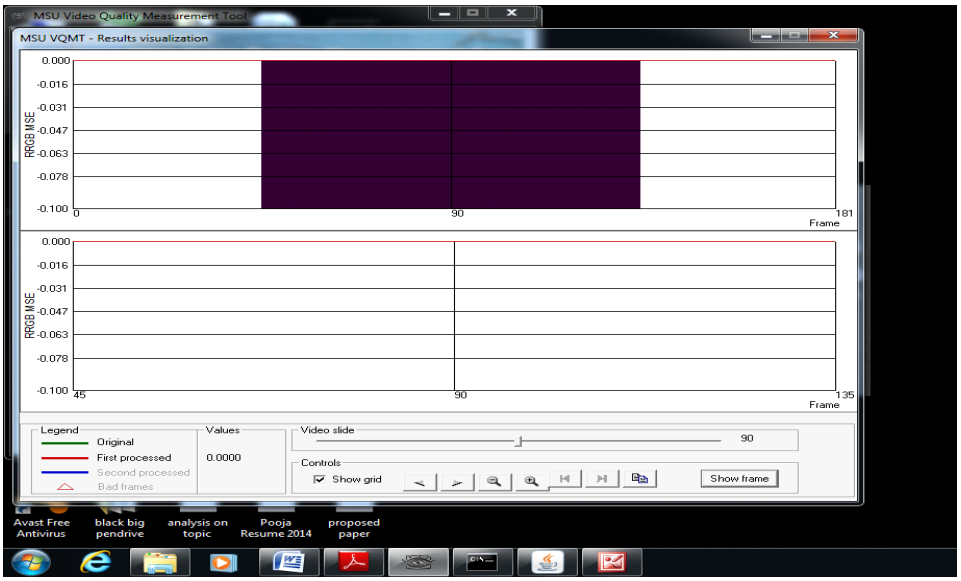

Figure 4.12.Graph for results obtained in NVS with PSNR =100

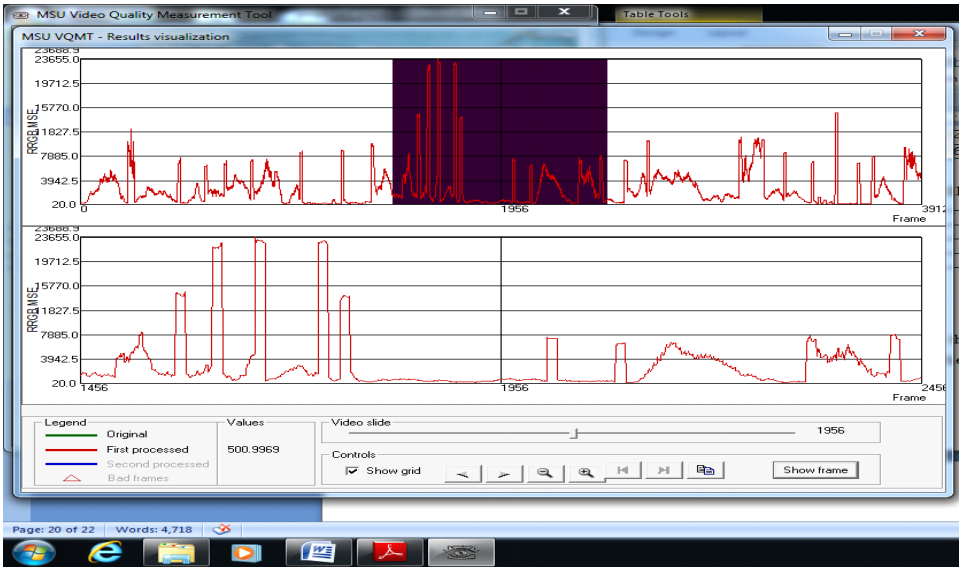

Figure4.13. Graph for mpeg video cover with MSE=500.99

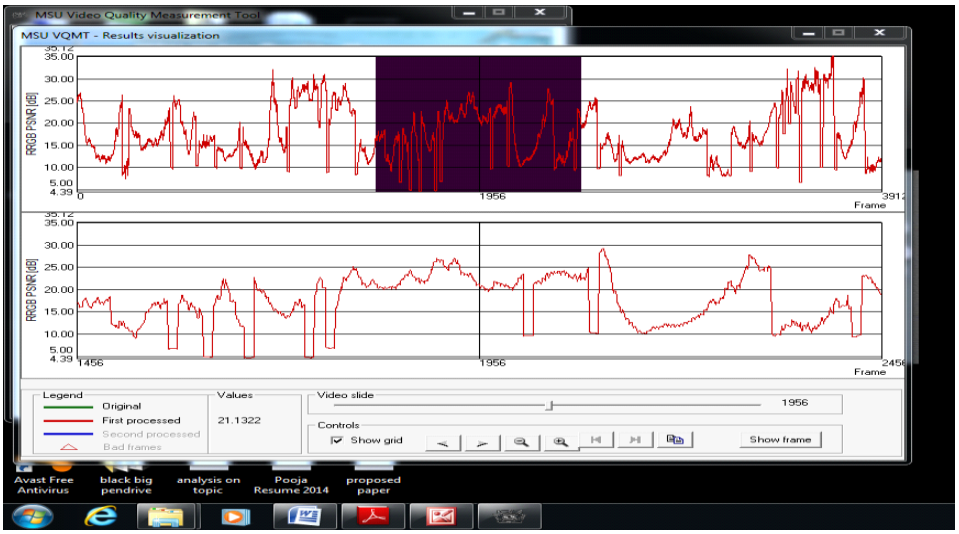

Figure4.14.Graph for mpeg video cover which has PSNR=21.13

V. CONCLUSION AND FUTURE SCOPE

A Novel Video Steganography technique has been presented in this thesis. With the aim of solving the problems like versatility, low embedding rate, security issues NVS technique has proved to be a better solution for Video Steganography. Performance analysis of the NVS with HLSB[13] and LSB[14] w.r.t.Peak Signal to Noise Ratio(PSNR) is high(approx.60%) and Mean Square Error (MSE) ratio is low(30%) which states that NVS is better than HLSB and LSB. In HLSB only avi files were used as cover whereas in the proposed technique different cover file formats can be used. The secret data that was used earlier was image, here NVS can use versatile data file format ranging from text to video. Although any type(text,image,audio,video) of data was embedded in the cover there is only slight change in size of stego video. The video quality is not compromised in steganography process. Thus NVS outperformed than existing techniques.

Future Work

In future, it is expected that the idea can be extended by embedding the text in the different frames of same video. Since the video consists of many number of frames, the text can be embedded in many methods like embedding in the consecutive frames based on the key, in the frames with the sequence number of multiples of key, in the frames with the sequence number of powers of key, etc., thereby providing a technique to embed large amount of data with additional security and making it difficult for the steganalysers to detect the secret data. Multiple frames embedding is possible. Now we are embedding in a single frame at a time, but in future multiple frames embedding is also possible.

The Proposed system is used to embed text, image, audio, video type of secret message files further it can be extended to be used with pdf, .exe, ppt, xls, etc files.

ACKNOWLEDGMENT

With great pleasure and deep sense of gratitude, I take this opportunity to express my sense of indebtedness to my HOD Prateek Gupta Sir , my guide Tasneem Bano Rehman and last but not least Dept. of Computer Science & Engineering, SRIST, Jabalpur for thier erudite guidance, affectionate encouragement and whole hearted involvement in my dissertation, without which it would have been difficult for me to complete this work. Finally, I am highly obliged to all my family members for their support and blessings.

REFERENCES

[1] POOJA SHINDE, TASNEEM BANO REHMAN "A SURVEY : VIDEO STEGANOGRAPHY TECHNIQUES"International Journal of Engineering Research and General Science Volume 1, Issue 1, August 2015 ISSN 2091-2730

[2] Sharone Gorla Report, "Combination of Cryptography and steganography for Secure communication in Video file" , California State University, Sacremento

[3] B.Sunetha,Hima Bindu & S.Sarath Chandra "Secured Data Transmission Based Video Steganography" International Journal of Mechanical and Production Engineering (IJMPE) ISSN No.: 2315-4489, Vol-2, Iss-1, 2013

[4] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta," Hash based Least Significant Bit Technique", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012

[5] A. Swathi, Dr. S.A.K Jilani,, "Video Steganography by LSB Substitution Using Different Polynomial national Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5

[6] Mritha Ramalingam: Stego Machine – Video Steganography using Modified LSB Algorithm World Academy of Science, Engineering and Technology Vol:50 2011-02-26

[7] Ashawq T. Hashim*, Dr.Yossra H. Ali** & Susan S. Ghazoul*" Developed Method of Information Hiding in Video AVI File Based on Hybrid Encryption and Steganography" Engg.and tech journal, vol 29,No.2,2011.

[8] R. Shanthakumari1 and Dr.S. Malliga, "Video Steganography Using LSB Matching Revisited Algorithm", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. IV(Nov – Dec. 2014), PP 01-06

[9] J. Jayaseelan and B. Kruthika," Noise Secures Secret Data! By Act as a Reference For Embedding", ICTACT Journal On Communication Technology, March 2014, Volume: 05, ISSUE: 01 ISSN: 2229-6948

[10] Sharma V. and kumar S. "A new approach to hide text in image using Steganography*" International journal of advanced research in computer science and software engineering* vol.3, issue 4, 2013.

[11] Steffy jenifer K. and Yogaraj G., "LSB approach for video Steganography to embed images" *International journal of computer science and information technology* vol.5 (1), 2014

[12] D. P. Gaikwad and Dr. S.J. Wagh, "Color Image Restoration for Effective Steganography", i-manager's Journal on Software Engineering, Vol. 4 l No. 3 l January - March 2010 65,pp.65-71

[13] ShengDun Hu, KinTak U," A Novel Video Steganography based on Non-uniform Rectangular Partition", EE International Conference on Computational Science and Engineering CSE/I-SPAN/IUCC 2011

[14] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav" Steganography Using Least Signicant Bit Algorithm", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp. 338-341

[15] S. Suma Christal Mary M.E (Ph.D)" Improved Protection In Video Steganography Used Compressed Video Bitstream", International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 764-766

[16] A.K. Bhaumik, M. Choi, R.J. Robles and M.O. Balitanas, Data Hiding in Video in International Journal of Database Theory and Application Vol. 2, No. 2, pp. 9-16, June 2009.

[17] Pritish Bhautmage, Prof. Amutha Jeyakumar, Ashish Dahatonde, " Advanced Video Steganography Algorithm", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 1, January -February 2013, pp.1641-1644

[18] M. Abomhara, Omar Zakaria, Othman O. Khalifa, "An Overview of Video Encryption Techniques", International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010 1793-8201.

[19] Prof. D P Gaikwad, Trupti Jagdale, Swati Dhanokar, Abhijeet Moghe, Akash Pathak," Hiding the Text and Image Message of Variable Size Using Encryption and Compression Algorithms in Video Steganography", International Journal of Engineering Research and Applications (IJERA)ISSN: 2248-9622.

[20] Mozo AJ., and Obien M.E., C.J. Rigor, "Video Steganography using Flash Video (FLV)" *I2MTC 2009 - International Instrumentation and Measurement Technology Conference Singapore*, 5-7 May 2009. [14]

[21] Hussein A. Aly *",* Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error*" IEEE transactions on information forensics and security*, vol. 6, no. 1, march 2011.

[22] Attallah M. and AI- shatnawi, "A new method in image steganography with improved image quality" *Applied mathematics sciences*, vol.6, 2012.

[23] Bodhak V. and Gunjal L., "Improved protection in video Steganography using DCT & LSB" *international journal of engineering and innovative technology (IJEIT)* vol. 1, issue 4, April 2012.

[24] Sunil. K. Moon, "Analysis of secured video Steganography using computer forensics techniques for enhances data security" *IEEE second international conference on image information processing* (ICIIP-2013).

[25] Tasdemir K. and Kurugollu F., "Video steganalysis of LSB based motion vector steganography" *International Conference on Communication Systems and Network Technologies* 2010.

[26] Kumar A, Sharma R, "A secure image Steganography based on RSA algorithm and Hash-LSB technique " *International journal of advanced research in computer science and software engineering vol.3,issue 4*, 2013vol.3, issue 7, July 2013.

