Analysis and Synthesis of Secure Image Using Stegnography,Cryptographyand WatermarkingTechniques

Rupesh Gupta[#1], Dr.Tanupreet Singh[#2]

[#]*Computer Science and Engg. Department*
ACET Amritsar, PTU Jalandhar, India
[1]gupta_rupesh_mani@yahoo.co.in
[2]tanupreet.singh@gmail.com

***Abstract*–In today's world lots of data security and data hiding algorithms have been developed to overcome the security issues which mostly arise in last decade; which is the key motivation for our research work. In this paper named "Stegnography& Cryptography with Watermarking Techniques are used" we have designed a system that will make a normal user to securely transfer text messages by hiding them in a digital image file using the local characteristics within an image. This paper is a combination of Stegnography and cryptography algorithms with watermarking; which provides a strong pillar for its security. While image processing perceivable distortion occurs and to limit this a system is proposed which hides data with in an image. This research paper has an advantage because the hidden text is in the form of images; which are not obvious text information carriers over other information security paper**

***Keywords*— Stegnography, Cryptography, watermarking, Security, Data hiding and Image Processing**

I. INTRODUCTION

In simple words, Stegnography is stated as traps and tricks of invisible communication which is accomplished through hiding information in other material; thus hiding the existence of the talked information. By combing cryptography and watermarking the strength of Stegnography can be amplified. However all digital file formats is used for Stegnography, but the formats which are most suitable are those which are having high degree of redundancy and the bits of an object that provide accuracy for the object's use and display is called as redundancy. Therefore redundant bits of an object are those bits that can be altered without the variation being detected easily. In our research some other file formats are uncovered for data hiding with respect to audio and image file. In digital presentation large amount of redundant bits are present especially on the digital image which are present on internet;[1][7]. Different image file format exists in the domain of digital images most of them for specific applications and these different steganography algorithms exist. JPEG file format is most favourite file format on the Internet; because of its size of the image.

Steganography and cryptography are much related to each other. It is difficult to understand the encrypted message by cryptography. Whereas there must be no knowledge of the message is made sure by the stegnography. Here we will make comparison between the plain text and the portion of the cipher text the cryptography; comparison is made between portions of the plaintext and portions of the cipher text. Stegnography is compared with in three media and these are cover-media; stegno-media; and potion of some message. Hence we get cryptography as a cipher text and stegnography as a stego-media [4]. The text/message in stegnography might or might not be encoded. And if it is encrypted then a cryptanalysis technique is utilized to withdraw the message. For achieving ultimate results we can combine cryptography and steganography. Encrypted data is most difficult to distinguish from obviously occurring phenomena than plain text is in the carrier medium. So, we have many tools by using which we can hide data before hiding it in the selected medium. And in some circumstances; sending a hide information will across suspicion while undetectable information will not do so. Here two methods are combined to produce healthier guard of the message. If in case, the Stegnography flops and the message can be identified; it will be of no usage as it is encrypted using cryptography methods [2][6].

This paper is organized as follows. Section II gives detail about Stegnography. In section III, Cryptography is presented. Watermarking is discussed in Section IV. In Section V gives view about discrete watermarking transform& Section VI presents the results. The conclusion used is described in Section VII.

II STEGNOGRAPHY

Steganography is the science of hiding information. The aim of steganography is to encrypt the data from a third party. In this article, we discuss what Steganography is and what purposes it serves [21].

Therefore below formula gives a generic description of the pieces of the Stegnography process:

Cover medium + hiddendata+stegokey = stegomedium

In this process the cover medium is the case in which we will hide data. Which may also be done using the stego key then

the result file is the stego medium. The cover medium (or, stego medium) is characteristically image or audio files. Here; we will concentrate on image files that will be referred to the cover image and stego image. Least significant bit insertion is an informal approach of hiding information within an image is called least significant bit (LSB) insertion [22]. Here we can take the binary significance of the encrypt data and overwrite the LSB of every byte within the cover image. And if here use 24-bit shade the amount of change will be minimum and imperceptible to the human eye [4][11][12].

III CRYTOGRAPHY

Cryptography is a technique to change the data into a jumbled code which could be interpreted and mailed across as public and private networks. It uses two main classes or methods of hiding data; symmetrical and asymmetrical. The symmetric encryptions or procedures use the same key for encryption as well as for the decryption. The other titles for this method of encryption are secret-key; shared-key; and private-key. Encryption key can be loosely related to the decryption key as it does not essentially need to be same copy. Symmetric cryptography is motivated to plain texture attacks and simpler cryptography means that they are hack capable and at times easy to decrypt. By good preparation of the coding and functions of this cryptographic system these coercions can be more reduced [17]. And asymmetric cryptography uses other encryption and decryption keys for encryption and decryption. This act on end user on a network private or public has a pair of keys one for encryption and one for decryption. Therefore these keys are considered or known as a public and private key in this case the private key can-not be derivative from the public key. Asymmetrical cryptography method has been verified to be safe in contrast to computational limited intruders. This safety is mathematical definitions depends upon the application of said hiding or encryption. And it necessary; asymmetric encryption is very calm as its applied use; this is defined by the technique in which the data is encrypted and for whatever use [5][17]. Thus asymmetrical encryption is in the application of sending messages where the sender encodes and the delivery party decodes the message by using a random key generated by the public key of the sender. Cryptography is the discipline of using arithmetic to encrypt and decrypt data. The Cryptography allows you to store complex information or communicate it across uncertain networks (like the Internet) so that it can-not be read by anybody [18].

Except the proposed recipient. The cryptography is the discipline of security data; cryptanalysis is the science of analysing and safe communication. And standard cryptography involves a stimulating mixture of analytical reasoning application of scientific tools pattern; patience; and determination. The Cryptology squeezes both cryptography and cryptanalysis. ‘There are two classes of cryptography in this domain: cryptography that will halt your younger one from understanding your files and cryptography that will stop major administrations from reading your files [19]. The Cryptography could be good or bad; as discuss overhead. The Cryptographic is restrained in the time and sources it would attain to cover the plaintext. Therefore result of strong cryptography is cipher text that is not very easy to decipher without possession of the proper decoding tool. Hence cryptographic procedure; or cipher; is a calculated function used in the encryption as well as decryption process. A cryptographic algorithm deals in combination with a key—a number; word or phrase—to encrypt the plaintext. Therefore same text encrypts with different keys to different cipher text. Hence security of hiding data is depends upon two things: the cryptographic technique and the safety of the key [8][13]. Cryptographic technique, every key and protocol that make it work comprise a cryptosystem. In simple cryptography, also called symmetric-key encryption; one key is used both for encryption and decryption [20]. The Data Encryption Standard (DES) is an example of a conventional cryptosystem which is used by the government.

IV WATERMARKING

In recent years the art adding images; video; music audio and text documents is easier. The widespread and increase use of the World Wide Web digital forms of these media (still figures audio video texture) are easily access. It is easier to market and sell others works of art. This property threatens copyright protection. It is easy to copy the digital documents and to distribute them; allowing for pirating. Hence there is a lot of methods for protecting ownership and one of these is known as digital watermarking.

Digital watermarking is the technique of implanting a digital pattern or signal into digital content. Thus signal defined as a watermark can be used to know the ownership, authorize the content, and to unauthorized copies of the work. Thus Watermarks of changing degrees of evident are added to presentation media as an assurance of authenticity, ownership, quality, and source. Then particular; it must be transparent; and good. The Robust acquires that it be capable to survive any alteration or distortion that information may undergo adding calculated attacks to eliminate the watermark data; to make the data more efficient to store and transmit. Hence owner can still be identified. Then transparency attains a watermark to be observable so that it does not affect the quality of the material to make detectable and removal by pirates is less possible. Media of concentrate in paper is still image [10][12]. There are two main categories of image watermarking techniques and these are based on domain in which the watermark is created: the frequency domain (producing spectral watermarks) and the spatial domain (producing spatial watermarks)[16]. The effectiveness of a watermark technique is improved by known properties of the visual system of humans. Hence these are known as perceptually depended techniques of watermarking. In this category; the class of figure-adaptive watermarks finds most effective. Then in conclusion; figure watermarking methods which take benefit of possessions of the human video system; and the features of image create the most healthy and

transparent watermarks. The Digital watermarking is a skill for hiding various types of message in digital form. In general; signal of safe copy and finding the cogency of data is hided as a watermark.

A digital watermark belongs to digital knowledge or categories introduced into digital material. Then digital material could be a still image or an audio clip or a video clip or can be a text document or some form of digital information that the maker or possessor would like to protect. Then main reason of the watermark is to identify who is the owner of the digital data is but it can also identify the projected recipient [15][16].

V DISCRETE WAVELET TRANSFORM

DWT technique is used for digital figure. Many DWTs are present which are use depending on the requirements which gives proper answer which one should be used. The informal transform is haar transform. To encrypt text information integer wavelet transform (ITW) could be used. When DWT transform is applied to a figure it is disintegrated into 4 sub bands LL(Lower to Lower), HL(Higher to Lower), LH(Lower to Higher) and HH(Higher to Higher). LL part contains the most important features. So if the message is encrypt in LL part the stego figure can survive density or other manipulate. But sometimes loss may be shaped in the stego image and then some other sub bands can be utilized.

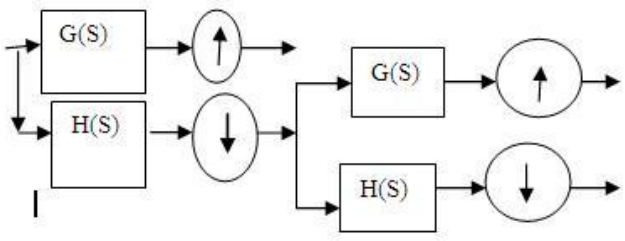

Figure 1: Multi-level Breakdown using low pass and high pass filters

Quantization's approaches is followed by our algorithm that divide the input figure in 4 filter factors as shown below, Further quantization act on previous step of window and low order filter. Quantization relies upon the highest numbers of decomposition levels to be entered are three for DWT. DWT exploits inter pixel redundancy to extract excellent un-correlation for natural images. Hence, all the transform coefficients without compromising coding efficiency can be encoded independently [10][14] adding to the DWT packs energy in the low frequency regions. Thus, part of the high frequency matter is removed without major quality loss. This type of quantization scheme causes further reduction in the entropy. At Last, it is finalized that high temporal correlation exhibits successive frames in a video transmission. This correlation is used in improving the coding efficiency. The above-mentioned characteristics of the DWT have headed to its wide spread development in virtually every figure/video processing classical of the last 10 years, for e.g., JPEG (classical), MPEG- 1, MPEG-2, MPEG-4, MPEG-4 FGS, H.261, H.263 and JVT (H.26L). However; the DWT still offers new research directions in the current and upcoming image/video coding standards [12].

VI RESULT AND DISCUSSION

The Figure 2 is the main GUI window which act as home window contains two buttons for adding watermark and stegnography on video and another for extracting it.

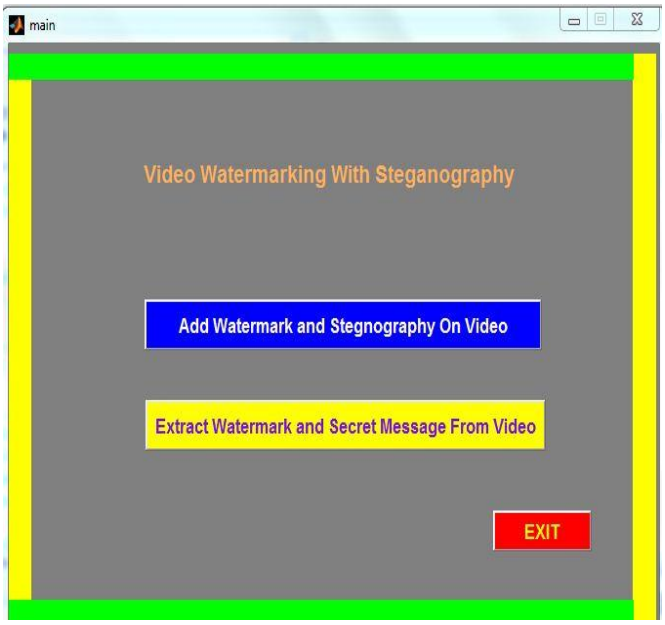

Figure 2: Opening GUI.

System is to provide Figure 3 is 2nd window that appears which is enabling user to load video of any format like Mpeg, Avi or Flv. After loading video it took approx. 5 sec to load and to creating frames of that video.

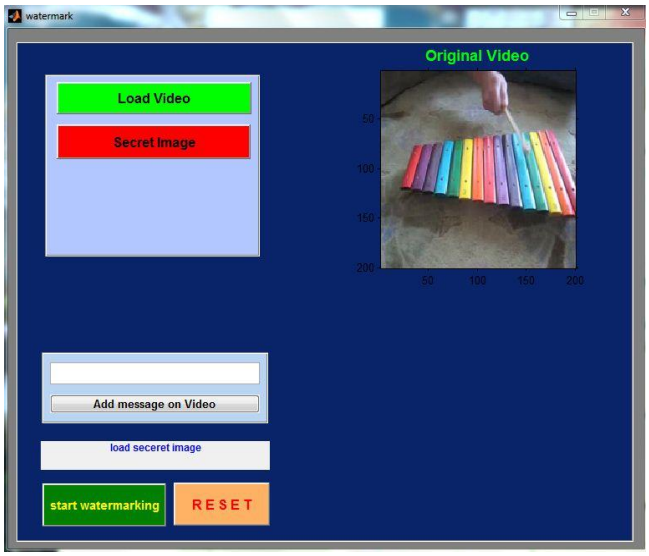

Figure 3: Input Video is loaded

Figure 4 is the screen shot after the video is loaded and the secret image is about to load in video

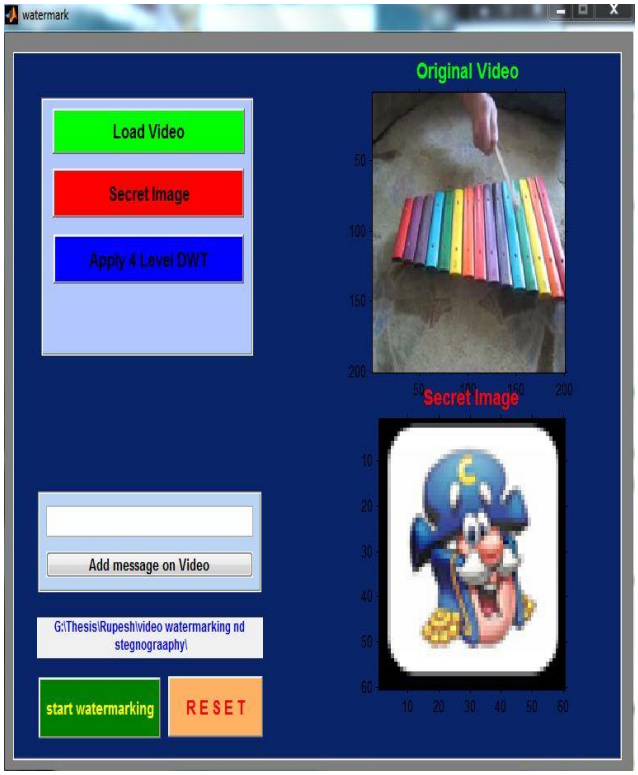

Figure 4: Secret Image Is loaded

Figure 5 is showing the buttons of 4 level DWT and 5 level DWT which will be applied to video in next step. Also in this step watermark is applied on the video.

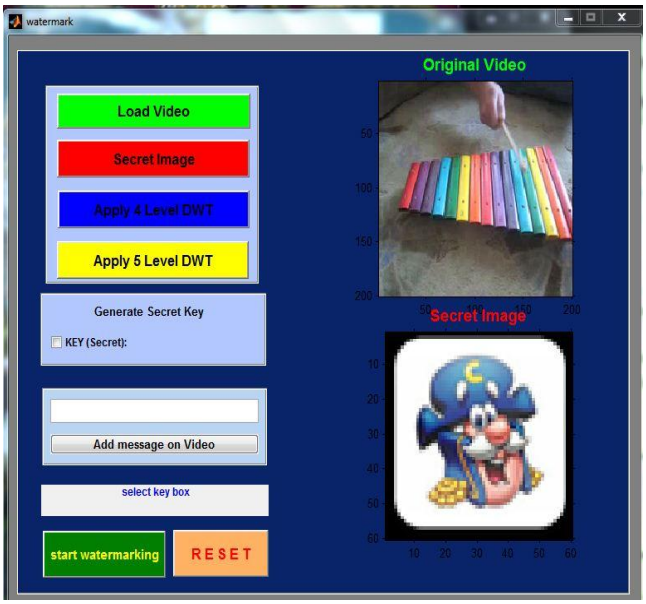

Figure 5:Watermarking is applied

Figure 6 is the snap shot of adding password and secret key to the video.

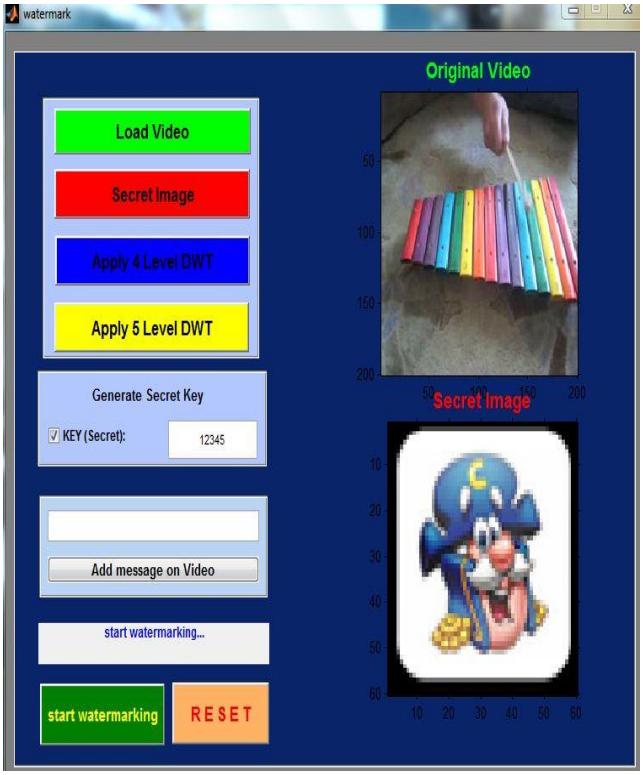

Figure 6: Password is added

Figure 7 is the process of applying stegnography to video which is the second last step.

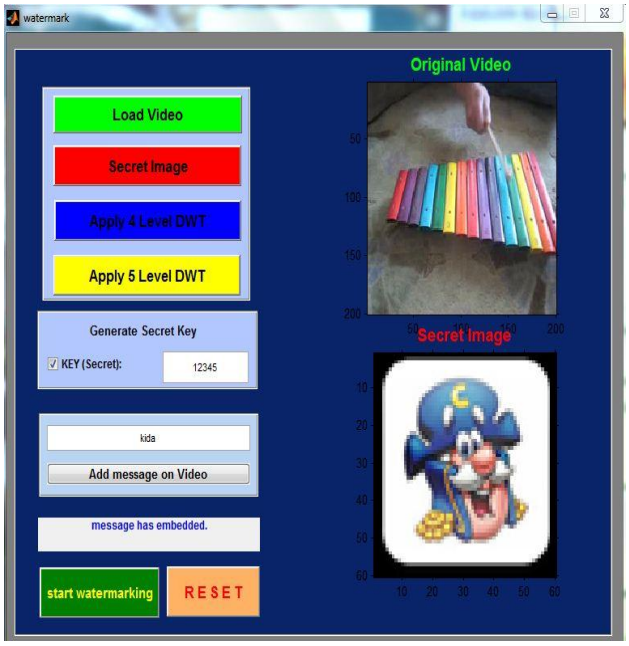

Figure 7: Stegnography is applied

Figure 8 is the last screenshot of decoding side which is extracting the video and secret image.

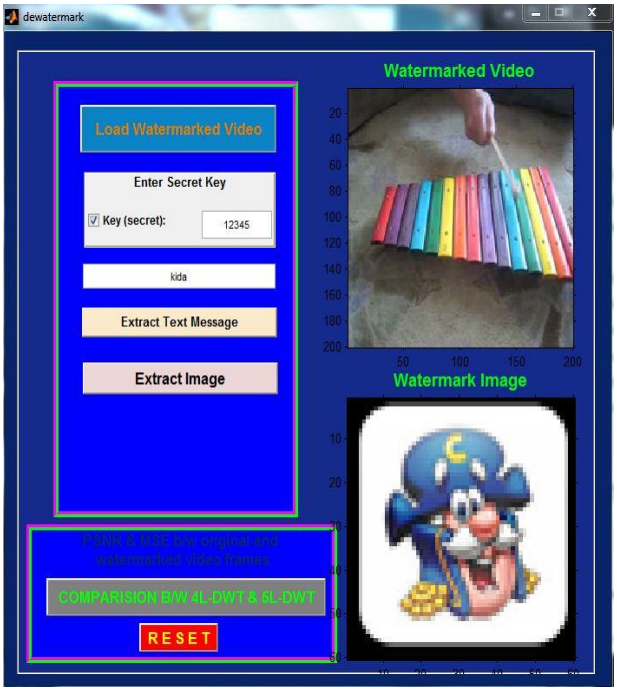

Figure 8: Decoder Side, Message is extracted

The figure 9 is the graphical representation of the parameter MSE which clearly shows that the new technique that is 5L DWT is showing better results that the previous technique.

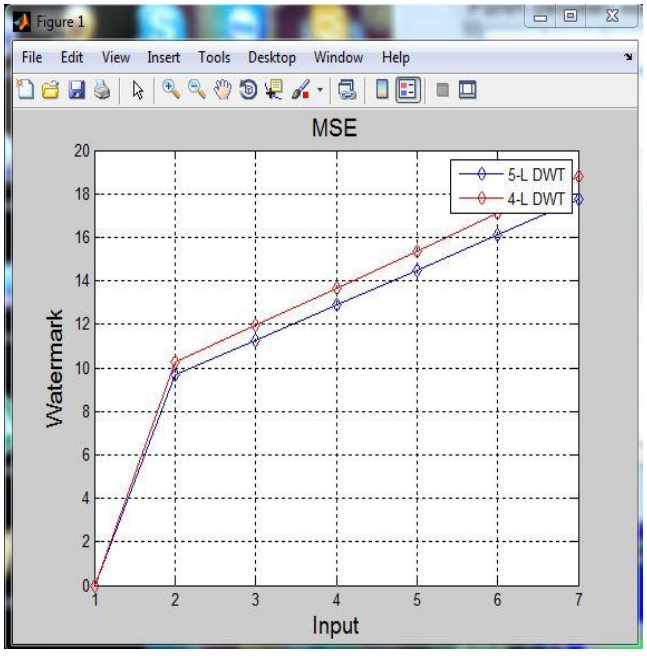

Figure 9: Graph of MSE between 5L and 4L DWT.

Figure 10 is another graphical representation of parameter PSNR which is again showing that new technique is providing better PNSR results by 10%..

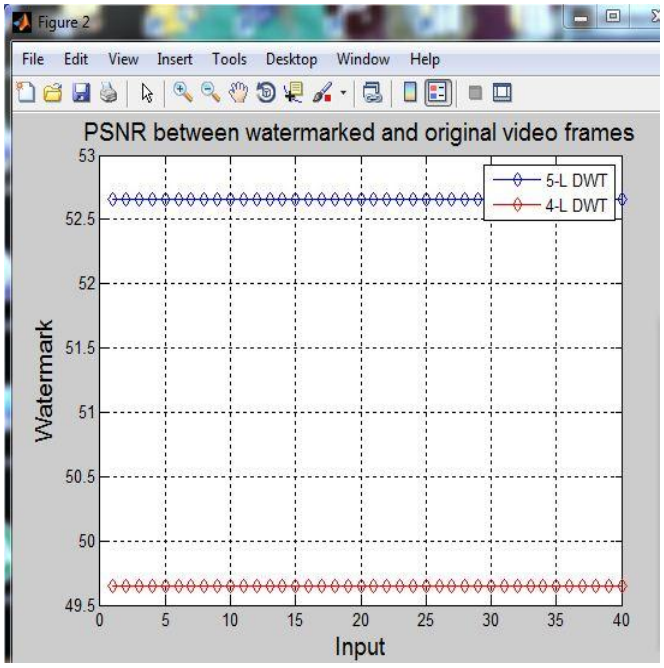

Figure 10: PSNR between watermarked and original video frames

Figure 11 is screen shot of PSNR 4 L DWT technique results.

Figure 11: PSNR for 4-L DWT

Figure 12 is the snap shot of PSNR 5L DWT Technique

Figure 12: PSNR for 5-L DWT

Figure 13 is the screen shot of parameter embedding capacity which is more than the previous algorithm which was 50%

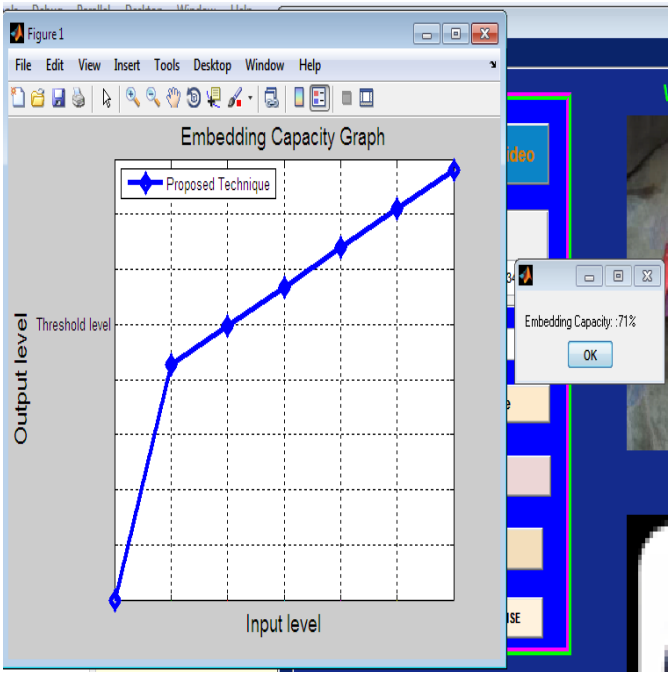

Figure 13: Embedding capacity graph between input level and threshold value

Figure 14 is the screen shot showing the data transmitted after noise attacks which value is 34.7%

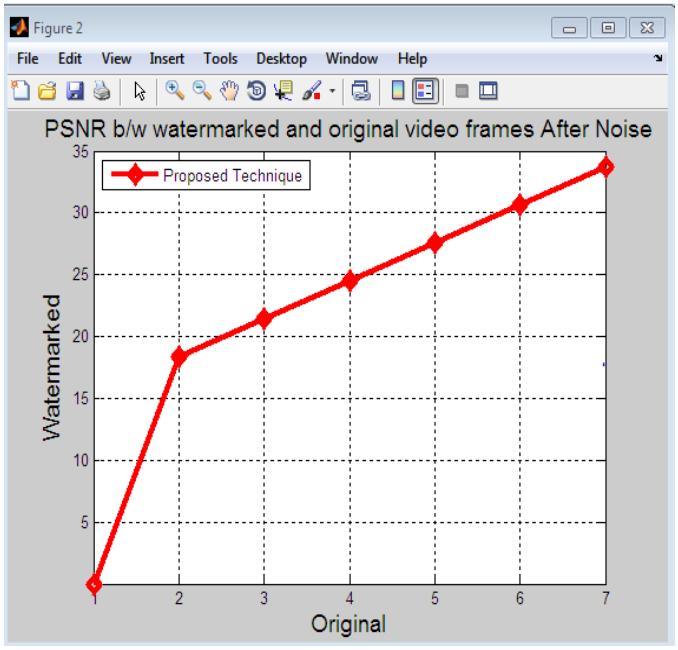

Figure 14: Graph between watermark and digital image showing PSNR between watermark and original video frames after noise

VII CONCLUSION

We proposed image based Stegnography and Cryptography with Watermarking. The main benefit of this technique is highsureness for key material exchanging which is also convenient in communications for codes and self-error improvement. It can add remedial video or image data in case exploitation occurs due to poor linking or broadcast. Thus concluding that the new technique is providing better results approx. around 10% in case of MSE and PSNR parameters are considered. This new technique is combing the few major security mechanism like stegnography, watermarking resulting better results.

REFERENCES

[1]Sunil.K. Moon Rajshree.D.Raut "Analysis of Secured Video Steganography UsingComputer Forensics Technique for Enhance Data Security" Proceedings of the 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013)

[2]S.Lyu and H. Farid , "Steganography using higher order image statistics , " IEEE Trans. Inf. Forens. Secur. 2006.

[3]Z.Zhou, G.R.Arce, and G.DiCrescenzo, "Halftone Visual Cryptography", IEEE Tans. On Image Processing,vol.15, No.8, August 2006, pp. 2441-2453

[4]http:/ aakash.ece.ucsb.edu./data hiding/stegdemo.aspx.Ucsb data hiding online demonstration. Released on Mar .09,2005.

[5]N . Provos, "Defending Against Statistical Steganography," Proc 10th USENEX Security Symposium 2005.

[6]Venkatraman , s, Abraham , A . &Paprzycki M." Significance of Steganography on Data Security " ,Proceedings of the International Conference on Information Technology : Coding and computing , 2004.

[7] N . Provos and P. Honeyman, "Hide and Seek: An introduction to Steganography," IEEE Security & Privacy Journal 2003.
[8]Fredric , J ., Goljan M., and Hogea , D ; New Methodology for Breaking stenographic Techniques for JPEGs. "Electronic Imaging 2003".
[9]MitsuguIwanmoto and Hirosuke Yamamoto, "The Optimal n-out-of-n Visual Secret Sharing Scheme for GrayScale Images", IEICE Trans. Fundamentals, vol.E85- A, No.10, October 2002, pp. 2238-2247.
[10]Katzenbeisser and Petitcolas , "Information Hiding Techniques for Stenography and Digital watermaking" Artech House, Norwood, MA. 2000.
[11]DoronShaked, Nur Arad, Andrew Fitzhugh, Irwin Sobel, "Color Diffusion: Error Diffusion for Color Halftones", HP Laboratories Israel, May 1999.
[12]E.R.Verheul and H.C.A. Van Tilborg, "Constructions and properties of k out of n visual secret sharing scheme", Designs, Codes, and Cryptography, vol.1, no.2, 1997, pp.179-196.
[13]M.Naor and A.Shamir, "Visual Cryptography", in Proceedings of Eurocrypt 1994, lecture notes in computer science, 1994, vol.950, pp. 1-12.
[14]Robert Ulichney, "The void-and-cluster method for dither array generation", IS&T/SPIE Symposium on Electronic Imaging and Science, San Jose, CA, 1993, vol.1913, pp.332-343.
[15] Steven W. Smith , The Scientist and Engineer's Guide to Digital Signal Processing.
[16] www.seminarprojects.net
[17] www.pandianss.com
[18] www.samoore.com
[19] www.surfkit.ln
[20] www. home7.inet.tele.dk
[21] www.garykesseler.net
[22] BhargaviKaipa "Staticalstegnalysis of images using open source software', IEEE Long Island System Application and technology, 2010

