Journal of Advanced Computing and Communication Technologies ***(ISSN:* 2347 - 2804*)***
Volume No.5 Issue No.2, April 2017

ANALYSIS AND DESIGN OF MULTIPLE WATERMARKING IN A VIDEO FOR AUTHENTICATION AND COPYRIGHT PROTECTION

By

1st Mr. Yogendra Sharma, 2nd Mr. Ankur Goyal
1st Research Scholar, Computer Science Engineering Department, Yagyavalkya Institute of Technology (YIT),Jaipur
2nd Assistant Professor,Computer Science Engineering Department. Yagyavalkya Institute of Technology (YIT),Jaipur
1st yogendras1988@gmail.com, 2nd ankur_gg5781@yahoo.com

ABSTRACT
Watermarking technique be employ instance & for a second time for validation and protection of digital data (images, video and audio files, digital repositories and libraries, web publishing). It is helpful to copyright protection and illegal copying of digital data like video frames and making digital data more robust and imperceptible. With the advent of internet, creation and delivery of digital data has grown many fold. In that Scenario has to need a technique for transferring digital data securely without changing their originality and robustness. In this paper proposed a plan of latest watermarking method which involves inserting and adding two or more digital data or pictures in a single video frame for the principle of protection and replicate the similar procedure for N no video frames for authentication of entire digital video. After that digital video is encrypted and decrypted by using motion vector bit-xor encryption and decryption technique.

Keywords
Multimedia; Watermarking; Steganography; Cryptography; LSB; PSNR; Video Frame

1.INTRODUCTION
Nowadays there is a hasty augmentation in the communication organizations & open server domains like Internet. Many performers, filmmakers, photo-graphers etc. be uploading own data online. Because they search for employ of digital networks to propose multimedia for income sources, they have a tough concern in protecting their ownership rights. Information technology has alleviation the copying, usage and the act of spreading of digital information in modern time which has outcome in the demand for safe ownership of digital images. A vital apprehension for the multimedia proprietors and distributors has data authentication and protection of copyrights. The answer to these troubles has Digital Watermarking. The watermarking is that the method of embedding a proof in to alternative signal robustly and invisibly at a similar time, the embedded signal is termed watermark and also the alternative signal is termed cover or host signal. In this paper, represent the brief summary of digital video watermarking methods to propose a video watermarking algorithm with encryption and decryption method by use of the Least Significant Bit (LSB) method. Different method has a number of pros and cons other than the LSB technique has to especially fine give and take among parameters like robustness, payload capacity and quality of video frames, fragility reliability and imperceptibility.

In the theory of data hiding three techniques watermarking, steganography and cryptography has important processes. Watermarking is the initial part of steganography in which hidden data can be relate to hosting data rather than in steganography hidden data once concealed not to be perceived by user.

On the other hand in Cryptography method changing data incoherent form and it only decode only by allowed used with a secrete key. Simply numerous progresses were ready to turn into cipher data using encryption process and end user can decrypting by specific key. Therefore additional complicated technique was planned to propose the security than what it recommends. [1]

As most excellent recognized methods to protect information is cryptography. It is the method of distribution and acquires encrypt messages that can be decrypt simply by the dispatcher or the recipient. Encryption & decryption are gifted processes with numerical algorithm in form of mode that no individual can be read and only receiver can decrypting and find message. [2]

Data hiding is the method of implanted knowledge hooked on an owner side. In commonly, video and audio based multimedia is desired appropriate to their extensive occurrence & the easiness of person percepts organization concerned. Through, the common collection of data hiding method some multimedia data not to be depend by host multimedia data.

Occurrence of multimedia data hiding split a lot of general points; video data hiding need more difficult to implements as a outcome of the further temporal measurement. Video information hiding persists to comprise a dynamic study field.

There are mainly two types of data or information hiding methods:
1) Bitstream-level and
2) Data-level

In bitstream-level, the redundancies within the current compression standards are exploited. Normally, encoder systems have a variety of choices for the duration of encoding & these liberties of assortment are appropriate for operation of data hiding. Nevertheless, such technique highly relies on the organization of the bitstream; therefore, it reasonably fragile, in the logic that in numerous containers they cannot endure any set-up alteration, still with no significant losing of visualization feature. As an outcome of that kind of information hiding techniques is usually planned for uses, like authentication. On the other hand, data hiding technique are more robust to attacks. As a result, such technique is suitable for higher limit of multimedia functions. In spite of their fragile form, the bitstream-based techniques are more striking for information hiding functions. [3]

2. LITERATURE SURVEY
A. WATERMARKING
Watermarking methods triumph over the authentication and copyright protection laws for multimedia information. To establish such kind of ownership watermark embed within digital data. Protect information from attacks in video frame like compression, crop,

rotate, expand, blur, and filter such kind of frames or image. After that attacker altered actual data with key if it has.

In Digital watermark process a message of video frame or image has embedded with multimedia data like image or video. Watermark process is concealed within the host information by an approach of indivisible as of the information & as a result of many anti-operations not corrupting the host information. Therefore watermarking process has effort to easily fend other than enduring noticeable.

Basically watermarking has specified into two types:

1. on the original video frame or multimedia picture visible watermark overlaying visible partial transparent secret data in text or picture. In digital data format visible watermark is promising achieve Robust property against video frame and also retained copyright and authentication property.

2. Human eyes is sensible for little changes in RGB model on lesser bits that's why invisible watermark processed to embed an image into original data and such data only identified & fetched by specified software. Outcome can be achieved by extraction process to identify the copyright protection. To proving its authenticity uses a marking process on digital data such as text, image or video frame. [4]

B. LEAST SIGNIFICANT BIT (LSB)

The least Signification bit (LSB) method is to embed message in order of uncomplicated operation within host image. The hidden information or data can be altered by LSB bit technique that present in a host image.

Even if starting 8bytes of the framework was embedded through numbers, the bits of first to four bit altered by use of embedded message. According to the operation only half range of data bits in a video frame will be change to modify of cover frame to conceal secret information or msg. The level of LSB least bit changes then only least priority bit only altered and its quality was low, due to that reason human eyes not perceived these changes. Simply take out the altered bits, as that was executing very effortless procedures in passive attacks and scanned and cracked its vulnerability.

Took an example of cover picture pixel is given as 11001000 by the use of 1st LSB technique inserting secret data bit as 001 and finds resultant change pixel value as 11001001 as shown in Fig.1.

1	1	0	0	1	0	0	0

Bit Value of Pixel

0	0	1

Data bit of Secret message

1	1	0	0	1	0	0	1

Bit value of altered Pixel

Fig.1. 1st bit LSB process

In the multimedia cover picture dimension is 128*128 pixel picture, so it accumulate a sum of 16,384 bits otherwise 2,048 bytes of embed information. [5]

LSB watermark image is secreted a new picture in positive bit.

The process of LSB 1st bit as describes:

Picture bits are reading of both cover images as well as secrete message image. After that matrix of both images count in Row & Column format. Exhibit the real gray scale picture. Calculate size of picture pixels and showing that picture. At the last collect the final picture of LSB watermarking. [6]

Least Significant Bit (LSB) technique of substitution is extremely well-liked approach of embedding conceals information with effortlessness. The basic thought at this time is to introduce the conceal information at the bit of least signification bits of the multimedia picture. This terminology is quite useful because the human eyes not responsive sufficient of such colour modification. Fundamental algorithm for this is LSB substitution that acquired the initial N no of pixel of cover image where N is the primary communication of conceal information which is embed bits. Later than each of the pixels ending bit could be swapped by one of the information bits. LSB at the additional expressions 8th bit of several bytes within a picture is altered to conceal information bit.

Here taken an example of Cover picture in form of bytes 1 to 8 bit prototypes:

1st byte to 8th byte patterns

10101100 01101101 11001100 11001011

11010010 10101100 10010101 10110100

Assume a information bit "I" is to embedding into 1st to 8th byte pattern. At the moment the ASCII sign of I=10111100. Simple embedding such bits into bit pattern, eight no of bytes is required. Therefore, 8 bytes of the cover picture was captured. At the present swapped the LSB of last bit of the cover information via every last bit of embedded data as 10111100. In this approach each pixel's last bit is swapped by the outstanding information msg bits. [7]

C. MULTIMEDIA OUTLINE

Multimedia means many to one media in it; simply 'the combination of two or more media' is called multimedia. The multimedia in it media consists of text, images, photography frames, audio, video and animation. Every solitary serves as a authoritative communiqué medium aim for in cooperation of meaningful and realistic functions. While dissolved collectively media would permit at additional active and attractive occurrence Resultant is recovered on smooth additional after present is collaboration and organization among the dissimilar multimedia mechanisms.

"The multimedia is the communication" expression is given by a foremost & prominent multimedia communication philosopher Marshall McLuhan. He said that the aim of medium outlined and organizes the level with set of actions to be performed with proper delivery for that information message that working associates with human.

Multimedia consists of graphics, text, pictures, sound and audio with video frames and basically it together uses the name of multimedia associates with interactive media.

The basic meaning of media is the plural of medium. It has evolved to mean "facilitating or linking communication"—be it using a phone, the Web, TV, or some other instrument. Speaking directly with a person one on one is immediate and does not require mediation. This is communication in its purest form. [8]

D. DIGITAL VIDEO

Digital video has turned out to be standard and is being utilized as a part of an extensive variety of utilizations including DVD, computerized TV, HDTV, video communication, and remotely coordinating and in numerous web applications. These computerized video applications are attainable due to the advances in configuring and correspondence innovations and effective video compress calculations. The quick arrangement and reception of these advances was conceivable essentially as a result of standardization and the economies of scale realized by rivalry and standardization. The vast majority of the video compressed techniques depend on an arrangement of rule that decrease the excess in computerized video. The Red-Green-Blue (RGB) shading space is regularly used to catch and show advanced pictures. Every pixel is therefore spoken to by one R, G, and B parts. The 2D cluster of pixels that constitutes a photo is really three 2D exhibits with one exhibit for each of the RGB segments. A determination of 8 bits for each segment is generally adequate for run of the mill shopper applications. [9]

MPEG-4

The most imperative new elements of MPEG-4, ISO/IEC 14496, concerning video compression are the support of even lower transmission capacity devouring applications, e.g. portable units, and then again applications with to a great degree high caliber and practically boundless data transfer capacity. The making of studio motion pictures is one such a case [9]. A large portion of the contrasts between MPEG-2 and MPEG-4 are components not identified with video coding and in this way not identified with surveillance applications MPEG includes completely encoding by key casings through the JPEG calculation and assessing the movement changes between these key edges. Since insignificant data is sent between each four or five edges, a significant bits required to depict the picture comes about resultant video frames. Thus, proportions over 100:1 are normal. The plan is asymmetric; the MPEG encoder is exceptionally mind boggling and puts an overwhelming computational load for motion estimation. Decoding is substantially less complex and should be possible by today's desktop CPUs or with ease decoder chips.

AVI

It was first developed in late 1992 as a means to allow both video and audio playback at the same time. Its file compression capabilities made it a popular choice among users who had limited space in their hard drives. Advances in both compression techniques and information-sharing technology allowed AVI to maintain its popularity for years, as the file format continues to be one of the most downloaded multimedia video formats. AVI videos bear the .avi file extension.

H.264

H.264 is the consequence of a joint venture between the ITUT's Video coding Experts group and the ISO/IEC Moving Picture Experts Group (MPEG). ITU-T is the division that handles Telecommunication standard in the interest of the International Telecommunication Union. ISO remains for International Organization for Standardization and IEC remains for International Electro technical Commission, which supervises measures for all electrical, electronic and related innovations. H.264 is the name utilized by ITU-T, while ISO/IEC has named it MPEG-4 Part 10/AVC since it is introduced as another part in its MPEG-4 suite. The MPEG-4 suite incorporates, for instance, MPEG-4 Part 2, which is a standard that has been utilized by IP-based video encoders and system cameras. [9]

The terms that are frequently utilized when discussing digital multimedia documents are 'record organize', 'wrapper', "container" and 'codec'. A codec might be put away within a record, a wrapper or a container.

Document Formats, Wrappers and Containers are basically the same, in spite of the fact that the terms wrapper and container are employed to demonstrate the capacity to store distinctive types of codecs as restricted to putting away just a solitary type. For example Windows Media Files (.wmv) will just store Windows Media codecs. QuickTime and MXF are alluded to as wrapper or container since they can store many types of codecs including DV, MPEG2, Uncompressed and more.

To separate further, there are separate codecs stored for sound and video. Since we have our wording settled, how about we take a gander at codecs. The term codec is gotten from the terms encoding/decoding and compression/decompression. Fundamentally concern with these terms as they identify with advanced varying multimedia records, yet the encoding and compressing of information can obtain position in the analog domain as well, that might be an enhanced entry to recognizing the ideas occupied. [10]

3. PROPOSED WORK

Propose an art of embedding two watermarks in a given video of different formats and analyze its performance and quality of watermarking, and then encrypt the video using bit xor technique for only motion vector of the video after the completion of encryption at user side other reverse operation as decryption performed at receiver side. Decryption the dual watermarked video by using motion vector bit xor technique, and it will carry the watermark.

4.Process of Securing Information

In this process the sender reads a Video and extracts its frames, which can embed two watermarks, then the users inputs two different watermark images and converts the into vectors. Then the sender embeds first watermark in the first cover frame to provide the watermarked image using 1st Bit plane LSB technique. Then using the resultant cover frame the user embeds the second watermark using 3rd Bit Plane LSB technique. The above process is repeated for all the frames, each carrying two watermarks.

Following steps are processed for getting secure video:

1. Extract All Frames of Video and store them in a Vector and Embed First watermark in ith Frame at first LSB after that Embed first watermark in ith Frame at third LSB.
2. If i number of Frame is equal to Last Frame then performed encryption of dual watermarked video by using of motion vector Xor technique otherwise move to i+1 th frame and
3. Repeat same process and decrypt the dual Watermarked Video using Motion Vector Bit Xor technique. And it will carry the watermark.
4. At last resultant Secure Video for communication is ready.

The snapshots and results of watermarked video of all three types and their PSNR Values are shown as given below. For embedding has used two different watermarks which as follows:

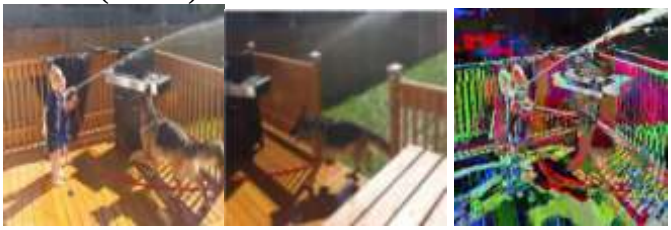
Watermark 1

Watermark 2

Fig.2. Watermark images

Snapshots of Video Original, Watermarked and Encrypted Video Frames are:

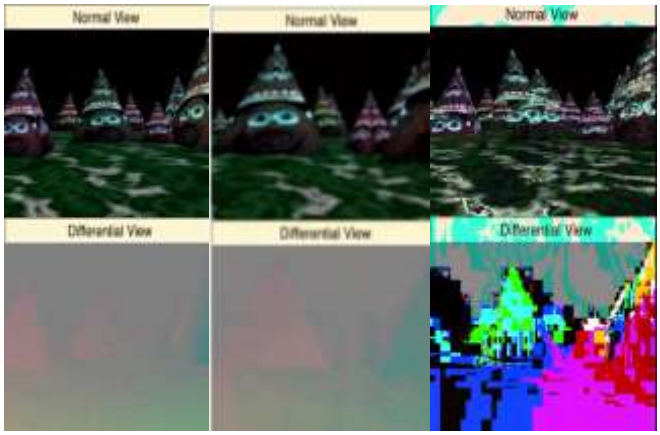
1. MP4 (H.264) Video



Original Video Frame Watermarked Video Frame Encrypted Video Frame

Fig 3(a) MP4 (H.264) video snapshots

2. MPEG Video



Original Video Frame Watermarked Video Frame Encrypted Video Frame

Fig 3(b) MPEG video snapshots

3. AVI Video

Original Video Frame Watermarked Video Frame Encrypted Video Frame

Fig 3(c) AVI video snapshots

Fig.3. (a, b, c) Snapshots of Original, Watermarked and Encrypted Video Frame

After performing all the experiments it is time to do the analysis of the results obtained of the outcome of the same. After processing such techniques in Mat lab, the Results and outcome comes in graphically which shown in fig.4 and scenario of outcome in different formats is as different according to different video formats.

Analyses the outcome of efforts made by the sender and results of watermarked video

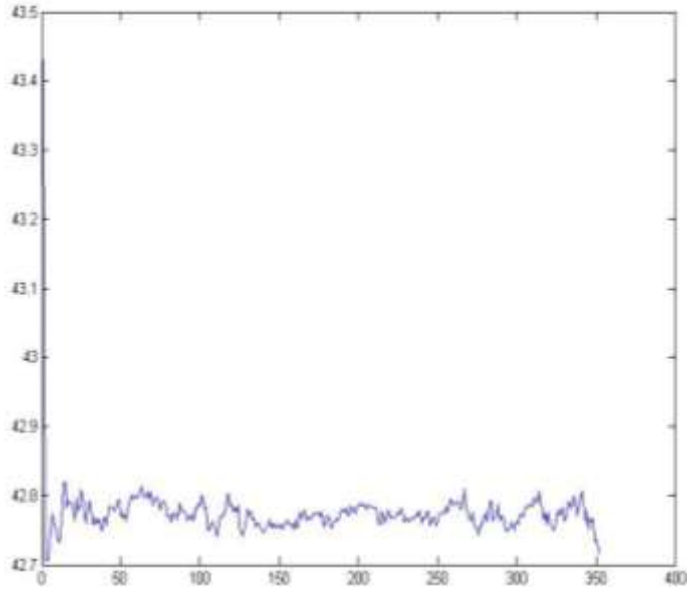


Fig.4. PSNR Graph of All the frames of AVI Video

The changes in PSNR over 350 iteration of training set of 400 to 10,000 are calculated and plotted for the AVI Video. The graph had shown in Fig.4 PSNR Graph of All the frames of AVI Video. The changes in PSNR over 325 iteration of training set of different values are calculated and plotted for the AVI Video. The graph had shown in Fig.5 PSNR Graph of All the frames of MP4 Video. The changes in PSNR approx. 30 iteration of training set of different training set values are calculated and plotted for the AVI Video. The graph had shown in Fig.6 PSNR Graph of All the frames of MPG Video.

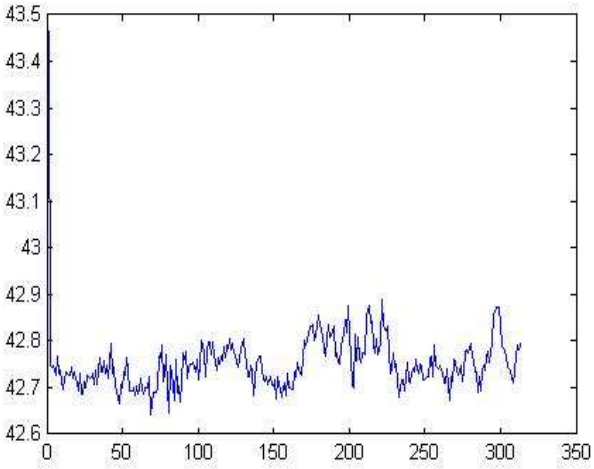


Fig.5. PSNR Graph of All the frames of MP4 Video

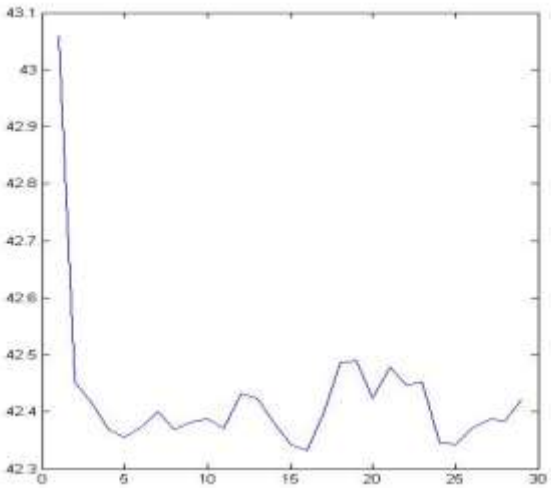


Fig.6. PSNR Graph of All the frames of MPEG Video

After plotting graph of different video formats, table contents showing the values of MSE and PSNR comparative between simple watermarking and proposed LSB video watermarking technique such table of contents shown in Table.1. As this result of analysis given best outcome in LSB watermarking technique in all video formats like mpg,mp4,avi.

TABLE.1. Comparative analysis of Video Watermarking Techniques through PSNR and MSE Value

Feature	Proposed Video LSB Watermarking Technique			Simple Watermarking		
MSE(Mean Square Error)	3.88	3.78	3.69	4.962	4.284	4.218
PSNR(Peak Signal to noise Ratio)	42.43	42.75	42.71	41.23	41.82	41.87
FORMAT OF VIDEO	MPG	MP4	AVI	MPG	MP4	AVI

ANALAYIS OF RESULT	Best in all applying video formats.	Good but not best in such video formats

Graph of MSE as shown in fig.7, that graph considering three values assignment done between proposed and simple video watermarking technique. Series 1 showing proposed technique which is blue line and series 2 which is red line showing simple watermarking as analysis of that proposed technique is good rather than simple watermarking technique as shown in fig.7.

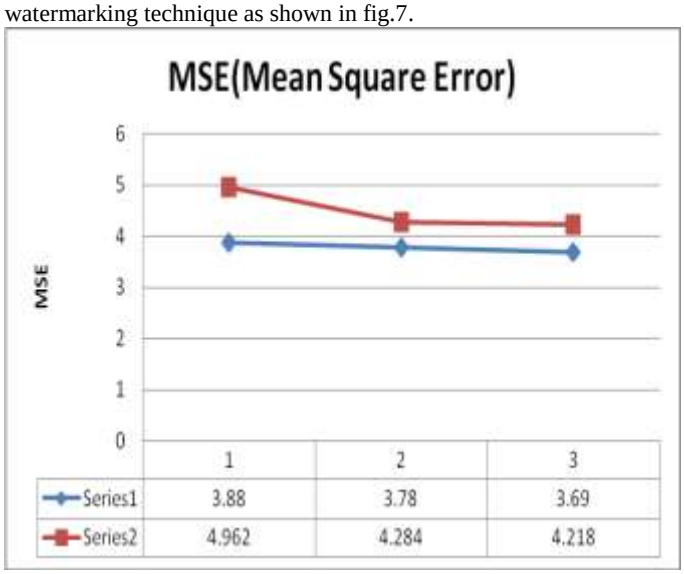


Fig.7. MSE Graph of proposed and simple video watermarking of all video formats

In PSNR graph shown in Fig.8. Series 2 which is red showing proposed watermring using LSB techniue which is better than series 1 which is blue line. As PSNR is much higher is showing good quality of video frames that was delivering by proposed method.

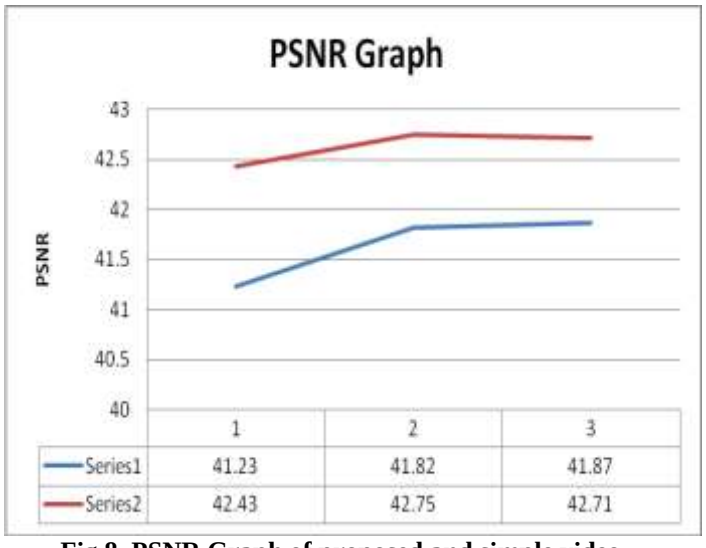


Fig.8. PSNR Graph of proposed and simple video watermarking of all video formats

The PSNR is calculated by
PSNR=10 log10 L2/MSE
Where L=Peak signal level for a frame of video.
The Value of MSE is calculated by
MSE = (1/HW) ΣHi=1 ΣWj=1 (P(i,j)*S(i,j))2
H=Height, W=Width, P (i,j) = Original Image, S (i,j) = Corresponding image

Maximum payload (bits per byte/bpb) for the technique has been obtained i.e. Maximum amount of data that can be embedded into the cover image without losing the fidelity of the original video.

5.CONCLUSION & FUTURE WORK

5.1 Conclusion

There are also many techniques of watermarking involving, Least Significant bit, Discrete Wavelet Transformation, Discrete cosine Transformation and many more, which effectively and more importantly they ensure and protected communication of the cover object which delivers the result of watermarking to the receiver with minimum redundancy.

Most of the existing techniques either embed only one watermark or they use two different types of watermarking techniques to generate a single watermark.

Here in this dissertation propose an art of embedding two watermarks in a given video of different formats and analyze its performance and quality of watermarking.

This benefits us in three ways first it helps us to increase the payload of the given cover frame of the video and also increases the security of the given frame of the video such that the even if someone cracks the hidden watermark then also there is still a second watermark which ensures authenticity or copy right of the given video and as the watermark.

In this work take three different types of video namely MP4 video, AVI video and MPEG video and embed two watermarks same in all three videos and then all these three videos are encrypted using motion vector bit-xor encryption technique. So that can judge the quality of watermark being embedded in all three formats.

As our results show that the PSNR of final output watermarked video is very good in terms of input video and the work done for securing the image for communication has also been achieved. The quality of H.264 (MP4) video and AVI video are almost same but the quality MPEG Video is bit less.

5.2 Future Work

In future one can perform the further task to enhance better results and good security:

1. Use embedding techniques like DCT or DWT
2. Use higher Payload using multiple watermark
3. Generate visible watermarks on the given image/
4. Use encryption techniques in random to the above work for better security too.

6. REFERENCES

[1]. Ankita Gharat, Preeti Tambre, Yogini Thakare, Prof. S.M. Sangave "Biometric Privacy Using Visual Cryptography" IJARCET, ISSN: 2278 – 1323, January 2013.

[2]. A.Angel Freeda, M.Sindhuja, K.Sujitha, "Image Captcha Based Authentication Using Visual Cryptography", IJREAT, ISSN: 2320 – 8791, April 2013.

[3]. K.Mohan, S.E.Neelakandan, "SECURED ROBUST VIDEO DATA HIDING USING SYMMETRIC ENCRYPTION ALGORITHMS", International Journal of Innovative Research in Engineering & Science ISSN 2319-5665,(January 2014, issue 3 volume 1).

[4]. Santhoshi Bhat, Arghya Ray , Avishake Ghosh, Ananya Ray, "Image Steganography and Visible Watermarking using LSB Extraction Technique", IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO) 2015.

[5]. Gil-Je Lee, Eun-Jun Yoon, Kee-Young Yoo "A new LSB based DigitalWatermarking Scheme with Random Mapping

Function", 2008 International Symposium on Ubiquitous Multimedia Computing.
[6]. N. SenthilKumaran, and S. Abinaya "Comparison Analysis of Digital Image Watermarking using DWT and LSB Technique", International Conference on Communication and Signal Processing, April 6-8, 2016, India
[7]. M. C. Padma,Yashaswini. J,"Hiding Data in Encrypted Image with LSB Substitution", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2 Issue 6, June 2013
[8]. Jennifer Coleman Dowling (Author), "Multimedia Demystified Paperback" ISBN-13: 978-071770644 ISBN-10: 007177064X Edition: 1st, the McGraw Hill Publication, 2012.
[9]. S. Ponlatha and R. S. Sabeenian, "Comparison of Video Compression Standards", International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013
[10] "A Primer on Codecs for Moving Image and Sound Archives & 10 Recommendations for Codec Selection and Management "by chris lacinak president audiovisual preservation solutions.

[11]. P. Geum-Dal,; Y. Eun-Jun,; Y. Kee-Weng , (2008) "A New Copyright Protection Scheme with Visual Cryptography", Second International Conference on Future Generation Communication and Networking Symposia. pp. 60-63.
[12]. Shashikala Channall, Ajay Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering Vol.1 (3), 2009, 137-141.
[13]. C. Cachin, "An Information-Theoretic Model for Steganography", in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318, 1998.
[14]. Mohammad Shirali-Shahreza, "A new method for real time steganography", ICSP 2006 Proceedings of IEEE.
[15]. Yuk Ying Chung, fang Fei Xu , "Development of video watermarking for MPEG2 video" City university of Hong Kong ,IEEE 2006.
[16]. Jordi Nin, Sergio Ricciardi, "Digital Watermarking Techniques and Security Issues in the Information and Communication Society", WAINA, 2013-03, ISBN: 978-1-4673-6239-9, pp: 1553-1558.