ISSN:0975-9646

"Analysis & Design of multiple watermarking in a Video for Authentication & Copyright Protection"

Yogendra Sharma
(Student)
Computer Science Engineering Department
Yagyavalkya Institute of Technology (YIT)
Jaipur, India

Jitender Kumar
(Assitant Professor)
Computer Science Engineering Department
Compucom Institute of Technology & Management(CITM), Jaipur,India

Yogesh Rathi
(Assistant Professor)
Computer Science Engineering Department
Yagyavalkya Institute of Technology (YIT)
Jaipur, India

***Abstract*— Watermarking has been used time and again for authentication & security of Video. Digital watermarking refers to embedding watermarks in a multimedia documents and files in order to protect them from illegal copying and identifying manipulations. Watermarking is a promising solution to protect the copyright of multimedia data through Transcending, because the embedded message is always included in the data. Because of the fidelity constraint, watermarks can only be embedded in a limited space in the multimedia data. Watermarking techniques can be classified into two types: -1. Spatial & 2. Frequency Domain.**
In this work proposed to design a new watermarking technique which involves embedding two or more messages or images in a single frame of video for the purpose of security and repeat the same process for N-frames of the video for authentication of whole video.

Keywords*— Watermarking; Video; Multimedia; LSB; PSNR; Stegnography; DCT; frame; encryption

I. INTRODUCTION

Multimedia consists of many things in one. The simplest definition of multimedia is "the combination of two or more media." The media in multimedia comes in various forms: graphics, photography, text,
audio (sound effect, music, voice-over and so on), video and animation. Each one serves as a powerful communication vehicle for both expressive and practical purposes. When melded together media will allow for a more dynamic and engaging experience. Whereas resultant is improved on even further when there is cooperation and coordination between the disparate media components. Multimedia is a synergistic process whereby various media elements work together to make a stronger, more cohesive whole. A combination of media adds richness and provides a complete sensory experience.

Media, by definition, is the plural of medium. It has evolved to mean "facilitating or linking communication"—be it via 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. The purpose of a medium is to assist in the conveying of a message. When using more than one type of medium, we refer to it as multimedia, whether or not it is computer-based. At one time, media mainly applied to newspapers as a way to disseminate news and information to the masses. Now, media encompasses many forms of communication.

Multimedia is a synergistic process whereby various media elements work together to make a stronger, more cohesive whole. A combination of media adds richness and provides a complete sensory experience. Multimedia once meant a slide projector and a tape recorder being played simultaneously. For instance, 50 years ago, photographic images in slide form were projected on a screen or wall while audio attempted to synchronize with the sequence or played as "background" music.

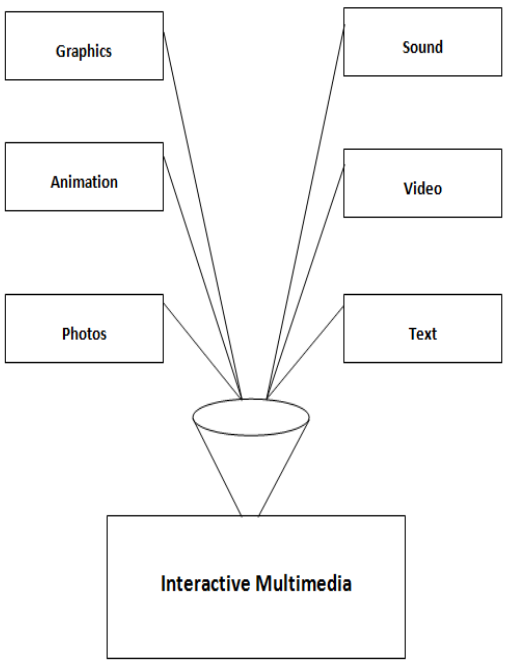


Fig 1 Multimedia Introduction

Multimedia can be broadly divided into linear and nonlinear category. Progress linear activities without any navigation control audience, such as film screenings**.**

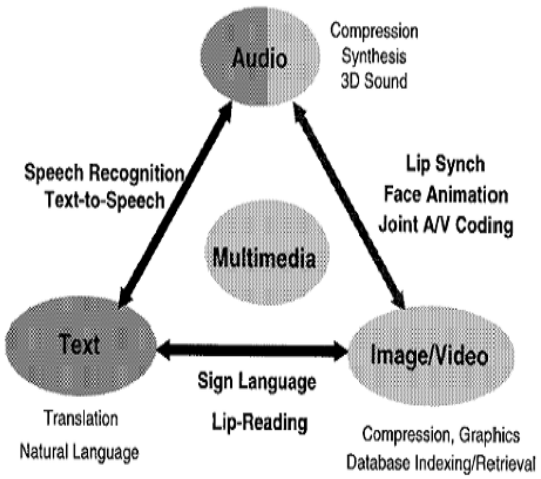


Fig 2. Multimedia catagories

Nonlinear content providers for the use of user interaction with a computer game or self-paced computer-based training to control the progress. Nonlinear content is also known as hypermedia content.

II. MULTIMEDIA ITEMS GENERALLY FALL INTO ONE OF FIVE MAIN CATEGORIES AND USE VARIED TECHNIQUES FOR DIGITAL FORMATTING

Text: It may be an easy content type to forget when considering multimedia systems, but text content is by far the most common media type in computing applications. Most multimedia systems use a combination of text and other media to deliver functionality.

Images: Digital image files appear in many multimedia applications. Digital photographs can display application content or can alternatively form part of a user interface. Interactive elements, such as buttons, often use custom images created by the designers and developers involved in an application. Digital image files use a variety of formats and file extensions. Among the most common are JPEGs and PNGs.

Audio: Audio files and streams play a major role in some multimedia systems. Audio files appear as part of application content and also to aid interaction. When they appear within Web applications and sites, audio files sometimes need to be deployed using plug-in media players. Audio formats include MP3, WMA, Wave, MIDI and RealAudio.

Video: Digital video appears in many multimedia applications, particularly on the Web. As with audio, websites can stream digital video to increase the speed and availability of playback. Common digital video formats include Flash, MPEG, AVI, WMV and QuickTime. Most digital video requires use of browser plug-ins to play within Web pages, but in many cases the user's browser will already have the required resources installed.

Animation: Animated components are common within both Web and desktop multimedia applications. Animations can also include interactive effects, allowing users to engage with the animation action using their mouse and keyboard. The most common tool for creating animations on the Web is Adobe Flash, which also facilitates desktop applications. Using Flash, developers can author FLV files, exporting them as SWF movies for deployment to users. Flash also uses Action Script code to achieve animated and interactive effects.

What is An Video: Digital video appears in many multimedia applications, particularly on the Web. As with audio, websites can stream digital video to increase the speed and availability of playback. Common digital video formats include Flash, MPEG, AVI, WMV and QuickTime. Most digital video requires use of browser plug-ins to play within Web pages, but in many cases the user's browser will already have the required resources installed.

Video Container and Video CODEC: Video format consists of different technology concept: one is containers and another is codec. Containers are sometimes called as wrappers. Container basically describes the structure of file: where the various pieces are stored, how they are interleaved and which codec are used by which pieces. A codec is a way of encoding audio or video into a stream of bytes such as MPEG1, H.264 etc.

III. STEGANOGRAPHY

Steganography is the ability and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word steganography is of Greek origin and means "concealed writing" from the Greek words stegano meaning "covered or protected", and graphy meaning "writing". A basic classification of steganographic algorithms operating in the spatial domain as the method for selecting the pixels distinguishes three main types: non-filtering algorithms, randomized algorithms and filtering algorithms.

Types of Steganography

Steganography can be split into two types, these are Fragile and Robust. The following section describes the definition of these two different types of steganography.

- **Fragile**:-Fragile steganography involves embedding information into a file which is destroyed if the file is modified. This method is unsuitable for recording the copyright holder of the file since it can be so easily removed, but is useful in situations where it is significant to prove that the file has not been tampered with, such as using a file as evidence in a court of law, since any tampering would have removed the watermark. Fragile steganography techniques tend to be easier to implement than robust methods. [3]
- **Robust**:-Robust marking aims to embed information into a file which cannot easily be destroyed. Although no mark is truly indestructible, a system can be considered robust if the amount of changes required to remove the mark would render the file useless. Therefore the mark should be hidden in a part of the file where its removal would be easily perceived.[4]

IV. WATERMARKING

Watermarking embeds identifying information in an image, which is not always hidden, in such a manner that it cannot easily be removed. It can also contain device control code that prevents illegal recording. Another application of watermarking is copyright control, in which an image owner seeks to prevent illegal copying of the image. Watermarking is a promising solution to protect the copyright of multimedia data through Transcending, because the embedded message is always included in the data. Because of the fidelity constraint, watermarks can only be embedded in a limited space in the multimedia data. [4]

Watermarking Process

A watermarking system is made up of a watermark embedding system and a watermark recovery system. The system also has a **key** which could be either a public or a secret key. The **key** is used to enforce security, which is prevention of unauthorized parties from manipulating or recovering the watermark. The inputs during the encoding process are the original data, the cover object and the output is the recovered watermarked data W.

The digital watermark embedding and retrieval is as shown in the figure 2.9 and figure 2.10**[9].** In the embedding process, the watermark to be embedded is hidden in the cover object, may be an image, audio or video file and during extraction, watermark is retrieved and removed from the image to obtain the original image.

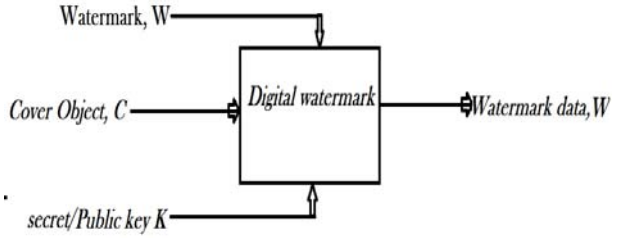


Fig.3.Watermark_Embedding [9]

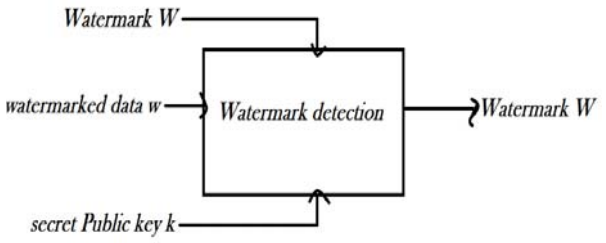


Fig. 4. Watermark Detection [9]

V. DATA HIDING TECHNIQUES

Binary File Techniques When we are trying to hide small key data inside a binary file, whether the top key data is a copyright watermark or only simple key text, we face the problem of alteration, i.e. if anyone alters the binary file it can also cause altering the execution. The main cause for this is the need to protect their copyright inside a binary program. One can find different ways of protecting copyright in application, such as sequential secrets, but if we look up on Internet, crucial generators for standard programs are commonly accessible and thus using sequential secrets would not be enough to protect the binary file's copyright.

Text Techniques Although it is very easy to see when we have committed a copyright infringement by photocopying a guide, since the feature is commonly different, it is more challenging when it comes to electronic versions of text. Copies are the exact same and it is difficult to share with if it's an authentic or perhaps a copied version. To introduce data inside a record we are able to clearly transform a number of their attributes. These can be also the text style or faculties of the characters. We may believe when we modify these faculties it can become obvious and clear to next events or attackers. The main element of this issue is that people modify the record in a way that it is simply not visible to the eye however it is probably decoded by computer.

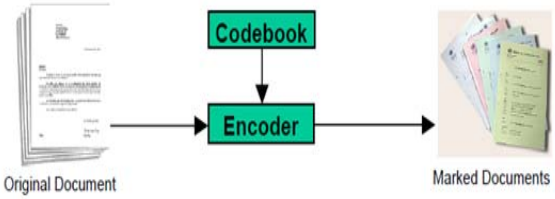


Fig 5. Document embedding process

This determination reveals the general theory in embedding concealed information in the document. Again, there's an encoder and to decode it, there will be a decoder. The codebook contains some principles which tell the encoder about the areas of the report it must change. It can be worth noticing that the marked papers may be either similar or different. By different means, we signify the same watermark is marked on the report but various characteristics of the papers are changed.

Image Techniques

- **Simple Watermarking**

A very easy however carefully applied process for watermarking images is to add a pattern along with a current image. Frequently this product is a graphic in itself - an emblem or something related, which distorts the underlying image. In an ordinary picture manager it probably will merge both images and get a watermarked image. So long as we realize the watermark, it is possible to change any undesirable effects so that the unique doesn't need to be kept. This process is only actually applicable to watermarking, whilst the product can be viewed and actually with no original watermark, it is probable to eliminate the pattern from the watermarked picture with some energy and skill.

- **LSB Least Substantial Bit Hiding (Image Hiding) -** This approach is probably the best means of hiding information in a graphic and however it is remarkably effective. It operates using the least substantial pieces of every pixel in one single picture to hide the absolute and most substantial components of another. So in a JPEG picture as an example, the following measures should be used.

1. First stock up both the sponsor picture and the picture we need to hide.

2. Next chose the number of pieces we wish to hide the trick picture in. The more the number of pieces used in the sponsor picture, the more it deteriorates. Increasing the number of pieces applied however demonstrably features a valuable reaction on the trick picture raising its clarity.
3. We now have to produce a new picture by mixing the pixels from equally images. If we decide for example, to use four pieces to hide the trick picture, you will have four pieces remaining for the sponsor image. (PGM - one byte per pixel, JPEG - one byte each for red, green, orange and one byte for leader route in some picture types)

Host Pixel: 10110001
Secret Pixel: 00111111
New Image Pixel: **10110011**

4. To get the original image back we just need to know how many bits were used to store the secret image. We then scan through the host image, pick out the least significant bits according the number used and then use them to create a new image with one change - the bits extracted now becomes the most significant bits.

Host Pixel: 10110011
Bits used: 4
New Image: **00110000**

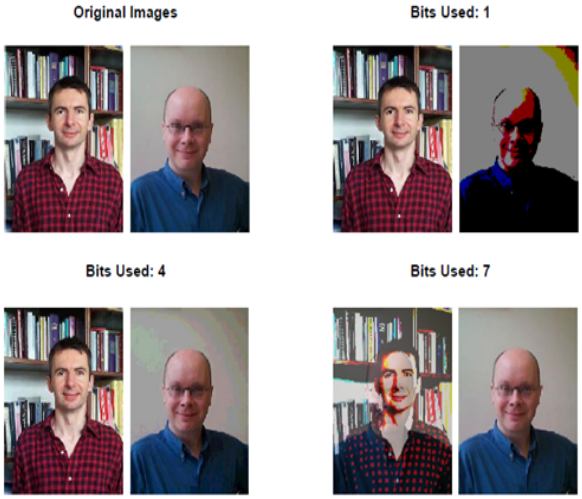


Figure 6. LSB HIDING

This method works well when both the host and secret images are given equal priority. When one has significantly more room than another, quality is sacrificed. Also while in this example an image has been hidden, the least significant bits could be used to store text or even a small amount of sound. All we need to do is change how the least significant bits are filled in the host image. However this technique makes it very easy to find and remove the hidden data.

❖ Direct Cosine Transformation

Yet another means of covering knowledge is through a primary cosine change (DCT). The DCT algorithm is among the primary elements of the JPEG pressure process works as follows

1. First the picture is separated into 8 x 8 squares.
2. Next all these sections are altered with a DCT, which results in a multidimensional array of 63 coefficients.
3. A quantized unit of all these coefficients, which basically is the pressure stage as that, is where knowledge is lost.
4. Small insignificant coefficients are spherical to 0 while greater types eliminate some of the precision.
5. As of this stage we should have numerous streamlined coefficients, which are more squeezed with a Huffman encoding scheme or similar.
6. Decompression is performed via an inverse DCT.

Hiding with a DCT pays to as somebody who only looks at the pixel prices of the picture would be ignorant that any such thing is amiss. Also the hidden knowledge can be distributed more equally over the entire picture in such a way as to create it more robust.

One process hides knowledge in the quantize stage. If we need to encode the bit price 0 in a certain 8 x 8 sq of pixels, we could try this by ensuring all the coefficients are actually, as an example by fine-tuning them. Bit price 1 can be stored by fine-tuning the coefficients so they are odd. In this way a sizable picture may keep some knowledge that's quite difficult to identify in comparison to the LSB method. This can be a quite simple process and while it is effective to keep down disturbances, it is at risk of noise.

Figure 7. Direct Cosine Transformations.

Other practices, which use DCT transformations, occasionally use different formulas for holding the bit. One employs pseudo noise to incorporate a watermark to the DCT coefficients while still another employs an algorithm to scribe and acquire a bit from them. These other practices are generally more technical and are more robust compared to strategy described.

VI. PROPOSED WORK

As discussed before and motivation generated from review literature we find that many techniques exist for watermarking a media using text, image or any other media as the watermark is embedded in the cover image. 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.

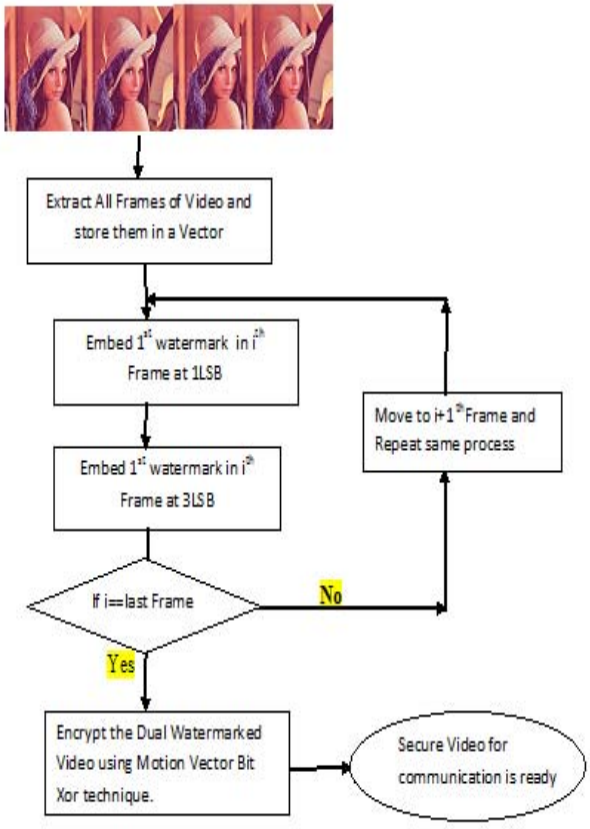
Most of the existing techniques either embed only one watermark or they use two different types of watermarking techniques to generate a single watermark.

Here in this we propose an art of embedding two watermarks in a given video of different formats and analyze its performance and quality of watermarking, and then we encrypt the video using bit xor technique for only motion vector of the video.

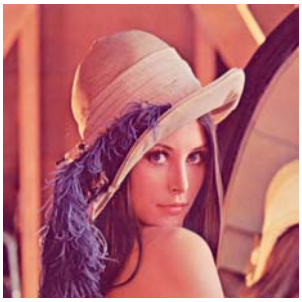
This benefits us in two ways first it helps us to increase the payload of the given cover frame of the video and also increases the security of the given frame of the video such that the even if someone cracks the hidden watermark then also there is still a second watermark which ensures authenticity or copy right of the given video.
In this work we take three different types of video namely MP4 video, AVI video and MPEG video and embed two watermarks same in all three videos so that we can judge the quality of watermark being embedded in all three formats.

❖ **Process of Watermarking & 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.
The flow chart at the sender end is as follows:



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


Watermark 1

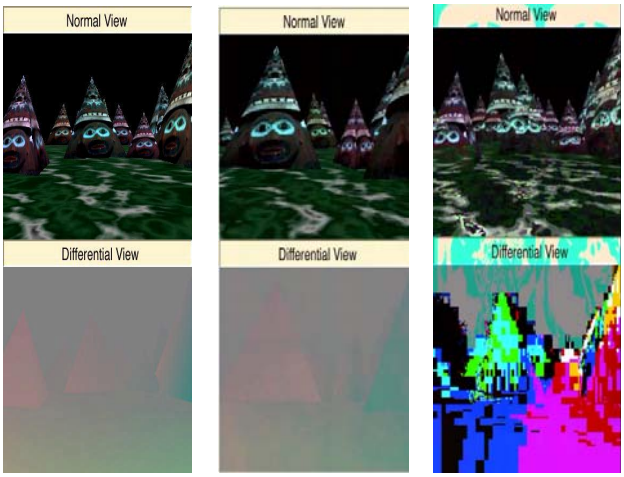

Watermark 2

Snapshots of Video both original and watermarked Video is:

1. **MP4(H.264) Video**


Original Video Frame, Watermarked & Encrypted Video Frame

2. **MPEG Video**

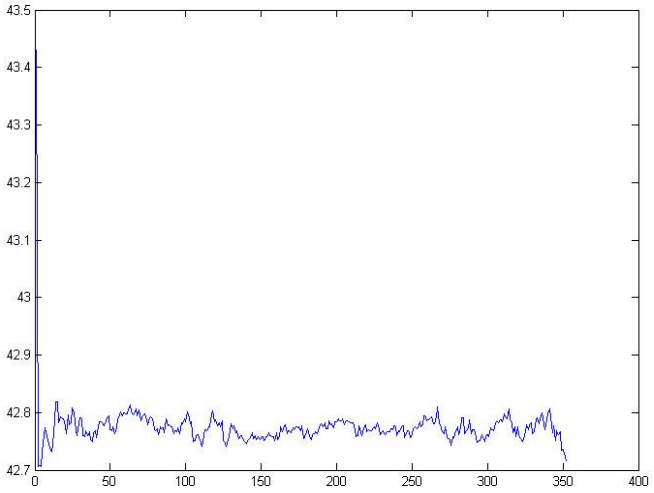


Original Video Frame, Watermarked & Encrypted Video Frame

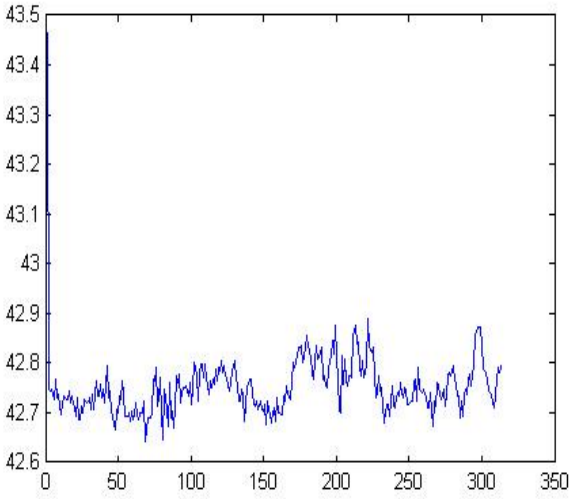
3. **AVI Video**


Original Video Frame, Watermarked & Encrypted Video Frame

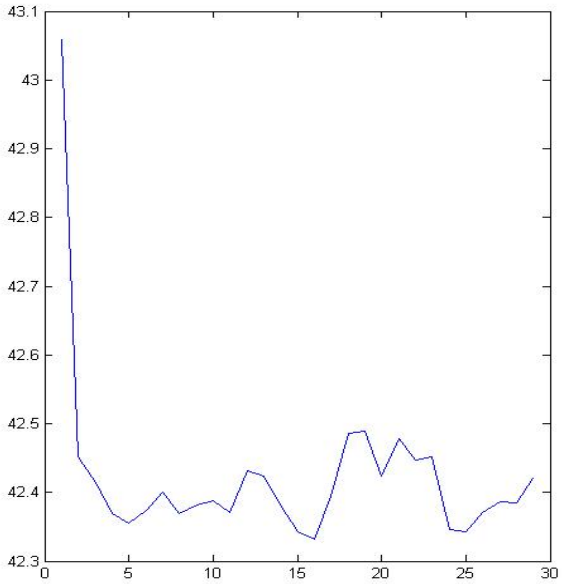
After performing all the experiments it is time to do the analysis of the results obtained of the outcome of the same. We analyses the outcome of efforts made by the sender and results of watermarked video



PSNR Graph of All the frames of AVI Video



PSNR Graph of All the frames of MP4 Video



PSNR Graph of All the frames of MPEG Video

VII. FUTURE WORK

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 work we 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 two 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.

In this work we take three different types of video namely MP4 video, AVI video and MPEG video and embed two watermarks same in all three videos are encrypted using motion vector bit xor encryption technique. So that we 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.

We also achieved the goal of ensuring authentication and copy right protection of the watermark video.

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 watermarks.
3. Generate visible watermarks on the given media.
4. Use encryption techniques in random to the above work for better security too.

. REFERENCES

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

[2]. A.Duraisamy, M.Sathiyamoorthy, S.Chandrasekar, “Protection of Privacy in Visual Cryptography Scheme Using Error Diffusion Technique Using Error Diffusion Technique”, IJCSN ISSN (Online) : 2277-5420 April 2013

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

[4]. Vilma Petrauskiene, Rita Palivonaite, Algiment Aleksa, Minvydas Ragulskis “Dynamic visual cryptography based on chaotic oscillations”, ELSEVIER, 2013.

[5]. Md. Tanbin Islam Siyam, Kazi Md. Rokibul Alam and Tanveer Al Jami, “An Exploitation of Visual Cryptography to Ensure Enhanced Security in Several Applications”, IJCA ISSN: 0975 – 8887, 2013

[6]. Anushree Suklabaidya, “Visual Cryptographic Applications”, IJCSE, ISSN: 0975- 3397, June 2013

[7]. M. L. Miller, I. J. Cox, and J. A. Bloom, "Informed embedding: exploiting image, Digital watermarking, Morgan Kaufmann Publishers Inc., San Francisco, CA, 2001.

[8]. Jitao Jiang, Xueqiu Zhou and Xiaohong Liu, “An improved algorithm based on LSB in digital image hidden”, Journal of Shandong University of Technology (Science and Technology), vol. 20(3), 2006, pp. 66-68, ISSN: 1672-6197.0.2006-03-018.

[9]. Juan Zhou, Shijie Jia, “Design and Implementation of Image Hiding System Based on LSB”, Computer Technology and Development, vol. 17 (05), 2007, pp. 114-116, doi: cnki: ISSN: 1673-629X.0.2007-05-034.

[10]. Gil-Je Lee, Eun-Jun Yoon, Kee Weng Yoo “A new LSB based Digital Watermarking Scheme with Random Mapping” in 2008 International Symposium on Ubiquitous Multimedia Computing.

[11]. Jianwei Zhang, Xinxin Fang, Junhong Yan, “Implement Of Digital Image Watermarking LSB”, Control & Automation, vol. 22(10), 2006, pp. 228-229, doi: cnki:ISSN:1008-0570.0.2006-10-083.

[12]. Qian-lan Deng Jia-jun Lin, “A Steganalysis of LSB based on Statistics”, Modern Computer, No.1, 2006, pp. 46-48, doi: cnki: ISSN: 1007-1423.0.2006-01-010.

[13]. Jian-quan Xie, Chun-hua Yang. “Adaptive hiding method of large capacity information”, Journal of computer applications, vol. 27(5), 2007, pp.1035-1037, doi: CNKI: ISSN: 1001-9081.0.2007-05-001.

[14]. Hongwei Lu, Baoping Wan, “Information Hiding Algorithm Using BMP Image”, Journal of Wuhan University of Technology, vol.28(6), 2006, pp. 96-98, doi: cnki: ISSN: 1671-4431.0.2006-06-027.

[15]. 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.

[16]. J.J. Eggers, J.K. Su and B. Girod, "A Blind Watermarking Scheme Based on Structured Codebooks," IEE Colloquium: secure image and image authentication, London, UK, April 2000

[17]. A. Westfield, A. Pfitzmann. “Attacks on steganographic systems”. In Proceedings of 3rd. International Workshop Computer Science (IH '99) Germany, 1999.