Copyright Protection of Data by using Video Watermarkings

Sharanjeet Kaur
Mtech Scholar (CSE)
CTIEMT,Shahpur
Jalandhar (Punjab)

Pooja
Assitant Professor (CSE)
CTIEMT, Shahpur
Jalandhar (Punjab)

Varsha
Assitant Professor(CSE)
CTIEMT, Shahpur
Jalandhar (Punjab)

ABSTRACT
Video Watermarking is a major technique of data hiding and maintain the originality of the images and videos. The major issues regarding information are raised about fake, frauds and pirated videos etc. these issues are overcome with the help of video watermarking concept. It also provides copyright protection and authenticity to the owner of the digital objects. It helps to keep the imperceptibility of the videos. The main aim of this paper is to give the review about general concept of video watermarking which includes its types, features, applications, techniques and various attacks applied on video files to check their authentication level.

General Terms
Data hiding, Watermarking, Robustness, Quality, Human Visual System (HVS)

Keywords
Video Watermarking, LSB, DCT, DWT, SVD, Watermarking Attacks

1. INTRODUCTION
Today word is full of technology i.e. the information or data can easily share or transfer over the internet and this is the major reason to protect information or data from the hackers is difficult. It also developed some issues like piracy, fraud, fake and misused of the information. To overcome this problem, with the help of data hiding techniques such as cryptography, steganography and watermarking. Watermarking is embed or insert into image, audio and video in such a way of doing which cannot be discover by HVS and maintain the quality of the information or data after extraction process.

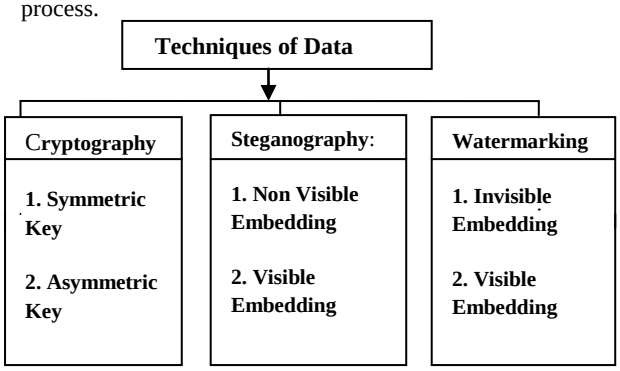

Fig 1: Classification of data hidden techniques

1.1 Watermarking
Watermarking is like a signature, which indicated the real owner of the digital objects and helps to maintain the imperceptibility of the multimedia objects. It protected our data or information from the hackers or unauthorized persons and Stop the reproduction of the film with the help of copy right protection. Watermarking is number of bits inserted into the multimedia object which helps to recognizing the copy right information. The word watermark is generated from the German term wessmark, which mean to resemble effect of water on paper. The watermark is embedded in such a manner which cannot be noticed by a person and also maintain the quality of original digital multimedia objects.

1.2 History of Video Watermarking
In ancient years, watermark first paper was developed by china. But later on watermark paper was developed by Italy in 13^{th} century but this paper did not published. In 18^{th} century Europe and America had been the first countries which used watermarks to indicate the original sheet and after that it also used on currency notes, for example, $(sign of dollar appear on the currency notes). It was firstly coined by Andrew Tirkel and Charles Osborne by 1992. And now all over world is use watermarking for securing information or data from the misused.

1.3 Cryptography Vs Watermarking
Cryptography is basically used to protect the content of message. It is also used to secure communication when third party is present. Cryptography is generated from the Greek word. Crypto means hidden and graphy means written. The aim of cryptography is converting plain text into cipher text and cipher text into plain text. But once the message is decrypted it doesn't provide security. Cryptography technique is not robust against attacks. But in case of watermarking, we insert a message in a video in a manner which cannot be removed or identify by a person. Watermark is highly robust against various attacks and hackers could not damage the information. It helps to enhance the imperceptibility of all the digital objects.

1.4 Watermarking Vs Steganography
In watermarking, the information is related to digital objects to be secured or to its owner. Steganography is used just to hide a message. Watermarking is one to many communications (for example, movies) while in case of steganography is one to one communication (for example, sender to receiver). Both are different in robustness criteria, steganography is deal with detection of hidden message. But watermarking deal with removed by a piracy.

2. CLASSIFICATION OF WATERMARKING
Digital watermarking can be characterized into four types:

2.1 According to human

It can be classified into two types visible and invisible watermarking. Visible watermarking is those in which watermark is detected by human eyes, for example, brands name. On the other hand, invisible watermarking is not recognized by human eyes.

2.2 According to type of media

It is based on four types:

a) Text file watermarking (.TXT)

b) Image file watermarking (.JPEG)

c) Video file watermarking (.AVI)

d) Audio file watermarking (.MP3)

2.3 According to extraction process

It can be divided into three extraction algorithm. These are as follow:

a) Blind algorithm: In which original data is not need to recover the watermark video. It need secret key.

b) Semi blind algorithm: It is the combination of both blind and non blind algorithm. It require secret key and watermark bit to recover video.

c) Non blind algorithm: It is only required an original video to recover a watermark video with secret key.

3. VIDEO WATERMARKING

Watermarking is also embedded in digital signals to protect audio or video from piracy, duplication. Watermark is embedded in a host signals in such a way which can't easily remove. It is used to solve problems of illegal copying and real ownership identification. It is used to embed watermark in the cover video in a manner which can't be find out by human visual system and not be remove from video. It used to hold the quality of video. The main goal of video watermarking is robustness, security, data payload size and imperceptibility.

3.1 Types of video watermarking

3.1.1 Symmetric and Asymmetric watermarking: Symmetric watermarking are those in which we used a same key for embedding and extraction process. But in case of asymmetric, we are used a different key for embedding and extracting watermarking, for example, passport .the owner of passport written his name twice on passport. One name is written in the normal text and second name is written in the hidden manner behind the passport images. If someone tries to misuse of passport by replacing owner images than he/ she can easily catch by hidden signatures of the owner.

3.2.2 Visible and Invisible watermarking: Visible watermarking are those which is find out by the human visual system. It is embedded in media, for ex, company logo. Invisible watermarking are those watermarking which are embedded into media file and it can't be detected by persons. It can be embed or extract using the algorithms. It is highly robust against different types of attacks.

3.1.2 Robust and fragile watermarking: Robust watermarking is a strong type of watermarking. It doesn't remove watermark when watermarked content is modified or remove, for ex, finger printing. In case of, fragile watermarking is a weak type of watermarking. It can easily remove when watermark content is modified, for ex, generalized bar codes and document like certificate.

3.2 Process of video watermarking

Video watermarking process is based on two steps i.e. embedding and extraction process.

3.2.1 Embedding process

Watermark is embedded into a video by using embedding algorithm to generate a watermark video. It is performed at sender side.

3.2.2 Extraction Process

It is a reverse process. This process is used to extract the watermark from the watermark video and obtain the original video. It is performed at receiver side.

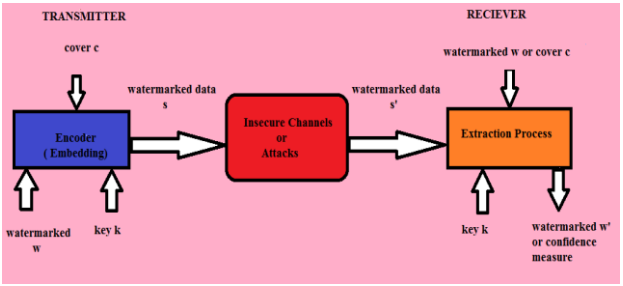

Fig 2: Embedding and Extracting process of Watermark

3.3 Feature's of Video Watermarking

Video watermarking has four major characteristics i.e. are robustness, imperceptibility, data payload size or capacity and security.

3.3.1 Robustness

The basic purposes of robustness protect the embedded watermark secure to the information from the hackers. Embedded watermarks present in the video even after the attacks. Watermarks could be removed intentionally or unintentionally by simple image processing operations like contrast or enhancement brightest gamma correction etc. Hence watermarks should be robust against variety of such attacks.

3.3.2 Imperceptibility

Imperceptibility means invisible. It is the concept in which after embedding a watermark in the original video no one can be able to detect the difference between original and watermark video. Imperceptibility is used to improve the visual quality of video.

3.3.3 Security

Watermark is basically used to secure the multimedia digital objects from third party or hackers. It can be enhance by using encryptions method. Security can also be checked by three applications i.e. certification (for ex, identity card or passports), authentication (this application is indicate changes in video) and conditional access.

3.3.4 Data payload size or capacity

How much data is embedded in a host signal is known as data payload size. Watermarked concept is also based on granularity. The total amount of information which is inserted

in watermark is known as capacity.

3.4 Application of Video Watermarking

a) Copyright Protection: It is used to prove the ownership. Copyright protection means video is used by only authorization persons who have permission to use it. It is basically used to remove the piracy from the film industry by using company logo.

b) Meta Data Insertion: It gives the information data about data. For example, passport carried DOB or name of owner.

c) Digital Fingerprinting: Its basics purpose to trace back a malicious user. The owner of video embedded a watermark into video to find out a customer who breaks there rules or license contract by copying the secure information and supply to hackers or third party.

d) Broadcast Monitoring: T.V is the good example of broadcasting because we just provided the code to station and this code is embed into media. This media is transmitted by the television and after that several geographic service channels are located to determine whether the code is broadcast or not.

e) Content Authentication: The purpose of this application is used to confirm or find out the truth of data by using govt ID'S or documents.

4. QUALITY METRICES

This is used to calculate the robustness, security and imperceptibility of the video.

4.1 Mean Square Error

$$\text{MSE}=\frac{1}{PQ}\sum_{i=1}^{P}\sum_{j=1}^{Q}(a(i,j)-b(i,j))^2 \quad (1)$$

MSE is used to measure the error ratio between original video and watermark video. Low the value of MSE, indicate a good quality of video.

4.2 Peak Signal to Noise Ratio

It is inversely proportional to the MSE. It is measured in decibels unit.

$$\text{PSNR}=10log_{10}\frac{255}{\sqrt{MSE}} \quad (2)$$

4.3 Bit Error Rate

The value of BER is closer to zero show algorithm is highly reliable and secure. It also measure with decibel units.

$$\text{BER}=\frac{1}{PSNR} \quad (3)$$

4.4 Structural similarity index metric

It is used to measure the similarity between original and watermark video. It is inverse relationship b/w SSIM and MSE. It also gives the information about the structure of the object.

$$\text{SSIM}=\frac{1}{MSE} \quad (4)$$

5. TECHNIQUES OF WATERMARKING

Video watermarking techniques is basically divided into two domains i.e. spatial or temporal domain. In spatial domain, watermark is directly embedded in host video. Least significant bit is the concept of spatial domain. In transform domain, we changes or modify the pixel value of the host video for embedding watermark. DCT, DWT is a methodology of transform domain.

5.1 Least Significant Bit

In LSB, the hidden information is embedded into the last bits of the pixels. Each pixel has 8- bit sequence and watermark is embedded in the last bit of selected pixel. LSB is easy to implement and less computational. But it doesn't robust against attacks is major drawback of LSB. For example: if W is a watermark, we want to embed in image. Firstly convert into ASCII code and then convert into binary values. After this, embed bits one by one in between the image bits.

Cover Image	**11001010**	**00110101**	**00011010**	**00000000**
Hidden Data	**01**	**01**	**10**	**11**
Wmrk Image	**11001011**	**00110010**	**00011100**	**00000011**

Fig 3: Example of LSB

5.2 Discrete Cosine Transform

DCT is used to express data in frequency space rather than amplitude space. Frequency space means analysis of mathematical function or signal with respect to frequency rather than time. DCT is divided into different frequency bands but middle frequency bands are used to embed the watermark. This technique is more robust than LSB. But this technique is expensive and weak against geometric attacks scaling, cropping etc.

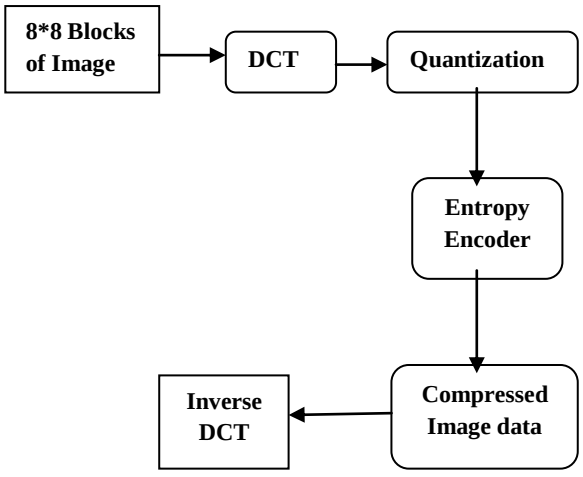

Fig 4: Process of DCT

5.3 Discrete Wavelet Transform

This technique is larger options of signal processing. This technique is basically divided into two parts i.e. low or high frequency parts. Low frequency parts again split into low and high frequency parts. We basically embed watermark into

1high frequency bands because it is less sensitive to human eyes. This technique is highly secure and robust against attacks. It also provided a good visual of video.

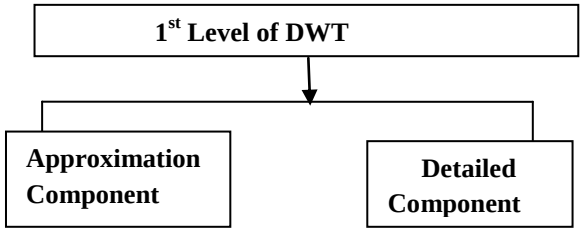

Fig 5: 1st level DWT

In approximation component, is just to represent the lower pixels of image. On the other hand, detailed component is used to represent the horizontal, vertical and diagonal component of an image.

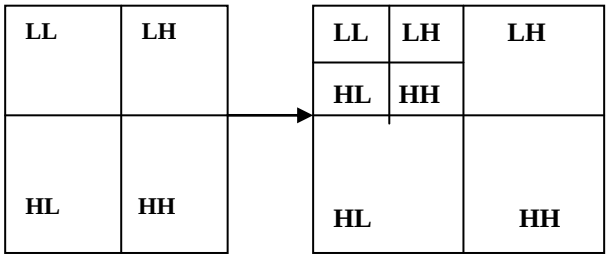

Fig 6: 2nd level DWT

In 2nd level DWT, image divided into four parts low, horizontal, vertical and high pass filter. This process is continued a multiple times.

5.4 SINGULAR VALUE DECOMPOSITON

Singular value decomposition is a style of extracting algebraic feature from an image. It is provide highly stability because when, embed a watermark in SVD matrix of an images, doesn't provide large variation. This technique is invented in 1956. SVD is also used in case of face recognition, compression and data mining. Mathematics formula for SVD is:

$$A = \begin{bmatrix} \\ U \\ \\ \end{bmatrix} \begin{pmatrix} W_1 & 0 & 0 \\ 0 & W_2 & 0 \\ 0 & 0 & W_n \end{pmatrix} \begin{bmatrix} \\ V \\ \\ \end{bmatrix}^T$$

Where,

$A=UWV^T$
U is m*m matrix
W is m*n diagonal matrix
V is n*n matrix

LSB	DCT	DWT	SVD
Not secure.	Expensive and less secure as compared to DWT.	Highly secure and flexible in nature.	SVD can be used to compute optimal low rank approximation of arbitrary matrixes.
Doesn't robust against attacks	Weak against geometrical attacks.	Highly robust against attacks and compression ratio.	It is provide good stability and easily to calculate.

Fig 6: Differences of Techniques

6. ATTACKS OF VIDEO WATERMARKING

The main goal of the attackers to destroy the important information and used it for an own purposes. Attackers want to destroy the information or make it unreadable for the receiver by applying some attacks on videos. Attackers attempt to damage or destroy watermark for the purposes of use with having to pay duplicity to the originator of the content.

6.1 Types of Attacks

6.1.1 Collusion Attack

This attack is used to construct a copy without watermark. In this attack, hackers used a number of copies of one piece of media to generate a watermarked to construct a copy without watermark. This type attack is mostly applied in film industry to make a pirated audio, videos.

6.1.2 Lossy Compression Attack

In this attack, quality degradation is done with loss of data. JPEG & MPEG are two examples of lossy compression attack.

6.1.3 Active Attack

This attack is basically used to remove or make it undetectable the watermark from video by applying geometrical transformation like cropping, scaling, rotating and resizing.

6.1.4 Passive Attack

Attackers try to recognized watermark is present or not into the video without any damage.

6.1.5 Geometrical distortion

These types of attacks are specific for images, videos. For examples are rotation, scaling, translation and cropping.

6.1.6 Ambiguity Attacks

This attack is applied to confuse the detector by designing a fake watermark from watermarked work. Thus it provides false information in the ownership of content.

6.1.7 Cryptographic Attacks

These attacks are used to determine the way to remove the inserted watermark information, and cracking a security of watermarking. These attacks have purpose to finding hidden information. For example, system attacks

7. CONCLUSION

Video watermarking is an active research field with wide range of application. Watermarking is used to protect the ownership of video from hackers and various attacks. Video watermarking is more robust, transparency and secure as compared to cryptography. Embedded and extracted a watermark into video by using various watermarking

algorithm. So in future work, to embed watermark inside the video to avoid criminal activities like fraud, piracy etc. It is very important aspects to stop misuse of the information and helps to provide a copyright protection and increase the security of the information or data.

8. ACKNOWLEDGMENTS

We like to thanks to the earlier work regarding different video watermarking that contribute the work made in this paper. All work done in this paper will help to the new researchers for future work on watermarking.

9. REFERENCES

[1] Amrinder Singh, Sukhjit Singh "A Robust Video Watermark Embedding and extraction Technique Based on Random Frame Selection" IJCA Vol. 2, NO.2, Feb 2014.

[2] Tanima Dutta, Arijit Sur, Sukumar Nandi, "A Robust Compressed Domain video watermark P-frame with Controlled Bit Rate Increase", IEEE 2013.

[3] Hamid Shojanazeri, Wan Azizun Wan Adnan, Sharifah Mumtadzah Syed Ahmad, M. Iqbal Saripan , "Analysis of Watermark Techniques in Video", IEEE 2011. pp 486-492.

[4] G.Prabakaran, R.Bhavani, M.Ramesh," A Robust QR-Code Video Watermarking Scheme Based on SVD and DWT Composite Domain", IEEE International Conference On Pattern Recognition, Informatics And Mobile Engineering (Prime), February 2013. pp 251-257.

[5] Mrs.Anita Jadhav, Mrs.Megha Kolhekar," Digital Watermarking in Video for Copy Right Protection" IEEE International Conference on Electronic Systems, Signal Processing and Computing Technologies, 2014. pp 140-144.

[6] Harshita Rawat, Ashwani Kumar, Satendra Kumar," Robust Digital Image Watermarking Scheme for Copyright Protection", Volume 75, No.18, August 2013.pp 27-32.

[7] Bhavna Goel, Charu Agarwal," An Optimized Un-compressed Video Watermarking Scheme based on SVD and DWT", IEEE 2013. pp 307- 312.

[8] Osama S.Fargallah," Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain", Elsevier 2012. pp 189 – 196.

[9] Majid Masoumi[a], Shervin Amiri[b],*," A blind scene-based watermarking for video copyright protection", Elsevier 2012. pp 528 – 535.

[10] Angshumi sarma, Amrita Ganguly," An Entropy based Video Watermarking Scheme" International Journal of Computer Applications, Volume 50, No.7, July 2012, pp33 –37.

[11] Jonathen Blake, Shahram Latifi,"Digital Watermarking Security" Defence Science Journal, Volume 61, NO.5, September 2011, pp 408-414.

[12] http://www.slideshare.net/vasanthimuniasamy/watermarking-lecture-4-16918992

[13] http://www.slideshare.net/qaisarayub/watermarking-inimageprocessing?related=1

[14] Gaurav Bhatnagar[*], Balasubramanian Raman[1]," Wavelet packet transform-based robust video watermarking technique" Indian Academy of Science, volume 37, no.3, June 2012, pp371-388

[15] Gopika V Mane[*], G.G. Chiddarwar**," Review Paper on Video Watermarking Techniques" International journal of Scientific and Research Publication, Volume 3, NO.4, April 2013. pp 1-5.

[16] http://www.slideshare.net/rupareliab14/digital-watermarking-8479007?related=3

[17] Ghassan.N Mohammed, Azman Yasin, Akram M.Zeki," Digital Image Watermarking, Analysis of Current Methods", IEEE International conference on Advanced Computer Science Application and Technologies, 2013. pp 324-329.

[18] Nilesh Kumar Dubey, Shishir Kumar," A Review of Watermarking Application in Digital Cinema for Piracy Deterrence", IEEE International Conference on Communication Systems and Networking Technologies, 2014. Pp 626-630.

[19] Min Liu," Study of Digital Image Watermarking", IEEE International Conference on Computer Science and Electronics Engineering, 2012. pp 77-80.

[20] Manekandan.GRS, Franklin Rajkumar .Vs," A Robust Watermarking Scheme for Digital Video Sequence using Entropy and Hadamard Transformation Technique", International Journal of Computer Application, volume 41, NO.18, March 2012. pp 24-31.

[21] Saeed Rastegar[a,*], Fateme Namazi[a], Khashayar Yaghmaie[b], Amir Aliabadian[a] ," Hybrid watermarking algorithm based on Singular value Decomposition and Radon Transform", Elsevier 2010. pp 658-663.

[22] Radu O. Preda[*], Dragos N. Vizireanu[1]," A robust digital watermarking scheme for video copyright protection in the wavelet domain", Elsevier 2010. pp 1720-1726.