Volume 2, Issue 11, November 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Digital Video Watermarking

Renuka.S.Mathapati
Dept of Computer Science
JSS SMI College, Vidyagiri
Dharwad, India

Jagadeesh.Pujari
Dept of Information Science
SDMCET, Davalgiri
Dharwad, India

Abstract— Watermarking is a technique used to hide data or identifying information within digital multimedia With the advent of internet ,creation and delivery of digital data (images, video and audio files) has grown many fold. With this, issues like protection of rights of the content and proving ownership arises. Digital image watermarking came as a technique and a tool to overcome shortcomings of current copyright laws for digital data .To prove ownership and protect right, a watermark is embedded in data but to save watermark from counterfeiters we need to find locations which are invariant to all kind of attacks(rotation ,expansion ,compression ,cropping ,filtering and blurring).Generally by image watermarking one is hiding a message signal into a host signal ,without any perceptual distortion of the host signal. We are developing a web based application on Digital Image Watermarking.

Keywords— Data encryption algorithm, Blind watermarking, LSB, encryption, decryption

I. INTRODUCTION

The recent growth in computer networks, and more specifically, the World Wide Web, has allowed multimedia data such as videos to be easily distributed over the internet. However, many publishers may be reluctant to show their work on the Internet due to a lack of security. Although digital data has many advantages over analog data, services providers are reluctant to offer services in digital form because they fear unrestricted duplication and dissemination of copyrighted material. Because of possible copyright issues, the intellectual property of digitally recorded material must be protected. To provide copy protection and copyright protection for digital audio and video data, two complementary techniques are being developed namely encryption and watermarking. Watermarking deals with embedding information like name of the creator, status, recipient, etc. into the host data in such a way that it remains transparent or undetectable. The watermark information should be embedded in such a way that this should not be detectable and removable even after many spurious or innocuous attempts. Watermarking can be done for any form of digital data- text, image, audio, or video where copyright needs to be protected.

Until recently encryption has been the primary tool available to help protect copy right of owners' contents such as movies, songs, photographs and the like [1]. Encryption protects the content during transmission from sender (host) to receiver. However, after receipt and subsequent decryption, the information remains no longer protected and is prone for danger of piracy .Watermarking techniques compliment encryption by embedding into the original data in such a way that it always remains present. A watermark is a secret code or image or pattern of bits incorporated into an original image, which acts to verify both the owner and content of the image. Such a watermark, for instance, is used for copyright protection, fingerprinting, indexing, broadcast monitoring, data authentication, and data hiding [1].According to the human perception, the digital watermarks are divided into two different types namely Visible and Invisible [7]. In Visible watermarking technique, the watermark is visible to the casual viewers. Visible watermarks change the image altogether such that the watermarked image is totally different from actual image.

II. OBJECTIVE OF WATERMARKING

The main goal of watermarking is to hide a message m in some image, audio or video (cover) data d, to obtain new data d practically indistinguishable from d, by people, In such a way that an eavesdropper cannot remove or replace m in d. Watermarking hides the message in one to many communications. Watermarking is adding "ownership" information in multimedia contents to prove the authenticity. For digital watermarking of video, different characteristics of the watermarking process as well as the watermark are desirable. These requirements are:

1. Invisibility: The digital watermark embedded into the video data should be invisible to the human observer.

2. Robustness: It should be impossible to manipulate the uncompressed or compressed video, at the same time, significantly thereby reducing its commercial value. Such operations are, for example, addition of signals, cropping, lossy compression, frame averaging, frame dropping and collusion.

3. Fidelity: A watermark is said to have high fidelity if the degradation it causes is very difficult for a viewer to perceive. However, it only needs to be imperceptible at the time that the media is viewed. If we are certain that the media will be seriously degraded due to other means such as transmission before being viewed, we can rely on that degradation to help mask the watermark.

4. Computational Cost: Different applications require the embedders and detectors to work at different speeds. In broadcast monitoring, both embedders and detectors must work in real time so they need to be fairly fast and should have low computational complexity. On the other hand, a detector for proof of ownership disputes, which are rare, and its conclusion about whether the watermark is present is important enough that the user will be willing to wait.

5. Interoperability: Even though many applications call for watermarking in the compressed video could compatibly be watermarked without having to encode it first. Also, the watermark should sustain the compression and decompression operations.

III. TYPES OF WATERMARK

1. Visible watermarks: Visible watermarks are an extension of the concept of logos. Such watermarks are applicable to images only. These logos are inlaid into the image but they are transparent. Such watermarks cannot be removed by cropping the centre part of the image. Further, such watermarks are protected against attacks such as statistical analysis. The drawbacks of visible watermarks are degrading the quality of image and detection by visual means only. Thus, it is not possible to detect them by dedicated programs or devices. Such watermarks have applications in maps, graphics and software user interface.

2. Invisible watermark: Invisible watermark is hidden in the content. It can be detected by an authorized agency only. Such watermarks are used for content and/or author authentication and for detecting unauthorized copier.

3. Public watermark: Such a watermark can be read or retrieved by anyone using the specialized algorithm. In this sense, public watermarks are not secure. However, public watermarks are useful for carrying IPR information. They are good alternatives to labels.

4. Fragile watermark: Fragile watermarks are also known as tamper-proof watermarks. Such watermarks are destroyed by data manipulation.

5. Private watermark: Private watermarks are also known as secure watermarks. To read or retrieve such a watermark, it is necessary to have the secret key.

6. Perceptual watermarks: A perceptual watermarks exploits the aspects of human sensory system to provide invisible yet robust watermark. Such watermarks are also known as transparent watermarks that provide extremely high quality contents.

7. Bit-stream watermarking: The term is sometimes used for watermarking of compressed data such as video.

8. Text document watermarking: Text document is a discrete information source. In discrete sources, contents cannot be modified. Thus, generic watermarking schemes are not applicable. The approaches for text watermarking are hiding watermark information in semantics and hiding watermark in text format.

IV. PROPOSED METHODS

In this project, wee have proposed techniques that extend the conventional spatial domain LSB watermarking technique and blind watermarking in the discrete wavelet domain.

1. LSB Technique:

In the LSB techniques for watermarking, the watermark bits are inserted into the least-significant bit of the original video to obtain the watermarked video. In this method, the input video is first divided into blocks according to the size of watermark video. Input image need not be of same size as watermark video. LSB plane is generated from the watermark video. Each bit of LSB plane is added to the least significant bit of the gray scale video to get the watermarked vide. For example, the 9 pixels of a video considered are shown in Fig. 1 (a). Fig. (b) Shows the LSB plane obtained from original data.

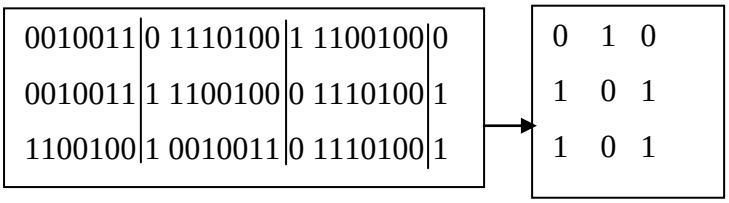

Fig.1 Plane a) original data b) LSB

Let the character A be embedded on this plane. The binary value (ASCII code) for A is 10000011, which acts as watermarked message. Inserting the binary value for A in the 9 pixels of original data, the new LSB plane is obtained by replacing original bits with 8 bits of the character and leaving the last bit unchanged in the LSB plane as shown in Fig.2 (a) and (b) gives new LSB plane.

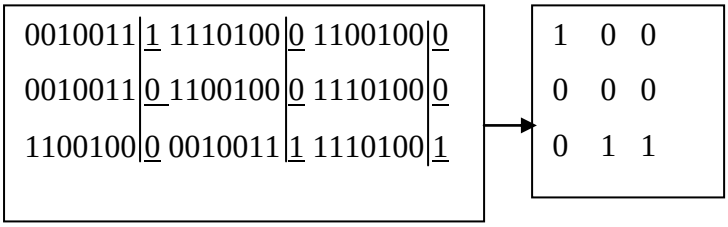

Fig.2 a) After LSB, adding plane b) new LSB plane

Binary value for letter A

The watermarking process is shown in fig 3:

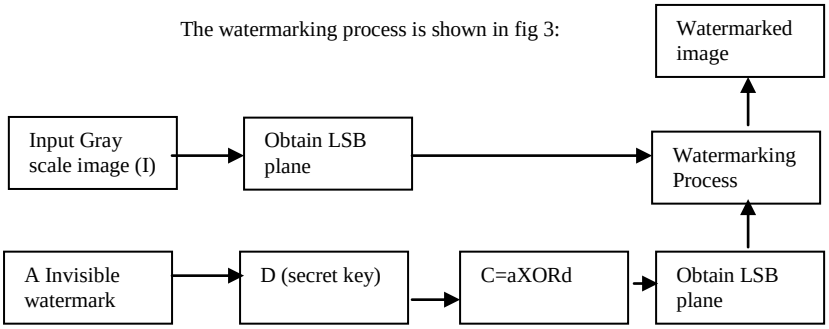

Fig 3 LSB watermarking process

In this work, in order to insert and scramble the watermark, we have considered gray scale image I (m, n) of size m x n.

An invisible watermark a is inserted without changing the size of I. The image I is first divided into blocks of size (ixj) and the watermark insertion procedure is applied independently to each block of the image. Let matrix $a_{m, n\ be}$ a binary image used as an invisible watermark. The watermark need not be of same size as I.A matrix $d_{m,n}$ is generated from a m,n using shift operation to generate a sequence of m bits. These m-bit sequence is used to scramble the watermark image $a_{m,n}$ by an exclusive-OR operation on $a_{m,n}$ with $d_{m,n}$ to form $c_{m,n}$

C(m,n)=a(m,n) XOR d(m,n).

$c_{m,n}$ is the new LSB plane that is inserted into the image. This is repeated until the watermark bits are completely utilized. The resulting bits are added to the original image to obtain the watermarked image. We have selected $d_{m,n}$ is used as a secret key for watermark extraction from the I (mxn) blocks. Through XOR operation, LSB plane with $d_{m,n}$ the watermark image $a_{m,n}$ is recovered. The advantage of this method is that any change in the image is easily detected. Security of this technique depends on the secret key not the algorithm.

2. BLIND WATERMARKING

The other is DWT watermarking technique. In this type, each level of decomposition produces four bands of data, one corresponding to the low pass band (LL) , and three other corresponding to horizontal (HL), vertical (LH), and diagonal (HH) high pass bands. The segmentation is used as a pre-processing step in the blind watermarking .Thus, the segementation when performed using two different final segmented images. The resulting segmented image is decomposed to obtain the DWT coefficients. The message is reshaped into vector. That vector is inserted into the three sub bands [LH, HL, HH] to get the watermarked video. Fiqure 4 shows original video and resulting video after DWT watermarking. The DWT watermarking is also called blind watermarking.

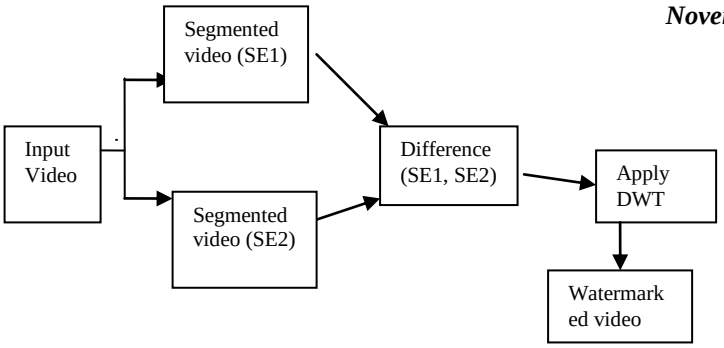

Fig 4 Blind watermarking based on segmentation

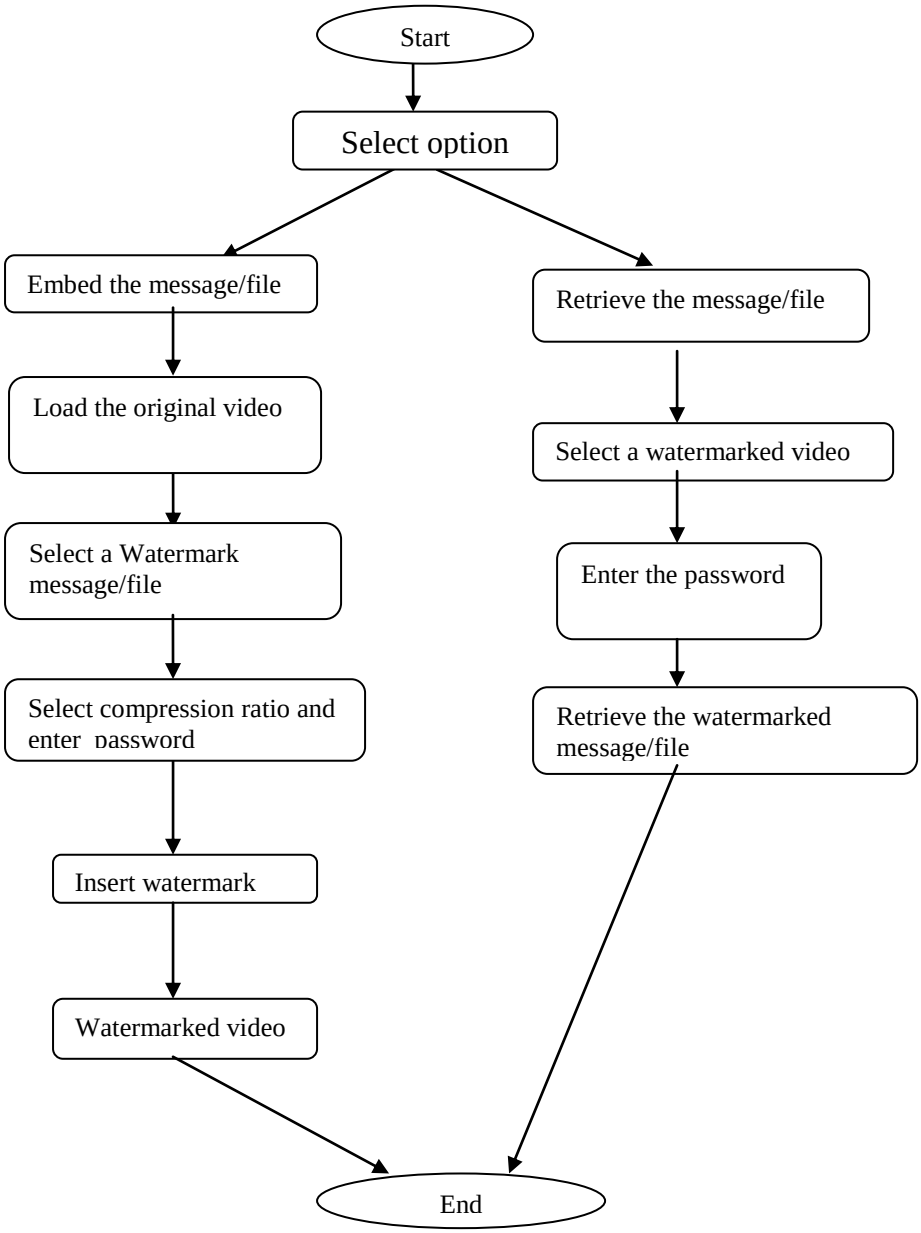

Fig 5 Proposed Watermarking

3. DES Algorithm

Data Encryption Standard (DES) is a widely-used method of data encryption using a private (secret) key that was judged so difficult to break by the U.S. government that it was restricted for exportation to other countries. For many years, and among many people, "secret code is making" and DES have been synonymous. The Data Encryption Standard (DES) is a block cipher that uses shared secret encryption. It was selected by the National Bureau of Standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

DES applies a 56-bit key to each 64-bit block of data. The process can run in several modes and involves 16 rounds or operations. Although this is considered "strong" encryption, many companies use "triple DES" which applies three keys in succession. This is not to say that a DES-encrypted message cannot be "broken". Early in 1997, Rivest-Shamir-Adleman, owners of another encryption approach, offered a $10,000 reward for breaking a DES message. A cooperative effort on the internet of over 14,000 computer users trying out various keys finally deciphered the message, discovering the key after running through only 18 quadrillion of the 72 quadrillion possible keys. Few messages sent today with Des encryption are likely to be subject to this kind of code-breaking effort.

V. IMPLEMENTATION OF DVW

While reviewing number of watermarking schemes based on LSB, it has been noticed that some algorithms are used for different types of spatial domain for embedding watermark. In this developed algorithm watermark is embedded in spatial domain with some pre-processing before and after the LSB technique. In all spatial domain watermarking schemes, there is a conflict between robustness and transparency. If the watermark is embedded in perceptually most significant components, the scheme would be robust to attacks but it would be difficult to hide the watermark. On the other hand, if the watermark is embedded in perceptually insignificant components, it would be easier to hide the watermark.

Algorithm to embed the Watermark as text message

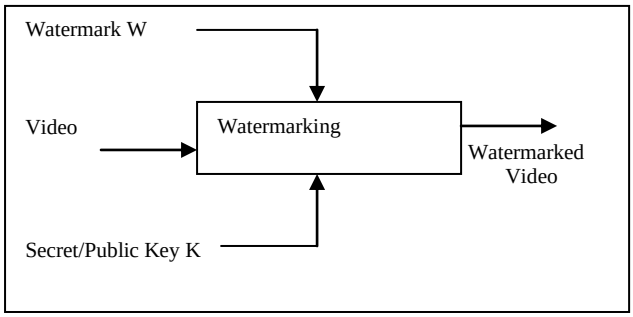

Fig 6. Block diagram of watermarking

Steps :

1) Get the original (colour) image as bitmap format.
2) Enter the plain text as string
3) Find the object tag as message in the GUI and get its string value where we save the plain text.
4) Change the string value to its equivalent binary vale.
5) Change the rgb (colour) image to gray image for finding the image edges easily.
6) Taking the edges of 8 consecutive pixel binary values for saving the binary equivalence of the text message which is to be hidden.
7) In this, steganalysis method, binary equivalent of the message (to be hidden) is distributed among the LSBs of each pixel.

Algorithm to retrieve the Watermark as text message

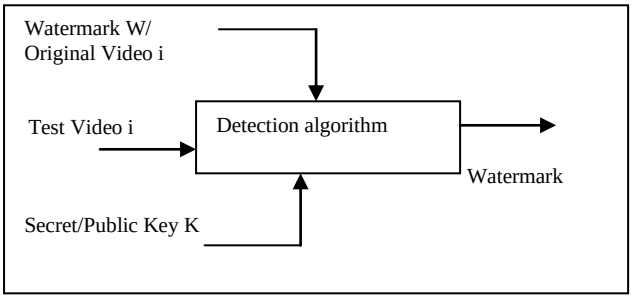

Fig 7 Block diagram of watermark extraction

Steps:

1) Read the watermarked (stego) image, with the watermark as text
2) Finds the object tag as Cipher Text in the GUI and get its string value
3) Convert the string to number for getting their length which is the stego key.
4) Change the rgb (colour) image to gray image for finding the image edges easily.
5) It checks and decodes all the edge pixel of the Least Significant bit alone.
   5.1) It gets the pixel value of the edge pixel (in decimal) value
   5.2) Change the decimal value to binary value of the Least Significant Bit alone.
   5.3) finally, we change the binary values to the characters.
6) Retrieved the message successfully without the help of Original video

VI. ATTACKS ON WATERMARKS

In the field of digital watermark, there are various categorizations of attacks on watermarks. These can be categorized as follows

A. *Subtractive Attack:* In this attack the adversary or malicious user tries to detect the presence, location of the watermark and tries to extract it from the host. An effective subtractive attack is one where the cropped object has retained enough original content to still be of value.

B. *Distortive Attack:* If an adversary or malicious user applies some distortive transformation uniformly over the object in order to degrade the watermark so that it becomes undetectable/unreadable. An effective distortive attack is one where one can no longer detect the degraded watermark, but the degraded object still has value to the adversary.

C. *Additive Attack:* An adversary or malicious user can augment host by inserting his own watermark W (or several such marks) . An effective additive attack is one in which adversary's mark completely overrides original mark, so that it can no longer be extracted or it is impossible to detect that the original mark temporally precedes the adversary's mark.

D. *Filtering:* Low pass filtering, for instance, does not introduce considerable degradation in watermarked images, videos or audio, but can dramatically affect the performance, since spread-spectrum like watermarks have non negligible high-frequency spectral contents.

E . *Cropping:* This is a very common attack since in many cases the attacker is interested in a small portion of the watermarked object, such as parts of a certain picture or frames of a video sequence. With this in mind, in order to survive, the watermark needs to be spread over the dimensions where this attck takes place.

E. *Compression:* This is generally an unintentional attack which appears very often in multimedia applications. Practically all the audio, video and images that are currently being distributed via Internet have been compressed. If the watermark is required to resist different levels of compression, it is usually advisable to perform the watermark insertion task in the same domain where the compression takes place. For instance, DCT domain image watermarking is more robust to JPEG compression than spatial domain watermarking.

F. *Rotation and Scaling:* It has been very successful with still images.
Correlation *based* detection and extraction fail when rotation or scaling is performed on the watermarked image because the embedded watermark and the locally generated version do not share the same spatial pattern anymore. Obviously, it would be possible to do exhaustive search on different rotation angles and scaling factors until a correlation peak is found, but this is prohibitively complex.

G. *Statistical Averaging:* An attacker may try to estimate the watermark and then 'unwatermark' the object by subtracting the estimate. This is dangerous if the watermark does not depend substantially on the data.

VII. BENEFITS OF DIGITAL WATERMARKING

I. *Creates a persistent identity to enable content to be managed more effectively and help enable new business models, greater security and broader consumer choice*

---Readable by computers/devices supporting numerous applications while remaining imperceptible to humans

---Enables content identification or rights enforcement in digital or analog content distribution

---Communicates copyright information and associated rights.

II Applicable to all content types

---Photos and images, secure documents, advertisements, TV programming, movies, music etc.

---Offers copyright stakeholder's persistent content identification and authentication

III Robust to standard content processing techniques

---A/D and D/A conversion, cropping, scaling, compression, encryption/decryption, printing and scaling, etc.

IV .Adaptable to all media types, platforms, distribution and transmission methods

---Complementary and enhanced security for encryption/decryption based DRM systems.

V. Supports new business models and consumer experiences by enabling copyright stakeholders the freedom to embrace and balance various management, protection and delivery choices.

VIII. APPLICATIONS OF WATERMARKING

Watermarking methods are often evaluated based on the common properties of robustness, tamper resistance, and fidelity. However, examination of these properties without careful consideration of the application can often be misleading. The major applications include copy control, broadcast monitoring, fingerprinting, video authentication, copyright protection and enhanced video coding.

A. *Copy Control:* It is possible for recording and playback devices to react to embedded signals. In this way, a recording device might inhibit recording of a signal if it detects a watermark that indicates recording is prohibited. Watermarking here complements the available technologies in which the information is secured in the header and prevents the copying of data when it is converted into analog.

B. *Broadcast Monitoring:* Many valuable products are distributed over the television network. As a result, a broadcast surveillance system has to be built in order to check all broadcasted channels. We can use watermarks for broadcast monitoring by putting a unique watermark in each video or sound clip prior to broadcast. Automated monitoring stations can then receive broadcasts and look for these watermarks, identifying when and where each clip appears.

C. *Fingerprinting:* Electronic distribution of content allows each copy distributed to be customized for each recipient. This allows a unique watermark to be embedded in the copy of each customer like customer name or ID. This allows the distribution companies to track down the source of illegal copy in case of a leakage. Another important issue is the illegal copying of brand new movies projected onto cinema screens by means of a handhold video camera. A watermark can be embedded during the show time identifying the cinema, the presentation date and time. If the illegal copy created with a video camera is found, the watermark is extracted and the cinema to blame is identified.

D. *Video Authentication:* There are many applications in legal and medical imaging where it is important to preserve the content from tempering. Authentication can be carried out by storing the signature in header field but this header will still be prone to tampering. A preferable solution to this problem is to embed the signature directly into the image using watermarking. This ensures that the signal stays with the image and any change made to the image will also propagate to the watermark.

E. *Copyright Protection:* The underlying strategy consists in embedding a watermark, identifying the copyright owner, in digital multimedia data. The rightful owner can show the watermark in case of a dispute. Watermarking algorithms are consequently required to be non-invertible in order to provide copyright protection services especially in cases of multiple ownership issues.

IX. CHALLENGES OF VIDEO WATERMARKING

The challenges for video Watermarking are as follows:

A. Video media is susceptible to increaser attacks than any other media
B. Video content is sensitive to subjective quality and Watermarking may degrade the quality.
C. Video compression algorithms are computationally intensive and hence there is less headroom for Watermarking computation
D. Video is bandwidth hungry and that is why it is mostly carried in compressed domain. Therefore, Watermarking algorithm shall be adaptable for compress domain processing.
E. For low-bitrate video, Watermarking poses additional challenges, as there is less room for watermark data.
F. During video transmission, frame drops are very usual. If watermark data spreads over many frames, in case of frame drops, watermark data may become irretrievable. Watermarking should be robust enough against this phenomenon.

X. FUTURE SCOPE

As a future scope the concept of Cryptography and Digital Watermarking can be combined to implement more secure Digital Watermarking system. We can experiment this watermarking technique in the frequency domain of various watermark application, whereas watermark as image itself. Also we can implement in other spatial domain techniques and cryptography algorithms for most advanced encryption technique to encrypt the messages.

XI. CONCLUSION

Digital Watermarking is emerging as a favourite technique over traditional encryption for digital rights management (DRM). A lot of research is still going on and new methods are emerging. Current methods for Digital Video

Watermarking are extension form image Watermarking and there is scope of more innovations. As more and more low-bit rate compression standards fir video are emerging, and with the progress of wireless technology, a lot of challenges are now thrown to Video Watermarking and simple extension of image Watermarking method would not be withstanding. This technology has a great future in store and is going to significantly change the way digital media is managed.

REFERENCES

[1] "Survey on Digital Video Watermarking Techniques and Attacks on Watermarks" T.Jayamalar et. Al. International Journal of Engineering Science and Technology Vol.2 (12), 2010, 6963-6967.

[2] "Perceptual Watermarking of Digital Video using the variable temporal length 3D- DCT", A Thesis Submitted in Partial Fulfilment of the Requirements for the Degree of M.Tech. By Vivek Kumar Agrawal.

[3] "Multi-Scale Morphological Image Segmentation Based Modified Watermarking Techniques" Basavaraj.S.Anami, J.D.Pujari, Rajesh Yakkundimath K.L.E, Institute of Technology, Hubli, INDIA.

[4] "Digital Watermarking for MPEG video", Author Biswajit Biswas, Tata elxsi engineering creativity.

[5] "A Short Summary of Digital Watermarking Techniques for Multimedia Data" F.Y. Duany I. Kingz Department of Computer Science & Engineering. The Chinese University of Hong Kang Shatin, N.T., Hong Kong, China.

[6] "Hardware Implementation Perspectives of Digital Video Watermarking Algorithms" Nebu John Mathai, *Student Member, IEEE,* Deepa Kundur, *Member, IEEE,* and Ali Sheikholeslami, *Member, IEEE. IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL 51, NO. 4, APRIL 2003.*

[7] www.wikipedia.com

