# Watermarking and Compression of Digital Video Using DNA Sequence

**Dr.S.A.Arunmozhi[1], J.Rohini[2], B.Pavithra[3], C.Rajathi[4]**
[1] Assistant Professor, Dept of Electronics and Communication
[2, 3, 4]Dept of Electronics and Communication
[1, 2, 3] Saranathan college of engineering, Tiruchirapalli-620012, TamilNadu, India

***Abstract-*** *The Video Watermarking is implemented in Web Based Application for protection of data. It is used for limiting the type of Digital Theft Protection. A 3D video by watermarking the Image-based Representations of a 3D video is stereoscopic, Depth-image-based Rendering and Multi-view Video Watermarking. A pirated copy of a digital video can now be easily distributed to a global audience. DNA sequence is used as a digital watermark, as the DNA sequences are unique and difficult to copy*

***Keywords***- Video Watermarking, Depth-image-based rendering, DNA sequence

## I. INTRODUCTION

Today digital media is available in a large scale, which can be easily copied and rapidly spread. Today digital data security covers such topics as access control, authentication, and copyright protection for still images, audio, video, and multimedia products. The watermarking techniques are categorized based on the domain in which the watermark is embedded.

Video piracy is the act of acquiring, copying and then selling or distributing a copyrighted video without the consent of the copyright owner. Over the last decade, online video piracy has become a significant concern for studios and movie producers. With the availability of high-speed broadband access and a multitude of Internet streaming sites, a pirated copy is readily accessible to a global audience for viewing online and downloading within just days of its release to theatres. A block diagram illustrating the unauthorized distribution of a copyrighted video is shown in Fig. 1. Usually, a movie is first released to theatres and then to digital versatile disk (DVD) after approximately sixteen weeks. Currently, camcorder theft is one of the most significant problems facing the film industry and is the single largest source of video piracy. When this type of theft occurs, a copy of a digital movie is captured from a large-screen movie theatre using a camcorder and then distributed worldwide via the Internet without any copyright protection.

## II. RELATED WORKS

### 1. Robust Histogram Shape-Based Method for Image Watermarking

Cropping and random bending are two common attacks in image watermarking. In this paper we propose a novel image-watermarking method to deal with these attacks, as well as other common attacks. In the embedding process, we first pre-process the host image by a Gaussian low-pass filter. Then, a secret key is used to randomly select a number of grey levels and the histogram of the filtered image with respect to these selected gray levels is constructed. After that, a histogram-shape-related index is introduced to choose the pixel groups with the highest number of pixels and a safe band is built between the chosen and non-chosen pixel groups. A watermark-embedding scheme is proposed to insert watermarks into the chosen pixel groups. The usage of the histogram-shape-related index and safe band results in good robustness. Moreover, a novel high-frequency component modification mechanism is also utilized in the embedding scheme to further improve robustness. At the decoding end, based on the available secret key, the watermarked pixel groups are identified and watermarks are extracted from them. The effectiveness of the proposed image-watermarking method is demonstrated by simulation examples.

A new image watermarking method that is robust to common attacks to deal with signal processing attacks, a Gaussian low-pass filter is employed to pre-process the host image such that watermarks will only be embedded into the low-frequency component of the host the image. To tackle geometric attacks (including cropping attacks and RBAs), a histogram-shape-related index is utilized to form and select the most suitable pixel groups for watermark embedding. Besides, a safe band is introduced between the selected pixel groups and the non-selected pixel groups to improve robustness to geometric attacks.

### 2. Time-Spread Echo-Based Audio Watermarking With Optimized Imperceptibility and Robustness

We present a time-spread echo-based audio watermarking scheme with optimized imperceptibility and robustness. Specifically, convex optimization based finite-impulse-response(FIR) filter design is utilized to obtain the optimal echo filter coefficients. The desired power spectrum of the echo filter is shaped by the proposed maximum power spectral margin (MPSM) and the absolute threshold of hearing (ATH) of human auditory system (HAS) to ensure the optimal imperceptibility. Meanwhile, the auto-correlation function of the echo filter coefficients is specified as the constraint in the problem formulation, which controls the robustness in terms of watermark detection. In this way, a joint optimization of imperceptibility and robustness can be quantitatively performed. As a result, the proposed watermarking scheme is superior to existing solutions such as the ones based on pseudo noise (PN) sequence or modified pseudo noise (MPN) sequence. Note that the designed echo kernel is also highly secure in that only with the same filter coefficients can one successfully detect the watermark. Experimental results are provided to evaluate the imperceptibility and robustness of the proposed watermarking scheme.

Watermark embedding regions and the trade-off between psychoacoustic model based imperceptibility control and the robustness against lossy compression are discussed. To study the robustness properties, we considered a comprehensive list of attacks which serve as a union set of all important attacks that have been considered in the existing works. The attacks are further categorized into basic and advanced attacks further; a rigorous definition of de synchronization attacks is given in this paper, which consists of 6 different attacks. Comprehensive evaluations of robustness against all the considered attacks are provided Current challenges for audio watermarking system design are revealed

### 3. A Literature Survey – Various Audio Watermarking Techniques and their challenge

Embedding a digital data into the host signal under perceptual constraints is called audio watermarking. Existing Literature in this field gives vast algorithms providing solutions to the audio watermarking constraints. A survey on different domains such as spatial domain, frequency domain and the hybrid domain of digital audio watermarking has been carried out in this paper. The algorithms that are implemented have been studied and reviewed, the challenges posed in this algorithms and their drawbacks have been presented in the paper. The best possible solution to them has been engrossed as future work in this survey**.**

I. Spatial domain,
II. Frequency domain,
III. Hybrid domain.

This section discusses the detailed review of existing audio watermarking techniques such as LSB replacement, spread-spectrum, echo hiding, patchwork, DWT.

The various existing audio watermarking techniques in different domains are spatial domain, frequency domain and hybrid domain. It is then concluded that different methods provide different solutions to audio watermarking problems. A comparative analysis of existing algorithms provides advantages and disadvantages of the algorithms. It is thus found that attacks such as TSM and Cropping are still a big challenge under high payload. In future, the focus will be to design a high payload audio watermarking robust against TSM and Cropping by integrating properties of different domains.

### 4. A Blind High Definition Video Watermarking Scheme Robust To Geometric and Temporal Synchronization Attack

Due to the availability of high speed online streaming sites, a pirated copy of a digital video can be easily distributed to a global audience. Technique based on the dual-tree complex wavelet transform that can protect this pirated digital video content. In this scheme, the watermark is embedded into the chrominance channel of the video frames to provide a high quality watermarked video. The watermark is detectable without reference video content as well as the original watermark which makes this method robust to temporal synchronization attacks such as frame dropping and frame rate conversion. The proposed method is also robust to geometric attacks such as arbitrary downscaling in resolution, rotation, up scaling, and cropping.

Any watermarking methods have been proposed to fulfil different requirements of digital video watermarking. A blind watermarking approach proposed in [embedded the watermark into the magnitude of level 3 and level 4 high- pass complex coefficients of a 4-level DT CWT of the luminance channel. Since, the watermark is embedded in the luminance channel; the quality of the watermarked video can-not be maintained. This method is robust to up scaling, rotation, cropping, and lossy compression but not to temporal synchronization attacks and arbitrary downscaling in resolution as the watermark was extracted only from the highest level coefficients of the DT CWT. Another approach was pro-posed in where the watermark is embedded into level 3high-pass complex coefficients of a 3-level DT CWT decomposition of the chrominance channel. This method

supports a high strength watermark and as a result, is more robust to attacks when compared to the luminance embedding methods. The method is also robust to up scaling, rotation, cropping, and lossy compression but provides limited performance in the presence of downscaling and frame rate conversion.

A blind HD video watermarking algorithm based on the DT CWT as it has perfect reconstruction, shift invariance, and good directional selectivity which provide robustness to geometric attacks such as rotation, up-scaling, and cropping. The watermark is embedded in the chrominance channel which maintains the original quality of the watermarked video in a fashion that an attacker cannot remove the watermark by applying estimation and removal attacks or by averaging a group of frames. The watermark ex-traction is performed in a blind fashion within the frame using all levels of the DT CWT decomposition to ensure robustness to downscaling in resolution and temporal synchronization attacks.

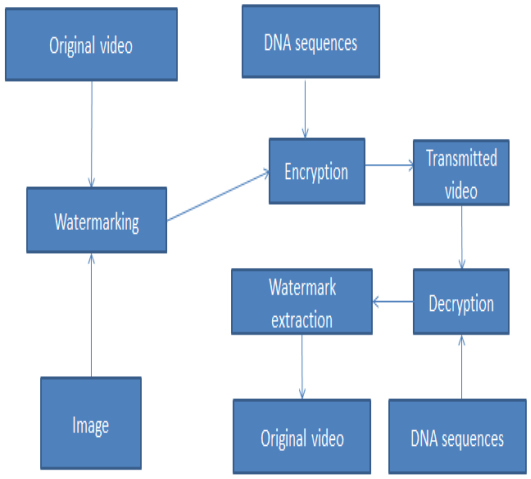
**Video Watermarking:**

Digital Watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. Video copy detection is the process of detecting illegally copied videos by analysing them and comparing them to original content.

**Depth-image-based rendering:**

A DIBR system, which is considered to be a convenient and practical 3D representation technology consists of the center view and depth map. The center view and depth map are transmitted over the channel rather than the left and right color views. At the receiver, the virtual left and right views are synthesized from them. It should be noted that not only can the left and right views generated using a DIBR technique be distributed as 3D content but the center, left and right views can also be distributed individually as 2D content. Therefore, protecting them from unauthorized distribution is becoming very important.

## III. SYSTEM ARCHITECTURE




Watermarking, which also contains a secret message within the host data, is a particular form of data hiding with a different purpose than steganography. It is the process of marking different types of digital data, such as text, audio, images, video or 3D models, to claim ownership of their copyright. It embeds information, which can be a company logo, image or any particular kind of content, in the host data. The embedded information can be either visible or invisible depending on the type of application while it must be perceptually invisible in steganography. In the case of watermarking, it must be statistically detectable when the secret key used for embedding is known, but it can be statistically detectable or undetectable when such a key is unknown. On the other hand, it must be statistically undetectable in steganography, although it is not the requirement in watermarking when the key is not known. Therefore, steganography is a particular case of watermarking, where the statistically undetectability constraint is considered. Of particular note is the fact that a watermarking system must be robust to intentional attacks aimed at removing the hidden message whereas robustness is typically not required for a steganographic system. A watermarking system consisting of an encoder and decoder is shown in Fig. 3. Before the release of a movie, a watermark is embedded in the video content, with illegal contents able to be protected by a watermark-decoding filter being provided to an Internet Service Provider (ISP). Then, when a user requests that a video be downloaded from the server, the ISP can filter it to check for the presence of a watermark. The presence of a watermark indicates that the request to download the movie should be cancelled. As the popularity of 3D videos is increasing daily due to the availability of low-cost 3DTVs, not only 2D but also 3D video content can be distributed illegally without any copyright protection. 3D data are usually distributed in image-based representations, not only as a 3D video but also individually as

2D content. Therefore, protecting these views from unauthorized distribution is becoming very important. In the literature, many different watermarking techniques have been proposed and overviews of these techniques are provided in many papers, each focusing on a specific component. For example, the algorithms described in the literature based on the applications, technology and system requirements of different media types, such as digital images, video, audio and text). A brief overview of the RGB (red, green and blue) and YUV colour spaces commonly used for watermark embedding is provided with the watermarking techniques classified based on the domain in which the watermark is embedded. Complete pictures of these techniques, including an overview of their backgrounds, and pros and cons as well as relevant literature, are also provided. Geometric invariant watermarking techniques are discussed. Image-based representations of a 3D video are classified and some existing works related to these techniques are discussed.

## IV. PROPOSED SYSTEM

In existing system, AES based scheme has been implemented. RSA algorithm has been implemented. The one-time-pad mechanism based on DNA sequences is designed for encryption.

The proposed system is implemented based on DNA Encoding. DNA is called as the 'blue print of life', because it contains the whole information about a particular organism. The main objective of the proposed systems is to design a new watermarking algorithm using DNA concepts.

### Traditional DNA Encryption Algorithm

We propose two methods to encrypt the plaintext using DNA, so that it could be send securely over a network.

### Encryption

**Step1:** The binary data, text or image, is used under the form of ASCII code (in decimal format).
**Step2:** These numbers are then grouped in blocks and encrypted in using a traditional method.
**Step3:** This encoded message is then changed to binary format.
**Step4:** Then these digits are grouped into two and substituted as A for 00, T for 01, G for 10, and C for 11.
**Step5:** We then fit the primers on either side of this message. Primers will act as stoppers and detectors for the message. This has to be given to the receiver prior to the communication.
**Step6:** This message is followed by our own DNA sequence followed by another stopper/primer.
**Step7:** This message is then flanked by many sequences of DNA or by confining it to a microdot in the microarray.
**Step8:** If considered as a pseudo method: this sequence is transferred to the receiver through the Internet. Else the micro-array is sent physically.

### Decryption

**Step1:** The DNA sequence is searched for the primers (start primer and end primer). The message in between them is retrieved and the next DNA sequence before the next primer (our DNA) is retrieved.
**Step2**. The ATGC characters are substituted accordingly (00, 01, 10, 11 respectively).
**Step3**. They are then converted into ASCII code and then the message is retrieved.

### Proposed Methodology

The problem with traditional DNA encryption method is with security of key. An another approach to solve that problem is complimentary pair approach.

A → T
C → A
G → C
T → G

Let us consider a reference sequence:

S = ACGGAATTGCTTCAG

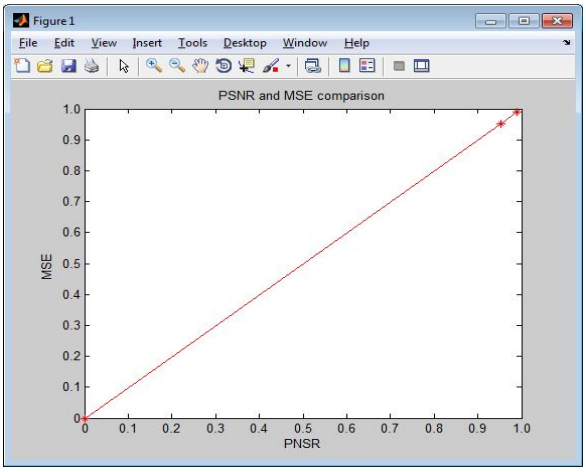
Using the complimentary pair approach the new sequence S' will be:

S' = TACCTTGGCAGGATC

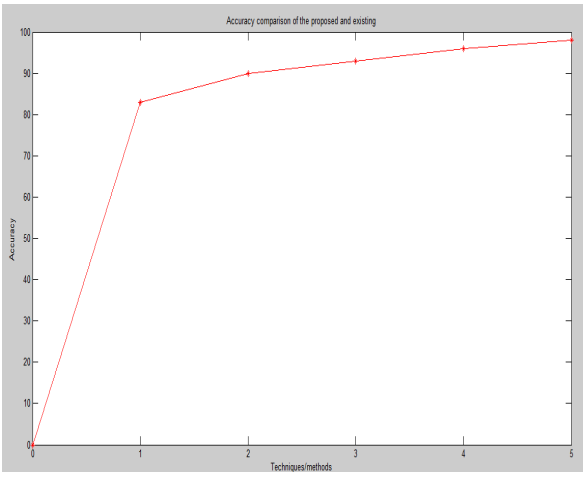
The complimentary approach with substitution approach and we will generate S' from S with help of plain text (M) steps may be as follows:

**Step1:** Send both S and S' by using any steganography technique in order to generate more security.
**Step2:** Receiver will generate plaintext from S and S'.

## V. RESULTS




PSNR vs MSE




Existing system vs Proposed system

## VI. CONCLUSION

Digital watermarking techniques for both 2D and 3D video contents are surveyed. Firstly, an overview of digital video watermarking applications and their challenges, such as the imperceptibility and security of a watermark, blind detection and robustness to attacks was provided. In the literature, a great deal of work has been undertaken by researchers to develop a digital image or video watermarking algorithm that deals with these issues. The watermark embedding techniques were classified based on the domain in which they embedded the watermark, including compressed, spatial and transform. Each technique was discussed in detail and some existing works related to them were then reviewed. Transform domain watermarking techniques were considered to be robust, stable and provide more imperceptibility than spatial and compressed domain-based approaches.

Watermarking in 2D and 3D videos has become more demanding. It is currently a fundamental part of research into the applications of copyright protection, broadcast monitoring, copy control and video authentication. These illegal copies are obtained from poorly supervised movie theaters and distribute illegally days after the movie's release. The illegal copies are then mass-produced for global online distribution. Therefore, the most urgent research requirement is the need for theatrical content protection and online copy control. Watermarking can also be used in the applications of content filtering as well as online location of the illegal content.

## REFERENCES

[1] Gopika V Mane and G. G. Chiddarwar, "Review Paper on Video Watermarking Techniques" in International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013.

[2] Alka N. Potkar and Saniya M. Ansari, "Review on Video Watermarking Techniques".

[3] Koushik Pal1, G. Ghosh and M. Bhattacharya, "A Novel Digital Image Watermarking Scheme for Data Security Using Bit Replacement and Majority Algorithm Technique".

[4] Mr Mohan A Chimanna and Prof.S.R.Khot, "Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery" in International Journal of Engineering Research and Applications (IJERA) Vol. 3, Issue 2, March -April 2013

[5] Hamid Shojanazeri , Wan Azizun Wan Adnan , Sharifah Mumtadzah Syed Ahmad, "Video Watermarking Techniques for Copyright protection and Content Authentication" in International Journal of Computer Information Systems and Industrial Management Applications Volume 5 (2013) .

[6] Archana Srivastava and Prof. Darshana Mistry, "Digital Video Watermarking Techniques:A Review Study" in IJSRD - International Journal for Scientific Research & Development Vol. 1, Issue 2, 2013