Anti-Piracy for Movies using Forensic Watermarking

M. Adimoolam
Assistant Professor
Information Technology
Christ College of engineering and technology
Puducherry, India.

A. John
Assistant Professor
Information Technology
Christ college of engineering and technology
Puducherry, India

M. Gunashanthi
UG Student
Information Technology
Christ college of engineering and technology
Puducherry, India

ABSTRACT
In the past decade internet worked perfectly with distribution of the digital data for pictures, music and videos. Although digital data have many advantages over analogue data, the rightful ownership of the digital data source is at of risk. The copyright protection for digital media becomes an important issue of piracy. Watermarking is a very important field for copyrights of various electronic documents and multimedia. This paper presents a digital forensic watermarking method for authorization against copying or piracy of digital video. The core idea is to use biometric generated keys in the embedding process of watermark. The host video is first randomized by Heisenberg decomposition and Discrete Fourier Transform (DFT). The invisible watermark is embedded in the I-frame of the host video. The watermarks are embedded in the least significant bit (LSB) of the each block. The forensic watermark provides "The Chain of Custody" throughout the life cycle of the video distribution. The experimental result of test sequence demonstrates that the proposed work gives high security and robustness.

General Terms
Algorithms, Security, Watermarking.

Keywords
Forensic watermarking, Discrete Fourier Transform (DFT), the Least Significant Bit (LSB), piracy.

1. INTRODUCTION
The use of digital video application such as video-conferencing, digital television, digital cinema, distance learning, videophone and video-on-demand has grown very rapidly over the last few years. Today it is much easier for the digital data owners to transfer multimedia data over the internet and hence the data could be perfectly duplicated and can rapidly redistribute on a large scale [1]. As advance in digital video technology increases the possibility for illegal distribution of copyright content at high quality of data, content and right owners increasingly need robust protection against piracy. Digital Right Management (DRM) technologies for conditional access are own level of content protection, but DRM doesn't provide complete security to digital media. The Digital Watermarking techniques add another significant layer of protection, acting towards the owners to trace the source of the violation. Digital watermarking is an effective way to protect the copyright of multimedia data even after its transmission [2, 3]. Watermarking refers to the process of adding a hidden structure called a watermark into a multimedia data that carries either the information about the owner of the cover or the recipient of the original data object. The Watermark application includes broadcast monitoring, copy control, transaction tracing, and copyright protection. Robustness, invisibility and security are the three most important properties that need to be satisfied for such application [1,4].

The Copyright piracy [5] is the phenomenon that can prevalent worldwide. Piracy means unauthorized reproduction, copying or distribution of either the whole document or a substantial part of works protected by the copyright. The author has some certain exclusive rights in their works, so they have an Intellectual property rights to their content. And so, the copyright owners are free to share, reproduce, to publish and translate to worldwide. The copyright owners have their rights to sell and assign licenses for their work to provide authorization. Copyright piracy is also considered as a theft for digital content. Particularly in the area of cinematography, there are many losses for the producer due to the piracy. To achieve the copyright infringement in cinematography is more complex because there exists a variety of copyright infringement in the single work. That is many people can insert their own copyright and can overlap.

The DRM provides various rights to the property owners. For a movie it as "Theatrical Right" i.e. right to exhibit the movies in the corresponding theatres. In this case the producer is the copyright holder/owner [6]. The producer gives the theatrical rights to the distributors to exhibit the movies in the theater. The theatrical right can change from time and place. The distributors have the rights to sell the movies in the video cassettes. So the other people can buy and watch the movies. The producer sells the video rights to the other party, who can buy a copy of it and seeing with the family members. Such video cassettes can't' be used for showing movies in the cables or by satellite channels. Because exhibiting movies on the satellite channels or through cables require an appropriate set of rights such as "satellite right" and "cable right" [5,7].

In response to the ever-shifting media validation challenges, a variety of techniques are developed and deployed security protection for the video content over its full Lifecycle. The technique used to protect the video throughout its life cycle is called "forensic watermarking" [8]. Which is nothing but the use of digital watermarking for digital video content, which gives an emerging technologies combined with new added and improved approaches, there are as many as promising aspects that directly affect the key challenges to provide security and maintain the digital video content throughout he distribution system. In particular, forensic watermarking provides a virtual path called "Chain of Custody" for the digital content that accurately discovers the source of unauthorized replicates and track the address of the original source and made a copyright infringement over the digital video [9].

In order to increase the security to the multimedia content especially for videos and digital movies, we proposed a new biometric watermark forensic video watermarking technique. For this purpose we using Discrete Fourier Transform (DFT) for the frame transformation, to invoke DFT the Fast Fourier Transform (FFT) algorithm is used. Since the FFT algorithm is used for spatial domain, it give the property of frequency transition under the spatial domain [10]. First the iris of the user/owner are captured by iris recognition method and the iris is converted into codes. These codes are stored in the database and give the details of the digital video. The digital codes only give the authentication of the digital video. Here iris is used as a watermark image. To avoid the ambiguity attack we are inserting the watermark bits in the Least Significant Bit (LSB) [11, 12].

This paper proposes the (i) Key generation, (ii) Embedding and (iii) Watermark extraction process. The algorithm analysis and feasibility analysis are done to prove the watermark is secure and robust.

2. MATHEMATICAL PRELIMINARIES

In this phase the basic preliminaries are used in the proposed system which is useful give maximum robust and performance to the proposed system.

2.1 SURF

Speeded Up Robust Feature (SURF) is a robust image detector and it was firstly introduced in 2006. The SURF has almost the performance as SIFT, yet it is about six times faster than the SIFT, because of the usage of integral image. SURF detector is based on the estimation of the Hessenberg matrix. For example give a point p= (x, y) in an image I,

The Hessian matrix in p at the scale σ is defined as,

$$H(p,\sigma) = \begin{bmatrix} L_{xx}(p,\sigma) & L_{xy}(p,\sigma) \\ L_{xy}(p,\sigma) & L_{yy}(p,\sigma) \end{bmatrix} \quad (1)$$

Where L_{xx} (p, σ) is a convolution of the Gaussian second order derivative with t (e, image I in point p=(x, y) and similarly for L_{xx} (p, σ) and L_{xx} (p, σ) [13].

2.2 Hessen berg Decomposition

Hessen berg decomposition is a matrix decomposition of matrix A into a unitary matrix P and a Hessen berg matrix H such that

$$PHP^{H} = A \quad (2)$$

Where P^{H} denotes the conjugate transpose. Hessen berg decomposition is the first step in the Schur decomposition. Hessen berg decomposition of an n×n matrix requires 14 $n^3/3$ arithmetic operations.

2.3 LSB Substitution

The most common and easiest way of concealing secret data is an LSB substitution method [14]. The primary concept of the LSB is to conceal the secret in the least significant bit of the image. For example, for the hiding image E into image H which we assume both of them to be n-bit grayscale images, a suitable technique is to conceal E into the position of the least significant bit of H. At first, the rightmost k LSBs from each pixel of H are extracted to create a k-bit grayscale image, R, called the residual image which equals E in size. Next, E is changed to a k-bit units and processing each pixel of E into various small k-bit image unit as a single pixel. The result of this decomposition is E'. Eventually, R is replaced by E'. The embedding result is Wi which is illustrated in figure 1.

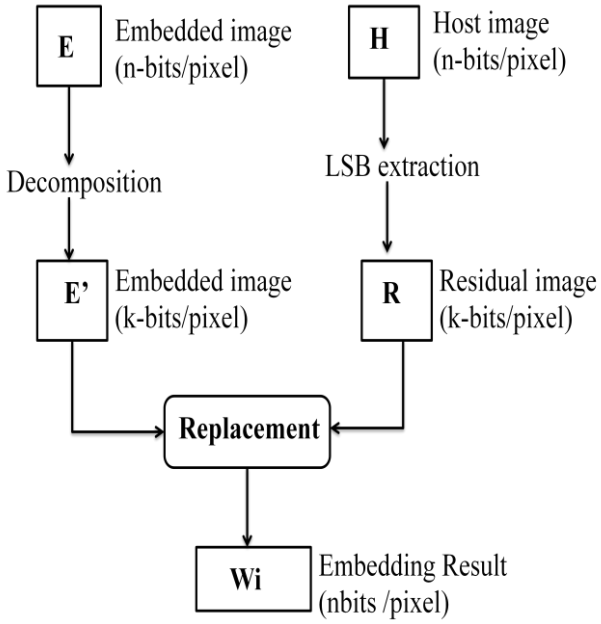


Fig 1: LSB substitution

2.4 DFT

DFT [15] is mathematically defined as,

$$F_n = [w_n^{kl}]\ 0 \le k, l < n \quad (3)$$

Where $w_n = exp(2\pi i/n)$ is the primitive n-th root of unity. Throughout, e_i^m, $0 \le i < m$, is the vector size m with a 1 in the i^{th} component.

3. FAST FOURIER TRANSFORM (FFT)

The Fast Fourier Transform (FFT) [16] is an algorithm for the calculation of the DFT and it was first published in 1965 by J.W.Cooley and J.W.Tuckey. It has a revolutionized the modern experimental mechanics, signal and system analysis, acoustics, and paved the way for the introduction of modal analysis. The FFT algorithm applies only when signals comprising of a number of components, which is adequate to 2m. Its main advantage is that it can significantly reduce the computation time by a factor of the order m/log2m , i.e. more than 100 times from a sample of 1024 elements.

The Fourier Transform decomposes the image into the real and imaginary parts, which can be represented the image in the frequency domain. For FFT, the input signal is an image then the number of absolute frequencies in the frequency field is adequate to the number of pixels in the spatial domain or in the image [17]. For reorganization the inverse transform of re-transforms the absolute frequencies of the image in the spatial field is done. The mathematical function for the FFT and its reverse of the given 2D image are shown in below equations:

$$F(X) = \sum_{n=0}^{N-1} f(n) e^{-j2\pi\left(\times\frac{n}{N}\right)} \quad (4)$$

$$F(n) = \frac{1}{\mathrm{N}}\sum_{n=0}^{N-1} f(x)e^{j2\pi\left(\times\frac{n}{N}\right)} \quad (5)$$

The equation shows, f (m, n) is the pixel at coordinates of (m, n). Then F (x, y) is the asses of the image in the absolute frequency field representing the coordinates of (x, y) and (M, N) are the proposition of the image in the 2D plane [18].

The equation gives; a native implementation of the FFT algorithm is very complex. But the FFT is that it is separable, but the 2D transform can also be done as 1D transforms as shown in below equation. The equation gives the horizontal direction followed by the other signal in the erect direction, on the consequence of the horizontal transform. Then the result is equivalent to performing of the 2D transform in the frequency space.

$$F(X,Y) = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} F(m,n)e^{-j2\pi\left(x\frac{m}{M}+y\frac{n}{N}\right)} \quad (6)$$

$$F(\mathrm{m},\mathrm{n}) = \frac{1}{\mathrm{MN}}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} F(\mathrm{x},\mathrm{y})e^{j2\pi\left(x\frac{m}{M}+y\frac{n}{N}\right)} \quad (7)$$

Matlab's function fft () performs the DFT. The FFT is a technique for efficiently evaluating the Fourier transform over discrete sets of data. The DFT is the orientation of the Fourier Transform and therefore it does not contain all the frequencies that used to forming an image, but only a set of samples which is most sufficiently enough to describe the spatial domain image [19].

4. PROPOSED SYSTEM

Video watermarking application is also called as "forensic tracking", the goal of the watermark is to help to identify the source of an unauthorized copy of media files and retrace them back to the copyright authorized recipient or legitimate content holder. The presence of or identifying the watermark will arise the copyright infringement over the third party. And to deter piracy in the content distribution the user is a media-aware-before-hand-that the content is made traceable to the last authorized recipient.

In the below diagram (Fig 3) shows, the compressed and encrypted content is delivered to a subscriber [20]. The received work is watermarking enabled and embeds invisible identifying on formation in the content before it leaves the receiver. The insertion of the watermarking payload does not affect the fair and legal consumer use of the content, and it is invisible through normal display and personal-use recording. If, however, the content is detected in illegally distributed from e.g. on DVD or through an internet P2P file sharing network, it may be of sufficient concern to the rights owners and distributors to identify the source.

Through the forensic extraction service, the watermark can be recovered. The watermark payload server as an index into the transaction database used to identify the source, after which the rights owner will determine any further action. This could offend copy with a trailer of the same content together with the purchase / viewing option Fig 3 shows how the forensic watermark is extracted and embedded.

4.1 Iris Recognition

The Iris recognition system is an automated method of the biometric identification methods that uses the mathematical pattern-recognition techniques on the video images of their ides of an individual's eyes, because everyone has a unique iris pattern. And those complex random patterns are unique and they can see from some distance [21].

The Most of the iris recognition systems assume the images of the iris in the visible orientation about (400-700 nm) or neared infrared range of (700-900 nm) of the electromagnetic spectrum. Each iris wavelength is distinguishes different features of the iris within one NIR and VW is receiving information from the iris by obtaining its texture and pigmentation.

The majority of the iris recognition systems can function within the longer NIR range which can be penetrated through dark-colored element called irides, the dominant the phenotype of the human population, by revealing texture are not easily detected in the VW spectrum. The NIR range is also reduces the iris pattern infectivity by blocking the ambient corneal reflections [22].

The process of capturing an iris into a biometric template is made up of 3 steps

1. Catching the image
2. Determining the location of the iris and modifying the image
3. Storing and equating the image.

The iris are encoded with a unique set of 2048 bits which can serve as the fundamental identification of that person's particular iris. These iris bit codes can be stored in a database and then compared to uniquely identify a person [23]. The size of 2048 is sufficiently large to store the data of several particular filters on the most angles of the iris, while also being sufficiently small to be easily stored in a database and manipulated quickly. We extract the phase information from the iris as opposed to amplitude information since the phase information is not skewed by pupil deformation. We use Gabor filters to extract this phase information.

The Gabor filter is an application of the Gabor wavelet. This will return two bits depending on which the quadrant normalized resulting imaginary number from this lies in. This equation can be simplified for computation by considering it as a combination of two filters, such as one filter representing the real part of the integral and the other representing the imaginary part. Each of these filters consists of a combination of Gaussian and sinusoidal filter. The parameters α, β and ω are then tuned by constraining the Gaussian filter to range over one standard deviation and the sinusoidal filter to range from - π to π [24].

4.2 Watermark Embedding Process

At first the proposed scheme performs the operation of the watermarking algorithm in the spatial domain directly modifies the intensities or color values of some of the selected pixels.

The general flowchart diagram of the proposed work is shown in the fig. 2. The necessary steps to embed the watermark into an input video data for the copyright protection purpose are as follows:

- Convert the loaded color video into correspondent frames.
- Apply the block matching and motion estimation techniques on the sequential frames.

- Select only the frames that have the sufficient number of the motion blocks in which it is compatible with watermark size.
- From the selected frames, use the given threshold to select the best blocks during the matching process.
- Perform the Fourier transformation on the selected blocks.
- Embed Hessen berg decomposition as a proposed watermark into the selected blocks.
- Extract the embedded watermark
- Apply some related attacks on the watermarks frames in the video
- Evaluate the conducted results using PSNR ratio for embedding and similarity for extracting process before and after the attacks

In the MPEG multiplexed stream, shown in (Fig 4), there are typically three kinds of coded images in each group of pictures, such as I (Intra) -frame compressed using only intra-frame coding, P (Predicted) -frame coded with the motion compensation using I-frame or P-frame and also by B (Bidirectional) -frame, coded by the motion compensation by either past or future I or P frames.

In order to achieve a low complexity and improve the robustness, we only use the I-frame to embed the watermark [10].

4.3 Extraction process

The extraction processes of the proposed system same as the embedding process. The Fig3 shows that the forensic watermark embedding and extraction process. After the verification is done the watermark is extracted from the video. And the ID of the iris extracts from the host video. Then, then each set of the I-frames, extract the watermark vector. The flow chart gives the similar process for the extraction. The fig 2 shows how the watermark is embedded and removed from the host video (H).

Extract the watermark by a

$$WE=BPn*Vw' \quad (9)$$

Where BP_n is the comparison between two frames.

$$BPn= inv(U) * BPE * inv(V') \quad (10)$$

Where U, V are rearranged to video, the feasibility analysis is done between the watermarked and unwatermarked frames.

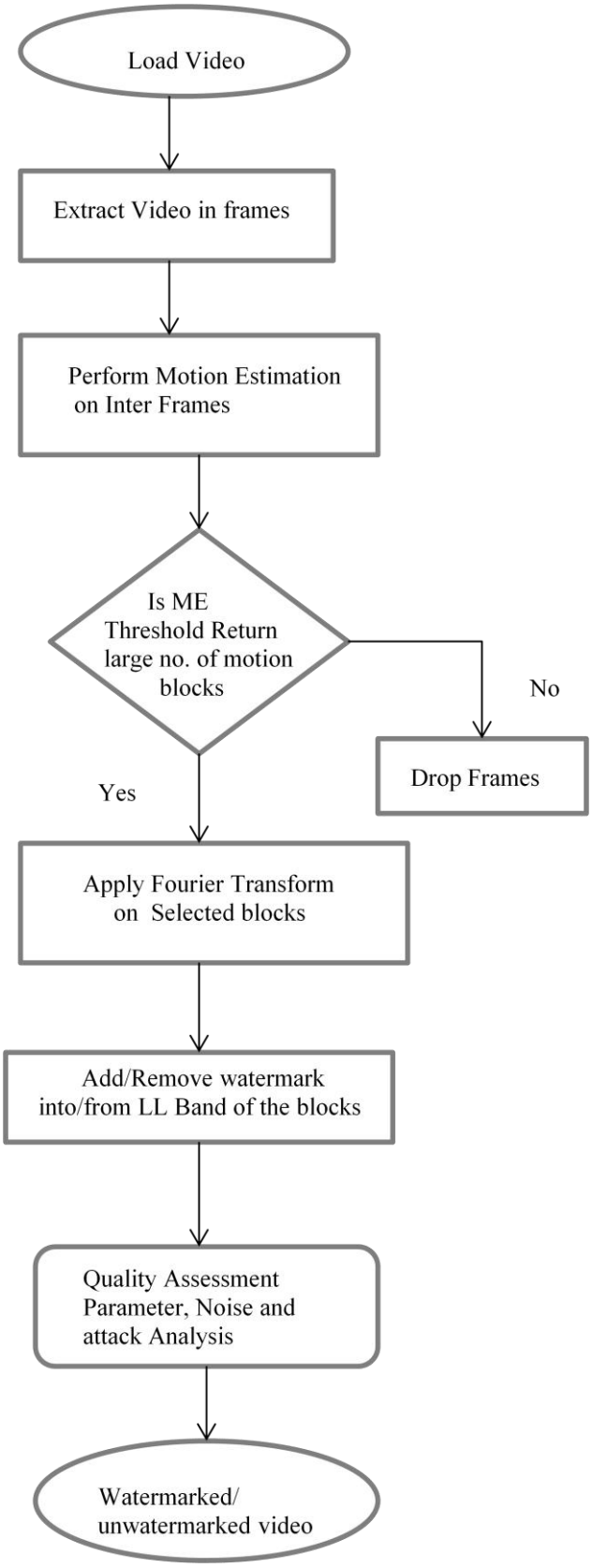


Fig 2: Flow Chart for watermark insertion and extraction

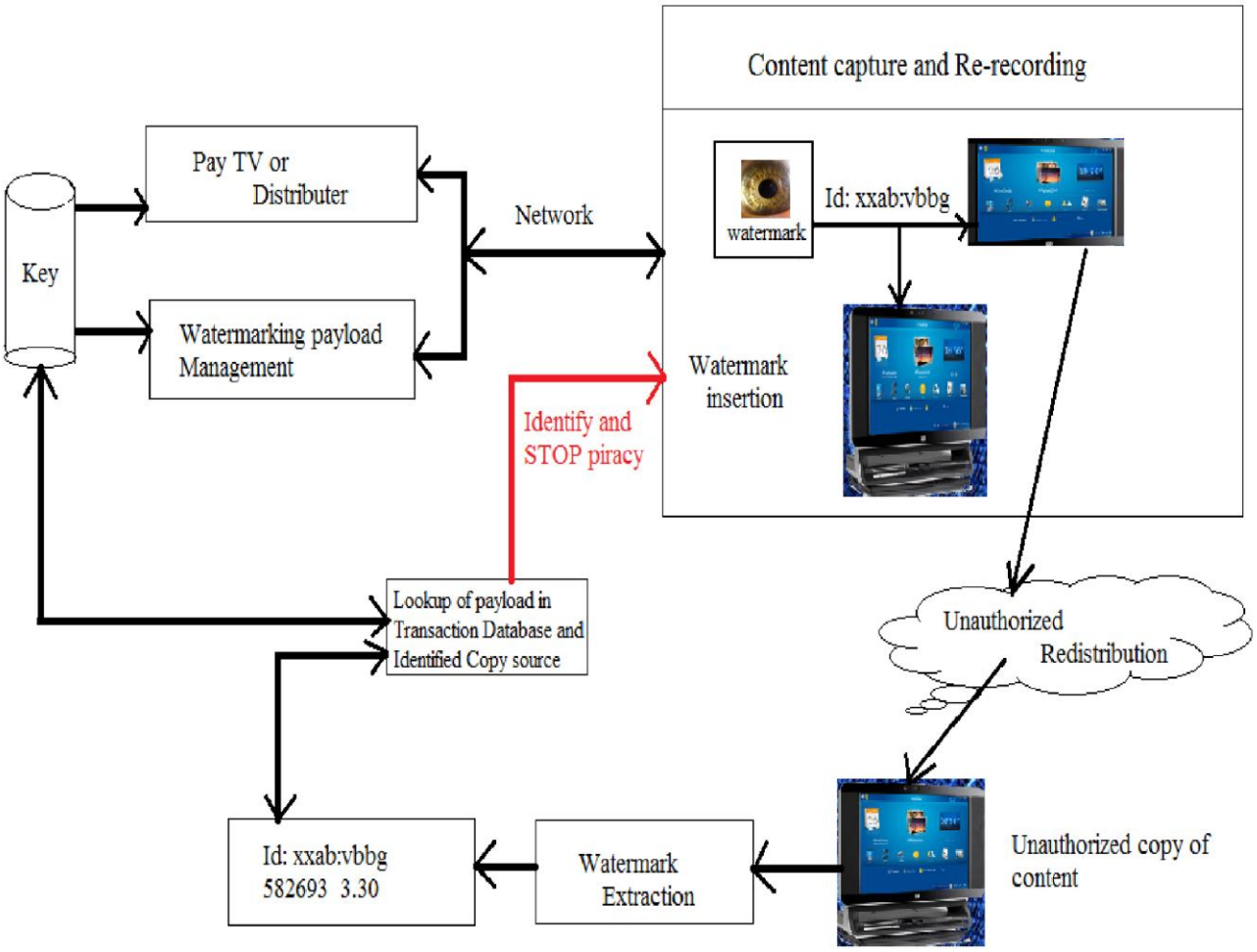


Fig 3: Forensic Marking and Extraction concept

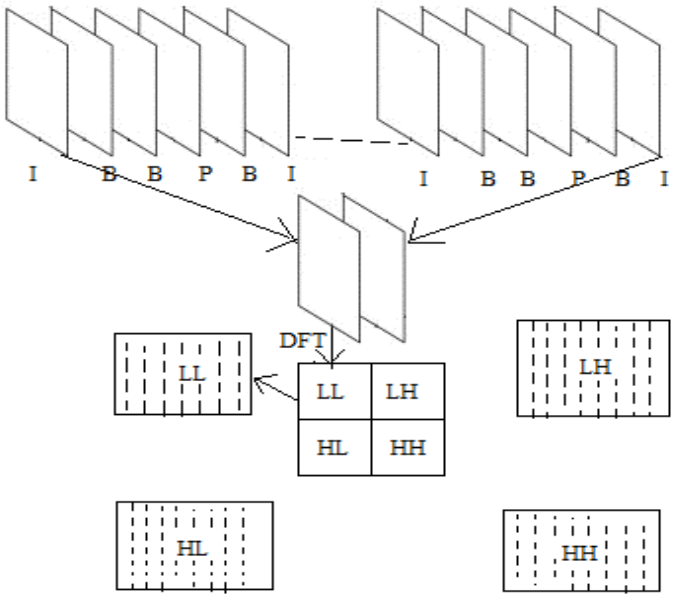


Fig 4: Embedding watermarks on I-Frames

5. EXPERIMENTAL RESULT

In this section, illustrate the performance of the proposed algorithm. The Bio-inspired Forensic watermark was done on the Matlab platform.

To evaluate the performance of the approach, calculated Peak Signal to Noise Ratio (PSNR).

The peak signal to noise ratio (PSNR is compressed between a p bit depth image I and its watermark and the watermarked work $I_{wd.}$

$$PSNR(I, I_{wd}) = 10log_{10}\left(\frac{(2^p-1)^2}{MSE}\right) \qquad (11)$$

$$\mathrm{MSE}(\mathrm{I}, \mathrm{I}_{\mathrm{wd}}) = \frac{1}{\mathrm{HL}}\sum_{\mathrm{k}=1}^{\mathrm{L}}(\mathrm{I}(\mathrm{k}) - \mathrm{I}_{\mathrm{wd}}(\mathrm{k}))^2 \quad (12)$$

Where L corresponds to the number of pixels of I.

To conform the imperceptibility of the watermark embedding algorithm, randomly extract some frames and compare the video frames before and after watermarking of the frames, Fig 5 illustrates the experimental results for video sequence. For this, the watermarked frame and unwatermarked frame are taken and calculated PNSR values for each frame. Then generate the values and plotted as the graph. The Fig 5 shows that the noise ratio between the frames of with watermark and without watermark.

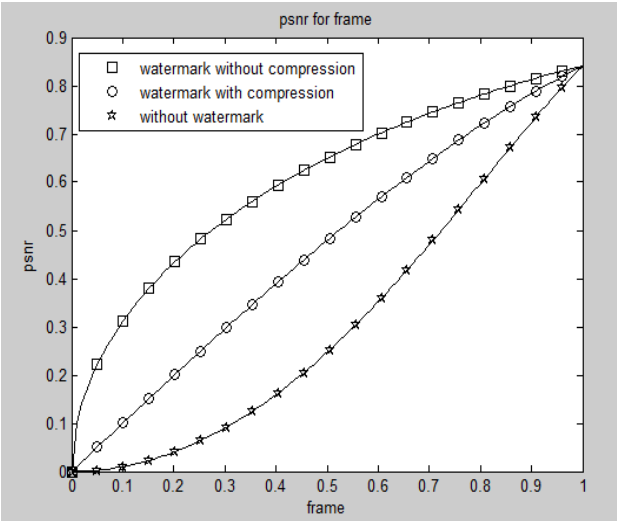
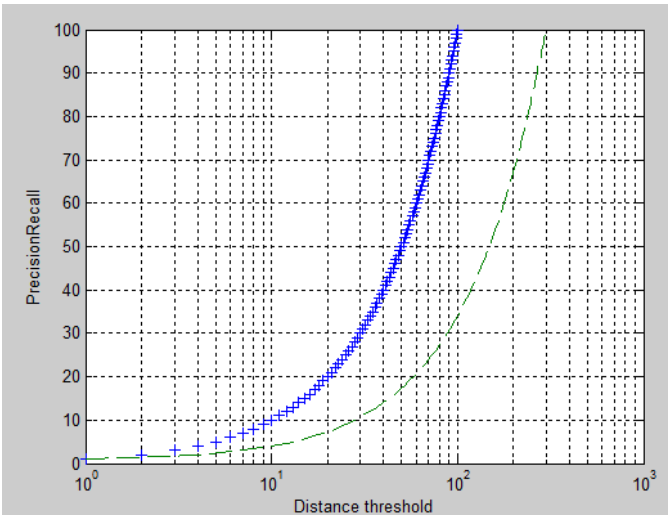


Fig 5: PSNR change of I-frame

In this experiment, apply individual transformations on the query videos. This is made to test the robustness of the proposed algorithm against video changes that usually occur in practice when videos are copied.

Then, computed the average values across the experiments for the corresponding values of the threshold. Then plot the average precision and recall a value which is shown in figure 5. The figure 5, shows that at the threshold of 0.18, the proposed algorithm can still achieve 100% precision with 85% recall. The insertion point of the precision and recall and precision have a relatively high value 90%, given that copied clips of the videos have been significantly changed from the original ones.




Proposed Algorithm


Existing Algorithm

Fig 6: Performance Analysis

The equation peak signal-to-noise ratio, often abbreviated as PSNR, is an engineering term that gives the ratio between the maximum possible ability of the signal and the ability of altering noise that strikes the fidelity of its visibility. Because many of the signals have a very wide dynamic signaling rate, PSNR is generally expressed in terms of the logarithmic decibel standard. A higher PSNR would normally indicate that there is high quality of signal threshold in the receiver side.

The PSNR is most easily defined through the Mean Square Error (MSE) which holds for two m×n frames f and f' where one of the Frames is considered as a noisy approximation of the other frames.

The fig 6 shows the performance analysis of the existing and proposed watermarked work. The performance analysis is done by calculating the values between Distance threshold and precision recall for the watermark in the frame

6. CONCLUSION

We have proposed a new technique for the secured video creation and delivery. As for the importance of providing security and authentication for movies and digital video distribution, we introduce a forensic watermark technique to trace and prevent the videos from unauthorized users. Our process is about the watermark processing, video preprocessing, and watermark embedding and watermark detection. Since we use iris of owner/user as the watermark, we provide additional security to videos, so they can't overwrite the watermark. Experiments are conducted to demonstrate that our scheme is robust against attacks such as, frame dropping, frame averaging and statistical analysis. For the security, attacks particularly ambiguity attack and comparability analysis confirms the high security, efficiency and robustness of the proposed watermarking technique.

7. ACKNOWLEDGMENTS

Our thanks to the experts who have reviewed our paper and given valuable suggestions. We also thank our students

Hemachandran, Prabavathi, Prasanth and Melbin for their support in the constant development and contribution to this project. We also thank our college management for providing the necessary infrastructure and constant support

8. REFERENCES

[1] Cox, I.J., Miller, M.L., Bloom, J.A.: Digital Watermarking. Morgan Kaufmann, San Francisco (2001)

[2] R.G. Schynded, A. Tirkel and C. Osborne, "A digital watermark, Proc. IEEE Int. Conf. Image Processing (ICIP), pp. 86-90, 1994.

[3] E.J. Delp and R.B. Wolfgang "A watermark for digital images", in Image Processing, Lausanne Switzerland, vol. 3, pp. 215-218, Sept. 1996.

[4] Digital watermarking schemes for authorization Against copying or piracy of color images.

[5] "Study on copyright piracy in India", ministry of human resource development Government of India, N.K. Nair, A. K. Barman, Utpal Chattopadhyay,

[6] Cox et al, Digital watermarking: principles and practice, Morgan Kaufmann, 2002.

[7] Cox, A Secure Robust Watermark for Multimedia,

[8] T. Kalker, G. Depovere, M. Maes, J. Haitsma, , "The Video watermarking System for broadcast monitoring", proceedings of the SPIE, vol. 3657, pp. 103-112, (1999).

[9] G.C. Langelaar, I. Setyawan, R.I. Lagendijik, Watermarking digital image and video data, IEEE Signal Processing Magazine 17 (5) (2000) 20–46.

[10] Information Hiding in Computer Science, Vol. 1174, pp. 183-206, 1996

[11] "Pease FFT Algorithm", J.R. Johnson nov 3, 1998.

[12] "Biometrics inspired watermarking based on a fractional dual tree complex Wavelet transform", Gaurav Bhatnagar, Q.M. Jonathan Wu, Department of Electrical and Computer Engineering, University of Windsor, Windsor, Ontario, ON, N9B 3P4, Canada, Future Generation Computer Systems 29 (2013) 182–195.

[13] "Speeded-Up Robust Features (SURF)", Herbert Bay a , Andreas Ess , Tinne Tuytelaars, and Luc Van Gool .

[14] "Image hiding by optimal LSB substitution and genetic algorithm" Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, Elsevier Pattern Recognition Volume 34, Issue 3, March 2001, Pages 671-683.

[15] "Watermarking digital 3D volumes in the Discrete Fourier Transform domain", Vassilios Solachidis, Member, IEEE, and Ioannis Pitas, Fellow, IEEE.

[16] J. W. Cooley, P. A. Lewis, and P. D. Welch. History of the fast Fourier transform. In Proc. IEEE, volume 55, pages 1675–1677, October 1967

[17] J. W. Cooley and J. W. Tukey. "An algorithm for machine calculation of complex Fourier series". Mathematics of Computation, 19:297–301, 1965.

[18] "Generation of 1D and 2D FFT function in MATLAB", Parul Goyal, Department of Electronics & Communication Engineering, Uttaranchal Institute of Technology, International Journal of Science, Technology & Management; December-2010.

[19] Swiss Federal Institute of Technology Zurich, "Fast Fourier Transform", Numerical Analysis Seminar; Stefan Worner.

[20] S. Perreault and P. Hebert. Median Filtering in Constant Time. IEEE Transactions on Image Processing, 16 (9) : 2389-2394, 2007.

[21] Daugman, John. (2004). How Iris Recognition Works. IEEE Trans. CSVT, 14 (1), 21-30.

[22] Daugman, John. (2003). Demodulation by Complex-valued Wavelets for Stochastic Pattern Recognition. International Journal of Wavelets, Multi-resolution and Information Processing, 1 (1), 1-17.

[23] "How Iris Recognition Works", John Daugman, PhD, OBE, University of Cambridge, The Computer Laboratory, Cambridge CB2 3QG, U.K.

[24] "Effect of Server Image Compression on Iris Recognition Performance", Information Forensics and Security, IEEE Transaction on March 2008, Daugman J, Dowing C, University of Cambridge, Cambridge. Volume:3, Issue: 1page (s): 52-6.