A Survey on Various Digital Video Watermarking Schemes

Nitin A. Shelke
Computer Science and Engineering
Government College of Engineering
Amravati, India
nitinashelke@gmail.com

Dr. P.N.Chatur
Computer Science and Engineering
Government College of Engineering
Amravati, India
chatur.prashant@gcoea.ac.in

Abstract— Due to vast usage of internet large amount of exchange has been done over the web. Now a day in the world of internet, many pirated video uploaded on the internet. Video Piracy becomes a serious problem. The mounting interest with reference to digital watermarking throughout the last decade is certainly due to the increase in the need of copyright protection. Video Watermarking plays an important role in copyright protection. In this paper, we introduce the survey of various technique that are available for digital Video Watermarking and features required to design a robust watermarked video for valuable application and focus on various domains of video watermarking techniques.

Keywords-Digital video watermarking, LSB, DCT, DFT, PCA, DWT, SVD, MPEG.

I. INTRODUCTION

Digital video watermarking is a new technology used for copyright protection of digital media. Digital watermarking attracted the attention of Researchers during the early to mid. One of the primary motivations for applying watermarking is the protection of intellectual property rights video watermarking is characterized by the temporal and inter frame characteristics, which require specific approaches for video watermarking. The watermarking concept is similar to the stegnography. In stegnography they give the stress on the concept of Encryption and Decryption, also the main idea of stegnography is the embedding of secret information into data under the assumption that others cannot know the secret information in data. The main idea of watermarks is to check the logo embedded in data or not.

Watermarking has existed since approximately the many years and in the past watermarks was used on the papers to identify from which mill which it was produced. Watermarking is an important mechanism applied to physical objects like bills, papers, garment labels, product packing. Physical objects can be watermarked using special dyes and inks or during paper manufacturing. The term “watermark” was probably originated from the German term “wassermarke”. It plays a major role in the paper industry. Watermark is of two type visible watermark and invisible watermark. Both watermarks give the security to the video, image and document. But invisible watermark is having advantage over visible watermark such that visible watermark visible to human eyes so attacker can easily attacked on this by frame cropping, frame averaging like operation. So all researcher are interested in invisible watermark which they embed in Digital video. The watermarking scheme that allows extraction of embedded information using the original, unwatermarked data is known as non-blind watermarking scheme, otherwise it is known as blind.

The basic components involved in robust watermarking are *watermark embedding*, *attack*, and *watermark detection*. In watermark embedding, a watermark signal (Text, image or audio etc) is constructed and then embedded into an original signal (Video in context with this paper) to produce the watermarked signal. Once embedding is done, the watermarked video can be subjected to various attacks. During watermark detection, the watermark detector is given a test signal that may be watermarked, attacked or not. The watermark detector reports whether the watermark is present or not on examining the signal at its input. The figure1 shows watermark embedding in which video is taken as an input and watermark W is embedded using the watermarking algorithm.

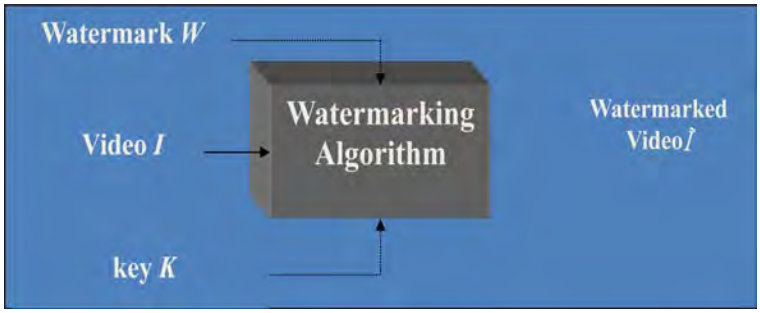

Figure1. Watermark Embedding

A. Properties of Digital Video Watermark

For digital watermarking of video, the different characteristics of the watermarking are given below.

- Invisibility: The digital watermark that we embed should be invisible to the human eyes. So that attacker does not aware the presence of watermark.
- Robustness: robustness refers to the Attack that should be performing on watermarked video and analyze how it shows the resistant to various type of attack. a video watermark is highly robust then it can say that it having more resistant power. High robustness preserves the quality of video.
- Perceptible: A digital watermark is called perceptible if the presence of that mark is noticeable. Achieving the Imperceptibility is great task for researcher.
- Capacity: capacity refers to the length of the embedded message into digital video.
- Fidelity: It is the similarity at the point at which the watermarked content is provided to the customer that count weather video given to the customer is degraded or not. A watermark is said to be high fidelity if degradation it causes is very difficult for a viewer to see.
- Computational Cost: it refers to the cost or time required for embedding and extracting the watermark from the digital video. For better working digital video watermarking scheme computational cost should be minimized.
- Interoperability: it refers, the watermark should remain in video even the compression and decompression operations are performed on that video.
- Blind/informed detection: in the Informed watermarking schemes the detector requires access to the unwatermarked original video. In Blind watermarking Detectors do not require any original information.
- False positive rate**:** A false positive refers detection of watermark information from a digital media such as video, image that does not actually contain that watermark.

B. Digital Video Watermarking Application

Digital video watermarking has huge application in the field of digital media which are as follows.

- Copyright Protection: Traditional textual copyright notices “Copyright date owner” “© date owner” “Copr. Date owner But Disadvantages for textual copyright notices it is easily removed from a document when it is copied and Copyright notices printed on the physical medium are not copied along with the digital content. Since watermarks are imperceptible and inseparable from the work, they are obviously superior to textual copyright
- Source tracking: Watermark information is embed in the product that company will have to send from source to a particular destination. For tracking the product information is extracted from that product and checks it with a original.
- Broadcast Monitoring: TV or radio advertisements should be monitored to prevent airtime overbooking. Watermarking is an obvious alternative method of hiding identification information
- Fingerprinting: A watermark is embedded in the video which will give protection to the video so that no can make the copy of video. It is use in Movie piracy. In this, we embed the name of person who made the First copy of the video and giving protection of the video.
- Video Authentication: using watermark it will check weather particular video is authenticated or not. This will give protection to that video.

- Copyright Protection: the embed watermark in video identifying the copyright owner, in digital multimedia data. it shows the ownership of the video.
- Tamper proofing: Tamper proofing refers to a watermarking system's resistance to hostile attacks. Attacks are of two type active attack and passive attack. In active attack the attacker tries to remove the watermark or make it unnoticeable. In passive attack it only checks whether the watermark is present or not.
- Content authentication: it refer to that weather content are authenticated or not.
- Media digital rights management (DRM) in content supply chain.
- Security: For transferring sensitive video from source to destination there is a chance of attack by third person on that video, so to prevent this watermark is embedded in that video which will provide the security to that video. The ability to resist hostile attacks, unauthorized removal, Eliminating attacks, Masking attacks and
- Collusion attacks. Due to high security unauthorized embedding is not possible.
- Information Hiding: Making the information imperceptible that is invisible to the human eyes and
- Keeping the existence of information secret.
- Copy Control: Watermarking in copy control Combining every content recorder with watermark detector When a copy-prohibit watermark is detected, the recording device will refuse to copy.

B. Video Watermarking Attack

The attacks on video watermarking are frame dropping, frame averaging, statistical analysis, lossy compression, cropping and various signal processing and geometrical attacks. There are two type of attack intentional and unintentional attack. Intentional attack is like adding noise and unintentional attack are like compression of the video.Figure1 shows various attacks that perform on watermark video.

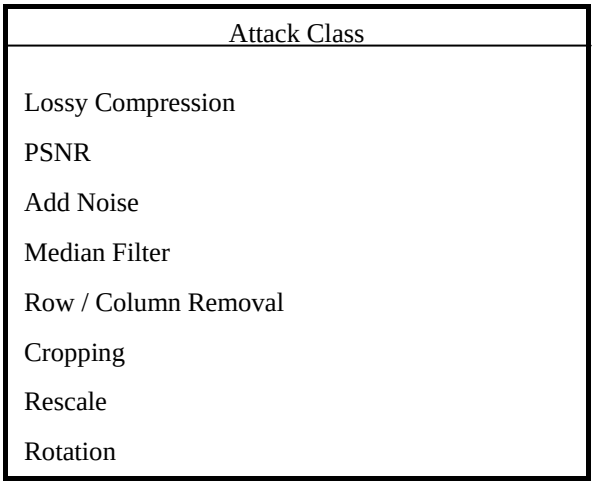

Figure1. Various Attacks on watermark video

II. RELATED WORK

Many digital watermarking schemes have been proposed in the literature for Digital video watermarking.

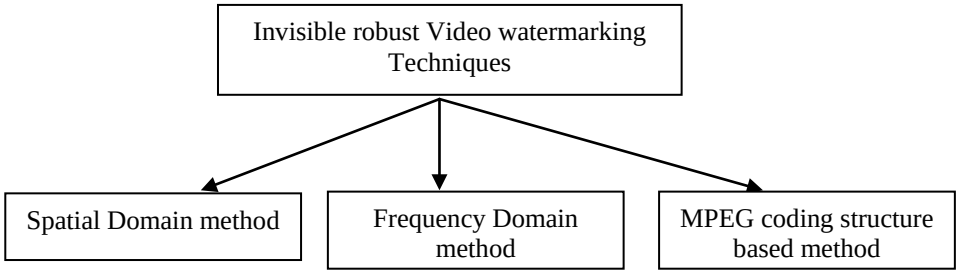

Figure2. Classification of Video watermarking method.

A classification of the existing video Watermarking techniques is divided in three main categories.

A. Watermarking in Spatial Domain

B. Watermarking in Frequency Domain

C. Watermarking in MPEG coding structure based domain

A. Watermarking in Spatial Domain

The following characteristics of spatial domain methods are

a) The watermark is applied to the pixel or coordinate domain.

b) No transforms are applied to the host signal during watermark embedding.

c) Combination with the host signal is based on simple operations, in the pixel domain.

d) The watermark can be detected by correlating the expected pattern with the received signal

1. Correlation-Based method

For watermark embedding, correlation properties of additive pseudo-random noise patterns as applied to a Video frame are used**.** A code W(x, y) is added to the covert video frame I(x, y). According to (1)

$$I(x, y) = I_w (x, y) + K*W(x, y) \quad (1)$$

Where *K* denotes the gain factor and Iw is the resulting watermarked video frame. Increase in ***K*** increases the robustness of watermark at the expense of quality of the watermarked image. To recover the watermark, the video frame is embed with the same key and the correlation between the noise pattern and the watermarked image is calculated. If the correlation exceeds a certain threshold T, the watermark is detected and a single bit is set. This method is easily extended to a multiple-bit watermark by dividing the image into blocks and performing the above procedure independently on each block. The algorithm is modified by pre-filtering the video frame before applying the watermark, and then increasing the higher resulting correlation. If the correlation exceeds a certain threshold T, the watermark is detected, and a single bit is set. This method can easily be extended to a multiple-bit watermark; this is done by dividing the image into blocks, and performing the above procedure independently on each block. The algorithm can be improved in a numerous ways. Firstly, the notion of a threshold is used for determining a '1' or '0' can be eliminated by using two separate pseudorandom noise patterns. One pattern is designated as a logical '1' and the other a '0'. The above procedure is then performed once for each pattern, and the pattern with the higher resulting correlation is used. This increases the probability of a correct detection, even if the image has been subjected to an attack [19].

2. Least Significant Bit Modification method

It is simple method of watermarking. Initially it had been applied in image watermarking where image was seen as a matrix. Image is viewed as a 1 or 0 format. In the LSB domain we change the least significant bit from 1 to 0 and 0 to 1. The information of digital image s is represented by an array of value. These value represent the intensities of the three color describe a pixel that is red, green and blue. It is the most known method for hiding the information in images, video and audio.

Video frame is described in terms of pixel and pixels of a grey level video frame are represented by an 8-bit data value, the video frame can be sliced up into an 8 bit planes. The least significant bit plane of video frame does not contain visually significant information so it can easily be replaced by a huge amount of watermark bits.

B. Watermarking in Frequency Domain

The Frequency domain base method are Discrete cosine Transform (DCT), Discrete Fourier Transform(DFT), Singular value decomposition(SVD), Principal Component Analysis(PCA) and Discrete wavelet transform(DWT) which used as the methods of data transformation.. The frequency domain methods are comparatively more robust than the spatial domain watermarking schemes, mainly in cropping, scaling, noise intrusion, lossy compression, pixel removal, frame removal, frame averaging and rotation.

1. Discrete Cosine Transform

Features of DCT are

- The Characteristics of DCT coefficients must utilize few coefficients for providing excellent signal approximations.
- Since the frequency components are ordered in a sequential order, starting with low frequency, mid frequency and high frequency components, a proper selection of the components can be prepared.
- The most of the high frequency coefficients are zero. When represented by smooth block.
- An edge block is represented, if the low frequency coefficients have large absolute values.

DCT is faster and can be implemented in O (n log n) operations. DCT is highly used method in image watermarking. DCT gives accurate result using DCT method. Using The Discrete cosine transform image get decompose into different frequency bands, and we are interested in middle frequency band. In this watermark information is easily embed into the middle frequency band of the. The middle frequency bands are chosen because it avoids the most visual important parts of the image which is off low frequency without exposing themselves to removal through compression and noise attacks. This is important method for video processing. DCT gives accurate result in video watermarking also and show the resistance against various attacks. Discrete cosine transform has a advantage that it break a video frame is into different frequency bands, which make it more easier to embed watermarking information into the middle frequency bands of an video frame.DCT also improve the Peak signal to noise ratio. Also DCT is more robust against various attack such as frame averaging, frame dropping [3].

2. Discrete Fourier Transform

The frequency of the host signal is controlled by The Discrete Fourier Transformation. This is a multi-bit watermarking technique for video sequences. An N-bit message is embedded in one unit of video fragment, in which a scene is employed as a watermarking unit. The proposed algorithm is fundamentally based on the three-dimensional discrete Fourier transform (DFT). In order to generate a watermark with optimum weighting factors, the perceptual properties for all the three-dimensional DFT coefficients should be computed, but this strategy seems to be undesirable due to the high computational complexity. So, we design a perceptual model of an image in the DFT domain, and apply it to the video watermarking. The proposed perceptual model is expected to give high fidelity and effective, compared to fully calculate visual masks, since it derives all the masks from one reference mask with a well-known estimation method. Through the computer simulations, it will be shown that the proposed watermarking algorithm with the perceptual model yields effective performance for fidelity. The DFT method select the good area where watermark information is embed and give more perceptibility and robustness [13].

3. Singular value decomposition (SVD)

Singular Value Decomposition (SVD) is mathematical technique for diagonal matrices in that the transformed domain consists of basis states that are optimal. The singular value decomposition (SVD) is a method of representing a image in a matrix for with many application in image processing. The singular value decomposition of a *complex* matrix X is given by (2)

$$X=U\,\Sigma V^{*} \qquad (2)$$

Where U is an $m \times m$ real or complex unitary matrix, Σ is an $m \times n$ rectangular diagonal matrix with nonnegative real numbers on the diagonal, and V^{*} is an $n \times n$ real or complex unitary matrix. The diagonal entries of Σ are called the singular values of A and are assumed to be arranged in decreasing order the columns of the U matrix are called the left singular vectors while the columns of the V matrix are called the right singular vectors of A. Singular value of the matrix shows the luminance of an video frame layer while the corresponding pair of singular vectors specifies the geometry of the video frame layer. In the SVD-based watermarking, an video frame is treated as a matrix, which further broke by SVD base method into the three matrices such as U, $\sum$ and V. the small changes in the elements of matrix$\sum$ does not affect visual perception o f the quality of the cover video frame, SVD-based watermarking algorithms add the watermark information to the singular values of the diagonal matrix $\sum$ in such a way to meet the imperceptibility and robustness requirements of effective digital image watermarking algorithms.

In SVD based watermarking, proposed two effective, robust and imperceptible video watermarking algorithms. The two algorithms are based on the algebraic transform of Singular Value Decomposition (SVD). In the first algorithm, watermark bit information are embedded in the SVD-transformed video in a diagonal-wise fashion, and in the second algorithm bits are embedded in a blocks-wise fashion. The concert of the two proposed algorithms evaluated on the verge of imperceptibility, robustness and data payload. Both algorithms showed similar but high level of imperceptibility, however their performance varied with respect to robustness and payload. The diagonal-wise based algorithm achieved better robustness results, while the block-wise algorithm gave higher data payload rate. Each algorithm embeds the watermark in the transform-domain YCbCr space thus spreading the watermark in each frame of the video. The first algorithm suggests hiding watermark information in a diagonal-wise manner in one of three SVD matrices; U, S and V. On the other hand, the second algorithm hides the watermark information in a block-wise manner in either the U or V matrices [15].

4. Principal Component analysis

Principal component analysis (PCA) is a process or method which uses an orthogonal transformation procedure to change a set of observations of possible correlated variables into a set of values of uncorrelated variables which we called as principal components. The number of principal components is not greater than equal to the number of original variables. PCA highlights the similarities and dissimilarities of the data. Since patterns in data are difficult to find in data of high dimension, graphical representation is not available, PCA is a

powerful tool for examining data. The other major advantage of PCA is to identify patterns in the data and then the data is compressed by reducing the number of dimensions, without a lot of information loss. It plots the data into a new coordinate system where the data with maximum covariance are plotted together and is known as the first principal component.

The main thing that are observed that purpose of embedding the watermark in the video frame performed for robustness reasons by inserting in each color channel of each frame while the PCA based watermarking scheme allowed to select the appropriate area of PCA coefficients for embedding and we could analyzed that it is always possible to watermark a color video file without affecting its perceptual quality [16].

5. Discrete Wavelet Transform

Discrete wavelet transform (DWT) is a tool for continuously decomposing an image. DWT is the multi-resolution description of an image. The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. As the human eyes are less sensitive to the changes in the edges the high frequency components are used for watermarking. There is various level of decomposition, after the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. For each successive level of decomposition, the LL sub band of the previous level is used as the input. To perform second level decomposition, the DWT is applied to LL1 band which decomposes the LL1 band into the four sub bands LL2, LH2, HL2, and HH2. To perform third level decomposition, the DWT is applied to LL2 band which decompose this band into the four sub-bands: LL3, LH3, HL3, HH3.if we increase the level of decomposition for embedding the watermark then proposed video watermarking scheme made much robust.

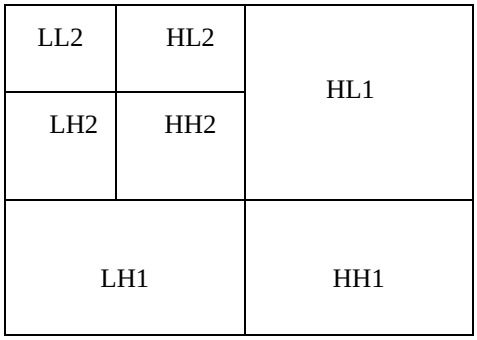

Figure3. 2- Level DWT sub-bands

In this, proposed a digital video watermarking technique based on identical frame extraction in 3-Level Discrete Wavelet Transform (DWT). In the proposed method, first the host video is divided into video shots. Then from each video shot one video frame called identical frame is selected for watermark embedding. Each identical frame is decomposed into 3-level DWT, and then select the higher sub band coefficients to embed the watermark and the watermark are adaptively embedded to these coefficients and thus guarantee the perceptual invisibility of the watermark. For watermark detection, the correlation between the watermark signal and the watermarked video is compared with a threshold value obtained from embedded watermark signal. The experimental results demonstrate that the watermarking method has strong robustness against some common attacks such as cropping, Gaussian noise adding, Salt & pepper noise adding, frame dropping and frame adding Index [14].

6. Discrete Wavelet Transform and Principal component analysis

In this paper, a hybrid approach for digital video watermarking is introduced, where a watermark logo is embedded into the video frames. Each video frame is decomposed into sub-images using 2 level discrete wavelet transform then the Principle Component Analysis (PCA) transformation is applied for each block in the two bands LL and HH.). PCA helps in reducing correlation among the wavelet coefficients obtained from wavelet decomposition of each video frame thereby dispersing the watermark bits into the uncorrelated coefficients the watermark is embedded into the maximum coefficient of the PCA block of the two bands. The proposed scheme is tested using a number of video sequences. Experimental results show high imperceptibility where there is no noticeable difference between the watermarked video frames and the original frames. The proposed scheme shows high robustness against several attacks such as JPEG coding, Gaussian noise addition, histogram equalization, gamma correction, and contrast adjustment [9].

C. Watermarks Based on MPEG Coding Structures

Digital Video watermarking method that uses MPEG-1, MPEG-2 and MPEG-4 coding structures as primitive components are mainly used with a the aim of combining watermarking and compression to reduce real-time video processing complexity. One of the major disadvantages of method based on MPEG coding

structures is that they are highly susceptible to re-compression with different parameters, as well as conversion to formats other than MPEG.

The motivation of combining the compression with watermarking introduce the techniques that use MPEG-2 or MPEG- 4 coding structure as the basic components. These techniques apply for real-time applications to reduce the overall time of processing. The method of block based compression such as MPEG-2 remove the temporal redundancy by using forward and bi-directional prediction, and statistical methods to remove spatial redundancy. The main drawbacks of this method are re-compression with other parameter or converting the compression format to another format is not being able to be done. It is easy for Employing cloud watermark for authenticating compressed MPEG-2 videos which is also able to differentiate malicious attacks from natural processing. In this method, the video is initially separated into video shots and the feature vectors are extracted. These feature vectors act as watermarks which will be embedded into the videos. The cloud model is used to demonstrate the randomness and fuzziness which exist in language values largely and the relationship between them, a kind of transforming model between qualitative concept and its numerical representation. The authentication process is done by a comparison between the watermark derived from the extracted cloud drops and scrambled and modulated features of the received video shots. Tamper detection is promised in this work although very limited attacks have been tested on this method, so the performance still remained a question. However, they could make an improvement by using some unique characteristics of each shot in cloud generating [17] [18].

III. CONCLUSION AND FUTURE SCOPE

It is observed from the work of various researchers that different method was proposed for digital video watermarking. Through all these method we can solve the problem of Video piracy but there is need to combine the existing method and try to develop a new hybrid method for digital video watermarking which will give the better result against various attacks and preserving the quality of video.

In the future, researcher may try to combine all the previous method for digital video watermarking and try to develop a new Hybrid approach of video watermarking which gives more accurate result against various type of attack and also improve the PSNR value.

REFERENCES

[1] Rakesh Kumar1 and Savita Chaudhary “Video Watermarking Using Wavelet Transformation” International Journal of Computer Trends and Technology (IJCTT) - volume4 Issue5–May 2013.

[2] Hamid Shojanazeri, Wan Azizun Wan Adnan, Sharifah Mumtadzah Syed Ahmad,, M. Iqbal Saripan ”Analysis of Watermarking Techniques in Video” 2011 IEEE.I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[3] Sadik Ali M. Al-Taweel, Putra Sumari, and Saleh Ali K. Alomar.“Digital Video Watermarking in the Discrete Cosine Transform Domain” Journal of Computer Science 5 (8): 536-543, 2009.

[4] Sanjana Sinha, Prajnat Bardhan, and Swarnali Pramanick,, "Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis," International Journal of Wisdom Based Computing, Vol. 1 (2), August 2011.

[5] Hanane,Hien,Yasnuori and Zensho “Digital Video Watermarking Based on Principal Component Analysis” 2007 IEEE.

[6] N. Leelavathy, E. V. Prasad and S. Srinivas Kumar “A Scene Based Video Watermarking in Discrete Multiwavelet Domain”, International Journal of Multidisciplinary Sciences and Engineering, Vol. 3, No. 7, July 2012.

[7] Lahouari Ghout and Ahmed Bouridane “Digital Image Watermarking Using Balanced Multiwavelets.”IEEE transactions on signal processing, vol. 54, no. 4, april 2006.

[8] Mrs Neeta Deshpande and Dr. Archana rajurkar “Review of Robust Video Watermarking Algorithms” (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 3, March 2010.

[9] Nisreen I. Yassin, Nancy M. Salem, and Mohamed I. El Adawy “Block Based Video Watermarking Scheme Using Wavelet Transform and Principle Component Analysis” IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3, January 2012

[10] T. Khatib, A. Haj, L. Rajab, H. Mohammed, “ A Robust Video Watermarking Algorithm”, Journal of Computer Science, vol. 4, pp. 910-915, 2008.

[11] Ying Li, Xinbo Gao, Member, IEEE, Hongbing Ji, Member, IEEE, “A 3D Wavelet Based Spatial-Temporal Approach for Video Watermarking,” Proceedings of the Fifth International Conference on Computational Intelligence and Multimedia Applications (ICCIMA’03)

[12] Sarabjeet Singh “Digital Watermarking Trends” International Journal of Research in Computer Science ISSN 2249-8257 Volume 1 Issue 1 (2011) pp. 55-61.

[13] Young-Yoon Lee ,Han-Seung Jung and Sang-Uk Lee “Lee 3D DFT-based Video Watermarking Using Perceptual Models” 2004 IEEE.

[14] Tamanna Tabassum and S.M. Mohidul Islam “A Digital Video Watermarking Technique Based on Identical Frame Extraction in 3-Level DWT”IEEE 2011

[15] Lama Rajab Tahani Al-Khatib and Ali Al-Haj “Video Watermarking Algorithms Using the SVD Transform “European Journal of Scientific Research ISSN 1450-216X Vol.30 No.3 (2009), pp.389-401

[16] Xiaoli Li, Student Member, IEEE, Sridhar (Sri) Krishnan, Senior Member, IEEE, and Ngok-Wah Ma, Senior Member, IEEE, A Wavelet-PCA-Based Fingerprinting Scheme for Peer-to-Peer Video File Sharing ,*IEEE Transactions on Information Forensics and Security, VOL. 5, NO. 3*, September 2010

[17] Ming Jianga, b, Zhao-Feng Mao, b, Xin-xin Niua, Yi-Xian Yang,” Video Watermarking Scheme Based on MPEG-2 for Copyright

[18] Hartung F and Girod B 1998” Watermarking of uncompressed and compressed video.” *Signal Processing* 66(3): 283–301

[19] Mayank Vatsa, Richa Singh and P. Mitra"2004 IEEE lntemational Conference on Systems, Man and Cybernetics Digital Watermarking based Secure Multimodal",

AUTHOR BIOGRAPHY

Nitin A. Shelke completed B.E. in Computer Science and Engineering from Sipna's College of Engineering Amravati, India in 2011 and now pursuing M.Tech in Computer Science and Engineering branch from Government college of Engineering Amravati. His area of research includes image processing, network security, pattern recognition, Data Mining, and neural networks.

Dr. P. N. Chatur has received his M.E. degree in Electronics Engineering from Govt. College of Engineering, Amravati, India and PhD degree from Amravati University. He has published twenty national level papers and fifteen international papers. His area of research includes Neural Network, data mining. Currently working as a head of Computer Science and Engineering department at Govt. College of Engineering, Amravati.