ISSN: 2454-6135 (Online) [Volume. 02 Issue.01, January-2016]

A Survey on Watermarking Different Techniques and Attacks

UrviShrivastava[1], Daya Shankar Pandey[2]

P.G. Scholar, Department of Computer Science and Engineering

RKDF Institute of Science and Technology, Bhopal, Madhya Pradesh.

Assistant Professor, Department of Computer Science and Engineering

RKDF Institute of Science and Technology, Bhopal, Madhya Pradesh.

India

1 * Correspondence author

Abstract

With the increase in the internet digital world is growing rapidly in large scale. As the digital data is made easy to transfer from one place to another. This easy movement of data leads to big issue of the copyright or the originality of the digital data for all this there watermarking authentication technique has been developed. In order to provide watermarking for different digital data like image, audio, video, etc. various techniques have been developed. This paper give different requirement, features for video watermarking. As hiding data is watermarking but it goes under some kind of attacks which are also cover in this paper as they are the best measure for comparing different techniques of watermarking.

Keywords: *Digital Data, Digital Watermarking, Image segmentation.*

---

1. INTRODUCTION

Digital watermarking is a kind of information or data hiding process by this digital data authentication is provided. This can be understood as the ease of transfer of the data from one place to another. This is so fast and flexible that manipulation of the original content might possible, so it might get difficult for the user or the end party that the content it using is original or not. In order to provide some procedure for checking the originality of the digital content this technique of digital watermarking has been developed. Now some important parameters which should be taken care are to balance the hiding content into the original one. This can be understand as if the original content is overload by the hiding content then chance of the original content loss is more.

So watermarking techniques has to care a lot for the complete authentication of the originality as well as without affecting the data. Whole process of authentication is done in two steps.

In first step original information is taken as input with the watermark or data to hide. Now apply embedding data in the original data. As shown in fig. 1 here some time key is required for the embedding then watermarked information is read to transfer.

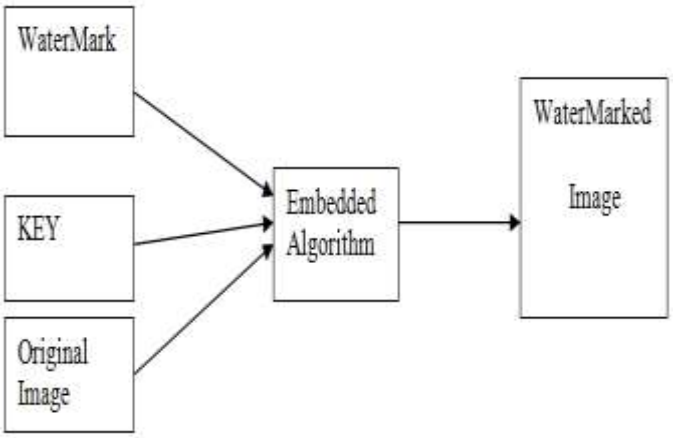

Figure.1. Embedding of watermark

Second step is to extract watermark information from the received data. This step is known as watermark extraction. As shown in fig. 2 if key is use for embedding then exact watermark is obtained if correct key is use during extraction.

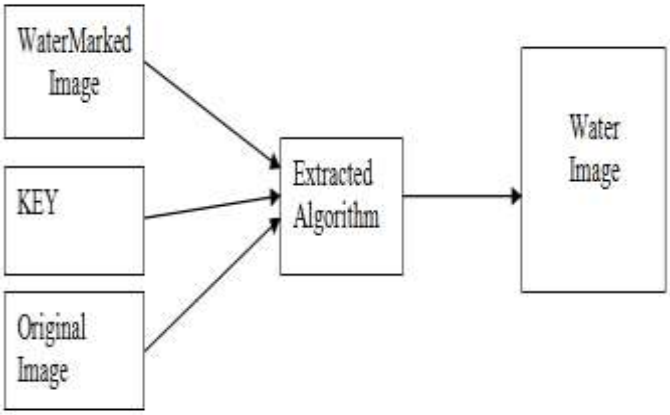

Figure2 Extraction process.

Watermark embedding and extraction algorithm should have below requirement for the proper effectiveness.

A. Unobtrusive – It is desired that watermark information is invisible.

B. Robustness – Embedding and extraction algorithm are need to be so strong that no one can crack the watermark even after whole algorithm steps are known publicly. Algorithm should be robust against various attacks like geometrical, noise, etc.

1) **Common signal processing:** Watermark steps should be robust against common signal processing of analog to digital and digital to analog changes. So under this changes information is need to unaltered
2) **Geometrical attacks:** Here some kind of rotational attacks are apply. Cropping of image or video frame is also come under geometrical attacks. Increase or decrease dimension of the image.
3) **Subterfuge attacks:** Here different user has copies of watermark then it should be robust to construct new copy of watermark. Moreover, it should be impossible to combine the copies to create a new valid watermark.

C. Unambiguous – Watermark should identified the owner uniquely. As same watermark conflict user for the identification of real dat.

D. Loyalty - A watermark has a high reliability, if the degradation it causes is very difficult to perceive for the viewer. (Reliability)

E. Computational Cost - Embedding and extraction of watermark from the video both should be fairly fast and should have low computational complexity.

2. DIGITAL IMAGE WATERMARKING CLASSIFICATION AND ATTACKS

Some of the important types of watermarking based on different watermarks [3] are given below:

2.1 Visible watermarks

This type of watermarking resembles the concept of the logos on different item to specify the product. Now these are visible in the whole data such as in case of video one constant light background or presence of logi in the video

act as visible digital video watermarking, then in case of image a kind of figure appear in the image but it is not the part of the image.

2.2 Invisible watermark

In this type of watermarking watermark data is hiding in the original data. This can be understand as some frame part which are constantly changing are those part where if small changes are made then those part is not detectable of the presence of the unrelated content so it cannot be judge by the naked eyes. This kind of watermark is known as invisible watermarking.

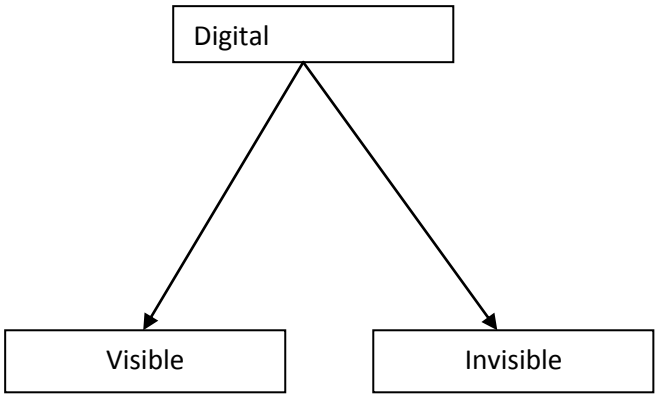

Figure3Different types of watermarking methodologies.

3. FEATURE FOR VIDEO WATERMARKING

Different features for object detection: - As video is collection or sequence of frame and each frame is treat as single image which is a kind of matrices. In order to identify an object in that image some features need to be maintained as different object have different feature to identify them which are explain as follows:

3.1 Colure feature: Here as video is collection of frames and each frame is collection of pixels, where each pixel represent the colour intensity. Now pixel value of the image actually represents colour. Calculation of the colour feature is cost effective as compare to other features. This colour plays important property of the frame when any object need to identified. As object geometry change frame to frame but pixel colour is almost same. So colour plays an important role in object detection as well as image retrieval.

As image or videos are available in different colour format where each format has its own range for pixel value. This can be understand as if frame is in gray format then pixel value lie in 0-255 range while in case of RGB pixel value lie in 0-1. In case of HSV format Hue value lie in 0360 while Saturation and Value lie in 0-1 range. As these colour help in face detection as in [8].

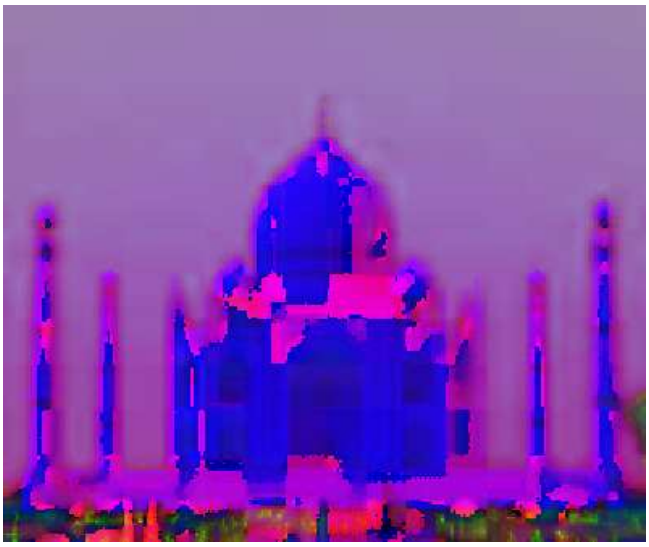

Figure.4. Represent the HSV (Hue Saturation value) format of an image.

3.2 Edge Feature: Each frame of video or image contains different objects where each object is identified by drawing its boundary. Once boundary is identified then colour makes its appearance attractive.

With change in the pixel value edge feature is identified. Here different edge detection algorithm is utilized for this feature such as canny, sobel, perwitt, etc [5]. Canny is best algorithm for the edge detection as it idenfied correct pixel position of the image. Example of the edge of the image is shown in fig. 5.

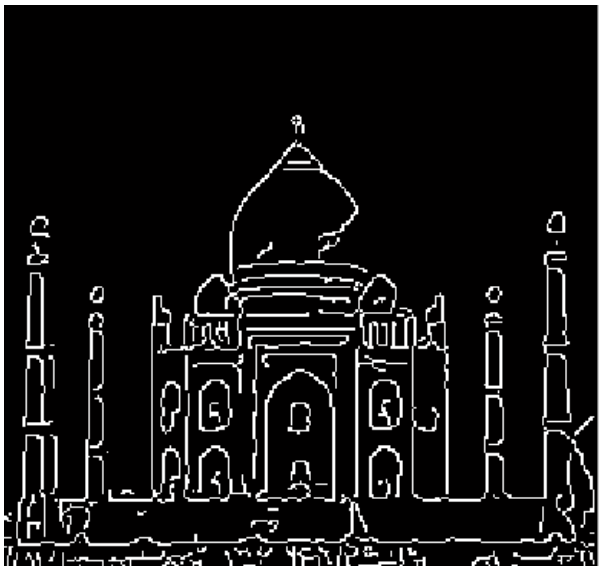

Figure.5 Represent Edge feature of an image.

Texture Feature: In order to calculate smoothness or regularity of the surface of image one important feature is texture of the image. Here this feature calculate different energy of the image in form of CCM (Co-Occurrence matrix). As this calculation is less sensitive to the image intensity changes.

Corner Feature: In order to stabilize the video frames in case of moving camera it require the difference between the two frames which are point out by the corner feature in the image or frame. So by finding the corner position of the two frames one can detect resize the window in original view. This feature is also use to find the angles as well as the distance between the object of the two different frames. As they represent point in the image so it is use to track the target object.

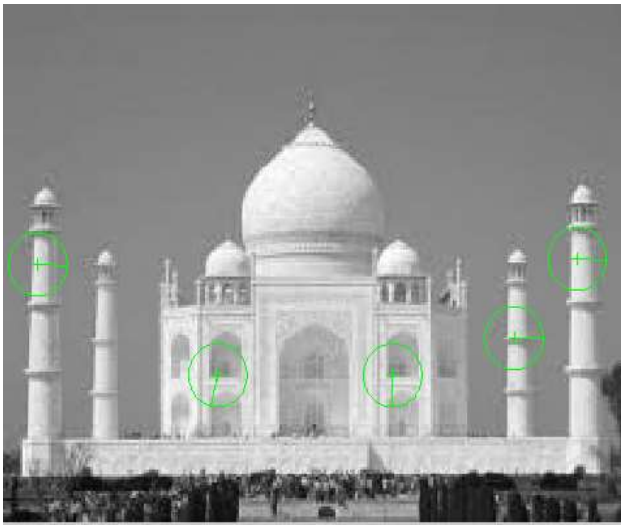

Figure.6 Represent the corner feature of an image with Red point.

DWT (Discrete Wavelet Transform):

Figure.7 DWT of image from [5]

LL: The upper left quadrant consists of all coefficients, which is filtered by the analysis low pass filter along the rows and then filtered along the corresponding columns with the analysis low pass filter again. This subblock is denoted by LL and represents the approximated version of the original at half the resolution.

HL/LH: The lower left and the upper right blocks were filtered along the rows and columns with low and high pass filter alternatively. The LH block contains vertical edges,

mostly. In contrast, the HL blocks shows horizontal edges very clearly.

HH: The lower right quadrant was derived analogously to the upper left quadrant but with the use of the analysis high pass filter which belongs to the given wavelet. We can interpret this block as the area, where we find edges of the original image in diagonal direction.

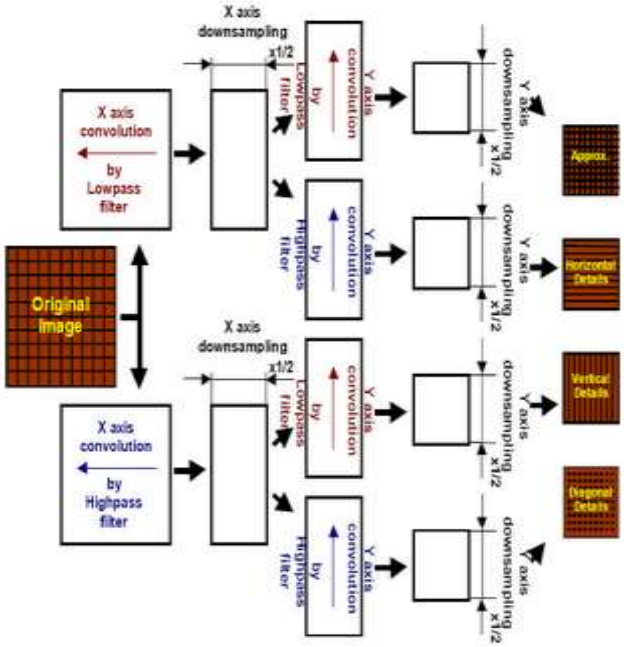

Figure.8 PCA (Principal component Analysis)

4. VIDEO WATERMARKING TECHNIQUES

In [1] video is partitioned into frames where PCA technique is applied on the scenes. Each scene is divide into cubes of fix size. Now all cubes are analyzed for the selection of watermark embedding this selection is based on the selected pixel average. Apply DWT on the selected cubes follow by PCA. Whole process is apply on all the selected cubes till watermark information is hide. In extraction whole process is repeat as done in embedding part where video is divide into scene then cube and selected cubes are utilize for retrieving watermark from each cube.

In [3] DWT technique is applied for embedding watermark. Here 3-level DWT is applying on the video frame. So, video impression into separate frames of RGB format. Now convert each RGB frame to gray format. Now embedded water mark in LL portion of the 3 level DWT. Finally inverse DWT is applying for the image.

In [8] watermarking in video is done by utilizing modified DCT and LSB technique. Video is first divide into frames for analyzing the embedding positions. Here selected frames have minimum information loss is consider for embedding by utilizing LSB technique.

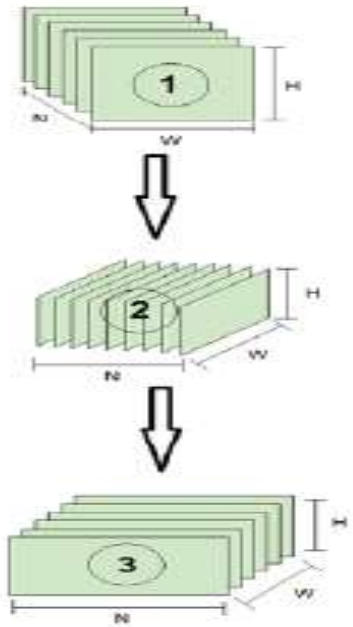

Figure.9 Side view conversion of video frames

In [2] as shown in fig. 9 watermarking of video is done by using side matrix of the frames. In order to make side view rotate the frame by 90 degree for the frame. Now apply DWT on this side view. After this apply the Singular Value

Decomposition (SVD) in the horizontal part of the DWT then embedded the watermark in this part and reconstruct the video frame in reverse order.

In [9] one more algorithm has developed using the PCA and DWT technique. Here divide the video frame and convert RGB frames in to YUV components. Then for each frame, choose the luminance Y component and apply DWT to decompose the Y frames in to four multi resolution sub bands LL, HL, LH, HH. After this divide the two sub bands LL and HH into n x n non overlapping blocks and apply PCA to each block in the chosen sub band LL and HH. Now embedded the watermark in to LL and HH bands with the help of DWT and PCA for HH band, the watermark bits are embedded. At last apply inverse PCA on the modified PCA component of the two -bands to obtain modified wavelet coefficient.

5. WATERMARK ATTACKS

Different kind of attacks are done on the digital watermarked video, the main effect of these attack is that extraction of watermark is quite difficult or not possible by the algorithm if proper precaution is not taken in prior steps of watermark embedding.

Noise Attack: As watermarked video is send in the channel for communication then some kind of noise normally generate by which exact water is not extract from the received data [6]. Different kinds of noise are: Salt Pepper Noise, Gaussian Noise Attack, Speckle Noise Attack, etc.

Filter Attack: Here video is passing through different filter, which is generally done after receiving signal from the network. So this attack is normally happen and for this the embedding as well as extraction algorithm of the video watermarking should be robust, so that effective method is developed. Some filtering attacks are: average filter, median filter, sharpen filter and motion filter [6,7].

Compression Attack: Here video is pass through different compression techniques, which is generally done after receiving signal from the network [7]. So this attack is normally happen and for this the embedding as well as extraction algorithm of the video watermarking should be robust, so that effective method is developed. Some filtering attacks are: MPEG compression, Mp4 compression, etc.

5.1 Detection-disabling attacks

Some time watermarking algorithm are based on the correlation and to make detection of the watermark so by changing this correlation make it impossible to fetch watermark from the received data. 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 [3, 6]. Mostly, they make some geometric distortion like zooming, shift in temporal direction, rotation, cropping or pixel permutation, removal or insertion.

5.2 Ambiguity attacks

Here by introducing different watermark to confuse the detector by producing fake watermarked data to discredit the authority of the watermark by embedding several additional watermarks.

6. CONCLUSION

Here whole paper has described different techniques of watermarking. Paper has shown that techniques are categorize into visible and invisible watermarking. Different features of the video are also analyzed for the video which can be use for selection of pixels where watermark information can be embedded. Paper has also give detail description of the various attacks on the watermarked video. Detail discussion of various paper has also done with their implementation algorithm. Strength and weakness for all the watermarking techniques are studied. In future a novel hybrid techniques is essential to meet out the robustness against various attacks

REFERENCES

1. HaniehKhalilian, *Student Member, IEEE,* and Ivan V. BajicVideo "Watermarking With Empirical PCA-Based Decoding" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 12, DECEMBER 2013.
2. Walter Godoy Jr., Charles Way Hun Fung " A novel DWT-SVD video watermarking scheme using side view" 978-1-4577-1180-0/11/$26.00 ©2011 IEEE.
3. TamannaTabassum, S.M. Mohidul Islam "A Digital Video Watermarking Technique Based on Identical Frame Extraction in 3-Level DWT" vol. 13, no. 7, pp. 560 –576, july 2003.
4. Frank Hartung, Jonathan K. Su, and Bernd Girod "Spread Spectrum Watermarking: Malicious Attacks and Counterattacks". of Multimedia Contents" International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308
5. "CHAPTER 2. WAVELET TRANSFORMS ON IMAGES"*sundoc.bibliothek.uni-halle.de/diss-online/02/03H033/t4.pdf*
6. A.F.ElGamal, N.A.Mosa ,W.K.ElSaidA Fragile Video Watermarking Algorithm for Content Authentication based on Block Mean and Modulation Factor *International Journal of Computer Applications (0975 – 8887) Volume 80 – No.4, October 2013.*
7. Nallagarla.Ramamurthy and Dr.S.Varadarajan. "Effect of Various Attacks on Watermarked Images. "International Journal of Computer Science and Information Technologies, Vol. 3 (2) , 2012,3582-3587
8. Priya Porwal1, Tanvi Ghag2, Nikita Poddar3, AnkitaTawde DIGITAL VIDEO WATERMARKING USING MODIFIED LSB AND DCT TECHNIQUE. International Journal of Research in Engineering and Technology eISSN: 2319-1163.
9. Mr Mohan A Chimanna 1,Prof.S.R.Kho "Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery" Vol. 3, Issue 2, March -April 2013, pp.839-844839.