Live Video Copyright Adaptive Multiwavelet-Based Watermarking

[1] Vijayashri Dangale, [2] Anil Warbhe, [3] Shyam Dubey

[1] Department of Computer Science and Engineering
Nuva College of Engineering and Technology, Nagpur, India

[2, 3] Assistant Professor, Department of Computer Science and Engineering
Nuva College of Engineering and Technology, Nagpur, India

Abstract - Rapid development and wide use of Internet, and transmitting information faces a big challenge of security. Hence, for transmission of an information people need a safe and secured way. Digital watermarking is a technique of data hiding, which provide security to the data. Detection and prevention of video tampering and to distinguish it from common video processing operations, such as noise, and increase brightness, recompression using a practical watermarking scheme to authenticate real-time digital video is important. Our method can be easily configured to adjust robustness, transparency, and the system capacity according to the specific application. In addition, content-based cryptography increases the security of the system. This paper presents a critical review on various techniques. In addition, it introduce the main key performance indicators which involve robustness ,capacity, speed, fidelity ,imperceptibility and computational complexity.

Keywords - *Watermarking Image Authentication, Copyright Protection, Multimedia Security.*

1. Introduction

Ease of access to digital information has improved due to rapid development of new information technologies. It also cause the problem of illegal copying and redistribution of digital media . Among these media, video is becoming most important in a variety of applications, such as video surveillance, video broadcasting, DVDs, video conference, and video on demand applications, where authenticity and integrity of the video data is critical. Content-based video authentication concept builds upon the increasing need for trustworthy digital multimedia data in many applications such as commerce, industry, defence, surveillance, journalism and video broadcast etc.

Without authentication a video a consumer (or viewer) cannot verify that the video being viewed is really the original one or that was not transmitted by a producer . May be there is some eavesdroppers who modify the video content intentionally to harm both the producer and the consumer interests (or viewer). For providing value added protection on top of data encryption and scrambling for content protection, Digital Watermarking is intended by its developers .

This paper addresses the problem of ensuring the authenticity and the integrity for video and also provides security with the help of concept of content-based cryptography. Hence, fidelity, robustness and imperceptibility are the critical indicators for effective technique.

2. Background

2.1 Digital Watermarking

This technique is used to hide data or identify information within digital multimedia. This digital multimedia includes image, text , audio or video media. Without significantly degrading its visual quality, the digital watermarking process embeds a signal into the media. Watermark information can be embedded into different kind of media by using digital watermarking process. The information inside a signal, which cannot be easily extracted by the third party, is hide by using Digital Watermarking process. Its widely used application is copyright protection of Digital Information. It differs from the Encryption process. It protects the ownership of the content but allows the user to access, view and interpret the signal. One or more watermark is embedded into single multimedia object in multiple watermark. Multiple watermark is a process to provide extra security to an image by embedding multiple number of secret messages into the cover image. In the present, both copyright as well as authentication information are hidden by using concept of multiple watermarking into colour image.

2.2 Classification of Watermarking Attacks

Operations that destroy watermark data are called attacks [8]. They affect the watermarking algorithms and destroy it to damage video frame. Few best known attacks are as follows,

- **Simple attacks:** Simple attacks attempt to impair the embedded watermark by manipulations of the whole watermarked data, without an attempt to identify and isolate the watermark.

- **Detection-disabling attacks:** (also called as “synchronization attacks”) It causes recovery of the watermark impossible or not feasible for a watermark detector by breaking correlation, mostly by geometric distortion like zooming, shift in (for video) direction, cropping, rotation, sub-sampling, pixel permutations, removal or insertion of pixels or pixel clusters.

- **Ambiguity attacks:** (other possible names include “Deadlock attacks,”“Inversion attacks”) It attempt to confuse by producing fake watermarked data or fake original data [6].

- **Removal attacks:** are attacks that try to analyze the watermarked data, also estimate the host data or watermark, separating both watermarked data and host data but only the watermark is discarded [6].

- **Cryptographic attack:** Cryptographic attacks also involve cracking of the security.

2.3 General Watermarking System

In general, digital watermarking scheme, allow us to embed some Information (i.e., watermarks) into some host signal , even if cover objects are corrupted by a small amount of permissible noise, in such a way that these watermarks can later extracted or detected. A watermarking scheme consists of three major components. Desired watermarks for a particular application are generated by using a watermark generator, which are optionally dependent on some keys. Watermark is embedded into the cover object by using embedder which is based on an embedding key. The existence of some predefined watermark is detected by using detector in a cover object, and sometimes it is desirable to extract a message from the watermarked cover object [16].

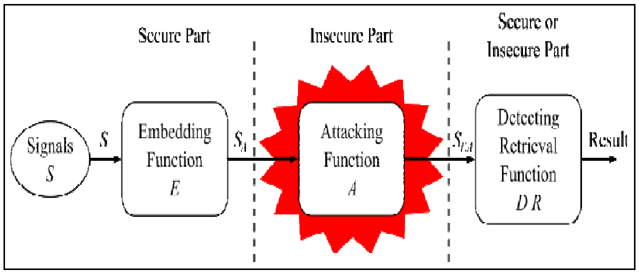

Fig1: Digital Watermarking Systems

2.4 Discrete Cosine Transform (DCT)

DCT has good energy compaction capability; it is feasible to incorporate the HVS characteristics; the sensitivity of HYS to the DCT basis images has been extensively studied resulting in a default JPEG quantization table. Generally speaking, in order to be resistant to noise the watermark has to be added to frequencies of high energy. A sequence of finitely many in terms of a sum of cosine functions oscillating at different frequencies are expressed by discrete cosine transform (DCT) [22].DCTs are important to numerous applications in engineering and science, such as lossy compression of images and audios, where small high frequency components can be discarded. In these applications , the use of cosine rather than sine functions is critical: for compression, fewer functions are needed to approximate a typical signal. It turns out that cosine functions are much more efficient. The main advantage of DCT techniques is in robustness against generally simple image processing modifications such as low pass filtering, brightness, contrast adjustment and blurring.In this according to the name whole data is encrypted. So it re- quires more execution time.

2.4.1 Selective Encryption

In this technique whole I-frame is encrypted. It requires the less execution time as compare to full encryption but cannot satisfy actual instance necessity. And it cannot satisfy the actual moment.

2.4.2 Slice Level Encryption

|The MPEG which is the standard of video compression is used to protect the video.MPEG 2 having the inaccuracy

circulation property. Because of this requires less computational workload. The fundamental proposal behind the proposed approach is to reduce the workload of encrypting the I-frames by exploiting the inaccuracy circulation property in MPEG2 standard. The slide contains the micro blocks. Because of inaccuracy circulation Property, if only first micro block is encrypted then the successive micro blocks are encrypted. This technique takes less computational workload and requires less execution time than other approaches. In this, first the live video is captured and then converted it into the number of frames. And after the encryption whole video we are getting as it is. The below figure shows the how much percent of the frames are encrypted. The shaded portion shows the encrypted region. In level 0, there is no encryption takes place. In level 1, only header is encrypted and at level 2, only I block is encrypted. In level 3, I frame and I block is encrypted [1]. SECMPEG is the secure MPEG.

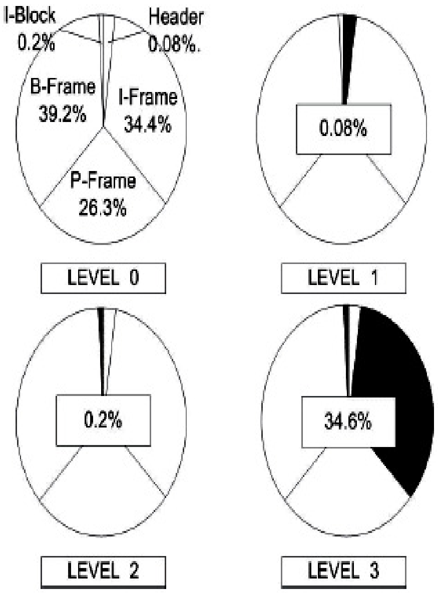

Fig 2 : Slice Level Encryption

2.4.3 Overview of I, B, P-Frames

I-frames are the slightest compressible but don't have need of other video frames to decipher. P-frames can utilize information from preceding frames to decompress and are extra compressible than I-frames. B-frames can utilize equally preceding and front-ward frames for information reference to get the maximum quantity of information density. An I-frame is an 'Intra-coded picture', in result a entirely precise image, like a predictable stationary picture file. P-frames and B-frames clutch just fraction of the image information, so they need less space to store than an I-frame, and thus rove video compression rates. A P-frame ('Predicted picture') holds only the changes in the image from the preceding frame. For example, in a scene where a car moves across a stationary back- ground, only the car's movements need to be encoded. The en- coder does not need to store the unchanging surroundings pixels in the P-frame, thus saving space. P-frames are also called as delta-frames. A B-frame ('Bi-predictive picture') saves even extra space by using differences between the present frame and both the past and subsequent frames to identify its substances.

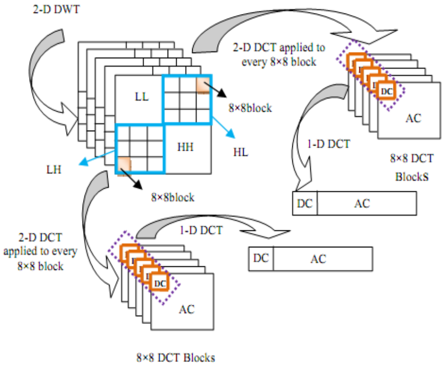

Fig.3: Overview of I, B, P-Frames

Algorithm :

Video sequence characteristics, the B-frame and P-frame are dependent on the I-frame. A sequence of several still images can also be considered as raw video data. The flowchart of the proposed method

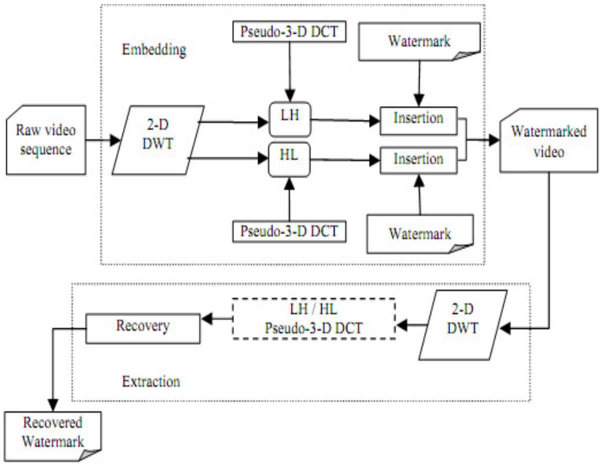

Fig. 4: Flowchart

4. Proposed System

A watermark is a digital code permanently embedded into cover content into a video sequence. Any information you can imagine can be carried by watermark but the amount of the information is unlimited. The more information a watermark carries the more vulnerable that information the amount is absolutely limited by the size of particular video sequence. Watermarking prefers robustness to capacity to watermark, thus a watermark typically carries tens to thousands of hidden information bits per one video frame.

Nowadays, several particular watermarking techniques have been developed. One of the particular problems in digital watermarking applications is synchronizing a detector to deal with geometric warping distortion of a watermarked image or video. A number of techniques have been developed for dealing with geometric distortion[17] in watermarked images. By embedding it in attributes of the image that are relatively invariant to geometric distortion as well as non linear geometric distortion watermark are made more robust to geometric distortion. While this improves detection in some of the cases, it typically does not address all forms of more complex, non-linear geometric distortion as well as geometric distortion. Another technique is used for detection and estimation of the geometric distortion parameters, such as scaling and rotation which include geometric calibration features in the watermark signal .

In our proposed method, narrowband signals are transmitted over a much larger bandwidth. To keep energy in any one bin very small and certainly undetectable, watermark is spread over very many frequency bins. DCT (Discrete Cosine Transformation) should apply first in order to insert a watermark in the frequency domain of an image because it is a standard way to represent an image in frequency domain and spatio-temporal domain.

In one implementation, to transform an image block in the watermarked image to a position approximating an original orientation of the image block in the watermarked image, the method uses an estimate of affine geometric distortion parameters. It then shifts the transformed image block to neighboring locations. By finding the correlation between the transformed block and the watermark signal at its location and each of the neighboring locations, the method computes a correlation surface. The method finds a correlation maximum, formed by the correlation values in the neighborhood, in the correlation surface. The location of the correlation maximum provides an offset value that further refines the orientation of the image data. From the watermarked image, message decoder decodes the watermark message adjusted by the offset value. Additionally, to provide more security a content based cryptography is used.

Architectural Data Flow Diagram:

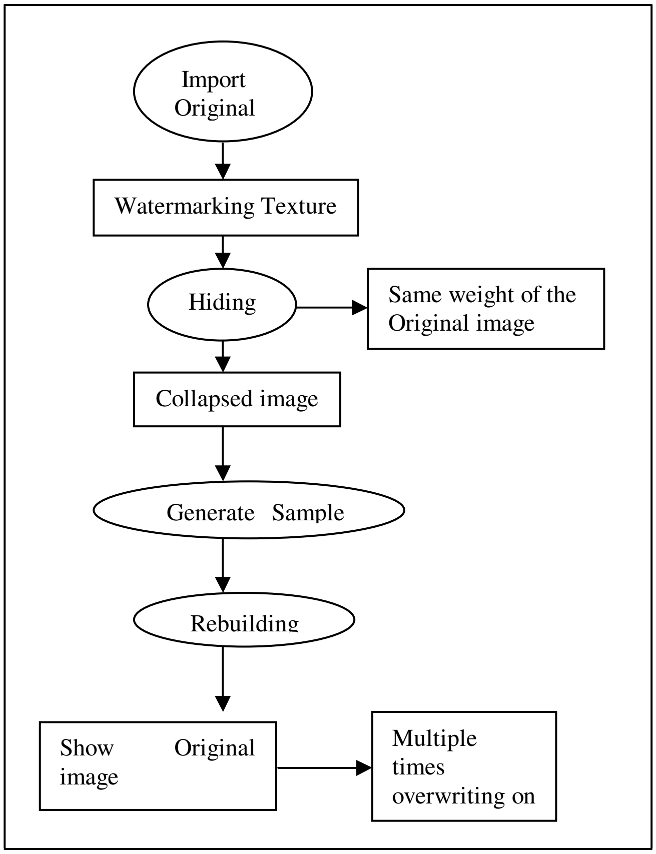

Fig 5: Data Flow Diagram

Method presented by the multiple-watermarking has shown to be suitable for use in medical images. To embed patient information in a private and secure manner ,the annotation watermark can be used, while the fragile watermark offers tamper detection. Watermarked image visual quality is very good. Under some general image manipulation attacks, the effectiveness of the fragile part in tamper detection has been proven. The annotation watermark is meant without increasing storage space requirement, to store context information in a private manner. Nevertheless using malicious attack techniques it is possible to destroy it. Instead of in the image borders, the annotation watermark should be embedded in textured regions of the image to overcome such weakness. In addition, to improve its security a hash-block-chaining watermarking approach can be adopted in the fragile watermarking part. These issues will be investigated in our ongoing work.

A multiple Watermarking Scheme for Medical Image in the Spatial Domain

Watermarking Properties

The watermarking properties are the parameters allowing the identification of signature characteristics.

Without distorting visual quality of the image, the watermarking system must embed the watermark in the image. To verify the imperceptibility of the watermarking algorithm, suitable metric must be used. In this project, I did not use any mathematical metric to quantify the distortion due to watermarking. Instead, we commented on the visual quality of images, by comparing how the original image and watermarked image look. In fact, the watermarking system must embed the watermark in the image in such a way that the visual quality of the image is not perceptibly distorted.

The insertion capacity depends generally on the application used for the image. In fact, in the medical field the signature can express information on the patient medical stereotype. Each time the size of the signature increases there will be degradation of the medical image.
Specificity The watermark must be sufficiently specific to be clearly identifiable during its extraction. It must also be exact to identify clearly the concerned person and any mistake can change the result. Security of watermarking and encryption techniques are very much similar. A watermarking technique is actually protected if algorithms used to embed and extract the watermark does not allow an unauthorized party to detect the presence of the watermark.

We have shown that compared with the existing similar methods, which also embed bits inside video frames, significantly smaller video distortion occurs in our method, leading to a noise degradation of about 0.08 dB and structural similarity index decrease of 0.0090 with only 0.05% increase in bit rate, and with the bit correct rate of 0.71 to 0.88 after recompression. At the distortion level, the bit rate in increases bout 2.13% compared with 0.06% in our method. For example, if the original bit rate is 200 kb/s, using , we will need to support a 56.8-kb/s increase of the bit rate, compared with only 0.48-kb/s increase using our method, which is orders of magnitude better than Morphological filter provides better robustness against Gaussian noise, recompression, and brightness increase; however, its robustness against salt and pepper noise has not be reported. Our proposed scheme and both work perfectly against temporal attacks, such as frame dropping. Our method is robust against attacks, such as, jittering, dropping and delay, since extracting and detecting the secret bits are only based on each single frame and independent from other frames. This is very useful for networked applications where these attacks can happen frequently. The experimental results show that the distortion caused by our system is very low on average, is -0.88 dB, increasing bit rate is just 0.05%, and after recompression is 0.71–0.88. Security of the video is increased by adding content-based cryptography to the watermarking system.

The performance of any watermarking system can be improved by applying . In our system, one bit in each is assigned for frame indexing, as explained before. We need 10 bits for frame indexing, and there are about 99 bits to embed the frame's index. For example, using 10 bits can be converted to 15 and the 15 bits repeated five times in each frame. The type of and repeating depends on the application's requirements.

For instance, surviving against Gaussian noise needs a good filter whereas increasing the repeating time increases robustness against burst errors. In our experimental results, to get robustness against . recompression, it was sufficient to use the repeating idea. After recompression, the frames' indices are extracted successfully.

5. Conclusion

This paper reviews basic watermarking techniques as applied to different media types. Watermarking is an important technique that has the potential of incorporating an embedding process and preventing easy separation of watermark from content. It also has an enabling technology for a number of applications which imposes different requirements on the watermarking system. Owing to these strengths, digital watermarking is suggested as the ultimate solution to protect digital properties from piracy and copyright infringement .The use of watermarking related consists of digital rights management systems, remote sensing applications and video surveillance, digital insurance claim evidence and trusted cameras. In security monitoring, watermark is used to make sure that all video inputs are from authorized sources. A watermark which describes the work is sometimes used in these applications. It is important that the description of the file is unique and hard to obtain by an attacker.

References

[1] Dong Zheng , Sha Wang, and Jiying Zhao, Member IEEE"RST Invariant Image Watermarking Algorithm With Mathematical Modeling and Analysis of the Watermarking Processes" IEEE Transactions On Image Processing, Vol. 18, No. 5, May 2009.

[2] Mehdi Fallahpour, Shervin Shirmohammadi,Senior Member,IEEE,Mehdi Semsarzadeh, and Jiying Zhao, Member, IEEE"Tampering Detection in Compressed Digital VideoUsing Watermarking" IEEE Transactions On Instrumentation And Measurement, Vol. 63, No. 5, May 2014.

[3] P.-C. Su,C.-S. Wu, I.-F. Chen, C.Y.Wu, and Y. C. Wu,"A practical design of digital video watermarking in H.264/AV for content authentication,"Signal Process, Image Commun.,vol. 26, nos.8–9, pp. 413–426, Oct. 2011.

[4] Manjunath.M , Prof. Siddappaji " A New Robust Semi blind Watermarking Using Block DCT and SVD"IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT) 2012.

[5] Deepshikha Chopra1, Preeti Gupta2, Gaur Sanjay B.C.3,Anil Gupta "Lsb Based Digital Image Watermarking For Gray Scale Image" IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 1 (Sep-Oct. 2012), PP 36-41.

[6] S. Radharani, Dr. M.L. Valarmathi "Multiple Watermark- ing Scheme for Image Authentication and Copyright Protection using Wavelet based Texture Properties and Visual Cryptography" International Journal of Computer Applications (0975 – 8887) Volume 23– No.3, June 2011.

[7] Preeti Gupta,"Cryptography based digital image water- marking algorithm to increase security of watermark data", International Journal of Scientific & Engineering Research, Volume 3, Issue 9 (September 2012) ISSN 2229-5518 .

[8] B.Surekha, Dr G.N. Swamy, "A Spatial Domain Public Watermarking", International Journal of Security and It Applications Vol. 5 No. 1 January, 2011.

[9] Brigitte Jellinek,"Invisible Watermarking of Digital Image for Copyright Protection" University Salzburg, pp. 9 – 17, Jan 2000.

[10] Lihong Cui and Wenguo Li "Adaptive Multiwavelet Based Watermarking Through JPW Masking" IEEE Transactions On Image Processing, Vol. 20, No.4, April 2011.

[11] Satyendra N. Biswas , Sabikun Nahar, Sunil R Das, Emil M. Petriu, Mansour H. Assaf, and Voicu Groza "MPEG-2 Digital Video Watermarking Technique" IEEE Conference 2012

[12] Jihah Nah, Jongweon Kim " A digital watermarking Robust to geometric distortion" a Springer access on Computer Applications for Web, Human Computer Interaction, Signal and Image Processing, and Pattern Recognition Volume 342, 2012, pp 55-62 .

Vijayashri Dangale BE (Information Technology) from Priydarshanis J.L.College of Engineering, Nagpur in 2012. Appearing Mtech 4th sem (computer science) from Nuva College of Engineering & Technology , Nagpur.

Ass. Prof. Anil Warbhe BE, ME from M.I.E.T College Of Engineering Gondia Anilwarbhe.miet@gmail.com

Ass. Prof. Shyam Dubey Shyam.nuva@rediffmail.com