A Watermarking Scheme with Scrambled Watermark for Authentication of Video

[1] J.V. Bagade, [2] Nilesh Khare, [3] Nikhil Patil, [4] Abhijeet Kumar

[1, 2, 3.4] Department of Information Technology, VIIT
Pune, Maharashtra 411048, India

Abstract- Digital video is one of the popular multimedia for exchanging data over internet. Due to their perfectly replicable nature many unauthorized copies of the original video can be reproduce. Therefore, methods are required to protect copyrights of the authorized owner and prevent illegal piracy. In this paper, a robust Discrete Wavelet Transform (DWT)-based blind digital video watermarking scheme with scrambled watermarks based on scene changes has been proposed for authentication of digital video, which embeds different parts of a single watermark into different scenes of a video. The watermarking algorithm is very powerful against the attacks of frame dropping, averaging and compression, which are some of the common types of attacks applied particularly on the video and due by the use of DWT it can also withstand geometrical attacks making the watermark perceptually invisible. The proposed algorithm has been compared with an existing DWT based watermarking scheme and is found to exhibit better robustness.

Keywords- *DWT, Video Watermarking, Encryption*.

1. Introduction

Video is always a three-dimensional array of color pixels. Two dimensions serve as horizontal and vertical directions of the moving pictures, and one dimension represents the time domain. Digital video evolved as a growing presence in various areas, from digitized course lectures to archival footage housed in the campus library. Video conferencing, Internet-based communication and teaching, video on demand are some of the key areas which include usage of video. Technology has been advanced in such a rapid rate that it has given multimedia users the ability to tamper with, produce copies of, and illegally redistribute digital material. The fast growing use of internet can facilitate piracy or duplication on a large scale. The owner of the particular digital content, always ensures that all access to the content is authorized under the rules of a license (conditional access), and unauthorized reproductions cannot be easily made, and any illegal copies that are created can be detected and traced .If these security issues are not solved, digital multimedia products and services cannot be boomed in an e-commerce setting [1]. An ideal and unique solution to this problem would be to somehow integrate or join the security information directly into the content of the multimedia document, such that the security information should not be separated from the document during its useful lifespan. Also, the additional information should be perceptually invisible as the multimedia documents are eventually processed by humans who view it or listeners and the contents should not be affected. Watermarking provides the desired and feasible solution. In watermarking methods, the presence of the embedded information is not known to unauthorized parties who can access to the data, and can perform attacks. Also, many digital watermarking schemes have been proposed for still images and videos too. Most of them operate on uncompressed videos [2, 3], while others embed watermarks directly into compressed videos [4, 5]. The work on video watermarking can be further found in [6, 7, 8, 9].

Some weakness of the existing algorithms is:

(i) The watermark is not robust to attacks if specifically targeted at videos and even if the watermark is robust, they fail to resist when image attacks are performed on them.
(ii) None of the existing watermarking schemes prevents the attacks.

This is specifically because most of these techniques have been taken from the image watermarking algorithms. Video watermarking consists of number of issues which are not present in image watermarking. Since there are large amounts of data and inherent repetition between frames, video signals have high possibilities to piracy attacks, including frame averaging, frame dropping, frame swapping.

All the proposed algorithms in the literature do not solve these problems in an efficient manner. Hence a watermarking scheme which shows robustness against video and image attacks and yet enables blind retrieval of the watermark is proposed in this paper.

2. Literature Survey

Jantana Panyavarapom[1] et.. al..The growth of video watermarking technologies that can be used for copyright protection of video sequences is increasing at the same pace as the growth in digital communication technologies. Copyright protection involves the authentication of video content and/or ownership and can be used to identify illegal copies of a video. One approach for copyright protection is to introduce an invisible signal known as a digital watermark. There are many contributions in applying watermark in image and video sequence from previous researchers. However, we found that different researchers proposed the adoption of watermark techniques in different way. There are many different watermark algorithm proposed for digital images. The images contain multifold bands compared to the three bands in RGB color images. A robust DWT based blind digital video watermarking scheme with scrambled watermarks based on scene changes has been proposed for authentication of digital video, which embeds different parts of a single watermark into different scenes of a video .

Raghavendra K and Chetan K.R [2] et..al.. Digital video is one of the popular multimedia data exchanged in the internet. Due to their perfectly replicable nature many illegal of the original video can be made. Methods are needed to protect copy- rights of the owner and prevent illegal copying. A video can also undergo several intentional attacks like frame dropping, averaging, cropping and median filtering and unintentional attacks like addition of noise and compression which can compromise the owner information thereby denying authentication.

In this paper, a robust Discrete Wavelet Transform (DWT)-based blind digital video watermarking scheme with scrambled watermarks based on scene changes has been proposed for authentication of digital video, which embeds different parts of a single watermark into different scenes of a video. The video watermarking algorithm is robust against the attacks of frame dropping, averaging and compression, which are considered as some of the common types of attacks applied particularly on the video and due to the use of DWT it can also withstand geometrical attacks making the watermark perceptually invisible. Furthermore, it allows blind retrieval of embedded watermark which does not need the original video. The proposed algorithm has been compared with an existing DWT based watermarking scheme and is found to exhibit better robustness. Digital watermarking is a phenomenon to transform a digital signal by embedding some auxiliary information. So that it is not recognized by the third party. It is analogues to Cryptography.

Aaron T. Sharp[3] et..al.. Digital authentication can provide a medium for ensuring integrity in such platforms. Authentication can be critical for applications such as video surveillance, where a malicious user could potentially intercept and distort important data. For this reason, it is crucial to incorporate a robust method of authentication into video surveillance systems. Video watermarking presents a viable means to ensure data integrity and allows for a robust method of authentication in these systems .Current techniques that could be used to authenticate video systems are not focused on security and can be easily exploited. In one scenario, additional data is appended to a video stream. However, this adds overhead to both the encoder and decoder of the system and can easily be intercepted by an attacker. Another scenario involves watermarking video with a known authentication key. Unfortunately, an attacker with knowledge of the encoder could potentially emulate this watermark and forge authentication.

There are two components of digital watermark:-
I. Watermark embedded
II. Watermark detector

I. Watermark Embedded

In watermark embedded an object U is embedded with another data message P to produce watermarked object X.

II. Watermark Detector

With the help of watermark detector the convert data message P is recognized with the help of key K from the watermarked object.

There are two characteristics that a good watermark should posses:-
I. Robustness
II. Blind detection

I. Robustness

The watermark should survive a variety of imperceptible modification. The watermark should remain intact as long as the perceptual content remains.

II. Blind Detection

It is the ability to detect the watermark in absence of original document. It is an important requirement for video watermarking. Digital watermarking or in simple terms information hiding refers to the methods for embedding data into data to simplicity the data

embedding process , watermarking is done in bit-stream domain. This is necessary to avoid high computation burden while decoding process.

2.1 Desirable Characteristics for Digital Watermarking Of Video Are As Under

I. Invisibility
It should be invisible to no man observer.

II. Security
Unauthorized removed of watermark must be impossible once it has been embedded.

III. Complexity
Watermark retrieval should have no complexity.

IV. Compressed Domain Processing
The distributor will always store the video in compressed format.

V. Constant Bit Rate
The bit rate should not be increased when watermark in bit stream is done.

VI. Interoperability
Uncompressed video should compatibility de-watermarked without having to encode first.

2.2 Gaps

I. The watermark is not robust to attacks which are specifically targeted at videos and even if they do, they fail to resist when image attacks are performed on them.

II. The bit rate of the watermark is low. Some algorithms embed only one bit information as the watermark.

III. One of the most difficult problems in digital video watermarking is watermark recovery in the presence of geometric attacks like frame shift, cropping, scaling, rotation, and change of aspect ratio, especially when some of these are combined together.

2.3 Objectives

I. To secure the data of the creator and restrict piracy.
II. To authenticate the video.
III. To guarantee the ownership of video.
IV. To provide security for video.

3. Research Methodology

3.1 Mathematical Modeling

Let, V=x/x is video……. (1)
We are dividing video into number of scenes.
Let, S be set of scenes
S= S1, S2, S3... Sn…….. (2)
From (1) and (2)
S E V
Let, W be set of watermarks
Therefore, W= w1, w2, w3…wn
S=W
i.e. number of scenes is equal to number of watermarks in video.
For all x, x S,
F C x
Where F is set of frames in scene
F= F11, F12, F13, F14
i.e. one scene frame is divided into four subscenes
Fij= B11, B12…. Bnm
Where B C F C V
Fij be set of new frame i.e. embedded data containing frame
Therefore,
S = (Fij U Fij) (Fij)
V = S1 U S2 U S3 . U Sn
// video created with watermark at the time of Decryption
V ¡= V w
Hence,
V ¡= S1 U S2 U S3 U S4...U Sn w1, w2, w3 ,.., wn
Therefore,
V = (S1 w1) U (S2 w2) U .. U (Sn wn)

3.2 Proposed Methodology

A blind and robust Video Watermarking Scheme with Scrambled Watermark is pro- posed. The basic purpose is on developing a blind, invisible and robust watermark which can defend unintentional attacks. The mark must be re- coverable, not only in the complete work, but also in truncated, filtered, dilated, and otherwise processed clips, in a concatenation of unrelated content, and in the presence of noise. The proposed video watermarking scheme comprises of different modules such as video preprocess, watermark preprocess, watermark embedding, and watermark detection. Proposed watermarking scheme is shown in figure:-

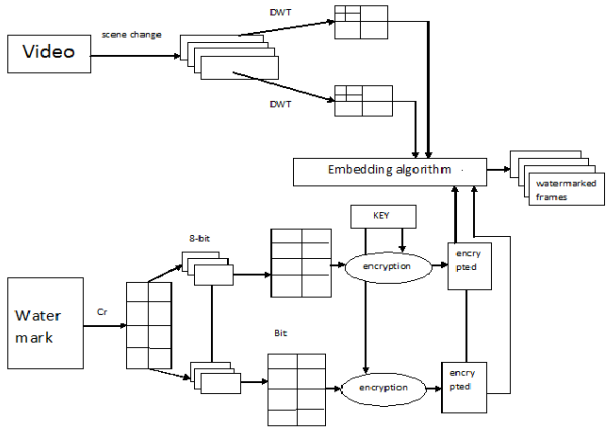

Figure : Proposed System Architecture

3.3 Algorithm

3.3.1 Embedding Process

Step1: Convert video into frames.
Step2: Convert each pixel value into binary data.
Step3: Take the watermark and convert it into bit plane.
Step4: Embed the watermark bits into frames.
Step5: Stop.

3.3.2 Extraction Process

Step1: Take watermarked video.
Step2: Convert each pixel value into binary data.
Step3: Extract embedded bits of watermark from frames using reverse embedding (IDWT) process.
Step4: Stop.

4. Conclusions

The watermarking scheme takes the major advantages in resisting the attacks and partial removal of the watermark. The results also show that the scheme is robust against different image processing attacks like addition of noise, median filtering and cropping. The approach cultivates an innovative idea of embedding different bits of a watermark in the frames of video and its advantages were clearly seen from the experimental results. The security for the confidential videos of company or defence department is very much important. This system can provide more security to the video. We can restrict piracy and unauthorized downloading of video

Acknowledgments

An endeavor is successful only when it is carried out under proper guidance & blessings. We would like to thank people who helped us in carrying out this work by lending invaluable assistance to us in carrying out this work. We are hereby thankful to Prof. Mr. S.R. Sakhare, Head of Department, Information Technology, VIIT, Pune & Prof. Mr. Narendra Pathak, Project Coordinator, Department of Information Technology, VIIT, Pune who encouraged at this venture. We sincerely thank Prof. Mrs. J.V. Bagade, Project Guide, VIIT, Pune for their constructive & encouraging suggestions. We also thank all Teaching and Non-teaching staff of Department of Information Technology, VIIT, Pune for their kind of co-operation during our course. Finally we are extremely thankful to our Family & Friends who helped us in our work & made the project a successful one.

References

[1] Jantana Panyavarapom,"Wavelet based Video Watermarking Scheme",978-1-4577-2166 3/11©2011 IEEE.

[2] Raghavendra K and Chetan K.R,"A Blind and Robust Watermarking Scheme with Scrambled Watermark for Video Authentication" 978-1-4244-4793-0/09©2009 IEEE.

[3] Aaron T. Sharp" Digital Video Authentication with Motion Vector Watermarking", 978-1-4244-7907-8/10/ ©2010 IEEE