International Conference on Recent Innovations in Engineering and Management
Dhananjay Mahadik Group of Institutions (BIMAT) Kolhapur, Maharashtra (ICRIEM-16)
23rd March 2016, www.conferenceworld.in ISBN: 978-81-932074-5-1

WATERMARKING TECHNIQUE FOR SECURITY

Mr.J. K. Ravan[1], Dr.T.C.Thanuja[2]

[1]*Assistant Professor,Dhananjay Mahadik Group Of Institutions, Kolhapur, Maharashtra(India)*

[2]*Professor,Visvesvaraya Technical University, Belagavi, Karnataka (India)*

Abstract:

The term "digital watermark" was first coined in 1992 by Andrew Tirkel and Charles Osborne. A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements.

Keywords: Watermarking, SINR, Discrete Wavelet transform, DFT, FFT, and DCT.

I. INTRODUCTION

Digital watermarking technology started as early as 1282 in Italy, where paper watermarks were used to indicate the paper brand and the mill that produced it. After this invention, the method quickly spread over Italy and then over Europe. Although originally intended for paper brand and mill identification, the technique was later enhanced to include paper format, quality and strength. They were also used to date and authenticate paper.[10]

During 18th century, this technique was first used for installing anti-counterfeiting measures on money and other documents(http://www.ncd.matf.bg.ac.yu/casopis/05/Vuckovic/ Vuckovic.pdf). They are still widely used as security features in currency today. The first watermark, that is the base of today's technology, is the patent filed in 1954 by Emil Hembrooke for identifying musical works.

It was only after 1995, interest in digital watermarking increased and several organizations began including watermarking technology in different standards. The Secure Digital Music Initiative (SDMI, 1999) adopted watermarking as a central component to its music protection system. The Copy Protection Technical Working Group (CPTWG) (Bell, 1999) considered watermarking technology for video content protection on DVDs. The International Organization for Standardization (ISO) showed an interest in watermarking for designing MPEG standards (Cox et al., 2008). VIVA (Depovere et al., 1999) and Talisman (Hartung and Kutter, 1999), both sponsored by European Union, employed the technology for broadcast monitoring.

Digital watermarking is the embedding or hiding of information within a digital file without noticeably altering the file itself. Now digital image watermarking is increasing attention due to the fast developing in the internet traffic. Digital watermarking achieved is popularity due to its significance in content authentication and copyright protection for digital multimedia data. It is inserted invisible in host image so that it can be extracted at later times for the evidence of rightful ownership [1]. Various digital watermarking techniques are purposed

for copyright protection of multimedia data from being misused [2, 3]. Watermarking is the process of embedding data into a multimedia element such as an image, audio or video file for the purpose of authentication. This embedded data can be later extracted or detected the multimedia data for security purposes. A watermark is information about origin, ownership and copy control. This information is embedded in multimedia content with take care of imperceptibility and robustness. According to the embedding domain of the host image, digital image watermarking techniques can be categorized into one of the two domains via spatial and transform. The simplest technique in the spatial domain methods is to insert the watermark image pixels in the least significant bits (LSB) of the host image pixels [4]. In capacity of data hiding is high in these methods but hardly robust. Watermarking in transform domain is more secure and robust to various attacks. In Frequency domain, watermark is not added to the image intensities or pixels, but to the values of its transform coefficients. Then to get the watermarked image, one should perform the transform inversely. It includes DCT (Digital Cosine Transform), DFT (Digital Fourier Transform), and DWT (Digital Wavelet Transform).

II. DIGITAL WATERMARKING SCHEMES

Watermarking schemes can be classified as follows:

1) Spatial Domain: The watermarking system directly alters the main data elements (like pixels in an image) to hide the watermark data.

2) Transformed Domain: The watermarking system alters the frequency transforms of data elements to hide the watermark data. This has proved to be more robust than the spatial domain watermarking.

III. LITERATURE SURVEY

The term “digital watermarking” came into existence only after 1988 and was coined by Komatsu and Tominaga (1988). Since then, there has been a huge interest in the field of digital watermarking and several different techniques have been proposed. Even though watermarks can be included with any digital content, this research focuses on image watermarking and the following sections review only those implementations that are related to this field.[6]

Shaikh Shoaib, Mahajan R. C. [5] propose implementation of 3-Level DWT algorithms and to have more secure data a secret key is used. The secret key is given to watermark image during embedding process and while extracting the watermark image the same secret key is used. To check effectiveness of the watermark video MSE and PSNR parameters are used. In a typical authentication watermark technique an authentication signature (AS) is computed from the whole image data and inserted into the image itself. in cryptography, AS is called message authentication code (using secret-key) or digital signature (using public/private-key). Secret key contains information about the image that may be checked to verify its integrity. However, inserting the AS into the image alters the image itself, hence modifying its AS and invalidating the watermark AWT for binary images that has good visual quality when applied to a generic binary image. It is used in conjunction with secret-key or public/private key.

Kazuto Ogawa and Go Ohtake [2] propose a watermarking method for HEVC/H.265 video streams that embeds information while encoding the video. HEVC/H.265 uses a kind of arithmetic coding (CABAC) and it is not easy to substitute a code with another one in a stream. Researchers proposed a watermarking method that

embeds information into HEVC streams. In our method, each receiver selects some packets according to their identifiers, and therefore, it is necessary to force the receiver to select correct packets by using encryption schemes. According to [8] it is possible to embed information into a compressed stream using this method without degrading the content and with an appropriate robustness that meets the requirements of the users.

Somayyeh Mohammadi [3] proposes a novel video watermarking algorithm based on wavelet transform and chaotic maps. Researcher apply the two dimensional wavelet transform on I-frames and then insert the chaotic watermark into part of the sub-band coefficients. Since chaotic maps are sensitive to initial values, initial values of the chaotic maps and their chaotic parameters are exploited as secret keys in our algorithm. Our watermarking system operates on video compressed using the MPEG-2 compression standard. The watermark is embedded in the selected wavelet coefficients of the luminance Y of I-frames of the video stream. For watermark embedding procedure, I-frames are preferred because of two chief reasons. Firstly, their existence in a video sequence is necessary. Secondly, the two frames P and B are extremely compressed by motion compensation.

Vladimír bánoci, Martin Broda, Gabriel Bugár, Dušan Levický [4] propose two dimensional spread spectrum watermarking framework based on Direct Spread Spectrum theory using PN sequences. The presenting schema allows acquiring a high level of robustness with desired imperceptibility. The aim of this paper was to present robust and adaptive watermarking system for multimedia protection, where hidden watermark provides a desired requisition against copyright infringement. Media content delivery system incorporated by cryptographic public-key was proposed in the paper as part of. The framework concept was applied to digital video content to simulate 2D-level spreading technique of hidden watermark data. Several watermarks can be superimposed using this technique if different pseudo-noise sequences are used for modulation. This requires application of PN sequences with very low cross-correlation properties, where different pseudo-noise sequences are in general orthogonal and they can be retrieved in arbitrary order and independently from each other. Thus, the pseudo-noise signal is the secret key for embedding and retrieval of watermark, and for security reason, PN sequences should be used that are not easy to guess.

Tianrui Zong, Yong Xiang, and Iynkaran Natgunanathan [5] propose a histogram-based image watermarking method to tackle with both cropping attack and RBAs. In this method first the gray levels are divided into groups. Secondly the groups for watermark embedding are selected according to the number of pixels in them, which makes this method fully based on the histogram shape of the original image and adaptive to different images. Then the watermark bits are embedded by modifying the histogram of the selected groups. Since histogram shape is insensitive to cropping and independent from pixel positions, the proposed method is robust to cropping attack and RBAs. Besides, it also has high robustness against other common attacks. The histogram of an image is naturally insensitive to cropping and independent from pixel positions, so it is ideal to be exploited in image watermarking to tackle with cropping attack and RBAs. Compared to the traditional histogram-based method, the superior performance of proposed method is demonstrated by simulation examples by authors in the research article.

Ming Li, Ngwe Thawdar, Dimitris A. Pados, Stella N. Batalama, Michael J. Medley [6], investigate the problem of embedding data in raw video sequences with minimum video mean-square distortion for any required data recovery error rate. In particular, for any given video frame sequence and any (block) transform domain of

interest, we find the optimal carrier and scalar parameterized linear operator on the video data that maximize the output signal-to-interference-plus-noise ratio (SINR) of the maximum-SINR data receiver filter or, equivalently, minimize the average embedding distortion for any target message extraction error rate. The procedure is extended from single-carrier to multi-carrier (multiple messages) embedding. As a practical consideration, a sub-optimal computationally efficient embedding algorithm is also proposed. Extensive experimental results demonstrate that sub-optimal embedding as described has video distortion versus data extraction error rate performance comparable to optimal embedding. Our studies also demonstrate the robustness of the optimal (and sub-optimal) embedding schemes to H.264 compliant encoding. This paper considered the problem of single-carrier and multi-carrier (multiple sessions) data embedding in linearly modified (transform) domains of raw video sequences with minimum video mean-square distortion for any required data recovery error rate. Sub-optimal, single-frame-only designed embedding was also considered.

The issues with all described approaches arises when we consider the resistance against decryption attacks of the algorithms. The spatial additive watermarks can directly be detected and subtracted to find unsecure original image. The approach of transform algorithms such as 2 dimensional DFT, FFT, DWT, and DCT also has limitations as they are non-robust against component analysis approaches such as advanced modified PCA or ICA. The static temporal watermarks are also susceptive against forced iterative detection algorithms.

The text or symbolic watermarks can also be broken as they have a limited combinations. For example a numeric key generated of length 8 characters will have 10^8 (10,00,00,000) combinations, for which a forced key-detection algorithm can be written with intelligent and advanced programming skills.

IV. PROPOSED METHOD

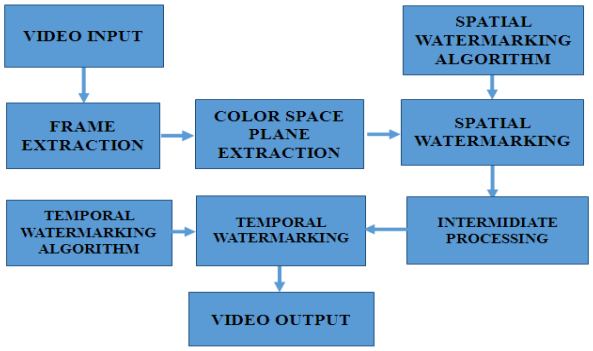

Figure. A general block diagram of proposed methodology

VI. PROPOSED METHODOLOGY

The proposed methodology will consider implementation of both spatial and temporal watermarking algorithm.

1. The spatial watermarking algorithm will introduce a static opaque or completely invisible spatial watermark in each color frame. In Spacial domain the watermark is inserted into the intensity values. It embed the watermark by modify the pixel value of the host image. Low computational complexity and simplicity are the main strengths of the special domain methods.

2. The temporal watermarking algorithm will introduce a temporally dynamic watermark which will be slightly different for each frame.

The multiple watermarking algorithms varying spatially as well as temporally will ensure a great robustness against variability and decryption attacks.

VII. CONCLUSION

Our approach is to generate an ideal digital watermark having improved properties which help to implement it for security and copyright protection. By using a hybrid spatial and temporal watermarking we can implement an advanced frequency domain technique, which is mostly invisible to naked eyes.

REFERENCES

[1] Shaikh Shoaib, Prof. R. C. Mahajan "Authenticating Using Secret Key in Digital Video Watermarking Using 3-Level DWT" 2015 International Conference on Communication, Information & Computing Technology (ICCICT), Jan. 16-17, Mumbai, India

[2] Kazuto Ogawa and Go Ohtake "Watermarking for HEVC/H.265 Stream" 2015 IEEE International Conference on Consumer Electronics (ICCE).

[3] Somayyeh Mohammadi "A Novel Video Watermarking Algorithm based on Chaotic Maps in the Transform Domain", 2015 international symposium on AISP.

[4] Vladimír bánoci, Martin Broda, Gabriel Bugár, Dušan Levický "2D - Spread Spectrum Watermark Framework for Multimedia Copyright Protection" 2014 IEEE

[5] Tianrui Zong, Yong Xiang, and Iynkaran Natgunanathan "Histogram Shape-Based Robust Image Watermarking Method" IEEE ICC 2014, Communication and Information Systems Security Symposium

[6] Ming Li, Ngwe Thawdar, Dimitris A. Pados, Stella N. Batalama, Michael J. Medley "Minimum-Distortion Data Embedding in Video Streams" IEEE ICC 2014 SP for CS.

[7] D.MATHIVADHANI ,"Multiple Watermarking Approaches Using Enhanced Image Processing Techniques And Visual Cryptography" , A phd thesis submitted in 2012 at Avinashilingam Institute for Home science and Higher Education for Women, Coimbatore, 2012.

[8] Jianchao Yang, ,John Wright, Thomas Huang ,Yi Ma, "Image Super-Resolution via Sparse Representation", IEEE, 2004

[9] Matt L. Miller, "WATERMARKING WITH DIRTY-PAPER CODES" , 2001 IEEE.

[10] Chun-Shien Lu, Hong-Yuan Mark Liao, "Multipurpose Watermarking for Image Authentication and Protection", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 10, NO. 10, OCTOBER 2001

[11] Frank hartung and Bernd Girod "Watermarking of Uncompressed and compressed video" vol no 3 may 1998

[12] Tae-Yun Chung, Min-Suk Hong, Young-Nam Oh, Dong-Ho Shin and Sang-Hui Park, "DIGITAL WATERMARKING FOR COPYRIGHT PROTECTION OF MPEGP COMPRESSED VIDEO" , IEEE, June 17, 1998