IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Review on Video Watermarking Techniques

Miss. Shital Divekar[1], Prof. Nitin Dawande[2], Prof. Suresh Rode[3]

Student of Electronics and Telecommunication, D. Y. Patil School of Engg, Ambi, Pune, India[1]

Associate Professor & PG Co-ordinator, D. Y. Patil College of Engg, Ambi, Pune, India[2]

Assistant Professor Electronics and Telecommunication, D. Y. Patil School of Engg, Ambi, Pune, India[3]

Abstract: Due to increasing popularity of the internet use of digital multimedia is increased more rapidly. Many websites allows the user to upload and share multimedia objects such as audio, images, and videos. Without adding security information it is impossible to automatically verify the authenticity of the uploaded multimedia objects so the digital watermarking is used to protect the information against the illegal changes in the form of images, videos and audios. A digital watermark is the process of embedding watermark in a noise-tolerant signal such as an audio, video or image data used to identify ownership of the copyright of such signal. The robustness, fidelity, capacity are essential requirements of watermarking techniques so that they can handle several types of image artefacts. This paper gives survey of different watermarking techniques for protecting digital contents.

Index Terms: DCT, Watermark, hash value, QIM, Tamper Detection, DWT, RSA, PSNR.

I. INTRODUCTION

Now a day's digital multimedia are transmitted more easily and rapidly due to increased popularity of internet, together with the availability of inexpensive and reliable storage devices and editing software's which leads to forgeries and unauthorized sharing of multi-media such as audio, image and video. Among these digital media, video is becoming more important in different applications such as, video broadcast, DVDs, video surveillance, video on-demand, video conferencing , where two factors of video data are very important that is authenticity and integrity. However, due to currently available low-cost video editing software's, it became easy to eavesdroppers, who modify the video content intentionally to harm the interests of either the owner or the consumer. Tamper with videos, makes them unreliable and defeating the purpose of such applications at its first place. Without authentication a video viewer or a consumer cannot verify that the video being viewed is the original one that was transmitted by a producer. And if the video is tampered, then there is a need to detect tampering in video, as well as to locate the area where the tampering is done.

There are various techniques available for the authentication and of the digital multi-media such as encryption and digital watermarking. Encryption can be used to prevent the unauthorized access to the digital media. However Encryption has limitations in protecting the intellectual property rights, once the digital content gets decrypted, so there is nothing to prevent the unauthorized user from altering it. Another technology is obviously needed to prove the ownership rights. This need attracted attention from the researcher community and industry leading to creation of information hiding technique, called Digital Watermarking. The basic idea behind the watermarking is to create the metadata containing information about the digital content to be protected, the metadata can be a string of characters or any binary image as illustrated in Figure 1. The metadata is then converted into the digital sequence of 1's and 0's, called watermark. This watermark is then embedded into the digital media such as audio, video, audio and image. The watermark should be robust against common signal processing operations as well as the malicious attacks.

For the authentication of the digital media such as audio, image and video there is need to add the information in the digital media. For example, the copyright information need to associate with images to identify the legal owner of the image, the frame indexing is needed to embed into video. The copyright information can be placed in the header of the image but the information gets lost on format conversion.

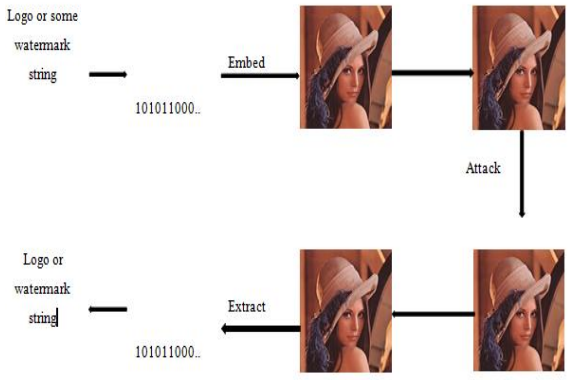

Fig. 1. General digital watermarking concept

II. TYPES OF DIGITAL WATERMARKING TECHNIQUES

The watermarking techniques can be classified into different types based on the type of the document being watermarked, human perception, properties of the watermark, and watermark embedding domain. Based on

DOI 10.17148/IJARCCE.2016.5509

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

the human perception watermarking technique can be classified in three types as shown in Figure 2.

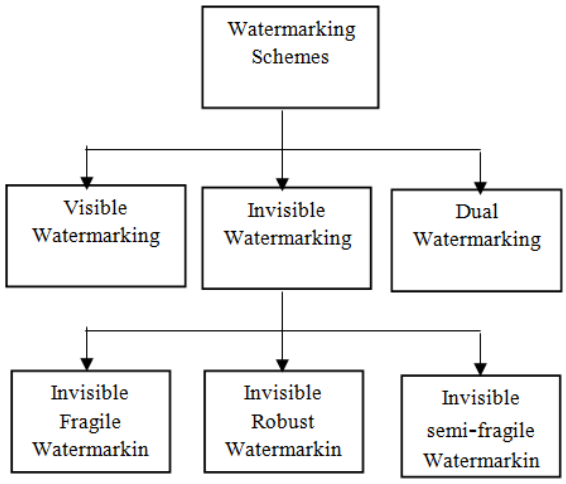

Fig. 1. Types of watermarking scheme based on human perception

The watermarking Techniques can be classified based on watermark embedding domain as shown in the Figure 3.

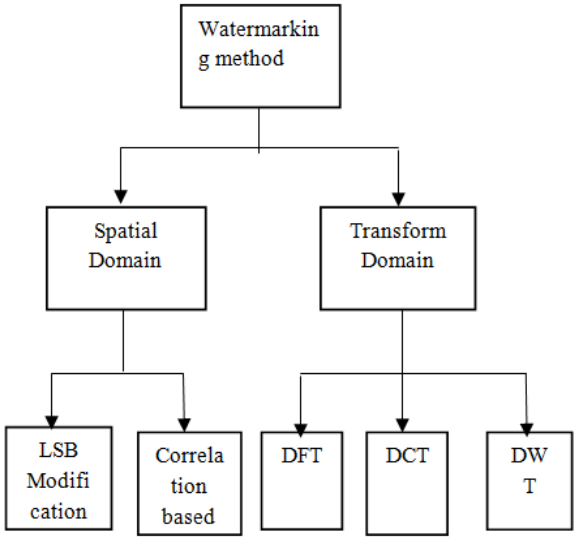

Fig. 3. Types of watermarking scheme based on watermark embedding domain

III. PROPERTIES OF WATERMARK

1) Imperceptibility

The imperceptibility refers to perceptual transparency i.e. the watermarked media must be perceptually equivalent to media before watermarking. To reduce the perceptual difference between original and watermarked media the watermark is embedded into the perceptually insignificant portion of the host signal which is highest frequency coefficients of transform domain.

2) Capacity

Capacity is nothing but the amount of information or watermark bits embedded into the host signal. The capacity can be increased at the expense of the robustness and imperceptibility.

3) Robustness

Robustness refers to the strength of watermark to survive against common signal processing, geometric transformation and malicious attacks. To increase the robustness of the watermark against compression the watermark should be embedded into the visually significant portion of the image as compression discards visually insignificant information. But embedded into visually significant portion of the image produce visual distortion. Not all the applications of watermarking require the robust watermark for example where fragility is required. Depending on the applications, there is trade of in properties.

IV. RELATED WORK

Mehdi Fallahpour, Shervin Shirmohammadi, Mehdi Semsarzadeh, and Jiying Zhao proposed approach in paper,"Tampering Detection in Compressed Digital Video Using Watermarking", [1] that is based on the semi-fragile video watermarking technique to detect the tampering in compressed videos. The fragile watermarking method cannot distinguish the tampering from common video processing operation such as compression, sharpening, brightness increasing. To distinguish the tampering from common video processing applications semi-fragile video watermarking scheme is designed. The watermark is generated by the macroblock's and frame's indices, and watermark is embedded in highest zero quantized DCT level within each block. They have implemented and evaluated the method using the H.264/AVC codec also in order to increase the security of system algorithm also takes advantage of content-based cryptography. The method stated in this paper is used to detect the tampering in videos in spatial and temporal domain. The method is designed in such a way that it is easy to configure the system to adjust transparency, capacity, and robustness according to specific application in hand. This method leads to smaller video distortion i.e. degradation of PSNR is 0.88dB and decrease in structural similarity index by 0.0099 with 0.05% bit rate increase.

Bhaskaran et al. proposed approach in patent , " Fragile Watermark for Detecting Tampering in images",[2] that is related to the fragile watermarks for tamper detection in images. The watermarking scheme for images which includes techniques for insertion and extraction of fragile watermark in DCT domain and to determine whether the image so watermarked has been tampered with or not. In watermark insertion process the bits of the digital signature of the hash function of image are embedded into the frequency coefficients of the image.

The tamper detection is done by extracting the watermark which is embedded during watermark insertion process from the image, hash value computed as in insertion process and verified by using public key whether the extracted watermark is valid signature of the hash value.

Copyright to IJARCCE
DOI 10.17148/IJARCCE.2016.5509

H.-Y. Huang, C.-H. Yang, and W.-H. Hsu, proposed approach in paper, "A video watermarking technique based on pseudo-3-D DCT and quantization index modulation," [3] that is an effective watermarking scheme using pseudo-3-D DCT and quantization index modulation (QIM). The watermark insertion process is done by adjusting the correlation between the selected blocks in uncompressed domain. The watermark is extracted by blind process. The embedding factor is calculated by using the pseudo 3-D DCT. With the help of QIM the watermark is embedded into compressed domain into the quantization regions of successive frames and secrete embedding key is generated which is further useful in extraction of the watermark. The proposed method have good transparency and robustness also the method survive against filtering, luminance change, compression and noise attacks but the proposed method is not robust against geometric transformation such as rotation, scaling, and cropping.

De Oliveira, P. R. , Andreia Fondazzi Martimiano, L. ; Delisandra Feltrim, V. ,Brasilino Marcal Zanoni, G., proposed approach in paper " Energy Consumption Analysis of the Cryptographic Key Generation Process of RSA and ECC Algorithms in Embedded Systems", [4] states the characteristic of safety related authentication, the author in this paper presents the energy consumption analysis between the key generators for the RSA and ECC algorithms. To improve the security of communication cryptographic keys can be used between entities that are communicating for authentication process. To check the correlation between energy consumption and runtime test is conducted. They have implemented algorithm in C language and the executions were carried out in the Beagle Board platform. The ECC algorithm presented has a lower energy consumption than the RSA algorithm.

Maneli Noorkami, and Russell M. Mersereau, proposed approach in paper "Digital Video Watermarking in P-Frames With Controlled Video Bit-Rate Increase." [5] states a common approach for embedding the watermark in I-frames. They have shown that the video bit rate increase can be held to reasonable value by limiting the watermark to nonzero-quantized ac residuals in P-frames. Since the nonzero-quantized ac residuals in P-frames correspond to non-flat areas that are in motion, temporal and texture masking are exploited at the same time. They proposed watermark embedding in nonzero quantized ac residuals with spatial masking capacity in I-frames. Since locations of nonzero-quantized ac residuals is lost after decoding.

Jordi Serra-Ruiz and David Megias, proposed approach in paper " DWT and TSVQ-based semi-fragile watermarking scheme for tampering detection in remote sensing images," [6] presents the semi-fragile image watermarking scheme used in remote sensing images. The signature of hyper spectral or multispectral image is used to embed the watermark in suggested scheme. The scheme suggested in this paper detects a forgery of the watermarked image, e.g. a tampered region. The original image which is to be watermarked is segmented in 3-D blocks and, for each block, DWT and a tree structured vector quantizer is built. By using iterative algorithm these trees manipulated the selected condition gets satisfied by resulting image. The tampering attacks can be avoided by partially modifying each tree according to secret key. The internal structure of the tree is determined by using this secret key. The trees are built using only the LL sub-band of the DWT to make watermarked image robust against near lossless compression. The results show that the method is robust against JPEG2000 compression and works correctly with remote sensing images also detects copy and replace attacks within same image segments.

J. Zhang, A. T. S. Ho, G. Qiu, and P. Marziliano, proposed approach in paper, " Robust video watermarking of H.264/AVC," [7] that is based on a framework for detecting tampered information in digital videos. Using the proposed technique it is possible to detect several types of tampering with a pixel granularity. The framework uses a combination of temporal and spatial watermarks that do not decrease the perceived quality of the host videos. We use a modified version of Quantization Index Modulation (QIM) algorithm to store the watermarks. Since QIM is a fragile watermarking scheme, it is possible to detect local, global, and temporal tampers and also estimate the attack type. The framework is fast, robust, and accurate.

Y. Wang and A. Pearmain, proposed approach in paper, " Blind MPEG-2 video watermarking in DCT domain robust against scaling," [8] that is blind watermarking technique which does not need original information in watermark detection process, as explained in are more desirable in watermark extraction. The DCT domain blind MPEG-2 watermarking technique is presented, which is generally robust against geometric transformation such as arbitrary ratio scaling. The turbo codes are used for error correction. The method is used for block-DCT-based video compression techniques. Simplicity and blindness are the main advantage of proposed scheme.

V. ACKNOWLEDGMENT

I express my gratitude towards **Prof. N. A. Dawande project guide, Prof. Rode S. co-guide and Prof. V. V. Thorat,** P.G. coordinator and **Prof. S. G. Bari**, Head of Department of Entc Engineering , DR.D.Y. Patil School of Engineering Academy, Ambi, who guided and encouraged me in completing this paper. I would like to thanks our Principal **Dr. V. N. Nitnaware** for allowing us to publish paper.

VI. CONCLUSION

In this review paper we have focused on the different watermarking techniques and their concept. It shows that the transform domain techniques are more efficient over the spatial domain because LSB substitution does not provide robustness so it is not very efficient approach for digital video watermarking. DCT domain watermarking contains considerable amounts of random noise. The

wavelet domain watermarking is well proved to be highly resistant to both compression and noise, with less amounts of visual degradation. This will make the original images over the internet more secure. Along with these, an introduction to digital watermarking and different aspects of watermarking has been presented.

REFERENCES

[1]. Mehdi Fallahpour, Shervin Shirmohammadi, Mehdi Semsarzadeh, and Jiying Zhao, "Tampering Detection in Compressed Digital Video Using Watermarking," IEEE Transactions on Insrumentation and Measurement, vol. 63, no. 5, May 2014.

[2]. Bhaskaran et al.," Fragile Watermark for Detecting Tampering in images", U. S. Patent Number 6064764, may 16,2000.

[3]. H.-Y. Huang, C.-H. Yang, and W.-H. Hsu, "A video watermarking technique based on pseudo-3-D DCT and quantization index modulation," IEEE Trans Inf. Forensics Security, vol. 5, no. 4, pp. 625–637, Dec. 2010.

[4]. De Oliveira, P. R. ,Andreia Fondazzi Martimiano, L. ; Delisandra Feltrim, V. ; Brasilino Marcal Zanoni, G.," Energy Consumption Analysis of the Cryptographic Key Generation Process of RSA and ECC Algorithms in Embedded Systems", Latin America Transactions, IEEE (Revista IEEE America Latina) Volume:12 , Issue: 6 , Pages: 1141-1148, sept 2014.

[5]. Maneli Noorkami, and Russell M. Mersereau," Digital Video Watermarking in P-Frames With Controlled Video Bit-Rate Increase", IEEE Transactions on Information Forensics and Security, VOL. 3, NO. 3, SEPTEMBER 2008.

[6]. Jordi Serra-Ruiz and David Megias, "DWT and TSVQ-based semi-fragile watermarking scheme for tampering detection in remote sensing images," 2010 Fourth Pacific-Rim Symposium on Image and Video Technology.

[7]. J. Zhang, A. T. S. Ho, G. Qiu, and P. Marziliano, "Roubust video watermarking of H.264/AVC," IEEE Trans. Circuits Syst., vol. 54, no. 2, pp. 205–209, Feb. 2007.

[8]. Y. Wang and A. Pearmain," Blind MPEG-2 video watermarking in DCT domainrobust against scaling," IEE Proc.-Vis. Image Signal Process., Vol. 153, No. 5, October 2006.

[9]. Putri Ratna, A.A., Dewi Purnamasari, P., Shaugi, A., Salman, M.," Analysis and comparison of MD5 and SHA-1 algorithm implementation in Simple-O authentication based security system", QiR (Quality in Research), 2013 conference, pages 99-104, June 2013.

[10]. Riaz,S., Javed,M.Y., Anjum,M.A.,"Invisible watermarking schemes in spatial andfrequency domains" Emerging Technologies, 2008. ICET 2008. 4th International Conference, Pages: 211 – 216, Year: 2008.

[11]. Q. B. Sun, D. J. He, Z. S. Zhang, and Q. Tian, "A secure and robust approach to scalable video authentication," in Proc. Int. Conf. Multimedia Expo, vol. 2. Jul. 2003, pp. 209–212.

[12]. B. G. Mobasseri and M. J. Sieffert, "Content authentication and tamper detection in digital video," in Proc. IEEE Int. Conf. Image Process.Vancouver, BC, Canada, 2000, pp. 458–461.

BIOGRAPHIES

Miss. Shital Divekar, Student of Electronics and Telecommunication, D. Y. Patil School of Engg, Ambi, Pune, India, also Working as Assistant professor at HSBPVT'SCOE, Kashti

Prof. Nitin Dawande Assistant Professor and P.G. Co-Ordinator VLSI And Embedded System, D. Y. Patil College of Engg, Ambi, Pune, India

Prof.Suresh Rode Assistant Professor Electronics and Telecommunication, D. Y. Patil School of Engg, Ambi, Pune, India

DOI 10.17148/IJARCCE.2016.5509