ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

A Survey on Efficient Video Watermarking and Image Data Encryption Technique

Priya D. Sonawane[1], Sujata S. Mane[2], Reshma N. Nazirkar[3], Priya P. Barhalikar[4],

Prof. Aruna Verma[5]

B.E. Students, Dept.of Computer Engineering, Dhole Patil College of Engineering, Wagholi, Pune, Maharashtra, India[1,2,3,4]

Asst. Professor, Dept.of Computer Engineering, Dhole Patil College of Engg, Wagholi, Pune, Maharashtra, India[5]

ABSTRACT: Watermark is a digital signal or pattern inserted into a digital document such as text, graphics or multimedia, and carries information unique to thecopyright owner. Data hiding should be used concealed transmissions, closed captioning, indexing, or watermarking. It is in contrast to cryptography, where the survival of the message itself is not masked, but the content is hidden. Video Watermarking is implemented in different fields such as military and Industrial applications. The 2D Barcode with a digital watermark is a widely interesting research in the security field. In this project propose a video watermarking with text data (verification message) by using the Quick Response (QR) Code technique. The QR Code is prepared to be watermarked via a robust video watermarking scheme based on the lossless video watermarking using DCT techniques messages can be sent and received securely. Traditionally, video watermark was based on hiding secret information in image files .Lately, there has been growing interest in implementing video watermarking techniques to video files. The advantage of using video files in hiding information is to be added security against hacker attacks due to the relative complexity of video compared to image files. Video-based watermark techniques are mainly classified into spatial domain and frequency domain based methods. The main aim of video watermark is to hide information in the other wrap media so that other persons will not observe the existence of the information. This is a major distinction between this method and the other methods of secret exchange of information because, for example, in cryptography, the individuals perceive the information by considering the implied information but they will not be able to realize the information. In the reverse process check the logo and QR code for authorized ownership.

KEYWORDS: Image processing, dwt, dct, fft, svd, psnr, ncc, ber.

I. INTRODUCTION

Internet has become indispensible and thus the security and the privacy issue have come to the fore of the computing fraternity. These issues need to be addressed with utmost urgency and highest level of dedication. Watermarking addresses the privacy and security issues. Watermarking has helped not just in security but also in resolving numerous copyright and privacy issues, which became one of the most contentious issues while the expansion of internet. This proposal explores the state of art introduces a novel technique to tackle the elephant in the room. Watermarking techniques can be segregated on the basis of domain based, document based, Perception based and application based. Domain of watermarking technique is divided in to two parts such as on the basis of spatial domain and other is on the basis of frequency domain. In spatial domain watermarking, watermark is embedded by modifying the pixels value of the host image/ video directly. The main advantages of pixel based methods are that they are conceptually simple and have very low computational complexities and therefore are widely used in video watermarking where real-time performance is a primary concern. However, they also exhibit some major limitations. The need for absolute spatial synchronization leads to high susceptibility to de-synchronization attacks; lack of consideration of the temporal axis results in vulnerability to video processing and multiple frame collusion; and watermark optimization is difficult using only spatial analysis techniques. In frequency domain, the watermark is embedded for the robustness of the watermarking mechanism. There are three main methods of data transmission in frequency domain. As DCT DFT

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

andDWT. The main strength offered by transforming domain techniques is that they can take advantage of special properties of alternate domains to address the limitations of pixel-based methods or to support additional features. Generally, transform domain methods require higher computational time. In transform domain technique, the watermark is embedded distributive in overall domain of an original data. Host video is first converted into frequency domain by transformation techniques. The transformed domain coefficients are then altered to store the watermark information. The inverse transform is finally applied in order to obtain the watermarked video. On the basis of document watermarking can be apply on Image, Text, Audio and Video. According to the human perception watermarking is divided in to two parts visible watermark media and invisible watermark media. Invisible watermark is further are of two types robust watermarking and fragile watermarking. For effective watermarking the watermarking techniques need to be imperceptible (watermark should not degrade the quality of multimedia), robust (after applying attacks quality of multimedia should not be degrade), and secure from various attacks.
In Most of the watermarking techniques, the watermark is embedded into the frequency domain instead of the spatial domain for the robustness of the watermarking mechanism. Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT) and Discrete Wavelet Transformation (DWT) are the three main methods of data transformation in this domain. The main strength offered by transforming domain techniques is that they can take advantage of special properties of alternate domains to address the limitations of pixel-based methods or to support additional features.

II. RELATED WORK

Author present a theoretical framework [1] for the linear collusion analysis of watermarked digital video sequences, and derive a new theorem equating a definitionof statistical invisibility, collusion-resistance, and two practical watermarkdesign rules. The proposed framework is simple and intuitive; the basicprocessing unit is the video frame and we consider second-order statisticaldescriptions of their temporal inter-relationships. Within this analytical setup,we define the linear frame collusion attack, the analytic notion of a statisticallyinvisible video watermark, and show that the latter is an effective counterattackagainst the former.
Author develops a novel video watermarking framework [2] based on the collusion resistantdesign rules formulated in a companion paper. Author propose to employa spatially-localized image dependent approach to create a watermark whosepair wise frame correlations approximate those of the host video. To characterizethe spread of its spatially-localized energy distribution, the notion of awatermark footprint is introduced. Then Author explain how a particular type ofimage dependent footprint structure, comprised of subframes centered arounda set of visually significant anchor points, can lead to two advantageous results:pairwise watermark frame correlations that more closely match those of the host video for statistical invisibility, and the ability to apply image watermarksdirectly to a frame sequence without sacrificing collusion-resistance.
Author present effective steganalysis techniques for digital video sequences basedon interframe collusion [3] that exploits the temporal statistical visibility of a hiddenmessage. Steganalysis is the process of detecting, with high probability,the presence of covert data in multimedia. Present image steganalysis algorithmswhen applied directly to video sequences on a frame-by-frame basis are suboptimal; Author present methods that overcome this limitation by usingredundant information present in the temporal domain to detect covert messagesembedded via spread-spectrum steganography.
Digital image watermarking plays an important role in Multimedia securityfield [4]. Methods developed under this are used to protect Intellectual propertyrights of digital data such as video, image, audio, etc. without affecting thefidelity of the original data. In this paper a Wavelet based digital image watermarkingis applied on input '.bmp' image to generate watermark embeddedimage by inserting a logo '.bmp' image with non-zero scaling factor [5]. A compactlysupported Daubechies Orthonormal Wavelet Transform (dB) methodand wavelet packet transform method are used. Extracted logo image and receivedimage after both watermarking process are analysed in terms of signalto error ratio.
It started with concealing messages within the lowest bits of noisyimages [7] or sound files. We shall perform steganography on video files and hidethe message in an encrypted format, thus achieving a multiple cryptographicsystem. The most commonly used technique is Least Significant Bit steganography(LSB steganography). But instead of traditional LSB encoding, Author willuse a modified encoding technique which will first transform the video usinga Lazy Lifting Wavelet transform and then apply LSB in the sub-bands of thevideo that has been obtained. The proposed approach to video steganographyutilizes the visual as well as the audio component. The lazy wavelet

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

transformis applied to the visual frames, and the data is stored in the coefficients of thevisual component. The length up to which it is stored is hidden using LSBin the audio component.

III. PROPOSED ALGORITHM

A .ALGORITHM FOR EMBEDDING PROCESS

Step 1: Read the video file and extract RGB P-frame, B-frame, and I-frame.
Step 2: Read the I-frame image as a cover image.
Step 3: Generate a QR code image with company name.
Step 4: Apply SVD to I frame and get three singular coefficients as u, v
Step 5: Add secrete message with components of an SVD image to get an SVD coverimage
Step 6: Apply DWT on both SVD cover image and QR code image to getcombined image
Step 7: Take the inverse DWT on the combined image to get Watermarked Iframe
Step 8: Finally watermarked I frame image to get the watermarked video files.

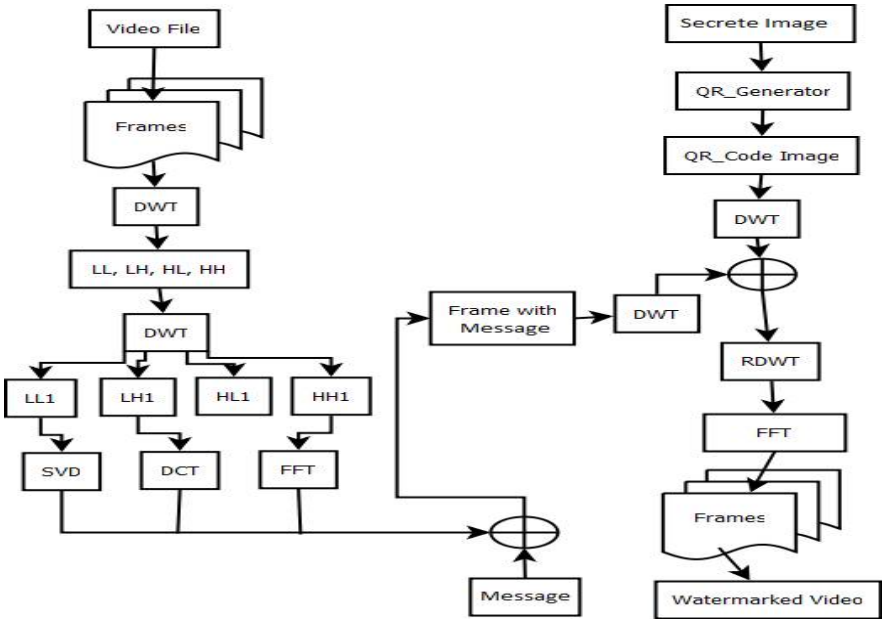

Fig 1:Embedding Process

B. ALGORITHM FOR DECODING PROCESS

Step 1: Read the watermarked video files and extract Watermarked I frame.
Step 2: Read the original video file and extract original Video I frame.
Step 3: Apply DWT on both videos I frame.
Step 4: Subtract watermarked video I frame coefficient with original video Iframe coefficient and take Inverse DWT to get a QR code image.
Step 5: By using QR code reader extract company name From QR code image.
Step 6: Apply SVD on watermarked I frame to recover the logo by using thesingular value component.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

C. MATHEMATICAL MODULE FOR VIDEO WATERMARKING

Set S= I, O, Fn, En, S, F
Where I is the input provided to the project
O is the output of the project and Fn is the function get performedduring project.
S and F is depends on the success or failure of the project.
I=V,L, T3
Where V is the video in .mpge format is the image and message which isget embedded to the video, and T is the test data which is the secretemessage embedded with video.
O=EV Where Ev is the embedded video which contains imageand textual data hided in the video frame.
Fn=Frame splitting using dwt, dct, fft, and svd
En= Video Encrypted
S=successfully embedded logo and text to the video frame
F=Failure message with reason of failureMathematical Module for Image Encryption and compression

D. MATHEMATICAL MODULE FOR IMAGE ENCRYPTION AND COMPRESSION

Set (P) = p0, p1, p2, p3, p4, p5, p6, p7
p0=Select data for send.
p1=Select Image for send.
p2=Apply Steganography encryption.
p3=Apply Encryption algorithm.
p4=Send encrypted image.
p5=receive image.
p6=apply decompression.
p7=apply steganography decryption.

IV. PROPOSED SYSTEM

Provide his input video file, text data and security key for hiding data into Video. The process of system is to collect necessary input from user and Encode the data into Video and Generate Watermark Video Similar to Input Video. When user wants to decode it then user needs to provide watermark video file and security key which is already used for encoding process. System validate watermark video and security key of user and decode the message from the video which is called as extracted data from the video. It is more secure.

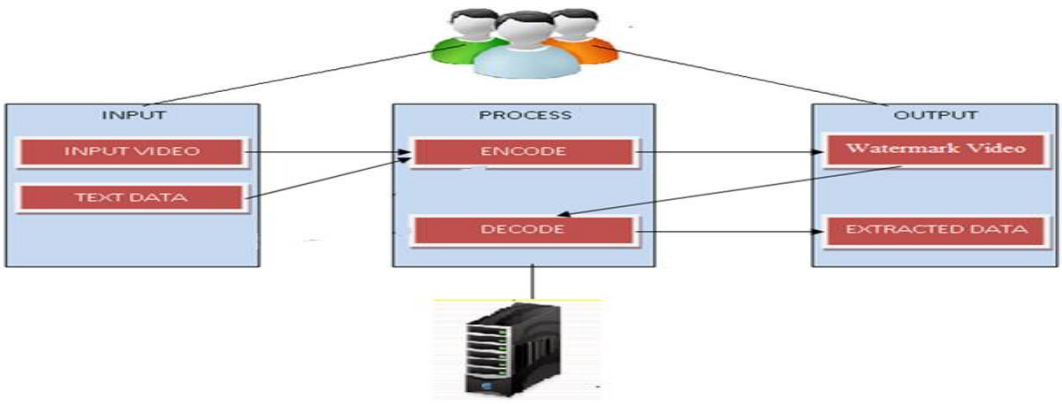

Fig 3: System architecture

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

In the Above architecture diagram describes user provide his input video file, text data and security key for hiding data into Video. The process of system isto collect necessary input from user and encode the data into Video and GenerateWatermark Video Similar to Input Video. When user wants to decode it then userneeds to provide watermark video file and security key which is already used forencoding process. System validate watermark video and security key of user anddecode the message from the video which is called as extracted data from the video.It is more secure.

V. CONCLUSION

This method has achieved the improved imperceptibility and security watermarking.In this QR code encoding process and get excellent performances. In the first methodwatermark was embedded in the diagonal element. On the other hand embeddingtext messages in the QR code image. So, the dual process given two authenticationdetails. The logo is located very safely in the QR code image. This method isconvenient, feasible and practically used for providing copyright protection. Experimentalresults show that our method can achieve acceptable certain robustness tovideo processing.

REFERENCES

[1] SuppatRungraungsilp, MahasakKetcham, TaneeWiputtikul, KanchanaPhonphak,and SartidVongpradhip,"Data Hiding Method for QR Code Based onWatermark by comparing DFT with DWT Domain" ICCCT', May 26-27,2012.
[2] ThitapaPoomvichid, PantidaPatirupanusara and MahasakKetcham, The QRCode for Audio Watermarking using Genetic Algorithm", IMLCS' 2012, pp11-12, 2012.
[3] Shanjun, Zhang; Kazuyoshi, Yoshino,"DWT-Based Watermarking Using QRCode Science Journal of Kanagawa University, pp3-6, 2008.
[4] Ray-Shine Run,Shi-Jinn Horng,Jui-Lin Lai,Tzong-Wang Kao, Rong-JianChen, An improved SVD-based watermarking technique for copyright protection",Expert Systems with Applications 39,2012,pp-673-689.
[5] Ahmad A. Mohammad, Ali Alhaj, Sameer Shaltaf, An improved SVD-basedwatermarking scheme for protecting rightful ownership" Signal Processing,Vol-88, 2008, pp: 2158- 2180.
[6] Bai Ying Lei n, IngYannSoon, ZhenLi, Blind and robust audio watermarkingschemes based on SVD-DCT" Signal Processing, Vol- 91, 2011, pp-1973-1984.
[7] VeyselAslantas. An optimal robust digital image watermarking based onSVD using the differential evolution algorithm" Optics Communications, Vol-282, 2009, pp-769-777. (3:59:58 PM) [8] Chin-Chen Chang a, Piyu Tsai b,Chia-Chen Lin, 2008". SVD-based digital image watermarking scheme. PatterRecognition Letters, Vol- 26, 2005, pp-15771586.
[8] Fangjun Huang, Zhi-Hong Guan "A hybrid SVD-DCT watermarking methodbased on LPSNR "Pattern Recognition Letters Vol-25, 2004, pp-1769-1775.
[9] Ming Jianga, b, Zhao-Feng Mao, b, Xin-xinNiua, Yi-Xian Yang, VideoWatermarkingScheme Based on MPEG-2 for Copyright Protection" in InternationaConference on Environmental Science and Information Application TechnologyESIAT 2011, Procedia Environmental Sciences, Vol-10, 2011, pp-843 848.
[10] Min-JeongLee,Dong-HyuckIm, Hae-YeounLee,Kyung- SuKim,Heung-KyuLee "Real-time video watermarking system on the compressed domain forhigh-definition video contents: Practical issues" Digital Signal Processing,vol-22, 2012,pp-190-198.
[11] He Yingliang, Yang Gaobo, Zhu Ningbo" A real-time dual watermarking algorithmof H.264/AVC video stream for Video-on- Demand service Int. J. Electron.Commune. (AE), Vol-66, 2012, pp-305312.