

A Robust QR-Code Video Watermarking With DCT Domain

¹Khandve Ashwini B. ²Udhane Priyanka P. ³Parkar Shalaka B. ⁴Kulthe Sagar A

BE Computer, PGMCOE, Wagholi. Pune.,Maharashtra.

BE Computer, PGMCOE, Wagholi, Pune,Maharashtra.

BE Computer, PGMCOE, Wagholi., Pune.,Maharashtra.

., BE Computer, PGMCOE, Wagholi., Pune.,Maharashtra.

Abstract—Domestic or industrial facilities on the internet and social media sites lacks in security to improve protection. The digital watermark embedded 2D Barcode is a most popular research in the digital field. This paper gives a watermarking of video with text data by applying the Quick Response (QR) Code method. The QR Code is generated to be watermarked via a robust video watermarking method based on the SVD and DWT. In addition to that logo (or) watermark gives the authorized ownership of video document. An attractive algebraic transform is SVD for applications of watermarking. SVD is applied to the cover I-frame. After extraction of the diagonal value it is fused with logo (or) watermark. After that DWT is applied on SVD cover image and QR code image. The watermarked image is inverse transformed and added to the frame into video which is then watermarked (include logo and QR code image) the video file sends to authorized customers. In reverse of this process we check the logo and then QR code for authorization of ownership. The imperceptibility and certain robustness in video processing can be used and achieved after experimental results.

Keywords-2D Barcode; Quick Response (QR) Code; singularvalue decomposition (SVD); Discrete Wavelet Transform (DWT).

I. INTRODUCTION

Concealed transmissions should be used using Data hiding, watermarking, closed captioning, indexing. It results in contrary to cryptography, where masking of the survival of the message itself is not done, but actually it shows hidden content. 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. By using the Quick Response (QR) Code technique in this paper we propose a video watermarking with text data (verification message). The QR Code is prepared to be watermarked via a robust video watermarking scheme which is based on the lossless video watermarking using DCT techniques messages can be sent and received in a secured way. Previously, video watermark was based on hiding of the secret information in image files.

The standard specifies 40 versions (sizes) of the QR code from the smallest 21x21 up to 177x177 modules in

size. An advantage with QR code is also there relatively small size for a given amount of information. The QR code is available in 40 different square sizes each with a user selectable error correction level in four steps. With the highest level of error correction used up to ~30% of the code words can be damaged and still be restored. The maximum capacity for QR codes depending on the encoding scheme (using the lowest possible error correction overhead).

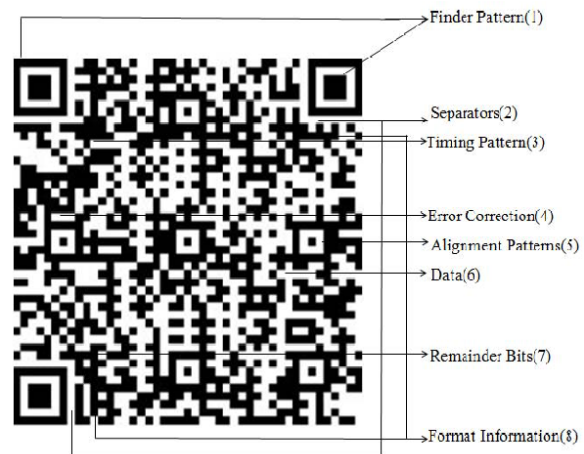


Figure 1. QR code

1) Finder Pattern:

The finder pattern contains of three similar structures which are resided in all corners of the QR Code except resided at the right side of bottom. Each pattern is based on a 3x3 matrix of black modules which is surrounded by white modules that are again surrounded by black modules. The Finder Patterns allows the decoder software to recognize the QR Code and determine the correct orientation.

2) Separators:

The separators which are white have a width of one pixel which helps in improving the recognized ability of the Finder Patters as they help in separating the actual data.

3) Timing Pattern:

The Timing Pattern contains alternating black and white modules which enable the decoder software to determine the width of a single module.

4) Error Correction:

The error correction codes are stored in 8 bits long code words in the error correction section is similar to the data section.

3) Alignment Patterns:

Alignment Patterns helps in supporting the decoder software which compensates for moderate image distortions. Version 1 QR Codes does not contain Alignment Patterns. As the code size grows then more Alignment Patterns are added.

4) Data:

Conversion of data is into a bit stream and after that it is stored in 8 bit parts (known as code words) in the data section.

5) Remainder Bits:

The above section consists of empty bits of data in which error correction bits cannot be divided into 8 bit code words in absence of remainder. The Quiet Zone surrounds entire QR Code and an area in the same color shade as white modules which helps in improving code recognition by the decoder software.

6) Format Information:

This section consists of 15 bits next to the separators and then information is stored about the error correction level of the QR Code and the chosen masking pattern.

4) Capacity and Error correction code:

On several factors the capacity of a QR Code is dependable. On the other side, the version of the code that decides its size the selected error correction level and the variety of encoded data influence capacity. Error Correction in QR Codes relies on Reed-Solomon Codes, a particular form of BCH error correction codes. In Error correction, there are four levels (Table 3) that can be selected by the user at the time of creation. Higher error correction levels expands the percentage of error correction capacity and therefore decreasing the error level.

II. LITERATURE SURVEY

The authentication and keeping integrity of region of are the important features necessary to be calculated by the watermarking system techniques which are good at these features are termed below.

Pan J. et al. [3] Proposed Digital watermarking is used in the concealing of a secret data within an original message and its extraction at its end. The secret message is integrated as water mark can be almost anything, for eg: a serial number, rawtext, image, etc. Zain et al. [8, 9] proposed a LSB-based technique for ultrasound images, where the previous image can be found completely. In

embedding stage, an SHA-256 hash code is solved for the ROI choosed. Next, the hash code is Integrated into the Least significant bits of RONI. The disadvantage of these two types is that the changeability of the technique is dependent on the truth that the previous values of RONI pixels were zeros before integrating, but for nonzero values, the scheme is not changeable. Zain et al. [10, 11] also proposed two techniques to embed the ability of finding change of state and finally regaining the image. In embedding process, therefore the image is splitted into partitions of 8×8 pixels each. Each partition B is further splitted into four sub-partitions of 4×4 pixels. The watermark, which is embedded using LSBs, in each sub-block, is a 3-tuple (v, p, r). The drawbacks of these two schemes are the lack of reversibility and using of averages as recovery information. Chiang et al. [7] proposed two reversible schemes based on difference expansion technique (DE) for tamper detection and recovery [2]

In the two techniques, the image is splitted into partitions of 4×4 each, and each partition is changed using two level DE scheme. Only smooth partitions, with same pixel values, are taken for integrating watermark. The disadvantage of this scheme is the limited capacity since only smooth partitions are used for integrating; therefore, it cant be used for all image modalities.

Wu et al. [6] proposed two schemes based on modulo 256 and discrete cosine transform (DCT). At first, the image is divided into several blocks, and for each block, an adaptive robust digital watermarking method combined with modulo operation is used to hide the watermark. The drawback of this scheme is limited hiding capacity, where only authentication and recovery data are embedded. Besides, the scheme is not reversible exactly due to preprocessing used to avoid pixel flipping.

Uma mageswari et al. [10] proposed a reversible watermarking technique to embed information into medical images. In this paper Region of interest (ROI) and Region of non interest (RONI) is defined. ROI is protected and effort is made to embed data in RONI. When medical image shared through network, for the compression purpose the JPEG2000 algorithm is proposed and to improve the information security to maintain the secrecy, reliability and accessibility of the embedded data Arnold's cat map method (Arnold Transform) is proposed. Patient information and disease information is embedded into DICOM images. Increase in authentication can be achieved using Kerberos technique. Prbhakaran et al. [4] proposes a video watermarking with text data (verification message) by using the Quick Response (QR) Code technique. A quick response (QR) code is a two dimensional barcode invented by the Japanese corporation Denso Wave. The QR Code is watermarked via a robust video watermarking scheme based on the (singular value decomposition) SVD and (Discrete Wavelet Transform) DWT.

This method is convenient, feasible and practically used for providing copyright protection. SVD is an algebraic transform for watermarking applications. SVD is applied to the cover I-frame. The extracted diagonal value is fused with logo (or) watermark. DWT is applied on

SVD cover image and QR code image. This method has achieved the improvement in perceptibility and security watermarking. Chakraborty et al. [1] proposes a digital watermarking technique which is a class of fragile reversible watermarking that constitutes and finds application in authentication of medical and military imagery. Reversible watermarking techniques ensure that after watermark extraction, the original cover image can be recovered from the watermarked image pixel by pixel. This paper also proposes a novel reversible watermarking technique as an improved modification of the existing histogram bin shifting technique. It develops an optimal selection scheme for the “embedding point” (gray scale value of the pixels hosting the watermark), and takes advantage of multiple zero frequency pixel values in the given image to embed the watermark. Experimental results for a set of images shows that the adoption of these techniques improves the peak signal-to-noise ratio (PSNR) of the watermarked image compared to previously proposed histogram bin shifting techniques.

III. PROPOSED SYSTEM

Aim of the project is to provide software that usually works (send a message a video unable for a human eye detect). The digitized video is inserted after & before. The video files that appeared to have no substantial differences.

The architecture of our system is:

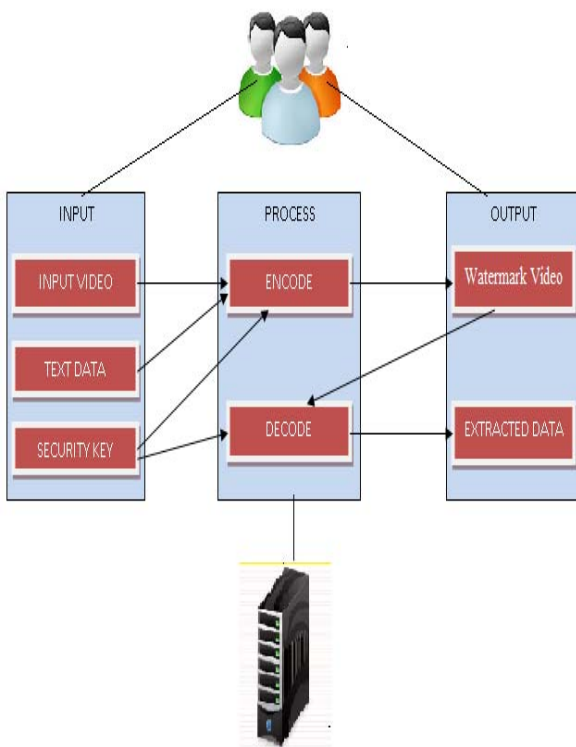


Figure 2. System Architecture

It explains user provide & it is security key, no of files video & large no text data used for hiding data. In

that process collect no of data & encode that data into that video file & formed the watermark video. In decoding process no of user provide key for security & that key is also used in the process of encoding. That system checks watermark video and security key of any user. Then extraction process is occurred i.e. decode the message from the video. The process of encoding & decoding is very secure in watermarked video.

A. 1. functionality of product

- a. Before and after sending any user find the text.
- b. any kind of text send.
- c. See the size of file any person.
- d. For Video Watermark Support of no of video file is necessary.
- e. It gives more security for play the video in any video file. Standard format for our application, so it is easy to handle for the user.
- f. It makes user-friendly & anyone can handle it.

2. Algorithm:

The Compressed video secure watermark-process

- 1) Cover video U, key stream key, message S:i/p.
- 2) Watermark-video X, adjust coefficient β :o/p.

B. 1. Preprocess:

Step a: message Encrypt
 $E_{key}(M) \rightarrow C$

Step b: Every I frame i in F it calculates value pixel in variance $2\sigma_{Fi}$ within DCT DC coefficients of DC & accuracy prediction of the accuracy & then it proposes another measure to find out the rule changes of the prediction.

Step c: The each frame is payload.

Step d: The each s_i , message are arranged bit for available AC DCT coefficients, estimate the change of special pixel values variance ΔDi .

Step e: Find out the correlation of ΔDi and $2\sigma_{Fi}$

If $\text{Corr}_{Fi} > T$
 then goto step c & adjust the coefficient β are adjusted.

IV. WORKING OF PROPOSED SYSTEM

A. Embedding Process

In the embedded process video file we have taken the I-frame and apply SVD. Insert a logo and take DWT on both I-frame with logo and QR code image was composite with DWT co-efficient. Next apply IDWT to obtain the watermarked image. Finally watermarked I-frame add in a video file. The schematic representation of extracting

process was given in the Fig 4. Figure 4. Shows the proposed embedded process.

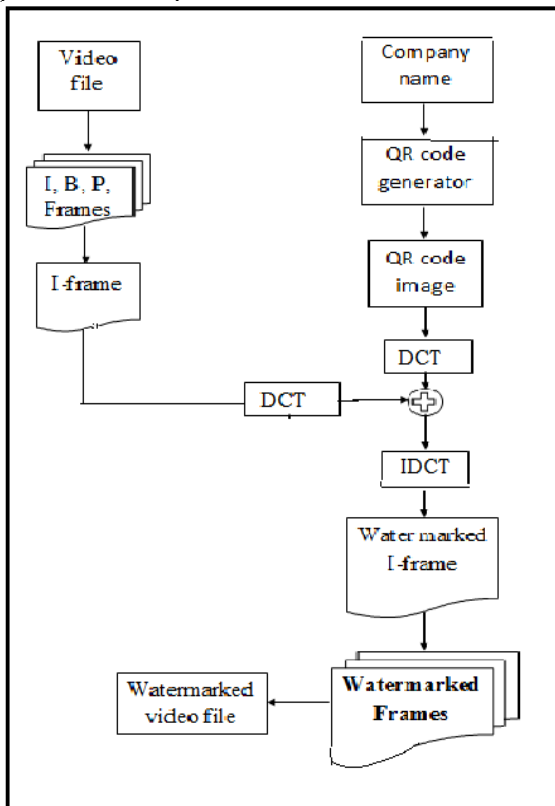


Figure3. Proposed Embedded Process

1) *Algorithm For Embedding Process:*

- Step 1: After reading video file extract RGB P-frame, B-frame, and I-frame.
- Step 2: Take the I-frame image as a cover image.
- Step 3: With company name generate a QR code image
- Step 4: To get combined image apply DWT on SVD cover image and also on QR code image
- Step 5: To get Watermarked I frame, take the inverse DWT on the combined image
- Step 6: Finally we have watermarked I frame image to get the watermarked video files.

B. *Extracting Process*

In extracting process, SVD is applied to watermarked image and recover the logo. Apply DWT on original video file and watermarked I-frame extract wavelet coefficient fusion process on the wavelet co-efficient, take the IDWT to obtain the QR code image. Finally extraction of verification text is done. The schematic representation of extracting process was given in the Fig 5. 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME).

C. *Extracting Process*

In extracting process, SVD is applied to watermarked image and recover the logo. Apply DWT on original video file and watermarked I-frame extract wavelet coefficient fusion process on the wavelet co-efficient, take the IDWT to obtain the QR code image. Finally extract the verification text. The schematic representation of extracting process was given in the Fig 5. 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME).

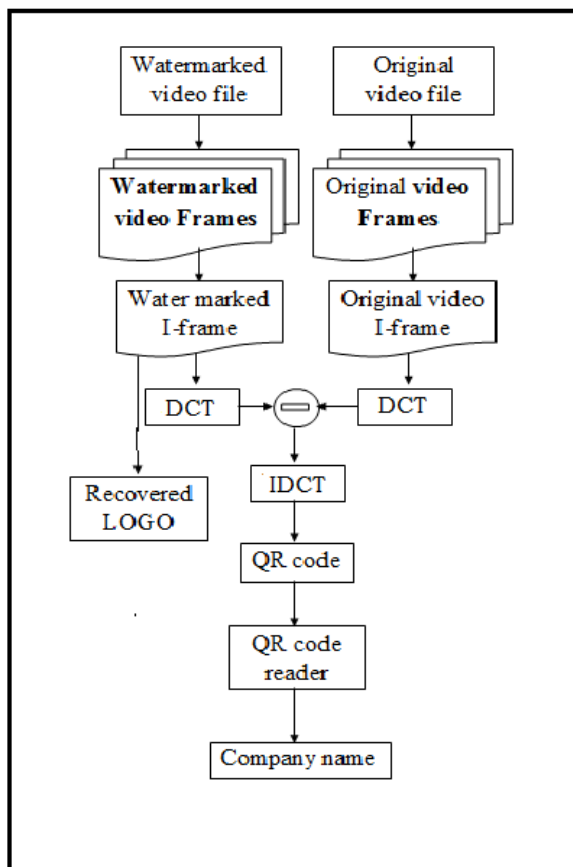


Figure 4. Proposed Extraction system

1) *Algorithm For Decoding Process*

- Step 1: After reading watermarked video files extract Watermarked I frame.
- Step 2: From original video file extract original Video I frame.
- Step 3: Apply DCT on both I frame of video.
- Step 4: To get a QR code image, subtraction of watermarked video I frame coefficient with original video I frame coefficient and take the Inverse DCT.
- Step 5: By using QR code reader extract the company name From QR code image.
- Step 6: From I frame we recover the logo.

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 method in the diagonal element watermark was embedded. On the other hand embedding text messages in the QR code image. So, the dual process given two authentication detail. The logo is located very safely in the QR code image. This is a method which is convenient, feasible and practically used for providing copyright protection. The experimental results shows that our method can achieve acceptable certain robustness to video processing.

ACKNOWLEDGMENT

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression, “One of us (R.B.G.) thanks . . .” Instead, try “R.B.G. thanks”. Put applicable sponsor acknowledgments here; DO NOT place them on the first page of your paper or as a footnote.

REFERENCES

- [1] Suppat Rungraungsilp, Mahasak Ketcham, Tanee Wiputtikul, Kanchana Phonphak, and Sartid Vongpradhip, “Data Hiding Method for QR Code Based on Watermark by comparing DFT with DWT Domain” ICCCT, May 26-27, 2012.
- [2] Thitapa Poomvichid, Pantida Patirupanusara and Mahasak Ketcham, “The QR Code for Audio Watermarking using Genetic Algorithm”, IMLCS’2012, pp 11-12, 2012.
- [3] Shanjun, Zhang; Kazuyoshi, Yoshino, “DWT-Based Watermarking Using QR Code” Science Journal of Kanagawa University, pp3-6, 2008.
- [4] Ray-Shine Run, Shi-Jinn Horng, Jui-Lin Lai, Tzong-Wang Kao, Rong-Jian Chen, “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-based watermarking scheme for protecting rightful ownership” Signal Processing, Vol-88, 2008, pp: 2158–2180.
- [6] Bai Ying Lei n, IngYannSoon, ZhenLi, “Blind and robust audio watermarking schemes based on SVD–DCT” Signal Processing, Vol- 91, 2011, pp-1973–1984.
- [7] Veysel Aslantas, “An optimal robust digital image watermarking based on SVD using the differential evolution algorithm” Optics Communications, Vol-282, 2009, pp-769–777.. Electronic Publication: Digital Object Identifiers (DOIs):
- [8] Chin-Chen Chang a, Piyu Tsai b, Chia-Chen Lin, 2008”. SVD-based digital image watermarking scheme.” Patter Recognition Letters, Vol- 26, 2005, pp-1577–1586.
- [9] Fangjun Huang, Zhi-Hong Guan “A hybrid SVD-DCT watermarking method based on LPSNR” Pattern Recognition Letters Vol-25, 2004, pp-1769–1775.
- [10] Ming Jianga, b, Zhao-Feng Mao, b, Xin-xin Niua, Yi-Xian Yang, “Video Watermarking Scheme Based on MPEG-2 for Copyright Protection” in International Conference on Environmental Science and Information Application Technology ESIAT 2011, Procedia Environmental Sciences, Vol-10, 2011, pp-843 – 848.
- [11] Min-Jeong Lee, Dong-Hyuck Im, Hae-Yeoun Lee, Kyung-SuKim, Heung-Kyu Lee “Real-time video watermarking system on the compressed domain for high-definition video contents: Practical issues” Digital Signal Processing, vol-22, 2012, pp-190–198.
- [12] He Yingliang, Yang Gaobo, Zhu Ningbo” A real-time dual watermarking algorithm of H.264/AVC video stream for Video-on-Demand service “Int. J. Electron. Commune. (AEÜ), Vol-66, 2012, pp-305–312.
- [13] Dooseop Choi, HoseokDo, HyukChoi, TaejeongKim, “A blind MPEG-2 video watermarking robust to camcorder recording”, Signal Processing, Vol-90, 2010, pp-1327–1332..