Robust and Secured Image Watermarking using DWT and Encryption with QR Codes

Vinita Gupta
M. Tech. Scholar, Department of CSE
O.I. S.T, Bhopal (M.P.), India

Atul Barve
Asst. Professor, Department of CSE
O.I. S.T, Bhopal (M.P.), India

ABSTRACT:
The paper proposed a colour image watermarking scheme based on the encrypted watermark with QR code and DWT. In this research, we are working on the security enhancement of image watermarking technique with the latest QR codes. The proposed methodology making image watermarking system more secure and robust adding encryption of watermark being embedded in cover image. The advantages of our proposed methodology is the watermark is completely invisible in cover image as well as the encryption process is quite simple but robust in nature .The recovered watermark is about nearest the main watermark. Experimental results show that the proposed algorithm enhances the anti- attack capability and the hidden nature of the image, increases the security of the watermarking detection, and has maximum robustness to cutting, random noise attack and JPEG compression.

Keywords
Watermarking, QR codes, Encryption, DWT.

1. INTRODUCTION
A Digital image watermarking systems have been proposed as an efficient means for copyright protection and authentication of digital image content against unintended manipulation(spatial chromatic)[1].Watermarking techniques tries to hide a message related to the actual content of the digital signal, watermarking is used for providing a kind of security for various type of data (it may be image, audio, video, etc.). Digital watermarking generally falls into the visible watermarking technology and hidden watermarking technology [3]. Visible and invisible watermarks both serve to deter theft but they do so in very different ways.

"Visible watermarks" are especially useful for conveying an immediate claim of ownership. The main benefit is that they virtually eliminate the commercial value of the document to a would-be thief without lessening the document's utility for genuine, authorized purposes. A common example is in the video domain where a logo is placed in a corner of the screen image. Invisible watermarks, on the other side, are more of a serve in catching the thief than disappointing the theft in the first place. In general, "visible watermarks" diminish the commercial value of a document or pictures, whereas invisible watermarks raise the likelihood of successful trial. The invisible watermark may also act as a deterrent if perpetrator is aware of their possible use.

There are two types of watermarking embedding domain: spatial domain and transform domain. Spatial watermarking can also be applied using colour partition such that the watermark appears in only one of the colour bands. However, the watermark appears when the colours are separated for printing. Spatial domain process involves addition of fixed amplitude pseudo-noise into the pictures. These approaches change the least significant bits of original contents. The watermark can be concealed into the data to assume that the LSB data are visually irrelevant.

There are many techniques proposed based on transformation based watermarking. Watermarking can be applied in the transform domain; including such transforms are discrete Fourier, discrete cosine, and wavelet. In this firstly the main data is transformed and then modifications are applied to transformed coefficients. Watermark is embedded in DFT, DCT and DWT domain coefficients.

Using digital watermarking, copyright information can be implemented into the multimedia data. This is implemented by using some algorithms. Information such as, picture, number or text with special implication can be fixed. The purpose of this information can be for copyright protection, hidden communication, authenticity distinguish of data file, text files etc. [4].

Digital watermarking systems can be classified in three schemes - they are Blind, Semi-blind and Non-blind. Blind watermarking scheme is also known as public watermarking method. This is the most difficult type of watermarking system as it requires neither the cover (original data), nor the embedded watermark, WT. These systems remove n bits of the watermark data from the watermarked data (i.e the watermarked image).

$$I' \times KY \rightarrow WT$$

Note: I' is the watermarked data, KY is the key

Semi-blind watermarking scheme is also known as semi-private watermarking scheme. This system does not require the cover (original data) for recognition. The purpose of this system to search whether that the watermark can be detected.

$$I' \times KY \times WT \rightarrow \{0,1\}$$

Non-blind watermarking scheme is also known as private watermarking scheme. This system requires as a minimum the cover (original data) for detection.
This scheme is to be understood as the most robust than the other methods as it exchanges very little information and requires access to secret material.

2. DISCRETE WAVELET AND QR CODE ANALYSIS
2.1 DWT (Discrete Wavelet Transform)
Wavelet analysis is a new technology of the time – scale analysis and multiresolution analysis, its basic idea is partly frequency separation to signal, that is multi-resolution decomposition. The image signal is two-dimensional signal, wavelet transform for image analysis is image multiresolution decomposition, the image is decomposed into a different space,

different frequency sub-image. Through wavelet transform, image is split into horizontal, vertical, diagonal, and low frequency four bands. Low frequency part is called the approximation sub-image; the remaining three parts are called the detail sub-image. 2 level wavelet decomposition process of the image shown in figure 3, HL, LH, HH are the horizontal high frequency, the vertical high frequency and the diagonal high frequency part, LL is the approximation low frequency part.

DWT based watermarking schemes use the same guidelines as DCT based schemes, i.e., concept is the same; however, transformation process of a picture into its transform domain varies and hence the resulting coefficients are different.

Wavelet transforms use different kind of filters to transform the image. There are various filters, but the most commonly used filters for watermarking are Daubechies Bi-Orthogonal Filters, Haar Wavelet Filter and Daubechies Orthogonal Filters. These filters decomposes the picture into many frequencies. First level decomposition gives four frequency sub band of the images. These four are called the LL, LH, HL, HH sub bands as shown in Fig.1

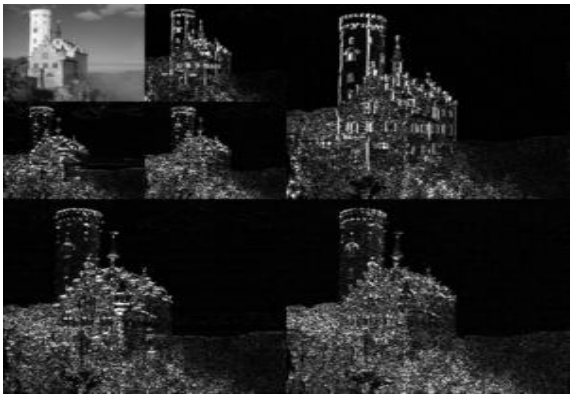

Figure 1: Two level decomposition using DWT.

In this part, we discuss wavelet based watermarking algorithms. We categorize these methods based on their decoder requirements as Non-blind Detection or Blind Detection. In, blind detection , original image for detecting the watermarks doesn't need; but, non-blind detection needs the original or cover picture.

1) High frequency coefficients are not well suited because they are removed during JPEG compression and other low frequency characteristics based computation like median filtering, salt and pepper noise.
2) Low frequency coefficients provide the more robustness against JPEG compression, low frequency characteristics filtering. It is more robust against the many noises.

QR(Quick response) code

QR Code is the trademark for a type of matrix barcode. Two-dimensional bar code technology comparing with the traditional one dimensional bar

QR code has the many advantages:

1. higher information density

2. It can express different characters like Chinese characters, pictures and sound with error correction function. In recent times, the system has become accepted outside the industry due to its fast readability and large storage capacity compared to standard UPC barcodes. The code consists of black modules (square dots) arranged in a square pattern on a white background. QR Code is able of managing all types of data, such as alphabetic characters, and numeric , symbols, binary, and control codes. Characters can be encoded in one symbol up to the 7,089 characters . Data can be restored even if the symbol is partially dirty or damaged. A maximum 30% of code words can be restored.

3. LITERATURE SURVEY

In image watermarking field, recently some work have been done, which is :

1. Qing Liu,Jun Ying(2012),"Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis"

In this paper, firstly, original image is transformed by using the DWT (Discrete wavelet transform) upto the 3-layers, means apply 3 times ,so that image is divided into the different sub band(LL,LH,HL and HH) and watermarked image is embedded into the intermediate frequency sub band. Blind watermarking technique is used to extract the watermark. Spread spectrum technic provides protected communications because signal is "hidden" like noise but it increases bandwidth of signal and increases the complexity and also used blind detection technique to extract the watermark is used.

2. Zhaoshan Wang, Shanxiang Lv,Yan Shna (2012)"A Digital Image Watermarking Algorithm Based on Chaos and Fresnel Transform"

In this paper, a digital image watermarking algorithm based on chaos and Fresnel transform is proposed. The original image is changed by using the concept of Fresnel diffraction plane by distance parameter, and watermark image is embedded after scrambled by chaotic sequence. The watermark image can be extracted without original image, and there is some changes on the original image after embedding. Chaotic scrambling encrypts watermark information. This technique, provide both good robustness and security.

3. Jithin VM,K K Gupta (2013)"Robust invisible QR code image watermarking in DWT domain",In this paper, QR code used as a watermark picture, this makes watermarked image more robust but if the embedding algorithm is known to unauthorized person then by using the QR code scanner software ,watermarking key can be easily extracted.

4. Nan Lin; Jianjing Shen; Xiaofeng Guo; Jun Zhou, (2011) title of paper is "A robust image watermarking based on DWT-QR decomposition"

A new blind watermarking technique based on QR decomposition. The method is implemented in wavelet domain and its robustness has been evaluated against some image processing attacks and the results have been compared with two classical methods i.e., SVD and DCT. It is shown that while the proposed scheme has low computational complexity, it has better robustness against some In In this paper , image processing attacks in comparison with SVD and DCT methods.

Copyright protection and authentication have become increasingly more important in routine life. The digital watermark is one of the method invented to handle this issue. In this paper, a digitally invisible watermark is embedded in a QR code image by means of wavelet transform. In the embedding methods, a binary picture, logo, is transformed into a equivalent watermark and then embedded into a selected sub

band. The experimental results shows that, for all the cases considered in this paper is more robustness to attacks and as such it can serve as a viable copyright protection and authentication tool.

4. PROPOSED METHODOLOGY

The proposed methodology is explained in this section here we have explained the block diagram of the watermark encryption and embedding process in the figure 2 and the execution if the algorithm explained using flow chart in the figure 3.

4.1 Watermarking Embedding Algorithm

The steps of the our proposed watermarking methodology is described as follows:

1. Select image I and Apply DWT on the Cover image
2. Select a key k to generates the QR(Quick Response) code as a secrete key.
3. QR code and Watermark is encrypted by using simple X-OR operation

   $$E(I,j)=W(I,j)\ \Theta\ QR(I,j)$$
4. Encrypted Watermark is embedded into the cover image by applying simple condition

   IF(E(I,j)==0)

   Then Red (I(I,j))=Red(I(I,j))+1

   Then Green (I(I,j))=Red(I(I,j))+1

   Then Blue (I(I,j))=Red(I(I,j))+1
5. Then apply Inverse DWT on the embedded watermarked image

   $$WI(I,j)=IDWT(I(I,j))$$

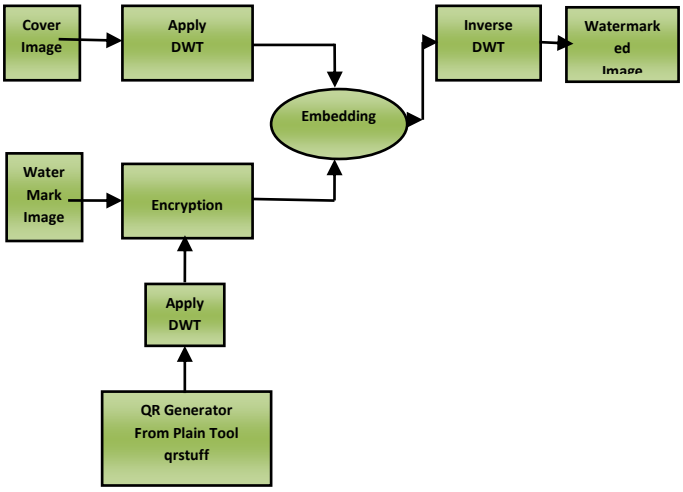

Fig. 2: Block diagram of Proposed Methodology Watermark Embedding

After encryption and embedding of watermark in cover image we have to recover the watermark and decryption shown in the block diagram and execution of the algorithm is shown in the figures.

Extraction Of Watermark. Select the watermarked image WI(I,j) and apply the DWT on the the watermarked image.

$$WD(I,j) = DWT(WI(I,j))$$

1. Select the original cover image I(I,j) and then apply the DWT on the Cover image.
2. Compare the transformed original image and watermarked image and get encrypted watermark E(I,j).
3. apply the decryption algorithm on the E(I,j)
   W(I,j)=QR(I,j) X-NOR E(i.j)

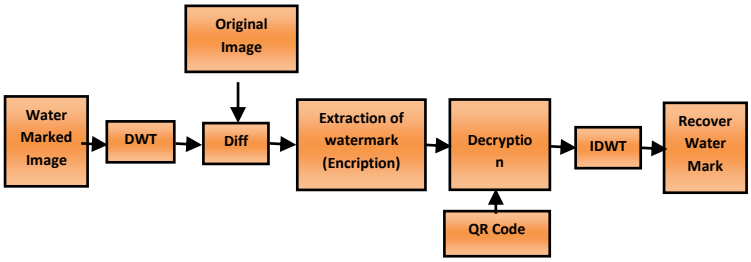

Fig. 3: Block diagram of Proposed Methodology Watermark Recovering

5. SIMULATION RESULTS

The simulation of the proposed watermarking methodology has been implemented on MATLAB simulation tool Release R2011a version 7.12. The simulation results shows the efficiency and experimental analysis of the proposed methodology in terms of PSNR, RMSE and MSE i.e. Peak Signal to Noise, Root Mean Square Error and Mean Square Error respectively.

The simulation results of whole watermarking process is given in the figures shown below. In figure 4, the original cover image and its histogram is shown, and in the figure 5, watermark image is shown. In figure 6 the QR code image is shown which can be generated from the any of the online websites which generates the QR Codes. The figure 7, shows the encrypted watermark after performing XOR operation of QR Code and Watermark.

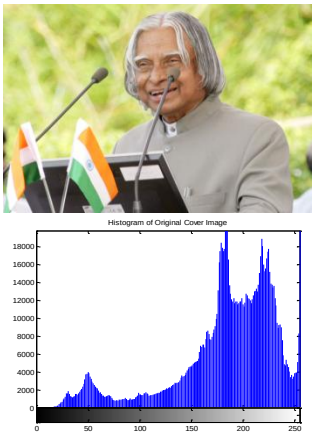

Fig. 4: Cover Image and its histogram

Fig. 5: Watermark

Fig. 6: QR Code image to encrypt Watermark before embedding

Fig. 7: Encrypted Watermark

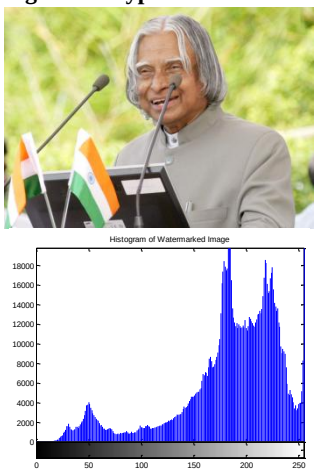

Fig. 8 Watermarked Image and its histogram

The figure 8 shows watermarked cover image and its histogram.

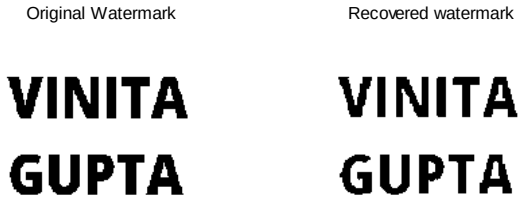

Fig. 9: Recovered Watermark

In figure 9, the recovered watermark is compared with the original watermark, which shows the efficiency of the proposed methodology.

After all the such embedding and recovering operation of watermark. We have analysed the various attacks i.e. JPG Compression attack, Gaussian Noise attack, Poisson Noise attack, Salt and Pepper Noise attack. The watermarked image after these attacks have been shown in the figures below from fig. 10 to 12.

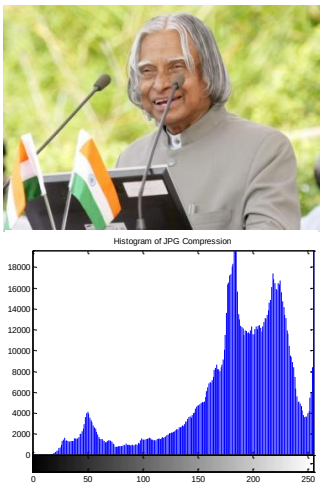

Fig. 10: JPEG Compression Attack

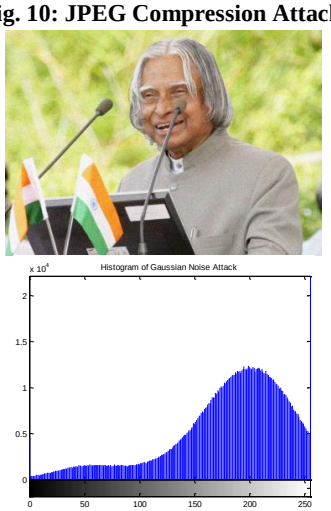

Fig. 11:Gaussian Noise Attack

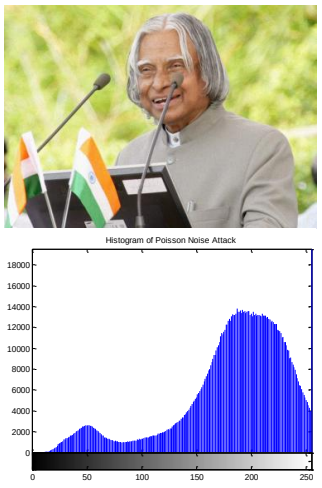

Fig. 12: Poisson Noise Attack

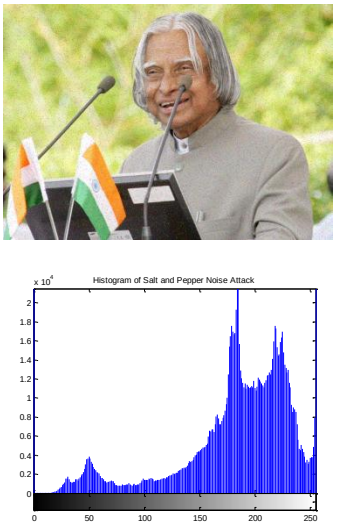

Fig. 13: Salt & Pepper Noise Attack

The above attacks have been also analysed using calculations of Peak Signal to Noise Ratio (PSNR), Root Mean Square Error(RMSE) and Mean Square Error (MSE) values which is described in the Table 2.

Table 2: Analysis of PSNR, RMSE and MSE values

Attack	PSNR	RMSE	MSE
Watermark Image	61.668dB	0.211	0.045
JPEG Compression	43.500dB	1.711	2.927
Poisson Noise	25.771dB	13.173	173.532
Gaussian Noise	20.471dB	24.250	588.054
Salt & Pepper Noise	17.743dB	33.195	1101.941

This algorithm is quite simple because of using simple X-OR operation for encryption and PSNR ratio of in analysis on various images is approax 62 DB.This algorithm is suitable on different kind of attacks on watermarked images like JPEG Compression, Possion Noise Attack, Salt & Pepper Noise and Gaussian Noise also.

6. CONCLUSION AND FUTURE SCOPE

After analysis of simulation of the proposed watermarking methodology it has been clear that the security of water mark does not change the quality of watermarked images but enhances the security of watermark significantly. The various attacks also reveals that the proposed methodology is also robust and better than the previous methods and techniques from security and robustness point of views. The upcoming era needs higher security enhancements in watermarking technologies in which the various high security encoding techniques can be used in the watermarking techniques as well as the techniques which significantly recover the watermark from watermarked image after various attacks.

7. REFERENCES

[1] Cox, IJ, Miller, ML & Bloom, JA 2002, Digital Watermarking, Morgan Kaufmann Publisher, San Francisco, CA, USA 2002.

[2] D.S. Xiang, G.L. Yang,YS. Xiong, "Survey of Digital Watormarking," ComPuter Engineering and Design, vol 2, pp.326-328,2005.

[3] Guan-Ming Su, "An Overview of Transparent and Robust Digital Image Watermarking", 2001.

[4] Kundur. D., Hatzinakos, D., "Digital Watermarking using Multiresolution Wavelet Decomposition", Proc. IEEE Int. Conf. On Acoustics, Speech and Signal Processing, Seattle, Washington, vol. 5, pp. 2969-2972, May 1998.

[5] Qing Liu,Jun Ying(2012),"Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis"

[6] Zhaoshan Wang, Shanxiang Lv,Yan Shna (2012)"A Digital Image Watermarking Algorithm Based on Chaos and Fresnel Transform", 2012.

[7] Jithin VM,K K gupta (2013)"Robust invisible QR code image watermarking in DWT domain",2013.

[8] Nan Lin; Jianjing Shen; Xiaofeng Guo; Jun Zhou, "A robust image watermarking based on DWT-QR decomposition," Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp.684,688, 27-29 May 2011.

[9] Naderahmadian, Y.; Hosseini-Khayat, S., "Fast Watermarking Based on QR Decomposition in Wavelet Domain," Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on , vol., no., pp.127,130, 15-17 Oct. 2010.

[10] Panyavaraporn, J.; Horkaew, P.; Wongtrairat, W., "QR code watermarking algorithm based on wavelet transform," Communications and Information Technologies (ISCIT), 2013 13th International Symposium on , vol., no., pp.791,796, 4-6 Sept. 2013.