Survey of Digital Watermarking algorithm of Quick Response Code Based on Discrete wavelet transform (DWT)(Review)

[1]Shaikh Ajij Amirsab, [2]Kajal Vikram More

[1]Ph.D Student, [2]Bachelor of Engineering
[1]KALINGA UNIVERSITY, [2]SRTM UNIVERSITY

***Abstract*—Digital watermark has been presently utilized as a possible solution for intellectual property rights protection. It is a technique for labeling multimedia data, including digital images, text documents, video and audio clips, by hiding secret information in the data. This embedded hidden information is unperceivable so the watermarked data appear identical to the original non-watermarked data. Moreover, this hidden information can neither be removed nor decoded without the required secret keys or algorithms. The current classical algorithm contains spatial domain algorithm and transformed domain algorithm. With the spatial domain algorithm, the embedding and the distilling of watermarking are finished in spatial domain, by emending directly or comparing the gray-level value or colour value. The classical spatial domain algorithms including several ways as follow: the least significant bit (LSB), Patchwork method with streak block map decoding, the method based on district intersecting and so on. Then the main current transformed domain algorithms are spread spectrum, DCT transformation method and DWT transform method.**

***Keywords—Image watermarking;* Human Auditory System (HAS); Human Visual System (HVS); Quantization; Quantization Index Modulation (QIM); Dither Modulation (DM); Mean Quantization; Vector Quantization**

1. Introduction

The objective of the project work aims to find out the benefits of using QR Code within companies and give reasonable recommendations on companies QR Code usage. In order to achieve this objective, this research is to explore the application of QR Code in We Chat and the characteristics of c. Moreover, examples are used to explore and explain the benefits of using QR Code. There are many popular techniques for this such as Steganography, Digital signature, Fingerprinting, cryptography and Digital watermarking but Digital watermarking is proved best out of them. Digital watermarks are of different types as robust, fragile, semi fragile, visible and invisible. Application is depending upon these watermarks classifications. There are some requirements of digital watermarks as integrity, robustness and complexity.

Any watermarking technique should exhibit at least the following four desirable characteristics:

1) Readability: A watermark should convey as much information as possible so the ownership and copyright can be ambiguously identified.

2) Security: A watermark should be secret and must be undetectable by an unauthorized user in general.

3) Imperceptibility: A watermark should not introduce any perceptible artifacts into the original image.

4) Robustness: A watermark should not be removed after attacks. It should be detected after a variety of distortions, such as JPEG compression and geometric operations. In digital watermarking, a watermark is embedded into a cover image in such a way that the resulting watermarked signal is robust to certain distortion caused by either standard data processing in a friendly environment or malicious attacks in an unfriendly environment. This project presents a digital image watermarking based on two dimensional discrete wavelet transform (DWT),MSE(Mean Squared Error),NC (Normalized correlation factor), PSNR(Peak Signal to Noise Ratio) are computed to measure image quality for each transform.

The basic idea of discrete wavelet transform (DWT) in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district. Then transform the coefficient of sub-image. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one low-frequency district(LL) and three high-frequency districts(LH,HL,HH). If the information of low-frequency district is DWT transformed, the sub-level frequency district information will be obtained. A two-dimensional image after three-times DWT decomposed Where, L represents low-pass filter, H represents high-pass filter. An original image can be decomposed of frequency districts of HL1, LH1, HH1. The low-frequency district information also can bedecomposed into sub-level frequency district information of LL2, HL2, LH2 and HH2. By doing this the original image can be decomposed for n level wavelet transformation. Most signal information of original image is in this frequency district. The frequency districts of LH, HL and HH respectively represents the level detail, the upright detail and the diagonal detail of the original image.

The qualified significant wavelet coefficients and their texture and luminance content across two different coarse scales (level 2 and level 3 wavelet decompositions) are utilized to determine the positions and the magnitudes to adaptively embed the digital watermark.

1.1 Advantages

- Digital Watermarking allows embedding of arbitrary information (the watermark) into digital media (such as video or images) by applying imperceptible, systematic alterations to the media data.

Higher level of security**:** Security and confidentiality of the embedded information is provided by a secret key. Without this key the watermark cannot be accessed or modified. Watermarks can be designed in such a way that the embedded information is still retrievable even after the carrier medium changed.

The advantage of digital watermarking is that the product of the embedding process is still a digital medium. Customers can do everything with a marked medium that they can do with an unmarked one. Watermarked media can be played or copied without any restrictions

Digital Watermarking is non-restrictive – only misuse is detectable and traceable.

1.2 ssDisadvantages

Digital watermarking is a recent research field; therefore its intrinsic limits are not well understood yet.

On the other hand, more insight into the technical possibility of satisfying the requirements imposed by practical applications is needed, if the practical possibility of using watermarking for copyright protection is to be evaluated. In the following, some of the most common limits shared by digital watermarking schemes are described.

Visible watermark can be easily removed.

A watermarking algorithm which is really robust does not exist yet. In the image case, robustness is still an open issue. More specifically, resistance to geometric manipulations such as cropping is recognized as a very difficult goal to achieve in a computationally efficient way

2. LITRETURE SURVEY

2.1Usha Pal,Dinesh Chandra "Survey Of DigitalWatermarking Using DCT" International Journal on Computer Science and Engineering (IJCSE) Vol. 4 No. 09 Sep 2012 [2]

The aim of digital watermarking is hidden information added into content of multimedia. DCT technique issued and when size of image is increase then also increases PSNR without decreasing power of embedded factor[2] (alpha factor) in same format. Digital Watermarking represents an effective method for authentication and ownership right protection.It involves embedding watermark data into original information .Watermark information cannot be stored in file header because anyone with a computer and a digital editing workstation would be able to convert the information to another format and remove the watermark. Thus the watermark always embedded to multimedia a signals. There are a lot of processes performed by unauthorized persons who aim to damage or corrupt the embedded information. These processes are called Attacks

2.2Sushila Kamble, Vikas Maheshkar , Suneeta Agarwal , Vinay KSrivastava "*DWT-SVD Based Secured Image Watermarking For Copyright Protection Using Visual Cryptography*" JSE-2012. [3]

A new robust watermarking technique for copyright protection based on Discrete Wavelet Transform and Singular Value Decomposition is proposed. The high frequency subband of the wavelet decomposed cover image is modified by modifying its singular values. A secret key is generated from the original watermark with the help of visual cryptography to claim the ownership of the image. The ownership of the image can be claimed by superimposing this secret key on the extracted watermark from the watermarked image. Also, the visual quality of the watermarked image is undistinguished from the original image.

The most popular technique is the least significant bit (LSB) method. In transform domain the watermark is embedded by modifying the frequency coefficients of the transformed image. The common methods in the transform domain are Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT), etc. The proposed technique is divided in two sections, embedding technique and the extraction technique

2.3 W. N. Cheung"*Digital Image Watermarking In Spatial And Transform Domains*",2000 IEEE. [4]

In the spatial domain, differential PCM is used to detect the edge regions of the image so that data can be hidden on those pixels of the image when the differential signal is larger than a certain threshold level. The method is based on the visual masking phenomenon at large intensity transitions in the neighborhood of the pixel.

Watermarks are classified as being visible and invisible. A visible watermark is intended to be seen with the content of the images and at the same time it is embedded into the material in such a way that its unauthorized removal will cause damage to the image. Firstly, the mark must not degrade the image as perceived by human, although the digital image has been modified by the watermark. Secondly, the information embedded in the watermark must be recoverable from the marked image by authorized persons for ownership identification, while at the same time it must not be accessible by unauthorized persons. Thirdly, the embedded watermark must remain secure in the material even if the image is subject to various processing operations such as compression and linear transformation.

2.4 Pravin M. Pithiya , H.L.Desai "*DWT Based Digital Image Watermarking, De Watermarking & Authentication*", Volume 7, Issue 5 (June 2013), PP. 104-109[6]

In this technique the embedding and extraction of the watermark is simple than other transform. In this algorithm watermarking, de watermarking of the image is done and it also checks the authentication of the watermarked image and de watermarked image.

This paper also successfully explains digital image watermarking based on discrete Wavelet transform by analyzing various performance parameters like PSNR, MSE, SNR and NC.There are many types of algorithms for digital image watermarking. Each type of algorithms has its own advantages and disadvantages. No method has perfect solution for digital watermarking. Each type has robustness to some type of attacks but is less efficient to some other types of attacks. each type of

digital watermarking depends on the nature of application and requirements. In this paper we presented a new method of embedding watermark into colour image. The RGB image is converted to YCbCr and watermarked by using discrete wavelet transform (DWT).

The luminance component Y of image is considered for embedding watermark. The performance of the proposed method can be evaluated by PSNR,SNR,MSE and NC for RED,BLUE and GREEN. Existing techniques have worked on the gray scale of image, we have taken results for RED,BLUE and GREEN separately[6]. Proposed technique results have shown that technique presented in this paper is very effective for watermarking and de watermarking authentication and also support more security and exact correlation between original watermark and extracted watermark.

2.5 Himanshu M. Parmar "Comparison of DCT and Wavelet based Image Compression Techniques" 2014 IJEDR | Volume 2, Issue 1 | ISSN: 2321-9939 [7]

Image compression approximately no reluctance. Through our approach of watermark embed and extraction in which wavelet as well as DCT domain is exploited, we can conclude that it is robust against the intentional compression attack as our target images are those that can be put on the internet with least possible defines as reducing the amount of data required to represent digital image. Transform coding, on the other hand, first transforms the image from its spatial domain representation to a different type of representation using some well-known transform and then codes the transformed values (coefficients). Image compression is urgently needed for very large medical or satellite images, both for reducing the storage requirements and for improving transmission efficiency [9].

3. SYSTEM MODELING

3.1Watermark embedding and extracting process using wavelet transform

A digitally invisible watermark is embedded in a QR code image by means of wavelet transform. In the embedding process, a binary image, logo, is transformed into a corresponding watermark and then embedded into a selected sub band Digital watermark is a pattern of bits inserted into a digital image, audio or video that identifies the copyright and authenticate information. The goal of watermark technique is to embed the secret information seamlessly hidden within into original message, which is robust against attacks. In recent years, some researchers have proposed the adoption of watermark techniques. The watermark can also be inserted in the original spatial domain of the image [18]. In the main disadvantage of spatial domain was that it easy to be hacked and attacked. In the proposed method embedded the copyright image into the original image using (N, N) secret sharing scheme. This method could resist contamination such as JPEG compression, resize and noise additional..

The concept, a tweak of the traditional bar code, has started to pop up in many places outside of manufacturingIt was a decision between our familiarity with Java, and the robust image and math tools available in MATLAB. In the end, we decided on MATLAB to take advantage of all the built in features for image processing. Additionally, we made the important decision to pare down the scope of the QR code reader – instead of designing it to read QR codes found in the wild, of the standard design, we built a custom "language" that our reader would recognize.

There are many techniques to embed the watermark into frequency domain of the original image. The techniques operating on a frequency domain use transformations such as Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) we will propose the blind watermarking algorithm by means of two-level discrete wavelet transform (DWT) embedded in a QR code image. Digital watermarking techniques can be classified into two categories with respect to operational domains, which are:

1. Spatial domain watermarking, the embedding process is done by directly modifying the pixel values.
2. Frequency domain watermarking, the embedding process is done by embedding the information in the transform space by modifying for example the frequency coefficients.

Nevertheless, most signal processing paradigms found in recent literature can be well characterized as the frequency domain operation. Moreover, several good perceptual models are developed in the frequency domain, with great successes reported. The process of embedding this watermark was performed on a QR code image on its frequency domain. The QR code image was first decomposed by a two-level two-dimensional wavelet transform. There were two steps in our algorithm: watermark embedding and watermark extraction.

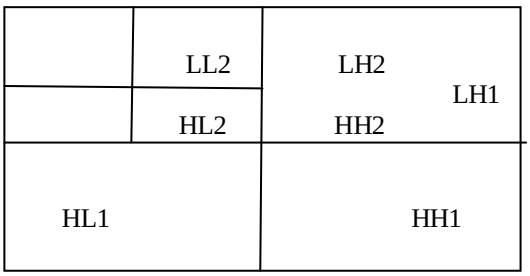

Figure3.1-level2-dimensional wavelet transform

A. Watermark Embedding

The step of embedding process are outlined as follows:Step of watermark image with secret key

I. The watermark image was produced as a bit sequence of watermark **S**. The data and background values were set to 1 and –1, respectively.

Step of QR code image

I. The two-level DWT of MxM image ti was computed for QR code image.

II. II. A watermark was then embedded in subband LH2 or where *N* is the total number of pixels in the watermark image.

III. ii. The pseudo-random sequence **(P)** whose each number can take a value either 1 or –1 was randomly generated with a secret key for embedding and extracting of the watermark[19].

Step of QR code image

I. The two-level DWT of MxM image ti was computed for QR code image.

II. A watermark was then embedded in sub band LH2 or HL2 or HH2. According to the rule

this processing was essential to turning getting accurate results during the decoding. The process is not perfect, as there is some fuzzing in certain areas, and it does not handle the part of the code that was brightened by lights (which could be commonplace with flash on phones).

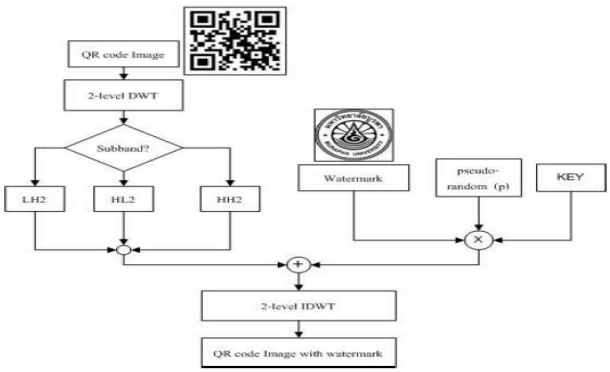

Figure 3.2 Watermark embedding process using wavelet transform

B. Watermark Extraction

The watermark extraction algorithm did not used the original QR code image. A prediction of the original value of the pixels is however needed. Thus, a prediction of the

original value of the pixels was performed using noise elimination technique. In this paper, we use an averaging 3×3 mask whose elements were fixed to 1/9. The extraction

Process is outlined as follows:

I. The predicted image it could be obtained by smoothing the input image i t with a spatial convolution mask. The prediction of

$$\hat{t}_i = \frac{1}{c \times c} \sum_{i}^{c \times c} t_i^*$$

the original valuecanbedefinedas:

Where *c* is the size of the convolution mask. The watermarked image and the predicted image were DWT transformed independently.

II. The estimate of the watermark

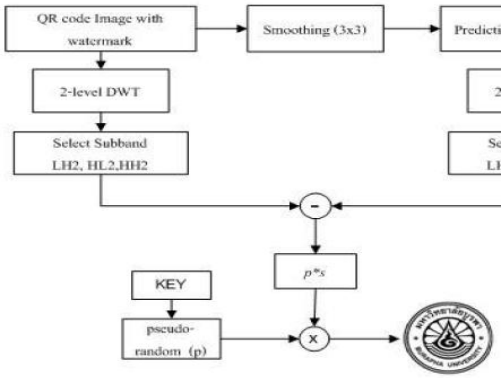

Figure 3.3 Watermark extracting process inverse using wavelet transforms (IDWT)

III. The sign of the difference between the predicted and the actual value is the value of the embedded bit:

$$sgn(\delta_i) = p_i . \hat{s}_i$$

IV. Compute NC

The watermark was then estimated by multiplying pseudo- random number to the embedded bit. If an incorrect pseudo random sequence was to be used, the scheme would not work.

4. CONCLUSION

The Experimental results prove that the quality of the watermarked image is better. Furthermore, the extracted watermark can be easily identified. The key to the successful implementation is to understand the advantages and the limitations of the watermark technology, and to use the watermark technology as a complimentary element to the existing security elements. Digital Watermarking describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video.They are characterizing patterns, of varying visibility, added to the presentation media as a guarantee of authenticity, quality, ownership, and source

REFERENCES:

[1] Y. Trank and W. Frank," Robust Image Watermarking in The Spatial Domain", Signal Processing, vol. 13, no 14, pp. 385-403, 1997.
[2]UshasPal,Dinesh Chandra*"SurveyOf DigitalWatermarking Using DCT"* International Journal on Computer Science and Engineering (IJCSE) Vol. 4 No. 09 Sep 2012
[3]Sushila Kamble, Vikas Maheshkar , Suneeta Agarwal , Vinay KSrivastava "*DWT-SVD Based Secured Image Watermarking For Copyright Protection Using Visual Cryptography*" JSE-2012.
[4] W. N. Cheung"*Digital Image Watermarking In Spatial And Transform Domains*", 2000 IEEE.
[5]W. N. Cheung"*Digital Image Watermarking In Spatial And Transform Domains*",2000 IEEE.
[6]Pravin M. Pithiya , H.L.Desai "*DWT Based Digital Image Watermarking, De Watermarking & Authentication*", Volume 7, Issue 5 (June 2013), PP. 104-109.
[7]Himanshu M. Parmar "Comparison of DCT and Wavelet based Image Compression Techniques" 2014 IJEDR |Volume 2, Issue 1 | ISSN: 2321-9939 [7]
[8] M. Barni and B. Bovid, "Digital Watermarking for Copyright Protection: A Communication Perspective", IEEE Communication Magazine, vol. 39, no. 8, pp. 90-91, 2001.
[9] A. Kumar and V. Santhi, "A Review on Geometric Invariant Digital Image Watermarking Techniques", International Journal of Computer Applications, vol. 12, no. 14, pp.31-36, 2010.
[10] F. Petitcolas, R. Anderson and M. Kuhn, "Attacks on Copyright Marking Systems in Information Hiding", LNCS, Berlin, vol. 1524, pp. 218-238, 1998.
[11] C. C. Chang and P. Tsai, "SVD-based Digital Image Watermarking Scheme", Pattern Recognition Letters, vol. 26, pp. 1577-1586, 2005.
[12] T. V. Nguyen and J. C. Patra, "A Simple ICA based Digital Image Watermarking Scheme", Digital Signal Processing, vol. 18, pp. 762-776, 2007.
[13] I. J. Cox and J. P. Linnartz, "Some General Methodsfor Tampering With Watermark", IEEE Journal on Selected Areas in Communications, vol. 16, pp. 587-593, 2010.
[14] Z. Bojkovic and D. Milovanovic, "MultimediaContents Security :Watermarking Diversity and Secure Protocols",6th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Service, TELSIKS, vol. 1, no. 3, pp. 377-383, 2003.
[15] S.J. Lee, S. H. Jung, "A Survey of Watermarking Techniques Applied to Multimedia", IEEE Transactions on Industrial Electronics, vol. 12 pp. 272-277, 2001.
[16] A.H. Ali, M. Ahmad, Digital audio watermarking based on the discrete wavelets transform and singular value decomposition, Eur. J. Sci. Res. vol. 39 no. 1, pp.6-21, 2010.
[17]W.Lu,H.LuandF.L.Chung,"FeatureBased Watermarking Using Watermark Template Match", Applied Mathematics and Computation, vol.177, no.1,pp. 886-893, 2011.
[18] Hamdy, S., El-messiry, H., Roushdy, M., & Kahlifa, E. (2010). Quantization Table Estimation in JPEG Images. International Journal of Advanced Computer Science and Applications - IJACSA, 1(6), 17-23.
[19] Babu, P. R. (2010). A Comprehensive Analysis of Spoofing. International Journal of AdvancedIJACSA, 1(6), 157-162.
[20] P. K. Dhar and M.I. Khan, "A New DCT-based Watermarking Method for Copyright Protection of Digital Audio", International Journal of Computer Science &Information Technology (IJCSIT), vol. 2, no. 5, pp. 91- 97, 2010.
[21] M. Tsai and H. Hung, "DCT and DWT-based Image Watermarking Using Sub sampling," in Proc. of the IEEE Fourth Int. Conf. on Machine Learning and Cybernetics, China, pp: 5308-5313, 2005.
[22] S. C. Liu and S. D. Lin, "BCH code based robust audio watermarking in the cestrum domain," Journal of Information Science and Engineering, vol. 22, pp. 535–543, 2006.
[23] H. B. Kekre, D. Mishra, "Image retrieval using image hashing", Techno-Path: Journal of Science, Engineering & Technology Management, SVKM"s NMIMS vol.2, n1,pp.230-240, 2010.
[24] D. Simitopoulo**s,** Fast Watermarking of MPEG-1/2 Streams Using Compressed-Domain Perceptual Embedding and a Generalized Correlator Detector EURASIP Journal on Applied Signal Processing,2004(8), pp 1088-1106, 2004. [25] M. A. T. Alsalami and M. M. Al-Akaidi, "Digital Audio Watermarking: Survey", Proc. 17th European Simulation multiconference,De Montfort UK, pp. 1-14, 2003. [26] C. Neubauer, and J. Herre, "Audio watermarking of MPEG-2 AAC bit streams", Preprints-Audio Engineering Society, 2000. [27] P. Artameeyanant, Wavelet audio watermark robust against MPEG compression, *Control Automation and Systems (ICCAS), Inter. Conf. on* , vol., no., pp.1375-1378, 27-30 Oct. 2010.
[28] E. V. Buskirk, "Are Digital Music Watermarks a BlessingoraCurse?",2007.http://www.wired.com/entertainment/music/commentary/listeningpost/2007/08/listeningpost 0820.

[29] C. Neubauer, and J. Herre, "Digital Watermarking and its Influence onAudio Quality", 105th AES Convention, San Fransisco, California.Preprint 4823, 1998.
[30] J. Lacy, R. Quackenbush, A. Reibman, D. Shur and J. Snyder, On "Combining Watermarking with Perceptual Coding". ICASSP Seattle, Washington. MMSP1.9, 1998. [31] L. Boney, A. H. Tewfik, K. N Hamdy 1996 Digital Watermarks for Audio Signals.EUSIPCO-96, VIII European Signal Proc. Conf.,Trieste,
[39] T.H. Chen, D.S. Tsai, Owner–customer right protection mechanism using a watermarking scheme and a watermarking protocol, Pattern Recognition 39 (8) (2006) 1530–1541.
[40] C.Y. Lin, S.F. Chang, A robust image authentication method distinguishing JPEG compression from malicious manipulation, IEEE Trans. Circ. Syst. Video Technol. 11 (2) (2001) 153–168.
[41] C.T. Hsu, J.L. Wu, Hidden digital watermarks in images, IEEE Trans. Image Process. 8 (1) (1999) 58–68.
[42] P. Loo, N. Kingsbury, Watermark detection based on the properties of error control codes, IEE Proc. Vis. Image Signal Process. 150 (2) (2003) 115–121.