2017

A QR Code Watermarking Approach based on the DWT-DCT Technique

Yang-Wai Chow
University of Wollongong, caseyc@uow.edu.au

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Joseph Tonien
University of Wollongong, dong@uow.edu.au

Wei Zong
University of Wollongong, wz630@uowmail.edu.au

A QR Code Watermarking Approach based on the DWT-DCT Technique

Abstract

The rapid growth in Internet and communication technology has facilitated an escalation in the exchange of digital multimedia content. This has resulted in an increase in copyright infringement, which has led to a greater demand for more robust copyright protection mechanisms. Digital watermarking is a means of detecting ownership and illegal use of digital products. This paper presents an approach to watermarking images by embedding QR code information in a digital image.

Keywords

dwt-dct, qr, watermarking, technique, approach, code

Disciplines

Engineering | Science and Technology Studies

Publication Details

Chow, Y., Susilo, W., Tonien, J. & Zong, W. (2017). A QR Code Watermarking Approach based on the DWT-DCT Technique. Lecture Notes in Computer Science, 10343 314-331. Auckland, New Zealand ASCIPS 2017: 22nd Australasian Conference on Information Security and Privacy

A QR Code Watermarking Approach based on the DWT-DCT Technique

Yang-Wai Chow, Willy Susilo, Joseph Tonien, Wei Zong

Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Wollongong, Australia
{caseyc, wsusilo, dong}@uow.edu.au, wz630@uowmail.edu.au

Abstract. The rapid growth in Internet and communication technology has facilitated an escalation in the exchange of digital multimedia content. This has resulted in an increase in copyright infringement, which has led to a greater demand for more robust copyright protection mechanisms. Digital watermarking is a means of detecting ownership and illegal use of digital products. This paper presents an approach to watermarking images by embedding QR code information in a digital image. The notion of the proposed scheme is to capitalize on the error correction mechanism that is inherent in the QR code structure, in order to increase the robustness of the watermark. By employing the QR code's error correction mechanism, watermark information contained within a watermarked image can potentially be decoded even if the image has been altered or distorted by an adversary. This paper studies the characteristics of the proposed scheme and presents experiment results examining the robustness and security of the QR code watermarking approach.

Keywords: Data hiding; Discrete cosine transform; Discrete wavelet transform; Error correction; QR code; Watermarking

1 Introduction

Advances in Internet and communication technology have given rise to an increase in the exchange and sharing of digital multimedia content. However, this has also facilitated the rise in copyright infringement, which has resulted in the demand for better and more robust copyright protection techniques.

Digital watermarking is an effective solution for detecting copyright infringement and the illegal usage of digital products. The notion of watermarking is to embed extra information in an original signal, and when needed, the watermark can be extracted [17]. The embedding of additional information in the original signal, also known as host data, must be done in a way that does not interfere with the normal usage of data [31]. Hence, to be a successful watermarking scheme, the difference between the watermarked and the original signal should be imperceptible. In addition, the watermark should be robust against signal alteration, up to a point at which the host signal is damaged and loses its commercial value [32].

The field of digital watermarking is an area that has been studied extensively for many years [11]. Panah et al. [31] describe four main properties of any watermarking system; namely, invisibility, capacity, robustness and security. Invisibility is the property whereby the watermark should be imperceptible by a human; capacity refers to the amount of data that can be embedded; robustness is the ability of the watermarking scheme to withstand alterations or distortions to the signal; and security is the watermarking scheme's resistance against any intentional attempt by an adversary to impair the watermark [10, 31].

Over the years, researchers have proposed various watermarking techniques for embedding information in various multimedia signals, including images, video and audio [35]. The work in this paper focuses on invisible watermarking for digital images. There are two main categories of invisible digital watermarking; namely, the spatial domain and the frequency domain. Spatial domain techniques work by altering the gray levels of some pixels. Whereas, the other category focuses on modifying coefficients in the frequency domain [19].

There are various advantages of operating in the frequency domain, such as, being able to incorporate features of the human visual system in watermarking more effectively, the ability spreading the energy of the embedded signal in the frequency domain over all pixels in the spatial domain, and being able to operate in the compressed domain since most image compression standards are based on the frequency domain [19]. For this reason, numerous researchers have proposed watermarking techniques in the frequency domain based on the Discrete Cosine Transform (DCT) and the Discrete Wavelet Transform (DWT) [4, 25, 28]. In recent years, the use of DWT-DCT hybrid techniques as a way of improving the robustness of the watermark has also received much attention [1–3, 12, 14, 21, 26, 35].

This paper proposes a QR code watermarking technique that is based on the DWT-DCT approach. The QR code is a two-dimensional barcode that has seen widespread adoption in many different applications over the last few years, due to its convenience and ease of use, as any smartphone equipped with a camera and QR code reader can retrieve the information encoded within a QR code. The fundamental idea behind the technique proposed in this paper is to capitalize on the error correction mechanism that is inherent in the QR code structure. The purpose of this is to increase the robustness of the resulting watermark against alterations or distortions, as the information contained within the QR code can still be decoded as long as the corrupted data does not exceed the QR code's error correction capacity.

Our Contribution. In this paper, we present a watermarking technique for embedding QR code information in a host signal by adopting a combined DWT-DCT approach. This paper focuses on applying the proposed technique to digital images. We examine the scheme based on the key properties of a watermark; namely, invisibility, capacity, robustness and security. The capacity of the scheme is simply the data capacity of the embedded QR code, which depends on its version and error correction level. For the other properties, this paper shows results

of our experiments demonstrating the invisibility characteristics of the scheme using conventional image quality metrics. In addition, we present results examining the proposed scheme's robustness and security properties under varying conditions and against common image alterations and attacks.

2 Background

This section provides a brief background to some of the key concepts and techniques used in this research.

2.1 The QR Code

The company Denso Wave [13] invented the Quick Response Code (QR code) in 1994 for the automotive industry in Japan. After its inception, the International Organization for Standardization (ISO) established a standard for the QR code [20]. Since then, QR codes have seen widespread adoption worldwide due to its ease of use, robustness, fast decoding, high data capacity and so on.

A QR code symbol is constructed as a two-dimensional array of light and dark squares, referred to as modules. There are forty sizes of QR code symbol versions ranging from versions 1 to 40, each consisting of a different number of modules, resulting in different data capacities. A QR code can encode different types of data (i.e. alphanumeric, binary, Kanji or a combination of these) and has support for four error correction levels (i.e. L, M, Q and H). The error correction mechanism provides a means for data recovery even when a certain amount of modules in a QR code are corrupted. The four error correction levels correspond to error tolerances of approximately 7%, 15%, 25% and 30% respectively. The QR code error recovery capability increases at the expense of message length. Fig. 1 shows an example of a QR code version 1 with error correction level H; it encodes the word "message".

Fig. 1. QR code version 1, error correction level H.

2.2 Discrete Cosine Transform (DCT)

The Discrete Cosine Transform (DCT) converts a signal into the frequency domain and is often used in image processing, especially in JPEG compression [19,

33]. Given an input image, x, the computation of the DCT coefficients for the transformed output image, y, is obtained using the equation shown in Eq. 1. Once transformed, the original image can be recovered using the inverse DCT, as given by Eq. 2 [2, 33].

$$y(u,v) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\alpha_u\alpha_v \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} x(m,n)\cos\frac{(2m+1)u\prod}{2M}\cos\frac{(2n+1)u\prod}{2N} \tag{1}$$

where

$$\alpha_u = \begin{cases} \frac{1}{\sqrt{2}} & u = 0 \\ 1 & u = 1, 2, ..., N-1 \end{cases}$$
$$\alpha_v = \begin{cases} \frac{1}{\sqrt{2}} & v = 0 \\ 1 & v = 1, 2, ..., N-1 \end{cases}$$

$$x(m,n) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\alpha_u\alpha_v \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} y(u,v)\cos\frac{(2m+1)u\prod}{2M}\cos\frac{(2n+1)u\prod}{2N} \tag{2}$$

The blocked based DCT approach separates an image into non-overlapping blocks, before applying the DCT to each block [22]. Watermark data is typically embedded in the mid-band coefficients of each DCT transformed block in order to keep visual alteration of an image to a minimum [4].

2.3 Discrete Wavelet Transform (DWT)

The Discrete Wavelet Transform (DWT) is another technique that is widely used in image and signal processing. The DWT technique for images involves the decomposition of an image into frequency channels of constant bandwidth on a logarithmic scale [25, 30]. A 2D image is decomposed into four sub-bands, which are denoted as LL, LH, HL and HH at level 1 in the DWT domain. The LL sub-band represents the coarse-level coefficients, whereas the LH, HL and HH sub-bands represent the finest scale wavelet coefficients. Each sub-band can be decomposed further until the desired number of levels is reached. The human visual system is more sensitive to the LL sub-band (i.e. the low frequency component), watermarking is typically embedded in one or more of the other three sub-bands to maintain better image quality [25].

2.4 Arnold Transform

The Arnold transform is a invertible method that can be used for pixel scrambling, and has been adopted in various watermarking schemes [22]. The purpose of applying this transform is due to the fact that adjacent pixels in image data have strong correlation to each other. By using the Arnold transform, this high

pixel correlation can be disrupted. The Arnold transform is shown in Eq. 3 [16], where p and q are positive integers, $\det(A) = 1$, and (x', y') are the new coordinates of the pixel after Arnold transform is applied to a pixel at position (x, y). The period of the Arnold transform depends on p, q and the size N of the image. After several iterations of applying the transform, the correlation among adjacent pixels can be disturbed completely.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} \mod N = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mod N \tag{3}$$

The Arnold Transform has also been used for image encryption [16]. The underlying notion for this is that the shuffling the pixels in the spatial domain confuses the relationship between the cipher image and the plain image. For image encryption, the parameters p, q and the number of iterations of applying the transform, can all be used as the secret keys.

3 Related Work

The QR code has seen a variety of applications in the area of information security. For example, QR codes have been used for secret sharing [8], authentication and transaction verification [7], authenticating visual cryptography shares [36] as well as for e-voting authentication [15].

Researchers have also proposed schemes for using the QR code in the area of data hiding and steganography. Among the work conducted in this area, Wu et al. [37] proposed a data embedding approach for hiding a QR code in a digital image. Their purpose was to camouflage the appearance of a QR code in an image so as not to degrade the visual quality of the picture. Huang et al. [18] developed a reversible data hiding approach for images with QR codes. The purpose of their method was to be able to restore a portion of an image that was covered by a QR code. A nested image steganography scheme was proposed by Chen and Wang [5] using QR codes, where two types of secret data, i.e. text (lossless) and image (lossy), are embedded in a cover image. The text portion was embedded in the form of a QR code. A similar approach was reported in Chung et al. [9].

In addition, QR codes have been used in a number of recent digital watermarking schemes. A method of embedding a QR code in the HH component at the first level of the DWT domain of a cover image was previously proposed [34]. The objective of this approach was to be able to detect malicious interference by an attacker based on a unique image registry code. A digital watermarking scheme using a Just Noticeable Difference (JND) model for embedding QR codes in images was described by Lee et al. [27]. The aim of their approach was to improve the imperceptibility of a watermark based on JND, which is the maximum difference at which the human visual system is not able to detect a difference. Kim et al. [24] studied a method of using 2D barcodes, e.g., QR codes, to insert a digital object identifier tag in digital content without degrading its quality. Kang et al. [22] proposed a watermarking approach based on the combination of DCT,

QR codes and chaotic theory. In their approach, a QR code image is encrypted with a chaotic system to enhance the security of the watermark. Others have also proposed different QR code watermarking approaches [6, 38].

The motivation behind the QR code watermarking technique proposed in this paper is to increase the robustness of the watermark against image alteration and/or distortion. The proposed approach capitalizes on the error correction mechanism that is inherent in the QR code structure. By embedding a QR code watermark into a digital image, the QR code can be decoded correctly as long as the data in the QR code has not been corrupted above its error correction capacity. As such, this approach attempts to increase the resulting robustness of the invisible watermarking scheme against watermarking attacks where an adversary tries to remove the watermark by altering or distorting the image.

4 Proposed QR Code Watermarking Scheme

4.1 The Embedding Process

The proposed QR code watermarking scheme takes a QR code, which contains the watermark information, and embeds it in a cover image. An overview of the process for embedding the QR code in the cover image is depicted in Fig. 2.

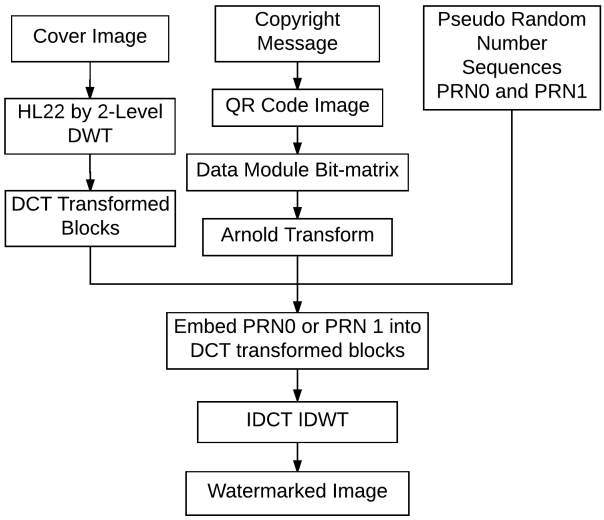


Fig. 2. Overview of the QR code watermark embedding process.

For generating the QR code, the QR code's mask pattern and error correction level are predetermined beforehand. This is so that the QR code's format information can be omitted in the embedding process, and only the data modules will be embedded in the cover image. The reason for this is to ensure that

the format information cannot be corrupted even if the resulting watermarked image undergoes alteration or distortion. In that manner, when the QR code is extracted from the watermarked image, it can be correctly decoded with the predetermined format information as long as the data modules have not been corrupted beyond the QR code's error correction capacity. The QR code's data modules are extracted into a binary matrix, which is scrambled using Arnold transform to increase its robustness against alteration or distortion. This produces the data matrix that will be use for embedding the QR code data in the cover image.

The cover image will be decomposed using DWT into four sub-bands as depicted in Fig. 3(a). This can be continued to the desired level. In our experiments, we decomposed the HL sub-band to level 2, as shown in Fig. 3(b), and used the HL22 sub-band for embedding the watermark. The contents of this sub-band are then separated into non-overlapping blocks where the DCT is applied to each block. Only the mid-band coefficients of the DCT transformed blocks are modified to keep the visual alteration to a minimum, as depicted in Fig. 3(c). In addition, two non-correlated Pseudo-Random Number (PRN) sequences, are generated to represent bit '0' and bit '1' (i.e. PRN0 and PRN1). The length of each PRN sequence matches the number of mid-band DCT coefficients. The data matrix containing the QR code data is then embedded in the DCT coefficient blocks using the PRN sequences, according to Eq. 4, where x is the respective mid-band coefficient, x' is the modified coefficient and α is the gain factor. Finally, the inverse DCT and inverse DWT are applied to obtain the resulting watermarked image.

$$x' = \begin{cases} x + \alpha \times PRN0, \text{ if the bit is '0'} \\ x + \alpha \times PRN1, \text{ if the bit is '1'} \end{cases} \tag{4}$$

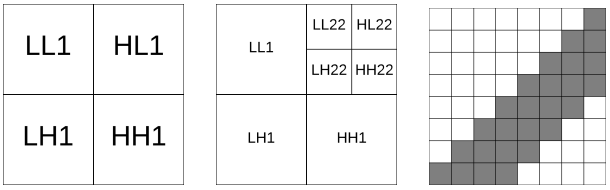


Fig. 3. (a) DWT at level 1; (b) DWT at level 2; (c) Mid-band coefficients of an 8×8 DCT block.

4.2 The Extraction Process

Image pre-filtering techniques have been used to improve watermark extraction results [29]. Therefore, we first apply a sharpening and the Gaussian of Laplacian

filters to the watermarked image to increase the contrast between the watermark and the cover image related sections [23]. The resulting pre-filtered image then undergoes the same DWT and DCT procedure as the embedding process to decompose the image into sub-bands and non-overlapping blocks. The data matrix can be extracted based on the correlation between the known PRN sequences and the mid-band coefficients of each DCT transformed block. The inverse Arnold transform is then applied to the data matrix using the known transform parameters to obtain the QR code data, which can be decoded based on the format information to obtain the encoded message. This process is shown in Fig. 4.

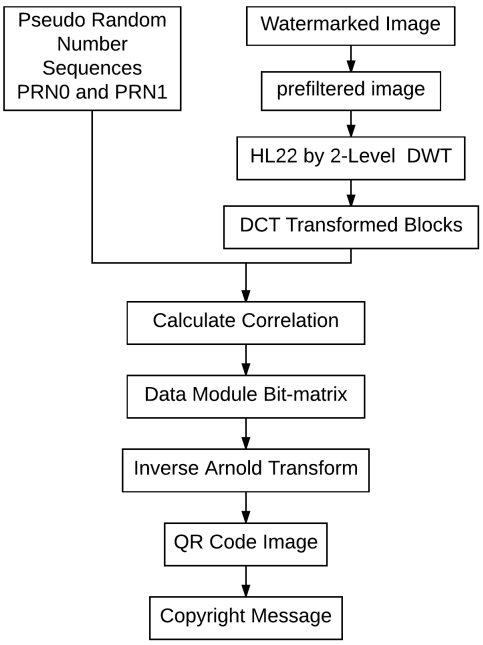


Fig. 4. Overview of the QR code extraction process.

5 Results and Discussion

To evaluate the proposed watermarking scheme, experiments implementing the watermarking process in MATLAB were conducted on three well know cover images; namely Lena, Peppers and Baboon. These images are shown in Fig. 6. The choice of these images was due to the varying degrees of variance in the images. These were 8-bit gray scale images with the dimensions of 512×512. The QR code that was previously shown in Fig. 1 was used as the watermark

in the experiments. It was constructed with the error correction level H, which means that data corruption of below approximately 30% can still be decoded correctly. In the experiments, the range of PRN values were varied between a range of values that were centered on zero.

5.1 Invisibility

Quantitative measurements to ascertain the degree of imperceptibility of the watermark were conducted using the Peak Signal-to-Noise Ratio (PSNR), which is a commonly used image quality metric, between the original image and the watermarked image. Fig. 5 shows a plot of the PSNR values for Lena that were obtained by varying the PRN range, with $\alpha = 4$, using different pseudo-random seed values. The other images have the same characteristics. Greater PSNR values mean less difference between the watermarked image and the cover image. On the other hand, the larger the PRN range, the more robust the watermark is to image alterations. Nevertheless, larger ranges also produces greater distortion in the resulting watermarked image since there will be greater modification of the DCT coefficients. This is evident from the decreasing PSNR values in Fig. 5 at larger PRN ranges.

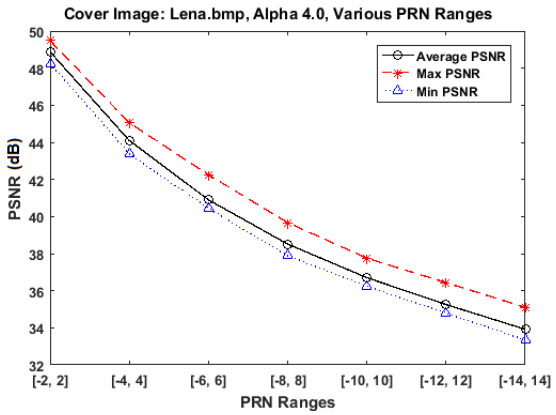


Fig. 5. Characteristic PSNR values.

Fig. 6(a) to Fig. 6(e) gives a visual comparison of the watermarked image based on different watermark parameters. The stronger the watermark (i.e. more robust and higher chance of successful watermark extraction), the higher the distortion in the resulting watermarked image. The original cover images are shown in Fig. 6(a). Fig. 6(b) show watermarked images with very low distortion obtained from a PRN range of ± 4 and $\alpha = 2$; in Fig. 6(c) the parameters where PRN: ± 6, $\alpha = 4$; in Fig. 6(d) the parameters where PRN: ± 10, $\alpha = 6$; Fig. 6(e) in turn shows an example of a watermarked image with very distortion with

PRN: ± 14, $\alpha = 14$. It can be seen that the watermark is imperceptible from the perspective of the human visual system when the watermarked images were generated with lower parameters, while the distortion can clearly be seen with high parameter values. When the distortion is perceptible in the watermarked image, it looses its commercial value.

5.2 Robustness and Security

To evaluate the robustness and security of the proposed scheme, some common distortions and attacks were applied to the watermarked images; namely, JPEG compression, salt-and-pepper noise and cropping.

First, the robustness of the proposed scheme was evaluated by varying PRN ranges for the three images, as depicted in Fig. 7(a) to Fig. 7(c), respectively. Since the QR code that was used had an error correction level of H, this means that codeword errors below 30% gives rise to a high probability that the extracted QR code can be decoded correctly. It can be seen that the percentage of codeword errors in the watermarked Lena image, Fig. 7(a), is very much below the 30% threshold. While the watermarked Peppers image, Fig. 7(b), shows similar characteristics, note that the percentage of codeword errors are higher. Nevertheless, the errors are still below the threshold. On the other hand, Fig. 7(c), which shows the watermarked Baboon image, has a much higher percentage of codeword error. This is largely due to the fact that the variance in the Baboon image is much greater than the other two images. This implies that larger PRN ranges have to be used in the proposed scheme for images with large variances.

JPEG Compression. Fig. 8 provides a depiction of the scheme's robustness to JPEG compression. JPEG compression is one of the commonly used attacks for watermark removal. MATLAB's inbuilt JPEG compression function was used for the experiments. The function accepts parameters ranging from 0 (i.e. low quality compression) to 100 (i.e. high quality compression), inclusive. It should be noted that once the JPEG compression quality is above a certain threshold the image quality significantly degrades to the point of having no commercial value.

It can be seen that the watermarked Lena and Peppers images, Fig. 8(a) and 8(b) respectively, are consistently robust to JPEG compression. The robustness of the watermarked Baboon image, Fig. 8(c), is less that the other two images, but the watermark can still be decoded under favorable conditions. This is due to the larger amount of variance in the Baboon image compared to the other two images. Fig. 8(d) to Fig. 8(f) show comparative robustness results when the watermark's strength was increased. It can be seen that with increased watermark strength, the watermark information can consistently be extracted successfully even for the Baboon image.

Salt-and-Pepper Noise. A salt-and-pepper noise attack is where an adversary deliberately introduces sparse random black and white pixels in a watermarked

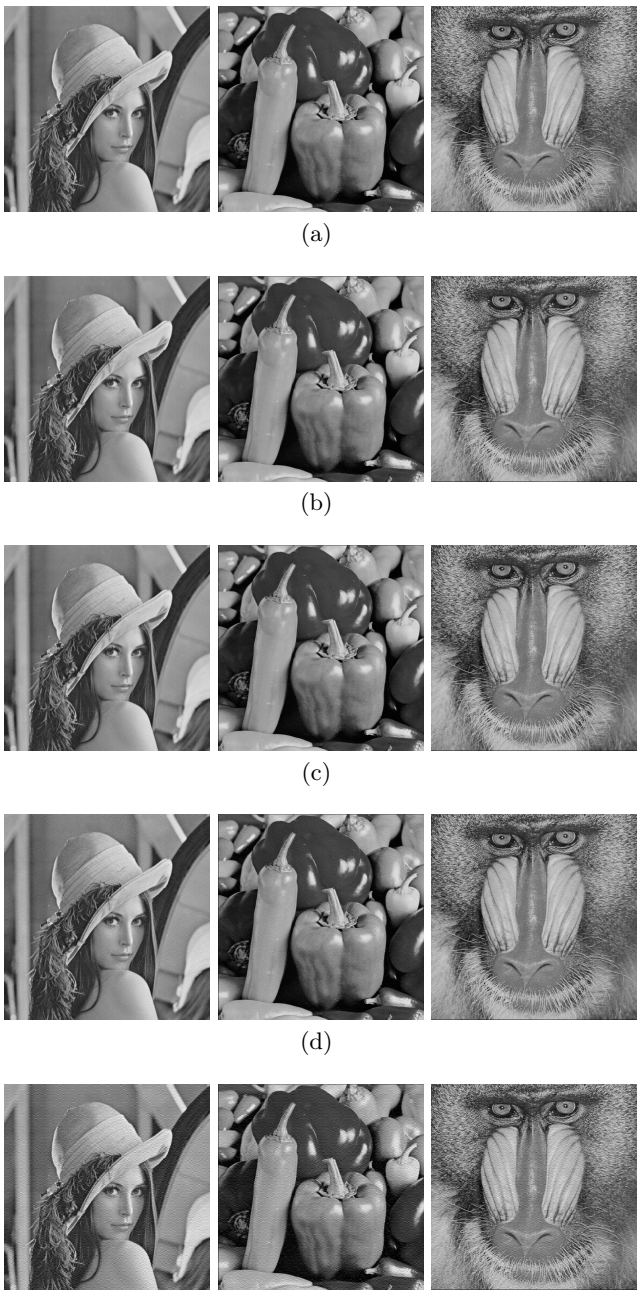
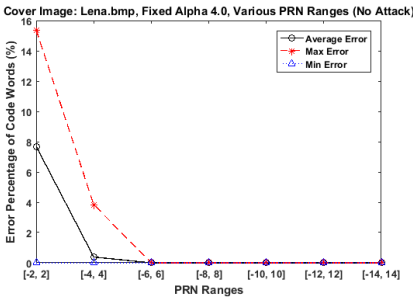
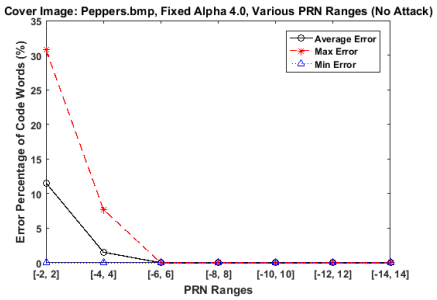


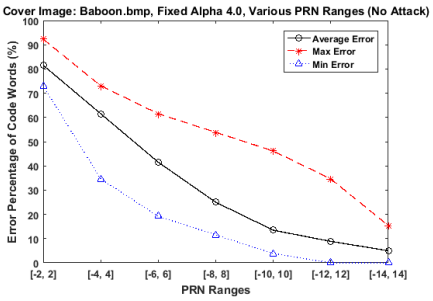
Fig. 6. Comparison between the images with different watermark strengths and levels of distortion; (a) very low distortion; (b) low distortion; (c) mid distortion; (d) high distortion; (e) very high distortion.



(a) Lena

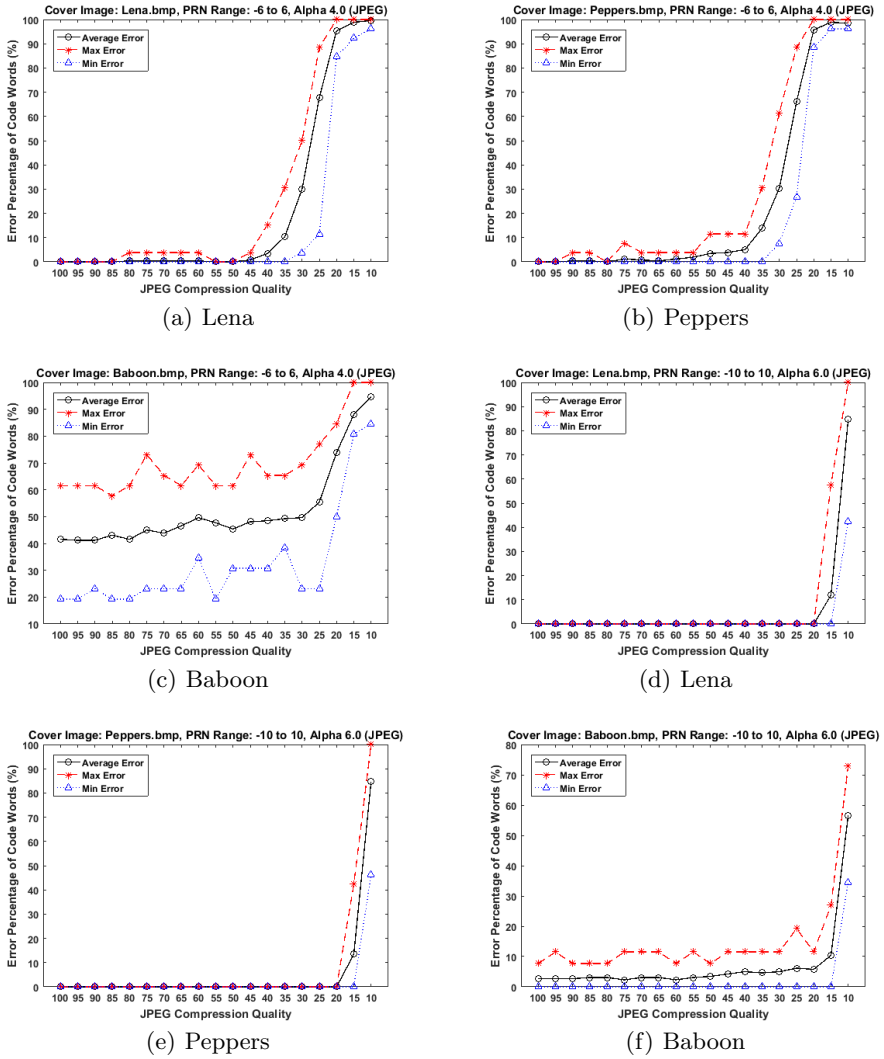


(b) Peppers



(c) Baboon

Fig. 7. Percentage of codeword errors based on various PRN ranges for the respective watermarked images.

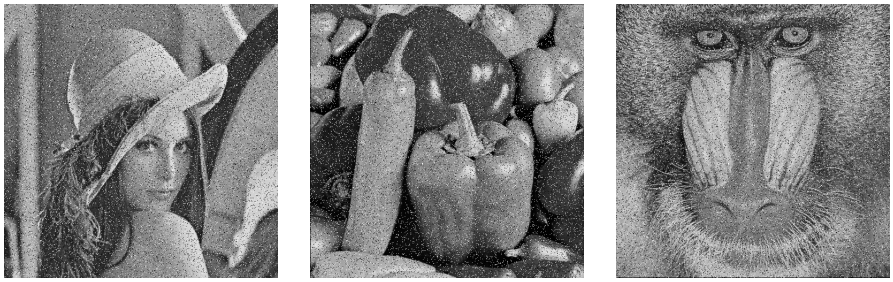


(a) Lena (b) Peppers

(c) Baboon (d) Lena

(e) Peppers (f) Baboon

Fig. 8. Robustness to JPEG compression for the respective watermarked images; (a) to (c) medium strength watermark; (d) to (f) high strength watermark.



(a) Lena (b) Peppers (c) Baboon

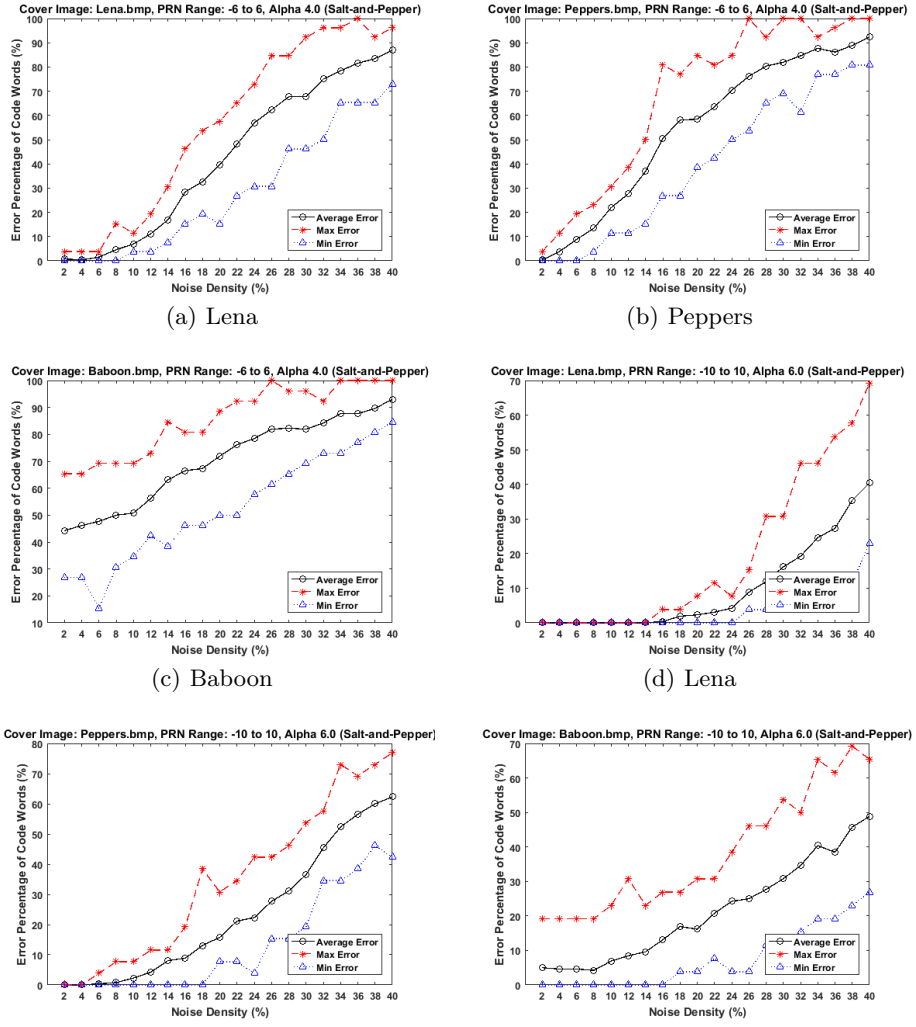
Fig. 9. Watermarked images containing 10% salt-and-pepper noise.

image in an attempt to corrupt the embedded watermark. For the experiments, the noise density represents the percentage of pixels that were altered by salt-and-pepper noise. Fig. 9(a) to Fig. 9(c) show examples of the test images which contain 10% salt-and-pepper noise. Fig. 10(a) to Fig. 10(c) present a depiction of the amount of error in the watermark as a result of varying the intensity of the salt-and-pepper noise in the respective test images. Fig. 10(d) to Fig. 10(f) in turn show the results when the strength of the watermark was increased in the test images.

As can be seen from the experiment results, the QR code can be successfully decoded when some salt-and-pepper noise is present. Obviously as the density of the noise in the watermarked image is increased, the watermark information is increasingly corrupted and cannot be decoded if too much noise is introduced. Nevertheless, this type of noise adversely affects the quality of the noisy image. In addition, the level of desired watermark robustness is related to the level of acceptable distortion in the watermarked image, as previously discussed, increasing the strength of the watermark signal also increases the amount of distortion in the resulting image.

Image Cropping. Another commonly used watermark attack is a cropping attack, in which the adversary attempts to remove a section of the pixels from a watermarked image with the intention of removing embedded watermark information. Examples of the respective test watermarked images that were used in the experiment are provided in Fig. 11(a) to Fig. 11(c). In these images, it can be seen that a central square area of the image has been cropped out. For the experiments, the size of the cropped area was varied.

Fig. 12(a) to Fig. 12(c) show the robustness of the watermark scheme against an increasing percentage of the image being cropped out, and Fig. 12(d) to Fig. 12(f) in turn show the results with increased watermark strength. It can be seen that the proposed scheme is robust against cropping below a certain threshold. In practice, cropping an image by too much will adversely affect the commercial viability of the resulting cropped image.



(a) Lena (b) Peppers

(c) Baboon (d) Lena

(e) Peppers (f) Baboon

Fig. 10. Robustness to salt-and-pepper noise for the respective watermarked images; (a) to (c) medium strength watermark; (d) to (f) high strength watermark.

(a) Lena (b) Peppers (c) Baboon

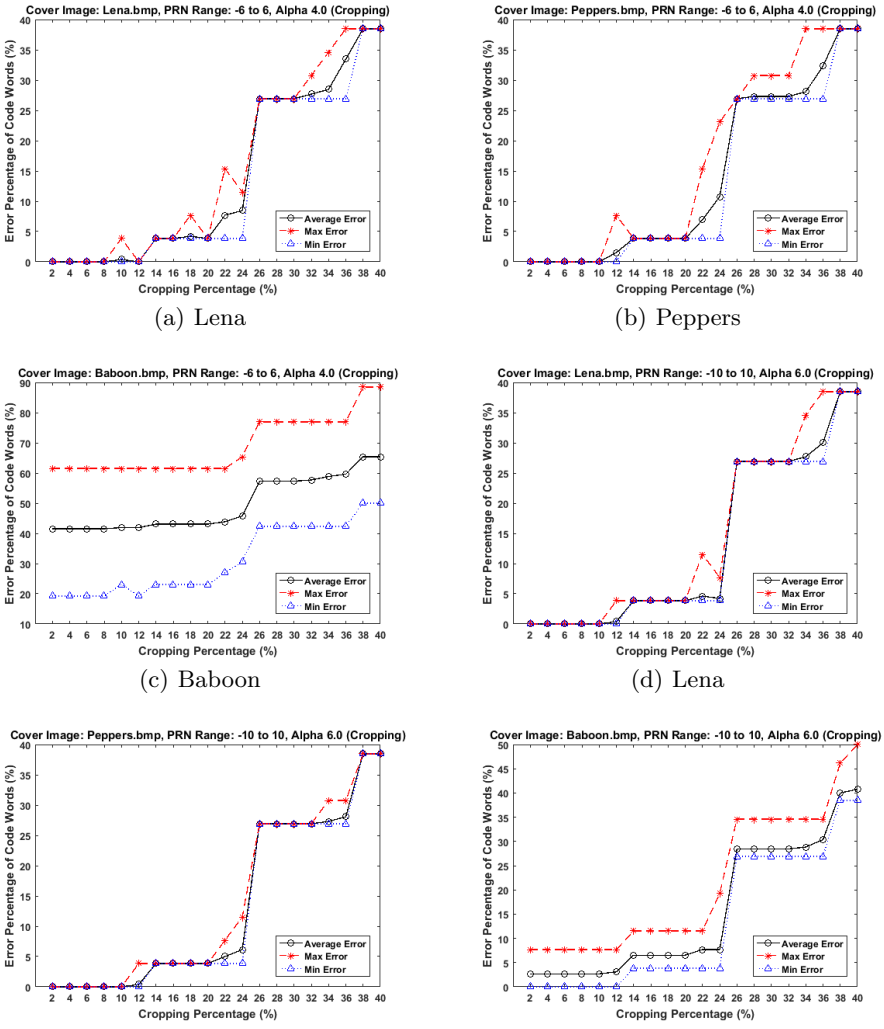
Fig. 11. Watermarked images with their central square area cropped out.

6 Conclusion and Future Work

This paper presents an approach to QR code watermarking for digital images. The proposed approach involves the use of a hybrid DWT-DCT technique in conjunction with the error correction mechanism this is inherent as part of the QR code structure. The aim of embedding QR code information within an image lies behind that fact that the QR code can be correctly decoded even if the watermarked image is distorted, as long as the QR code's error tolerance capacity has not been overwhelmed. The quality of the resulting watermarked image is examined and experiment results demonstrating the robustness and security characteristics of the proposed scheme are presented in this paper against a number of commonly used watermark attacks. Future work will focus on determining an acceptable level of distortion from the human visual perspective, the use of color images, and methods of using different types of two-dimensional barcodes in the proposed scheme.

References

1. A. Akter, Nur-E-Tajnina, and M. A. Ullah. Digital image watermarking based on dwt-dct: Evaluate for a new embedding algorithm. In *2014 International Conference on Informatics, Electronics Vision (ICIEV)*, pages 1–6, May 2014.
2. A. Al-Haj. Combined dwt-dct digital image watermarking. *Journal of Computer Science*, 3(9):740–746, 2007.
3. S. K. Amirgholipour and A. R. Naghsh-Nilchi. Robust digital image watermarking based on joint DWT-DCT. *JDCTA*, 3(2):42–54, 2009.
4. M. Barni, F. Bartolini, V. Cappellini, and A. Piva. A dct-domain system for robust image watermarking. *Signal Process.*, 66(3):357–372, May 1998.
5. W.-Y. Chen and J.-W. Wang. Nested image steganography scheme using qr-barcode technique. *Optical Engineering*, 48(5):057004–057004, 2009.
6. D. Cho. Study on method of new digital watermark generation using qr-code. In *2013 Eighth International Conference on Broadband and Wireless Computing, Communication and Applications, Compiegne, France, October 28-30, 2013*, pages 585–588. IEEE, 2013.



(a) Lena (b) Peppers

(c) Baboon (d) Lena

(e) Peppers (f) Baboon

Fig. 12. Robustness to cropping for the respective watermarked images; (a) to (c) medium strength watermark; (d) to (f) high strength watermark.

7. Y. Chow, W. Susilo, G. Yang, M. H. Au, and C. Wang. Authentication and transaction verification using QR codes with a mobile device. In G. Wang, I. Ray, J. M. A. Calero, and S. M. Thampi, editors, *Security, Privacy, and Anonymity in Computation, Communication, and Storage - 9th International Conference, SpaCCS 2016, Zhangjiajie, China, November 16-18, 2016, Proceedings*, volume 10066 of *Lecture Notes in Computer Science*, pages 437–451, 2016.
8. Y. Chow, W. Susilo, G. Yang, J. G. Phillips, I. Pranata, and A. M. Barmawi. Exploiting the error correction mechanism in QR codes for secret sharing. In J. K. Liu and R. Steinfeld, editors, *Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part I*, volume 9722 of *Lecture Notes in Computer Science*, pages 409–425. Springer, 2016.
9. C.-H. Chung, W.-Y. Chen, and C.-M. Tu. Image hidden technique using qr-barcode. In *Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09. Fifth International Conference on*, pages 522–525. IEEE, 2009.
10. I. Cox, M. L. Miller, and J. A. Bloom. *Digital Watermarking*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2002.
11. I. J. Cox and M. L. Miller. The first 50 years of electronic watermarking. *EURASIP Journal on Advances in Signal Processing*, 2002(2):820936, 2002.
12. K. Deb, M. S. Al-Seraj, M. M. Hoque, and M. I. H. Sarkar. Combined dwt-dct based digital image watermarking technique for copyright protection. In *2012 7th International Conference on Electrical and Computer Engineering*, pages 458–461, Dec 2012.
13. Denso Wave Incorporated. QRcode.com, http://www.qrcode.com/en/.
14. S. Emek and M. Pazarci. *Additive vs. Image Dependent DWT-DCT Based Watermarking*, pages 98–105. Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.
15. S. Falkner, P. Kieseberg, D. Simos, C. Traxler, and E. Weippl. E-voting authentication with qr-codes. In *Human Aspects of Information Security, Privacy, and Trust*, volume 8533 of *Lecture Notes in Computer Science*, pages 149–159. Springer, 2014.
16. Z.-H. Guan, F. Huang, and W. Guan. Chaos-based image encryption algorithm. *Physics Letters A*, 346(13):153 – 157, 2005.
17. F. Hartung and M. Kutter. Multimedia watermarking techniques. *Proceedings of the IEEE*, 87(7):1079–1107, Jul 1999.
18. H.-C. Huang, F.-C. Chang, and W.-C. Fang. Reversible data hiding with histogram-based difference expansion for qr code applications. *Consumer Electronics, IEEE Transactions on*, 57(2):779–787, 2011.
19. J. Huang, Y. Q. Shi, and Y. Shi. Embedding image watermarks in dc components. *IEEE Transactions on Circuits and Systems for Video Technology*, 10(6):974–979, Sep 2000.
20. International Organization for Standardization. Information technology — automatic identification and data capture techniques — qr code 2005 bar code symbology specification. ISO/IEC 18004:2006, 2006.
21. A. M. Joshi, S. Gupta, M. Girdhar, P. Agarwal, and R. Sarker. *Combined DWT–DCT-Based Video Watermarking Algorithm Using Arnold Transform Technique*, pages 455–463. Springer Singapore, Singapore, 2017.
22. Q. Kang, K. Li, and J. Yang. A digital watermarking approach based on dct domain combining qr code and chaotic theory. In *2014 Eleventh International Conference on Wireless and Optical Communications Networks (WOCN)*, pages 1–7, Sept 2014.

23. S. A. Kasmani and A. M. Sharifi. A pre-filtering method to improve watermark detection rate in DCT based watermarking. *Int. Arab J. Inf. Technol.*, 11(2):178–185, 2014.
24. J. Kim, N. Kim, D. Lee, S. Park, and S. Lee. Watermarking two dimensional data object identifier for authenticated distribution of digital multimedia contents. *Signal Processing: Image Communication*, 25(8):559 – 576, 2010.
25. C. C. Lai and C. C. Tsai. Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Transactions on Instrumentation and Measurement*, 59(11):3060–3063, Nov 2010.
26. R. H. Laskar, M. Choudhury, K. Chakraborty, and S. Chakraborty. *A Joint DWT-DCT Based Robust Digital Watermarking Algorithm for Ownership Verification of Digital Images*, pages 482–491. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.
27. H.-C. Lee, C.-R. Dong, and T.-M. Lin. Digital watermarking based on jnd model and qr code features. In *Advances in Intelligent Systems and Applications-Volume 2*, pages 141–148. Springer, 2013.
28. S. D. Lin and C.-F. Chen. A robust dct-based watermarking for copyright protection. In *2000 Digest of Technical Papers. International Conference on Consumer Electronics. Nineteenth in the Series (Cat. No.00CH37102)*, pages 10–11, June 2000.
29. C. Ling and O. Ur-Rehman. *Watermarking for Image Authentication*, pages 43–73. Springer International Publishing, Cham, 2015.
30. S. Mallat. A theory for multiresolution signal decomposition: The wavelet representation. *IEEE Trans. Pattern Anal. Mach. Intell.*, 11(7):674–693, 1989.
31. A. S. Panah, R. V. Schyndel, T. Sellis, and E. Bertino. On the properties of non-media digital watermarking: A review of state of the art techniques. *IEEE Access*, 4:2670–2704, 2016.
32. C. I. Podilchuk and E. J. Delp. Digital watermarking: algorithms and applications. *IEEE Signal Processing Magazine*, 18(4):33–46, Jul 2001.
33. K. R. Rao and P. Yip. *Discrete Cosine Transform: Algorithms, Advantages, Applications*. Academic Press Professional, Inc., San Diego, CA, USA, 1990.
34. P. P. Thulasidharan and M. S. Nair. {QR} code based blind digital image watermarking with attack detection code. {*AEU*} - *International Journal of Electronics and Communications*, 69(7):1074 – 1084, 2015.
35. X. Y. Wang and H. Zhao. A novel synchronization invariant audio watermarking scheme based on dwt and dct. *IEEE Transactions on Signal Processing*, 54(12):4835–4840, Dec 2006.
36. J. Weir and W. Yan. Authenticating visual cryptography shares using 2d barcodes. In *IWDW*, volume 7128 of *Lecture Notes in Computer Science*, pages 196–210. Springer, 2011.
37. W.-C. Wu, Z.-W. Lin, and W.-T. Wong. Application of qr-code steganography using data embedding technique. In *Information Technology Convergence*, pages 597–605. Springer, 2013.
38. W. Zhang and X. Meng. An improved digital watermarking technology based on qr code. In *2015 4th International Conference on Computer Science and Network Technology (ICCSNT)*, volume 01, pages 1004–1007, Dec 2015.