A DUAL-WATERMARKING WITH QR CODE AGAINST CROPPING AND RESIZING ATTACK

LAU WEI KHANG

A dissertation submitted in fulfillment of the requirement for the award of the Degree
Master's of Computer Science (Information Security)

Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia

January 2016

To my beloved parent and my family members

ACKNOWLEDGEMENT

First of all, my deepest gratitude is expressed to my supervisor, Dr. Kamaruddin Malik b. Mohamad for the support to my project, for his patience, motivation, enthusiasm, and immense knowledge. Dr. Kamaruddin Malik b. Mohamad gave a lot of useful comments and suggestions for me throughout the development of the study of watermarking techniques that are robust against cropping and resizing attack. I could not imagine having a better advisor and mentor for my project. Besides that, I would like to thank my family and friends for their encouragements and supports. Appreciation also goes to everyone involved directly or indirectly towards the compilation of this thesis. In addition, I would like to thank FSKTM and library of UTHM'library for providing me useful reference books, thesis and comfortable laboratory and discussion rooms to do my project. Thanks to all the lecturers who has given me a helping hand throughout the project. Last but not least, I would also like to take this opportunity to thank my friends and coursemates. They have accompanied me along the journey to finish this project. Without their help and support, the project might not be a success.

ABSTRACT

Watermarking is a pattern of bits inserted into a digital image, audio or video file (digital file) that identifies the file's ownership copyright information. It is one of the techniques to discourage illegal duplication of intellectual property. However, there is still a room for improvement for new techniques applied to digital files to withstand against cropping and resizing attack. In this Dual-watermarking with QR code project, both visible and invisible watermark are used. The proposed technique is compared with MOHANTY and HSU & WU techniques. First, visible QR code watermark is embedded into the image using LSB 7 (embed at the 7^{th} bit from the left of the binary number) technique. Then, the invisible QR Code watermark was embedded into image using LSB 1 (embed at the 1^{st} bit from the left of the binary number) technique. The proposed technique shows the watermark can be successfully extracted when image is enlarged up to 90 percent or shrank up to 90 percent (resizing attack). If enlarging and shrinking are combined to the same watermarked image, watermark can still be extracted and scanned. Final result for cropping attack shows that watermark can be successfully extracted when image is cropped up to 36 percent. If it is more than 36 percent, watermark is extractable but can not be scanned by QR Code scanner device. Besides that, PSNR result also shows that the proposed technique DWQR is 15 percent better than HSU & WU technique.

ABSTRAK

Watermarking merupakan salah satu corak yang memasukkan *bits* ke dalam satu imej digital, fail bunyi atau video yang dapat mengenal pasti maklumat tentang hak cipta pemilik. Ia merupakan salah satu teknik untuk mengelakkan pertindihan harta intelek daripada seseorang. Walau bagaimanapun, masih terdapat ruang untuk penambahbaikan bagi teknik-teknik baru untuk menahan serangan pengubahan saiz imej (*resizing attack*) dan serangan pangkas (*cropping attack*). Dalam projek *Dual-Watermarking with QR code* ini, *watermark* yang ketara (*visible watermark*) dan *watermark* yang tersembunyi (*invisible watermark*) telah digunakan. Teknik yang dicadangkan telah dibandingkan dengan teknik MOHANTY dan teknik HSU & WU. Pertama, *watermark* kod QR yang ketara ditanam ke dalam imej dengan menggunakan teknik *LSB 7* (tanam pada *bit* ketujuh dari kiri nombor binari). Kemudian, *watermark* kod QR yang tersembunyi ditanam juga ke dalam imej dengan menggunakan teknik *LSB 1* (tanam pada *bit* pertama dari kiri nombor binari). Hasil kajian menunjukkan bahawa teknik yang dicadangkan menunjukkan bahawa *watermark* berjaya dikeluarkan apabila imej dibesarkan sehingga sembilan puluh peratus atau disusut sehingga sembilan puluh peratus. Jika teknik membesar dan menyusut digabungkan pada imej yang sama, maka *watermark* masih boleh dikeluarkan dan diimbas. *Watermark* berjaya dikeluarkan apabila imej diserang dengan serangan pangkas sehingga tiga puluh enam peratus. Jika melebihi tiga puluh enam peratus, *watermark* masih boleh dikeluarkan tetapi kod QR tidak dapat diimbas oleh peranti imbasan. Selain itu, hasil PSNR menunjukkan teknik *Dual-Watermarking with QR code* lima belas peratus lebih baik daripada teknik HSU & WU.

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURES

LIST OF ABBREVIATIONS

BMP	Bitmap File Format
QR Code	Quick Response Code
FFT	Fast Fourier Transform
IPR	Intellectual Property Rights
MPEG	Motion Picture Experts Group
TV	Television
2-D	2 Dimension
MSB	Most Significant Bit
DFD	Data Flow Diagram
GUI	Graphical User Interface
JPEG	Joint Photographic Experts Group
JPG	Joint Photographic Experts Group
LSB	Least Significant Bit
PNG	Portable Network Graphics
RP	Rapid Prototyping
PHP	PHP Hypertext-Preprocessor
MATLAB	Matrix Laboratory software
TIFF	Tagged Image File Format
GIF	Graphics Interchange Format
DWQR	Dual-Watermarking with QR Code
OS	Operating System
UTHM	Universiti Tun Hussein Onn Malaysia
FSKTM	Faculty of Computer Science and Information Technology

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Digital watermark is a kind of information security and protection technology. It is typically used to identify ownership of copyright media (digital library, video broadcasting, and other multimedia services). Watermarking is mostly similar to steganography in a number of respects. The main idea of steganography is embedding hidden information into data under assumption that others cannot know the secret information in data. There are two types of watermarking, visible watermarking and invisible watermarking. For visible watermarking for images, a secondary image (the watermark) is embedded into a primary image such that watermark is intentionally perceptible to a human observer. Visible watermarking is an effective technique for preventing unauthorized use of an image, based on the insertion of a translucent mark, which provides immediate claim of ownership. Digital watermarking technology primarily joins the rightful owner of totem to the protected media. Once the media are suspect to be illegally used, an open algorithm can be used to extract the digital watermark, for showing the media's ownership but it is difficult to develop a visible watermarking algorithm that satisfies all types of attack and works effectively for all types of images [1]. Moreover, a visible watermark can always be tampered by certain softwares. To detect such kind of illegal use of image, an invisible watermark can be used as a backup. When a visible watermarked image is being questioned, the invisible watermark can provide appropriate ownership information in order to protect the ownership copyright.

Besides that, this project is looking into another useful technique that can be applied into digital watermarking. QR Code (Quick Response Code) is the trademark for a type of matrix barcode (two-dimensional code). QR Code was invent in Japan by the Toyota subsidiary Denso Wave in 1994 to track vehicles during manufacturing [2] due to its fast readability and large storage capacity compared to UPC barcode standard that consists of black modules arranged in a square pattern on a white background. The information encoded can made up of four standardized types of modes of data that are similar to numeric, alphanumeric, byte, binary, kanji, through supported extensions or virtually any kind of data [3]. Therefore, the QR Code has become the focus of advertising strategy, since it provides quick and effortless access to the brand's website.

In this project, a proposed technique is dual-watermarking algorithm which is use of QR Code embed into image with both visible and invisible watermarking technique.

1.2 Problem Statement

Although several researches have been done on digital watermarking using difference scheme, there are still several issues to be addressed. In digital watermarking many researchers only focus on certain attack that applies to watermarked image. Beside, most of researchers try to increase the watermark capacity by compromising image quality in order to tradeoff among data rate, security and imperceptibility of watermarked image.

For a watermark to be useful it must be robust against any possible attack and image processing by those who seek to corsair the material, researchers have considered various approaches like JPEG compression, geometric distortions, resizing, salt and pepper and many more attack to the digital watermark. Most of works from previous studies against only certain attack but not multiple attacks that would apply to watermarked image. The most common attack that always happed to smartphone user are cropping attack and resizing attack. By using smartphone application, smartphone user can easily download image from internet source and crop or resize the image without knowing the image was protected by digital

watermark. Once the image attacked by cropping attack, the digital watermark are damaged and not retrivedable anymore. This happed to resizing attack too. Both shrink and enlarge attack to an image will course pixel of image change or damage. It will make digital watermark unable to be retrived.

1.3 Project Aim

Through this project, the aim is to work on the watermarking and to devise some robust means to make the watermark withstand the attack from resizing and cropping.

1.4 Objectives

The objectives of this project is to ensure that the proposed version of dual-watermarking strengthen to make it more reliable than the previous versions. A watermark cannot defend against all form of attack but with improved watermarking algorithm, a watermarking algorithm can defend against multiple attacks. On the other hand, the current watermarking algorithm could not always be useful to prevent evolving forms of attack. Hence, an improved algorithm is needed to protect the intellectual property. The proposed algorithm is to overcome the problem stated above. The followings are the objectives of this project:

- To propose a Dual-watermarking technique to withstand against cropping and resizing attacks using QR Code.
- To develop the proposed algorithm.
- To test the strength of the proposed algorithm against resizing and cropping attacks.

1.5 Scope

In this project, experimentation and testing against cropping and resizing attacks will be using JPEG and TIFF image only.

1.6 Contribution

This project contributes to the image protection by solving the following issues. Firstly, this project is expect to come up with a combination of dual-watermarking technique that is more secure as compare to a single watermarking technique. Both visible and invisible watermark will be embedding into a cover image in order to against cropping attack and resizing attack. Secondly, the proposed visible watermark used QR Code as watermark image, QR Code can store information and QR Code has up to 30% of error correcting function. It will be harder to be deleted or tampered. Lastly, this project will provide an alternative option for the researchers to choose between the available versions of watermark algorithm for their image protection. The followings are the outline of the contributions.

- Increase protection of image by combining two watermarking techniques (visible watermark and invisible watermark) to a more reliable one.
- Visible watermark give smartphone user a hint that image is under protected by digital watermark.
- Give researchers another option to explore more techniques and could use this algorithm to integrate with other techniques for a more robust watermark.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

In this part of the project, all related items are described in details to prove and to disclose how the previous development were achieved and how to proceed and develop a much better system.

2.2 Digital Watermarking

Digital watermarking is a technique which allows an individual or an organization to add hidden copyright notices or verification messages to media element such as audio, video, image or documents. The term digital watermarking was introduced by Andrew Tirkel and Charles Osborne [5]. This term was originally from Japanese word *denshi sukashi* which means an “electronic watermark”. Digital watermark is similar to steganography. Both are used to hide information into a media element [6]. Functionally, the term digital watermark is used to describe the differences between copies of the "same" content in undetectable manner. Many watermarking system hide the data so that erasure attempt will resulted in degradation of the quality of the content.

The difference between watermarking and steganography is watermark data are hidden in the message without the end user's knowledge, although some watermarking techniques have the steganographic feature of not being perceivable by the human eyes. Watermarking techniques tend to divide into two categories, text and image, according to the type of document to be watermarked [7]. For image watermarking, several different methods enable watermarking to be used in spatial domain. The simplest technique is to flip the lowest-order bit of chosen pixels in a grayscale or colour image. This will only work well if the image does not have any human or noise modification. Spatial domain watermarking is illustrated in Figures 2.1 and 2.2 that demonstrate how the degree of visibility of the watermark depending on its intensity and the nature of the background.

Figure 2.1: Fifty percent visibility of watermark

Figure 2.2: Hundred percent visibility of watermark

Figure 2.1 and 2.2 are two identical watermarked images but different in term of the intensity of the image. Considerable latitude is available, in terms of placement, size and intensity to blend the watermark into a graphic. A robust watermark can be embedded into an image in the same way that a watermark is added to paper. Such techniques may superimpose a watermark symbol over an area of the picture and

then add some fixed intensity value for the watermark to the varied pixel values of the image. The outcome of watermark may be visible or invisible depending on the value of the watermark intensity. Nevertheless, this watermark is highly exposed to cropping attack, as a part of the image without watermark can be cropped and may be used without permission. Spatial watermarking can also be applied using colour separation [8]. In this way, the watermark appears in only one of the colour bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. However, the watermark appears immediately when the colours are separated for printing or xerography. This renders the document useless to the printer unless the watermark can be removed from the colour band. This approach is used commercially by journalists to inspect digital pictures from a photo-Stackhouse before buying un-watermarked versions. Watermarking can be applied in the frequency domain and other transform domains by first applying a transform like the Fast Fourier Transform (FFT) [9]. In a similar manner to spatial domain watermarking, the values of chosen frequencies can be altered from the original. Since high frequencies will lost by compression or scaling, the watermark signal is apply to lower frequencies, or better yet, applied adaptively to frequencies that contain important information of the original picture (feature-based schemes). Since watermarks apply to the frequency domain will be dispersed over the entirety of the spatial image upon inverse transformation, this technique is not as susceptible to defeat by cropping as the spatial technique. However, there is more of a tradeoff here between invisibility and decodability, since the watermark is affected indiscriminately across the spatial image.

The main idea of a digital watermark is a digital signal or pattern combined with a digital image. Since this signal or pattern is presented in each copy of non-editable original image, the digital watermarking may also characterize as digital signature that represent the owner. There have two types of digital watermarks techniques that common used nowadays, visible watermark and invisible watermark. Visible watermark are used in the same way as their ancestors, which is by adding an extra digital “stamp” into digital image. Visible watermarks are extension of the logos concepts [10]. Such watermarks are applicable to images only. Logos inserted into the image are transparent. Such watermarks cannot be removed by cropping the centre part of the image. In addition, such watermarks are protected against attacks such as statistical analysis. But as mentioned before, it is difficult to develop a

watermarking algorithm that can prevent from all kinds of attack. Cropping attack, that deal with certain small parts of image does not protect the image from being used without permission. However, the drawbacks of visible watermarks are degrading the quality of image and detection by visual means only. Thus, it is not possible to detect them by dedicated programs or devices. Such watermarks have applications in maps, graphics and software user interface.

Invisible watermarks are potentially useful as means of identifying the source, author, creator, owner, and distributor or authorized consumer of a document or image [11]. It can be detected by authorized agency only. For this purpose, the objective to add a watermark into an image is to permanently and unalterably marked the image so that the credit or assignment is beyond being questioned. If the digital image is being detected as illegally used, the watermark would facilitate the claim of ownership, receipt of copyright payment, or the success of prosecution [12].

Other than visible and invisible watermark techniques, there are other watermark techniques for copyright protection such as public watermark, fragile watermark, private watermark, perceptual watermark, bit-stream watermark and text document watermark. Public watermark can be read or retrieved by anyone using specialized algorithm. In this sense, public watermarks are not secured. However, public watermarks are useful for carrying *intellectual property rights* (IPR) information. They are good alternatives to labels. Fragile watermarks are also known as tamper-proof watermarks. Such watermarks are destroyed by data manipulation. Private watermarks are also known as secure watermarks. To read or retrieve such watermark, it is necessary to have the secret key. A perceptual watermark exploits the aspects of human sensory system to provide invisible yet robust watermark. Such watermarks are also known as transparent watermarks that provide extremely high quality contents. The term of bit-stream watermark is sometimes use for watermarking compressed data such as video. Lastly, text document watermarking are hidden watermark information in semantics and hidden watermark in text format. The hierarchy of watermarks is shown in Figure 2.3 [13].

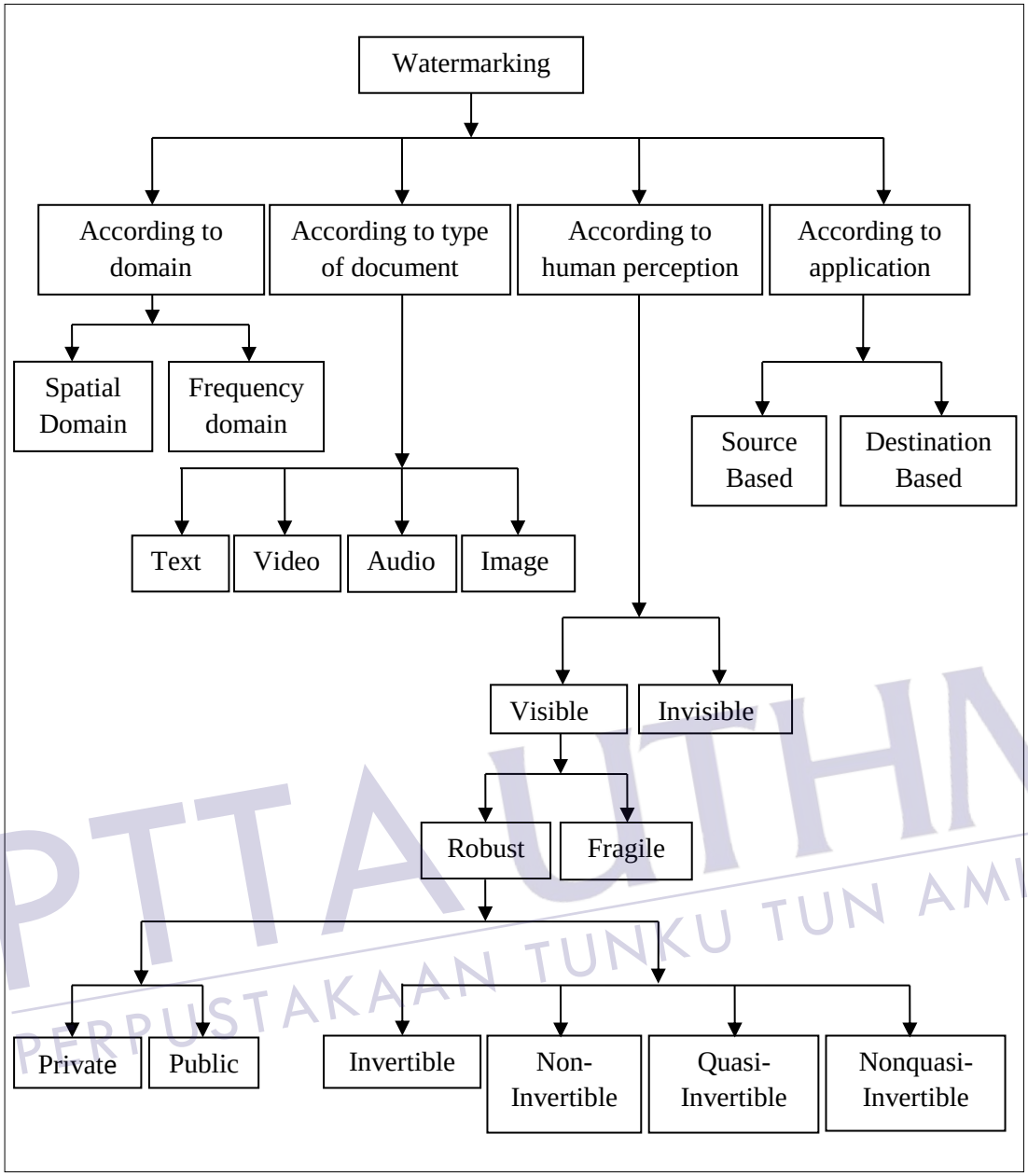

Figure 2.3: Classification of watermarks [13]

Digital watermarking software looks for noise in digital media and replaces it with useful information or owner details. A digital media file is nothing more than a large list of 0's and 1's. The watermarking software determines which of these 0's and 1's correspond to too many or irrelevant details. For example, the software might identify details in an image that is too small for the human eyes to see and flag the corresponding 0's and 1's as irrelevant noise. Then the flagged 0's and 1's can be replaced by a digital watermark. Watermarking process is shown in Figure 2.4 and 2.5.

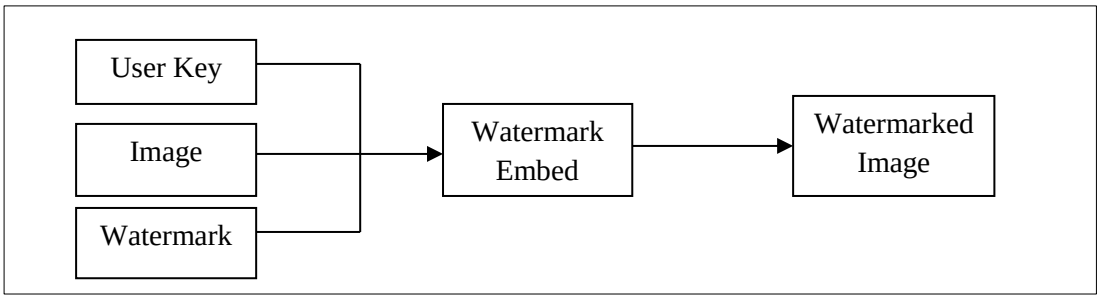

Figure 2.4: Watermark embed spatial domain watermarking

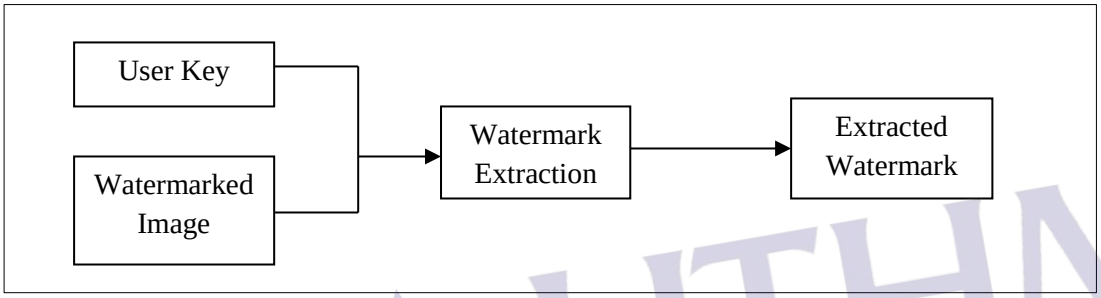

Figure 2.5: Watermark Eextraction spatial domain watermarking

Figure 2.4 and 2.5 demonstrate a typical spatial domain watermark embedding and extraction process applied to a static image. It is notable that a slight degradation of the original image occurs when the watermark is embedded. However, the retrieved watermark is very close to the original watermark, which can help resolve ownership issues.

2.2.1 Visible Watermark

Visible watermark are an extension of the concept of logos. Such watermarks are applicable to images only. These logos are inlaid into the image but they are transparent. Such watermarks cannot be removed by cropping the centre part of the image. Moreover, such watermarks are protected against attacks such as statistical analysis.

2.2.2 Invisible Watermark

A code hides secretly in a cover image and carry copyright information or other secret messages. An invisible watermark consists of a very slight change of contrast over large areas of the picture, invisible to the human eyes, even fainter than the watermark on a piece of paper. Suitable software can recover the invisible watermark even if the image has been printed out, photographed, and scanned.

2.2.3 Public Watermark

Such a watermark can be read or retrieved by anyone using specialized algorithm. In this sense, public watermarks are not secured. However, public watermarks are useful for carrying *Intellectual Property Rights* (IPR) information. Public watermark are good alternatives to labels.

2.2.4 Fragile Watermark

Fragile watermarks are also known as tamper-proof watermarks. Such watermarks will be destroyed if data are manipulated. Fragile watermark is similar to invisible watermark, it can only be extracted by suitable program and if the image which embeds with fragile image be manipulated or edited, then the fragile watermark will appear to be different when it is extracted and compared to the original watermark.

REFERENCES

[1] Yeung, M.M. (1997). *Digital Watermarking for High-Quality Imaging, Proc. IEEE First Workshop on Multimedia Signal Processing, New Jersey,* pp. 357-362.

[2] Borko, F. (2011). *Handbook Of Augmented Reality, Springer,* pp.341-349.

[3] Denso-Wave. (2011). *QR Code Features*, Retrieved from : http://www.qrcode.com/en/

[4] Scott, M.C. (2000). *Hiding Information in Images: An Overview of Watermarking, Cryptography Research Paper.* Retrieved from : http://www.cim.mcgill.ca/~scott/RIT/CryptoPaper.html

[5] Tirkel, A.Z., Rankin, G.A., Schyndel, R.M.V., Ho, W.J., Mee, N.R.A. and Osborne, C.F. (1992). *Electronic Water Mark. DICTA 93, Macquarie University,* pp.666-673.

[6] Gao, X.B., Yuan, Y., Cheng, D. and Li, X.L. (2011). *Lossless data embedding using generalized statistical quantity histogram, IEEE Transaction on circuits and systems for video technology,* vol. 21, No. 8, pp. 1061-1070.

[7] Vidyasagar, M.P., Song, H. and Elizabeth, C. (2005). *A Survey of Digital Image Watermarking Techniques, 3rd IEEE International Conference on Industrial Informatics (INDIN),* pp.709-713.

[8] Masoud, N., Ronak, K. and Hojat, A.H. (2012). *Short Communication on Digital Watermarking in Images. Shaneh Branch Islamic Azad University. Vol (2), No (4),* pp.220-223.

[9] Pranab, K.D. and Kim, J.M. (2011). *Digital Watermarking Scheme Based on Fast Fourier Transformation for Audio Copyright Protection International Journal of Security and Its Applications,* Vol. 5 No.2 , pp.33-48.

[10] Petitcolas, F.A.P., Anderson, R.J. and Kuhn, M.G. (1999). *Proceedings of the IEEE,* Volume 87, Issue 7, pp.1062-1078.

[11] Jaspreat, K. and Karmjeet, K. (2012). *Digital Watermark : A Study. International Journal of Advanced Research in Computer Science and Software Engineering*. Volume 2, Issue 8

[12] Ruanaidh, Boland, F. and Dautzenberg, C. (1995). *Watermarking Digital Images for Copyright Protection, Proc. IEE Conf. Image Processing and It's Applications*, pp.87-94.

[13] Vanwasi, A.K. (2011). *Digital Watermarking-Steering the future of security*. Retrieved from: http://www.networkmagazineindia.com/200108/security1.html

[14] Yue, L., Yang, J. and Ming, J.L. (2008,). *Recognition of QR Code with mobile phones, Control and Decision Conference Chinese*, pp. 203-206.

[15] Denso-Wave. (2012). "*Version and Maximum Capacity Table*". Retrieved from: http://www.qrcode.com/en/about/version.html

[16] Denso ADC. (2011). " *QR Code Essentials*."
Retrieved from: http://www.nacs.org/LinkClick.aspx?fileticket=D1FpVAvvJuo%3D&tabid=146&mid=4802

[17] Phaisarn, S. and Wichian, P. (2010). *QR Code Generator Eighth International Conference on ICT and Knowledge Engineering. Thailand*, pp. 90-101.

[18] Murray, James, D., Van, R. and William. (1996). *Encyclopedia of Graphics File Formats (Second ed.,* pp. 1152-1169.

[19] Pachghare, V.K. (2005). *Comprehensive Computer Graphics: Including C++. Laxmi Publications*, pp. 93-97.

[20] MOHANTY, S.P. (1999). *A Dual-watermarking Technique for Images*, *Proc. 7th ACM International Multimedia Conference, ACM-MM'99, Orlando, USA*, pp. 49-51.

[21] Hsu, F.H. and Wu, M.H. (2012). *Dual-watermarking by QR Code Applications in Image Processing, 9th International Conference on Ubiquitous Intelligence and Computing*, pp. 638-643.

[22] Gersho, A. and Gray, R.M. (1993). *Vector Quantization and Signal Compression. Boston, MA: Kluwer*, pp. 159-165.

[23] Chen, T.S. (1998). *A virtual image cryptosystem based upon vector quantization*. *IEEE Trans. Image Process,* 7(10), pp. 1485-1488.