ROBUST DISCRETE COSINE TRANSFORM BASED TECHNIQUE FOR IMAGE WATERMARKING AGAINST CROPPING ATTACKS

MOHAMMAD JAVAD RAJABI

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy

Advanced Informatics School
Universiti Teknologi Malaysia

December 2018

DEDICATION

To my lovely mother, who gave me endless love, trust, constant encouragement over the years, and for her prayers.

To my Family, for their patience, support, love, and for enduring the ups and downs during the completion of this thesis.

This thesis is dedicated to them.

ACKNOWLEDGEMENT

This thesis would not have been completed without the valuable assistance of so many dear persons around me. I am profoundly grateful for all those who encouraged me to embark on this enlightening journey and to complete it, both at a professional and at a personal level.

I express my deep gratitude to my supervisor, Associate Professor Dr Mohd Shahidan Bin Abdullah, whose inspiration, critique, and direction brought out the best in me. His continuous search for the highest quality challenged me always and taught me never to compromise quality, even in the very smallest details. It is only in this way that we can be truly proud of our achievements.

The work would not have been achieved without the encouragement and support of my parents, whose eagerness to see me reach the Phd level gave me the strength and perseverance to complete this long journey. I am profoundly indebted to my family: my father, and my mother whose love fuelled my energy throughout this period.

My thanks also go to Dr Majid Bakhtiari whose believe in my capabilities and their continuous support and encouragement to proceed with my work at times of desperation provided an exemplary model of partnership and mutuality.

ABSTRACT

Watermarking is a common technique for authentication and message hiding. Watermarking should be invisible and robust to common processing and attack. So far, current research has succeeded in maintaining the high normalized correlation (NC) quality of watermark only up to 25 percent cropping level. The purpose of this research is to enhance the current quality of NC and maintain the robustness of watermark in higher cropping level. This research was divided into four phases. First, this project analyzed different frequency domain watermarking techniques against cropping attacks. Second, a discrete cosine transform (DCT) based technique for image watermarking against cropping attacks was synthesized from the literature. The proposed watermarking technique hides watermark image as logo into a host image. The host image was first divided into 8x8 blocks, and then DCT transformation was applied on each block. Next, Arnold's cat map was applied on watermark image and embedded into the host image using zigzag symmetric technique introduced in this research. In the third phase, the design of improved watermarking technique was tested and evaluated against cropping attack. Experiment results showed that the proposed algorithm was undetectable and robust against 50% cropping attack. Several kinds of cropping attacks on the watermarked image were implemented, which included top half cropping, right half cropping, bottom half cropping, and left half cropping. The watermark from attacked watermarked image was then extracted and compared to the original watermark logo using NC. Even though the watermarked image was impaired, the watermark remained almost intact with high quality of NC. The compression of the proposed method showed a decrease in size of the image compare with JPEG compression. The results of NC for extracted watermark from five standard watermarked Lena, Peppers, Baboon, Goldhill and Barbara images within acceptable value of NC, that was above 0.99 after 50% of cropping attack. In addition, compression comparison between the proposed method and other watermarking techniques based on the Lena image as the host image showed the results surpassed 5% to 25% of the current results in the literature. Therefore, this research has improved the robustness of image watermarking against cropping and compression attacks.

ABSTRAK

Watermarking adalah teknik yang biasa untuk pengesahan dan menyembunyikan mesej. *Watermarking* seharusnya tidak kelihatan dan kukuh untuk pemprosesan dan serangan biasa. Setakat ini, penyelidikan berjaya mengekalkan kualiti korelasi *Normalized* (NC) *Watermark* sehingga 25 peratus. Tujuan kajian ini adalah untuk meningkatkan mutu semasa NC dan mengekalkan ketahanan *watermark* dalam tahap pemotongan yang lebih tinggi. Kajian ini dibahagikan kepada empat fasa. Pertama, projek ini menganalisis teknik *watermarking* domain frekuensi yang berbeza terhadap serangan pemotongan. Kedua, teknik berasaskan *discrete cosine transform* (DCT) yang mantap untuk *watermarking* imej terhadap serangan pemotongan dilaksanakan. Teknik *watermark* yang dicadangkan menyembunyikan imej *watermark* sebagai *logo* ke dalam imej tuan rumah. Imej hos pertama kali dibahagikan kepada blok 8x8 dan kemudian transformasi *DCT* diterapkan pada setiap blok. Seterusnya, peta kucing *Arnold* telah digunakan pada imej *watermark* dan dimasukkan ke dalam imej tuan rumah menggunakan teknik simetri *zigzag* yang diperkenalkan dalam kajian ini. Dalam Fasa ketiga, reka bentuk teknik *watermarking* yang lebih baik telah diuji dan dinilai terhadap serangan tanaman. Hasil eksperimen menunjukkan bahawa algoritma yang dicadangkan tidak dapat dilihat dan teguh sebanyak 50% terhadap serangan pemotongan. Beberapa jenis serangan penangkapan pada imej *watermark* telah dilaksanakan, termasuk pemotongan separuh bahagian atas, potongan separuh bahagian kanan, potongan separuh bahagian bawah dan potongan separuh bahagian kiri. *Watermark* dari imej *watermarked* yang diserang kemudian diekstrak dan dibandingkan dengan *logo watermark* asal menggunakan NC. Walaupun imej *watermarked* terjejas, *watermark* masih mengekalkan kualiti tinggi NC. Kaedah mampatan yang dicadangkan, menunjukkan penurunan saiz imej berbanding dengan pemampatan JPEG. Hasil NC untuk *watermark* yang diekstrak dari lima imej *watermarked Lena*, *Peppers*, *Baboon*, *Gooldhill* dan *Barbara* dalam nilai NC yang dapat diterima berada di atas 0.99 selepas 50% serangan pemotongan. Di samping itu, perbandingan mampatan antara kaedah yang dicadangkan dan teknik *watermarking* lain berdasarkan imej *Lena* sebagai imej tuan rumah menunjukkan hasil telah melepasi 5% to 25% dari hasil semasa dalam kajian lepas. Oleh itu, kajian ini telah meningkatkan kekukuhan imej *watermark* terhadap serangan dan pengurangan serangan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

DCT	-	Discrete Cosine Transform
DWT	-	Discrete Wavelet Transform
DFT	-	Discrete Fourier Transform
IT	-	Information Technology
LSB	-	Significant Bit
ACF	-	Least Auto Correlation Function
ML	-	Maximum Likelihood
MAP	-	Maximum a Posteriori Probability
MMSE	-	Minimum Mean Square Error
NVF	-	Noise Visibility Function
SVD	-	Singular Values Decomposition
TAF	-	Tamper Assessment Function
NC	-	Normalized Correlation
PSNR	-	Peak Signal to Noise Ratio

LIST OF APPENDIXS

CHAPTER 1

INTRODUCTION

1.1 Overview

As computer hardware and software are developing, the internet is becoming the most common channel for transferring several types of digital media. Due to the open environment of internet, it has become very important to protect the digital data especially images. Therefore, it became a very important topic of research recently (Ali *et al.*, 2014).

To accomplish a copyright protection, digital watermarking has been used to protect the images. It is the process of embedding significant data (watermark) into an image such that the embedded watermark can be detected or extracted later to make an assertion about the image (Agrawal and Prajapati, 2017).

Overall, a watermarking technique contains three parts which are; the watermark, the watermark embedding stage and the watermark verification stage. The watermark embedding algorithm fits the watermark into the host image, where the verification algorithm pulls out and verifies the watermark determining the ownership of the image. Regularly, the watermark is a visually identifiable logo or a set of meaningless character strings that shows the copyright of the owner or legal users. If a watermark can be pulled out from an image in the verification stage, it possibly will prove the copyright of the owner (Shih, 2017).

For instance, digital watermarking is a technique in which the second data is embedded directly into digital data such as image, video, or audio signals, it is also called host data or original data, to make watermarked data. Compared to watermarks in paper documents, digital watermark has more limitations. The embedded data must still be decoded from the watermarked data, even if the watermarked data is processed, copied, or re-distributed. Potential applications of digital watermarking include copyright protection, distribution tracing, authentication and conditional-access control. Thus, the information could be for example a user-ID, a serial number for a certain copy of a document, or authentication information (Nematollahi *et al.*, 2017a).

1.2 Background of the Problem

With the development of internet and information digitalizing, digital media is drastically predominated over the traditional analog media. Nevertheless, as one of the related side-effects, it is becoming simpler for some groups and individuals to copy and transmit of digital products without gaining permission from the owner. To solve this problem, digital watermark is being introduced (Nematollahi *et al.*, 2017b).

Watermarking is able to show the ownership or track copyright intrusion, into the digital image, video or audio. Watermarking should be invisible and robust to common processing and attack. Digital watermarking technologies are categorized into two divisions; spatial domain and transform domain watermark. Spatial domain technique is easy to implement and is developed earlier but its disadvantage is that it is limited in robustness. Transform domain technique embeds watermark in host's transform domain. It is more complex and robust (Mahsa Boreiry, 2017).

Spatial techniques are generally abandoned because of their weakness in robustness, and frequency algorithm based on Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) becomes the research focus (Guo *et al.*, 2015).

An important aspect of any watermarking technique is its robustness against attacks. The notion of robustness is intuitively clear: A watermark is robust if it cannot be impaired without even rendering the attacked data useless (Shih, 2017).

There are still many attacks which can affect the watermark. The problem arises when attacks can affect image watermarking. The watermark should be able to resist attacks, even if these attacks are deliberately made. These attacks are reasons that robustness in watermarking techniques need to improve (Ali *et al.*, 2014)

In watermarking terminology, an attack is any processing that may impair detection of the watermark or communication of the information conveyed by the watermark. The processed, watermarked data is then called attacked data. An important aspect of any watermarking technique is its robustness against attacks. The aim of digital watermark is to provide copyright protection to digital products, and prevent and track illegal copying and transmission (Fazli and Moeini, 2016).

Cropping attacks aim at the complete removal of the watermark information from the watermarked data without cracking the security of the watermarking algorithm, e.g., without the key used for watermark embedding. That is, no processing, even prohibitively complex, can recover the watermark information from the attacked data. This category includes cropping, denoising, quantization (e.g., for compression), remodulation, and collision attacks. Not all of these methods always come close to their goal of complete watermark removal, but they may nevertheless damage the watermark information significantly (Azeem *et al.*, 2016).

Sophisticated removal attacks try to optimize operations like denoising or quantization to impair the embedded watermark as much as possible while keeping the quality of the attacked document high enough. Usually, statistical models for the watermark and the original data are exploited within the optimization process. Collision attacks are applicable when many copies of a given data set, each signed with a key or different watermark, can be obtained by an attacker or a group of attackers. In such a case, a successful attack can be achieved by averaging all copies or taking only small parts from each different copy (Das *et al.*, 2014).

1.3 Problem Statement

One of the most famous attacks in watermarking is cropping attacks. Cropping attack aims to make the watermark undetectable. This process may result in the complete removal of the watermark and recovering the original host data. This kind of attack by cropping a part of watermarked image makes the watermark undetectable. All of the digital watermarking need to be robust against cropping attacks (Zong *et al.*, 2016).

As mentioned by articles Halima *et al.* (2015), Abraham and Paul (2016), Pokudom and Rangsanseri (2013), Heidari *et al.* (2016), Moosazadeh and Ekbatanifard (2016), Wei and Zhaodan (2016) and Yuliani and Rosiyadi (2015) watermark image was successfully extracted from the watermarked image with maximum 25 percent cropping attacks with high normalized correlation (NC) quality of watermark. This means if cropping is more than 25 percent image owner cannot extract the watermark image with acceptable normalized correlation. Because of mentioned weakness in recent articles this research tries to improve robustness of digital watermarking against cropping attacks in higher cropping level maintaining the high quality of NC.

1.4 Research Questions

The research questions are as follow:

i. What is the best current image watermarking techniques against cropping attacks?
ii. How to implement a DCT image watermarking technique to improve the robustness against cropping attacks?
iii. How to evaluate the robustness of the proposed technique?

1.5 Research Objectives

The main purpose of the research is to improve the robustness of a DCT based technology image watermarking. The other objectives of the research are presented below:

i. To analyze current image watermarking techniques against cropping attacks.
ii. To propose an improved DCT image watermarking technique against cropping attacks.
iii. To evaluate the proposed robust DCT technique.

1.6 Project Aim

As discussed earlier, there are not enough studies conducted to investigate the attacks on DCT based image watermarking. This research aims to investigate the attacks on DCT based image watermarking and most importantly the research will determine techniques to increase the robustness of DCT technology to make it more resistant to the attacks and aim to propose and implement a DCT image watermarking technique to improve the robustness against cropping attacks.

1.7 Scope of Research

i. Five images have been selected from standard images used in image processing application to analysis the proposed technique. All images are assigned to the standard size row and column 512x512 (257 KB) in grey scale format with bmp extension.
ii. There are two kinds of watermarking technologies, spatial domain technologies and frequency domain technologies. Frequency domain watermarking technique will be used in this research. Frequency

image transformations include the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and others that in this research will be used Discrete Cosine Transform (DCT).

1.8 Significance of Research

The findings and results of the research are expected to serve users of image watermarking specially DCT based technology to increase their robustness as well as the ways to enhance the technology they use. Moreover, the result of the research will contribute to the body of knowledge in watermarking science.

1.9 Thesis Outline

In first chapter, introduction to the subject matter, problems, importance and the research objectives are indicated. In chapter two the concept of digital watermarking, its different classifications and attacks on digital watermarking have been discussed. Review of the literature related to DCT image watermarking, DCT compression, attacks, Arnold Cat map. Recent articles published in related fields are reviewed for comparison purpose. The chapter three presents the research methodology applied in this technique; first by explaining the research design and operational framework involved in initial planning, review, designing and implementation, testing, and report, followed by research approach, instrumentation, and data analysis, and finally data sources. The importance of chapter four is hard to gauge as this chapter can depict the technique and methodology have been used in this research. This research based on two sections of embedding and extracting processes. In chapter five, the proposed technique is examined on five standard images (Lena, Baboon, Peppers, Goldhill, Barbara) which are cropped to top, down, left and right sides. Then all cropped images compared with themselves and with other different images. Next, compressed proposed method analyzed with JPEG compression which leads to improvement in smaller size of image and higher

percentage of compression in contrast with JPEG. At the end of this chapter, results of proposed technique on image cropping attack have been compared with other recent researches in this field. Results demonstrate that the NC of proposed technique is remarkably higher than other methods updated by today. In last chapter, research conclusion and recommendations for further research are provided.

REFERENCES

Abdullatif, M., Zeki, A. M., Chebil, J., and Gunawan, T. S. (2013). Properties of digital image watermarking. *Signal Processing and its Applications (CSPA),* 2013 IEEE 9th International Colloquium on, 235-240.

Abraham, J., and Paul, V. (2016). An imperceptible spatial domain color image watermarking scheme. *Journal of King Saud University-Computer and Information Sciences*.

Aggarwal, A., and Singla, M. (2011). Robust Watermarking of Color Images under Noise and Cropping Attacks in Spatial Domain. *image, 6*(9), 11.

Agrawal, A., and Prajapati, A. (2017). A Review of Digital Watermarking Technique for The Copyright Protection of Digital Data using Transform Function.

Agrwal, S. L., Yadav, A., Kumar, U., and Gupta, S. K. (2016). Improved invisible watermarking technique using IWT-DCT. *Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO),* 2016 5th International Conference on, 283-285.

Al-Gindy, A., and Ghunaim, S. (2015). Attackmark: A Tool for Generating Attacks on Watermarking Algorithms. *Developments of E-Systems Engineering (DeSE),* 2015 International Conference on, 115-119.

AL-Shaaby, A. A., and AlKharobi, T. (2017). Cryptography and Steganography: New Approach. *Transactions on Networks and Communications, 5*(6), 25.

Al-Vahed, A., and Sahhavi, H. (2011). An overview of modern cryptography. *World Applied Programming, 1*(1), 3-8.

Ali, M., Ahn, C. W., and Pant, M. (2014). A robust image watermarking technique using SVD and differential evolution in DCT domain. *Optik-International Journal for Light and Electron Optics, 125*(1), 428-434.

Azeem, N., Ahmad, I., Jan, S. R., Tahir, M., Ullah, F., and Khan, F. (2016). A New Robust Video Watermarking Technique Using H. 264/AAC Codec Luma Components Based On DCT. *International Journal of Advance Research and Innovative Ideas in Education, Online ISSN-2395-4396*.

Azez, A. S. (2015). OPS-A Review on Data Hiding using Steganography & Visual Cryptography. *International Journal of Research, 2*(10), 355-361.

Babu, K. R., Kumar, S. U., and Babu, A. V. (2010). A Survey on Cryptography and Steganography Methods for Information Security. *International Journal of Computer Applications, 12*(3), 13-17.

Bansal, N., Deolia, V. K., Bansal, A., and Pathak, P. (2015). Comparative analysis of LSB, DCT and DWT for Digital Watermarking. *Computing for Sustainable Global Development (INDIACom),* 2015 2nd International Conference on, 40-45.

Bhatt, S., Ray, A., Ghosh, A., and Ray, A. (2015). Image steganography and visible watermarking using LSB extraction technique. *Intelligent Systems and Control (ISCO),* 2015 IEEE 9th International Conference on, 1-6.

Bhattacharya, D. C. (2013). Microbial degradation of Phthalates: Present status and future prospects.

Blackledge, J. M. (2011). *Cryptography and Steganography: New Algorithms and Applications*: Center for Advanced Studies Warsaw University of Technology.

Chandran, S., and Bhattacharyya, K. (2015). Performance analysis of LSB, DCT, and DWT for digital watermarking application using steganography. *Electrical, Electronics, Signals, Communication and Optimization (EESCO),* 2015 International Conference on, 1-5.

Chauhan, A. (2015). Digital Watermarking-Revisit. *IJCSIT) International Journal of Computer Science and Information Technologies, 6*(1), 833-838.

Chen, K., Lin, D., and Yung, M. (2016). Information Security and Cryptology: Springer International Publishing.

Cohen, F. (2011). A Short History of Cryptography ". 1995.

Daras, N. J., and Rassias, M. T. (2015). Computation, cryptography, and network security: *Springer*.

Das, C., Panigrahi, S., Sharma, V. K., and Mahapatra, K. (2014). A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. *AEU-International Journal of Electronics and Communications, 68*(3), 244-253.

Durvey, M., and Satyarthi, D. (2014). A review paper on digital watermarking. *International Journal of Emerging Trends and Technology in Computer Science, 3*(4), 99-105.

Fazli, S., and Moeini, M. (2016). A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks. *Optik-International Journal for Light and Electron Optics, 127*(2), 964-972.

Febryan, A., Purboyo, T. W., and Saputra, R. E. (2017). Steganography Methods on Text, Audio, Image and Video: A Survey. *International Journal of Applied Engineering Research, 12*(21), 10485-10490.

Gaata, M. T., and Jaafar, R. A. (2016). Iris Image Authentication based on Adaptive Watermarking System. *Int J Comput Trends Technol, 34*(2), 63-67.

GL, S., and Baburaj, E. (2016). A Survey on Information Security. *International Journal of Engineering Science, 2152*.

Goli, M. S., and Naghsh, A. (2017). Introducing a new method robust against crop attack in digital image watermarking using two-step sudoku. *Pattern Recognition and Image Analysis (IPRIA),* 2017 3rd International Conference on, 237-242.

Guo, J., Zheng, P., and Huang, J. (2015). Secure watermarking scheme against watermark attacks in the encrypted domain. *Journal of Visual Communication and Image Representation, 30,* 125-135.

Halima, N. B., Khan, M. A., and Kumar, R. (2015). A novel approach of digital image watermarking using HDWT-DCT. *Computer & Information Technology (GSCIT),* 2015 Global Summit on, 1-6.

Hamid, M., and Wang, C. (2016). A simple image-adaptive watermarking algorithm with blind extraction. *Systems, Signals and Image Processing (IWSSIP),* 2016 International Conference on, 1-4.

Hariyanto, E., and Rahim, R. (2016). Arnold's Cat Map Algorithm in Digital Image Encryption. *International Journal of Science and Research (IJSR), 5*(10), 1363-1265.

Heidari, M., Karimi, N., and Samavi, S. (2016). A hybrid DCT-SVD based image watermarking algorithm. *Electrical Engineering (ICEE),* 2016 24th Iranian Conference on, 838-843.

Hsu, L.-Y., and Hu, H.-T. (2017). Robust blind image watermarking using crisscross inter-block prediction in the DCT domain. *Journal of Visual Communication and Image Representation, 46,* 33-47.

Jiang, K., Zhu, K. Q., Huang, Y., and Ma, X. (2013). Watermarking road maps against crop and merge attacks. *Proceedings of the first ACM workshop on Information hiding and multimedia security*, 221-230.

Katz, J., and Lindell, Y. (2014). Introduction to modern cryptography: CRC press.

Khan, M., Kushwaha, A., and Verma, T. (2015). A new digital image watermarking algorithm based on image interlacing, DWT, DCT. *Industrial Instrumentation and Control (ICIC),* 2015 International Conference on, 885-890.

Kokaram, A. (2016). The DCT and JPEG Image and Video Processing. 24.

Krishnagopal, S., Pratap, S., and Prakash, B. (2015). *Image encryption and steganography using chaotic maps with a double key protection.* Paper presented at the Proceedings of Fourth International Conference on Soft Computing for Problem Solving, 67-78.

Kumar, R. (2014). *Research methodology: A step-by-step guide for beginners*: Sage.

Kumar, S., and Dutta, A. (2016). *A study on robustness of block entropy based digital image watermarking techniques with respect to various attacks.* Paper presented at the Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE International Conference, 1802-1806.

Lau, W. K. (2016). *A dual-watermarking with QR code against cropping and resizing attack.* Universiti Tun Hussein Onn Malaysia.

Li, B., He, J., Huang, J., and Shi, Y. Q. (2011). A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing, 2*(2), 142-172.

Lutovac, B., Dakovic, M., Stankovic, S., and Orovic, I. (2017a). Watermark Detection in Impulsive Noise Environment Based on the Compressive Sensing Reconstruction. *Radioengineering, 26*(1), 309.

Lutovac, B., Daković, M., Stanković, S., and Orović, I. (2017b). An algorithm for robust image watermarking based on the DCT and Zernike moments. *Multimedia tools and applications, 76*(22), 23333-23352.

Mahajan, D. L., and Gogate, S. A. (2016). Overview of Digital Watermarking and its Techniques. *KHOJ: Journal of Indian Management Research and Practices*, 197-204.

Mahsa Boreiry, M. R. K. (2017). Classification of Watermarking Methods Based on Watermarking Approaches. *Artificial Intelligence and Robotics*, 4.

Manoria, M., and Dixit, P. (2012). An efficient DCT compression technique using Strassen's matrix multiplication algorithm. *International Journal of Computer Applications, 60*(9).

Marcus, M. (2014). JPEG image compression. *Dartmouth College*.

Mathai, J. (2011). History of computer cryptography and secrecy system. *Fordham University, http://www. d sm. fordham. edu/~ mathai/crypto. html, Accessed, 13*.

Mazumdar, H., Anand, P., Soni, S. J., Joshi, M., Rajeev, K., and Rajak, M. (2015). Human visual system models in Digital Watermarking. *Computing and Communication (IEMCON)*, 2015 International Conference and Workshop on, 1-7.

Mohammadabadi, A. A., and Chalechale, A. (2016). Parallelization of a color DCT watermarking algorithm using a CUDA-based approach. *Computer and Knowledge Engineering (ICCKE)*, 2016 6th International Conference, 100-105.

Moosazadeh, M., and Ekbatanifard, G. (2016). Robust image watermarking algorithm using DCT coefficients relation in YCoCg-R color space. *Information and Knowledge Technology (IKT)*, 2016 Eighth International Conference on, 263-267.

Muhammad, K., Ahmad, J., Sajjad, M., and Zubair, M. (2015). Secure image steganography using cryptography and image transposition. *arXiv preprint arXiv:1510.04413*.

Nematollahi, M. A., Vorakulpipat, C., and Rosales, H. G. (2017a). Image Watermarking. In *Digital Watermarking* (pp. 57-66): Springer.

Nematollahi, M. A., Vorakulpipat, C., and Rosales, H. G. (2017b). Preliminary on Watermarking Technology. In *Digital Watermarking* (pp. 1-14): Springer.

Nyeem, H., Boles, W., and Boyd, C. (2014). Digital image watermarking: its formal model, fundamental properties and possible attacks. *EURASIP Journal on Advances in Signal Processing, 2014*(1), 135.

Obaid, A. H. (2015). Information hiding techniques for steganography and digital watermarking. *Problems of Human-Computer Interaction.–Collection of scientific papers.* Ulyanovsk: USTU, 2015.– *306 p.*, 63.

Parah, S. A., Sheikh, J. A., Loan, N. A., and Bhat, G. M. (2016). Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing. *Digital Signal Processing, 53*, 11-24.

Parashar, P., and Singh, R. K. (2014). A survey: Digital image watermarking techniques. *Int. J. Signal Process. Image Process. Pattern Recognit, 7*(6), 111-124.

Pokudom, K., and Rangsanseri, Y. (2013). Design and development of ant colony system algorithms for block-based DCT watermarking. *Journal of Signal Processing, 17*(3), 51-60.

Preda, R., and Vizireanu, D. (2015). Watermarking-based image authentication robust to JPEG compression. *Electronics Letters, 51*(23), 1873-1875.

Qureshi, M. A., and Deriche, M. (2016). A new wavelet based efficient image compression algorithm using compressive sensing. *Multimedia Tools and Applications, 75*(12), 6737-6754.

Raid, A., Khedr, W., El-Dosuky, M., and Ahmed, W. (2014). JPEG image compression using discrete cosine transform-A Survey. *arXiv preprint arXiv:*1405.6147.

Rana, A., and Pareek, N. (2017). Comparative Study of DCT and DWT Techniques of Digital Image Watermarking. *International Conference on Information and Communication Technology for Intelligent Systems*, 377-382.

Razzaq, M. A., Sheikh, R., Baig, A., and Ahmad, A. (2017). Digital image security: Fusion of encryption, steganography and watermarking. *International Journal of Advanced Computer Science and Applications (IJACSA), 8*(5).

Saini, L. K., and Shrivastava, V. (2014). A survey of digital watermarking techniques and its applications.1407.4735.

Sarkar, T., and Sanyal, S. (2014). Digital Watermarking Techniques in Spatial and Frequency Domain. 1406.2146.

Sarmah, D. K., and Bajpai, N. (2010). Proposed System for data hiding using Cryptography and Steganography. *International Journal of Computer Applications, 8*(9), 7-10.

Saroya, N., and Kaur, P. (2014). Analysis Of Image Compression Algorithm Using DCT And DWT Transforms. *International Journal of Advanced Research in Computer Science and Software Engineering, 4*(2).

Shih, F. Y. (2012). *Digital watermarking and steganography: fundamentals and techniques*: CRC Press.

Shih, F. Y. (2017). *Digital watermarking and steganography: fundamentals and techniques*: CRC Press.

Singh, A. K., Kumar, B., Dave, M., Ghrera, S. P., and Mohan, A. (2016). Digital Image Watermarking: Techniques and Emerging Applications. *Research on Modern Cryptographic Solutions for Computer and Cyber Security* (pp. 246-272): IGI Global.

Singh, D., and Singh, S. K. (2017). DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. *Multimedia Tools and Applications, 76*(11), 13001-13024.

Singh, P., and Chadha, R. (2013). A survey of digital watermarking techniques, applications and attacks. *International Journal of Engineering and Innovative Technology (IJEIT), 2*(9).

Stallings, C., and RSA, C. (2010). Network security. *PHI*.

Struss, K. (2009). A Chaotic Image Encryption. *Spring, Mathematics Senior Seminar*.

Sundari, M., Revathi, P., and Sumesh, S. (2015). *Secure Communication Using Digital Watermarking with Encrypted Text Hidden in an Image.* Paper presented at the International Symposium on Security in Computing and Communication, 247-255.

Verens, K. (2009). *JQuery 1.3 with PHP*: Packt Publishing Ltd.

Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J. J., and Su, J. K. (2001). Attacks on digital watermarks: classification, estimation based attacks, and benchmarks. *Communications Magazine, IEEE, 39*(8), 118-126.

Wei, C., and Zhaodan, L. (2016). Robust watermarking algorithm of color image based on DWT-DCT and chaotic system. *Computer Communication and the Internet (ICCCI)*, 2016 IEEE International Conference on, 370-373.

Yen, C.-T., and Huang, Y.-J. (2016). Frequency domain digital watermark recognition using image code sequences with a back-propagation neural network. *Multimedia Tools and Applications, 75*(16), 9745-9755.

Yuliani, A. R., and Rosiyadi, D. (2015). A watermarking scheme based on DCT using HVS characteristic. *Computer, Control, Informatics and its Applications (IC3INA),* 2015 International Conference on, 165-168.

Zong, T.-R., Xiang, Y., Elbadry, S., and Nahavandi, S. (2016). Modified moment-based image watermarking method robust to cropping attack. *International Journal of Automation and Computing*, *13*(3), 259-267.