DISCRETE WAVELET TRANSFORM (DWT) BASED DUAL WATERMARKING FOR AUTHENTICATION AND COPYRIGHT PROTECTION

LIM CHEN GEN

FACULTY OF COMPUTING
UNIVERSITI MALAYSIA PAHANG

SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Computer Science (Graphics & Multimedia Technology)

_____

(Supervisor's Signature)

Full Name : Profesor Madya Ts. Dr. Ferda Ernawan

Position : Senior Lecturer

Date : 10/07/2023

_____

(Co-supervisor's Signature)

Full Name :

Position :

Date :

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

_____

(Student's Signature)

Full Name : LIM CHEN GEN

ID Number : CD20136

Date : 7/6/2023

DISCRETE WAVELET TRANSFORM (DWT) BASED DUAL WATERMARKING FOR AUTHENTICATION AND COPYRIGHT PROTECTION

LIM CHEN GEN

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Computer Science (Graphics & Multimedia Technology)

Faculty of Computing
UNIVERSITI MALAYSIA PAHANG

JUNE 2023

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to Dr. Ferda Ernawan, my research supervisor, for his invaluable guidance, support, and expertise throughout my thesis journey. His unwavering commitment to academic excellence and his passion for research have been a constant source of inspiration for me.

I am grateful to Dr. Ernawan for his patience, encouragement, and insightful feedback that significantly contributed to the development and refinement of my research work. His expertise in the field has been instrumental in shaping my research methodology and enhancing the quality of my findings.

I would also like to extend my appreciation to the faculty members and staff who have provided assistance, resources, and a conducive research environment during my academic pursuit. Their support and dedication have been instrumental in my growth as a researcher.

I am indebted to my family and friends for their unwavering support, understanding, and encouragement throughout this thesis journey. Their belief in my abilities and constant motivation have been the driving force behind my accomplishments.

Lastly, I would like to acknowledge all the researchers, scholars, and authors whose works and contributions have provided the foundation and inspiration for my research. Their insights and discoveries have paved the way for advancements in the field and have been instrumental in shaping my understanding.

ABSTRACT

Digital media faces significant challenges related to unauthorized access, manipulation, and copyright infringement, necessitating effective authentication and copyright protection mechanisms. This thesis proposes a novel dual watermarking scheme based on the Discrete Wavelet Transform (DWT) to address these concerns.

The primary objective of the proposed scheme is to provide robust copyright protection. A watermark, carrying ownership and copyright information, is embedded in the spatial domain using the DWT. This watermark acts as a digital signature, enabling the identification and tracing of the rightful owner of the content. The frequency domain embedding enhances the watermark's robustness against common attacks.

In addition to copyright protection, the scheme incorporates a fragile watermark for authentication purposes. The fragile watermark is embedded in the least significant bit which is highly sensitive to any modifications or tampering. By extracting and comparing the fragile watermark, the integrity and authenticity of the content can be verified.

Comprehensive experimental evaluations have been conducted to assess the performance of the proposed dual watermarking scheme. The results demonstrate its effectiveness in providing robust copyright protection and authentication capabilities. The scheme exhibits high imperceptibility, preserving the visual quality of the watermarked content, while ensuring a high level of sensitivity to unauthorized alterations.

TABLE OF CONTENT

DECLARATION

TITLE PAGE

ACKNOWLEDGEMEMTS **i**

ABSTRACT **ii**

TABLE OF CONTENT **iii**

LIST OF TABLES **vi**

LIST OF FIGURES **vii**

LIST OF ABBREVIATIONS **ix**

LIST OF APPENDICES **x**

CHAPTER 1 INTRODUCTION **1**

1.1 Background 1

1.2 Problem Statement 2

1.3 Research Objective 4

1.4 Research Scope 4

CHAPTER 2 LITERATURE REVIEW **5**

2.1 Introduction 5

2.2 Overview of Watermarking Technique 5

2.2.1 Dual Watermarking Scheme 6

2.2.2 Watermarking for Copyright Protection 6

2.2.3 Watermarking for Authentication 7

2.2.4 Embedding Sub-bands and Sub-block 8

2.2.5 Singular Value Decomposition (SVD) 8

2.2.6 Embedding Luminance Y Component from RGB Conversion 9

2.3 The Existing Dual Image Watermarking Scheme 10

2.4 Summary of The Existing Dual Image Watermarking Scheme 11

2.5 Relevance of Comparison 12

CHAPTER 3 METHODLOGY 13

3.1 Introduction 13

3.2 Research Framework 13

3.3 Research Requirement 15

3.4 Propose Design 16

3.4.1 Copyright Protection Watermarking Algorithm 19

3.4.2 Authentication Watermarking Algorithm 20

3.4.3 Tamper Localization Algorithm 21

3.4.4 Watermark Extraction Algorithm 22

3.5 Evaluation Plan 23

3.5.1 Imperceptibility Measurement 23

3.5.2 Robustness Measurement 24

3.5.3 Tamper Localization Measurement 25

3.6 Potential Use of Proposed Solution 26

3.7 Gantt Chart 26

CHAPTER 4 RESULT AND DISCUSSION 27

4.1 Introduction 27

4.2 Imperceptibility Experiment 28

4.3 Tamper Detection and Watermark Extraction under Regular Attack 32

4.4 Tamper Detection under Irregular Attack Experiment 39

4.5 Watermark extraction under Image Processing Attack 42

CHAPTER 5 CONCLUSION 48

5.1 Research Conclusion 48

5.2 Future Work 49

Reference **50**

APPENDIX **53**

LIST OF TABLES

Table 2.1	Summary of existing watermarking	10
Table 4.1	Comparison data PSNR and SSIM	29
Table 4.2	Comparison data of tamper detection performance under regular attacks	34
Table 4.3	Comparison data of extraction under regular attacks	37
Table 4.4	Data of tamper detection performance under irregular attacks	41
Table 4.5	Various image processing detail and its abbreviation	42
Table 4.6	NC BER result data and comparison	44

LIST OF FIGURES

Figure 2.1	Example Decomposition of DWT	7
Figure 3.1	Research Framework	14
Figure 3.2	Images and logo used for the experiment	15
Figure 3.3	The block diagram showing process of the proposed watermarking scheme	16
Figure 3.4	The block diagram showing process of the watermark extraction	17
Figure 3.5	The block diagram showing process of the tamper detection	18
Figure 4.1	Dual Watermarked Images Showing High Imperceptibility Embedding	28
Figure 4.2	Comparison PSNR values of the dual watermarked image between the schemes	29
Figure 4.3	Comparison SSIM values of the dual watermarked image between the schemes	30
Figure 4.4	Image with regular attack from 10% to 50% (a-e 1), detected tamper (a-e 2), correct detected tamper (a-e 3), and watermark extraction from the regular attact (a-e 4)	33
Figure 4.5	Precision Comparison of Tamper Detection from Different Tampering Rate	34
Figure 4.6	F1-Score Comparison of Tamper Detection from Different Tampering Rate	35
Figure 4.7	Accuracy Comparison of Tamper Detection from Different Tampering Rate	35
Figure 4.8	NC Comparison of Watermark Extraction from Different Tampering Rate	37
Figure 4.9	BER Comparison of Watermark Extraction from Different Tampering Rate	37
Figure 4.10	Watermarked images (a-f 1), irregular attacked images (a-f 2), red marked tamper detection images (a-f 3), correct detected area (a-f 4)	40

Figure 4.11 Images with image processing attack and its watermark extraction 43

Figure 4.12 NC Comparison of image processing attack (Lena) 46

Figure 4.13 BER Comparison of image processing attack (Lena) 46

Reference

Ahmadi, S. B. B., Zhang, G., Rabbani, M., Boukela, L., & Jelodar, H. (2021). An intelligent and blind dual color image watermarking for authentication and copyright protection. *Applied Intelligence*, *51*(3), 1701–1732. https://doi.org/10.1007/s10489-020-01903-0

Aminuddin, A., & Ernawan, F. (2022). AuSR1: Authentication and self-recovery using a new image inpainting technique with LSB shifting in fragile image watermarking. *Journal of King Saud University - Computer and Information Sciences*, *34*(8), 5822–5840. https://doi.org/10.1016/j.jksuci.2022.02.009

Bolourian Haghighi, B., Taherinia, A. H., & Harati, A. (2018). TRLH: Fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and halftoning technique. *Journal of Visual Communication and Image Representation*, *50*, 49–64. https://doi.org/10.1016/j.jvcir.2017.09.017

Daren, H., Jiufen, L., Jiwu, H., & Hongmei, L. (2001). *A DWT-BASED IMAGE WATERMARKING ALGORITHM*.

Das, C., Panigrahi, S., Sharma, V. K., & Mahapatra, K. 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. https://doi.org/10.1016/j.aeue.2013.08.018

Deepa B. Maheshwari. (2018). *An Analysis of Wavelet Based Dual Digital Image Watermarking Using SVD*. IEEE.

Dey, N., Samanta, S., Chakraborty, S., Das, A., Chaudhuri, S. S., & Suri, J. S. (2014). Firefly algorithm for optimization of scaling factors during embedding of manifold medical information: An application in ophthalmology imaging. *Journal of Medical Imaging and Health Informatics*, *4*(3), 384–394. https://doi.org/10.1166/jmihi.2014.1265

Dimple Bansal, & Manish Mathuria. (2017). *Color Image Dual Watermarking using DCT and DWT Combine Approach*.

Donald, D. A., Everingham, Y. L., Mckinna, L. W., & Coomans, D. (2009). *3.23 Feature Selection in the Wavelet Domain: Adaptive Wavelets*.

Duan, S., Wang, H., Liu, Y., Huang, L., & Zhou, X. (2020). A Novel Comprehensive Watermarking Scheme for Color Images. *Security and Communication Networks*, *2020*. https://doi.org/10.1155/2020/8840779

Ernawan, F. (2016). Robust image watermarking based on psychovisual threshold. *Journal of ICT Research and Applications*, *10*(3), 228–242. https://doi.org/10.5614/itbj.ict.res.appl.2016.10.3.3

Ernawan, F., & Ariatmanto, D. (2019). Image watermarking based on integer wavelet transform-singular value decomposition with variance pixels. *International Journal of Electrical and Computer Engineering*, *9*(3), 2185–2195. https://doi.org/10.11591/ijece.v9i3.pp2185-2195

Hsu, L. Y., & 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. https://doi.org/10.1016/j.jvcir.2017.03.009

Huang, R., Liu, H., Liao, X., & Sun, S. (2019). A divide-and-conquer fragile self-embedding watermarking with adaptive payload. *Multimedia Tools and Applications*, *78*(18), 26701–26727. https://doi.org/10.1007/s11042-019-07802-y

Hussein, J. A., & Sulaimani, -. (2012). Luminance-based Embedding Approach for Color Image Watermarking. *International Journal of Image, Graphics and Signal Processing*, *4*(3), 49–55. https://doi.org/10.5815/ijigsp.2012.03.08

Jagadeesh, B., Kumar, P. R., & Reddy, P. C. (2016). Robust digital image watermarking based on fuzzy inference system and back propagation neural networks using DCT. *Soft Computing*, *20*(9), 3679–3686. https://doi.org/10.1007/s00500-015-1729-y

Jobin Abraham, & Dr. Varghese Paul. (2017). *A Dual Domain Digital Image Watermarking Scheme*. IEEE.

Lai, C. C. (2011). An improved SVD-based watermarking scheme using human visual characteristics. *Optics Communications*, *284*(4), 938–944. https://doi.org/10.1016/j.optcom.2010.10.047

Laouamer, L., & Tayan, O. (2018). Performance Evaluation of a Document Image Watermarking Approach with Enhanced Tamper Localization and Recovery. *IEEE Access*, *6*, 26144–26166. https://doi.org/10.1109/ACCESS.2018.2831599

Liu, X. L., Lin, C. C., & Yuan, S. M. (2018). Blind Dual Watermarking for Color Images' Authentication and Copyright Protection. *IEEE Transactions on Circuits and Systems for Video Technology*, *28*(5), 1047–1055. https://doi.org/10.1109/TCSVT.2016.2633878

Lusia Rakhmawati, Wirawan, Suwadi, Claude Delpha, & Pierre Duhamel. (2020). *Dual Watermarking Schemes for Image Authentication and Copyright Protection with Recovery Capability*. https://doi.org/10.1109/ACCESS.2017.Doi

Makbol, N. M., Khoo, B. E., & Rassem, T. H. (2016). Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image Processing*, *10*(1), 34–52. https://doi.org/10.1049/iet-ipr.2014.0965

Molina-Garcia, J., Garcia-Salgado, B. P., Ponomaryov, V., Reyes-Reyes, R., Sadovnychiy, S., & Cruz-Ramos, C. (2020). An effective fragile watermarking scheme for color image tampering detection and self-recovery. *Signal Processing: Image Communication*, *81*. https://doi.org/10.1016/j.image.2019.115725

Mun, S. M., Nam, S. H., Jang, H., Kim, D., & Lee, H. K. (2019). Finding robust domain from attacks: A learning framework for blind watermarking. *Neurocomputing*, *337*, 191–202. https://doi.org/10.1016/j.neucom.2019.01.067

Nasir N. Hurrah, Shabir A. Parah, Nazir A. Loan, Javaid A. Sheikh, Mohamed Elhoseny, & Khan Muhammad. (2018). *Dual Watermarking Schemes for Image Authentication and Copyright Protection with Recovery Capability*. https://doi.org/10.1109/ACCESS.2017.Doi

Singh, D., & Singh, S. K. (2019). Block Truncation Coding based effective watermarking scheme for image authentication with recovery capability. *Multimedia Tools and Applications*, *78*(4), 4197–4215. https://doi.org/10.1007/s11042-017-5454-7

Singh, S. P., & Bhatnagar, G. (2018). A new robust watermarking system in integer DCT domain. *Journal of Visual Communication and Image Representation*, *53*, 86–101. https://doi.org/10.1016/j.jvcir.2018.03.006

Thakral, S., & Manhas, P. (2019). Image processing by using different types of discrete wavelet transform. *Communications in Computer and Information Science*, *955*, 499–507. https://doi.org/10.1007/978-981-13-3140-4_45