UNIVERSITI PUTRA MALAYSIA

IMAGE AUTHENTICATION USING ZERNIKE MOMENT WATERMARKING

HAMID SHOJANAZERI

IMAGE AUTHENTICATION USING ZERNIKE MOMENT WATERMARKING

By

HAMID SHOJANAZERI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

July 2013

COPYRIGHT

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science.

IMAGE AUTHENTICATION USING ZERNIKE MOMENT WATERMARKING

By

HAMID SHOJANAZERI

July 2013

Chair: Wan Azizun Wan Adnan, PhD

Faculty: Engineering

The rapid development of internet and digital image editing softwares facilitated the access and illegal usage of digital images. Digital watermarking emerged as a unique tool to protect the authenticity of the image. It is a technique of insertion of a message into a cover media imperceptibly.

In this thesis, the main objective is to design and develop a watermarking system for image authentication. A semi-fragile watermarking system using content-based techniques is proposed in this work to solve the problems with the previously proposed methods which are not robust against normal image processing operations such as rotation, scale, translation, noise addition and JPEG compression. The Zernike moments and Sobel edge map are used as watermarks to provide malicious attack classification and locating tampered area. The Zernike moments are chosen due to special characteristics such as robustness against rotation, scale, translation (RST) and noise. Also an image can be reconstructed from the extracted Zernike moments. These watermarks are generated from the approximation component of discrete wavelet decomposition in third level. The Sobel edge map is fused in wavelet coefficients of the corresponding component, and Zernike moments vector is fused

in Sobel edge point of the original image. A comparison between recovered Zernike moments and generated Zernike moments form watermarked image at receiver determine the authenticity of the image. In case of authenticity failure, a comparison between recovered Sobel edge map and recently obtained Sobel edge map from the watermarked image detect the location of tampered areas. The results from the test show that the proposed algorithm has good performance in discriminating the malicious from non-malicious modifications which is the main character of an image authentication algorithm. This work significantly improves the robustness of semi-fragile characteristics of watermarking. It accepts scale, translation, noise pollution, rotation and JPEG compression modifications on the watermarked images, so it can solve the problem with previous methods with flaw of discrimination between malicious and non-malicious attacks. The adding or replacing a portion of the image is regarded as malicious attacks and rejected by this algorithm. Using two different watermarks lead to a good classification of incidental and malicious modifications and locating the tampered areas. Experimental results showed that this algorithm achieves better bit error rate against JPEG compression, rotation, scale and noise attacks in comparison with other reviewed schemes in this work. A great improvement is also achieved in the capacity of the watermarking system as shown in chapter Four. This scheme also offers better classification of malicious modifications over the other reviewed schemes in this work.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains.

PENGESAHAN IMEJ MENGGUNAKAN TERA AIR ZERNIKE MOMENT

Oleh

HAMID SHOJANAZERI

Julai 2013

Pengerusi: Wan Azizun Wan Adnan, PhD

Fakulti: Kejuruteraan

Perkembangan pesat internet dan perisian pengubahsuaian imej digital telah memudahkan akses kepada dan penggunaan imej digital secara haram. Tera air digital telah muncul sebagai alat yang unik yang boleh melindungi kesahihan imej. Konsep tera air digital adalah dengan penyisipan mesej ke media pelindung menyebabkan kemerosotan yang ketara pada imej. Teknik ini dapat menangani masalah tersebut dengan penyulitan kehadiran maklumat dalam media penutup selepas penyahsulitan. Objektif utama tesis ini ialah untuk merekabentuk dan membangunkan sistem tera air untuk pengesahan imej. Satu sistem separa-rapuh yang menggunakan teknik berasaskan kandungan dicadangkan dalam kajian ini untuk menyelesaikan masalah dengan kaedah yang dicadangkan sebelum ini yang tidak teguh terhadap operasi pemprosesan imej biasa seperti putaran, skala, terjemahan, penambahan bunyi dan pemampatan JPEG. Moments Zernike dan Sobel edge map digunakan sebagai tera air untuk memberi klasifikasi serangan berniat jahat dan mencari kawasan yang diganggu. Moments Zernike dipilih kerana memiliki cirri-cirri khans seperti keteguhan terhadap putaran, skala, terjemahan, dan

hingar. Imej juga boleh dibina semula dari Zernike moments yang telah diekstrak. Tera air ini dihasilkan daripada komponen anggaran penguraian wavelet diskrit di peringkat ketiga. Sobel edge map ditanam di dalam pekali wavelet dalam komponen yang sama, dan vektor Zernike moments ditanam di titik pinggir sobel imej asal. Perbandingan antara Zernike moments yang didapati dengan yang dihasilkan daripada imej yang melalui proses tera air pada penerima akan menentukan kesahihan imej. Dalam kes kegagalan kesahihan, perbandingan antara sobel edge map yang didapati dengan yang baru diperoleh dari imej yang telah melalui proses tera air dilakukan begi mengesan lokasi kawasan yang diganggu. Keputusan dari ujian menunjukkan bahaw algoritma yang dicadangkan mempunyai prestasi yang baik dalam membezakan pengubahsuaian yang berniat jahat dan yang bukan berniat jahat yang merupakan watak utama dalam sesuatu algoritma pengesahan imej. Kajian ini meningkatkan keteguhan cirri-cirri semi-rapuh tera air dengan ketara. Ia menerima besaran, terjemahan, pencemaran bunyi, putaran dan pengubahsuaian mampatan JPEG imej tera air.Penambahan atau penggantian sebahagian imej dianggap sebagai serangan berniat jahat dan ditolak oleh algoritma ini. Penggunaan dua tera air yang berbeza membawa kepada klasifikasi pengubahsuaian sampingan dan berniat jahat yang sangat baik dan mencari kawasan yang diganggu. Keputusan ujikaji menunjukkan algoritma ini mencapai kadar ralat bit yang lebih baik terhadap pemampatan JPEG, putaran, skala dan serangan hingar di bandingkan dengan lain-lain skim yang dikaji dalam kajian ini supaya ia boleh menyelesaikan masalah ini dengan kaedah sebelumnya dengan kelemahan diskriminasi antara serangan berniat jahat dan bukan berniat jahat. Satu peningkatan yang besar juga dicapai dalam kapasiti sistem tera air seperti yang ditunjukkan dalam hasil kajian. Skim ini juga menawarkan klasifikasi pengubahsuaian berniat jahat yang lebih baik berbanding skim lain yang dikaji dalam kajian ini.

I certify that a Thesis Examination Committee has met on 15 July 2013 to conduct the final examination of Hamid Shojanazeri on his thesis entitled "Image Authentication using Zernike Moment Watermarking" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.

Members of the Thesis Examination Committee were as follows:

Syed Abd Rahman Al-Haddad bin Syed Mohamed, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Abd. Rahman bin Ramli, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Syamsiah binti Mashohor, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Riza Sulaiman, PhD
Associate Professor Ir.
Universiti Kebangsaan Malaysia
Malaysia
(External Examiner)

NORITAH OMAR, PhD
Associate Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 19 September 2013

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the Master of Science. The members of the Supervisory Committee were as follows:

Wan Azizun Wan Adnan, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

M. Iqbal Bin Saripan. Dr
Assco Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

BUJANG BIN KIM HUAT, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

DECLARATION

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

_____

HAMID SHOJANAZERI

Date: 15 JULY 2013

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

RST	Rotation, Scale and Translation
BER	Bit Error Rate
dB	decibell
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
HVS	Human Visual System
IDWT	Inverse Discrete Wavelet Transform
LSB	Least significant Bit
MPEG	Moving Picture Experts Group
MSE	Mean Square Error
PFR	Probability of False Rejection
PSNR	Peak to Signal to Noise Ratio
QF	Quality Factor
RVR	Relationship Vector Recovery
STFT	Short-Time Fourier Transform
SARI	Self Authentication and Recovery Images
VRML	Virtual Reality Modeling Language
WEC	Weighted Euclidean Distance
ZMMs	Zernike Moments

CHAPTER 1

INTRODUCTION

1.1 General Overview

Development of internet and image processing softwares ease illegal manipulation of images. Encryption emerged as solution for protection of multimedia materials. The flaw of encryption system is with respect to unprotected data after decryption. It means, encryption can only provide the security during the transmission. Digital watermarking can be the solution since it can provide the security after decryption of data. Many applications such as copyright protection, broadcast monitoring, fingerprinting and content authentication etc. exploits digital watermarking techniques to achieve their goals.

Today, in digital world image authentication becomes an important research area. Digital images are being transmitted over the networks and stored on different storages, manipulations on these images such as tampering can be considered as attacks. Hence, watermarking is reputed as a unique tool aims to protect the images against illegal modifications.

The aim of a watermarking system is to fuse a subliminal message into the cover media such as image, text, video or audio signal. It must satisfy imperceptibility,

robustness, capacity and speed. There is trade off between these requirements which depends on the application. A robust scheme needs more information to be fused which affects the imperceptibility of the image. For example, in copyright protection application, it needs to be robust to any attacks in order to protect the fused information. On the other hand, image authentication focuses more on fragile or semi-fragile to detect the tampering rather than robust techniques.

The classification of digital watermarking can be performed from different view of points such as host media, visibility, fused domain, robustness of algorithm and type of detection, as shown in Table 1.2.

Table 1.1. The Classification of Watermark Techniques

Host Signal	Fusion Domain	Detection	Robustness	Visibility	Watermark data
Image	Spatial domain	Blind	Robust	Visible	Noise
Audio		Semi-Blind	Fragile		Image
Video	Frequency domain	Non-Blind	Semi-fragile	Invisible	Authentication
Text					Information

Table 1.2. The Classification of Watermark Techniques

This thesis explores the content-based image watermarking as envisioned by [1] which uses the perceptual features of images as watermark. A comparison in receiver between recovered watermark and current features of the watermarked image validates the received image. Different features have been used in this content-based approaches as will be discussed in the Literature Review found in Chapter Two. Image moments are region based descriptors. Their names correspond to the specific polynomial that image is projected on. Orthogonal moments addressed the problem with geometric moments in redundancy of information. Zernike moments which were introduced by [4] are orthogonal moments and defined on a unit disk. The Zernike moments have special characteristics such as robustness against rotation, scale, translation (RST), and noise [4, 5]. Additionally an image can be reconstructed from the extracted Zernike moments. These properties are exploited by researchers

to develop RST robust watermarking systems. Furthermore, the RST invariance of Zernike moments can be used for authentication of images due to their ability in discrimination of malicious from non-malicious modifications [1, 6].

1.2 Problem Statement

The motivation behind this research is the importance of image authentication in new digital paradigm.Due to the vast developments in internet and image editing software any image can be easily forged or altered maliciously today, so this can violate the privacy of people. Sometimes an image is a critical piece of evidence in a legal case and it must be authentic hence an image authentication watermarking system can prevent illegal modifications of an image. Many image authentication approaches have been developed using watermarking in different domains such as spatial and frequency with their respective strengths and weaknesses. The previously developed schemes usually are capable of detecting the tampered areas. However, they are not capable of discriminating between malicious and non-malicious modifications [7, 8]. As a result, every modification is considered as malicious attack even after normal image processing operations. Therefore, these approaches can not fulfil image authentication system requirements which should have the following characteristics namely:

- blind detection
- discrimination between malicious and non-malicious attacks
- tamper location detection

1.3 Objectives

The main aim of this study is to design and develop a semi-fragile watermarking system to authenticate the images. A semi-fragile watermarking as a remedy for image authentication are more robust than fragile watermarking. These approaches are less sensitive to incidental modifications. The non-malicious attacks such as rotation, scale, translation, noise and JPEG compression should be different from a malicious manipulation like adding or removing a significant portion of a image. Therefore, the objectives of this study are:

- to develop an image authentication watermarking system that can discriminate between malicious and non-malicious attacks.
- to evaluate the performance of the developed watermarking system based on its accuracy, capacity and attack discrimination.

1.4 Scope of Work

The scope of this study only involves image authentication watermarking. A semi-fragile content-based watermarking is proposed by exploiting the invariant moments theory. The Zernike moments are employed to represent the image features. The implementation of Zernike moments computation is done in Matlab software. The five standard test images in this work are selected from the website www.imageprocessingplace.com. The test images are Lena, Baboon, Cameraman, Peppers, and Jetplane which are frequently used by researchers in this area.

1.5 Outline of Thesis

This thesis consists of five chapters. Chapter One (this chapter) presents a brief introduction to principle terms of problems related to this research. It also discusses the scope of this study and the objectives of this work.

In chapter Two, a survey on existing image watermarking methods is done and watermarking domains are classified. The concept of content-based watermarking and categorization of its techniques is covered in this chapter as well.

Chapter Three explains the methodology used in this research. This chapter is organized into three parts where the first part provides tools used in this work and the process flow of the system. The second part includes feature selection, the flow of watermarking system and authentication process. The evaluation of the system, different tests and metrics are discussed in third part.

Chapter Four presents the results of proposed watermarking system as discussed in chapter Three. In this chapter, the feature selection results are presented. The proposed watermarking scheme tested under different malicious and non-malicious attacks using the standard images is also presented. The performance results of images fidelity after watermarking, accuracy of recovered watermarks, and categorizing of attacks are presented in this chapter. The last part of this chapter performs a comparison between the proposed work and other schemes.

Finally, chapter Five concludes the study, and a further work is suggested.

REFERENCES

[1] C. Kao and L. Chang, "Zernike moments and edge features based semi-fragile watermark for image authentication with tampering localization," in *Proceedings of APSIPA ASC 2009*, APSIPA ASC, 2009.

[2] C. Deng, X. Gao, X. Li, and D. Tao, "A local tchebichef moments-based robust image watermarking," *Signal Processing*, vol. 89, no. 8, pp. 1531–1539, 2009.

[3] X. Wang, Y. Yang, and H. Yang, "Invariant image watermarking using multi-scale harris detector and wavelet moments," *Computers & electrical engineering*, vol. 36, no. 1, pp. 31–44, 2010.

[4] M. Teague, "Image analysis via the general theory of moments*," *JOSA*, vol. 70, no. 8, pp. 920–930, 1980.

[5] N. Kim, "Object edge watermarking," Apr. 23 2002. US Patent App. 10/131,584.

[6] L. Hongmei, Y. Xinzhi, and H. Jiwu, "Semi-fragile zernike moment-based image watermarking for authentication," *EURASIP Journal on Advances in Signal Processing*, vol. 2010, 2010.

[7] Z. Hao, H. Li, and P. Yu, "Semi-fragile watermarking technique for image tamper localization," in *International Conference on Measuring Technology and Mechatronics Automation, 2009. ICMTMA'09.*, vol. 1, pp. 519–523, IEEE, 2009.

[8] G. Zhaoqian, G. Fei, and S. Cheng, "Implementation of dwt domain-video watermarking fast algorithm in blackfin dsp," *Mechanical Engineering and Technology*, pp. 773–778, 2012.

[9] I. Cox, M. Miller, J. Bloom, and C. Honsinger, "Digital watermarking," *Journal of Electronic Imaging*, vol. 11, p. 414, 2002.

[10] E. Trucco and A. Verri, *Introductory techniques for 3-D computer vision*, vol. 93. Prentice Hall Upper Saddle Rive, 1998.

[11] H. Nyeem, W. Boles, and C. Boyd, "On the robustness and security of digital image watermarking," in *Proceedings of International Conference on Informatics, Electronics & Vision*, 2012.

[12] D. Zheng, Y. Liu, J. Zhao, and A. Saddik, "A survey of rst invariant image watermarking algorithms," *ACM Computing Surveys (CSUR)*, vol. 39, no. 2, p. 5, 2007.

[13] C. Podilchuk and E. Delp, "Digital watermarking: algorithms and applications," *IEEE Signal Processing Magazine,*, vol. 18, no. 4, pp. 33–46, 2001.

[14] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing,*, vol. 6, no. 12, pp. 1673–1687, 1997.

[15] P. Chan, M. Lyu, and R. Chin, "A novel scheme for hybrid digital video watermarking: approach, evaluation and experimentation," *IEEE Transactions on Circuits and Systems for Video Technology,*, vol. 15, no. 12, pp. 1638–1649, 2005.

[16] G. Langelaar, I. Setyawan, and R. Lagendijk, "Watermarking digital image and video data. a state-of-the-art overview," *IEEE signal processing magazine,*, vol. 17, no. 5, pp. 20–46, 2000.

[17] S. Bhattacharya, T. Chattopadhyay, and A. Pal, "A survey on different video watermarking techniques and comparative analysis with reference to h. 264/avc," in *IEEE Tenth International Symposium on Consumer Electronics, 2006. ISCE'06. 2006*, pp. 1–6, IEEE, 2006.

[18] X. Luo, D. Wang, P. Wang, and F. Liu, "A review on blind detection for image steganography," *Signal Processing*, vol. 88, no. 9, pp. 2138–2157, 2008.

[19] N. Cvejic and T. Seppanen, "Increasing robustness of lsb audio steganography using a novel embedding method," in *Proceedings of International Conference on Information Technology: Coding and Computing, 2004. ITCC 2004.*, vol. 2, pp. 533–537, IEEE, 2004.

[20] F. Shih and S. Wu, "Combinational image watermarking in the spatial and frequency domains," *Pattern Recognition*, vol. 36, no. 4, pp. 969–975, 2003.

[21] M. Barni, F. Bartolini, and A. Piva, "Improved wavelet-based watermarking through pixel-wise masking," *IEEE Transactions on Image Processing,*, vol. 10, no. 5, pp. 783–791, 2001.

[22] R. Liu and T. Tan, "An svd-based watermarking scheme for protecting rightful ownership," *IEEE Transactions on Multimedia,*, vol. 4, no. 1, pp. 121–128, 2002.

[23] A. Piva, M. Barni, F. Bartolini, V. Cappellini, A. De Rosa, and M. Orlandi, "Improving dft watermarking robustness through optimum detection and synchronization," in *Multimedia and Security Workshop at ACM Multimedia*, vol. 99, pp. 65–69, 1999.

[24] H. Zhang, J. Li, and C. Dong, "Multiple video zero-watermarking based on 3d dft to resist geometric attacks," in *2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012*, pp. 1141–1144, IEEE, 2012.

[25] X. Zhou, X. Duan, and D. Wang, "A semifragile watermark scheme for image authentication," in *Proceeding of 10th International Conference on Multimedia Modelling , 2004.*, pp. 374–377, IEEE, 2004.

[26] M. Paunwala and S. Patnaik, "Dct watermarking approach for security enhancement of multimodal system," *ISRN Signal Processing*, vol. 2012, 2012.

[27] A. Elahian, M. Khalili, and S. Shokouhi, "Improved robust dwt-watermarking in ycbcr color space," *arXiv preprint arXiv:1209.1949*, 2012.

[28] H. Shi, N. Wang, Z. Wen, Y. Wang, H. Zhao, and Y. Yang, "An rst invariant image watermarking scheme using dwt-svd," in *International Symposium on Instrumentation & Measurement, Sensor Network and Automation (IMSNA), 2012*, vol. 1, pp. 214–217, IEEE, 2012.

[29] H. Kumar *et al.*, "Watermark attacks and applications in watermarking," in *IJCA Proceedings on National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing 2011*, no. 10, Foundation of Computer Science (FCS), 2012.

[30] C. Rey and J. Dugelay, "A survey of watermarking algorithms for image authentication," *EURASIP Journal on Applied Signal Processing*, vol. 2002, no. 1, pp. 613–621, 2002.

[31] C. Lin and S. Chang, "Semifragile watermarking for authenticating jpeg visual content," in *Electronic Imaging*, pp. 140–151, International Society for Optics and Photonics, 2000.

[32] G. Li, S. Pei, G. Chen, W. Cao, and B. Wu, "A self-embedded watermarking scheme based on relationship function of corresponding inter-blocks dct coefficient," in *13th International Conference on Computer Supported Cooperative Work in Design, 2009. CSCWD 2009.*, pp. 107–112, IEEE, 2009.

[33] S. Hsieh, I. Tsai, C. Yeh, and C. Chang, "An image authentication scheme based on digital watermarking and image secret sharing," *Multimedia Tools and Applications*, vol. 52, no. 2, pp. 597–619, 2011.

[34] K. Maeno, Q. Sun, S. Chang, and M. Suto, "New semi-fragile image authentication watermarking techniques using random bias and nonuniform quantization," *IEEE Transactions on Multimedia,*, vol. 8, no. 1, pp. 32–45, 2006.

[35] H. Kang and J. Park, "A semi-fragile watermarking using jnd," *Proc. of STEG*, pp. 127–131, 2003.

[36] E. Lin, C. Podilchuk, and E. Delp III, "Detection of image alterations using semifragile watermarks," in *Electronic Imaging*, pp. 152–163, International Society for Optics and Photonics, 2000.

[37] J. Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal processing*, vol. 66, no. 3, pp. 303–317, 1998.

[38] C. Lin, M. Wu, J. Bloom, I. Cox, M. Miller, and Y. Lui, "Rotation, scale, and translation resilient watermarking for images," *IEEE Transactions on Image Processing,*, vol. 10, no. 5, pp. 767–782, 2001.

[39] Y. Xin, S. Liao, and M. Pawlak, "Circularly orthogonal moments for geometrically robust image watermarking," *Pattern Recognition*, vol. 40, no. 12, pp. 3740–3752, 2007.

[40] E. Tsougenis, G. Papakostas, D. Koulouriotis, and V. Tourassis, "Performance evaluation of moment-based watermarking methods: A review," *Journal of Systems and Software*, 2012.

[41] B. Ouyang, *Watermarking based on unified pattern recognition framework*. PhD thesis, SOUTHERN METHODIST UNIVERSITY, 2010.

[42] C. Singh, E. Walia, and N. Mittal, "Fusion of zernike moments and sift features for improved face recognition," in *IJCA Proceedings on International Conference on Recent Advances and Future Trends in Information Technology (iRAFIT 2012)*, no. 6, pp. 26–31, Foundation of Computer Science (FCS), 2012.

[43] Å. Wallin and O. Kubler, "Complete sets of complex zernike moment invariants and the role of the pseudoinvariants," *IEEE Transactions on Pattern Analysis and Machine Intelligence,*, vol. 17, no. 11, pp. 1106–1110, 1995.

[44] J. Flusser, T. Suk, B. Zitov, and I. Ebrary, *Moments and moment invariants in pattern recognition*. Wiley Online Library, 2009.

[45] Y. Hu and D. Han, "Using two semi-fragile watermark for image authentication," in *Proceedings of International Conference on Machine Learning and Cybernetics, 2005.*, vol. 9, pp. 5484–5489, IEEE, 2005.

[46] M. Misiti, Y. Misiti, G. Oppenheim, and J. Poggi, "Wavelet toolbox," *The MathWorks Inc., Natick, MA*, 1996.

[47] M. Tsai, K. Yu, and Y. Chen, "Joint wavelet and spatial transformation for digital watermarking," *IEEE Transactions on Consumer Electronics,*, vol. 46, no. 1, p. 237, 2000.

[48] V. Jayanthi, V. Rajamani, and P. Karthikayen, "Performance analysis for geometrical attack on digital image watermarking," *International Journal of Electronics*, vol. 98, no. 11, pp. 1565–1580, 2011.

[49] C. Teh and R. Chin, "On image analysis by the methods of moments," *IEEE Transactions on Pattern Analysis and Machine Intelligence,*, vol. 10, no. 4, pp. 496–513, 1988.

[50] H. Liu, J. Rao, and X. Yao, "Feature based watermarking scheme for image authentication," in *IEEE International Conference on Multimedia and Expo, 2008*, pp. 229–232, IEEE, 2008.

[51] H. Liu, J. Lin, and J. Huang, "Image authentication using content based watermark," in *IEEE International Symposium on Circuits and Systems, 2005. ISCAS 2005.*, pp. 4014–4017, IEEE, 2005.