UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Authors full name : KHALID HASSAN MOHAMED EDRIS

Date of birth : 10th NOVEMBER 1977

Title : ROBUST IMAGE WATERMARKING TECHNIQUES USING IMAGE FEATURES

Academic Session : 2015/2016

I declare that this thesis is classified as:

☐ **CONFIDENTIAL** (Contains confidential information under the Official Secret Act 1972)*

☐ **RESTRICTED** (Contains restricted information as specified by the organization where research was done)*

☑ **OPEN ACCESS** I agree that my thesis to be published as online open access (Full text)

I acknowledge that University Malaysia Pahang reserve the right as follows:

1. The Thesis is the Property of University Malaysia Pahang.
2. The Library of University Malaysia Pahang has the right to make copies for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified By:

(Student's Signature) (Supervisor's Signature)

P02061304 PROFESSOR. DR. JASNI MOHAMAD ZAIN

New IC/Passport Number Name of Supervisor

Date: Date:

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 Doctor of Philosophy in Computer Science.

_____

Supervisor's Signature

Full Name : PROFESSOR.DR. JASNI MOHAMAD ZAIN

Position : PROFESSOR

Date :

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citation 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.

_____

Author's Signature

Name : KHALID HASSAN MOHAMED EDRIS

ID Number : PCC11008

Date :

ROBUST IMAGE WATERMARKING TECHNIQUES USING IMAGE FEATURES

KHALID HASSAN MOHAMED EDRIS

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Doctor of Philosophy in Computer Science

Faculty of Computer Systems & Software Engineering
UNIVERSITI MALAYSIA PAHANG

SEPTEMBER 2016

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AR	Accuracy Rate
BE-SIFT	Brief and Efficient Scale Invariant Feature Transform
CZMs	Complex Zernike Moments
DCT	Discrete Cosine Transform
DT-CWT	Dual-Tree Complex Wavelet Transform
DWT	Discrete Wavelets Transform
HVS	Human Visual System
ICA	Independent Component Analysis
IPR	Intellectual Property Right
JPEG	Joint Picture Expert Group
LCR	Local Circular Region
PSNR	Peak Signal-to-Noise Ratio
ROI	Region of Interest
RST	Rotation, Scaling, Translation
SIFT	Scale Invariant Feature Transform
SVD	Singular Value Decomposition
SVM	Support Vector Machine
TA	Trusted Authority
WPSNR	Weighted Peak Signal-to-Noise Ratio
ZMs	Zernike Moments

ROBUST IMAGE WATERMARKING TECHNIQUES USING IMAGE FEATURES

KHALID HASSAN MOHAMED EDRIS

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Doctor of Philosophy in Computer Science

Faculty of Computer Systems & Software Engineering
UNIVERSITI MALAYSIA PAHANG

SEPTEMBER 2016

ABSTRAK

Tesis ini menangani isu keteguhan imej tera air dalam menghadapi serangan terutamanya serangan geometri. Objektif kajian ini, memperbaiki keteguhan teknik watermarking berdasarkan kepada ciri-ciri imej setempat, dan mencadangkan teknik sifar tera air yang teguh mengikut ciri-ciri global imej. Untuk mendapatkan ciri setempat imej, ciri pengekstrak adalah sangat penting. Skim tera air yang telah ditambahbaik menggunapakai ciri pengekstrak yang lebih baik seperti Brief and Efficient Scale Invariant Feature Transform. Selain itu, ia turut menggunapakai ciri pengekstrak lain yang seperti kumpulan ekstrak sudut Harris, supaya ciri yang lebih kukuh dapat dipilih sekaligus meningkatkan tahap keteguhan tera air tersebut. Skim ini menggunakan dua teknik watermarking iaitu rantau pekeliling setempat dan blok kosinus diskret berubah, untuk menerapkan watermark kepada dua jenis kawasan dan mengekstraknya. Bagi terapan pada rantau pekeliling setempat, teknik Brief and Efficient Scale Invariant Feature Transform akan digunakan untuk mengekstrak ciri utama, dan rantau pekeliling setempat akan diperolehi. Akhir sekali, watermark tersebut diterap pada rantau pekeliling setempat menggunakan histogram. Untuk terapan ke dalam blok kosinus diskret berubah, kumpulan ekstrak sudut Harris mengekstrak ciri utama, kemudian imej ini dibahagikan kepada 80 × 80 blok tidak-bertindih untuk mencari blok calon, kemudian setiap blok calon dibahagikan kepada 8 × 8 sub-blok tidak-bertindih dan menerapkan tera air ke dalam komponen DC bagi setiap sub-blok menggunakan kekuatan berasaskan HVS. Untuk mengekstrak tera air dari Rantau Pekeliling Setempat, pertamanya, ciri utama BE-SIFT yang kukuh diekstrak, kemudian Rantau Pekeliling Setempat akan ditemui, dan diakhiri dengan mengira histogram setempat untuk mengekstrak watermark. Untuk mengekstrak tera air dari Blok DCT, pertama, kumpulan ekstrak sudut Harris yang mantap diekstrak. Kedua, Delaunay tessellation dan pemadanan segitiga digunakan untuk memulihkan imej yang diuji. Ketiga, imej yang diuji dibahagikan kepada 80 × 80 blok tidak- bertindih. Keempat, setiap blok dibahagikan kepada 8 × 8 sub-blok tidak- bertindih. Kelima, sub-blok tersebut diubah menjadi sub-blok DCT. Keenam, watermark diekstrak daripada nilai DC. Keputusan eksperimen menunjukkan bahawa skim yang telah ditambahbaik adalah lebih teguh terhadap pelbagai serangan. Khususnya, ia adalah lebih kukuh dalam menghadapi serangan geometri. Kaedah yang dicadangkan mempunyai prestasi 100% lebih baik dalam menentang serangan ke atas imej Lena dan Pepper, dan sekurang-kurangnya 84% prestasi yang lebih baik pada imej Barbara dan Plane berbanding dengan kaedah Deng, dan ia mempunyai prestasi 100% lebih baik berbanding kaedah lain. Di samping itu, skim sifar tera air yang kukuh berdasarkan ciri utama imej global menggunakan detik-detik Zernike kompleks adalah dicadangkan, kaedah ini menggunakan detik-detik Zernike kompleks, yang boleh memberikan keteguhan lebih baik terhadap serangan geometri dan menyediakan lebih banyak maklumat mengenai imej dan lebih banyak ruang untuk penerapan dan sifar watermarking. Sebelum mengira detik-detik Zernike kompleks, penterjemahan dan penskalaan imej yang diuji perlu dilaksanakan, selepas mendapat binarisasi nilai argumen, imej yang dipaparkan dibina dan operasi XOR dengan logo imej dilaksanakan untuk menjana imej pengesahan. Keputusan eksperimen menunjukkan bahawa skim yang dicadangkan sangat teguh dalam menghadapi pelbagai serangan terutama serangan geometri. Skim yang dicadangkan mempunyai prestasi sekurang-kurangnya 70% lebih baik dalam menentang serangan ke atas imej yang diuji berbanding dengan kaedah lain.

ABSTRACT

This thesis addresses the issue of image watermarking robustness against attacks and especially geometrical attacks. The objectives of this research were, improve robustness watermarking technique based on local image features, and propose robust zero watermarking technique according to the global features of image, To obtain the local feature of image, the feature points extractor is very important. The improved robustness watermarking scheme adopted better feature points extractions named Brief and Efficient Scale Invariant Feature Transform, also adopted another feature points extractions named grouping Harris corner, so they can choose more robust feature points, then increase the robustness of watermark. This scheme used two watermarking techniques, namely, local circular region and block discrete cosine transform, to embed the watermark into two types of regions and extract it. To embed in local circular region, Brief and Efficient Scale Invariant Feature Transform extracts feature points, and then Local Circular Regions for embedding are found, finally, the watermark is embedded into Local Circular Regions by using Histogram. To embed into block discrete cosine transform, grouping Harris corner extracts feature points, and then the image is divided into 80 × 80 non-overlapping block to find candidate blocks, then each candidate block is divided into 8×8 non-overlapping sub-blocks and embeds the watermark in the DC components of each sub-block using its HVS-based embedding strength. For extracting watermark from Local Circular Regions, firstly, robust BE-SIFT feature points is extracted, then, Local Circular Regions are found, finally, the local histogram is computed to extract the watermark. For extracting watermark from Block DCT, first, grouping robust Harris corner feature points is extracted. Second, Delaunay tessellation and triangle matching are applied to restore the probe image. Third, the probe image is divided into 80×80 non-overlapping blocks. Fourth, each block is divided into 8×8 non-overlapping sub-blocks. Fifth, any sub-block is transformed into DCT sub-block. Sixth, the watermark is extracted from DC values. The experimental results showed that the improved scheme is robust against a wide variety of attacks. In particular, it is more robust against geometric attacks. The proposed method has 100% good performance for resisting attacks on Lena and Pepper images, and at least 84% good performance on Barbara and Plane images compared with Deng's method, and it has 100% good performance compared with other methods. In addition, robust zero watermarking scheme based on global feature of image using complex Zernike moments is proposed, the contribution of this method is adopting complex Zernike moments, which can provide better robustness against geometric attacks and provide more information about image and more space for embedding and zero watermarking. Before calculating complex Zernike moments, standard translation and scaling of the tested image is performed, after getting the binarization of the argument value, the feature image is constructed and XOR operation with logo image is executed to generate verification image. Experimental results demonstrated that the proposed scheme has strong robustness to various attacks especially geometric attacks. The proposed scheme has at least 70% good performance of resisting attacks on tested images compared with the other methods.