OPTIMIZE PERCEPTUALITY OF DIGITAL IMAGE FROM ENCRYPTION BASED ON QUADTREE

HUSSEIN A. HUSSEIN

A thesis submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Science (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

JULY 2014

This thesis is dedicated to my family for their endless support and encouragement.

ACKNOWLEDGEMENT

First and foremost, I would like to express heartfelt gratitude to my supervisor **Prof. Dr. Dzulkifli Mohamed** for his constant support during my study at UTM. He inspired me greatly to work in this project. His willingness to motivate me contributed tremendously to our project. I have learned a lot from him and I am fortunate to have him as my mentor and supervisor

Besides, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities such as Computer laboratory to complete this project with software which I need during process.

ABSTRACT

Image compression is a large area of research. The objective of image compression is to reduce irrelevance and redundancy of the image data in order to be able to store or transmit data in an efficient form. There are so many problems in the digital grayscale encrypted image transferring over the internet, such as security level of encrypted image, the speed of internet, time of encrypted image transferring and so on. One of these problems is the insufficient of internet bandwidth that the encrypted image will transferred through it, so to solve the problem of insufficiently of internet bandwidth, the grayscale image will compressed by using quadtree fractal compression method before encrypting this image and transferring it via internet. Quadtree fractal compression method has advantage of high compression ratio but also has disadvantage with a long time of compression process which it effected on the decompressed image quality. In this thesis, we focused on quality problem of decompressed decrypted image, it is mean, how to improve quadtree fractal image compression to keep the image quality with reducing in compression time. So to solve this problem, the strength and limitations of current compression scheme has been investigated, design and develop new scheme that improved quality to overcome the limitation, and finally evaluate the new schemes using application scenarios. The proposed scheme improved the image quality by presenting improved quadtree fractal compression algorithm, which change the searching way for the best corresponding domain transformation and ranges, by dividing the image in to 3 self-similarity areas. Maximum and medium and minimum self-similarity areas. So the matching process had less time and better quality. The results shows that the proposed improved quadtree fractal compression get the best PSNR 37dB and compression ratio 35.9 and processing time with 65msc.

ABSTRAK

Pemampatan imej merupakan kawasan yang besar penyelidikan. Objektif pemampatan imej adalah untuk mengurangkan penyimpangan dan lebihan daripada data imej untuk dapat menyimpan atau menghantar data dalam bentuk yang cekap. Terdapat banyak masalah dalam imej skala kelabu digital yang disulitkan memindahkan melalui internet, seperti tahap keselamatan imej disulitkan, kelajuan internet, masa imej disulitkan memindahkan dan sebagainya. Salah satu masalah-masalah ini adalah tidak mencukupi jalur lebar internet yang imej disulitkan akan dipindahkan melaluinya, jadi untuk menyelesaikan masalah tidak cukup lebar jalur internet, imej skala kelabu akan dimampatkan dengan menggunakan kaedah mampatan fraktal quadtree sebelum menyulitkan imej ini dan memindahkan ia melalui internet . Kaedah pemampatan Quadtree fraktal mempunyai kelebihan nisbah mampatan yang tinggi tetapi juga mempunyai kelemahan dengan masa yang panjang proses pemampatan yang ia dilaksanakan pada kualiti imej didekompresi. Dalam tesis ini, kami memberi tumpuan kepada masalah kualiti imej dibuka didekompresi, adalah min, bagaimana untuk meningkatkan pemampatan imej quadtree fraktal untuk menjaga kualiti imej dengan mengurangkan dalam masa mampatan. Jadi untuk menyelesaikan masalah ini, kekuatan dan batasan skim mampatan semasa telah disiasat, reka bentuk dan membangunkan skim baru yang meningkatkan kualiti untuk mengatasi had, dan akhirnya menilai skim baru menggunakan senario permohonan. Skim yang dicadangkan baik kualiti imej yang lebih baik dengan mengemukakan quadtree algoritma pemampatan fraktal, yang mengubah cara pencarian yang terbaik transformasi domain sama dan julat, dengan membahagikan imej dalam 3 kawasan sendiri persamaan. Kawasan sendiri persamaan maksimum dan sederhana dan minimum. Jadi proses pemadanan mempunyai masa yang kurang dan lebih berkualiti. Keputusan menunjukkan bahawa quadtree baik mampatan fraktal yang dicadangkan mendapatkan yang terbaik PSNR 37dB dan nisbah mampatan 35.9 dan pemprosesan masa dengan 65msc.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xi
	LIST OF FIGURES	xii
1	**INTRODUCTION**	
	1.1 Introduction	1
	1.2 Problem Background	2
	1.3 Problem Statement	5
	1.4 Project Objectives	5
	1.5 Research Scope	6
	1.6 Thesis Organization	6
2	**LITERATURE REVIEW**	
	2.1 Introduction	8
	2.2 Data Security	8
	2.2.1 Data encryption	9
	2.3 Overview of Encryption	10
	2.4 The Necessity of Encryption	10
	2.5 Fundamental of Image Encryption	12
	2.5.1 Cipher	14

2.5.2 AES encryption 16
2.5.2.1 AES Transformations 17
2.5.2.2 Byte Substitution 17
2.5.2.3 Shift Rows 20
2.5.2.4 Mix Columns 20
2.5.2.5 Add Round Key 22
2.5.3 Key Expansion 23
2.5.4 AES Decryption 25
2.5.4.1 Inverse Add Round Key 25
2.5.4.2 Inverse Shift Row 25
2.5.4.3 Inverse Sub Bytes 26
2.5.4.4 Inverse Mix Column 26
2.6 Digital Image Encryption Literatures 27
2.6.1 Image Quality 27
2.7 Image Compression 29
2.7.1 Image Compression Definition 30
2.7.2 Different classes of compression techniques 30
2.7.2.1 Lossless vs. Lossy compression 30
2.7.2.2 Predictive vs. Transform coding 31
2.7.3 Typical Image Coder 31
2.7.3.1 Source Encoder (or Linear Transformer) 31
2.7.3.2 Quantizer 32
2.7.3.3 Entropy Encoder 32
2.8 Various Compression Algorithms 33
2.9 Quadtree Fractal Compression 34
2.10 Quality of the image 37
2.10.1 Measurement Performance of Quality in PSNR and SSIM 37

3 RESEARCH METHODOLOGY

3.1 Introduction 40
3.2 Research Framework 40
3.3 Methodology Phases 43

3.3.1 Phase 1: Initial Planning 43
3.3.2 Phase 2: Analysis 43
3.3.3 Phase 3 Designing and Implementing 44
3.4 Testing Performance 45
3.5 Research Environment 45
3.6 Data Set 46
3.7 Summary 48

4 DESIGN AND IMPLEMENTATION
4.1 Introduction 49
4.2 Notation 49
4.3 System Design 50
4.3.1 Quadtree Fractal Compression and Encrypting Procedure 50
4.3.1.1 Conventional Quadtree Fractal Compression 52
4.3.1.1.1 Step 1 : Determining Block Sizes of Domains and Ranges 52
4.3.1.1.2 Step 2 : Partitioning Image in to Ranges and Domains 52
4.3.1.1.3 Step 3 : Calculating Transformation for Domains 53
4.3.1.1.4 Step 4 : Matching Process 54
4.3.1.2 Improved Quadtree Fractal Compression 54
4.3.1.3 AES encryption 57
4.3.2 Decryption and Decompression Procedure 57
4.3.2.1 AES Decryption 58
4.3.2.2 Quadtree Fractal Decompression 59
4.3.2.2.1 Step 1 : Invers Matching Process 60
4.3.2.2.2 Step 2 : De-partitioning Image 60

5 RESULTS ANALYSIS AND DISCUSSION

5.1 Introduction 61

5.2 Compressing and Encryption procedure 61

5.3 Decryption and Decompress Procedure 62

5.4 Requirements Unit 62

5.5 Tested Images 63

5.6 Relation between Compression Ratio and PSNR 63

5.7 Quality of Decompressed image 64

5.7.1 Analysis on Error Limit and Quality for Decompressed Images 65

5.8 Comparative Study 65

6 CONCLUSION

6.1 Introduction 67

6.2 Conclusion 68

6.3 Research Contribution 68

6.4 Future Work 69

REFERENCES 70

LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	A comparison of symmetric and asymmetric algorithms (Azzedine Boukerche, et al. 2010)	12
2.2	Various fractal image techniques with the value of PSNR for difference image size	39
3.1	Selected Samples Of The Images From The Data Set	47
4.1	Notation of proposed scheme	49
5.1	Results of the Improved Image Compression Algorithm Allow the Error Limit 0.5	63
5.2	Results of the Improved Image Compression Algorithm Allow the Error Limit 0.2	64
5.3	Obtained PSNR for various images for different error limits	65
5.4	Comparison of Quality (PSNR) between Available and Proposed Scheme	66

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
2.1	The general scheme of a cryptosystem	13
2.2	The general scheme of operation of a symmetric cipher	14
2.3	AES Encryption Flow-diagram	16
2.4	Bytesub Transformation	17
2.5	S-box for Bytesub operation	19
2.6	S-box for inverse Bytesub operation	19
2.7	Shift-Rows operation	20
2.8	Illustrates the mix column transformation	21
2.9	Add Round Key operation	22
2.10	Invers Sub Bytes operation	26
2.11	The series of decoded Lena with size 512 × 512 at different received data rate using the proposed scheme.	36
3.1	Research Framework (Compressing-Encrypting phase)	41
3.2	Research Framework (Decrypting-Decompressing phase)	42
4.1	Compression and Encryption Procedure	51
4.2	The scale transformations for one of domain blocks	53
4.3	The Offset Transformations for one of domain blocks	53
4.4	The (A,B,C) same-similarity areas of Lenna Image	56
4.5	Decryption and Decompression procedure	58
4.6	AES Decryption	59

CHAPTER 1

INTRODUCTION

1.1 Introduction

With the rapid development of internet technology and information processing technology, the image is transmitted commonly online. People enjoy the convenience and shortcut, but people have to face a premonition that the information is important in the transfer of the image, which is easily intercepted by unknown persons or hackers. In order to enhance the security of the image information, encryption becomes an important research direction of image (Christof Paar, 2009).

Image compression is a large area of research. The objective of image compression is to reduce irrelevance and redundancy of the image data in order to be able to store or transmit data in an efficient form. Image compression may be lossy or lossless. Lossless compression is preferred for archival purposes and often for medical imaging, technical drawings, clip art, or comics. Lossy compression methods, especially when used at low bit rates, introduce compression artifacts. Lossy methods are especially suitable for natural images such as photographs in applications where minor (sometimes imperceptible) loss of fidelity is acceptable to achieve a substantial reduction in bit rate. The lossy compression that produces imperceptible differences may be called visually lossless (Dhawan S, 2011).

Large amount of image data is transmitted over internet, which raises the issue of how to efficiently compress the transmitted image. The goal of image compression is to represent an image with as few numbers of bits as possible while/ keeping the quality of the original image. Fractal compression approach has been widely used because of its high compression ratio. However, conventional fractal compression approach needs more time to code the original image. In order to reduce encoding time, an improved fractal image coding algorithm based on the quadtree scheme is proposed in this paper. This fractal image compression coding algorithm will dramatically decrease encoding time in an image compression (Hongtao Hu, 2012).

Confidential communication has long been a common practice in the social life. However as information can be communicated electronically, it is exposed in the public domain and unavoidably resulted in interceptions. A scientific approach to respond the demands on achieving the sense of security is cryptography. The term cryptosystem, also called cipher, is often used in cryptography. Intuitively, its meaning is clear enough which refers to an encryption system. The central idea of encryption is to transform the message in which its original information can only be reconstructed by a designated recipient (Kumar, Mishra et al., 2014).

1.2 Problem Background

A novel scheme of compressing encrypted images with auxiliary information was proposed by (Xinpeng Zhang *et al.*, 2014). The content owner encrypts the original uncompressed images and also generates some auxiliary information, which will be used for data compression and image reconstruction. Then, the channel provider who cannot access the original content may compress the encrypted data by a quantization method with optimal parameters that are derived from a part of auxiliary information and a compression ratio-distortion criteria, and transmit the compressed data, which include an encrypted sub-image, the quantized data, the quantization parameters and another part of auxiliary information. At receiver side, the principal image content can be reconstructed using the compressed encrypted

data and the secret key. Experimental result shows the ratio-distortion performance of the proposed scheme is better than that of previous techniques.

The goal of image compression is to represent an image with as few number of bits as possible while keeping the quality of the original image. With the characteristics of higher compression ratio, fractal image coding has received much attention recently. However, conventional fractal compression approach needs more time to code the original image. In order to overcome the time-consuming issue, a Quadtree-based partitioning and matching scheme is proposed by (Hongtao Hu *et al*., 2012).

During the partitioning phase, an image frame is partitioned into tree-structural segments. And during a matching phase, a rang block only searches its corresponding domain block around previous matched domain block. Such local matching procedures will not stop until a predefined matching threshold is obtained. (Hongtao Hu *et al.*, 2012).

The preliminary experimental results show that such sub-matching rather than a global matching scheme dramatically decreases the matching complexity, while preserving the quality of an approximate image to the original after decoding process. In particular, the proposed scheme improves the coding process up to 2 times against the conventional fractal image coding approach. (Hongtao Hu *et al*., 2012).

With high compression ratio performance, fractal image compression technology becomes a hot topic of research of image compression techniques. However, the encoding time of traditional fractal compression technique is too long to achieve real-time image compression, so it cannot be widely used. Based on the theory of fractal image compression, (Hui Yu *et al*., 2010) raised an improved algorithm on quadtree fractal encoding is raised up: during the search of best matching domain block, search it in the area centered on last best matching one. form the aspect of image segmentation.

A way of improvement of compression ratio of fractal image compression is proposed by (Utpal Nandi *et al.,* 2014). The improvement of compression rates is done by applying the lossless compression techniques on the parameters of the affine transformations of the fractal compressed images. The Modified Region Based Huffman and its variant are used for this purpose. The PSNR of images are remained same. The comparison of the compression ratio and time are done between fractal image compression with quardtree partitioning schemes, the same with Huffman coding and its proposed improved versions. The proposed improved fractal image compression techniques offer better compression rates most of the times keeping the PSNRs unchanged. But, the compression time of proposed techniques are significantly increased than its counterparts.

(Ching Hung Yuen *et al.,* 2013) suggested a hybrid quadtree fractal image coding scheme based on traditional and no-search fractal image coding with the proposed progressive structure to solve the image quality problem. Simulation results show that its image quality at different received data rates is better than that without considering the quadtree level.

Quadtree fractal compression is a lossy compression method for digital images, based on fractals. The method is best suited for textures and natural images, relying on the fact that parts of an image often resemble other parts of the same image. Fractal algorithms convert these parts into mathematical data called "fractal codes" which are used to recreate the encoded image (Gaganpreet Kaur *et al.,* 2013).

Fractal image coding based on quadtree is a novel technique for still image compression. Compared with other image compression methods, fractal image coding has the advantage of higher compression ratio, higher decoding speed and decoded image having nothing to do with the resolution of image. However, it spends too much time to look for the best matching Ri block on encoding. To improve the encoding speed, the search range must narrow and improve the search skills to ensure the best match block falls within the range. An improved fractal

image compression algorithm based on quadtree is proposed by (Bohong Liu *et al.*, 2010).

First, improve the construction method of search attractor by constructing directly from the big Di block, so it can save a lot of searching time in encoding. Second, the attractors can be self-constructed, so it is not happened that the attractor is not found in the traditional methods. Experimental result shows that the algorithm makes image coding faster and more efficiency.

1.3 Problem Statement

There are so many problems in the digital grayscale encrypted image transferring over the internet, such as security level of encrypted image, the speed of internet, time of encrypted image transferring and so on. One of these problems is the insufficient of internet bandwidth that the encrypted image will transferred through it, so to solve the problem of insufficiently of internet bandwidth, the grayscale image will compressed by using quadtree fractal compression method before encrypting this image and transferring it via internet. Quadtree fractal compression method has advantage of high compression ratio but also has disadvantage with a long time of compression process which it effected on the decompressed image quality. In this thesis, we focused on quality problem of decompressed decrypted image, it is mean, how to improve quadtree fractal image compression to keep the image quality with reducing in compression time.

1.4 Project Objectives

Following are objectives to be achieved:

The following objectives were attempted to be achieved in this research:

(i) To investigate the strength and limitations of current compression scheme.
(ii) To design and develop new scheme that improved quality to overcome the limitation.
(iii) To evaluate the new schemes using application scenarios.

1.5 Research Scope

in this thesis, we mainly consider digital image watermarking schemes, below are the scopes of images watermarking project:

(i) Standard testing data set and camera snapshot of images will be used to test the scheme for quality of encryption image.
(ii) The standard hosts images with size 512×512, 256×256, 128×128 will be in grayscale format are used as test data.
(iii) Proposed scheme is implemented using MATLAB program to illustrate the main idea involved in encryption scheme.

1.6 Thesis Organization

This research is organized in six chapters, as shown below. Chapter 1 discusses the introduction. Chapter 2 reviews the literature and provides a background on fractal compression. The research methodology is explained in Chapter 3, which covers the research procedure, data and proposed algorithms. Chapter 4 discuss the design and implementation of the proposed algorithm, Chapter

5 contains the experimental results of the proposed method and discussion, while the conclusions and recommendations are in Chapter 6.

REFERENCES

Acharya, B., Panigrahy, S. K., Patra, S. K., & Panda, G. 2010 . Image encryption using advanced hill cipher algorithm. *Aceee International Journal on signal & Image processing*, 1 1 .

Boukerche, A., Ren, Y., & Mokdad, L. 2010, October . Applying symmetric and asymmetric key algorithms for the security in wireless networks: proof of correctness. In Proceedings of the 6th ACM workshop on QoS and security for wireless and mobile networks pp. 33-40 . ACM.

Choudhary, N. Y., & Gupta, R. Effectiveness and Performance of Image Encryption Techniques: A Survey.

Dhawan, S. 2011 . A review of image compression and comparison of its algorithms. International Journal of Electronics & Communication Technology, *IJECT, 2*.

Hu, H. T., & Liu, Q. F. 2012 . Improvement of Fractal Image Compression Coding Based on Quadtree. *Advanced Materials Research, 532, 1157-1161*.

Jain, A., Tiwari, N., & Shandilya, M. Image Based Encryption Techniques: A Review.

Kaur, G., & Kaur, M. Fractal Image Compression using Soft Computing.

Kwok, H. S., & Tang, W. K. 2007 . A fast image encryption system based on chaotic maps with finite precision representation. *Chaos, solitons & fractals, 32 4 , 1518-1529.*

Liu, B., & Yan, Y. 2010, October . An improved fractal image coding based on the quadtree. *In Image and Signal Processing CISP , 2010 3rd International Congress on Vol. 2, pp. 529-532 . IEEE.*

Liu, Z., Xu, L., Liu, T., Chen, H., Li, P., Lin, C., & Liu, S. 2011 . Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. *Optics Communications, 284 1 , 123-128*.

Mir, J., & Raja, G. 2012 . Quad tree fractal compression for brain MRI images. *Nucleus, 49 1 , 21-27*.

Nandi, U., & Mandal, J. K. 2014, February . Fractal image compression by using loss-less encoding on the parameters of affine transforms. *In Automation, Control, Energy and Systems ACES , 2014 First International Conference on pp. 1-6 . IEEE.*

Nat Queen 2001, Modern Cryptography. PGP and security utilities for RISC OS, *Queen clara website.*

Olanrewaju, R. F., Khalifa, O. O., Hashim, A. H., Zeki, A. M., & Aburas, A. A. 2011 . Forgery Detection in Medical Images Using Complex Valued Neural Network CVNN . *Australian Journal of Basic and Applied Sciences, 5 7 , 1251-1264.*

Preneel, B., Paar, C., & Pelzl, J. 2009 . Understanding cryptography: a textbook for students and practitioners. *Springer.*

Sreeda Perikamana., 2013 . Image Encryption Using AES Key Expansion. Seminar Report. *Scribd website.*

Sultana, R., Ahmed, N., & Basha, S. M. 2011 . Advanced Fractal Image Coding Based on the Quadtree. *Computer Engineering and Intelligent Systems, 2 3 , 129-136.*

Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. 2004 . Image quality assessment: from error visibility to structural similarity. *Image Processing, IEEE Transactions on, 13 4 , 600-612.*

Yu, H., Li, L., Liu, D., Zhai, H., & Dong, X. 2010 . Based on Quadtree Fractal Image Compression Improved Algorithm for Research. *In 2010 International Conference on E-Product E-Service and E-Entertainment pp. 1-3 .*

Yuen, C. H., Lui, O. Y., & Wong, K. W. 2013 . Hybrid fractal image coding with quadtree-based progressive structure. *Journal of Visual Communication and Image Representation, 24 8 , 1328-1341.*

Zhang, X., Ren, Y., Shen, L., Qian, Z., & Feng, G. Compressing Encrypted Images with Auxiliary Information.

Zhang, Y., Yang, Q., Yang, C., & Zhang, Q. 2012, May . A universal entropy masking model in digital watermarking system. *In Fuzzy Systems and Knowledge Discovery FSKD , 2012 9th International Conference on pp. 2875-2878 . IEEE.*

Zhu, C. 2012 . A novel image encryption scheme based on improved hyperchaotic sequences. *Optics Communications, 285 1 , 29-37.*

Zhu, H., Zhao, C., & Zhang, X. 2013 . A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem. *Signal Processing: Image Communication, 28 6 , 670-680*.

Zizzi, S. 2001 . U.S. Patent No. 6,185,681. Washington, DC: U.S. Patent and Trademark Office.