IMAGE COMPRESSION AND ENCRYPTION

ZUHAIRIAH BINTI ZAINAL ABIDIN

A thesis submitted as a partial fulfillment of requirements for the award of the Degree of Master of Engineering (Electrical)

Electrical Engineering Department
Kolej Universiti Teknologi Tun Hussein Onn

November 2003

Dedicated to:

Ayah, Ibu, K. Long and B. Long, K. Ngah and B. Ngah, Uda and Akak, Imran, Farzana, Raffissa, Zakwan, and Abang for giving me an unconditional love and caring.....

ACKNOWLEDGEMENT

I would like to take the opportunity to thank the All Mighty God, Allah, which with His bless; I managed to complete this thesis.

In this spirit, it is a pleasure for me to record the many archival and intellectual debts that I have accumulated while completing this thesis. To put everyone name on the list is an impossible job. However, I would like to name some of them whom I am deeply indebted.

Firstly, I would like to thank my respectful supervisor, Prof. Dr. Hashim B. Saim for the advices that have helped me in completing this project. Secondly, I would like to express my appreciation for the support and ideas that have been given to me by Assoc. Prof Dr. Syed Abdul Rahman Syed Abu Bakar and lastly, I am deeply thankful to my mother and father whose unconditional love and pride have nurtured my education and accomplishment in life.

ABSTRACT

Uncompressed multimedia data (image) requires considerable storage capacity. However, all classified image file, has to be protected against unauthorized access. The purpose of this project was to implement the combinational of image compression and encryption to overcome this problem. In this project, the image compression process involved the usage of the wavelet transform. Eight images have been used in this project for its implementation. The original image was decomposed until ten levels of decomposition by using Daubechies2 (db2). The aforementioned was recursively done from Daubechies2 (db2) to Daubechies10 (db10). After the decomposition stage, the image that performs optimum percentage of coefficients was suppressed to zero (PERF0) and the percentage of perfect reconstruction (PERFL2) is chosen. Thereafter, the chosen image was compressed and finally, encrypted. In this project, the RC4 encryption algorithm has been used. This project utilized MATLAB Wavelet Toolbox Version 6.5 thoroughly for its implementation. The output of the image compression and encryption was then be analyzed by using mean-square error (MSE), peak signal to noise ratio (PSNR), percentage of coefficients suppressed to zero (PERF0) and percentage of perfect reconstruction (PERFL2).

ABSTARK

Data multimedia (imej) yang tidak dimampatkan memerlukan kapasiti storan yang amat besar. Namun begitu, fail imej yang sulit perlu dilindungi daripada capaian oleh pihak yang tidak berkenaan. Tujuan projek ini adalah untuk pelaksanakan penggabungan imej mampatan dan kod rahsia *(encryption)* bagi mengatasi pemasalahan tersebut. Dalam projek ini, proses pemampatan imej melibatkan penggunaan penjelmaan anak gelombang (*wavelet*). Lapan imej digunakan dalam melaksanakan projek ini. Imej asal telah diurai sehingga 10 aras penguraian dengan menggunakan Daubechies2 (db2). Proses penguraian ini berterusan sehingga Daubechies10 (db10). Selepas proses penguraian dilakukan, imej yang memberikan nilai PERF0 dan PERFL2 yang optimum dipilih dan imej ini dimampatkan dan seterusnya dikod rahsiakan. Di dalam projek ini, algoritma kod rahsia RC4 digunakan. Bagi pelaksanakan keseluruhan projek ini, MATLAB *Wavelet Toolbox* versi 6.5 digunakan. Keluaran bagi imej mampatan dan kod rahsia dianalisa dengan menggunakan ralat min kuasa dua (MSE), nisbah isyarat puncak berbanding hingar (PSNR), *percentage of coefficients suppressed to zero* (PERF0) dan *percentage of perfect reconstruction* (PERFL2).

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

dB	-	Decibels
db	-	Daubechies Wavelet
ω	-	Wavelet Coefficients
$x(t)$	-	Time - domain
$X(f)$	-	Frequency - Domain
a_0, a_n, b_n	-	Fourier Coefficients
$f(t)$	-	Time of the signal
t	-	Time
f	-	Frequency
π	-	pi
ψ	-	Mother Wavelet
$\hat{\psi}$	-	Fourier Transform of ψ
c_ψ	-	Admissibility Constant
$\psi(x)$	-	Wavelet Functions
$\phi(x)$	-	Scaling Function
ϖ	-	Overall transform coefficients
M	-	Peak to peak value of the original image
σ_{ms}	-	Mean square error

LIST OF ABBREVIATIONS

DWT	-	Discrete Wavelet Transform
DCT	-	Discrete Cosine Transform
MSE	-	Mean Square Error
PSNR	-	Peak Signal to Noise Ratio
JPEG	-	Joint Photographic Experts Group
MPEG	-	Moving Pictures Experts Group
ISDN	-	Integrated Services Digital Network
CPU	-	Central Processing Unit
RC4	-	Ron' Code # 4
PERF0	-	Percentage of Coefficients Suppressed to Zero
PERFL2	-	Percentage of Perfect Reconstruction
DFT	-	Discrete Fourier Transform
VQ	-	Vector Quantization
KLT	-	Karhunen-Loeve Transform
STFT	-	Short Time Fourier Transform
FAX	-	Facsimile Transmission
LPF_D	-	Decomposition Low Pass Filter
HPF_D	-	Decomposition High Pass Filter
LPF_R	-	Reconstruction Low Pass Filter
HPF_R	-	Reconstruction High Pass Filter
LPF	-	Low Pass Filter
HPF	-	High Pass Filter
GIF	-	Graphical Interchange Format

BMP	-	MS Windows Format
TIFF	-	Tagged Image File Format
RGB	-	Red – Green - Blue
cD	-	Diagonal coefficients
cA	-	Approximation coefficients
cH	-	Horizontal coefficients
cV	-	Vertical coefficients

LIST OF APPENDICES

CHAPTER I

INTRODUCTION

1.1 Background of the Problem

Image compression is used to minimize the amount of memory needed to represent an image. As one of the enabling technologies of the multimedia revolution, image compression is a key to rapid progress being made in information technology. It would not be practical to put images alone on website without compression [1]

What is image compression? And why do we need it? Many people may have heard of JPEG (Joint Photographic Experts Group) and MPEG (Moving Pictures Experts Group), which are standards for representing images and video. Image compression algorithms are used in those standards to reduce the number of bits required to represent an image or a video sequence. Compression is the process of representing information in a compact form. Image compression treats information in digital form that is, as binary numbers represented by bytes of data with very large data sets. Fox example, a single small 400 × 400 size color picture, scanned at 300 dots per inch (dpi) with 24 bits/pixel of true color, will produce a file containing more than 4 megabytes of data. At least three floppy disks are required to store such a picture. This picture requires more than one minute for transmission by a typical transmission line (64k bit/second ISDN). That is why large image files remain a major bottleneck in a distributed environment. Although increasing the bandwidth is a possible solution, the relatively high cost makes this less attractive. Therefore, compression is a necessary and essential method for creating image files with manageable and transmittable size.

The need for security in transferring data from one point to another requires the additional algorithms to the compression algorithms, which encrypt the data. In medicine, this problem of loosing performance in encrypting images that has to be transferred produces a conflict. The problem arises through the constraints of the physician, i.e. radiologist, which do not allow them to separate from patient data. Therefore, a protection of the image against unauthorized access must be made to protect the confidentiality of information when it must reside or be transmitted through otherwise unsafe environments [2].

1.2 Problem Statement

It has been suggested that a picture is worth a thousand words. This is all the more true in the modern era in which information has become one of the most valued of assets. Recent technology has introduced the paradigm of digital information and its associated benefits and drawbacks. When the time comes to store a photograph digitally, its worth is put to the test. A thousand words stored on a digital computer require very little capacity, but a single picture can require much more. A thousand pictures can require a very large amount of storage. While the advancement of computer storage technology continues at a rapid pace, a means for reducing the storage requirements of an image is still needed in most situations. Thus the science of digital image compression has emerged. Current methods of image compression, such as the popular Joint Photographic Experts Group (JPEG) standard, can provide good performance in terms of retaining image quality while reducing storage requirements. But even the popular standards like JPEG have limitations. Research in new and better methods of image compression is ongoing, and recent results suggest that some newer techniques may provide much greater performance than those developed just five years ago [3].

Compression aids encryption by reducing the redundancy of the file. Nearly all implemented encoding schemes, unless they have been designed with cryptography in mind, produce output that actually starts off with high redundancy. For example, the output of UNIX compress begins with a well known three byte "magic number". This produces a field of "known plaintext" which can be used for some forms of cryptanalytic attack. This encoding is generally of value, however, because it removes other known plaintext in the middle of the file being encrypted. In general, the lower the redundancy of the plaintext being fed an encryption algorithm, the more difficult the cryptanalysis of that algorithm [4].

In addition, the compression scheme shortens the input file, which shortens the output file and reduces the amount of Central Processing Unit (CPU) required to do the encryption algorithm, so even if there were no enhancement of security, compression before encryption would be worthwhile.

Compression after encryption is silly. If an encryption algorithm is good, it will produce output which is statistically indistinguishable from random numbers and no compression algorithm will considerably compress random numbers. On the other hand, if a compression algorithm succeeds in finding a pattern to compress out of an encryption's output, then a flaw in that algorithm has been found. In the majority of encryption utilities the data is first compressed before it is actually encrypted [4].

This study intends to implement a combinational of image compression and encryption. This study is concerned with a compression that uses wavelets. Wavelets, introduced by J. Morlet [5], are used to characterize a complex pattern as a series of simple patterns and coefficients that, when multiplied and summed, reproduce the original pattern. Meanwhile for encryption, the RC4 encryption algorithm is been used. Although RC4 is not the latest technology, but for this study the author intends to show

how the RC4 works in practice. According to Peter Meyer [6], the schemes are suitable for encryption of the original data or image, but in this study, the author tried to apply the encryption into the image compression. We also intend to show to the readers how the image compression and encryption works in practice.

1.3 Purpose of the Study

Briefly, this study has two main purposes:

i) Development of a wavelet-based image compression program using MATLAB Wavelet Toolbox 6.5
ii) Implement RC4 encryption algorithm into the wavelet-based image compression program

1.4 Scope of the Study

The scope of this study is the development of a wavelet-based image compression program using MATLAB Wavelet Toolbox 6.5 and the implementation of the RC4 encryption algorithm into the wavelet- based image compression program. To achieve this study, the author studied on RGB and gray-scale image, image compression and encryption methods. The results of this study will be qualitatively evaluated in peak signal to noise ratio (PSNR), mean square error (MSE), percentage of coefficients suppressed to zero (PERF0) and percentage of perfect reconstruction (PERFL2).

1.5 Outline of the Thesis.

This thesis is divided into 6 chapters, including:

Chapter 1	Overview of the project; background of the problem, problem statement, objectives and scope of the study.
Chapter 2	Literature review that outlines the groundwork of this study. A reviews on previous research related on image compression and encryption techniques.
Chapter 3	The theoretical background of image compression, wavelet and encryption.
Chapter 4	Description of project methodology.
Chapter 5	Presents the simulated results on image compression and encryption and discussion of the results.
Chapter 6	Conclude and summarizes the main finding of the study, along with ideas about the work needed for future direction of the study.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

From literature that has been reviewed, image compression and encryption is an ongoing research [4]. Researchers always make an improvement on image compression and encryption schemes to make these schemes more effective and computationally simple technique. Summaries of the image compression and encryption are described here.

2.2 Research Related to Image Compression Algorithm

(a) Discrete Cosine Transform

In 1974, Ahmed, N et al. [7] has discovered Discrete Cosine Transform (DCT) and it is an important achievement for the research community working on image compression. The DCT can be regarded as a discrete-time version of the Fourier-Cosine series. It is a close relative of Discrete Fourier Transform (DFT), a technique for converting a signal into elementary frequency components. An excellent analysis of

DCT and related transforms and their applications has been described by Tsai et al. [8]. In principle, the DCT introduces no loss to the source image samples; it merely transforms them to a domain in which they can be more efficiently encoded.

(b) Image Coding Using Wavelet Transform

Marc Antonini et al. [9] proposed the new scheme for image compression taking account pyschovisual features both in the space and frequency domains. This scheme combines the wavelet transforms and vector quantization (VQ). The wavelet transform used here attempts to exploit the masking effect of human eye, yielding encouraging results. The proposed method enables high compression bit rates while maintaining good visual quality.

(c) Image Compression Using the 2-D Wavelet Transform

In April 1992, Lewis and Knowles [10] have introduced the new approach to image compression based on wavelet transform. Through this approach, they achieved better compression than other standard subband coding methods. They also recovered that the errors introduced by their method is less visually annoying than for DCT compressed image due to the lack of blocking effects.

(d) Finding a Suitable Wavelet for Image Compression Applications

In this paper, Shahid Masud et al. [11] assess the relative merits of various types of wavelet functions for use in a wide range of image compression scenarios. They have delineated different algorithmic criteria that can be used for wavelet evaluation. The assessment undertaken includes both algorithmic aspects (fidelity, perceptual quality) as well as suitability for real-time implementation in hardware. Through a series of different tests they have quantitatively evaluated the suitability of different wavelets for use in image compression systems. The result indicates that the compression performance of biorthogonal filters appear to be well suited to the real-time image compression systems. However, in terms of statistical measures, the Daubechies filters perform better.

(e) Wavelet-based lossless compression of coronary angiographic images

The final diagnosis in coronary angiographic has to be performed on large set of original image. Therefore, lossless compression schemes play a key role in medical database management and telediagnosis applications. This paper proposes a wavelet-based compression scheme that is able to operate in the lossless mode. The quantization module implements a new way of coding of the wavelet coefficients that is more effective than the classical zerotree coding. The experimental results obtained on a set of 20 angiograms show that the algorithm outperforms the embedded zerotree coder, combined with the integer wavelet transform, by 0.38 bpp, the set partitioning coder by 0.21 bpp, and the lossless JPEG coder by 0.71 bpp. The scheme is a good candidate for radiological applications such as teleradiology and picture archiving and communications system (PACS's) [12].

(f) Orthogonal Transforms

Karhunen-Loeve Transform (KLT) is the optimal transform. It decorrelates the input data to the maximum possible extent. Based on the result in this project report, it shows that the KLT perform better compression than the DCT but KLT is not a practical transform as it is very slow on account of a large number of time-consuming matrix operations. It also requires large amounts of memory. [13].

REFERENCES

1. Xiao, P. (2001). "Image Compression By Wavelet Transform". East Tennessee State University: Master Thesis

2. Vorwerk, L., Engel, T. and Meinel, C. (2001). "Proposal for a combination of compression and encryption". Proceedings of SPIE – The International Society for Optical Engineering, Visual Communications and Image Processing

3. Martin, M. B. (1999). "Applications of Multiwavelets to Image Compression". Master Thesis - Virginia Polytechnic Institute and State University (Virginia Tech)

4. Hauter, A., Chacko, M.V., Ramanathan, R. (1995). "Compression and Encryption". CSI 801 Project Fall 1995

5. Morlet, J. (1983). "Sampling Theory and Wave Propagation". NATO ASI Series Vol. 1, Issues in Acoustic Signal/Image Processing and Recognition, Berlin. pp 233-261

6. Meyer P. (1994). "An Introduction to the use of Encryption". Found at http://serendipity.magnet.ch/hermetic/crypto/me5.htm

7. Ahmed, N., Natarajan, T., and Rao, K. R. (1974). "Discrete Cosine Transform". IEEE Trans. Computers, Vol. C-23, Jan. pp. 90-93

8. Tsai, M. J., Villasenor, J. D., and Chen, F. Stack (1996)."Run Image Coding". *IEEE Trans.CSVT, Vol. 6, No. 5, Oct., pp. 519-52,* http://www.icsl.ucla.edu/~ipl/papers/stack_run.html

9. Antonini, M., Barlaud M., Mathieu, P. and Daubechies, I. (1992). "Image Coding Using Wavelet Transform". IEEE Transaction on Image Processing Vol. 1. No. 2, April pp 205-220

10. Lewis, A.S and Knowles, G. (1992). "Image Compression Using the 2-D Wavelet Transform". IEEE Transaction on Image Processing Vol. 1. No. 2, April pp 244-250

11. Shahid Masud and Mc Canny. J. V. "Finding a Suitable Wavelet for Image Compression Applications". DSiP Laboratories, School of Electrical Engineering and Computer Science, The Queen's University of Belfast, Stranmillis Road, BT9 5AH, N. Ireland

12. Munteanu, A., Cornelis, J. and Cristea, P. (1999)."Wavelet-based lossless compression of coronary angiographic images". IEEE - Transactions – on Medical – Imaging. Vol. 18, No. 3, March pp 272-281

13. Bray, M. and Chappalli, M.B (2001)." Orthogonal Transforms". Computer Project Report 5. CSE/EE 485: Digital Image Processing I

14. Cheng, H. and Li, X. (2000). "Paertial Encryption of Compressed Images and Videos". IEEE Transactions on Signal Processing. Vol. 48. No. 8, pp 2439-2451

15. Rivest, R., Shamir, A. and Adleman, L. (1978). "A method for obtaining digital signatures and public key cryptosystems". Communication ACM, Vol. 21. No. 2, pp 120-126

16. Jones, D. (1998). "Applications of splay trees to data compression". Communication ACM. August, pp 996-1007

17. Huffman, D. A. (1952)."A method for the construction of minimum-redundancy codes". Proceeding IRE, Vol. 40, No. 2, pp 1098-1101

18. Witten, I. H., Neal, R. and Cleary, J. C. (1987). "Arithmetic coding for data compression". Communication ACM, Vol 30, pp 520-540

19. Bourbakis, N. and Alexopoulos, c. (1992). "Picture Data encryption using SCAN patterns". Pattern Recognition. Vol. 25, No. 6, pp 567-581

20. Chang, H.K-C and Liu, J-L (1997). "A linear quadtree compression scheme for image encryption". Signal Processing Image Communication. Vol. 10, No. 4, pp 279-290

21 Gonzalez, R. C., Richard E. Woods (2001)."Digital Signal Processing". Second Edition: Prentice Hall.

22. Sonka, M. Hiaual, V. Boyle, R. Image Processing, Analysis and Machine Vision, 2nd edition. Brooks/Cole Publishing Company

23. Project report "Application of wavelets to image compression" Found at http://www.ouray.cudenver.edu/~mbhatia/Project

24. Ramirez, R.W. (1995)."The FFT: Fundamentals and Concepts". New Jersey: Prentice-Hall, Inc

25. Sarkar, T.K and Su, C. (1998). "A Tutorial on Wavelets from an Electrical Engineering Perspective, Part 2: The Continuous Case". IEEE Antennas and Propagation Magazine. Vol. 40. No. 6. pp. 36-49.

26. Ahmed, M. D. and Jain, A. K. (1998). "A Rule Based Approach for Visual Pattern Inspection". IEEE Transaction of Pattern Analysis and Machine Intelligence. vol. PAMI-10, No. 1, pp 56-58

27. Rao, R. L (1995). "Multiresolution Techniques in Image Processing". Louisiana State University: PhD Thesis

28. Mallat, S. (1996). "Wavelet for a Vision". Proceedings of IEEE: Special Issue on Wavelets. Vol. 84 No. 4 pp 604-614

29. Misiti, M., Misiti, Y., Oppenheim, G. and Poggi, J.M. (1997). "Wavelet Toolbox for use with MATLAB". The MathWorks Inc. Englewood Cliffs, N.J: Prentice Hall. 6.84, 6.85, 6.23-6.26

30. RC4 Encryption Algorithm. Found at http://www.ncat.edu/~grogans

31. Donoho D. and Johnstone I. (1995). "Adapting to unknown smoothness via Wavelet Shrinkage". J. Amer Statistical Assoc. 1995

32. Ishak Ismail and Lu Wei (1994). "Wavelet Transform and Image coding". Proceedings of Malaysia Science and Technology Congress '94. Vol:1. Information Technology, Robotics & Telecommunications, Confederation of Scientific and Technological Associations in Malaysia (COSTAM). Kuala Lumpur. 221-230

33. Lees, K. (2002). "Image Compression using Wavelets". Master Thesis