OWNERSHIP AUTHENTICATION BY DIGITAL IMAGE WATERMARKING BASED ON BLOCK TRUNCATION CODING

FARANAK TOHIDI

A thesis submitted in partial fulfillment of

the requirements for the award of the degree of

Master of Computer Science (Information Security)

Advanced Informatics School

Universiti Teknologi Malaysia

December 2012

ABSTRACT

Image authentication methods have recently gained great consideration due to their importance for a huge number of multimedia applications. Digital images are increasingly conveyed over vulnerable channels such as the Internet. Protecting digital product is going to become important issue to ensure the secure transmission of the digital items. The existing algorithms cannot guarantee the whole security of the contents or ownership verification. The embedded watermark or data hiding into image can be used to identify the owner of the image. Also, The Block Truncation Coding (BTC) is one of the effective and real time application for data hiding. Most present BTC based watermarking methods cannot completely exploit visual perception of the cover images and do not obtain high data embedding rate. For more exploiting visual perception and high data embedding, an enhanced data hiding scheme based on BTC is proposed. In proposed method, considering the texture sub blocks and Least Significant Bits (LSBs of higher mean value and lower mean value) substitution combine together for designing improved the BTC watermarking scheme. It can obtain good balance between high embedding rate (capacity) and high quality. So, the texture sensitivity is exploited to recognize whether the image blocks or are smooth or complex. On the other hand, the LSB substitution method is employed to hide the indicator bits of each image block or sub block. The experimental results show that the proposed method increases capacity of data hiding compare to existing BTC watermarking with the same or higher quality.

Abstrak

Kaedah pengesahihan imej semakin banyak menerima tumpuan disebabkan kepentingannya kepada kegunaan aplikasi multimedia. Selain itu penghantaran Imej digital semakin banyak dilakukan melalui saluran komunikasi yang terdedah dan rentan seperti Internet. Melindungi produk digital menjadi suatu isu penting bagi memastikan transmisi yang selamat. Algortima sedia ada tidak dapat menjamin keselamatan kandungan ataupun pengesahan pemilikan produk digital tersebut Penyiratan tanda air atau penyembunyian data dalam imej digunakan untuk mengenalpasti pemilik sesuatu imej. Block Truncation Coding (BTC) adalah satu daripada kegunaan masa nyata yang efektif bagi menyembunyikan data. Kaedah tanda air yang berasaskan BTC tidak dapat mengeksploitasi persepsi visual terhadap imej hadapan dan tidak mengandungi kadar penyiratan data yang tinggi Bagi mengeksploitasi persepsi visual dan penyiratan data yang tinggi, satu skema penyembunyian data yang dipertingkat berasaskan BTC dicadangkan. Dalam kaedah yang dicadangkan, penggantian tesktur sub blok dan Least Significant Bits (LSB) iaitu yang mempunyai nilai min lebih tinggi dan nilai min lebih rendah digabungkan bagi meningkatkan prestasi skima BTC. Ia dapat mengimbangi diantara keperluan kadar penyiratan (kapasiti) dan juga kualiti. Sensitiviti tekstur dieksploitasi untuk membezakan blok imej atau blok sub yang licin atau kompleks. Kaedah penggantian LSB digunakan untuk menyembunyikan bit penunjuk blok setiap imej atau blok sub. Sensitiviti tekstur dieksploitasi untuk membezakan blok imej atau blok sub yang bersifat licin atau kompleks. Kaedah penggantian LSB digunakan untuk menyembunyikan bit penunjuk blok setiap imej atau blok sub. Hasil keputusan eksperimen menunjukkan bahawa kaedah yang dicadangkan bagi meningkatkan kapasiti penyembunyian data mempunyai kualiti yang sama atau lebih tinggi berbanding kaedah BTC sedia ada.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

AMBTC	Absolute Moment Block Truncation Coding
BTC	Block Truncation Coding
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
HVS	Human Visual System
LSB	Least Significant Bit
VQ	Vector Quantization

CHAPTER 1

INTRODUCTION

1.1 Overview

The illegal repetition of many kinds of media has been a topic for concern for several years. Currently, with the home computer being very general and extensive, digital repetition is easy and images, video, audio and text can be created rapidly and cost effectively. On the other hand, files can be edited or modified simply with different types of software and people often claim that these edited files are theirs when actually they were initially made by someone else. Therefore it is needed to distinguish whether a file is the original and also who has created the original. To control these digital duplicates and modified files some methods have been proposed and tested and until now, are not suitable completely [1].

Some of the existing technologies have been exploited to avoid illegitimate piracy, such as cryptography, but technology can not totally solve this problem, because the data encryption just provides security during the communication and transmission of data. When the data is delivered and decrypted, the creation will no longer be secure. To resolve the problem, people have tried to find a new effective copyright security of digital information produces and new method for data security maintenance is Digital watermark method [1, 2].

According to different kinds of watermark cover, digital watermark can be separated into: image, video and audio watermark.

There are different types of applications for digital watermarking technology and these types of application are increasing fast. For example, in the field of data security, watermarks may be used for certification, authentication. Certification is an significant subject for official papers, such as identity cards or passports. Also some other usages can be established in government cheques and paper money. Another usage is the authentication of image content or integrity. The aim of this style of application is to verify any changes and alterations in an image. This method has been edited and updated for digital images and also used for digital video, digital audio and text.

Old-style watermarking involved small visible marks in paper to confirm that they are original. Current watermarks are not visible to the human eye but can be perceived using a variety of methods [1].

1.1.1 Characteristics of Watermarking Schemes

An actual watermarking structure should have the following features [1]:

1) Imperceptibility: After inserting the watermark data, carrier for example cover image, audio or video should not change considerably. In other words, the attendance of the watermark data should not affect the carrier.

If a watermarking structure does not guarantee this condition, it can be happened that after inserting a secret data in a cover image quality is decreased so that the owner of the image will not like protecting mechanism alters his effort.

2) Robustness: The watermark data should not be damaged if someone does the common manipulations as well as malicious attacks. Its usage is depended on the application area.

3) Fragility: It means the secret data is altered or disturbed up to a certain extent when somebody does the common alterations & malicious attacks. Some application areas like tamper detection need a fragile watermark to know that some tampering is done with his work. Some application may need semi-fragility too. The semi-fragile watermark includes a fragile watermark part and a robust watermark part for example semi-fragile watermarks are robust to some kinds of attacks but fragile to the other attacks.

4) Robust to common signal processing: It is necessary that watermark be retrievable after common signal processing. These signal processing operations contain digital-to-analog and analog-to-digital alteration, re-sampling, re-quantization, and common signal improvements such as image contrast, brightness and color adjustment, high and low pass filtering, histogram equalization of an image and format change (for example: BMP image to JPEG image and so on)

5) Robust to common geometric alterations (image or video information): Watermarks in image and video information must also be immune from geometric image operations (rotation, translation, cropping and scaling). This characteristic is not essential for audio watermarking.

6) Robust to collusion attack and forgery: The watermark must be robust to collusion attack. Multiple individuals, who are owner of a watermarked copy of the data, may collude their watermark copies to emit the watermark presence and can create a copy of the original copy. Further, if a digital watermark is to be applied in litigation, it must be impossible for colluders to merge images to create a different legal watermark.

7) Unambiguousness: The watermark should unambiguously identify the owner. Furthermore, the accuracy of owner identification must not destroy.

1.2 Background of the problem

Nowadays it is possible for almost anyone to copy or manipulate digital information and without decreasing the quality. For example when artist signed him/her paintings with a brush to claim copyrights, currently artist can watermark him/her painting by hiding him/her name within the image. Therefore, the embedded watermark allows verifying of the owner of the work. In fact, this conception is also appropriate to other media such as digital video and digital audio. Presently the unauthorized distribution of digital audio over the Internet in the MP3 format is an important issue. Here digital watermarking can be beneficial to set up controlled audio distribution and to prepare copyright protection [2, 3].

As already mentioned, there are a lot of applications for digital watermarking technology and these kinds of application are increasing rapidly. For example, can be used for certification, authentication. Certification is big problem for official documents, such as identity cards or passports.

For example there is the identity number which is on the left of a protected identity card, and also it is hidden in the identity photo. Therefore swapping or manipulating the identity photo can be detected. Therefore someone else cannot claim that he/she is the owner of passport or identity cart. The other example, once photograph wants to show a picture is belong to him/her, he/she can use a watermarking technology that is inserted in digital cameras can help to solve the problem. If someone wants to tamper the information or the name of owner that is watermarked in picture, the watermark will be demolished this show that the information is tampered. So the others cannot claim photo is belonged to them [2, 3].

For these kinds of problems which are explained above, image authentication techniques have newly gained great attention due to their importance for a huge number of multimedia applications. Digital images are increasingly conveyed over non-secure channels such as the Internet.

Therefore, military, medical and quality control images should be safe against efforts to manipulate them;

Two techniques have been suggested for achieving the authenticity of digital images newly:

1. The digital signature-based
2. The digital watermark-based

The first technique uses an encrypted image hash (digital signature), which is produced in the capturing device.

A digital signature is based on the technique of Public Key Encryption. A private key is applied to encrypt a digest of the image. This encrypted digest of the image is named the signature of the image; it offers a way to confirm that it cannot be fake. This signature then go with the image .The authentication process of the image requires public key to have ability to decrypt the signature [3].

The image is hashed because of authentication and the obtained digest is matched to the decrypted signature. If they match then the image is correct and authentication is done. Authentication systems based on digital signature are fragile because any change to the image will consider the image tampered [3].

The second technique is the digital watermarking-based, which inserts invisible information into an image. For content authentication, the inserted watermark can be extracted and used for image confirmation aim.

These techniques are classified into three main categories: robust, fragile, and semi-fragile.

Robust systems are mainly applied in applications such as copyright protection and ownership confirmation of digital multimedia, because they are tolerance approximately all attacks [2, 3].

Fragile are applied to content authentication and integrity confirmation, because they are sensitive to nearly all modifications. On the other hand, semi-fragile methods are robust to incidental modification such as JPEG lossy compression, but fragile to other modifications [2, 3].

An actual authentication system must have the following appropriate features:

- Detect malicious image tampering;
- Integrate authentication data with host image rather than as a separate data file;
- Should not need the original image or watermark;
- Invisible
- Allow the watermarked image be kept in lossy compression format;
- Tolerant to incidental image alterations due to noise, etc.

An additional feature is the ability to find the tampering.
Previously published methods for image authentication do not satisfy all the requirements.

Watermarking is embedding data, which is able to verify the ownership or path copyright interruption, in the digital image, video or audio. For this aim (ownership authentication) determines that the watermark must be indivisible or robust to common processing and attack [2, 3].

On the other hands; in respect to the ownership authentication, hiding some invisible personalized information as verification key can be a considerable technique.

As already mentioned in watermarking characteristics, different types of watermark algorithm are developed for different purpose.

There are significant three types of watermarking: Robust watermarking for robustly transition ownership data, fragile watermarking to convey content-confirmation information and the last one to transport side information [2, 3].

Watermark can be visible or invisible. Normally ownership logos are provided with visible robust watermarking. To save more safe and copyright protection robust watermarking are made visually invisible.

The embedding methods of watermarking generally follow spatial domain analysis or transform domain analysis.

Watermarking in spatial domain is simply destroyable therefore they are better to fragile watermarking for authentication rather than robust watermarking. Any attack such as tampering, content alteration will abolish the fragile watermark. These kinds of watermarking are visually invisible and highly sensitive to external attack [2].

In compare, the transform domain does not work on some specific sample values, thus the watermark signal power is spread all over the content. Because of complex embedding these kinds of watermarking can resist against external attack. Due to this robustness, transform domain watermarking is preferred to claim ownership data. However, transform domain has little capacity of data hiding and tampering with locating is less accurate than spatial domain watermarking [3].

The most usually applied transform is the Discrete Cosine Transform, Discrete Fourier Transform, Discrete Wavelet Transform; the reason for watermarking in the frequency domain or transform domain is that the features of the human visual system (HVS) are better captured by the spectral coefficients.

Because, it can be seen in many articles which use DCT (Discrete Cosine Transform) algorithm and some other researchers use BTC (Block Truncation Coding) for ownership authentication application, therefore work should be done on these two algorithms. Since, several ownership verification and authentication schemes have been proposed for secure transmission of multimedia data over the Internet. Block Truncation Coding (BTC) is an efficient image coding method. Block truncation coding can be used

in real-time image transmission due to its simplicity, performance and superior channel resisting capability [4].

So, Block Truncation Coding can be selected as high performance algorithm for this aim.

1.3 Problem statement

In general, the watermark should have certain requirements; the most important requirements are such as:

- Imperceptibility to human eyes
- Robustness
- Unambiguousness to ownership authentication
- Security
- Capacity of data hiding to embed maximum information

Some of these requirements conflict with each other it results in many technical problems. For example, imperceptibility and capacity may conflict with robustness. Therefore, a reasonable compromise is needed to attain better performance for the especial applications [5].

Therefore the problem is the tradeoff between the above requirements for achieving better performance in ownership authentication.

On the other hand, hiding invisible personalized information as an ownership authentication key needs enough capacity for embedding, so capacity is important in ownership authentication purpose.

After reviewing literatures, it is understood that BTC can be suitable for this reason because of lots of papers which are existent and use these algorithms for

ownership authentication, and also for achieving ownership authentication semi fragile watermarking is more suitable. On the other hand, it can be seen, achieving high capacity and quality are considered more in this purpose [4].

1.4 Project Objectives

- To determine characteristics of BTC algorithm and investigate the existing ownership authentication watermarking methods in this category.
- To enhance data hiding capacity for watermarking based on BTC algorithm.
- To evaluate the enhanced algorithm and compare its results with some previous methods.

1.5 Project Aim

- The aim of this study is to determine characteristics of BTC techniques and then to enhance capacity of data hiding for an algorithm which is based on BTC, so that it can use for ownership authentication appropriately and finally evaluate the enhanced method and compare its results with some previous methods.

1.6 Project scope

- Digital image watermarking on ownership authentication application
- Enhance capacity in BTC algorithm
- use bitmap image format for examining

- Use MATLAB software for prototyping (because most of researcher use MATLAB for this kind of case)

1.7 Summary

Watermarking, which belong to the data hiding, has been a lot of research interest. There are a lot of works which are conducted in different branches in watermarking. Digital image watermarking is applied for many applications such as content security, copyright protection, content authentication, ownership authentication, tamper detection and so on. Also there are some classifications and requirements for digital image watermarking that must be attended, depend on their application. Therefore this study focusses on ownership authentication applications.

References

[1] Kaur, M., Jindal,S and Behal, S(2012). A study of digital image watermarking. *International Journal of Research in Engineering & Applied Sciences 126.* 2(2), 2249-3905.

[2] Lou, D.C., Wu, N. I., Wang, C.M., Lin, Z.H. and Tsai, C.S. (2010). A Novel Adaptive Steganography Based on Local Complexity and Human Vision Sensitivity, *Journal of Systems and Software*, 83(7), 1236-1248.

[3] Sakib, M., Alam S. B. , Rafi Sazzad, A. B. M., Shahnaz, C. and Fattah, S. A. (2010). A Basic Digital Watermarking Algorithm in Discrete Cosine transformation Domain. *Bangladesh University of Engineering and Technology* (BUET), Dhaka.

[4] Li, C. ,Lu, Zh. and Su, Y. (2011). Reversible data hiding for Btc compressed image based on bit plane flipping and histogram shifting of mean tables. Information technology journal. 10(7),1421-1426.

[5] Pun, C. M and Lam, I. T. (2009).Fingerprint Watermark Embedding by Discrete Cosine Transform for Copyright Ownership Authentication. *INTERNATIONAL JOURNAL OF COMMUNICATIONS.* 3(1)
Manpreet Kaur,Sonika Jindal,Sunny Behal

[6] TU, S. F and HSU, C. S. (2004). A BTC-BASED WATERMARKING SCHEME FOR DIGITAL IMAGES. *Information and security*. 15(2), 216-228

[7] Nyeem, H. and Boles, W. and Boyd, C. (2012). On the robustness
and security of digital image watermarking. *International Conference on Informatics, Electronics and Vision*.2012. Dhaka, Bangladesh.

[8] Chan, C.K. and Cheng, L.M. (2004). Hiding Data in Images by Simple LSB Substitution, *Pattern Recognition*, 37(3), 469-474.

[9] Piper, A. and Safavi-Naini, R. (2009). How to Compare Image Watermarking Algorithms. *In Transactions on Data Hiding and Multimedia Security IV*. 5510. 1-28. Springer Berlin / Heidelberg.

[10] Fen, Sh. and Sheng, Ch. (2004). A BTC-based watermarking scheme for digital images. Information and security. 15(2), 216-228.

[11] Yang. C. N. and Lu Z. M. (2011). A Blind Image Watermarking Scheme Utilizing BTC Bit planes. *International Journal of Digital Crime and Forensics.* 3(4), 42-53.

[12] Vidyasagar and Potdar, M. and Han, S. Chang, E. (2005). A Survey of Digital Image Watermarking Techniques. *3rd International Conference on Industrial Informatics*. 2005. Indian. IEEE

[13] Martino, F. D. Sessa, S. (2012). Fragile watermarking tamper detection with images *fuzzy transform*

[14] Liu, L. (2005). A Survey of Digital Watermarking Technologies

[15] SAXENA, V. (2008). *DIGITAL IMAGE WATERMARKING*. , NOIDA, INDIA

[16] Friedman, G. (1993). The trustworthy digital camera. *IEEE Transactions on Consumer Electronics*, vol. 39, no. 4, pp. 93-103.

[17] Changa, C. C. and Hub, Y. S. Lub, T. C. (2006). watermarking-based image ownership and tampering authentication scheme. Volume 27(5), 439–446.

[18] Yoseph Abatte. (2005). *DIGITAL IMAGEWATERMARKING*. Addis Ababa University.

[19] Bassem Abdel Aziz. (2003). Performance Analysis of a Content Authentication Semifragile Watermark. In *IEEE International Conference. 2003.* 2055 - 2058

[20] Ozgur Ekici. (2004). Comparative Evaluation of Semi fragile Watermarking Algorithms. *In Journal of Electronic*. 209 – 216.

[21] Tiwari, A. Sharma, M. (2012). Semifragile Watermarking Schemes for Image Authentication- A Survey. *I. J. Computer Network and Information Security*, 43-49.

[22] Wu, X. (2007). Reversible Semi fragile Watermarking Based on Histogram Shifting of Integer Wavelet Coefficients. *IEEE International Conference on Signal Processing*. 501 – 505.

[23] Cox, I. and Miller, M. and Bloom, J. (2002). Digital watermarking: principles and practice. Morgan Kaufmann Publishers. USA

[24] Cox, IJ. Miller, ML and Bloom, JA. (2002). Digital Watermarking, Morgan Kaufmann Publisher, San Francisco, CA, USA.

[25] Cox, I. Miller, M. Bloom, J. Fridrich, J. and Kalke, T. (2007). Digital Watermarking and Steganography. Burlington. Elsevier.

[26] Tefas, A. Nikolaidis, N. and Pitas, I. (2009). *Image Watermarking: Techniques and Applications.* Boston. Academic Press.

[27] Nyeem, H. and Boles, W. and Boyd, C. (2012). On the robustness and security of digital image watermarking. *International Conference on Informatics, Electronics and Vision*. 2012. Dhaka, Bangladesh.

[28] Mohammad Reza Khammar, Yunusa Ali Saied, and Marhaban, M. H. (2012). *A Digital Image Watermarking Method in the Discrete Cosine Transformation Domain. 2,* 2088-5334. ISSN.

[29] Zhang, D. Pan, Z. and Li. (2010). A Contour-based Semi-fragile Image Watermarking Algorithm in DWT Domain . *Second International Workshop on Education Technology and Computer cience(ETCS)* 3, 228.

[30] Chen, B. and Shen, H. (2009). A New Robust-Fragile Double Image Watermarking Algorithm. *Third International Conference on Multimedia and Ubiquitous Engineering*. November 2009. 153

[31] Md. Nazmus Sakib and Syed Bahauddin Alam. (2011). A Basic Digital Watermarking Algorithm in Discrete Cosine transformation Domain.

[32] Franti, P., Nevalainen, O. and Kaukoranta, T. (1994). Compression of Digital Images by Block Truncation Coding: A Survey. *The Computer Journal.* 37(4)

[33] Tsou, C. C., Wu, S. H. and Hu,Y. C. (2005). Fast Pixel Grouping Technique for Block Truncation Coding. *Workshop on Consumer Electronics and Signal Processing*. Nov. 17-18, 2005. Yunlin.

[34] Delp, E.J. and Mitchell, O.R. (1979). Image Compression using Block Truncation Coding. *IEEE. Trans. Communications*. 27,1335-1342.

[35] Fränti, P., Nevalainen, O. and Kaukoranta, T. (1994). Compression of Digital Image**s** by Block Truncation Coding**:** A Survey. 37,308-332.

[36] Chang, C. C. and Hu, Y. C. (1999). Hybrid Image Compression methods based on vector quantization and block truncation coding. *Society of Photo-Optical Instrumentation Engineers*. 38, 591.

[37] Somasundaram, K. and Sumitra, P. (2011).RGB & GRAY SCALE COMPONENT ON MPQ-BTC IN IMAGE COMPRESSION.3(4), 0975-3397. ISSN.

[38] Sun, W., Lu, Z. M., Wen, Y. C., Yu, Y. X. and Shen, R. G. (2011). High performance reversible data hiding for block truncation coding compressed images.

[39] Changa, C, C. Linb, C. Y. and Fanb, Y. H. (2007). Lossless data hiding for color images based on block truncation coding. *Department of Information Engineering and Computer Science.*41 , 2347 – 2357

[40] Pun, C. M and Lam, I. T. (2009).Fingerprint Watermark Embedding by Discrete Cosine Transform for Copyright Ownership Authentication. *INTERNATIONAL JOURNAL OF COMMUNICATIONS.* 3(1)

[41] Hong, W., Chen, T. S., Shiu, C. W. and Wu, M. C. (2011). Lossless Data Embedding in BTC codes Based on Prediction and Histogram Shifting. *Applied Mechanics and Materials. 65,182-185*

[42] Thodi, D.M. and Rodrguez, J.J. (2007). Expansion Embedding Techniques for Reversible Watermarking. *IEEE Transactions on Image Processing*. 16(3), 721-730.

[43] Tsai, P.Y., Hu, Y.C. and Yeh, H. L. (2009). Reversible Image Hiding Scheme Using Predictive Coding and Histogram Shifting. *Signal Processing*. 89(6), 1129-1143.

[44] Hong, W., Chen, T.S. and Shiu, C.W.(2008). Lossless Steganography for AMBTC Compressed Images. Cong. on Image and signal processing. 2, 13-17.

[45] Huang, S. C. and Jiang, C. F. (2012). A color image authentication and recovery method using block truncation code embedding.*Journal of Marine Science and Technology*. 20(1), 49-55.

[46] Chen, W. C. and Wang, M. S. (2009). A fuzzy c-means clustering-based fragile watermarking scheme for image authentication. *Expert Systems with Applications*. 36(2), 1300-1307.

[47] Lin, P. L., Hsieh, C. K., and Huang, P. W. (2005). A hierarchical digital watermarking
method for image tamper detection and recovery. *Pattern Recognition*, 38(12), 2519-2529.

[48] Lu, Z.M., Liu, C.H., Sun, S.H. (2002). Digital image watermarking technique based on block truncation coding with vector quantization. *Chin. J. Electron*. 11(2), 152–157.

[49] Lin, M.H., Chang, C.C. (2004). A novel information hiding scheme based on BTC. *Proceedings of 4th International Conference on Computer and Information Technology*. 66–71

[50] Chuang, J.C., Chang, C.C.(2006). Using a simple and fast image compression algorithm to hide secret information. *Int. J. Comput*. 28(4), 329–333.

[51] Hong, W., Chen, T.S. and Shiu, C.W. (2008). Lossless steganography for AMBTC compressed images. *Proceedings of 1st International Congress on Image and Signal Processing.*13–17

[52] Chen, J., Hong, W., Chen, T.S.and Shiu, C.W. (2010). Steganography for BTC compressed images using no distortion technique. *Imaging Sci. J.* 58(4), 177–185.

[53] Sun, W., Lu, Z. M., Wen, Y. C., Yu, F. X. and Shen, R. J. (2011). High performance reversible data hiding for block truncation coding compressed images.

[54] Chang, C. C., Lin, C. C., Tseng, C. S. and Tai, W. L. (2007).Reversible hiding in DCT-based compressed images. *Information Sciences*. 177, 2768-2786.

[55] Chang, C. C., Chen, T. S. and L. Z. Chung.(2002). A Steganographic Method Based upon JPEG and Quantization Table Modification. *Information Sciences*. 141, 123-138.

[56] Iwata, M., Miyake, K. and A. Shiozaki. (2004). Digital Steganography Utilizing Features of JPEG Images. *IEICE Trans. Fundamentals.* E87(4), 929–936.

[57] Lin C. C. and Shiu, P. F. (2009). DCT-based reversible data hiding scheme, Proc. of the 3rd International. *Conference on Ubiquitous Information Management and Communication*. 2009. (ICUIMC'09), 327–335,

[58] Lin, C. Y., Chang, C. C. and Wang, Y. Z. (2008). Reversible Steganographic Method with High Payload for JPEG Images, IEICE Trans. *Information and Systems*, 91(3), 836–845.

[59] Lin, C.C. (2010). High Capacity Data Hiding Scheme for DCT-based Images. *Information Hiding and Multimedia Signal Processing*. 1(3). 2073-4212. ISSN.

[60] Parameswaran, L. and Anbumani, K. (2008). Content-Based Watermarking for Image Authentication Using Independent Component Analysis. *Informatica.* 32, 299-306.

[61] Mona F. M. (2009). A DCT-Based Secure JPEG Image Authentication Scheme.

[62] Hong, W., Chen, T.S., Shiu, C.W. and Wu1,M.C.(2011). Lossless Data Embedding in BTC codes Based on Prediction and Histogram Shifting. Volume 65 (2011) pp 182-185. Trans Tech Publications.

[63] Keissarian, F. (2010). Hiding Secrete Data in Compressed Images Using Histogram Analysis

[64] Wu, X. and Sun, W. (2010). Data Hiding in Block Truncation Coding. *International Conference on Computational Intelligence and Security*

[65] Mohammad, N. Sun, X. and Yang, H. (2011). An Excellent Image Data Hiding Algorithm Based on BTC. *Information Technology Journal.*10(7), 1415-1420.

[66] Li, C. ,Lu, Zh. and Su, Y. (2011). Reversible data hiding for Btc compressed image based on bit plane flipping and histogram shifting of mean tables. Information technology journal. 10(7),1421-1426.

[67] Wang, K. , Hu, Y. and LU, Zh. (2012). Reversible Data Hiding for Block Truncation Coding Compressed Images Based on Prediction-Error Expansion. *Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*

[68] Zhang, Y. , Lu, Zh. and Zhao. D. (2012). An oblivious fragile watermarking cheme for images.

[69] Saha, B. and Sharma, S. (2012). Steganographic Techniques of Data Hiding using Digital Images. *Defence Science Journal*. 62(1), 11-18.

[70] Somasundaram, K. and Vimala, S. (2012). Multi-Level Coding Efficiency with Improved Quality for Image Compression based on AMBTC. *International Journal of Information Sciences and Techniques*. 2(2) .

[71] Mohammed, D. and Abou-Chadi, F. (2011). Image Compression Using Block Truncation Coding. *Journal of Selected Areas in Telecommunication.*