行政院國家科學委員會專題研究計畫成果報告

互動式網際網路電子資料交換支援彩色商務多媒體的所有權資訊確認及安全傳輸整合技術之設計與研發

計畫編號：NSC89-2416-H009-015
執行期限：88年8月1日至89年7 月31日

主持人：蔡銘箴　　國立交通大學資訊管理研究所
電子信箱: mjtsai@cc.nctu.edu.tw

一、中文摘要

本計畫的目是針對以網際網路為行銷主體的電子商務，對其互動式的及時性功能作研究，並對數位多媒體的電子商務資訊, 其所有權認證及專利權保護等技術做深入而廣泛的探討;從支援網際網路傳輸的互動式電子資料交換 (iEOI, Interactive EDI over Internet)，以整合「交換標準」和「通訊網路」此兩大議題著手，並對安全控管機制、商務多媒體的嵌入方式，以及相關的問題作研究，，譬如對數位多媒體加入不易察覺的標記簽章 - 如數位浮水印，給予交易雙方所有權的信賴，使得它能提供驗證者參考，確保所有權的歸屬，以保障合法使用者的權益，使電子商務的安全性有更高的保障。。

關鍵詞： 電子商務，商業自動化，互動式電子資料交換，網際網路電子資料交換，商務多媒體，專利所有權，認證，數位影像處理，數位浮水印，小波轉換，資訊安全。

Abstract

The purpose of this project will investigate the interactive property for real time response to support the format of Interactive Electronic Data Interchange over Internet (iEOI) for the enterprise electronic commerce in the Internet, also the ownership authentication and copyright protection for the digital business multimedia information. The research scope will cover the integration of interchange standard and communication network, the mechanism of data security, the encapsulation of business multimedia, and related topics. For example, adding the imperceptible digital label, such as watermarking, into the digital multimedia data could secure the trust for both transaction parties. The signature could offer the reference evidence, verify the ownership, protect the legal usage and higher security for the electronic commerce. We expect this study will create concrete results and provide the opportunity to explore the potential topics for associated researches.

Keywords: electronic commerce, business automation, interactive electronic data interchange, electronic data interchange over Internet, business multimedia, copyright ownership, authentication, digital image processing, digital watermarking, discrete wavelet transform, information security。

二、緣由與目的

緣由-在傳統的電子商務規模中[1][2][3]，**常把電子商務依照交易伙伴的對象分為兩類：一者為企業對企業的商務模式（**Business-to-Business），**另一者為企業對顧客的商務模式（**Business-to-Customer），**其進行的方式，概以電子資料交換（**EDI，Electronic Data Interchange）[4][5]**為基本的傳輸格式；從使用**EDI **來進行商務交易的角度來分析，前者到目前為止佔了大部分的應用規模。而此種依照企業和企業間建立的電子資料交換網路，從成本、效率和技術的考量，大都是以批次式電子資料交換（**Batch EDI）[6]**的方式來進行，因為企業間大量的資訊交換，並未對每筆交易都作即時回應或者訊息間的互相控制；但隨著資訊技術的日益成熟，進行電子商務的成本逐漸地降低，而網際網路的普及，更吸引了廣大的消費群眾利用網際網路來進行電子交易，基於時效經濟及實用性的考量，**Batch EDI **在此並無法完全滿足此種需即時互動和多方交換的行為模式**[7][8]。

尤其是在商業行為競爭激烈且複雜的今日，分、秒都在商務交易決策中，扮演著極為關鍵的角色；從消費者的角度來看，能夠得到互動、即時的回應，要比只拿到一個 acknowledgement receipt**來得有吸引力和保障，也更能夠隨時決定或更動個人的消費決策；而商業行為間的互相依賴程度，隨著商業活動全球化、自動化和資訊化後更形明顯，商務交易的主角也不僅僅侷限於買與賣雙方，多方的聯繫、參考、買賣情況越來越常出現。以上的原因，都促使著** Interactive EDI **系統出現來補足** Batch EDI **的不足狀況。**

目的 -越來越多的網際資料交換[9][10]，除了對一般商業的資訊進行交換外，也以多媒體格式資料來進行附註說明，使得商務多媒體在電子商務的商業架構模式中，成為廠商行銷時不可缺少的重要工具；而商務多媒體如數位影像的應用[11]，是電子商務上不可缺少的重要元件，譬如列印或傳送數位化附有簽名的支票影像，可成為銀行服務的項目之一，聲音及動畫更是如此[12]，因此，商務多媒體使電子資料交換的內容變得更富含吸引力及說服力。然而，在各種作業系統、瀏覽器內建功能的輔助下，網路數位資訊的重製相當容易，而相關多媒體處理軟體的操作容易，使得改造技術的取得，並不是件難事，這也使得數位多媒體資訊在電子商務的應用上，衍生出對所有權保護及認證技術的需求[13][14]，也就是交易的雙方必須對重要資訊來源的真實性及使用者的身份，提供確認。這一問題若沒有合理的解決途徑，除了容易造成交易的爭執外，廠商將不願將具有著作權的多媒體資訊放置在網際網路上進行交換，提供給消費者參考；流通資訊內容的缺乏，將阻礙了商務多媒體的應用，也影響到整體網際電子商務的發展。

因此，對數位資訊加入具有可資辨認的標記- 如浮水印[15][16]，使得它能很容易地被所有權者加入或移除，但卻不易被人所察覺，提供了認證的機 置[17]；而傳遞的資訊中，由於有相當於私人簽章的標記，可供作證的參考，使驗證者可確保所有權的歸屬，以保障所有權擁有者及合法使用者的權益。目前最常使用的浮水印技術[18-20]，基本上可分為spatial domain時域空間及frequency domain頻率空間的處理方式。spatial domain採取的方法，選擇性地對數位資訊單元做處理，由於只有局部區域經過改變，若是修改的範圍被有意圖者所洞悉，資料可以很輕易的做調換或更改，因此，所提供的安全保護並不周密；而以frequency domain作為處理的運算空間，一般而言，資料需經 Fast Fourier Transform快速傅立葉轉換、Discrete Cosine Transform 數位餘弦轉換或是Discrete Wavelet Transform小波轉換[21-24]，而經其在frequency domain處理後的資料，即使只有局部的修改，經由inverse transform後，浮水印的標記擴展到資料整體，而加註的信號，非常細緻而無法查覺，並且以不干擾到數位資料的主題為原則。所以，在frequency domain隱藏浮水印的信號，較spatial domain的處理有較高的安全保障。基於隱密性、安全性的考量，frequency domain的處理模式，將會是數位浮水印技術的主流，也是我們研究所採取的方法。

三、結果與討論

本研究計劃已獲得相當豐富的研究成果，由於前一年國科會計畫的前導，再加上這一年孜孜不倦的努力，在本年內，已有兩篇英文會議論文的發表以及兩篇SCI期刊的發表。

第一篇英文會議論文是發表在SCI'99 第三屆系統組織，人機介面，和資訊系統世界聯合會議 及ISA'99 第五屆資訊系統分析和合成國際會議，於民國 88 年 7 月 31 日至 8月4日在美國佛羅里達州奧蘭多市舉行，論文題目是"網際網路電子資料交換富含多媒體功能的資訊技術 - 使用SMTP和郵件代理人在商業應用的合作模式"，內容請見[25]及附件一

第二篇英文會議論文是發表在國際電機電子工程師學會2000年國際影像處理會議(ICIP2000)，於民國 89 年 9 月 10 日至 9月13日在加拿大溫哥華市舉行，論文題目是"可適性空間轉換的數位浮水印和小波封包對影像的確認"，論文內容請見[26]及附件二。

至於期刊論文，則有下述兩篇:

1. M.J. Tsai, K.Y. Yu and Y.Z. Chen, "Joint Wavelet and Spatial Transformation for Digital Watermarking", IEEE Trans. on Consumer Electronics, vol. 46, No. 1, pp. 241-245, Feb. 2000.
2. Min-Jen Tsai, "Very Low Bit Rate Color Image Compression by Using Stack-Run-End Coding", IEEE Trans. on Consumer Electronics, vol. 46, No. 2, pp. 368-374, May. 2000.

論文內容請見[27][28]。

四、計劃成果自評

本研究計劃研究成果，已獲得相當具體及深入的學術成果，可說是具延續性的專門研究，對促進學術交流及發展，有豐碩及成熟的表現；除了將繼續做更深入的探討外，也積極參與相關學術研討及論文發表，以達到有效應用為目的。

五、參考文獻

[1] Ravi Kalakota and Andrew B. Whinston, *Frontiers of Electronic Commerce*, Addison-Wesley, 1996.

[2] Ravi Kalakota and Andrew B. Whinston, *Electronic Commerce: A Manager's Guide*, Addison-Wesley, 1997.

[3] E. Koch, J. Rindfrey, and J. Zhao, "Copyright protection for multimedia data," *Proc. Int. Conf. Digital Media and Electronic Publishing*, 1994.

[4] P. Kimberley, "Electronic Data Interchange", McGraw-Hill, 1991. P. 5~16, 19~31.

[5] Pageant Ltd., "The Electronic Commerce Handbook", NCC BlackWell, 1996. P. 41~44.

[6] UN/EDIFACT Work Group, "UN/EDIFACT D97B", available on http://www.unece.org/trade/untdid/

[7] J. Veijalainen, "Issues in Open EDI", IEEE Telecommunications, 1992, P. 401~412.

[8] P.K.Sokol, "From EDI to Electronic Commerce", McGraw-Hill, 1994. P. 2~11, 13~49, 212~227.

[9] Institute for Information Industry, "Frequently Asked Questions about Electronic Business", Institute for Information Industry Taiwan, 1998.

[10] Kilpatric, "Standards and Electronic Commerce", The E-Commerce Handbook 1996, NCC BlackWell, 1996. P. 89~94.

[11] R.G. Schynde, A.Z. Tirkel, C.F. Osborne, "A digital watermark," *Proc. IEEE International Conference on Image Processing (ICIP'94)*, vol. 2, pp.86-90, 1994.

[12] I.J. Cox, J. Kilian, T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for image, audio and video," *Proc. IEEE International Conference on Image Processing (ICIP'96)*, vol.3, pp. 243-246, 1996

[13] J. Brassil, S. Low, N. Maxemchuk, and L. O'Gorman, "Electronic marking and identification techniques to discourage document copying." *Proc. Infocom'94*, pp. 1278-1287.

[14] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for data hiding," *Proc. SPIE*, vol. 2420, p.40, Feb. 1995.

[15] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21(2), pp. 120-126, Feb. 1978.

[16] M. D. Swanson, M. Kobayashi and A.H. Tewfik, "Multimedia Data-Embedding and Watermarking Technologies", *Proceeding of the IEEE*, Vol. 86, No.6, June 1998.

[17] N. Memon and P. W. Wong, "Protecting Digital Media Content", *Comm. of the ACM*, July 1998, vol. 41, No. 7.

[18] X.G. Xia, C.G. Boncelet and G.R. Arce, "A Multiresolution Watermark for Digital Images", *IEEE ICIP97*, vol. I, pp.363-368, June 1997, Santa Barbara, CA.

[19] W. Zhu, Z. Xiong, and Y.Q. Zhang, "Multiresolution Watermarking for Images and Video: A Unified Approach", *IEEE ICIP98*, vol. 1, MA11.09, Oct. 1998, Chicago, IL.

[20] R. Dugad, K. Ratakonda and N. Ahuja, "A New Wavelet-Based Scheme for Watermarking Images", *IEEE ICIP98*, vol. 2, TA10.07, Oct. 1998, Chicago, IL.

[21] Daubechies, "Orthonormal bases of compactly supported wavelets," *Comm. Pure Appl. Math.*, vol. XLI, pp. 909-996, 1988.

[22] S. Mallat, "A theory for multiresolution signal decomposition: the wavelet representation", *IEEE Trans. Pattern Analysis Machine Intell.* 7:674-693, 1989.

[23] M. Vitterli and C. Herley, "Wavelets and filter banks: theory and design," *IEEE Trans. On Signal Processing.*, vol. 40, pp. 2207-2232, Sep. 1992.

[24] M. Antonini, M. Barlaud, P. Mathieu, and I. Daubechies, "Image coding using wavelet transform", *IEEE Trans. Image Processing*, vol. 1, No. 2, pp. 205-220, Apr. 1992.

[25] M.J. Tsai, T.H. Wu, "The Information Technology for EDI over Internet with Multimedia Capability – A Collaboration Model Using SMTP and Mail Agent in Business Applications", vol. 8, pp. 370-375, SCI '99/ISAS '99, Orlando, Florida U.S.A., Jul 31~Aug 4, 1999.

[26] Min-Jen Tsai and Tien-Hwa Ho, "WWW and Telecommunication Collaboration Service for Mandarin Automatic Personal Phonebook Inquire Dialogue System", International Conference on Multimedia and Exposition 2000, New York City, U.S.A., July 31 - Aug 2, 2000.

[27] M.J. Tsai, K.Y. Yu and Y.Z. Chen, "Joint Wavelet and Spatial Transformation for Digital Watermarking", IEEE Trans. on Consumer Electronics, vol. 46, No. 1, pp. 241-245, Feb. 2000.

[28] Min-Jen Tsai, "Very Low Bit Rate Color Image Compression by Using Stack-Run-End Coding", IEEE Trans. on Consumer Electronics, vol. 46, No. 2, pp. 368-374, May. 2000.

附件一

The Information Technology for EDI over Internet with Multimedia Capability - A Collaboration Model Using SMTP and Mail Agent in Business Applications

Min-Jen Tsai
mjtsai@cc.nctu.edu.tw
Institute of Information Management, National Chiao Tung University
Hsin Chu, 300, Taiwan, R.O.C.

And

Tai-Hong Wu
Institute of Information Management, National Chiao Tung University
Hsin Chu, 300, Taiwan, R.O.C.

ABSTRACT

Electronic Data Interchange (EDI) has long been regarded as an efficient way to reduce the paper work with fast business information communication in the Value Added Network (VAN) environment. However, EDI are basically designed for the description of the text type data and does not support the multimedia information. With the booming of the Internet, VAN is apparently with much less popularity and limited accessibility and business globalization is in an inevitable trend. To reach the potential customers easier and faster through the wide accessible Internet, making business on the Internet has much lower cost than on the VAN. As long as the security issue could be well guarded with reliable connection, e-commerce will become main business model in the near future. To achieve this goal, an approach by using widely existing e-mail system in the business environment is developed. In this paper, we propose a complete business EDIINT (electronic data interchange over Internet) through e-mail system by supporting UN/EDIFACT and MIME formats and prove its feasibility and flexibility. In addition, multimedia service and applications are also provided.

Keywords: EDI over Internet (EDIINT), MIME Encapsulation, SMTP, Business Multimedia, Information Security.

1. INTRODUCTION

Electronic Data Interchange (EDI) is the basic document communication format for the Electronic Commerce (EC). The degree of the standardization and popularity of EDI could be regarded as the strong index of EC for Business-to-Business (B2B) and Business-to-Customer (B2C). By definition, Electronic Data Interchange (EDI) is the computer-to-computer exchange of business data in the standard formats. For EDI, information is organized according to a specified format set by both parties, allowing a “hands off” computer transaction that requires no human intervention or rekeying at either side [1-5].

The idea of EDI could be traced back to the 40's but the practical implementation appeared till late 70's, i.e. Electronic Funds Transfer (EFT) [6-7]. In 80's, personal computer and workstation systems has been widely used in the business daily practice and EDI based on the VAN environment also grows popular within the business or between the business. The EDI format could be different from business to business before the standardization [3,4] in early 90's. Currently, there are two widely used formats of EDI. One is ANSI ASC X.12 from ANSI [3] and the other one is UN/EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) of United Nation's ISO. ASC X.12 is developed earlier and UN/EDIFACT has much broad coverage for business applications. No matter which format, standard is accepted, a common business communication format is inevitable and EDI is the key component in business reengineering and competitive advantage.

With the boom of the Internet, the request for the EDI over Internet (EDIINT or EOI) instead of VAN has been formulated through the format standardization and communication openness. In addition, multimedia data along with text data are common in daily usage of business applications which should be considered as the important data formats for interchange. Therefore, EDIINT must support the multimedia data to enhance its flexibility in order to benefit the business globalization.

2. INTERNET ELECTRONIC DATA INTERCHANGE

Transmission Methods of Internet EDI

There are several communication methods on the Internet [8]:

- FTP (File Transfer Protocol): A protocol for transmitting text and binary files with speedy reliability. Suitable for large document communication [9].
- HTTP (Hypertext Transfer Protocol): A protocol for WWW and widely used on the Internet. Suitable for multimedia applications [10].
- IRC (Internet Relay Chat Protocol): A protocol designed for interactive discussion environment. Suitable for instant interactive data and information transmission [11].
- NNTP (News Network Transfer Protocol): A protocol of Internet discussion environment. Suitable for the packaging and transmission of distributed discussion and news files [12].
- SMTP (Simple Mail Transfer Protocol): A protocol for transmitting electronic mail. Combining with proper interface and encapsulation mechanism, it can be used for most of the data format file transmission [13].
- Socket Transmission: A host-to-host direct packaging transmission protocol.

Most of the protocols are pretty mature with certain degree of popularity in various applications. So, it is very optimistic that EDIINT can be widely accepted and implemented through above mentioned protocols in business utilization.

Among above protocols, using SMTP transmission protocol has the highest benefit vs. cost ratio by considering the restriction of the system installment expense and bandwidth limitation. The

附件一

EDIINT working group of the Internet Engineering Task Force (IETF) suggests that using Multipurpose Internet Mail Extensions (MIME) to envelope or encapsulate EDI objects then proceeding the SMTP transmission. The peer-to-peer property of SMTP could transmit multiple data to many business partners. SMTP daemon could quickly notice the host unreachable condition for further response.

In the past, e-mail or netnews needs to use uuencode/uudecode programs to package/unpackage multimedia information and non 7-bit ASCII language text information. This restriction makes the communication not convenient due to multiple data conversions. By using the characteristics of multi-party entity and content-transfer-encode of MIME to encapsulate the objects, it makes the communication fluently.

EDIINT'S BASIC STRUCTURE

Rik Drummond et al. [14] of IFTF's EDIINT working group have suggested EDIINT's basic structure in Fig. 1(a). There are four parts: company's internal information systems, EDI translator, communications interface and Internet or direct TCP/IP connection. These four steps form the EDIINT basic data flow and the implementation can be varied. A prototype structure of the proposed system in our study is displayed at Fig. 1(b) and the dash lines between Fig. 1(a) and 1(b) show the correspondence relationship. For example, company's internal business data like purchase order converts to the recognizable data for EDI translator. EDI translator then converts the data into EDI strings. RFC 822/RFC 1767 [15,16] makes the e-mail MIME encapsulation. Through SMTP and Internet transmission protocol, the e-mail envelop containing business data can be sent to the business partner and the reverse procedures at the receiver end will retrieve the original data to complete the data interchange action.

As mentioned before, entrepreneur must select an open standard as the EDI reference. In this study, UN/EDIFACT standard has been adopted since the format is widely used in Taiwan and its business partners. UN/EDIFACT hierarchical structure is shown in Fig. 2. Detailed description and definition could be found in [4]. Basically, as long as the sender and the receiver have the same or compatible EDI translator and MIME supported mail agent, the data interchange action can be easily achieved across the existing platforms. This concept can be utilized into WWW browser as well if suitable plug-in is provided. So, using the existing system and server could simplify the integration problem and reduce the installation cost.

SUPPORTING MIME'S AGENT

The information packaging protocols of the communication network includes RFC 821 & 822 (SMTP, Simple Mail Transfer Protocol & Standard for the format of ARPA Internet Text Message). They basically include the mechanism definition at the application level and the information exchange standard. In addition, RFC 2045/2046/2047 [17,18,19] define the MIME content, encoding definition and RFC 1767 [16] explains the MIME encapsulation. Selecting a suitable mail agent which supports those protocols is very cost effective and can quickly leverage the existing system functionality to adopt the EDI capability. Popularly used mail agents like mutt, eudora and browser's mailbox can be used in our proposed system design.

Multimedia Encapsulation

EDI standard (i.e. UN/EDIFACT) basically addresses the issues regarding the business text data. Due to the increasing computer speed and reduced cost of multimedia creation in digital format, multimedia information has been widely used in the Internet for commercial use. Therefore, EDIINT should be able to support the multimedia format to enhance its flexibility. Even the multi-part and content-transfer-encode properties of MIME could easily encode and encapsulate the textural and multimedia data, the relationship of the attached document does not reflect the correspondence in the EDIFACT strings. This is to say that even the mail header like Text Message Attachment and Content-Description Header declare the attached information but EDIFACT strings doesn't contain any description about the multimedia content. To compensate the insufficiency, we use the free text tag of the segment definition to link the multimedia in the EDI strings. An example is following:

FTX+MULTIMEDIA_RELATION_EXTENSION+2+IMAGE:
00001:JPEG:DESK0008.JPG:DESK_0008_NEW_CATA
LOG+VIDEO:00002:MPEG:HELLO.MPG:HELLO_TO_
PARTNERS_MESSAGE'

This is a product directory information and FTX indicates the segment of this free text. There are two files attached: DESK0008.JPG and HELLO.MPG with some description about the multimedia content. By comparing EDI information with the Headers of the e-mail, the EDI and multimedia files could be linked seamlessly.

3. IMPLEMENTATION AND EXPERIMENTS

An implementation flowchart of the EDIINT proposed system is shown in Fig. 3. This flowchart shows the consistent functions suggested in Fig. 1(a). The testing platform is Sun SPARC 10 with Sun OS4.1.4. Mail agent is mutt and the adopted EDI standard/message type is EDIFACT 98B/PAYEXT. There are eight steps (Fig. 2 ô - û) to complete an EDI data interchange with multimedia capability. Step ô performs the conversion from the business internal data into the flat file and multimedia format. Flat file is the input of the EDIFACT standard translator in step õ and EDI string is then generated. In the mean time, security control format could be inserted as well. Referring to the mail agent's MIME capabilities in step ö, e-mail is encoded/encrypted along with the attached multimedia data for the EDI data. Associated information is included in the mail header for necessary reference. SMTP server transmits the e-mail message in step ÷ from the sender to the dedicated receiver. Corresponding decoding procedures are performed at the receiver side to recover the original information. Mail agent unpacks the encapsulated mail message in step ø. If multimedia data is attached, multimedia application program is recalled to display the multimedia information in step ù. Standard translator of step ú at the decoder is utilized to convert the EDI strings back to the flat file. Flat file is then further transformed to the business internal data referring to the business partner's data in step û. After this, a complete sender to receiver e-mail transmission and data interchange is completed.

A financial payment instruction as the EDI example is shown in Fig. 4. It follows Fig. 3's procedures to complete the transmission. The business data in the payment instruction are the payer T.H. Wu (I.D. 11027686) intended to transfer three checks to payee M.J. Tsai (I.D. 11027687). The amounts of the checks are $250,000.00, $100,000.00 and $150,000.00 respectively. Payer's bank is IIM Bank (Bank I.D. 1116) and account is 00010061072156. The Payee's bank is NCTU Bank (Bank I.D. 11126) and the account is 00076154100786. The

transferring date is 1998/10/03 9:30AM and the auditer is J.Stanton of the K. department.

In the beginning, the business data is converted into the EDI strings in step ô. By using mutt as the mail agent to do the MIME encapsulation, PGVv2 encrypts the EDIFACT string and a scanned_original_doc.jpg multimedia file is attached in step õ. By using SMTP in step ö, EDI's e-mail has been transmitted from T.H. Wu to M.J. Tsai. After the decryption and de-encapsulation in step ÷, EDI string has been converted into the internal business data at step ø. The original information is kept intact at the receiver end. The whole function goes smoothly and very efficient.

As mentioned before, the proposed system using SMTP protocol is based on the availability of the existing system in the business. For those professions which have devoted a lot of resources in VAN-EDI, it is possible to build an EDI gateway to make the link between VAN-EDI and EDIINT to reach the inter-operable condition. This extension for the old system can extend the VAN accessibility to the Internet with the lowest expense.

There is no doubt that the security issues are the most concerned question for many businesses who plan to reach the globalization by the Internet. PGP/MIME or S/MIME are popular for MIME mail system with public key encryption system and certificate authentication (CA) management available. However, its encryption durability is still under debate and further stronger encryption system with better security control is needed. Other protocols like S-HTTP (HTTP over SSL) for EDIINT is also feasible and Java Applet and Plug-ins could load the business data and EDI from remote server during the downloading which can make the whole action on the fly. However, the similar situation for the security issue remained is the encryption restriction by the U.S. government for the export constraint. We are optimistic to expect the ban lifted and the web-based EDI environment is possible soon.

4. CONCLUSION

In this study, we propose a complete business EDIINT approach through mail system by combining existing UN/EDIFACT and MIME format and prove its feasibility. In addition, there are increasing need for business multimedia applications such as digital watermarking image, video and audio data. To provide the interrelationship between the EDI standard and the multimedia information, our system supports the business multimedia service and confirms its capability of integration. To achieve the secure communication, we specifically encapsulate the security control mechanism for the EDIINT. The technology completes the actual implementation for the safe Internet business electronic data interchange and transmission. Our study shows that it is easy to integrate the EDI translator with the mail agent for SMTP service, transfer EDI strings and business multimedia under the reliable PGP/MIME protocol.

Due to the speedy commercialization of the Internet and the fast prosperity of the E-commerce, we expect that our integrated technology study could behave as the reference for the development and the applications in the associated fields and further benefits the business globalization

ACKNOWLEDGMENTS

This work was partially supported by the National Science Council in Taiwan, Republic of China, under Grant NSC 88-2416-H009-021.

REFERENCES

[1] P. Kimberley, Electronic Data Interchange, McGraw-Hill, 1991. P.P. 5~16, 19~31.

[2] Pageant Ltd., The Electronic Commerce Handbook, NCC BlackWell, 1996. P.P. 41~44.

[3] ANSI ASC X.12 Work Group, “ANSI ASC X.12”, available on http://www.disa.org/

[4] UN/EDIFACT Work Group, “UN/EDIFACT D97B”, available on http://www.unece.org/trade/untdid/

[5] J. Veijalainen, “Issues in Open EDI”, IEEE Telecommunications, 1992, P.P. 401~412.

[6] Institute for Information Industry, QR/ECR Technical Handbook, Institute for Information Industry Taiwan, 1998.

[7] P.K.Sokol, “From EDI to Electronic Commerce”, McGraw-Hill, 1994. P.P. 2~11, 13~49, 212~227.

[8] Kilpatric, “Standards and Electronic Commerce”, The E-Commerce Handbook 1996, NCC BlackWell, 1996. P.P. 89~94.

[9] J. Postel & J.K. Reynolds, “File Transfer Protocol”, RFC 959, Oct 1985.

[10] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2068, Jan 1997.

[11] J. Oikarinen & D. Reed, “Internet Relay Chat Protocol”, RFC 1459, May 1993.

[12] B. Kantor & P. Lapsley, “Network News Transfer Protocol”, RFC 977, Feb 1986.

[13] J. Postel, “SMTP - Simple Mail Transfer Protocol”, Aug 1982, RFC 821.

[14] R. Drummond, “Signed, Sealed & Delivered: CommerceNet Test Results”, Network Computing, Sep 1997. P.P. 88~96.

[15] D. H. Crocker, “Standard for ARPA Internet Text Messages”, RFC822, 1982.

[16] D. H. Crocker, “MIME Encapsulation of EDI Objects”, RFC 1767, Mar 1995.

[17] N. Freed & N. Borenstein, “(MIME) Part One: Format of Internet Message Bodies”, RFC 2045, Nov 1996.

[18] N. Freed & N. Borenstein, “MIME Part Two: Media Types”, RFC 2046, Nov 1996.

[19] K. Moore, “MIME Part Three: Message Header Extensions for Non-ASCII”, RFC 2047, Nov 1996.

附件一

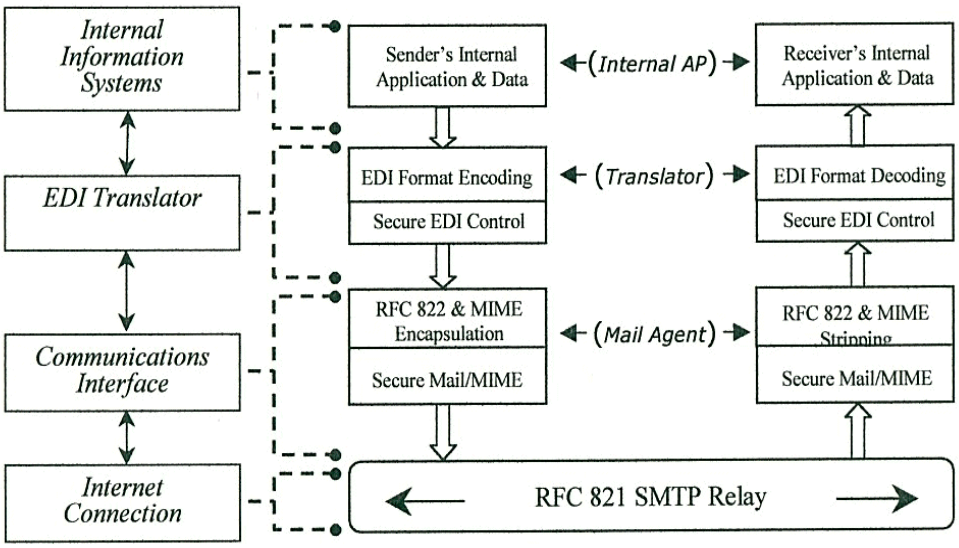

Fig 1.(a) The suggested EDIINT's basic structure from Rik Drummond et al. of IFTF's EDIINT working group.

1.(b) Proposed structure in this study.

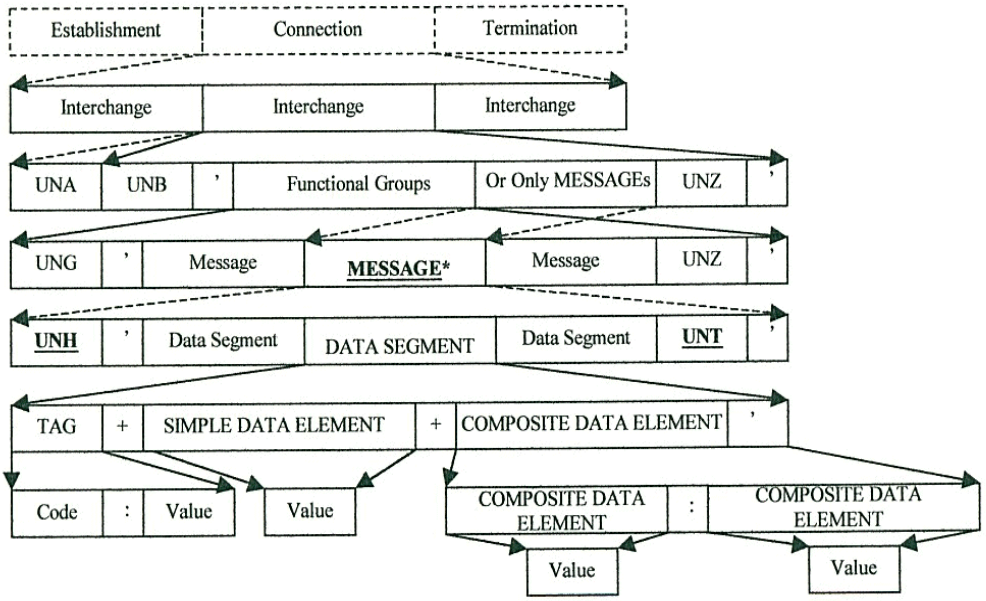

Fig. 2. UN/EDIFACT hierarchical structure.

附件一

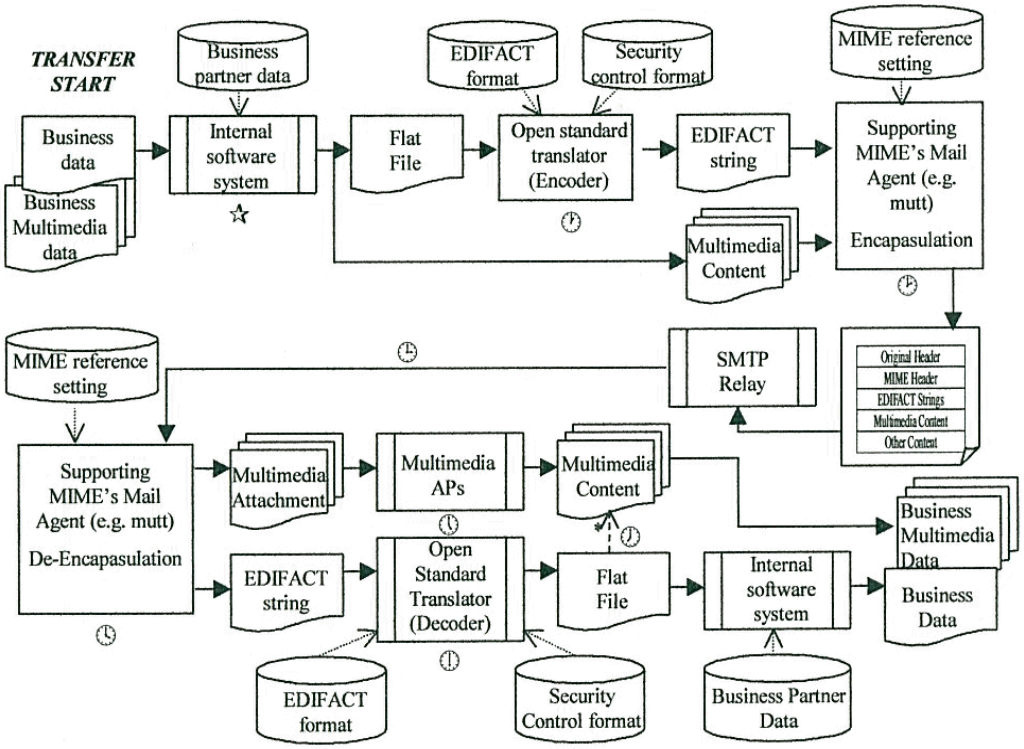

Fig. 3 The flow chart of the business data interchange of the proposed EDIINT system

Key procedures are labeled with the functions:

☆ Transferring business data to Flat files and business multimedia data

🕐 EDIFACT standard format translation

🕑 MIME Encapasulation of EDI and Multimedia Data

🕒 Transmitting e-mail through Internet by SMTP protocol

🕓 MIME De-Encapsulation

🕔 Multimedia display

🕕 Standard Format Translation

🕖 Transforming to the business data and multimedia data

附件一

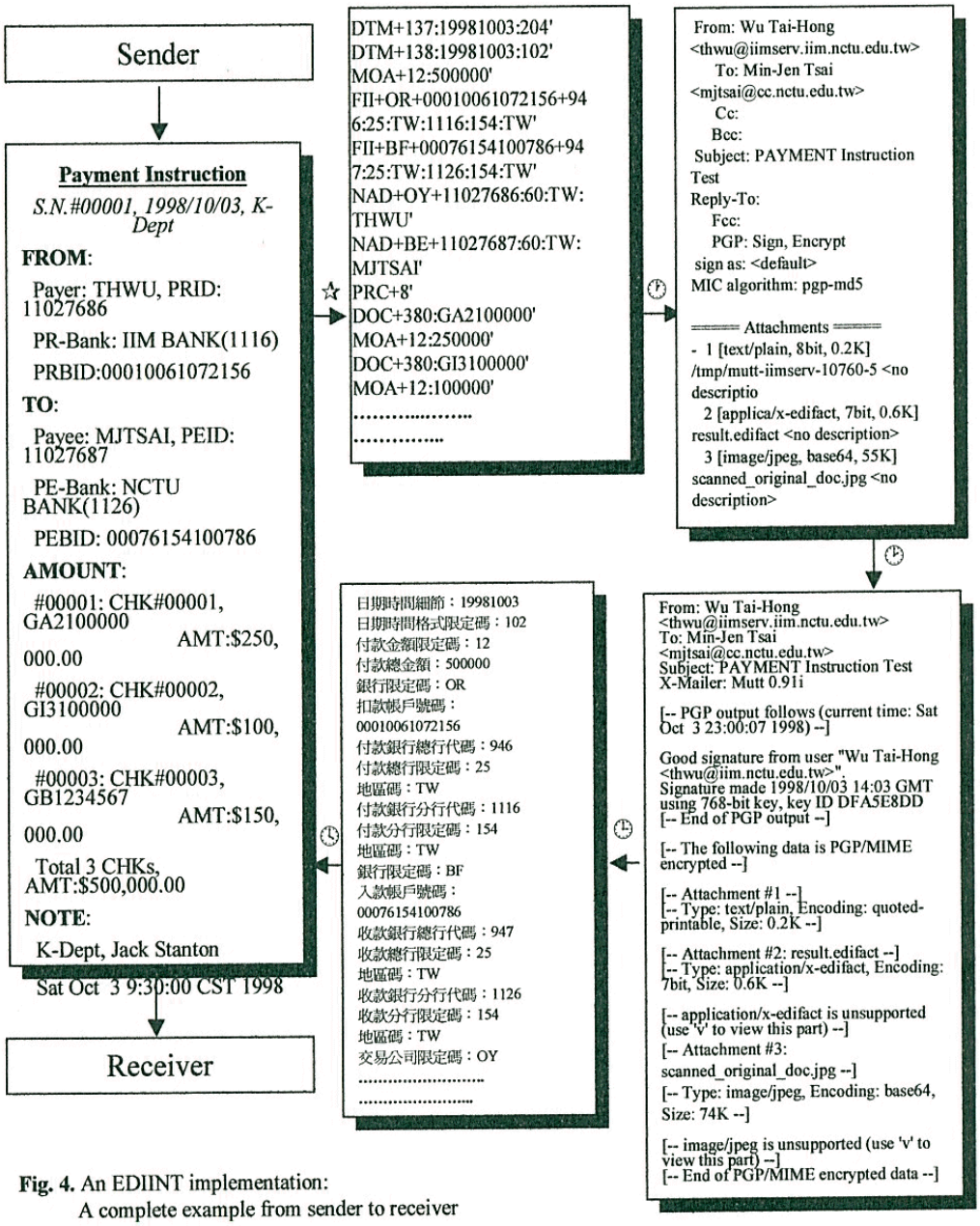

Fig. 4. An EDIINT implementation:
A complete example from sender to receiver

☆ At the sender side, business internal data converted into EDI strings

🕐 Using mutt mail agent to make MIME encapsulation and PGP encryption

🕑 E-mail sent to the receiver

🕒 Decryption and de-encapsulation of the e-mail with the corresponding EDI definition in Taiwan

🕓 At the receiver side, information converted back to the internal business data.

附件二

Wavelet Packet and Adaptive Spatial Transformation of Watermark for Digital Image Authentication*

Min-Jen Tsai[1], Kuang-Yao Yu[2], and Yi-Zhang Chen[1]
Institute of Information Management, National Chiao Tung University[1]
Institute for Information Industry[2]
E-mail: mjtsai@cc.nctu.edu.tw

ABSTRACT

A general watermarking scheme which adopts the multiresolution wavelet packet transform and content based watermarking scheme has been developed for digital image in this paper. The systematic approach of the watermarking includes the selection of the image content, the wavelet packet transform and the implementation of toral automorphism as the spatial transform for the watermark. To efficiently embed the watermark within the images and provide the robustness for the watermark detection under attacks, a modular based element classification and adjustment of the wavelet transformed coefficients has been utilized in this research. Instead of using the random number generator to create the watermark, the meaningful and recognizable seal image has been used as the watermark which provides immediately strong authentication information. In addition, the parameter settings of the choices among the transforms serve as the key information in decipher an watermarked image without referring to the original image. Compared with other watermarking methods, our technique provides a generalized approach for watermarking with robustness.

1. INTRODUCTION

Doing business on the Internet has become an important business model at present time. The Internet advances to an indispensable data and communication channel around the world. Since every transmitted data is digitized and can be easily duplicated, the problem of the copyright protection for commercial or sensitive data grows to an unavoidable situation for many businesses. Recently, we have seen the strong demands for digital watermark studies of audio, image or video multimedia data due to its ownership authentication mechanism. Even we focus our research on digital image watermarking in this paper, the method could be modified for other applications as well.

Watermarking schemes can be categorized into frequency domain [1,2] and spatial domain [3] based approaches. The basic requirement in watermarking is to make the embedded watermark invisible or difficult to notice for digital images. Generally speaking, frequency domain based approaches has better image fidelity preservation and robustness under attacks than spatial domain based techniques. The pioneering work from Cox et al [1] has shown the discrete cosine transform (DCT) based embedding scheme which uses random number as the watermark. Similar approach can be applied to other transform like the discrete wavelet transform (DWT) [4][5]. The drawback of this approach is that it is necessary to refer to the original image in order to extract the watermark which makes the authentication process difficult. This problem has been pointed out in [6] where authors developed a statistical detection scheme to resolve the problem. Even spatial domain based watermarking is not comparatively effective, the simplicity of the algorithm is usually its characteristic. How to leverage its usage in real application is also important.

To achieve a convincing ownership identification, a meaningful and recognizable watermark has been adopted in this research. Since the watermark has undeniable object content after the extraction procedure, the rightful authentication purpose can be more easily established. This paper is organized as following: in Section 2, we explain the general approach in the multidimensional wavelet based digital image watermarking in details. In Section 3, we summarize the experiment results and outline its characteristics with comparison. Finally, we conclude our integrated work with summary.

2. THE ALGORITHM

To start a wavelet transform based watermarking scheme, two things need to decide: where to insert the watermark and what kind of wavelet decomposition with embedding scheme to perform. The illustration of the consideration is shown in Fig. 1. Generally speaking, it will make attacks or forgery hard if the watermark is spread across the whole image. Since the content protection of the image is crucial, it is also often to insert the watermark within the major object or scene of the image to avoid the alteration of the background. Here, we use the spatial masks to decide the complex section of the image for watermark embedding. The criterion is based on the operation of the matrixes (1) $\begin{bmatrix}-1 & 0 & 1\end{bmatrix}$, (2) $\begin{bmatrix}-1\\0\\1\end{bmatrix}$ and (3) $\begin{bmatrix}0 & -\frac{1}{4} & 0\\ -\frac{1}{4} & 1 & \frac{1}{4}\\ 0 & \frac{1}{4} & 0\end{bmatrix}$ for the desired image section pixels in either horizontal, vertical or both direction. The average individual or summation value after the spatial masking provides an index factor to decide where to embed the watermark.

On the other hand, the hierarchical decomposition structure of the wavelet transform is the most often used in image compression and other image processing researches [7]. The more general wavelet packet decomposition can be utilized and worked as another key parameter during the transform. An example is shown in Fig. 1 (B). To further facilitate the operation, many good bases of wavelets with better image fidelity preservation [7,8] can be selected. In this study, the most common referred filters from [8]

*This work was partially supported by the National Science Council in Taiwan, Republic of China, under Grant NSC 88-2416-H009-021, NSC89-2416-H009-015 and Ministry of Economic Affairs, under contract number 89-EC-2-A-17-0208..

附件二

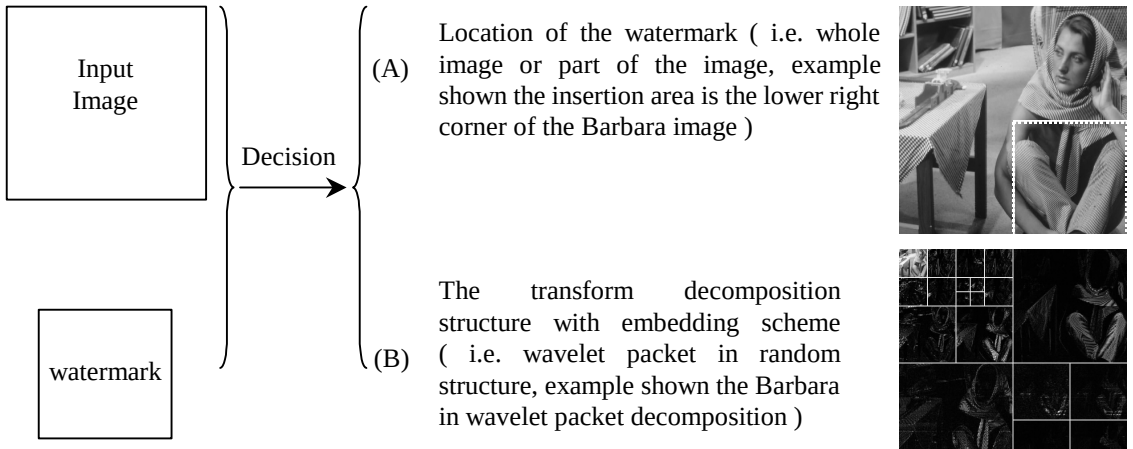

Figure 1. The decision procedure for watermarking an image.
(A) The selection of the watermark location in the original image (B) The selection of the wavelet decomposition

are implemented but the scheme can be used for other wavelet bases.

We developed a watermark embedding scheme in [9] which adopts the toral automorphisms [10] as chaotic two dimensional integer vector generators to select the location for the watermark embedding. A simple demonstration is shown in Fig. 2 where author's seal in Chinese character has been used as the watermark and Barbara image is the original image. A simple introduction of the algorithm is as following: It starts to transform the mxm digital watermark into an NxN matrix. The formula is as following:

$$A_N(k): \quad \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod } N)$$

Where k is a controlling parameter, N is the matrix size, (x, y) and (x', y') is the pixel location before and after the transform. If the formula $A_N(k)$ has the period T (which is generally quite irregular due to the integer arithmetic) , (x, y) can return to the original location after T times of $A_N(k)$ operation. Therefore, if the point (i, j) has n times of $A_N(k)$ operation ($n < T$), it needs extra $T - n$ operation of $A_N(k)$ to make (i, j) back to the original location. From the encryption point of view, given k, n is the key to encipher the data, $T - n$ will be another key to decipher the scrambled data back to the original order. An example in Fig. 2(B) has shown that the author's seal in Chinese character at the size 32x32 has been transformed into the image size at 64x64.

Setting	S = 16		S = 32		S = 48	
original	56.27 dB		50.55 dB		47.08 dB	
JPEG quality	JPEG image PSNR	Error points	JPEG image PSNR	Error points	JPEG image PSNR	Error points
100	54.22	0	49.89	0	46.75	0
90	40.05	5	39.77	0	39.35	0
80	36.77	28	36.65	0	36.43	0
70	34.89	106	34.81	1	34.67	0
60	33.52	162	33.46	8	33.36	0
50	32.50	257	32.45	23	32.36	1
40	31.46	333	31.42	80	31.35	5
30	30.15	390	30.13	149	30.07	46
20	28.26	428	28.25	304	28.21	126
10	25.39	438	25.38	398	25.37	319
0	17.15	465	17.14	417	17.15	399

Table 1: Tabulated value for S selection under JPEG compression attacks. The parameters are n = 16, k =12, (p1, p2)=(64,0), block size m = 32, N=64, $T_1 = S/4$ and $T_2 = S/4*3$.

In order to embed the transformed watermark into the selected wavelet coefficients, an area of image size of NxN at location (p_1, p_2) has been chosen from the wavelet transformed image as shown in Fig. 2(A). The NxN area could be any place within the transformed image but it is often within certain subband. A modular based threshold scheme has been developed in [9] to embed the watermark. The rules are as following:

1. Definition:
   set A - the chaotic transformed NxN matrix,
   set U - the collection of relocated watermark in A,
   set B - the wavelet transformed coefficients,
   S - modular value,
   set C - for each (i,j) which belongs to set B and U,
   $\delta(i,j)$ - for each (i,j) within C, $\delta(i,j) = C(i,j) \bmod S$.
2. For all points (i, j) in the intersection of set U and A:
   If $A(i,j) = 1$ and $B(i,j) \geqq 0$, then $C(i,j) = C(i,j) - \delta(i,j) + T_1$;
   If $A(i,j) = 0$ and $B(i,j) \geqq 0$, then $C(i,j) = C(i,j) - \delta(i,j) + T_2$;
   If $A(i,j) = 1$ and $B(i,j) < 0$, then $C(i,j) = C(i,j) + \delta(i,j) - T_1$;
   If $A(i,j) = 0$ and $B(i,j) < 0$, then $C(i,j) = C(i,j) + \delta(i,j) - T_2$;
   Where T_1 and T_2 are thresholds as the differentiation values for watermark embedding.

In Table 1, we listed the impact of selection of S which is directly related to the image quality of the watermarked image. The rules for watermark extraction are as following:

1. From the embedding procedures, there are n, k, p_1, p_2, m, N, S, T_1, T_2, key parameters which will be used in the detection steps.
2. Definition:

附件二

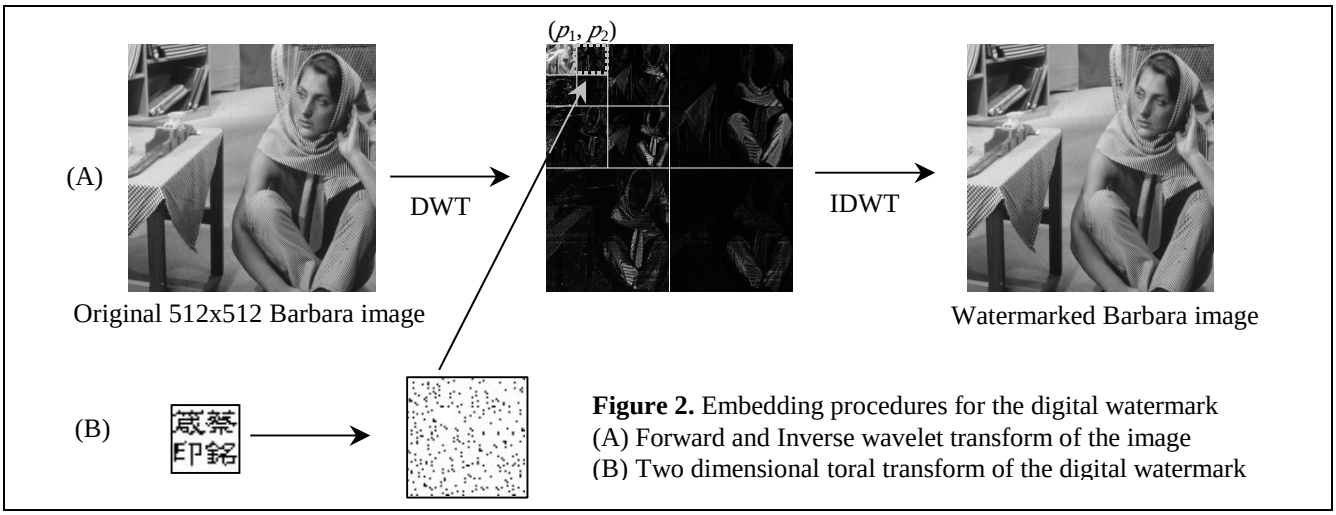

Figure 2. Embedding procedures for the digital watermark
(A) Forward and Inverse wavelet transform of the image
(B) Two dimensional toral transform of the digital watermark

set Y - Using the information of (p_1, p_2) to extract the NxN block area from the wavelet transform domain.
è(i,j) - for each (i,j) within Y, è(i,j) = Y(i,j) mod S.
set D - a NxN matrix.

3. For all points (i,j) within Y,
   If | è(i,j) |≧ $(T_1 + T_2)/2$, then D(i,j) = '0';
   If | è(i,j) | < $(T_1 + T_2)/2$, then D(i,j) = '1';
4. Use n, k, to perform $T - n$ times of $A_N(k)$ operations for D. The watermark will be located at the upper left corner of the reordered D set with size mxm.

The illustration of extraction procedure is just reverse the embedding processes as shown in Fig. 2 and some experiment results can refer to [9].

3. DISCUSSION

As mentioned earlier, we use the spatial mask to decide where to insert the watermark. The Barbara image is split into four parts with equivalent size. Table 2 shows the operation results where numbers are the average absolute values of the spatial difference in vertical, horizontal or both directions. Apparently, section four has the highest value as the complex content in the image from every spatial mask. Fig 3(a) and (b) illustrate the comparison of embedding the watermark only in the lower right corner and the whole image with different modular value under JPEG [11] attacks. Basically, both plots are very comparable with small variation. Even there is no significant difference in the PSNR and number of error points measure, it suggests that watermark embedding in fraction of the image could be as robust as the full frame embedding. Similar approach has been applied in Lena and several other images. For Lena image, the performance is not significant since the values from spatial masking could not uniquely indicate the complex content location. This means that if there is no particular representative content indication, embedding watermark in the whole image frame achieves the most robustness to preserve the image fidelity. However, the location of the embedding could be still a key during the watermarking.

Quadrant	1	2	3	4
Mask (1)	19.40	10.33	14.27	31.27
Mask (2)	53.61	54.06	48.33	59.89
Mask (3)	29.72	24.34	19.97	32.66
Sum of Mask(1)(2)(3)	88.73	102.73	82.57	123.82

Table 2: Average value after the spatial mask (1), (2), (3) operations (the matrixes are expressed in section 2.) applied to the Barbara image which is split as four quadrant from the center.

It is also possible to change the embedding area of the watermark in the subband as shown in Fig. 2(A) where the modular values N of the toral automorphism are 50 and 64 respectively. Fig 3 (c) and (d) illustrate that the behavior of the robustness and the performance are comparable for both embedding parameters. Further tests for wavelet packet decomposition achieve similar results which demonstrates that the packet decomposition structure could be another key during the watermark embedding.

4. CONCLUSION

In this paper, we introduce a general approach which incorporates the applications of wavelet packet and adaptive spatial transform for watermark where toral automorphism with the modular based threshold scheme for watermark embedding and extraction is adopted. The selection of the image embedding area, the wavelet packet transform and the implementation of toral automorphism can be used as the key information for the watermarking. In addition, the operations of spatial masking provides as a content indicator to decide the location for watermark embedding. The experiments have shown that the robustness under attack like image compression from fraction image embedding has comparable performance to the full frame embedding. In addition, the meaningful watermark provides strong ownership authentication capability. Compared with other watermarking methods, our technique is a generalized approach for watermarking with flexibility.

5. REFERENCES

[1] I. Cox, J. Kimedia", *IEEE Trans. on Image Processing*, vol. 6, no.12, pp.1637-1678, Dec. 1997.

附件二

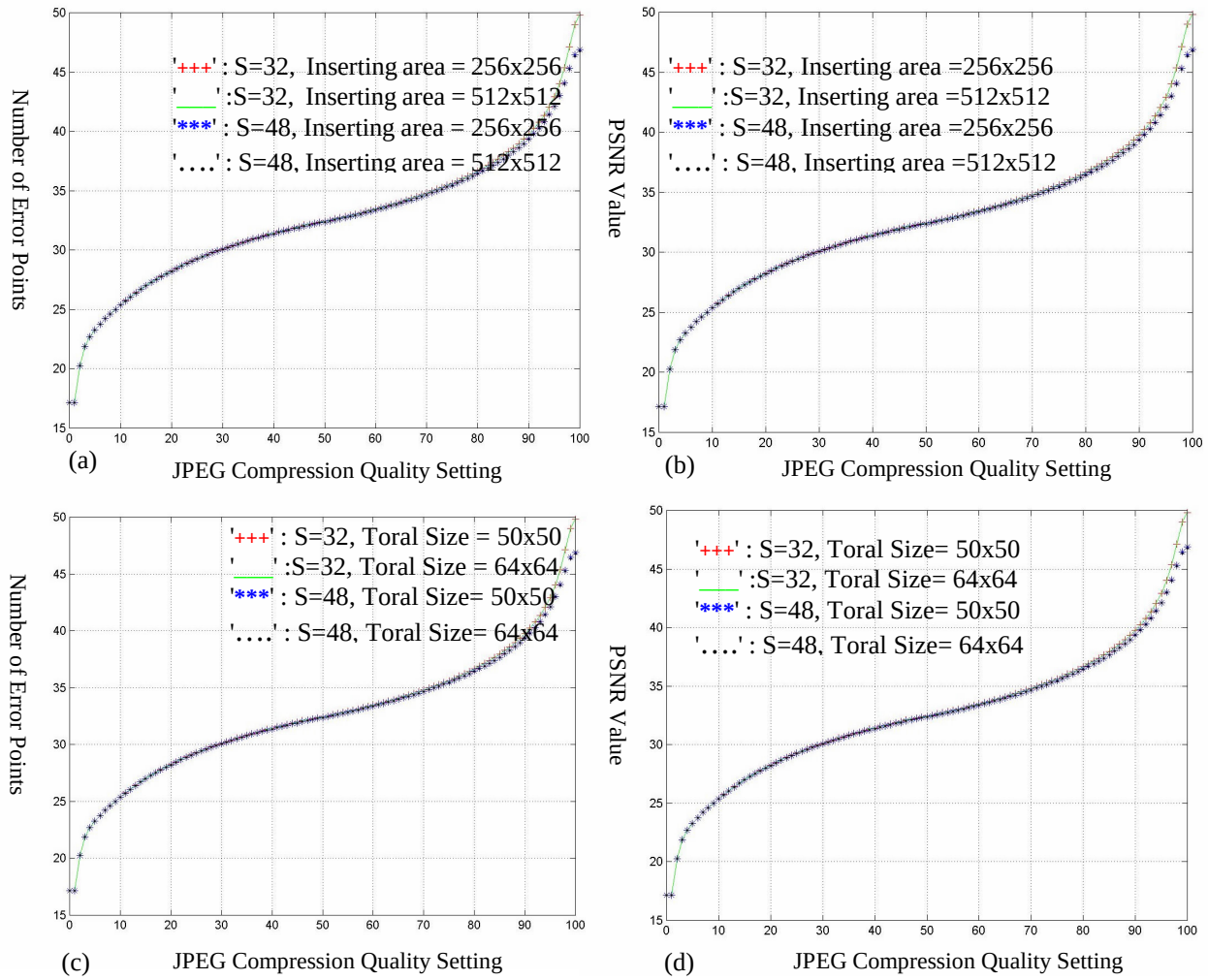

Figure 3. (a)(b) The plot of JPEG quality factors vs. the number of error points and PSNR value where modular value are 32 and 48, inserting areas are 256x256(lower right corner of the original image) and the full image respectively.

(c)(d) The plot of JPEG quality factors vs. the number of error points and PSNR value where modular value are 32 and 48, toral transform are 50x50 and 64x64 as shown in Fig. 2 (A) wavelet transform subband respectively.

[2] M. Swanson, M. Kobayashi and A. Tewfik, "Multimedia Data-Embedding and Watermarking Technologies", *Proceeding of the IEEE*, Vol. 86, No.6, June 1998.

[3] N. Memon and P. W. Wong, "Protecting Digital Media Content", *Comm. of the ACM*, July 1998, vol. 41, No. 7.

[4] X.G. Xia, C.G. Boncelet and G.R. Arce, "A Multiresolution Watermark for Digital Images", *IEEE ICIP97*, vol. I, pp.363-368, June 1997, Santa Barbara, CA.

[5] W. Zhu, Z. Xiong, and Y.Q. Zhang, "Multiresolution Watermarking for Images and Video: A Unified Approach", *IEEE ICIP98*, vol. 1, MA11.09, Oct. 1998, Chicago, IL.

[6] W. Zeng and B. Liu, "A Stastical Watermark Detection Technique Without Using Original Images for Resolving Rightful Ownerships of Digital Images", *IEEE Trans. on Image Processing*, vol. 8, no.11, pp.1534-1548, Nov. 1999.

[7] Daubechies, "Orthonormal bases of compactly supported wavelets," *Comm. Pure Appl. Math.*, vol. XLI, pp. 909-996, 1988.

[8] M. Antonini,M. Barlaud, P. Mathieu, and I. Daubechies, "Image coding using wavelet transform", *IEEE Trans. Image Processing*, vol. 1, No. 2, pp. 205-220, Apr. 1992.

[9] M. Tsai, K. Yu and Y. Chen, "Joint Wavelet and Spatial Transformation for Digital Watermarking" *IEEE. Trans. on consumer Electronics*, vol. 46, No. 1, pp. 241-245, Feb, 2000.

[10] G. Voyatzis and I. Pitas, "Applications of Toral Automorphisms in Image Watermarking", IEEE Int. Conf. on Image Processing, Vol. 2, pp. 237-240, September 1996.

[11] W.B. Pennebaker, J.L. Mitchell, "JPEG - Still Image Data Compression Standard", Van Nostrand Reinhold, New York, 1993.