

Encryption for JPEG2000 images using private probability table

何家?、張世旭

E-mail: 345902@mail.dyu.edu.tw

ABSTRACT

With the development of network technology and the digital technology, digital images are used more widely in our lives. Because digital images is easy to obtain, the security problem has been concerned. The JPEG2000 is a new still image compression standard. Because it provides lossy and lossless compression, JPEG2000 has good quality for image compression. JPEG2000 is a widely applications such as medical image, military image and remote sensing image. This paper proposed a new digital image encryption scheme for encrypting JPEG2000 images. The proposed scheme has a highly secure, and it is not modify the architecture of JPEG2000. The new method not only provide image encryption, but also not decrease the compressibility of the standard JPEG2000 coding scheme.

Keywords : JPEG2000、Qe probability table、EBCOT、MQ coder、RC4

Table of Contents

封面內頁 簽名頁 中文摘要 iii ABSTRACT iv 誌謝 v 目錄 vi 圖目錄 viii 表目錄 x 第一章 緒論 1 1.1 前言 1 1.2 研究背景 3 1.3 研究目的 5 1.4 論文架構 5 第二章 相關技術 6 2.1 JPEG2000 6 2.2 最佳切割嵌入式區塊編碼 8 2.2.1 有意義點判斷程序 10 2.2.2 數值增量點判斷程序 10 2.2.3 清除的程序 10 2.3 MQ編碼器 11 第三章 提出之方法 18 3.1 產生子金鑰 22 3.2 建立秘密機率表T 23 3.3 使用秘密機率表T進行編碼 24 第四章 實驗結果分析與探討 26 4.1 不同b值對JPEG2000壓縮加密演算法的影響 30 4.2 複雜度測試 33 4.3 安全度測試 33 4.4 漸進式壓縮技術 38 第五章 結論與未來研究方向 40 5.1 結論 40 5.2 未來研究方向 41 參考文獻 42

REFERENCES

- [1]C. J. Kuo and M. S. Chen, "A new signal encryption technique and its attack study," in Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on Security Technology., 1991, pp. 149-153.
- [2]B. Subramanyan, V. M. Chhabria, and T. G. S. Babu, "Image Encryption Based on AES Key Expansion," in Second International Conference on Emerging Applications of Information Technology (EAIT), 2011, pp. 217-220.
- [3]S. H. Kamali, R. Shakerian, M. Hedayati, and M. Rahmani, "A new modified version of Advanced Encryption Standard based algorithm for image encryption," in International Conference On Electronics and Information Engineering (ICEIE) 2010, pp. V1-141-V1-145.
- [4]H. K.-C. Chang and J.-L. Liu, "A linear quadtree compression scheme for image encryption," Signal Processing: Image Communication, vol. 10, pp. 279-290, 1997.
- [5]P. P. Dang and P. M. Chau, "Image encryption for secure Internet multimedia applications," IEEE Transactions on Consumer Electronics, vol. 46, pp. 395-403, 2000.
- [6]C.-C. Chang, M.-S. Hwang, and T.-S. Chen, "A new encryption algorithm for image cryptosystems," Journal of Systems and Software, vol. 58, pp. 83-91, 2001.
- [7]J.-L. Liu, "Efficient selective encryption for JPEG 2000 images using private initial table," Pattern Recognition, vol. 39, pp. 1509-1517, 2006.
- [8]O. Yang, L. Won-Young, and R. Kyung Hyune, "A flexible JPEG2000 image encryption based on arithmetic coding," in International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), 2007, pp. 400-403.
- [9]Information Technology-JPEG2000 Image Coding System-Part I: Core coding System, ISO/ISC International Standard 15444-1, ITU Recommendation T.8000 2000.
- [10]W. Hongjun and M. Di, "Efficient and secure encryption schemes for JPEG2000," in Proceedings. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 2004, pp. V-869-72 vol.5.
- [11]Y. Shiling and L. Qiu Hua, "Partial encryption of JPEG2000 images based on EBCOT," in International Conference on Intelligent Control and Information Processing (ICICIP), 2010, pp. 472-476.
- [12]M. D. Adams, "The JPEG-2000 still image compression standard, ISO/IEC JTC 1/SC 29/WG 1 N 2412, Dec.," ed, 2002.
- [13]吳炳飛, 胡益強, 瞿忠正 與 蘇崇彥, JPEG 2000 影像壓縮技術. 台北: 全華科技股份有限公司, 2003.
- [14]D. Taubman, "High performance scalable image compression with EBCOT," IEEE Transactions on Image Processing, vol. 9, pp. 1158-1170,

2000.

[15]D. Taubman, E. Ordentlich, M. Weinberger, and G. Seroussi, "Embedded block coding in JPEG 2000," *Signal Processing: Image Communication*, vol. 17, pp. 49-72, 2002.

[16]M. Adams. (2006). *Jasper Software Reference Manual (Version 1.900.0)*.

[17]Y. Yao, C. Jiang, and X. Wang, "Enhancing RC4 algorithm for WLAN WEP protocol," in *Chinese Control and Decision Conference (CCDC)*, 2010, pp. 3623-3627.

[18]The USC-SIPI Image Database. Available: <http://sipi.usc.edu/database/> [19]Kodak Lossless True Color Image Suite. Available: <http://r0k.us/graphics/kodak/>