使用秘密機率表之JPEG2000影像加密演算法

何家?、張世旭

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

摘 要

隨著數位化時代的來臨與網際網路的高速發展，許多影像資料逐漸的數位化並在日常生活中廣泛的使用，由於數位影像容易透過網際網路取得，因此產生許多數位影像的安全問題。 JPEG2000(Joint Photographic Experts Group 2000)是新的靜止影像壓縮標準，提供有損與無損的壓縮方式，能夠更好地保存影像，因此被廣泛的應用例如醫學影像、軍事影像與遙測影像等。 本篇論文提出一個針對JPEG2000壓縮演算法的數位影像加密技術，在提出更高的計算安全度下，同時也不會對JPEG2000硬體造成太大的修改，並且在加密數位影像時也能兼顧數位影像的壓縮率。

關鍵詞 : JPEG2000壓縮演算法、Qe機率表、最佳切割嵌入式區塊編碼、MQ算術編碼、RC4演算法

目錄

參考文獻

[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. Qiuhua, "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/