Fast image encryption based on lifting wavelet transform and advanced encryption standard

E-mail: 345901@ mail.dyu.edu.tw

ABSTRACT

In this thesis, We simulate wavelet hierarchical features, combined with the thelook-up table of Advanced Encryption Standard, and the mix column's finite fieldsGF(28) multiplication and addition, and propose a low-volume image encryptionalgorithm, which considers digital image as a big block and encryption of the bigblock. The selection and generation of subkey depends on the user's key, make theencryption, decryption and key generation system use the same algorithm. Theresults (effects) of encryption and decryption can be achieved by only changinglook-up table for encryption and decryption. The simulation results show the proposal can effectively resists various attackswhen the encryption rounds are at least more than two rounds (ex. statistical analysis,differential attack....). Our proposal uses the hierarchical concept of wavelettransformation as the concept of the rapid diffusion and confusion, with greatavalanche effect.

Keywords: Cryptography Image encryption Lifting wavelet transform Advanced encryption standard Finite fields

Table of Contents

REFERENCES

[1] C. Shannon, "Communication theory of secrecy systems," BellSystem Technical Journal, vol. 28, pp. 656-715, 1949.

[2] G. Chen, Y. Mao, and C. K. Chui, "A symmetric imageencryption scheme based on 3D chaotic cat maps," Chaos,Solitons & Fractals, vol. 21, pp. 749-761, 2004.

[3] S. Lian, J. Sun, and Z. Wang, "Security analysis of achaos-based image encryption algorithm," Physica A Statistical Mechanics and its Applications, vol. 351, pp.645-661, 2005.

[4] S. Lian, J. Sun, and Z. Wang, "A block cipher based on asuitable use of the chaotic standard map," Chaos, Solitons &Fractals, vol. 26, pp. 117-129, 2005.

[5] H. Gao, Y. Zhang, S. Liang, and D. Li, "A new chaoticalgorithm for image encryption," Chaos, Solitons & Fractals,vol. 29, pp. 393-399, 2006.

[6] H. S. Kwok and W. K. S. Tang, "A fast image encryptionsystem based on chaotic maps with finite precisionrepresentation," Chaos, Solitons & Fractals, vol. 32, pp.1518-1529, 2007.

[7] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," Chaos, Solitons & Fractals, vol. 35, pp. 408-419, 2008.

[8] Y. Wang, K.-W. Wong, X. Liao, T. Xiang, and G. Chen, "A chaos-based image encryption algorithm with variable control parameters," Chaos, Solitons & Fractals, vol. 41, pp. 1773-1783, 2009.

[9] K.-W. Wong, B. S.-H. Kwok, and C.-H. Yuen, "An efficient diffusion approach for chaos-based image encryption," Chaos, Solitons & Fractals, vol. 41, pp. 2652-2663, 2009.

[10] M. Amin, O. S. Faragallah, and A. A. Abd El-Latif, "A chaotic block cipher algorithm for image cryptosystems," Communications in Nonlinear Science and Numerical Simulation, vol. 15, pp. 3484-3497, 2010.

[11] K. Fallahi and H. Leung, "A chaos secure communication scheme based on multiplication modulation," Communications in Nonlinear Science and Numerical Simulation, vol. 15, pp. 368-383, 2010.

[12] J. Lang, R. Tao, and Y. Wang, "Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function," Optics Communications, vol. 283, pp. 2092-2096, 2010.

[13] C. Li, S. Li, and K.-T. Lo, "Breaking a modified substitution-diffusion image cipher based on chaotic standard and logistic maps," Communications in Nonlinear Science and Numerical Simulation, vol. 16, pp. 837-843, 2010.

[14] N. Singh and A. Sinha, "Chaos based multiple image encryption using multiple canonical transforms," Optics & Laser Technology, vol. 42, pp. 724-731, 2010.

[15] N. Singh and A. Sinha, "Chaos-based secure communication system using logistic map," Optics and Lasers in Engineering, vol. 48, pp. 398-404, 2010.

[16] F. Sun, Z. Lu, and S. Liu, "A new cryptosystem based on spatial chaotic system," Optics Communications, vol. 283, pp. 2066-2073, 2010.

[17] H. Yang, K.-W. Wong, X. Liao, Z. Wei, and P. Wei, "A fast image encryption and authentication scheme based on chaotic maps," Communications in Nonlinear Science and Numerical Simulation, vol. 15, pp. 3507-3517, 2010.

[18] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," Pattern Recognition Letters, vol. 31, pp. 347-354, 2010.

[19] J. W. Yoon and H. Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps," Communications in Nonlinear Science and Numerical Simulation, vol. 15, pp. 3998-4006, 2010.

[20] Q. Zhang, L. Guo, and X. Wei, "Image encryption using DNA addition combining with chaotic maps," Mathematical and Computer Modelling, vol. 52, pp. 2028-2035, 2010.

[21] A. Kumar and M. K. Ghose, "Extended substitution-diffusion based image cipher using chaotic standard map," Communications in Nonlinear Science and Numerical Simulation, vol. 16, pp. 372-382, 2011.

[22] M. Usama, M. K. Khan, K. Alghathbar, and C. Lee, "Chaos-based secure satellite imagery cryptosystem," Computers & Mathematics with Applications, vol. 60, pp. 326-337, 2010.

[23] K. Wang, W. Pei, L. Zou, A. Song, and Z. He, "On the security of 3D cat map based symmetric image encryption scheme," Physics Letters A, vol. 343, pp. 432-439, 2005.

[24] M. Asim and V. Jeoti, "On image encryption: comparison between AES and a novel chaotic encryption scheme," International Conference on Signal Processing, Communications and Networking, 2007.

[25] X. Huijuan, Q. Shuisheng, and D. Chengliang, "A composite image encryption scheme using AES and chaotic series," The First International Symposium on Data, Privacy, and E-Commerce, 2007.

[26] R. Doomun, J. Doma, and S. Tengur, "AES-CBC software execution optimization," in International Symposium on Information Technology, 2008, pp. 1-8.

[27] V. Rjimeno and J. Daemen. (2001, Announcing the Advanced Encryption Standard (AES). Available: http://csrc.nist.gov/archive/aes/index.html [28] S. Liu, L. Yu, and B. Zhu, "Optical image encryption by cascaded fractional fourier transforms with random phase filtering," Optics Communications, vol. 187, pp. 57-63, 2001.

[29] B. Hennelly and J. T. Sheridan, "Fractional fourier transform-based image encryption: phase retrieval algorithm," Optics Communications, vol. 226, pp. 61-80, 2003.

[30] W. He, X. Peng, W. Qin, and X. Meng, "The keyed optical hash function based on cascaded phase-truncated Fourier transforms," Optics Communications, vol. 283, pp. 2328-2332, 2010.

[31] M. Joshi, C. Shakher, and K. Singh, "Fractional fourier transform based image multiplexing and encryption technique for four-color images using input images as keys," Optics Communications, vol. 283, pp. 2496-2505, 2010.

[32] Q. Xu, "The asymmetrical fractional fourier transforms and its optical implement," International Journal for Light and Electron Optics, vol. 122, pp. 114-117, 2010.

[33] L. Chen and D. Zhao, "Optical image encryption based on fractional wavelet transform," Optics Communications, vol. 254, pp. 361-367, 2005.

[34] K. Martin, R. Lukac, and K. N. Plataniotis, "Efficient encryption of wavelet-based coded color images," Pattern Recognition, vol. 38, pp. 1111-1115, 2005.

[35] N. Taneja, B. Raman, and I. Gupta, "Selective image encryption in fractional wavelet domain," AEU - International Journal of Electronics and Communications, vol. 65, pp. 338-344, 2010.

[36] J. Morlet and A. Grossman, "Decomposition of hardy functions into square integrable wavelets of constant shape," SIAM J. on Mathematical Analysis, vol. 15, pp. 723-736, 1982.

[37] W. Sweldens, "The lifting scheme: A custom-design construction of biorthogonal wavelets," Applied and Computational Harmonic Analysis, vol. 3, pp. 186-200, 1996.