البحث رقم(1)

Puplished In:

IEEE TRANSACTIONS ON GEOSCIENCE AND REMOTE SENSING 1

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

Title

Combining Superresolution and Fusion Methods for Sharpening Misrsat-1 Data

Mohamed R. Metwalli, Ayman H. Nasr,
Osama S. Faragallah, S. El-Rabaie, Senior Member, IEEE, and Fathi E. Abd El-Samie

Abstract:

This paper presents an efficient technique for sharpening of Misrsat-1 data using superresolution (SR) methods and fusion methods. Due to the difference in spectral characteristics between bands 1 and 3 and the panchromatic (PAN) band of Misrsat-1, we implement SR on high details of these bands and use the resulting image to sharpen the bands of the multispectral (MS) image. Several SR methods are tested and compared in this paper for this purpose. The first class ofmethods uses spatial-domain SR, in which SR is performed on the high-pass details extracted from bands 1 and 3 and the PAN band. The superresolved high-pass details are used after that to enhance the spatial resolution of the MS data using the high-pass filter fusion method. The second class of methods depends on the interpolation of coefficients in the high-frequency subbands of a multiscale representation of bands 1 and 3 and the PAN band and an additive fusion method to add the high-frequency subband coefficients to different bands of theMS image. A comparison study between different SR methods belonging to the aforementioned classes such as nonuniform interpolation (NUI), projection onto convex sets (POCS), iterative back projection (IBP), structure-adaptive normalized convolution (SANC), and adaptive steering kernel regression (ASKR) is presented. The simulation results show that iterative SR methods such as IBP and POCS produce more noise than interpolation methods such as NUI, SANC, and ASKR. The results also reveal that combining the ASKR with a multiscale decomposition enhances the signalto- noise ratio.

Index Terms:

Fusion, Misrsat-1, superresolution (SR).

REFERENCES:

[1] T. Stathaki, Image Fusion: Algorithms and Applications, 1st ed. Amsterdam, The Netherlands: Elsevier, 2008.

[2] T. M. Maria and J. Núñez, "Super-resolution of remotely sensed images with variable-pixel linear reconstruction," IEEE Trans. Geosci. Remote Sens., vol. 45, no. 5, pp. 1446–1457, May 2007.

[3] V. Bannore, Iterative-Interpolation Super-Resolution Image Reconstruction. Berlin, Germany: Springer-Verlag, 2009.

[4] P. Vandewalle, L. Sbaiz, M. Vetterli, and S. Sustrunk, "Super-resolution from highly under-sampled images," in Proc. IEEE ICIP, 2005, vol. 1, pp. 889–892.

[5] J. C.-W. Chan, J.Ma, P. Kempeneers, and F. Canters, "Superresolution enhancement of hyperspectral CHRIS/Proba images with a thin-plate spline nonrigid transform model," IEEE Trans. Geosci. Remote Sens., vol. 48, no. 6, pp. 2569–2579, Jun. 2010.

[6] R. Y. Tsai and T. S. Huang, "Multiframe image restoration and registration," Adv. Comput. Vis. Image Process., vol. 1, pp. 317–339, 1984.

[7] B. Reddy and B. Chatterji, "An FFT-based technique for translation, rotation, and scale-invariant image registration," IEEE Trans. Image Process., vol. 5, no. 8, pp. 1266–1271, Aug. 1996.

[8] P. Vandewalle, S. Susstrunk, and M. Vetterli, "A frequency domain approach to registration of aliased images with application to superresolution," EURASIP J. Appl. Signal Process., vol. 2006, p. 233, Jan. 2006.

[9] H. Foroosh, J. Zerubia, and M. Berthod, "Extension of phase correlation to subpixel registration," IEEE Trans. Image Process., vol. 11, no. 3, pp. 188–200, Mar. 2002.

[10] J. J. Clark, M. R. Palmer, and P. D. Lawrence, "A transformation method for the reconstruction of functions from non-uniformly spaced samples," IEEE Trans. Acoust., Speech, Signal Process., vol. ASSP-33, no. 4, pp. 1151–1165, Oct. 1985.

[11] B. C. Tom and A. K. Katsaggelos, "Reconstruction of a high-resolution image by simultaneous registration, restoration, and interpolation of low resolution images," in Proc. IEEE Int. Conf. Image Process.,Washington, DC, 1995, vol. 2, pp. 539–542.

[12] J. Tian and K. Ma, "A MCMC approach for Bayesian super-resolution image reconstruction," in Proc. IEEE ICIP, 2005, vol. 1, pp. 45–48.

[13] H. Stark and P. Oskoui, “High resolution image recovery from image plane arrays, using convex projections,” J. Opt. Soc. Amer. A, Opt. Image Sci., vol. 6, no. 11, pp. 1715–1726, Nov. 1989.
[14] M. Irani and S. Peleg, “Improving resolution by image registration,” Graph. Models Image Process., vol. 53, no. 3, pp. 231–239, May 1991.
[15] S. P. Kim, N. K. Bose, and H. M. Valenzuela, “Recursive reconstruction of high resolution image from noisy undersampled multiframes,” IEEE Trans. Acoust., Speech, Signal Process., vol. 38, no. 6, pp. 1013–1027, Jun. 1990.
[16] S. C. Park, M. K. Park, and M. G. Kang, “Super-resolution image reconstruction: A technical review,” IEEE Signal Processing Mag., vol. 20, no. 3, pp. 21–36, May 2003.
[17] T. Q. Pham, L. J. van Vliet, and K. Schutte, “Robust fusion of irregularly sampled data using adaptive normalized convolution,” EURASIP J. Appl. Signal Process., vol. 2006, p. 236, Jan. 2006.
[18] H. Takeda, “Locally adaptive kernel regression methods for multidimensional signal processing,” Ph.D. dissertation, Elect. Eng., UC, Santa Cruz, CA, 2010.
[19] F. Xu, L. Xu, F. Huang, C. Huang, and A. Shi, “Robust super-resolution using kernel regression with outliers-reduction scheme,” Sci. Res. Essays, vol. 6, no. 18, pp. 3834–3844, 2011.
[20] J. Tian and K.Ma, “A survey on super-resolution imaging,” Signal, Image, Video Process., vol. 5, no. 3, pp. 329–342, 2011.
[21] H. Demirel and G. Anbarjafari, “Discrete wavelet transform-based satellite image resolution enhancement,” IEEE Trans. Geosci. Remote Sens., vol. 49, no. 6, pp. 1997–2004, Jun. 2011.
[22] N. Nguyen and P. Milanfar, “A wavelet-based interpolation–restoration method for superresolution,” Circuits Syst. Signal Process., vol. 19, no. 4, pp. 321–338, 2000.
[23] D. L. Ward, “Redundant discrete wavelet transform based superresolution using sub-pixel image registration,”M.S. thesis, Air Force Inst. Tech Wright-Patterson AFB OH Sch. Eng. Manage., Wright Patterson AFB, OH, 2003.
[24] A. A. Patil and D. J. Singhai, “Discrete curvelet transform based superresolution using sub-pixel image registration,” Int. J. Signal Image Process., vol. 4, no. 2, pp. 41–50, Jun. 2011.
[25] A. L. Cunha, J. Zhou, and M. N. Do, “The nonsubsampled contourlet transform: Theory, design, and applications,” IEEE Trans. Image Process., vol. 15, no. 10, pp. 3089–3101, Oct. 2006.
[26] Z. Wang, D. Ziou, C. Armenakis, D. Li, and Q. Li, “A comparative analysis of image fusion methods,” IEEE Trans. Geosci. Remote Sens., vol. 43, no. 6, pp. 1391–1402, Jun. 2005.
[27] T. Bretschneider and O. Kao, “Image fusion in remote sensing,” in Proc. 1st Online Symp. Electron. Eng., 2000, vol. 1, pp. 1–8.

[28] A. Amer, A. Mitiche, and E. Dubois, “Reliable and fast structure-oriented video noise estimation,” in Proc. IEEE ICIP, 2002, vol. 1, pp. 840–843.
[29] G. Xingfa, L. Xiaoying, M. Xiangjun, Y. Tao, S. Jijuan, Z. Yong, X. Hua, and G. Ding, “In flight MTF monitoring and compensation for CCD camera on CBERS-02,” Sci. China Ser. E Eng. Mater. Sci., vol. 48, no. Suppl. 2, pp. 29–43, Mar. 2005.

Authors:

Mohamed R. Metwalli received the B.Sc. and M.Sc. degrees in electrical engineering from Ain Shams University, Cairo, Egypt, in 1994 and 2002, respectively. He is currently working toward the Ph.D. degree in computer science and engineering at Menoufia University, Menouf, Egypt. He is also currently an Assistant Researcher with the Department of Digital Image Processing and Its Applications, Data Reception, Analysis and Receiving Station Affairs Division, National Authority for Remote Sensing and Space Sciences, Cairo. His areas of interest include image processing and geographic information system for different fields of remote sensing.

Ayman H. Nasr received the B.Sc., M.Sc., and Ph.D. degrees in electronics and communications from Cairo University, Cairo, Egypt. He is currently an Associate Research Professor with the National Authority for Remote Sensing and Space Sciences, Cairo, where he is also currently the Head of the Data Reception, Analysis and Receiving Station Affairs Division. He has published 28 scientific papers in various national and international journals and conferences. He has contributed in publishing four atlases and participated in more than 47 projects and research studies related to remote sensing fields. His areas of interest include image processing and geographic information system for different fields of remote sensing. This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception.

Osama S. Faragallah received the B.Sc., M.Sc., and Ph.D. degrees in computer science and engineering from Menoufia University, Menouf, Egypt, in 1997, 2002, and 2007, respectively. He is currently with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, where he was Demonstrator from 1997 to 2002 and has been a Lecturer since 2007. His research interests cover computer networks, network security, cryptography, Internet security, multimedia security, image encryption, watermarking, steganography, data hiding, and chaos theory.

S. El-Rabaie (SM'92) was born in Sires Elian, Egypt, in 1953. He received the B.Sc. degree (with honors) in radio communications from Tanta University, Tanta, Egypt, in 1976, the M.Sc. degree in communication systems from Menoufia University, Menouf, Egypt, in 1981, and the Ph.D. degree in microwave engineering from Queen's University of Belfast, Belfast, U.K., in 1986. In his doctoral research, he constructed a computer-aided design (CAD) package used in nonlinear circuit simulations based on the harmonic balance techniques. Up to February 1989, he was a Postdoctoral Fellow with the Department of Electronic Engineering, Queen's University of Belfast. He was invited as a Research Fellow in the College of Engineering and Technology, Northern Arizona University, Flagstaff, in 1992 and as a Visiting Professor at Ecole Polytechnique de Montreal, Montreal, QC, Canada, in 1994. He is currently a Professor of electronics and communications engineering with the Faculty of Electronic Engineering, Menoufia University. He has authored and coauthored more than 120 papers and technical reports and 15 books under the titles Computer Aided Simulation and Optimization of Nonlinear Active Microwave Circuits, The Whole Dictionary for the Computer and the Internet Terminologies, Basics and Technologies of Data Communications in Computer Networks, Technologies and Internet Programming, The Distance Learning and Its Technologies on the Third Millennium, Computer Principles and Their Applications in Education, Software Engineering (Volume 1), Management of Computer Networks (Volumes 1 and 2), Advanced Internet Programming, Data-Base Principles, Building of Compilers,

Software Engineering (Volume 2), and Ethics of Profession. He has participated in translating the first part of the Arabic Encyclopedia. He has been involved in different research areas, including CAD of nonlinear microwave circuits, nanotechnology, communication systems, and digital image processing. Dr. El-Rabaie was a recipient of the Egyptian Academic Scientific Research Award (Salah Amer Award of Electronics) in 1993 and 1995 and the Best Researcher Award on CAD from Menoufia University.

Fathi E. Abd El-Samie received the B.Sc.(Hons.), M.Sc., and Ph.D. degrees from Menoufia University, Menouf, Egypt, in 1998, 2001, and 2005, respectively. Since 2005, he has been a Teaching Staff Member with the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University. He is a coauthor of about 160 papers in international conference proceedings and journals. His current research areas of interest include image enhancement, image restoration, image interpolation, superresolution reconstruction of images, data hiding, multimedia communications, medical image processing, optical signal processing, and digital communications. Dr. Abd El-Samie was a recipient of the Most Cited Paper Award from the Digital Signal Processing journal in 2008.

البحث رقم (2)

Puplished In:

International Journal of Electronics and Communications (AEÜ)
journal homepage: www.elsevier.com/lo cate/aeue

Title

Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain

Osama S. Faragallah

Dept. of Computer Science & Engineering, Faculty of Electronic Engineering, Minufiya University, Menouf 32952, Egypt

Article history:

Received 5 April 2012 Accepted 26 July 2012

Keywords:

DWT Digital watermarking SVD Spatial and temporal redundancy
Multi-resolution Wavelet decomposition Attacks resilience

abstract

This paper presents an efficient, robust, and imperceptible video watermarking technique based on singular value decomposition (SVD) performed in the Discrete Wavelet Transform (DWT) domain. In the proposed DWT-based SVD video watermarking method, the video frames are transformed with the DWT using two resolution levels. The high frequency band HH and the middle frequency bands LH and HL are SVD transformed and the watermark is hidden in them. The proposed DWT-based SVD video watermarking method is characterized by two improvements: (1) a cascade of two powerful mathe-matical transforms; the Discrete Wavelet Transform (DWT)-based SVD using additive method, and (2) an error correction code is applied and embeds the watermark with spatial and temporal redundancy. The

aim of these improvements is to increase robustness against attacks based on video characteristics and the robustness against image processing attacks, realize high security level, protect the watermark against bit errors and obtain good perceptual quality. The proposed DWT-based SVD video watermarking method has been tested in the presence of video and image processing attacks and experimental results proved that the proposed DWT-based SVD video watermarking method survives attacks based on video characteristics and image processing techniques.

References:

[1] Kougianos E, Mohanty SP, Mahapatra RN. Hardware assisted watermarking for multimedia. Comput Electr Eng (Elsevier) 2009;35:339–58.

[2] Doërr G, Dugelay JL. A guide tour of video watermarking. Signal Process Image Commun 2003;18(4):263–82.

[3] Mohanty SP, Kougianos E, Ranganathan N. VLSI architecture and chip for com-bined invisible robust and fragile watermarking. IET Comput Digital Tech (CDT) 2007;1(5):600–11.

[4] Ye D, Zou C, Dai Y, Wang Z. A new adaptive watermarking for real-time MPEG videos. Appl Math Comput (Elsevier) 2007;185:907–18**.**

[5] Ling H, Wang L, Zou F, Lu Z, Li P. Robust video watermarking based on affine invariant regions in the compressed domain. Signal Process (Elsevier) 2011;91:1863–75.

[6] Wang X, Yang Y, Yang H. Invariant image watermarking using multi-scale Harris detector and wavelet moments. Comput Electr Eng (Elsevier) 2010;36: 31–44.

[7] Liu Y, Zhao J. A new video watermarking algorithm based on 1D DFT and Radon transform. Signal Process (Elsevier) 2010;90:626–39.

[8] Cho D, Do H, Choi H, Kim T. A blind MPEG-2 video watermarking robust to camcorder recording. Signal Process (Elsevier) 2010;90:1327–32.

[9] Phadikar A, Maity SP, Verma B. Region based QIM digital watermarking scheme for image database in DCT domain. Comput Electr Eng (Elsevier) 2011;37:339–55. **[10]** Biswas S, Das SR, Petriu EM. An adaptive compressed MPEG-2 video water-marking scheme. IEEE Trans Instrum Measure 2005;54:1853–61.

[11] Zhang J, Ho A, Qiu G, Marziliano P. Robust video watermarking of H.264/AVC. IEEE Trans Circuits Syst: II Express Briefs 2007;54:205–9.

[12] Dawei Z, Guanrong C, Wenbo L. A chaos-based robust wavelet domain water-marking algorithm. Chaos Solit Fract 2004;22:47–54.

[13] Al-Otum HA, Al-Taba'a AO. Adaptive color image watermarking based on a modified improved pixel-wise masking technique. Comput Electr Eng (Elsevier) 2009;35:673–95.

[14] Bao P, Ma X. Image adaptive watermarking using wavelet domain singular value decomposition. IEEE Trans Circuits Syst Video Technol 2005;15(1).

[15] Dixit M, Kulkarni P, Somasagar P, Angadi V. Variable scaling factor based invisi-ble image watermarking using hybrid DWT–SVD compression–decompression technique. In: IEEE students' conference on electrical, electronics and computer science (SCEECS). 2012. p. 978–81.

[16] Chang C, Tsai P, Lin C. SVD based digital image watermarking scheme. Pattern Recogn Lett 2005;26:1577–86.

[17] Lai CC, Tsai CC. Digital image watermarking method based on the singular value transformation and the wavelet transformation. IEEE Trans Instrum Measure 2010;26(11):3060–3.

[18] Yang G, Li J, He Y, Kang Z. An information hiding algorithm based on intra-prediction modes and matrix coding for H.264/AVC video stream. Int J Electron Commun (AE) (Elsevier) 2011;65:331–7.

[19] Yingliang H, Gaobo Y, Ningbo Z. A real-time dual watermarking algorithm of H.264/AVC video stream for Video-on-Demand service. Int J Electron Commun (AE) (Elsevier) 2012;66:305–12.

[20] Chandramouli R, Memon N. Analysis of LSB based image steganography tech-niques. In: Proceedings of the international conference on image processing, vol. 3. 2001. p. 1019–22.

[21] Langelaar G, Setyawan I, Lagendijk R. Watermarking digital image and video data. IEEE Signal Process Mag 2000;17:20–43.

[22] Mobasseri B. Direct sequence watermarking of digital video using m-frames. In: Proceedings of the international conference on image processing, vol. 2. 1998. p. 399–403.

[23] Lu W, Lu H, Chung F. Feature based robust watermarking using image normal-ization. Comput Electr Eng (Elsevier) 2010;36:2–18.

[24] Guzman V, Ramos C, Miyatake M, Meana H. Watermarking algorithm based on the DWT. IEEE Latin Am Trans 2006;4(4):257–67.

[25] Wang J, Liu JCL, Masilela M. A real-time video watermarking system with buffer sharing for video-on-demand service. Comput Electr Eng (Elsevier) 2009;35:395–414. **[26]** Maity SP, Kundu MK, Maity S. Dual purpose FWT domain spread spec-trum image watermarking in real time. Comput Electr Eng (Elsevier) 2009;35:415–33.

[27] Ramalingam A, Krishnan S. Robust image watermarking using a chirp detection-based technique. IEE Vis Image Signal Process 2005;152(6):771–8.

[28] Dietze M, Jassim S. Filters ranking for DWT domain robust digital watermarking. EURASIP J Appl Signal Process 2004:2093–101.

[29] Tao P, Eskicioglu AM. A robust multiple watermarking scheme in the DWT domain. In: Optics East 2004 symposium internet multimedia management systems V conference. 2004. p. 133–44.

[30] Tcheslavski GV. Wavelets fundamentals; April 2008. http://ee.lamar.edu/gleb/ dip/index.htm.

[31] Chan P, Lyu M. A DWT-based digital video watermarking scheme with error correcting code. Lect Note Comput Sci 2003;2836:202–13.

[32] Zou Y, Qin Q, Tian X, Xia S. Video watermarking based on adjacent frames com-parison in wavelet domain. In: Proceedings of image and signal processing conference (CISP). 2011. p. 376–80.

[33] Serdean CV, Ambroze MA, Tomlinson M, Wade JG. DWT based high-capacity blind video watermarking, invariant to geometrical attacks. In: Proceedings of the institute of electrical engineers vision image and signal processing, vol. 150. 2003. p. 51–8.

[34] Reyes R, Cruz C, Nakano-Miyatake M, Pérez-Meana H. Digital video water-marking in DWT domain using chaotic mixtures. IEEE Latin Am Trans 2010;8(3):304–10.

Biographies

Osama S. Faragallah received his BSc in 1997, MSc in 2002, and PhD in 2007, all in computer science and engi-neering, from Menoufia University, Faculty of Electronic Engineering, Egypt. He was a demonstrator at the Depart-ment of Computer Science and Engineering, at Menoufia University, from 1997 to 2002, became an assistant lec-turer in 2002, and was promoted to a lecturer in 2007. His research interests cover computer networks, net-work security, cryptography, Internet security, Medical imaging, multimedia security, image encryption, water-marking, steganographydata hiding, and chaos theory.

البحث رقم (3)

Puplished In:

Contents lists available at ScienceDirect
Chaos, Solitons and Fractals
www.elsevier.com/locate/chaosjournal homepage:

Chaos, Solitons and Fractals 42 (2009) 767–772

Title

Chaos-based hash function (CBHF) for cryptographic applications

Mohamed Amin a, Osama S. Faragallah b,
Ahmed A. Abd El-Latif a,*
a Dept. of Mathematics & Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
b Dept. of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

Article history:

Accepted 6 February 2009

abstract:

As the core of cryptography, hash is the basic technique for information security. Many of the hash functions generate the message digest through a randomizing process of the original message. Subsequently, a chaos system also generates a random behavior, but at the same time a chaos system is completely deterministic. In this paper, an algorithm for oneway hash function construction based on chaos theory is introduced. Theoretical analysis and computer simulation indicate that the algorithm can satisfy all performance requirements of hash function in an efficient and flexible manner and secure against birthday attacks or meet-in-the-middle attacks, which is good choice for data integrity or authentication.

References

[1] Menezes A, van Oorschot P, Vanstone S. Handbook of applied cryptography. New York: CRC Press; 1996.
[2] Stallings W. Cryptography and network security: principles and practice. 4th ed. Englewood Cliffs (NJ): Prentice-Hall; 2005.
[3] Peng Fei, Qiu Shui-Sheng. One-way hash functions based on iterated chaotic systems. In: IEEE conference proceedings: communications, circuits and systems, 2007. ICCCAS 2007. International conference on 11–13 July; 2007. p. 1070–74.

[4] Muhammad Khurram Khan, Jiashu Zhang, Xiaomin Wang. Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices. Chaos, Solitons & Fractals 2008;35(3):519–24.
[5] Stephen Lynch. Nonlinear discrete dynamical systems. In: Dynamical systems with applications using MATLAB. Boston: Birkhauser; 2004 [chapter 2].
[6] Baris Coskun, Nasir Memon. Confusion/Diffusion capabilities of some robust hash functions. In: IEEE conference proceedings: information sciences and systems, 2006 40th annual conference on 22–24 March; 2006. p. 1188–93.
[7] Di Xiao, Xiaofeng Liao, Shaojiang Deng. One-way hash function construction based on the chaotic map with changeable-parameter. Chaos, Solitons & Fractals 2005;24(1):65–71.
[8] Shiguo Lian, Jinsheng Sun, Zhiquan Wang. Secure hash function based on neural network. International Journal of Neurocomputing 2006;69(16–18):2346–50.

البحث رقم (4)

Puplished In:

Available online at www.sciencedirect.com
journal homepage: www.elsevier.com/locate/cose
computers & s e c u rity 3 1 (2 0 1 2) 4 3 7 e4 4 6

Title

Encryption-based multilevel model for DBMS

Ahmed I. Sallam, El-Sayed El-Rabaie, Osama S. Faragallah*
Department of Computer Science & Engineering, Faculty of Electronic Engineering, Menouf 32952, Egypt

Article history:

Received 7 September 2011
Received in revised form
31 December 2011
Accepted 13 February 2012

Keywords:

Database security Relational database Multilevel security SeaView model JajodiaeSandhu model SmitheWinslett model MLR model Belief-consistent model Multilevel database performance

Abstract

In this paper, we propose an encryption-based multilevel model for database management systems. The proposed model is a combination of the Multilevel Relational (MLR) model and an encryption system. This encryption system encrypts each data in the tuple with different field-key according to a security class of the data element. Each field is decrypted
individually by the field-key of which security class is higher than or equal to that of the encrypted field-key. The proposed model is characterized by three achievements: (1) utilizing an encryption system as an additional security layer over the multilevel security layer for the database, (2) reducing the multilevel database size, and (3) improving the response time of the data retrieval from the multilevel database. Also this paper summarizes our efforts in implementing a working multilevel secure database prototype. This prototype is used as a research tool for studying principles and mechanisms of the encryption-based multilevel model and multilevel secure database (MLS/DBMS) models (SeaView, JajodiaeSandhu, SmitheWinslett, MLR, and Belief-Consistent Model). This prototype is implemented to be used to perform a series of experiments to measure the performance cost for applying encryption in multilevel database security.

references

Bertino Elisa, Sandhu Ravi. Database security-concepts approaches, and challenges. IEEE Transaction on Dependable and Secure Computing 2005;2(1):2e19.

Cuppens Frederic, Gabillon Alban. Logical foundations of multilevel databases. Data & Knowledge Engineering 1999; 29(3):259e91.

Dave Pinal. Introduction to SQL server encryption and symmetric key encryption tutorial. Available, http://dotnetslackers.com/articles/sql/IntroductionToSQLServerEncryptionAndSymmetricKeyEncryptionTutorial.aspx; 2008.

Garuba Moses. Performance study of a cots distributed DBMS adapted for multilevel security. Ph.D. thesis, Department of Mathematics Royal Holloway, University of London, Egham, Surrey Tw20 0ex, England; 2003. Available: http://digirep.rhul.ac.uk/items/f076f347-2036-6bd0-98c8-e1d2dc9cf4ab/1/.

Garuba Moses, Appiah Edward, Burge Legand. Performance study of a MLS/DBMS implemented as a kernelized architecture. In: Proceedings of the international conference on information technology: coding and computing (ITCC'04); 2004. p. 566e70.

Imran Sohail, Hyder Irfan. Security issues in databases. In: Proceedings of the second international conference on future information technology and management engineering; 2009. p. 541e5.

Jukic Nenad A, Vrbsky Susan V. Asserting beliefs in MLS relational models. Proceedings of the SIGMOD Record 1997;26(3):30e5.

Jukic Nenad, Vrbsky Susan V, Parrish Allen, Dixon Brandon, Jukic Boris. A belief-consistent multilevel secure relational data model. Information Systems 1999;24(5):377e402.

Lee Sang-Won, Kim Yong-Han, Kim Hyoung-Joo. The semantics of an extended referential integrity for a multilevel secure relational data model. Data & Knowledge Engineering 2004; 48(1):129e52.

Pan Leon. Using criterion-based access control for multilevel database security. In: Proceedings of international symposium on electronic commerce and security; 2008. p. 518e22.

Pranjic Mario, Fertalj KreSimir, Jukic Nenad. Importance of semantics in MLS database models. In: Proceedings of the 24th international conference on information technology interfaces; 2002. p. 51e6.

Pranjic Mario, Jukic Nenad, Fertalj Krcsimir. Implementing beliefconsistent

multilevel secure relational data model: issues and solutions. In: Proceedings of the 25th international conference on information technology interfaces IT1; 2003. p. 149e54.
Rask Art, Rubin Don, Neumann Bill. Implementing row- and celllevel security in classified databases using SQL server 2005. Available, http://technet.microsoft.com/en-us/library/cc966395.aspx; 2005.
Rjaibi Walid, Bird Paul. A multi-purpose implementation of mandatory access control in relational database management systems. In: Proceedings of the 30th VLDB conference, Toronto, Canada; 2004. p. 1010e20.
Sandhu Ravi, Chen Fang. The multilevel relational (MLR) data model. ACM Transactions on Information and System Security 1998;1(1):93e132.
Zuo Xiao-Dong, Liu Feng-Mei, Ma Chao-Bin. A new approach to multilevel security based on trusted computing platform. In: Proceedings of the sixth international conference on machine learning and cybernetics, Hong Kong; 2007. p. 2158e63.

Authors:

Prof. S. El-Rabaie (Senior Member, IEEE'1992-MIEE-Chartered Electrical Engineer) was born in Sires Elian (Menoufia), Egypt in 1953. He received the B.Sc. degree with Honors in Radio Communications from Tanta University, Egypt, 1976, the M.Sc. degree in Communication Systems from Menoufia University, Egypt, 1981, and the Ph.D. degree in Microwave Device Engineering from the Queen's University of Belfast, 1986. He was a Postdoctoral Fellow at Queen's (Dept. of Electronic Eng.) up to Feb. 89. In his doctoral research he constructed a CAD package used in nonlinear circuit simulations based on the harmonic balance techniques. Since then he has been involved in the development of GaAs FET doublers, triplers and oscillators from X to K band. He was invited in 1992 as a Research Fellow in the North Arizona University (College of Engineering and Technology) and in 1994 as a visiting Prof. in Ecole Polytechnique de Montreal (Quebec), Canada. Prof. El-Rabaie has authored and co-authored more than 90 papers and

technical reports, fifteen books under the titles (Computer aided simulation and optimization of nonlinear active microwave circuits, The whole dictionary for the computer and the Internet terminologies, Basics and technologies of data communications in computer networks, Technologies and Internet programming, The distance learning and its technologies on the third millennium, computer principles and their applications in education, software engineering (1), Management of computer networks (1,2), Advanced Internet programming, data-base principles, building of compilers, software engineering (2), Ethics of profession). In 1993, he was awarded the Egyptian Academic Scientific Research Award (Salah Amer Award of Electronics) and in 1995, he received the award of the best researcher on (CAD) from Menoufia University. He has shared in translating the first part of the Arabic Encyclopedia. Now he is the Vice Dean of Postgraduate Studies and Research, Faculty of Electronic Engineering, Menoufi University. Address: Faculty of Electronic Engineering, 32952 Menouf, Egypt. E-mail: srabie1@yahoo.com, srabie1@hotmail. com. Mobile: 0184985170 e 0198699975. List of published books in computer science and educational technology:

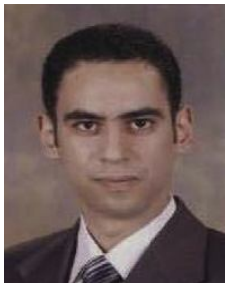
1) The whole dictionary for the computer and the Internet terminologies,
2) Basics and technologies of data communications in computer networks,
3) Technologies and Internet programming,
4) The distance learning and its technologies on the third millennium,
5) Computer principles and their applications in education,
6) Software engineering (1),
7) Management of computer networks (1),
8) Advanced Internet programming,
9) Management of computer networks (2)

10) Data-base principles,

11) Building of compilers,
12) Management of computer networks (2),
13) Ethics of profession,
14) Software engineering (2).

15) Computer aided design of nonlinear microwave circuits.

Osama S. Farag Allah was born in Menoufia, Egypt on August 29, 1974. He received B.S. in Computer Science & Engineering (1997) from Menoufia University, Faculty of Electronic Engineering, Egypt in 1997, M.Sc. in Computer Science & Engineering (2002) from Menoufia University, Faculty of Electronic Engineering, Egypt in 2002, and Ph.D. in Computer Science & Engineering (2007) from Menoufia University, Faculty of Electronic Engineering, Egypt in 2007. He was appointed as a demonstrator at the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, from 1997 to 2002. He became an Assistant Lecturer in 2002 and promoted to a Lecturer in 2007. His research interests cover Computer networks, Network security, Cryptography, Internet security, Multimedia security, Image encryption, Watermarking, Steganography, Data hiding, Chaos theory.



Ahmed I. Sallam was born in AL Gharbia, Egypt on April 10, 1982. He received B.S. in Computer Science & Engineering (2005) from Al Azhar University, Faculty of Engineering. He became a senior Software Engineer in Qarun Petroleum Company in 2008.c omp u t e r s & s e c u r i t y 3 1 (2 0 1 2) 4 3 7 e4 4 6

البحث رقم (5)

Puplished In:

Contents lists available at ScienceDirect
Commun Nonlinear Sci Numer Simulat
journal homepage: www.elsevier.com/locate/cnsns

Title

A chaotic block cipher algorithm for image cryptosystems

Mohamed Amin a, Osama S. Faragallah b,
Ahmed A. Abd El-Latif a,*
a Mathematics Department, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
b Computer Science and Engineering Department, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

Article history:

Received 13 January 2009
Received in revised form 22 December 2009

Accepted 23 December 2009
Available online 4 January 2010

Keywords:

Image cryptosystems Block cipher
Chaos Primitive operations Security analysis

a b s t r a c t

Recently, many scholars have proposed chaotic cryptosystems in order to promote communication security. However, there are a number of major problems detected in some of those schemes such as weakness against differential attack, slow performance speed, and unacceptable data expansion. In this paper, we introduce a new chaotic block cipher scheme for image cryptosystems that encrypts block of bits rather than block of pixels. It encrypts 256-bits of plainimage to 256-bits of cipherimage within eight 32-bit registers. The scheme employs the cryptographic primitive operations and a non-linear transformation function within encryption operation, and adopts round keys for encryption using a chaotic system. The new scheme is able to encrypt large size of images with superior performance speed than other schemes. The security analysis of the new scheme confirms a high security level and fairly uniform distribution.

References

[1] Lian Shiguo. Efficient image or video encryption based on spatiotemporal chaos system. Chaos Soliton Fract 2009;40(5):2509–19.
[2] Pareek NK, Patidar V, Sud KK. Image encryption using chaotic logistic map. Image Vision Comput 2006;24:926–34. doi:10.1016/j.imavis.2006.02.021.
[3] Gao Haojiang, Zhang Yisheng, Liang Shuyun, Li Dequn. A new chaotic algorithm for image encryption. Chaos Soliton Fract 2006;29(2):393–9.
[4] Gao T, Chen Z. Image encryption based on a new total shuffling algorithm. Chaos Soliton Fract 2008;38(1):213–20.
[5] Gao T, Gu Q, Chen Z. A new image encryption algorithm based on hyper-chaos. Phys Lett A 2008;374(4):394–400.
[6] Behnia S, Akhshani A, Mahmodi H, Akhavan A. A novel algorithm for image encryption based on mixture of chaotic maps. Chaos Soliton Fract 2008;35(2):408–19.

[7] Behnia S, Akhshani A, Mahmodi H, Akhavan A. Applications of tripled chaotic maps in cryptography. Chaos Soliton Fract 2009;40(1):505–19.
[8] Chen G, Mao Y, Chui CK. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Soliton Fract 2004;21(3):749–61.
[9] Kwok HS, Wallace K, Tang S. A fast image encryption system based on chaotic maps with finite precision representation. Chaos Soliton Fract 2007;32(4):1518–29.
[10] Xing-yuan Wang, Qing Yu. A block encryption algorithm based on dynamic sequences of multiple chaotic systems. Commun Nonlinear Sci Numer Simul 2009;14(2):574–81.
[11] Rhouma Rhouma, Belghith Safya. Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem. Phys Lett A 2008;372:5790–4.
[12] Alvarez G, Li S. Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption. Commun Nonlinear Sci Numer Simul 2009;14(11):3743–9.
[13] Rhouma Rhouma, Belghith Safya. Cryptanalysis of a new image encryption algorithm based on hyper-chaos. Phys Lett A 2008;372:5973–8.
[14] Mao Y, Chen G, Lian S. A novel fast image encryption scheme based on 3D chaotic baker maps. Int J Bifurcation Chaos 2003.
[15] Wang K, Pei Ws, Zou L, Song A, He Z. On the security of 3D Cat map based symmetric image encryption scheme. Phys Lett A 2005;343(6):432–9.
[16] Li C. On the security of a class of image encryption schemes, IACR's Cryptology ePrint Archive, Report 2007/339; 2007.
[17] Amin Mohamed, Faragallah Osama S, Abd El-Latif Ahmed A. Chaos-based hash function (CBHF) for cryptographic applications. Chaos Soliton Fract 2009. doi:10.1016/j.chaos.2009.02.001.
[18] Schneier Bruce. Applied cryptography – protocols, algorithms, and source code in C. 2nd ed. New York: John Wiley & Sons, Inc.; 1996.
[19] Ahmed Hossam El-din H, Kalash Hamdy M, Faragallah Osama S. Encryption efficiency analysis and security evaluation of RC6 block cipher for digital images. Int J Comput Inform Syst Sci Eng 2007;1(1):33–9. ISSN 1307-2331.
[20] Peng Jun, Jin Shangzhu, Chen Guorong, Yang Zhiming, Liao Xiaofeng. An image encryption scheme based on chaotic map. In: IEEE Conference Proceedings: fourth international conference on natural computation. doi:10.1109/ICNC.2008.227.
[21] Ahmed Hossam El-din H, Kalash Hamdy M, Faragallah Osama S. An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption. Int J Comput Inform 2007;31(1):121–9. ISSN 0350–5596.
Table 8 Performance of our scheme and other schemes.
Image size (in pixels) Image size on disk Encryption time (s) Proposed RC5 RC6
512 _ 512 257 KB 0.007 0.046 0.031
1024 _ 1024 1.00 MB 0.015 0.054 0.047

2048 _ 2048 4.00 MB 0.093 0.281 0.171
4096 _ 4096 16.00 MB 0.500 1.054 0.703
8192 _ 8192 64.00 MB 1.906 4.193 2.786

[22] Mazloom Sahar, Eftekhari-Moghadam Amir Masud. Color image encryption based on coupled nonlinear chaotic map. Chaos Soliton Fract 2009;42(3):1745–54.
[23] Shannon CE. Communication theory of secrecy system. Bell Syst Tech J 1949;28:656–715.
[24] Wei-bin Chen, Xin Zhang, Image encryption algorithm based on Henon chaotic system. In: International conference on image analysis and signal processing. IASP 2009, 11–12 April; 2009. p. 94–7. doi:10.1109/IASP.2009.5054653.
[25] Behnia S, Akhshani A, Akhshani A, Mahmodi H, Akhavan A. A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps. Phys Lett A
2007;366:391–6.
[26] Sun Fuyan, Liu Shutang, Li Zhongqin, Lü Zongwang. A novel image encryption algorithm based on spatial chaos map. Chaos Soliton Fract 2008;38:631–40.
[27] Elashry Ibrahim F, Farag Allah Osama S, Abbas Alaa M, El-Rabaie S, Abd El-Samie Fathi E. Homomorphic image encryption. J Electron Imaging 2009;18(3):033002.

M. Amin et al. /Commun Nonlinear Sci Numer Simulat 15 (2010) 3484–3497

البحث رقم (6)

Title

Divided two-part adaptive intrusion detection system

Nawal A. Elfeshawy • Osama S. Faragallah
N. A. Elfeshawy _ O. S. Faragallah (&)
Deptartment of Computer Science and Engineering, Faculty of Electronic Engineering, Minufiya University, Menouf 32952, Egypt
e-mail: osam_sal@yahoo.com

Abstract :

The main objective of this paper is to design a more complete intrusion detection system solution. The paper presents an efficient approach for reducing the rate of alerts using divided two-part adaptive intrusion detection system (DTPAIDS). The proposed DTPAIDS has a high degree of autonomy in tracking suspicious activity and detecting positive intrusions. The proposed DTPAIDS is designed with the aim of reducing the rate of detected false positive intrusion through two achievements. The first achievement is done by implementing adaptive self-learning neural network in the proposed DTPAIDS to gives it the ability to be automatic adaptively system based on Radial Basis Functions (RBF) neural network. The second achievement is done through dividing the proposed intrusion detection system IDS into two parts. The first

part is IDS1, which is installed in the front of firewall and responsible for checking each entry user's packet and deciding if the packet considered is an attack or not. The second is IDS2, which is installed behind the firewall and responsible for detecting only the attacks which passed the firewall. This proposed approach for IDS exhibits a lower false alarm rate when detects novel attacks. The simulation tests are conducted using DARPA 1998 dataset. The experimental results show that the proposed DTPAIDS [1] reduce false positive rate, [2] detects intrusion occurrence sensitively and precisely, [3] accurately self–adapts diagnose model, thus improving its detection accuracy.

Keywords:

Intrusion detection system (IDS)_FPs_RBF neural network_Anomaly intrusion detection system_Misuse detection_Intrusion prevention system (IPS)_Neural network

References

1. Symantec-Internet Security threat report highlights (Symantec. com), http://www.prdomain.com/companies/Symantec/new releases/Symantec_internet_205032.htm.

2. Ulvila, J., & Gaffney, J. (2003). Evaluation of intrusion detection systems. Journal of Research of the National Institute of Standards and Technology, 108(6), 453–473.

3. Guofei, G., Fogla, P., Dagon, D., Lee, W., & Skoric, B. (2006). Measuring intrusion detection capability: an information-theoretic approach. In proceedings of the, computer and communications security, pp. 90–101.

4. Durst, R., Champion, T., & Witten, B. (1999). Testing and evaluating computer intrusion detection systems. Communications of the ACM, 42(7), 53–61.

5. Linda, O., Vollmer, T., & Manic, M. (2009). Neural network based intrusion detection system for critical infrastructures, IJCNN'09, international joint INNS-IEEE conference on neural networks, Atlanta, Georgia, pp. 15–23.

6. Drum, R. (2006). IDS and IPS placement for network protection, CISSP, pp. 152–160.

7. Zhou, J., Carlson, A. J., & Bishop, N. (2005). Verify results of network intrusion alerts using lightweight protocol analysis, computer security applications conference IEEE computer society, pp. 52–60.

8. Hooper, E. (2006). An intelligent detection and response strategy to false positives and network attacks. In proceedings of the fourth IEEE international

Workshop on information assurance, University of London, Royal Holloway, United Kingdom, IEEE
Computer Society Press, pp. 12–31.
9. Al-Allouni, H., Shaarawy, M., & Taha, I. (2003). An intrusion detection approach to computer networks, Technical report, Department of Computer Engineering, Military Technical College, pp. 90–120.
10. Georgios, P, & Sokratis, K. (2009). Reducing false positives in intrusion detection systems, Department of Computer Science and Biomedical Informatics, University of Central Greece, available on Science Direct Search.
11. Lippmann, R., Haines, J. W., & Fried, D. J. (2000). The 1999 DARPA Off-line intrusion detection evaluation. The International Journal of Computer and Telecommunications Networking, 34(4), 579–595.
12. Kurose, J., & Ross, K. (2001). Computer networking: A top-down approach featuring the internet. Boston: Addison-Wesley.
13. Saaty, T. L., (2000). Fundamentals of decision making and priority theory with the analytic hierarchy process, 2nd edn, RWS Publications, Pittsburgh, PA. 478 pp., ISBN 0-9620317-6-3.
14. Alghamdi, A. S. (2009). Evaluating defense architecture frameworks for C4I system using analytic hierarchy process. Journal of Computer Science, 5(12), 1075–1081.
15. Forman, E. H., & Gass, S. I. The analytical hierarchy process-an exposition. Operations Research 49, 469–487, doi:10.1287/opre. 49.4.469.11231.
16. Bhushan, N., & Rai, K. (2004). Strategic decision making: Applying the analytic hierarchy process. Springer, London, ISBN: 1-8523375-6-7, p. 171.
17. Ahmad, I., Abdullah, A. B., Alghamdi, A. S. (2009). Application of artificial neural network in detection of DOS attacks. In proceedings of the 2nd international conference on security of information and Networks (Famagusta, North Cyprus, October 06–10, 2009). SIN '09. ACM, New York, NY, pp. 229–234.
18. Javitz, H. S., & Valdes, A. (1993). The NIDES statistical component: Description and justification, SRI International.
19. Kai, H., Zhengwei, Q., & Liu, B. (2009). Network anomaly detection based on statistical approach and time series analysis, waina, pp. 205–211, 2009 IEEE international conference on advanced information networking and applications workshops, Bradford, United Kingdom, May 26–May 29, ISBN: 978-0-7695-
3639-2.
20. Lee, W., Stolfo, S. J., & Mok, K. W. (1999). A data mining framework for building intrusion detection models. Proceedings of the 20th IEEE symposium on security and privacy, Oakland, CA.

21. Lee, W., & Stolfo, S. J. (1998). Data mining approaches for Intrusion detection system. Proceedings of the 7th USENIX security symposium, San Antonio, TX.
22. Portier, B., & Froment, J. (2000). Data mining techniques for Intrusion detection,'' Data mining term paper, The University of Texas, Spring 2000.
23. Marin, J., Ragsdale, D., & Surdu, J. (2001). A hybrid approach to the profile creation and intrusion detection, DARPA information survivability conference and exposition (DISCEX II'01), Vol I.
24. Shieh, S.-P. & Gligor, V. D. (1997). On a patter-oriented model for intrusion detection, IEEE transactions on knowledge and data engineering, Vol. 9, No. 4.
25. Shieh, S. -P., & Gligor, V. D. (1991). A pattern-oriented intrusion detection system and its applications. Proceedings of IEEE symposium research in security and privacy. Oakland, CA. pp. 327–342.
26. Kumar, S. (1995). Classification and detection of computer intrusions, Ph.D. dissertation, Purdue University.
27. Ilgun, R., Kemmerer, A., & Porras, P. A. (1995). State transition analysis: A rule- based intrusion detection approach, IEEE transactions on software engineering, pp. 181–199.
28. Lindqvist, U., & Porras, P. A. (1999). Detecting computer and network misuse through the production based expert system toolset (P-BEST). Proceedings of the 1999 IEEE symposium on security and privacy, Oakland, California. Wireless Netw
29. Lindqvist, U., & Porras, P. A. (2001). Expert -BSM: A hostbased intrusion detection solution for sun solaris. Proceedings of the 17th annual computer security applications conference, pp. 240–251, New Orleans, Louisiana Dec. 10–14, published by the IEEE Computer Society.
30. Golovko, V., & Kochurko, P. (2005). Intrusion recognition using neural networks, IEEE workshop on intelligent data acquisition and advanced computing systems: Technology and applications, Sofia, Bulgaria, pp. 108–111, 5–7 September.
31. Zhong, J., Li, Z., Feng, Y., & Ye, C. (2006). Intrusion detection based on adaptive RBF neural network. IEEE proceedings of the sixth international conference on intelligent systems design and applications, pp. 1081–1084.
32. Montazer, G. A., Sabzevari, R., & Khatir, H. G. (2007). Improvement of learning algorithms for RBF neural networks in a helicopter sound identification system. Neurocomputing, 71(1–3), 167–173.
33. Kruegel, C., Robertson, W., & Vigna, G. (2004). Using alert verification to identify successful intrusion attempts (pp. 80–89). Munchen: K.G. Saur Verlag.
34. Alfantookh, A. (2006). DoS attacks intelligent detection using neural networks. Journal of King Saud University, 18(12), 27–45.

35. Kruegel, C., Toth, T., & Kirda, E. (2008). Anomaly intrusion detection system. International Journal of Computer Science and Network Security, 8(8), 258–264.
36. Vollmer, T., & Manic, M. (2009). Human interface for cyber security anomaly detection systems. Second IEEE conference on human system interaction, Catania, Italy, pp. 121–129.
37. Julisch, K. (2003). Clustering intrusion detection alarms to support root cause analysis. TISSEC, 6(4), 443–471.
38. Ranum, M. J. (2003). False positives: A user's guide to making sense of IDS alarms, ICSA Labs IDSC.
39. Pietraszek, T. (2004). Using adaptive alert classification to reduce false positives in intrusion detection,'' RAID, Vol. 3224 of LNCS, Springer, pp. 102–124.
40. Hooper, E. (2006). An intelligent detection and response strategy to false positives and network attacks. In proceedings of the fourth IEEE international workshop on information assurance, University of London, Royal Holloway, United Kingdom, IEEE Computer Society Press, pp. 12–31.
41. Georgios, P., & Sokratis, K. (2009). Reducing false positives in intrusion detection systems, Deptartment of Computer Science and Biomedical Informatics, University of Central Greece, Science Direct Search.
42. Al-Allouni, H., Shaarawy, M., & Taha, I. (2003). An intrusion detection approach to computer networks. Technical report, Deptartmet of Computer Engineering, Military Technical College, pp. 90–120.
43. Kurose, J., & Ross, K. (2001). Computer networking: A top-down approach featuring the internet. Boston: Addison-Wesley.
44. Lippmann, R., Haines, J., & Fried, D. (2000). Analysis and results of the 1999 DARPA off-line intrusion detection evaluation. Proceedings of the 3rd international workshop on recent advances in intrusion detection, pp. 162–182.
45. Levin, I. (2000). KDD classifier learning contest. SIGKDD Explorations, ACM, SIGKDD, pp. 67–75.
46. Bolzoni, D., Crispo, B., & Etalle, S. (2007). An architecture for alert verification in network intrusion detection systems. 21st large installation system administration conference, pp. 141–152.
47. Kayacik, H., Heywood, A., & Heywood, I. (2006). A hierarchical SOM based intrusion detection system. Technical report, Faculty of Computer Science, Dalhousie University, pp. 11–150.
48. Golovko, V., & Vaitsekhovich, L. (2009). Intrusion detection in TCP/IP networks using immune systems paradigm and neural network detectors. PhD thesis, Brest State Technical University, Brest, Belarus, pp. 15–169.

Author Biographies

Nawal A. Elfeshawy received the Ph.D. degree in mobile communications the faculty of Electronic Eng., Menoufia university, Menouf, Egypt, in collaboration with Southampton university in 1991. Now she is the head of Computer Science and Engineering Dept., Faculty of Electronic Eng. Her research interest includes computer communication networks with emphasis on protocol design, traffic modeling and performance evaluation of broadband networks and multiple access control protocols for wireless communications systems and networks. Now she directed her research interests to the developments of security over wireless communications networks (mobile communications, WLAN, Bluetooth), VOIP, and encryption algorithms. She has served as a reviewer for many national and international journals and conferences. Also she participated in many technical program committees of major international conferences in wireless communications.

Osama S. Faragallah received his B.S. in 1997, MSc in 2002 and Ph.D. in 2007, all in Computer Sciences and Engineering from Menoufia University, faculty of Electronic Engineering, Egypt. He was a demonstrator at the Department of Computer Sciences and Engineering, at Menoufia University, from 1997 to 2002, become an assistant lecturer in 2002 and was promoted to a lecturer in 2007. His research interests cover computer networks, network security, cryptography, Internet security, multimedia security, image encryption, watermarking, stenography, data hiding and chaos theory.

البحث رقم (7)

Puplished In:

Journal of Electronic Imaging 21(2), 023024 (Apr–Jun 2012)

Title

Enhanced semi-automated method to identify the endo-cardium and epi-cardium borders

Osama S. Faragallah
Minufiya University
Department of Computer Science and Engineering
Faculty of Electronic Engineering
Menouf 32952, Egypt
E-mail: osam_sal@yahoo.com

Abstract:

We present two semi-automatic solution methods for the three dimensional (3D) segmentation of cavity and myocardium from a 3D cardiac multislice CT (MSCT) data. The main framework of the segmentation algorithms is based on random walks, in which the novelty lies in a seeds-selection method composed of region growing technique and morphological operation to locate and identify the cavity and myocardium of the left ventricle (LV). In the first solution, a semi-automatic segmentation approach (Method_1) is suggested to extract the epi-cardium and endo-cardium boundaries of LV of the heart. This proposed solution depends on the use of the normal random walker algorithm.

In the second solution, a semiautomatic segmentation approach (Method_2) based on improved
random walks is proposed. Segmentation is done within the framework of toboggan algorithm in combination with a random walk based technique. The two proposed semi-automatic segmentation methods either based on the normal random walker or the improved random walker algorithms utilized six-connected lattice topology and a conjugate gradient method to promote the segmentation performance of the 3D data. The two semi-automatic solution methods were evaluated using 20 cardiac MSCT datasets. Semi-automatic generated contours were compared to expert contours. For Method_1, 83.4% of epi-cardial contours and 74.7% of endo-cardial contours had a maximum error of 5mm along 95% of the contour arc length. For Method_2, those numbers were 94.3% (epi-cardium) and 92.3% (endo-cardium), respectively. Volume regression analysis revealed good linear correlations between manual and semiautomatic volumes, $r \geq 0.99$.
 [DOI: 10.1117/1.JEI.21.2.023024]

References

1. A. Rodgers and P. Vaughan, Reducing risks, promoting healthy life, Report No.: The 2002 World Health Report, World Health Organisation, Geneva, Switzerland (2002).
2. Integrated Management of cardiovascular Risk, World Health Organization, Geneva, Switzerland, p. 35 (2002). 9241562242
3. J. Leal, R. Luengo-Fernandez, and A. Gray, European cardiovascular disease statistics. British Heart Foundation, S. Petersen, V. Peto, and M. Rayner, Eds., British Heart Foundation, London, England (2005).
4. "Cardiovascular Diseases (CVDs)," World Health Organization, http://www.who.int/mediacentre/factsheets/fs317/en/index.html (September 2011).
5. L. M. Boxt, "CTAnatomy of the heart," Int. J. Cardiovasc. Imag. 21(1), 13–27 (2005).
6. M. Lynch, O. Ghita, and P. F. Whelam, "Automatic segmentation of the left ventricle vavity and myocardium in MRI data," Comput. Biol. Med. 36(4), 389–407 (2006).
7. O. Rabit, "Quantitative analysis of cardiac function," in Handbook of Medical Imaging: Processing and Analysis, I. N. Bankman, Ed., pp. 359–374, Academic Press, San Diego (2000).
8. K. S. Fu and J. K. Mui, "A survey on image segmentation," Pattern Recogn. 13(1), 3–16 (1981).
9. R. Duda, P. Hart, and D. Stork, Pattern Classification, Wiley-Interscience, New York (2000).

10. I. Bankman, Handbook of Medical Imaging: Processing and Analysis, Academic Press, San Diego (2000).
11. E. Angelini et al., “LV volume quantification via spatiotemporal analysis of real-time 3-D echocardiography,” IEEE Trans. Med. Imag. 20(6), 457–469 (2001).
12. T. R. Nelson and T. T. Elvins, “Visualization of 3D ultrasound data,” IEEE Comput. Graph. Appl. 13(6), 50–57 (1993).
13. V. Sorrell et al., “Left ventricular endocardial and epicardial border length delineation with perflutren contrast during transthoracic echocardiography,” Echocardiography 28(7), 761–766 (2011).
14. F. Orderud, G. Kiss, and H. Torp, “Automatic coupled segmentation of endo- and epicardial borders in 3D echocardiography,” IEEE Ultrasound Process. Symp., pp. 1749–1752, Norwegian Univ. Sci. & Technol. (NTNU), Trondheim (2008).
15. C. Kervrann and F. Heitz, “Statistical deformable model-based segmentation of image motion,” IEEE Trans. Image Process. 8(4), 583–588 (1999).
16. S. Mitchell et al., “Multistage hybrid active appearance model matching: segmentation of left and right ventricles in cardiac MR images,” IEEE Trans. Med. Imag. 20(5), 415–423 (2001).
17. J. C. Bezdek, L. O. Hall, and L. P. Clarke, “Review of MR image segmentation techniques using pattern recognition,” Med. Phys. 20(4), 1033–1048 (1993).
18. T. Fuchs, M. Kachelriess, andW. Kalender, “Systems performance multislice spiral computed tomography,” IEEE Eng. Med. Biol. Mag. 19(5), 63–70 (2000).
19. M. Krishnam et al., “Left ventricular ejection fraction using 64-slice CT coronary angiography and new evaluation software: initial experience,” Br. J. Radiol. 81(966), 450–455 (2008).
20. N. Lin,W. Yu, and J. Duncan, “Combinative multi-scale level set framework for echocardiographic image segmentation,” Med. Image Anal. 7(4), 529–537 (2003).
21. M. Lynch, O. Ghita, and P. F. Whelan, “Segmentation of the left ventricle of the heart in 3-D MRI data using an optimized nonrigid temporal model,” IEEE Trans. Med. Imag. 27(2), 195–203 (2008).
22. N. Paragios, “A level set approach for shape-driven segmentation and tracking of the left ventricle,” IEEE Trans. Med. Imag. 22(6), 773–776 (2003).
23. A. Sarti et al., “Maximum likelihood segmentation of ultrasound

images with Rayleigh distribution," IEEE Trans. Ultrason. Ferroelectr. Freq. Control 52(6), 947–960 (2005).
24. T. Chen et al., "Semiautomated segmentation of myocardial contours for fast strain analysis in cine displacement-encoded MRI," IEEE Trans. Med. Imag. 27(8), 1084–1094 (2008).
25. J. C. Nascimento and J. S. Marques, "Robust shape tracking with multiple models in ultrasound images," IEEE Trans. Image Process. 17(3), 392–406 (2008).
26. V. Zagrodsky et al., "Registration-assisted segmentation of real-time 3-D echocardiographic data using deformable models," IEEE Trans. Med. Imag. 24(9), 1089–1099 (2005).
27. G. Carneiro, J. C. Nascimento, and A. Freitas, "Robust left ventricle segmentation from ultrasound data using deep neural networks and efficient search methods," in From Nano to Macro, 2010 IEEE Int. Symp. on Biomedical Imaging, Rotterdam, pp. 1085–1088 (2010).
28. G. Carneiro and J. C. Nascimento, "Multiple dynamic models for tracking the left ventricle of the heart from ultrasound data using particle filters and deep learning architectures," in 2010 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), San Francisco, CA, pp. 2815–2822 (2010).
29. G. Carneiro et al., "Detection and measurement of fetal anatomies from ultrasound images using a constrained probabilistic boosting tree," IEEE Trans. Med. Imag. 27(9), 1342–1355 (2008).
30. L. Grady and G. Funka-Lea, "Multi-label image segmentation for medical applications based on graph-theoretic electrical potentials," ECCV, pp. 230–245, Springer Berlin/Heidelberg, Prague, Czech Republic (2004).

31. L. Grady, "Random walks for image segmentation," IEEE Trans. Pattern Anal. Mach. Intell. 28(11), 1–17 (2006).
32. N. Paragios and R. Deriche, "Geodesic active regions and level set methods for supervised texture segmentation," Int. J. Comput. Vis. 46(3), 223–247 (2002).
33. L. Zhang and E. Geiser, "An effective algorithm for extracting serial endocardial borders from 2-D echocardiograms," IEEE Trans. Biomed. Eng. BME-31(6), 441–447 (1984).
34. M. Sonka et al., "Segmentation of intravascular ultrasound images: a knowledge-based approach," IEEE Trans. Med. Imag. 14(4), 719–732 (1995).
35. M. Kass, A. Witkin, and D. Terzopoulos, "Snakes: active contour models,"

Int. J. Comput. Vis. 1(4), 321–331 (1998).
36. O. Bernard et al., “Variational B-spline level-set: a linear filtering approach for fast deformable model evolution,” IEEE Trans. Image Process. 18(6), 1179–1191 (2009).
37. I. Ben Ayed, S. Li, and I. Ross, “Embedding overlap priors in variational left ventricle tracking,” IEEE Trans. Med. Imag. 28(12), 1902–1913 (2009).
38. T. Cootes et al., “Active shape models-their training and application,” Comput. Vis. Imag. Understand. 61(1), 38–59 (1995).
39. T. Cootes et al., “A unified framework for atlas matching using active appearance models,” in Proc. Inf. Process. Med. Imag. LNCS, Vol. 1613, pp. 322–333 (1999).
40. S. Mitchell et al., “Multistage hybrid active appearance model matching: segmentation of left and right ventricles in cardiac MR images,” IEEE Trans. Med. Imag. 20(5), 415–423 (2001).
41. B. Georgescu et al., “Database guided segmentation of anatomical structures with complex appearance,” in IEEE Computer Society Conference on Computer Vision and Pattern Recognition, San Diego, USA, pp. 429–436 (2005).
42. P. Balzer et al., “Simultaneous and correlated detection of endocardial and epicardial borders on short-axis MR images for the measurement of left ventricular mass,” Radiographics 18(4), 1009–1018 (1998).
43. Y. Zheng et al., “Four-chamber heart modeling and automatic segmentation
for 3-D cardiac CT volumes using marginal space learning and steerable features,” IEEE Trans. Med. Imag. 27(11), 1668–1681 (2008).
44. L. Grady, “Space-variant computer vision: a graph-theoretic approach,” PhD Thesis, Boston Univ. (2004).
45. P. Doyle and L. Snell, Random Walks and Electric Networks, Vol. 22, Math. Assoc. of Am. Cornell Univ. (1984).
46. F. Harary, Graph Theory, Addison-Wesley, Massachusetts, USA (1994).
47. J. Roth, “An application of algebraic topology to numerical analysis: on the existence of a solution to the network problem,” Proc. Natl. Acad. Sci. U S A 41, 518–521 (1955).
48. J. Dodziuk, “Difference equations, isoperimetric inequality and the transience of certain random walks,” Trans. Am. Math. Soc. 284(2), 787–794 (1984).
49. G. Li, L. Qingsheng, and C. Jian, “A new fast random walk segmentation algorithm,” 2nd Intell. Info. Technol. Appl., Vol. 2, pp. 693–697 (2008).
50. J. Fairfield, “Toboggan contrast enhancement for contrast segmentation,” in IEEE Proc. 10th Int. Conf. Patt. Recog., Vol. 1, pp. 712–

716 (1990).
51. X. Yao and Y. P. Hung, “Fast image segmentation by sliding in the derivative
terrain,” Proc. SPIE 1607, 369–379 (1992).
52. Y.-C. Lin et al., “Comparison between immersion-based and tobogganbased
watershed image segmentation,” IEEE Trans. Image Process.
15(3), 632–640 (2006).
53. A. K. Sinop and L. Grady, “A seeded image segmentation framework unifying graph cuts and random walker which yields a new algorithm,” Proc. ICCV. (2007).
54. W. E. Higins, N. Chung, and E. L. Ritman, “Extraction of left ventricle chamber from 3D CT images of the heart,” IEEE Trans. Med. Imag. 9, 384–395 (1990).
55. J. Xuan, T. Adali, and Y. Wang, “Segmentation of magnetic resonance brain image: integrating region growing and edge detection,” Proc. Int. Conf. Imag. Process., Vol. 3, pp. 544–547 (1995).
56. M. S. Nixon and A. S. Aguado, Feature Extraction and Image Processing, 1st ed., Newnes (2002).
57. L. Grady and M. Jolly, “Weights and topology: a study of the effects of graph construction on 3D image segmentation,” Med. Imag. Comput. Assist Interv. 11(1), 153–161 (2008).
58. R. Magnus and E. Stiefel, “Methods of conjugate gradients for solving linear systems,” J. Res. Natl. Bur. Stand. 49, 409–436 (1952).
59. R. Barrett, M. Berry, and T. Chan, “Templates for the solution of linear systems: building blocks for iterative methods,” SIAM, 2nd ed., Philadelphia (1994).
60. M. de Bruijne and M. Nielsen, “Shape particle filtering for image segmentation,” in Proc. MICCAI, LNCS, Vol. 3216, pp. 168–175, Springer (2004).

Biographies

Osama S. Faragallah received his BS in computer science and engineering, MSc in computer science and engineering, and PhD in computer science and engineering from Menoufia University, Egypt in 1997, 2002, and 2007, respectively. He was appointed as a demonstrator at the Department

of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, from 1997 to 2002. He became an assistant lecturer in 2002, and was promoted to a lecturer in 2007. His research interests cover computer networks, network security, cryptography, medical image processing, internet security, multimedia security, image encryption, watermarking, steganography, data hiding, and chaos theory.

البحث رقم (8)

Puplished In:

Journal of Electronic Imaging 18(3), 033002 (Jul–Sep 2009)

Title

Homomorphic image encryption

Ibrahim F. Elashry
Kafrelshiekh University
Faculty of Engineering
Department of Electrical Communications
Kafrelshiekh, Egypt
Osama S. Farag Allah
Menoufia University
Faculty of Electronic Engineering
Department of Computers Engineering
Menouf, Egypt
Alaa M. Abbas
S. El-Rabaie
Fathi E. Abd El-Samie
Menoufia University
Faculty of Electronic Engineering

Department of Electronics and Electrical Communications
Menouf, Egypt
E-mail: fathi_sayed@yahoo.com

Abstract:

This paper presents a new homomorphic image cryptosystem. The idea of this system is based on encrypting the reflectance component after the homomorphic transform and embedding the illumination component as a least significant bit watermark into the encrypted reflectance component. A comparison study is held between the RC6 block cipher algorithm and the chaotic Baker map algorithm for the encryption of the reflectance component. We present a security analysis for the proposed cryptosystem against the entropy, brute-force, statistical, and differential attacks from a strict cryptographic viewpoint. Experimental results verify and prove that the proposed homomorphic image cryptosystem is highly secure from the cryptographic viewpoint. The results also prove that this cryptosystem has a very powerful diffusion mechanism (a small change in the plain text makes a great change in the cipher image). The homomorphic encryption using RC6 algorithm is more secure than that using the chaotic Baker map algorithm but not robust to noise. Thus, the proposed homomorphic cryptosystem can be used in different applications, depending on the core algorithm used. © 2009 Society of Photo-Optical Instrumentation Engineers. _DOI: 10.1117/1.3167847_

References:

1. National Bureau of Standards, Data Encryption Standard, Federal Information
Processing Standards Publication No. 46, U.S. Government Printing Office, Washington, DC _1977_.
2. National Bureau of Standards, Data Encryption Standard Modes of Operation, Federal Information Processing Standards Publication No. 81, U.S. Government Printing Office, Washington, DC _1980_.
3. R. L. Rivest, “The RC5 encryption algorithm,” Dr. Dobb’s J. 226_3_, 146–148 _1995_.
4. J. Daemen and V. R. Rijndael, “The advanced encryption standard,” Dr. Dobb’s J. 26_3_, 137–139 _2001_.

5. N. Singh and A. Sinha, “Optical image encryption using fractional Fourier transform and chaos,” Opt. Lasers Eng. 46_2_, 117–123 _2007_.
6. G. Alvarez and S. Li, “Some basic cryptographic requirements for chaos-based cryptosystems,” Int. J. Bifurcation Chaos Appl. Sci. Eng. 16_8_: 2129–2151 _2006_.
7. S. C. Koduru, and V. Chandrasekaran, “Integrated confusiondiffusion mechanisms for chaos based image encryption” in IEEE 8th Int. Conf. Computer and Information Technology Workshops, pp. 260–263 _2008_.
8. Y. B. Mao, G. Chen, and S. G. Lian, “A novel fast image encryption scheme based on the 3D chaotic baker map,” Int. J. Bifurcation Chaos Appl. Sci. Eng. 14_10_, 3613–3624 _2004_.
9. E. Bradley, “Autonomous exploration and control of chaotic systems,” IEEE Trans. Syst. Man Cybern. 26_5_, 499–519 _1995_.
10. J. Fridrich, “Secure image ciphering based on chaos,” Final report _April, 1997_.
11. G. Chen, Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3d chaotic cat maps,” Chaos, Solitons Fractals 21_3_, 749–761 _2004_.
12. J. S. Lim, Two-Dimensional Signal and Image Processing, Prentice Hall, Englewood Cliffs, NJ _1990_.
13. S. Li, X. Zheng, X. Mou, and Y. Cai, “Chaotic encryption scheme for real-time digital video,” Proc. SPIE 4666, 149–160 _2002_.
14. S. Lee, J. Wook Han, and D. Seo, “Optical encryption and decryption using personal fingerprint image,” presented at the 6th Int. at Conf. on Advanced Communi. Technol., Vol. 1, pp. 413–415 _2004_.
15. B. Schneier, Applied Cryptography—Protocols, algorithms, and source code in C, 2nd ed., Wiley, Hoboken, NJ _1996_.
16. H. E. H. Ahmed, H. M. Kalash, and O. S. Farag Allah, “Encryption efficiency analysis and security evaluation of RC6 block cipher for digital images,” Int. J. Comput. Inf. Sys. Sci. Eng. 1_1_, 33–39 _2007_.
17. R. L. Fivest, M. J. B. Robshad, R. Sidney, and Y. L. Yin, “The RC6 block cipher,” MIT Laboratory for Computer Science, Cambridge, MA, and RSA Laboratories, San Mateo, CA _1998_.
18. J. Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps,” Int. J. Bifurcation Chaos Appl. Sci. Eng. 8_6_, 1259–1284 _1998_.
19. J. Peng, S. Jin, G. Chen, Z. Yang, and X. Liao, “An image encryption scheme based on chaotic map,” presented at the 4th Int. Conf. on Natural Computation, Vol. 4, pp. 595–599 _2008_.
20. S. Li, G. Chen, and X. Zheng, “Chaos-based encryption for digital images and videos,” in Multimedia Security Handbook, Chap. 4,

CRC Press, Boca Raton, FL _2004_.
21. N. El-Fishawy and O. M. Abu Zaid, “Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher algorithms,” Int. J. Network Security 5_3_, 241–251 _2007_.
22. Y. Zhai, S. Lin, and Q. Zhang, “Improving image encryption using multi-chaotic map,” presented at Workshop on Power Electronics and Intelligent Transportation System, pp. 143–148 _2008_.
23. C. E. Shannon, “Communication theory of secrecy system,” Bell Syst. Tech. J. 28, 656–715 _1949_.
24. Y. B. Mao and G. Chen, “Chaos-based image encryption,” in Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neuralcomputing and Robotics, E. Bayro, Ed., pp. 231–265 Springer-Verlag, Berlin _2005_.
25. C. C. Chang, M. S. Hwang, and T. S. Chen, “A new encryption algorithm for image cryptosystems,” J. Syst. Softw. 58, 83–91 _2001_.
26. C. Alexopoulos, N. Bourbakis, and N. Ioannou, “Image encryption method using a class of fractals,” J. Electron. Imaging 4_3_, 251–259 _1995_.
27. C. J. Kuo, “Novel image encryption technique and its application in progressive transmission,” J. Electron. Imaging 2_4_, 345–351 _1993_.
28. H. K. C. Chang and J. L. Liu, “A linear quadtree compression scheme for image encryption,” Signal Process. Image Commun. 10_4_, 279–290 _1997_.
29. A. Sinha and K. Singh, “A technique for image encryption using digital signature,” Opt. Commun. 21_8_, 229–234 _2003_.
30. H. El-din, H. Ahmed, H. M. Kalash, and O. S. Farag Allah, “An efficient chaos-based feedback stream cipher _ECBFSC_ for image encryption and decryption,” Informatica 31_1_, 121–129 _2007_.

Authors:

Ibrahim F. Elashry graduated from the Faculty of Engineering, Kafrelshiekh University, Egypt in 2007. He is now a teaching assistant and MSc student. His interest is in security over wired and wireless networks and image processing.

Osama S. Farag Allah received his BS in 1997, MSc in 2002, and PhD in 2007, all in computer science and engineering, from Menoufia University, Faculty of Electronic Engineering, Egypt. He was a demonstrator at the Department of Computer Science and Engineering, at Menoufia University, from 1997 to 2002, became an assistant lecturer in 2002, and was promoted to a lecturer in 2007. His research interests cover computer networks, network security, cryptography, Internet security, multimedia security, image encryption, watermarking, steganography, data hiding, and chaos theory

Alaa M. Abbas received his BSc, MSc, and PhD in electrical engineering from Menoufia University, Egypt, in 1996, 2001, and 2008, respectively. He is currently a lecturer in the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University. His areas of interest are digital signal processing, image processing, motion estimation, pattern recognition, and face detection and recognition.

S. El-Rabaie received the BSc _with Honors _ in radio communications from Tanta University, Egypt, 1976, MSc in communication systems from Menoufia University, Egypt, 1981, and a PhD in microwave device engineering from the Queen's University

of Belfast in 1986. He Was a postdoctoral fellow in the Queen's University Department of Electronic Engineering until 1989. In 1992, he was a Research Fellow at the North Arizona University, College of Engineering and Technology, and in 1994 he served as a visiting professor at Ecole Polytechnique de Montreal, Quebec, Canada. Prof. El-Rabaie has authored and coauthored more than 70 papers and technical reports, and 15 books. In 1993, he was awarded the Egyptian Academic Scientific Research Award _Salah Amer Award of Electronics_, and in 1995, he received the Award of Best Researcher on CAD from Menoufia University. He is now the vice dean of postgraduate studies and research, Faculty of Electronic Engineering, Menoufia University.

Fathi E. Abd El-Samie received his BSc, and MSc, and PhD in electrical engineering from Menoufia University, Egypt, in 1998, 2001, and 2005, respectively. He is currently a lecturer in the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University. He received the most cited paper award from Digital Signal Processing Journal in 2008. His areas of interests are signal processing, image enhancement, restoration, super resolution and interpolation, and digital communications.

Puplished In:

J. Opt. Soc. Am. A/Vol. 27, No. 6/June 2010

Title

Satellite image fusion based on principal component analysis and high-pass filtering

Mohamed R. Metwalli,1 Ayman H. Nasr,1 Osama S. Farag Allah,2 S. El-Rabaie,3 and Fathi E. Abd El-Samie3,*

1*Data Reception, Analysis and Receiving Station Affairs Division, National Authority for Remote Sensing and Space Sciences, 23 Joseph Broz Tito St., El-Nozha El-Gedida, Cairo, Alf-Maskan 1564, Egypt*

2*Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt*

3*Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt*

**Corresponding author: fathi_sayed@yahoo.com*

Received July 23, 2009; revised March 30, 2010; accepted March 31, 2010;
posted April 2, 2010 (Doc. ID 114606); published May 19, 2010

الملخص
This paper presents an integrated method for the fusion of satellite images. Several commercial earth observation satellites carry dual-resolution sensors, which provide high spatial resolution or simply high-resolution (HR) panchromatic (pan) images and low-resolution (LR) multi-spectral (MS) images. Image fusion methods are therefore required to integrate a high-spectral-resolution MS image with a high-spatial-resolution pan image to produce a pan-sharpened image with high spectral and spatial resolutions. Some image fusion methods such as the intensity, hue, and saturation (IHS) method, the principal component analysis (PCA) method, and the Brovey transform (BT) method provide HR MS images, but with low spectral quality. Another family of image fusion methods, such as the high-pass-filtering (HPF) method, operates on the basis of the injection of high frequency components from the HR pan image into the MS image. This family of methods provides less spectral distortion. In this paper, we propose the integration of the PCA method and the HPF method to provide a pan-sharpened MS image with superior spatial resolution and less spectral distortion. The experimental results show that the proposed fusion method retains the spectral characteristics of the MS image and, at the same

time, improves the spatial resolution of the pan sharpened image.
OCIS codes: 100.0100, 100.02980, 280.0280.

REFERENCES

1. Z. Wang, D. Ziou, C. Armenakis, D. Li, and Q. Li, "A comparative analysis of image fusion methods," IEEE Trans. Geosci. Remote Sens. 43, 1391–1402 (2005).
2. Y. Yang, C. Han, X. Kang, and D. Han, "An overview on pixel-level image fusion in remote sensing," in Proceedings of the IEEE International Conference on Automation and Logistics (IEEE, 2007), pp. 2339–2344.
3. X. Otazu, M. González-Audícana, O. Fors, and J. Núñez, "Introduction of sensor spectral response into image fusion methods. Application to wavelet based methods," IEEE Trans. Geosci. Remote Sens. 43, 2376–2385 (2005).
4. J. Liu, "Smoothing filter-based intensity modulation: a spectral preserve image fusion technique for improving spatial details," IEEE Trans. Geosci. Remote Sens. 21, 3461–3472 (2000).
5. D. A. Yocky, "Multiresolution wavelet decomposition image merger of Landsat Thematic Mapper and SPOT panchromatic data," Photogram. Eng. Remote Sens. 62, 1067–1074 (1996).
6. J. Zhou, D. Civco, and J. Silander, "A wavelet transform method to merge Landsat TM and SPOT panchromatic data," Int. J. Remote Sens. 19, 743–757 (1998).
7. P. Scheunders and S. De Backer, "Fusion and merging of multispectral images with use of multiscale fundamental forms," J. Opt. Soc. Am. A 18, 2468–2477 (2001).
8. A. Garzelli and F. Nencini, "PAN-sharpening of very high resolution multispectral images using genetic algorithms," Int. J. Remote Sens. 27, 3273–3292 (2006).
9. B. Aiazzi, L. Alparone, S. Baronti, and A. Garzelli, "Context-driven fusion of high spatial and spectral resolution data based on oversampled multiresolution analysis,"

IEEE Trans. Geosci. Remote Sens. 40, 2300–2312
(2002).
10. L. Alparone, S. Baronti, A. Garzelli, and F. Nencini, “Remote
sensing image fusion using the curvelet transform,”
Inf. Fusion 8, 143–156 (2007).
11. T. Stathaki, Image Fusion: Algorithms and Applications 1st
ed. (Elsevier, 2008).
12. C. Laben and B. Brower, “Process for enhancing the spatial
resolution of multispectral imagery using pan-sharpening,”
U.S. Patent 6011875 (January 4, 2000).
13. B. Aiazzi, L. Alparone, S. Baronti, A. Garzelli, and M.
Selva, “MTF-tailored multiscale fusion of high-resolution
MS and pan imagery,” Photogrammetric Eng. Remote Sensing
72, 591–596 (2006).
14. T. Bretschneider and O. Kao, “Image fusion in remote sensing,”
in Proceedings of the Online symposium for Electronic
Engineers (2000).
15. A. Das and K. Revathy, “A comparative analysis of image
fusion techniques for remote sensed images,” in Proceedings
of the World Congress on Engineering WCE 2007, London,
2–4 July, 2007, Vol. I, pp. 639–644.
16. L. Shutao, “Multisensor remote sensing image fusion using
stationary wavelet transform: effects of basis and decomposition
level,” Int. J. Wavelets Multiresolution Inf. Processing
6, 37–50 (2008).
17. R. Gonzalez and R. Woods, Digital Image Processing 3rd ed.
(Prentice-Hall, 2007

البحث رقم (10)

Puplished In:

Information Security Journal: A Global Perspective, 21:285–295, 2012

ISSN: 1939-3555 print / 1939-3547 online
DOI: 10.1080/19393555.2012.699162

Title

Quadruple Difference Expansion-Based Reversible Data Hiding Method for Digital Images

Osama S. Faragallah
Department of Computer
Science & Engineering, Faculty
of Electronic Engineering,
Minufiya University, Egypt

KEYWORDS :

information hiding, reversible data embedding, lossless data embedding, steganography, difference expansion, payload capacity

ABSTRACT:

Lossless data hiding is a special type of data hiding technique that guarantees not only the secret data but also the ability of cover media to be reconstructed without any distortion. A latest lossless data hiding technique is proposed by Hong Lin Jin's that is based on hiding only one data bit in the spatial domain in gray-level image. However, this method uses double

difference expansion to embed bits which results in a small embedding capacity.
For this purpose, we propose an improved algorithm with the potential of increasing the payload capacity and maintaining good image quality. The proposed
improved algorithm is characterized by two aspects. First, the proposed improved reversible data hiding scheme is enhanced to exhibit data hiding in color palette images. Second, the embedding level is improved by using quadruple difference expansion to guarantee the embedding of 2-bit data into color images. Experiments of the proposed improved method have been conducted
over several well-known test images. The results show that the proposed improved method significantly improves the embedding capacity over Hong Lin Jin's scheme by the range of 15–35% for grayscale images and 20–46% for
color images while still maintaining the quality of the stego-images.

REFERENCES

Alattar, A.M. (2004). Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans. Image Process., 13(8), 1147–1156.

Celik, M.U., Sharma, G., Tekalp, A.M., and Saber, E. (2005). Lossless generalized-LSB data embedding. IEEE Trans. Image Process., 14(2), 253–266.

Feng, J., Lin, I., Tsai, C., and Chu, Y. (2006). Reversible watermarking: Current status and key issues. Int. J. Network Security, 2(3), 161–171.

Fridrich, J., Goljan, M., and Du, R. (2001). Invertible authentication. Proc. SPIE, 3971, 197–208.

Honsinger, C.W., Jones, P.W., Rabbani, M., and Stoffel, J.C. (2001). Lossless recovery of an original image containing embedded data. U.S. Patent, Docket No: 77102/E-D.

Jin, H.L. (2007). Lossless data hiding in the spatial domain for high quality images. The Institute of Electronics, Information and Communication Engineers Trans. Fundamentals, E90-A, 771–777.

Kamstra, L. and Heijmans, H.J.A.M. (2005). Reversible data embedding into images using wavelet techniques and sorting. IEEE Trans. Image Process., 14(12), 2082–2090.

Kim, H.J., Sachnev, V., Shi, Y., Nam, J., and Choo, H. (2008). A novel

difference expansion transform for reversible data embedding. IEEE Trans. Inf. Forensics Security, 3(3), 456–465.
Li, X. (2003).Watermarking in secure image retrieval. Pattern Recognition Lett., 24(14), 2431–2434.
Ni, Z., Shi, Y., Ansari, N., Su, W., Sun, Q., and Lin, X. (2008). Robust lossless image data hiding designed for semi-fragile image authentication. IEEE Trans. Circuits Syst. Video Technol., 18(4), 497–509.
Oliveira, S.R.M., Nascimento, M.A., and Zaiane, O.R. (2002, January). Digital watermarking: Its status, limitations and prospects. Technical Report TR-02-01, Department of Computing Science, Alberta University, Edmonton, Alberta, Canada.
Tian, J. (2003). Reversible data embedding using a difference expansion. IEEE Trans. Circuits Syst. Video Technol., 13(8), 890–896.
Thodi, D.M. and Rodríguez, J.J. (2007). Expansion embedding techniques for reversible watermarking. IEEE Trans. Image Process., 16(3), 721–730.
Vleeschouwer, C.D., Delaigle, J., and Macq, B. (2003). Circular interpretation of bijective transformations in lossless watermarking for media asset management. IEEE Trans. Multimedia, 5(1), 97–105.
Wu, X. and Memon, N. (1997). Context-based, adaptive, lossless image coding. IEEE Trans. Commun., 45(4), 437–444.
Zhao, Z., Yu, N., and Li, X. (2003). A novel video watermarking scheme in compression domain based on fast motion estimation. IEEE International Conference on Communication Technology Proceedings, 2, 1878–1882.
Zhu, B.B., Swanson, M.D., and Tewfik, A.H. (2004). When seeing isn't believing. IEEE Signal Process. Mag., 21(2), 40–49.
Zou, D., Shi, Y., Ni, Z., and Su, W. (2006). A semi-fragile lossless digital watermarking scheme based on integer wavelet transform. IEEE Trans. Circuits Syst. Video Technol., 16(10), 1294–1300.
Tsai, P., Hu, Y.C., and Yeh, H.L. (2009). Reversible image hiding scheme using predictive coding and histogram shifting. Signal Process., 89(6), 1129–1143.

BIOGRAPHY

Osama S. Faragallah received his BSc in 1997, MSc in 2002, and PhD in 2007, all in computer science and engineering, from Menoufia University, Faculty

of Electronic Engineering, Egypt. He was a demonstrator at the Department of Computer Science and Engineering, at Menoufia University, from 1997 to 2002, became an assistant lecturer in 2002, and was promoted to a lecturer in 2007. His research interests cover computer networks, network security, cryptography, Internet security, multimedia security, image encryption, watermarking, steganography, data hiding, and chaos theory.

قائمة بمجمل الإنتاج العلمي:-

Journal Publications:

1. Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Faragallah, "Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Images," Journal of Optical Engineering, vol. 45(10), 107003(1-7), 2006, SPIE (ISI JCR Impact Factor: 0.959).
2. Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, "Implementation of RC5 Block Cipher Algorithm for Image Cryptosystems," International Journal of Information Technology, vol. 3(4), pp. 245-250, 2006.
3. Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, "An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption," An International Journal of Computing and Informatics, vol. 31(1), pp. 121-129, 2007.
4. Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, "Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images," International Journal of Computer, Information, And Systems Science, and Engineering, vol. 1(1), pp. 33-39, 2007.
5. Mohamed Amin, Osama S. Faragallah, Ahmed A. Abd El-Latif, "Chaos-Based Hash Function (CBHF) for Cryptographic Applications," Chaos,

Solitons & Fractals, vol. 42(2), pp. 767-772, 2009, Elsevier (ISI JCR Impact Factor: 1.222).

6. Ibrahim F. Elashry, Osama S. Faragallah, Alaa M. Abbas ,S. El-Rabaie, Fathi E. Abd El-Samie, "Homomorphic Image Encryption," Journal of Electronic Imaging, vol. 18(3), 033002(1-14), 2009, SPIE (ISI JCR Impact Factor: 0.647).

7. E. El-Emam, M. Koutb, H. Kelash, and Osama S. Faragallah, "A Network Authentication Protocol Based on Kerberos," International Journal of Computer Science and Network Security (IJCSNS), vol. 9(8), pp. 17-26, 2009.

8. Mohamed Amin, Osama S. Faragallah, Ahmed A. Abd El-Latif, "A Chaotic Block Cipher Algorithm for Image Cryptosystems," Communications in Nonlinear Science and Numerical Simulation, vol. 15(1), pp. 3484–3497, 2010, Elsevier (ISI JCR Impact Factor: 2.806).

9. M. R. Metwalli, A. H. Nasr, Osama S. Faragallah, S. El-Rabaie, F. E. Abd El-Samie, "Satellite Image Fusion Based on Principal Component Analysis and High-Pass Filter," Journal of the Optical Society of America A, vol. 27(6), pp. 1385-1394, 2010, OSA (ISI JCR Impact Factor: 1.536).

10. Osama S. Faragallah, "An Efficient Block Encryption Cipher Based on Chaotic Maps for Secure Multimedia Applications," Information Security Journal: A Global Perspective, vol. 20(3), pp. 135-147, 2011, Taylor & Francis.

11. Osama S. Faragallah, "Digital Image Encryption Based on the RC5 Block Cipher Algorithm," Sensing and Imaging: An International Journal, vol. 12(3), pp. 73-94, 2011, Springer.

12. E. El-Emam, M. Koutb, H. Kelash, and Osama S. Faragallah, "An Authentication Protocol Based on Kerberos 5," International Journal of Network Security (IJNS), vol. 12(3), pp. 159-170, 2011.

13. Osama S. Faragallah, "Discrete Wavelet Transform–Based Spatial-Temporal Approach for Quantized Video Watermarking", Journal of Optical Engineering, vol. 50(7), 077402(1-10), 2011, SPIE (ISI JCR Impact Factor: 0.959).

14. Ahmed I. Sallam, El-Sayed El-Rabaie, Osama S. Faragallah, "Encryption-Based Multilevel Model for DBMS", Computers & Security, vol. 31(4), pp. 437-446, 2012, Elsevier (ISI JCR Impact Factor: 0.868).

15. Osama S. Faragallah, "An Enhanced Chaotic Key-Based RC5 Block Cipher Adapted to Image Encryption," International Journal of Electronics, vol. 99(7), pp. 925-943, 2012, Taylor & Francis (ISI JCR Impact Factor: 0.440).

16. Osama S. Faragallah, "Enhanced Semi-automated Method to Identify the Endo-cardium and Epi-cardium Borders," Journal of Electronic Imaging, vol. 21(2), 023024 (1-19), 2012, SPIE (ISI JCR Impact Factor: 0.647).

17. Nawal A. Elfeshawy, Osama S. Faragallah, "Divided Two-part Adaptive Intrusion Detection System," Journal of Wireless Networks, Digital Object Identifier: 10.1007/s11276-012-0467-7, 2012, Springer (ISI JCR Impact Factor: 0.520).

18. Ibrahim F. Elashry, Osama S. Faragallah, Alaa M. Abbas, S. El-Rabaie, Fathi E. Abd El-Samie, "A New Method for Encrypting Images with Few Details Using Rijndael and RC6 Block Ciphers in the Electronic Code Book Mode," Information Security Journal: A Global Perspective, vol. 21(4), pp. 193-205, 2012, Taylor & Francis.

19. Osama S. Faragallah, "Quadruple Difference Expansion-Based Reversible Data Hiding Method for Digital Images," Information Security Journal: A Global Perspective, vol. 21(5), pp. 285-295, 2012, Taylor & Francis.

20. M. R. Metwalli, A. H. Nasr, Osama. S. Faragallah, S. El-Rabaie, F. E. Abd El-Samie, "Combining Super-Resolution and Fusion Methods for Sharpening Misrsat-1 Data," IEEE Transactions on Geoscience and Remote Sensing, vol. 99, pp. 1-10, 2012, Digital Object Identifier: 10.1109/TGRS.2012.2209203, IEEE (ISI JCR Impact Factor: 2.895).

21. Ayman Mousa, E. M. Nigm, S. El-Rabaie, Osama S. Faragallah, "Query Processing Performance on Encrypted Databases by Using the Algorithm (REA)," International Journal of Network Security (IJNS), vol. 14(5), pp. 280-288, Sept. 2012.

22. Ayman Mousa, E. M. Nigm, S. El-Rabaie, Osama S. Faragallah, "Evaluating the Performance of Reverse Encryption Algorithm (REA) on

the Databases," Accepted for Publication in International Arab Journal of Information Technology (IAJIT), 2012, (ISI JCR Impact Factor: 0.127).

23. Osama S. Faragallah, "Efficient Video Watermarking Based on Singular Value Decomposition in the Discrete Wavelet Transform Domain," International Journal of Electronics and Communications (AEUE), In Press, Corrected Proof, Available online 27 August 2012, Digital Object Identifier:10.1016/j.aeue.2012.07.010, Elsevier (ISI JCR Impact Factor: 0.588).

24. Abd El–Naser A. Mohammed, Ahmed Nabih Zaki Rashed, Osama S. Faragallah, Mohamed G. El-Abyad, " New Trends of Multiplexing Techniques Based Submarine Optical Transmission Links for High Transmission Capacity Computing Network Systems," Canadian Journal on Science and Engineering Mathematics, vol. 3(3), pp. 112-126, March 2012.

25. Abd El–Naser A. Mohammed, Ahmed Nabih Zaki Rashed, Osama S. Faragallah, Mohamed G. El-Abyad, "Rigorous Progress on Algorithms Based Routing and Wavelength Assignment in Trans-Egypt Network (TEGYNET) Management," Canadian Journal on Electrical and Electronics Engineering, vol. 3(6), pp. 277-291, July 2012.

Conference Publications:

1. Osama S. Faragallah, Abdul Hamid M. Ragab, and Nabil A. Ismail, "Enhancements and Implementation of RC6TM Block Cipher for Data Security," IEEE Catalog Number: 01CH37239, pp. 133-137, 2001.
2. Osama S. Farag Allah, Abdul Hamid M. Ragab, and Nabil A. Ismail, "An Efficient Message Digest Algorithm (MD) For Data Security," IEEE Catalog Number: 01CH37239, pp. 191-197, 2001.
3. Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, "Encryption Efficiency Analysis and Security Evaluation of RC6 Block

Cipher for Digital Images," Proceedings of International Conference on Electrical Engineering, (ICEE), 2007, pp. 1-7, Digital Object Identifier: 10.1109/ICEE.2007.4287293.

4. Nawal A. El-Fishawy, Osama S. Faragallah, Hassan I. Sayed, "Neural Network Algorithms Performance Measure for Intrusion Detection," Proceedings of the International Computer Engineering Conference, (ICENCO), Cairo, Egypt, EG06, 2008
5. Nawal A. El-Fishawy, Osama S. Faragallah, Hassan I. Sayed, "Reduction the Rate of Alerts and False Positives of Intrusion Proceedings of the International Computer Engineering Conference, (ICENCO), Cairo, Egypt, EG07, 2008.
6. Ibrahim F. Elashry, Osama S. Faragallah, Alaa M. Abbas,; S. El-Rabaie, "A new diffusion mechanism for data encryption in the ECB mode," Proceedings of the International Conference on Computer Engineering & Systems (ICCES), Cairo, Egypt, pp. 288-293, 2009, Digital Object Identifier 10.1109/ICCES.2009.5383254.
7. E. El-Emam, M. Koutb, H. Kelash, and Osama S. Faragallah, "An optimized Kerberos authentication protocol," Proceedings of the International Conference on Computer Engineering & Systems (ICCES), Cairo, Egypt, pp. 508- 513, 2009, Digital Object Identifier 10.1109/ICCES.2009.5383213.

8. Mohamed R. Metwalli, Ayman H. Nasr, Osama S. Farag Allah, S. El-Rabaie, "Image fusion based on principal component analysis and high-pass filter," Proceedings of the International Conference on Computer Engineering & Systems (ICCES), Cairo, Egypt, pp. 63- 70, 2009, Digital Object Identifier 10.1109/ICCES.2009.5383308.
9. I. F. Elashry, O. S. Farag Allah, A. M. Abbas, S. El-Rabaie, and F. E. Abd El-Samie, "A Flexible Symmetric-Key Block Cipher Algorithm" Proceedings of the URSI National Radio Science Conference (NRSC), Cairo, Egypt, C23, 2010.
10. Ahmed I. Sallam, El-Sayed El-Rabaie, Osama S. Faragallah, "Comparative Study of Polyinstantiation Models in MLS Database," Proceedings of the International Computer Engineering Conference, (ICENCO), Cairo, Egypt, pp. 158-165, 2010.
11. M. R. Metwalli, A. H. Nasr, O. S. Faragallah, S. El-Rabaie, F. E A. El-Samie, "Sharpening Misrsat-1 data using Super-Resolution and HPF fusion methods," Proceedings of the URSI National Radio Science Conference (NRSC), Cairo, Egypt, C1, pp. 1-8, 2011, Digital Object Identifier: 10.1109/NRSC.2011.5873639.
12. A. Sarhan, F. Elgendy, T. Eltobely, O. S. Faragallah, "An efficient approach for image cryptosystem based on chaotic confusion-diffusion mechanisms," Proceedings of the URSI National Radio Science

Conference (NRSC), Cairo, Egypt, C8, pp. 211-221, 2012, Digital Object Identifier: 10.1109/NRSC.2012.6208526.

13. H. M. Elhosany, H. E. Hossin, H. B. Kazemian, O. S. Faragallah, "Chaotic encryption of images in the Fractional Fourier Transform domain using different modes of operation," Proceedings of the URSI National Radio Science Conference (NRSC), Cairo, Egypt, C9, pp. 223-235, 2012, Digital Object Identifier: 10.1109/NRSC.2012.6208527.

14. H. M. Kelash,; A. F. Alenezi, O. S. Faragallah, "Improved histogram-based reversible data hiding for digital images," Proceedings of the URSI National Radio Science Conference (NRSC), Cairo, Egypt, C10, pp. 237-244, 2012, Digital Object Identifier: 10.1109/NRSC.2012.6208528.

15. M. R. Metwalli, A. H. Nasr, O. S. Faragallah, S. El-Rabaie, F. E A. El-Samie, "Estimation of the optimal set of parameters for PAN-sharpening of satellite images based on the Non-Sub-sampled Contourlet Transform," Proceedings of the URSI National Radio Science Conference (NRSC), Cairo, Egypt, C14, pp. 271-278, 2012, Digital Object Identifier: 10.1109/NRSC.2012.6208532.

16. Osama R. Shahin, Hamdy M. Kelash, Gamal Mahrous, Osama S. Faragallah, "Breast Cancer Mass Detection in Mammograms using Modified K-means Clustering," Proceedings of the URSI National Radio

Science Conference (NRSC), Cairo, Egypt, C19, pp. 309-315, 2012, Digital Object Identifier: 10.1109/NRSC.2012.6208537.

17. Osama R. Shahin, Hamdy M. Kelash, Gamal Mahrous, Osama S. Faragallah, "Evolutionary Algorithm in the Classification of Calcification in Mammograms," Proceedings of the URSI National Radio Science Conference (NRSC), Cairo, Egypt, C20, pp. 317-324, 2012, Digital Object Identifier: 10.1109/NRSC.2012.6208538.