VERIZONA PUBLISHER
Publishing Your Ideas

www.verizonaonlinepublishing.com
Vol: 1, Issue: 1

Journal of Electronics and Communication Engineering Research

Advances in Medical Image Encryption

Nasim Hamidipour[1*] and Amir Sarvi Sarmeydani[2]

[1]Computer Science Department, Ferdowsi University of Mashhad, Iran

[2]GolbaharUniversity of Sciences and New Technologies, Golbahar, Iran

***Corresponding author:** Nasim Hamidipour, Computer Science Department, Ferdowsi University of Mashhad, Iran; E mail: faezeh.rohani@gmail.com

Article Type: Research, **Submission Date**: 24 October 2016, **Accepted Date:** 28 October 2016, **Published Date:** 28 November 2016.

Citation: Nasim Hamidipour and Amir Sarvi Sarmeydani (2016) Advances in Medical Image Encryption. J. Elec. Commu. Eng. Resol 1(1): 14-17.

Abstract

The content protection of digital medical images is getting more importance, especially with the advance of computerized systems and communication networks which allows providing high quality images, sending and receiving such data in a real-time manner. Medical concernslead healthcare organizations to encrypt every patient data, such as images before transferring the data over computer networks. Therefore, designing and developing qualified encryption algorithms is quite important for contemporary medicine.Medical image encryption algorithmstry to convert a digital image to another image data format which would bedefinitely hard to recognize. In this paper, we technically review image encryption methods for medical images. We do hope the present work can highlight the most recent contributions in the research area, and provide well-organized information to the medical image community.

Introduction

With the emerging of advanced technologies in medical domains, including high quality imaging devices, fast and accurate computerized systems, and reliable communication networks, the amount of diverse medical images has been recently booming up. Effective image encryption techniques for content protection of medical images became more important, and many robust encryption algorithms are available now to protect both two-dimensional (2D) and three-dimensional (3D) medical images. From a technical perspective, the developed algorithm could be categorized into two main methods as frequency domain encryption, or spatial domain encryption approaches, each one could be subcategorized by low-level and high-level methods [1-3].While in the low-level image encryption algorithms the content of the image remains understandable and visible, using high-level image encryption techniques the content of the image will be completely disordered and content of the original images would be invisible.

In the present paper, we are going to study and review medical image encryption algorithms in a technical way and discus their advantages and shortcomings.The contributions of the paper are as follows:

- To studycurrent advances in medical image encryption algorithms.
- To review the state of the art of image encryption methods in medical domain.
- To provide better insightsto the research community

This paper will serve as a guide for modernmedical image encryption. The paper is arranged as following. Section 2 covers the literature review. Section 3 further discusses the research and concludes the work.

Literature Review

Here, we review the recent advances in medical image encryption and present a taxonomy of medical image encryption systems developed in last few years.

In 2011, Indrakanti et al [4] utilized random pixel permutation technique to design a medical image encryption algorithm. Their method included three different steps towards encryption. First, the image has been partitioned into blocks and the block permutated. Then in the key generation stage,the values used in the encryption process are used to build a key, and finally, in as an identification process which requires the numbering of the shares that are generated from the encrypted image, the shares and key will transfer to the receiver. In 2011, the work was accomplished by Ulutas et al [5] offered medical image sharing among clinicians based on Shamir's secret sharing scheme, proposing confidentially and authenticity together.In 2011, Tafti et al [6] developeda statistical approach values for digital image encryption and eventually based on the spatial domain and they also established a digital image encryption algorithm by embedding the data into the frequency domain rather than the spatial domain [7]. In 2012,Subramanyamet al [8] proposed a novel technique to embed a robust Watermark in the JPEG2000 compressed encrypted images using three different existing watermarking schemes. They defined Digital asset management systems (DAMS) for tamper detection or ownership declaration or copyright management purposes. This planalsopreservesthevery private nature of contentastheembeddingisdoneonunreadabledata.In 2012, Rohani et al [9] combined singular value decomposition with one dimensional cellular automata to present a digital image encryption framework.

In 2013, Shaukatet al [10] presented digital watermarking algorithm that proposed on the chotiac map.The logistic guide was utilized in their proposed method to distinguish the positions for implementing the watermark in the image. In 2013, Tafti et al [11] combined different computerized methods including SVD and cellular automata to encrypt an image in the spatial domain.In 2014, Hassannia et al [12]developed image encryption techniques based on the cellular automata methodology. In 2015, Huet al [13] developed such algorithm utilizing image watermarking and alpha mattes. This strategy could precisely distinguish traded foreground images, traded background images, altered foreground images, and altered background images, and to identify forgery images made utilizing image matting or image in painting. Moreover, the system employed versatile limits, making the techniqueappropriate for useful applications. In 2015, Rohani et al [14] developed a method using LU decomposition based image encryption method. In 2015, Thippanna et al [15] novelly developed a masking algorithm to improve image encryption techniques and the obtained results were visually promising. Kanso et al [16] designed a selective and full block-based chaotic image encryption schemein 2015, in which the selection of blocks was based on a statistical approach, and the method was able to generate almost free of any correlation ciphered images.

In 2015, Kulasekaran et al [17] first discussed the need of security of medical images and then designed a technique to medical image encryption using a symmetric key, which gave the size of the tiles and the hash code of the image. The proposed encryption algorithm partitioned the image into tiles of arbitrary size, scrambled them and transforms the scrambled image using Discrete Wavelet Transform (DWT). The hash code in the key wasemployed to find out if tampering has taken place during the transformation of the medical image. In 2015, Zhang et al [18] developed an efficient cryptosystem for medical image encryption. The proposed technique was based on permutation-diffusion architecture. The designed permutation algorithm was able to contribute pixel value modification effect.

In 2016, Dai et al [19] took advantages of the chaotic system to develop a computational method for medical image encryption based on bit-plane decomposition. The proposed technique improved the security of key space and image efficiently. Cao et al [20] proposed lossless edge maps based image cryptosystem in 2016 to encrypt digital images, and the results showed promising security level in comparison with other approaches in the literature. In 2016, Praveenkumaret al [21] combineddifferent computational algorithms namely Deoxyribo Nucleic Acid (DNA) encryption and famous rule setencryption to tackle the problem of medical image protection. The authors performed extensive experiments to examine various parameters such asvertical ,diagonal, and horizontal correlation, and histograms. In 2016, Ajili et al [22] utilized a kind of watermarking approach for medical image encryption utilizing Discrete Cosine Transform (DCT) and Rivest-Shamir-Adleman (RSA) techniques to solve the problem. There have also been some study that tried to design algorithm to encrypt 3D imaging data rather than only 2D images [23-27]. Figure 1 shows a taxonomy of medical image encryption techniques developed in the last decade.

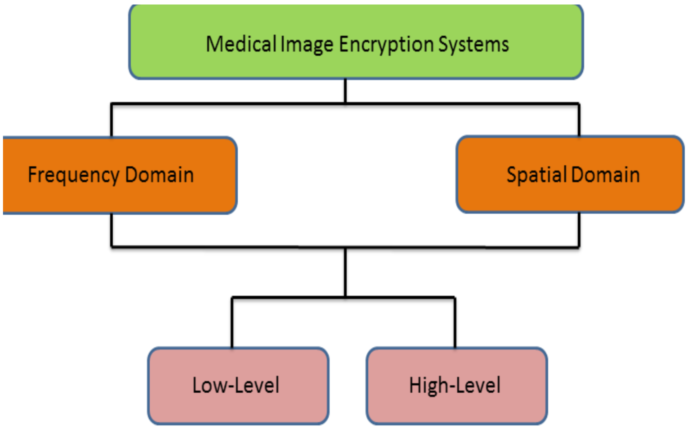

Figure 1: Taxonomy of medical image encryption algorithms

Discussion and Conclusion

Digital imaging and its operational application have made a big advance in biomedical and medical sciences ranging from CT and MR imaging to X-ray and microscopy vision[28-36]. While several valuable scientific contributions have been implemented to improve medical imaging technologies, many research and practical works should be accomplished to protect the large body of medical images. This work review and discussthe state of the art medical image encryption from the technical perspective. Not all medical image encryption algorithms are accurate and reliable enough in protecting 2D and 3D medical images, but we can find a bunch of extraordinary research studies in the literature. The accuracy and robustness of medical image encryptionalgorithmsare based on several internal and external parameters, such as type of the digital images, data dimensions (2D or 3D), watermark or encryption algorithms, or embedding data in frequency or spatial domain.

Efficient, reliable, and accurate medical image encryption methods still needed not just in the research area, but also in the industrial side. Combining the methods with other business and computational strategies, such as Internet of Things (IoT), Cloud infrastructures, distributed systems, business process modeling, and turning such algorithms into the WWW services would be pretty beneficial to the research community [37-51]. Recasting our gaze from the algorithms to application areas would be a great practical way to examine the accuracy of the proposed methods on real medical images. Incorporating medical image encryption methodologies on bigger datasets available on research communities will proof the robustness ad accuracy of the approaches in a better technical way.

References

1. Zeng W, Lei S. Efficient frequency domain video scrambling for content access control. Proceedings of the seventh ACM international conference on Multimedia (Part 1); 1999. p. 285-294.
2. Abraham L, Daniel N. Secure image encryption algorithms: A review. Entropy. 2013; 100(2).
3. Patel KD, Belani S. Image encryption using different techniques: A review. International Journal of Emerging Technology and Advanced Engineering. 2011; 1(1):30-34.
4. Indrakanti SP, Avadhani PS. Permutation based image encryption technique. International Journal of Computer Applications. 2011:0975–8887.

5. Ulutas M, Ulutas G, Nabiyev VV. Medical image security and EPR hiding using Shamir's secret sharing scheme. Journal of Systems and Software. 2011; 84(3):341-353.

6. Tafti AP, Malakooti MV, Ashourian M, Janosepah S. Digital image forgery detection through data embedding in spatial domain and cellular automata. In Digital Content, Multimedia Technology and its Applications (IDCTA). 7th International Conference; 2011. p. 11-15.

7. Tafti AP, Janosepah S. November. Digital images encryption in frequency domain based on DCT and one dimensional cellular automata. In International Conference on Informatics Engineering and Information Science; 2011. Berlin Heidelberg: Springer. p. 421-427.

8. Subramanyam AV, Emmanuel S, Kankanhalli MS Robust watermarking of compressed and encrypted JPEG2000 images. Multimedia, IEEE Transactions. 2012; 14(3):703-716.

9. Malakooti MV, Tafti AP, Rohani F, Moghaddasifar MA. RGB digital image forgery detection using singular value decomposition and one dimensional cellular automata. In Computing Technology and Information Management (ICCM). 8th International Conference; 2012 April. p. 483-488.

10. Jamal SS, Shah T, Hussain I. An efficient scheme for digital watermarking using chaotic map. Nonlinear Dynamics. 2013; 73(3):1469-1474.

11. Tafti AP, Maarefdoust R. Digital Images Encryption in Spatial Domain Based on Singular Value Decomposition and Cellular Automata. International Journal of Computer Science and Information Security. 2013; 11(4):121.

12. Tafti AP, Hassannia H. Active Image Forgery Detection Using Cellular Automata. In Cellular Automata in Image Processing and Geometry; 2014. Springer International Publishing. p. 127-145.

13. Hu WC, Chen WH, Huang DY, Yang CY. Effective image forgery detection of tampered foreground or background image based on image watermarking and alpha mattes. Multimedia Tools and Applications. 2015:1-22.

14. Far MAM, Rohani F, Brhravesh E. An Active Algorithm to Gray-scale Digital Image Forgery Detection based on Cellular Automata and LU Decomposition. J ComputSciSoftwDev. 2015; 1(001).

15. Thippanna G, Reddy TB, Sasikala C, Reddy PA. Medical Image Encryption and Compression Using Masking Algorithm Technique. American Journal of Computer Science and Information Technology (AJCSIT). 2015; 3(1):089-096.

16. Kanso A, Ghebleh M. An efficient and robust image encryption scheme for medical applications. Communications in Nonlinear Science and Numerical Simulation. 2015; 24(1):98-116.

17. Kulasekaran S, Sheeba F, Saivigneshu B, Dayalan C, Rex PC. Medical Image Encryption Using Block-Based Scrambling and Discrete Wavelet Transform. In 7th WACBE World Congress on Bioengineering; 2015; Springer International Publishing. p. 61-63.

18. Zhang LB, Yang BQ. An Efficient Cryptosystem for Medical Image Encryption. International Journal of Signal Processing, Image Processing and Pattern Recognition. 2015; 8(7):327-340.

19. Dai Y, Wang H, Wang Y. Chaotic Medical Image Encryption Algorithm Based on Bit-Plane Decomposition. International Journal of Pattern Recognition and Artificial Intelligence. 2016; 30(4):1657001.

20. Cao W, Zhou Y, Chen CP, Xia L. Medical Image Encryption Using Edge Maps. Signal Processing. 2016.

21. Praveenkumar P, Rajalakshmi P, Thenmozhi K, Rayappan JBB, Amirtharajan R. Research Article Horse DNA Runs on Image: A Novel Road to Image Encryption. 2016.

22. Ajili S, Hajjaji MA, Mtibaa A. Combining watermarking and encryption algorithm for medical image safe transfer: method based on DCT. International Journal of Signal and Imaging Systems Engineering. 2016; 9(4-5):242-251.

23. del Rey AM, Pastora JH, Sánchez GR. 3D medical data security protection. Expert Systems with Applications. 2016; 54:379-386.

24. Javidi B. Advances in 3D Imaging with Applications to Displays, Computational Imaging, Optical Security, and Healthcare. In Imaging Systems and Applications; 2016, July. Optical Society of America. p. IW5F-3.

25. Yang X, Zhang H. Encryption of 3D Point Cloud Object with Deformed Fringe. Advances in Optical Technologies. 2016.

26. Li XW, Wang QH, Kim ST, Lee IK. Encrypting 2D/3D image using improved lensless integral imaging in Fresnel domain. Optics Communications. 2016; 381:260-270.

27. You S, Lu Y, Zhang W, Yang B. 3-D color light field image encryption based on micro-lens array. Optical and Quantum Electronics. 2016; 48(8):402.

28. Ip IK, Raja AS, Seltzer SE, Gawande AA, Joynt KE, Khorasani R. Use of public data to target variation in providers' use of CT and MR imaging among Medicare beneficiaries. Radiology. 2015; 275(3):718-724.

29. Afshar-Oromieh A, Avtzi E, Giesel FL, Holland-Letz T, Linhart HG, Eder M, et al. The diagnostic value of PET/CT imaging with the 68Ga-labelled PSMA ligand HBED-CC in the diagnosis of recurrent prostate cancer. European journal of nuclear medicine and molecular imaging. 2015; 42(2):197-209.

30. Fahmi R, Eck BL, Levi J, Fares A, Wu H, Vembar M, et al. Effect of beam hardening on transmural myocardial perfusion quantification in myocardial CT imaging. In SPIE Medical Imaging; 2016 March; International Society for Optics and Photonics. p. 97882I-97882I.

31. Tafti AP, Kirkpatrick AB, Alavi Z, Owen HA, Yu Z. Recent advances in 3D SEM surface reconstruction. Micron. 2015; 78:54-66.

32. Tafti AP, Kirkpatrick AB, Holz JD, Owen HA, Yu Z. 3DSEM: A 3D microscopy dataset. Data in brief. 2016; 6:112-116.

33. Malakooti MV, Tafti AP, Naji HR. An efficient algorithm for human cell detection in electron microscope images based on cluster analysis and vector quantization techniques. In Digital Information and Communication Technology and it's Applications (DICTAP). Second International Conference; 2012 May; IEEE p. 125-129.

34. Shanklin W. 2D SEM images turn into 3D object models. 2016. arXiv preprint arXiv:1602.05256.

35. Eulitz M, Reiss G. 3D reconstruction of SEM images by use of optical photogrammetry software. Journal of structural biology. 2015; 191(2):190-196.

36. Bardosi Z, Granata D, Lugos G, Tafti AP, Saxena S. Metacarpal Bones Localization in X-ray Imagery Using Particle Filter Segmentation. 2014. arXiv preprint arXiv:1412.8197.

37. Assefi M, Liu G, Wittit MP, Izurieta C. Measuring the Impact of Network Performance on Cloud-Based Speech Recognition Applications.

38. Xia F, Yang LT, Wang L, Vinel A. Internet of things. International Journal of Communication Systems. 2012; 25(9):1101.

39. Rittinghouse JW, Ransome JF. Cloud computing: implementation, management, and security. CRC press; 2016.

40. Lundkvist A. Development of a Web GI System for Disaster Management. Examensarbete i geografiskinformationsteknik. 2016.

41. Frey LJ, Sward KA, Newth CJ, Khemani RG, Cryer ME, Thelen JL, et al. Virtualization of open-source secure web services to support data exchange in a pediatric critical care research network. Journal of the American Medical Informatics Association. 2015: p.ocv009.
42. Assefi M Optimizing The Locking Methods in Distributed Database Systems. In Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA); 2012 January. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). p. 1.
43. Assefi M, Wittie M, Knight A. Impact of Network Performance on Cloud Speech Recognition. In 2015 24th International Conference on Computer Communication and Networks (ICCCN); 2015 August; IEEE. p. 1-6.
44. Assefi M, Liu G, Wittie MP, Izurieta C. An Experimental Evaluation of Apple Siri and Google Speech Recognition. Proccedings of the 2015 ISCA SEDE.
45. Rohani F, Far MAM, Bavojdan FF. From Business Process Management to Flexible Image Analysis Applications: A Case Study.
46. Rohani F, Hassannia H, Moghaddasifar MA, Sagheb E. Human cell detection in microscopic images through Discrete Cosine Transform and Gaussian Mixture Model. Computational Biology and Bioinformatics. 2014; 2(4):52-56.
47. Tafti AP, Hassannia H, Piziak D, Yu Z. Selibcv: a service library for computer vision researchers. In International Symposium on Visual Computing; 2015 December. Springer International Publishing. p. 542-553.
48. Leo M, Medioni G, Trivedi M, Kanade T, Farinella GM. Computer vision for assistive technologies. Computer Vision and Image Understanding. 2016.
49. Tafti AP, Kirkpatrick AB, Owen HA, Yu Z. 3D microscopy vision using multiple view geometry and differential evolutionary approaches. In International Symposium on Visual Computing; 2014 December; Springer International Publishing. p. 141-152.
50. Far MAM, Rohani F, Behravesh E. An Active Algorithm to Gray-scale Digital Image Forgery Detection based on Cellular Automata and LU Decomposition. J ComputSciSoftwDev. 2015; 1(001).
51. Agrawal H. CloudCV: Deep Learning and Computer Vision on the Cloud (Doctoral dissertation, Virginia Tech; 2016.