*The Journal of Supercomputing*
Published: 26 May 2021

# Improved Authentication and Computation of Medical Data Transmission in the Secure IoT Using Hyperelliptic Curve Cryptography

**Prasanalakshmi.B***
Department of Computer Science, Center for Artificial Intelligence, King Khalid University, Abha, Saudi Arabia

**K.Murugan**
Department of Computer Science, Government College for Women, Kolar, India

**Karthik Srinivasan**
Department of Information Technology, College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia

**S.Shridevi**
Research Division of Advanced Data Science, Vellore Institute of Technology, Chennai, India

**Shermin Shamsudheen**
Faculty of Computer Science, College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia

**Yu-Chen Hu**
Department of Computer Science and Information Management, Providence University, Taichung, Taiwan

**Corresponding Author: Prasanalakshmi B -** prengaraj@kku.edu.sa

**Cite this article:**
Prasanalakshmi, B., Murugan, K., Srinivasan, K. *et al.* Improved authentication and computation of medical data transmission in the secure IoT using hyperelliptic curve cryptography. *J Supercomput* (2021). https://doi.org/10.1007/s11227-021-03861-x

- Accepted: 30 April 2021
- Published: 26 May 2021
- DOI: https://doi.org/10.1007/s11227-021-03861-x

*The Journal of Supercomputing*
Published: 26 May 2021

**Abstract:** Data transmission is a great challenge in any network environment. However, medical data collected from IoT devices need to be transmitted at high speed to ensure that the transmitted data are secure. This paper focuses on the security, speed and load of transmission. To prove security, combined steganographic methods involving cryptographic algorithms are used. The proposed model begins by updating two entries, medical image data and medical report data. Digital imaging and communications in medicine image data hold the medical report data to be encrypted and transmitted over the network channel. Although the proposed work follows the conventional method of data transmission from encryption until transmission, an effort has been made to split up the given data without transmitting them as such. As a public cryptography mechanism, the algorithm is also capable of transmission during decryption. The method of this article is genuine in proving its secure actions during the transmission of medical data and medical images. The proposed method justifies its performance when tested in hiding medical transcription data of different sizes varying across 30, 45, 64, 128 and 256 bytes in sample images with an average PSNR ranging from 55-70 dB, an MAE averaging from 0.2 to 0.7, and an SSIM, SC and correlation coefficient averaging to 1. This research is proven to work well in a simulation environment, and the results prove the genuine nature of the proposed technique.

***Keywords:*** *Cryptography, Internet of Things, steganography, discrete wavelet transforms, health information management, data privacy, digital preservation, information security.*

**Acknowledgement:** A special thanks to King Khalid University for providing me a good research environment.

***Funding Statement*:** This research is financial supported by the Deanship of Scientific Research at King Khalid
University under research grant number (RGP.2/164/42)

**Conflicts of Interest:** NIL

**Further reading:** https://link.springer.com/article/10.1007/s11227-021-03861-x

**References**

[1] Abdulaziz Shehab, Mohamed Elhoseny, Khan Muhammad, Arun Kumar Sangaiah, Po Yang, Haojun Huang, Guolin Hou , "Secure and robust fragile watermarking scheme for medical images", IEEE Access, vol. 6, pp. 10269–10278, 2018.

[2] Jain, M., Kumar, A. "RGB channel based decision tree grey-alpha medical image steganography with RSA cryptosystem", International Journal of Machine Learning & Cybersecurity, Vol 8,pp 1695–1705 2017.

[3] M. Preetha, M. Nithya, "A Study and Performance Analysis of RSA Algorithm," International Journal of Computer Science and Mobile Computing, Vol.2, No. 6, pp:126-139,2013.

[4] S. Karthik, A. Muruganandam, "Data encryption and decryption by using triple DES and performance analysis of crypto system," International Journal of Scientific Engineering and Research, Vol:2, No:11, pp:24-31,2014.

[5] K. M. Akash, P. Chandra, T. Archana, "Performance Evaluation of Cryptographic Algorithms: DES and AES," IEEE Conference on Electrical, Electronics and Computer Science, pp 1-5, 2012.

[6] S. Renukalatha, K.V. Suresh, "Automatic Roi Extraction in Noisy Medical Images," ICTACT Journal on Image and Video Processing, 2017; 7(4):1505-1514.

[7] S. M. Mousavi, A. Naghsh, S. A. R. Abu-Bakar, "A Heuristic Automatic and Robust ROI Detection Method for Medical Image Watermarking," Journal of Digit Imaging, 28:417-427.2015.

[8] S. Kazeminia, N. Karimi, S. M. R. Soroushmehr, S. Samavi, H. Derksen, K. Najarian, "Region of Interest Extraction for Lossless Compression of Bone X-Ray Images", Annual International Conference of IEEE Engineering in Medicine and Biology Society, 3061-3064. 2015.

[9] S. Ye, X. Yang, "Medical Image Retrieval Based on Extraction of Region of Interest," 2010 4th International Conference on Bioinformatics and Biomedical Engineering, Chengdu, pp. 1-4. 2010.

[10] M. C. Shin, "Comparison of Edge Detector Performance through Use in an Object Recognition Task", Computer Vision and Image Understanding, 2001, 84(1), 160–178.

[11] J. Pelzl, T. Wollinger, J. Guajardo, C. Paar, "Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves," International Workshop on Cryptographic Hardware and Embedded Systems, 2003, pp. 351–365.

[12] J. Pelzl, T. Wollinger, J. Guajardo, C Paar, "Low Cost Security: Explicit Formulae for Genus-4 Hyperelliptic Curves," International Workshop on Selected Areas in Cryptography, 2004, pp. 1–16.

[13] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, Frederik Vercauteren, "Handbook of Elliptic and Hyper Elliptic Curve Cryptography," Taylor and Francis, 2006

[14] P. Bh, D. Chandravathi, P. P. Roja, "Encoding and Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method," International Journal on Computer Science and Engineering, 2010, 2(5): 1904-1907.

[15] M. N. A. Wahid, A. Ali, B. Esparham, M. Marwan, "A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention," Journal of Computer Science Applications and Information Technology, 2018, 3(2):1-7.

[16] N. A. F. M. Zainon, S. A. Razak, "Master and Child Key Generation from Palm Vein," 2017 IEEE Conference on Application, Information and Network Security, Miri, Malaysia, 2017.

[17] K. Harmer, G. Howells, "Direct Template-Free Encryption Key Generation from Palm-Veins," 2012 Third IEEE International Conference on Emerging Security Technologies, Lisbon, Portugal, 2012.

[18] B. Prasanalakshmi, A. Kannammal, B. Gomathi, K. Deepa, R. Sridevi, "Biometric Cryptosystem Involving Two Traits and Palm Vein as Key," Procedia Engineering, 30:303-310.2012.

[19] N. Koblitz, "Hyperelliptic Cryptosystems," Journal of Cryptology, 1:139-150.1989.

[20] V. Miller, "Use of Elliptic Curves in Cryptography," in Advance in Cryptology - CRYPTO'85, LNCS 218, H. C. Williams, Ed. Berlin, Germany: Springer-Verlag, pp. 417-426, 1986.

[21] D. G. Cantor, "Computing in the Jacobian of a Hyperelliptic Curve," Mathematics of Computation, 1987, 48(177):95-101.

[22] R. Harley, "Fast Arithmetic on Genus Two Curves," 2000."

[23] T. Lange, "Efficient Arithmetic on Genus 2 Hyperelliptic Curves over Finite Fields via Explicit Formulae," In IACR Cryptology ePrint Archive, 2002, 121.

[24] K. Matsuo, J. Chao, S. Tsujii, "Fast Genus Two Hyperelliptic Curve Cryptosystems," Technical Report ISEC2001-23, IEICE, 2001, pages 89-96.

[25] Y. Miyamoto, H. Doi, K. Matsuo, J. Chao, S. Tsuji, "A Fast Addition Algorithm of Genus Two Hyperelliptic Curve," The 2002 Symposium on Cryptography and Information Security, Japan, 2002.

[26] M. Takahashi, "Improving Harley Algorithms for Jacobians of Genus 2 Hyperelliptic Curves," The 2002 Symposium on Cryptography and Information Security, Japan, 2002.

[27] K. I. Nagao, "Improving Group Law Algorithms for Jacobians of Hyperelliptic Curves," International Algorithmic Number Theory Symposium, 439-447. 2000.

[28] V. Miller, "Use of Elliptic Curves in Cryptography," In: H. C. Williams (eds) CRYPTO 1985: Advance in Cryptology – CRYPTO'85 Proceedings, Lecture Notes in Computer Science, vol 218, Berlin, Germany: Springer-Verlag, pp. 417-426, 1986.

[29] J. Pelzl, T. Wollinger, C. Paar, "Low Cost Security: Explicit Formulae for Genus-4 Hyperelliptic Curves," In: Matsui M., Zuccherato R.J. Selected Areas in Cryptography, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, vol 3006, 2003.

[30] J. Pelzl, T. Wollinger, J. Guajardo, C. Parr, "Hyperelliptic Curve Cryptosystems: Closing The Performance Gap to Elliptic Curves," CHES 2003: Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science, vol 2779, Springer Berlin Heidelberg, 351-365.2003.

[31] D. Mumford, Chidambaran Padmanabhan Ramanujam, Jurij Ivanovič Manin. Abelian Varieties. Vol. 108. Oxford: Oxford University Press, 1974.