ICAI 2023
12th International Conference on Applied Informatics
Eger, Hungary, 2023

Novel Method to Generate symmetric key from Iris Using Polynomial Interpolation and Zernike Moment

Hussein Lafta Hussein[a], Ahmed Abdulrudah Abbass[b], Jasim H. Lafta[c], Robert Tornai[d]

[a]Computer Science Department, College of Education for Pure Sciences, University of Baghdad, Baghdad, Iraq hussein.l.h@ihcoedu.uobaghdad.edu.iq

[b]College of Business Informatics, University of Information Technology and Communications, Baghdad, Iraq ahmed.alzamili@uoitc.edu.iq

[c]Department of Data Science and Visualization, Faculty of Informatics, University of Debrecen, Debrecen, Hungary jasim.hussein@inf.unideb.hu

[d]Department of Data Science and Visualization, Faculty of Informatics, University of Debrecen, Debrecen, Hungary tornai.robert@inf.unideb.hu

Abstract

Information security is considered one of the topics that attract the attention of researchers in computer technologies and information systems, this subject is very importance when transmitting data in insecure channels. There are several ways to protect important data from undesirable people to view this data; one of these methods is the data encryption process, which is the process of converting readable text into unreadable text, this process is done through the encryption algorithm and the encryption key. There are two types of encryption keys, the public key (Symmetric), and the secret key (Asymmetric). The main purpose of this research is to propose a new approach to generate an encryption key as a symmetric key type for the AES 128-bit algorithm. Using the Zernike moment to extract the features from the iris (biometric) and taking these features to find a set of points (control points). Polynomial interpolation (BSpline and Bezier interpolator) will use to generate the curves, where the curve will be drawn for each of them and the points of intersection between them will be found, from this points will take eight points of intersection between the two curves will represent an encryption key for

the AES 128-bit algorithm. As a result, this method of generating the encryption key is difficult to break it, because it depends on several criteria in the process of generating the encryption key.

Keyword:Encryption, polynomial, AES, Iris, key generation, Zernike moment, BSpline, Bezier

References

[1] CASIA-Iris database(2019), Institute of Automation, Chinese Academy of Sciences,http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp.

[2] Chee-Way Chong, P. Raveendran, R. Mukundan, (2003), "Translation invariants of Zernike moments PERGAMON ", Pattern Recognition, 36 ,1765 – 1773, https://doi.org/10.1016/S0031-3203(02)00353-9.

[3] David Kahaner, Cleve B. Moler, Stephen Nash, George Elmer Forsythe,(1989), "Numerical Methods andSoftware" , Prentice–Hall, Englewood Cliffs, NJ, ISBN: 0136272584,https://archive.org/details/numericalmethods0000kaha.

[4] David Kincaid, Ward Cheney,(2004), "Numerical Mathematics and Computing", Fifth edition, Brooks/ Cole Publishing Company, Belmont, CA, https://web.ma.utexas.edu/CNA/NMC5/manuals.html.

[5] Hanaa M. A. Salman, (2012), "Fuzzy Bio-Cryptography Key Generation", The 13th International Arab Conference on Information Technology ACIT, pp.538-543, Dec.10-13,
https://www.academia.edu/31437787/Fuzzy$_{B}io_{C}ryptography_{K}ey_{G}eneration$..

[6]$HeloiseHseandA.RichardNewton$, (2004)"$Sketchedsymbolrecognitionusing Zernikemoment$", $Proceedingsofthe$17$th InternationalConferenceonPatternRecognition, ICPR$2004, $Vol.$1, $pp.$367 − 370, $https://doi.org/$10.1109/$ICPR.$2004.1334128.

[7] J. Jagadeesan, T. Thillaikkarasi, K. Duraiswamy, (2010), "Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature", International Journal of Computer Applications, 2(6), pp. 16–26, https://doi.org/10.5120/673-946.

[8] Khotanzad, A., and Hong, Y.H.,(1990),"Invariant Image Recognition by Zernike Moments", Publisher:IEEE, On PAMI, Vol. (12), No. (5), pp. 289- 497, https://www.researchgate.net/
publication/289961546$_{I}mage_{R}ecognition_{U}sing_{M}odified_{Z}ernike_{M}oments.$

[9]$MingwuZhang, BoYang, WenzhengZhang, TsuyoshiTakagi$, (2011), "$MultibiometricBasedSecureEncryptionandAuthenticationSchemewithFuzzy Extractor$", $InternationalJournalofNetworkSecurity, Vol.$12, $No.$1, $PP.$50˘57. $https://www.researchgate.net/publication/49609196_{M}ultibiometric_{B}ased\ _{S}ecure_{E}ncryption_{a}nd_{A}uthentication_{S}cheme_{w}ith_{F}uzzy_{E}xtractor.$

[10] MMU-Iris Database, Multimedia-University Malaysia (2016).

[11] Peng Zhang, Jiankun Hu, Cai Li, Mohammed Bennamoun, Vijayakumar Bhagavatula, (2011), "A pitfall in fingerprint bio-cryptographic key generation", Computers amp; Security, Volume 30, Issue 5, July 2011,pp. 311–319.

[12] R.Seshadri, T. Raghu Trivedi, (2010) ,"Generation of key for Session key Distribution Using Bio-Metrics",International Journal on Computer Science and Engineering , pp. 1992-1995, Vol. 02, No. 06.

[13] Rorres Chris, Howard Anton,(2005), "Elementary Linear Algebra", Ninth Edition, John Wiley and Sons, New York.

[14] Sinan A Naji, Robert Tornai, Jasim H Lafta, Hussein L Hussein,(2020)," Iris Recognition Using Localized Zernike Features with Partial Iris Pattern",springer, New Trends in Information and Communications Technology Applications pp 219-232.

[15] Seyed Mehdi Lajevardi, Zahir M. Hussain,(2009), " Zernike Moments for Facial Expression Recognition" ,International Conference on Communication, Computer and Power (ICCCP'09), Muscat, Oman, 15-18.

[16] Teague, M.R., (1980),"Image Analysis via the General Theory of Moments", Journal of the Optical Society of America, 70 (8). 920-930, https://doi.org/10.1364/JOSA.70.000920.

[17] Teh, C. and Chin, R.T.(1988), "On Image Analysis by the Methods of Moments", Publisher:IEEE Trans. on PAMI, 10 (4),496-513, https://doi.org/10.1109/34.3913.

[18] U. Uludag, S. Pankanti, S. Prabhakar, and A. K.Jain,(2004), "Biometric cryptosystems: Issues and challenges",Proceedings of the IEEE, vol. 92, pp. 948-960,https://doi.org/10.1109/JPROC.2004.827372.

[19] Van Loan, Charles F,(1997), "Introduction to Scientific Computing", New Jersey: Prentice Hall.

[20] Bineet Kaur,SukhwinderSingh ,Jagdish Kumar,(March 2018), "“Iris Recognition Using Zernike Moments and Polar Harmonic Transforms",Arabian Journal for Science and Engineering,https://doi.org/10.1007/s13369-017-3057-2.

[21] WVU-Iris Database, West-Virginia-University (2019).

[22]Ahmed Abdulrudah Abbass, Wesam Bhaya, (2015),"Bio- cryptography using Zernike Moments and Key Generation by Cubic Splines", journal of Information Engineering and Applications, Vol.5, No.8, pp. 11-18.

[23]Wesam Bhaya, Ahmed Abdulrudah Abbass, (2015), "Mersenne Prime Number Generating using Cubic Spline to be used RSA Algorithm", Journal of Next Generation Information Technology, Volume 6, Number 1, pp. 1- 9.

[24]Ahmed Abdulrudah Abbass, et. Al.,(January 2022)," Efficient Eye Recognition for Secure Systems Using Convolutional Neural Network", Webology, Volume 19, Number 1,pp. 4967-4978 ,https://doi.org/10.14704/WEB/V19I1/WEB19333.