International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 4 April 2023, pp: 1748-1754 www.ijaem.net ISSN: 2395-5252

Generation of Hybrid Bio-Secret Key Based on Fingerprint

Author 1: Abdirahman Abdullahi mire, Author2: Dr. Ihab Abdalla
Uskudar University Institute of Science, Istanbul, Turkey.

Date of Submission: 20-04-2023 Date of Acceptance: 30-04-2023

ABSTRACT
Privacy policies that were previously limited to paper documents are becoming more prevalent in online commercial transactions. Internet commerce, medical privacy, and a variety of other fields benefit from highly secure connections. Individuals who communicate with one another through the Internet increasingly require secure connections. Various techniques, such as encryption, steganography, watermarking, and scrambling, can be used to keep data private, safe, and copyright-protected. Secure online transactions and other private networks necessitate the use of encryption, while sensitive data also necessitates the use of this technology in business. The most important thing that can be done to ensure data security is to keep it out of the hands of those who don't need it or are actively trying to gain it. Let me remind you at this point that there is an issue in that the server knows the PIN code, or, to put it another way, the PIN code is saved in the database. And, as we all know, utilizing a symmetric cryptography key requires the use of a single safe secret key. Therefore, we address this problem by producing a secret bio-key derived from a fingerprint image and using that key for encryption and decryption to protect the sensitive information. This study may also be validated by developing a PIN code that is independent of the system and can be thought of as a table based on the fingerprint image.
MATLAB, Advanced Encryption Standard, Fingerprint image, fingerprint recognition, all those things we used as a tool to develop this work.
Encrypted and decrypted with large text file by using generated Bio-Key and Advanced Encryption Standard (AES). The effectiveness of this research and be characterized by the development of a training for new approach that helps the user to isolate the PIN code from the system.

I. INTRODUCTION

Privacy guidelines, the likes of which were to paper documents alone, are increasingly turning up in online business dealings nowadays. E-commerce conducted over the internet, medical privacy, and other areas all benefit from communications that are extremely well protected. Secure connections between individuals who interact with one another through the Internet are now an absolute necessity. People can keep their data secure, confidential, and protected by copyright by utilizing a variety of methods, including cryptography, steganography, watermarking, and scrambling. Encryption, on the other hand, has made its way into the business sector because of the requirement for safe financial dealings in online commerce and other private networks, in addition to the security of sensitive data. When it comes to security, preventing information from being viewed by individuals who have no use for it or who are actively working to obtain it is the single most critical thing that can be done.

Within the scope of this thesis, we will generate a Bio-Key and using it into encrypt information utilizing one of the most well-known encryption protocols known as AES, which stands for Advanced Encryption Standard. In addition, rather than using an email address or any other form of identification, we will encrypt the data using a Bio-Key derived from a fingerprint image. We will concentrate on a few aspects, such as how generated key will be secure enough and effectively, we can do tasks such as using that key to encrypt and decrypt data, we will also create PIN code and brief explanation about how it is useful.

II. METHOD

The findings of this study will be presented in two sections. Processing the fingerprint and extracting the key from it is the first step in this procedure. The second step is to encrypt and decrypt the data with the AES algorithm and the key that was previously generated.

In addition, at the beginning of the process, the system is training all the stages, and after training, it is recognizing the steps of the process to make the data secure.

2.1 System Training

The following graphic provides an illustration of the sequence in which the system is training the process of learning all the phases. This illustration may be viewed below. It begins by acquiring knowledge of the individual's fingerprint, then moves on to acquiring knowledge of the individual's fingerprint's two separate types of ridges and bifurcations, and ultimately, it acquires knowledge of the individual's fingerprint's two distinct types of minutiae points. The figure illustrates all that has been discussed here. First, it will generate a filter for each of them on their own, then it will sort the arrays that were derived from the user's fingerprint, then it will learn how to concatenate the sorted arrays with the PIN code digits, then it will put together the sorted array and use it as a Bio-Key, and finally, AES will be used to encrypt it. This process will take place in the order listed above. Those are the actions that are going to be carried out. Nevertheless, there is something about this scenario that I need to make perfectly plain to you, and that is the fact that all those acts are essentially training the system, and the system was learning all those operations.

2.2 System Recognition

The process of system training starts with the person’s fingerprint, and the process of system recognition starts with the same situation. The training side only studies or saves the input data, not all the data or all the stages that were discussed above, but most of them. There are many similarities between these two systematic processes. The main distinction is that the training side only trains or saves the input data. And it happens only once, while the other one happens multiple times, which means the client is accessed multiple times.

What steps should be taken after the data has been saved?

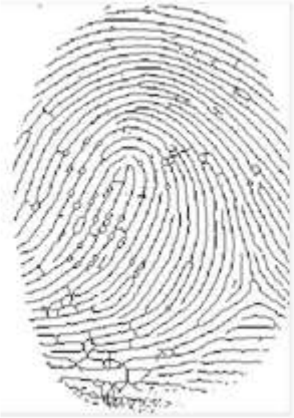
That is the topic that will be covered in this part. If a customer or user wanted to access his account or any other kind of restricted or authorized entity, then when he entered the pin code or key or password or any other kind of protocol that protected the data, there must be a backup, because after entering those digits, there could be a place that the key has been stored, and so the system then compares the key that was stored in the database and the new one that was entered, and if they are the same, then you did it. If they were different, unfortunately, the authorization would be denied.

The overall idea that these two stages are working together to demonstrate is really something along the lines of this illustration, and this side is the side that the system looks at to determine whether the customer has the authorization to view the information or not.

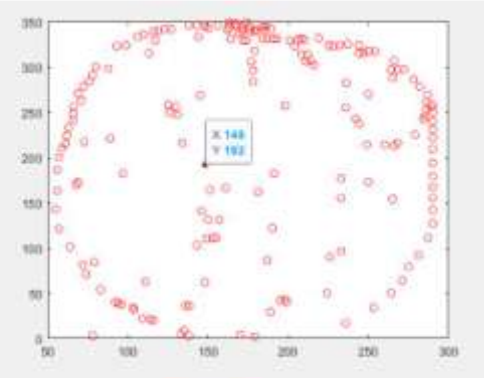
III. RESULTS

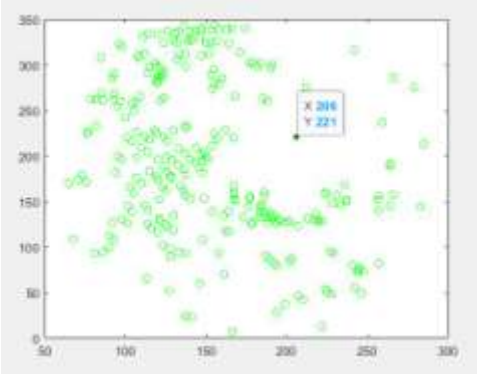
3.1 thinned Image

This is since the foreground is composed of all the lines of fingerprints that it includes. Don’t forget that the background has been erased from the image, so all that is visible is the foreground, and the background is empty of any content. It is just like an empty white page.So skeletonization or thinning is the process in which they use to reduce the width of the ridges of an image. The main purpose of this process is to get clean ridges to mark terminations and bifurcations or any needed intersections.



3.2 Ridge Endings and Bifurcations

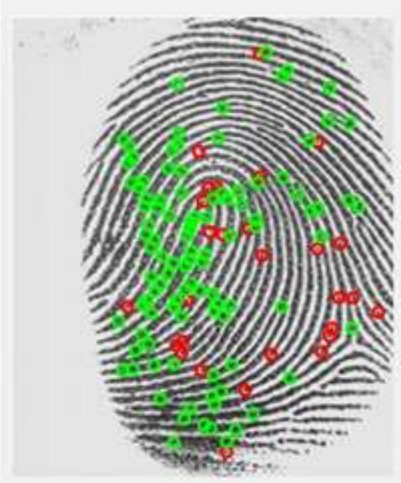




All the termination points and bifurcation points have been retrieved and added to the graph, such as the example point where X of ridge endings equals 148 and Y equals 192 while X of the bifurcation marked points equals 206 and Y equals 221 as you see in the above figures. X and Y are clearly visible in the photo, and each point has its own location in the graph, yet these points are not being put into an image, they are just being recovered. There are also several incorrect termination and bifurcation points in this model.

3.3 Extracted Minutiae Points

combining or bringing together in one graph all the termination points and bifurcation points, the fingerprint picture is then placed on it, at which time many false minutiae will emerge on both sides. In this situation, a red dot indicates the point at which a line in the image comes to an end, whereas a green dot indicates any place at which two lines intersect or branch off from one another. Also, it is filtered to get rid of all the irrelevant points of minutiae. This procedure will assist us in obtaining a few specifics about which we can be certain and in distinguishing the image from the regions that require marking. Also, this technique enables us to obtain a defined array that is a representation of all the points in the graph.



3.4 Center Point

Performing all those things, we were able to find the minute details that we needed, and we have placed them all in the locations that we wanted them to be marked in.

Therefore, what we need to do is figure out the center of gravity or the center point for each group. For instance, we need to figure out the center point for all the termination points, and we also need to know where the center point is for all the bifurcation points.

As can be seen in the above figure, the blue point belongs as the center point for all the minutiae points that are classified as bifurcation points, and the pink point belongs as the center point for all the minutiae points that are classified as termination points.

When we had finished finding all the points, we sorted the array, and then we utilized it as a Bio-Key as shown in the Table 1. An additional interesting feature is that we have chosen the first ten digits of the array and putted them on top of it from 0 to 9, which are the normal numbers required for each PIN code. as shown in the Table 2.

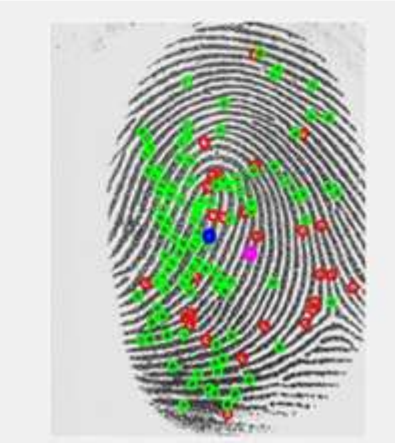


Table 1

The Bio-key	39	39	40	40	41	41	43	43	43	44	44	46	46	46	47	32

Table 2

Pin code digit	0	1	2	3	4	5	6	7	8	9
Selected Terms	167	136	111	102	99	98	88	83	81	80
Selected Bif	1	6	11	12	17	20	23	24	24	24

IV. CONCLUSION AND DISCUSSION

This research aimed to accomplish two goals at the same time: The first approach is to generate a key that is robust and dependable from a fingerprint image, then encrypt the data using that Bio-Key, AES, and decrypt it when it is required. In terms of usingAES, we are all aware that it is compatible with Symmetric Key Cryptography, which is founded on the usage of a single key.

The second approach is to generate a PIN code that is not associated with any system. To put it another way, it is a personal identification number (PIN) that is not kept in the database. The system does not know the PIN code; all it knows is the user's fingerprint when it is considering the validity of the PIN code.

Shengbao Wang, (2017), “Practical Identity-Based Encryption (IBE) in Multiple PKG Environments and Its Applications”, Department of Computer Science and Engineering, Shanghai Jiao Tong University, 800 Dongchuan Road, Shanghai 200240, China

REFERENCE

[1]. Bauer F. L. (2000), “Decrypted Secrets, 2nd edition, Springer”. ISBN 3-540-66871-3

[2]. Shi, Zhixin, Govindaraju, (Venu, 2006), “Fingerprint Image Enhancement Based on Skin Profile” PP 714 – 717 Approximation, VL - 3

[3]. Jinwei Gu, Jie Zhou, David Zhang, (2003). “a combination model for orientation field of fingerprint.” Department of automation Tsinghua university Beijing, Biometric technology center Department of computing Hong Kong Polytechnic university Kowloon Hong Kong.

[4]. Kristensen, Terje, (2010), “Fingerprint Identification - A Support Vector Machine Approach”, PP - 451 – 458, VL - 1

[5]. Alqadi, Ziad (2020), “Analysis of fingerprint minutiae to form fingerprint identifier”

[6]. VL - 4, DO - 10.30630/joiv.4.1.332, JO - JOIV: International Journal on Informatics Visualization

[7]. Jea, Tsai-Yang, Govindaraju, Venu, (2005), “A minutia-based partial fingerprint recognition system” PP 1672 – 1684, VL – 38.

[8]. Divyarajsinh N. Parmar , Brijesh B. Mehta (2013), “Face Recognition Methods & Applications” 1 P.G. Student of Computer Engineering 2Asst.Prof. Dept.of Computer Engineering C.U. Shah College of Engg. & Tech Wadhwan city, India

[9]. Elvira Nurfadhilah, Asril Jarin, Lyla Ruslana Aini, Siska Pebiana, Agung Santosa, Muhammad Teduh Uliniansyah, Eduward Butarbutar, Desiani and Gunarso

[10]. Conference: (2021) 9th International Conference on Information and Communication Technology (ICoICT), Year: 2021, Page 657

[11]. Roli Bansal , Priti Sehgal and Punam Bedi, (2011) “Minutiae Extraction from Fingerprint Images - a Review” Department of Computer Science, University of Delhi, New Delhi - 110001, India. Reader, Department of Computer Science, Keshav Mahavidyalaya, University of delhi, Pitampura , New Delhi - 110034, India. Associate Professor, Department of Computer Science, University of Delhi, New Delhi - 110001, India.

[12]. Al-Najjar, Yusra, Sheta, Alaa, (2008), “Minutiae extraction for fingerprint recognition” PP 1 – 5, SN - 978-1-4244-2205-0

[13]. Mann, V.A Diamond, R, Carey, S, (1979), “Development of voice recognition: Parallels with face recognition”, PP 153 – 165, VOL – 27

[14]. McGehee, Frances, (1944), “An Experimental Study of Voice Recognition” PP 53 – 65, VOL -35

[15]. F. Goudail, E. Lange, T. Iwamoto, K. Kyuma and N. Otsu, (1996) "Face recognition system using local autocorrelations and multiscale integration," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 18, no. 10, pp. 1024-1028

[16]. W. E. Burr, (2003), "Selecting the Advanced Encryption Standard," in IEEE Security & Privacy, vol. 1, no. 2, pp. 43-52

[17]. A.H. Johnston and G. M. Weiss, (2015), "Smartwatch-based biometric gait recognition," IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), 2015, pp. 1-6

[18]. Khan, Tariq M, Bailey, Donald G, Khan, Mohammad A. U, Kong, Yinan (2019),

[19]. “Efficient hardware implementation strategy for local normalization of fingerprint images” Journal of Real-Time Image Processing, PP 1263 – 1275, VL – 16

[20]. B. Stojanović, O. Marques, A. Nešković and S. Puzović, (2019), "Fingerprint ROI segmentation based on deep learning," 2016 24th Telecommunications Forum (TELFOR), pp. 1- 4

[21]. Dr. Neeraj Bhargava, Dr. Ritu Bhargava, Manish Mathuria, Pooja Dixit, (2013), “Fingerprint Minutiae Matching using Region of Interest” Department of Computer Science, School of Engineering & System Sciences, MDS University, Ajmer, Rajasthan, India, Department of MCA, Govt. Women Engineering College, Ajmer, Rajasthan, India, Department of CE & IT, Govt. Engineering College Ajmer Ajmer, Rajasthan, India, PP 1 – 3

[22]. Haralick, Robert M, (1983), “Ridges and valleys on digital images” PP 28 – 38, VOL – 22 Computer Vision, Graphics, and Image Processing, VL - 22, SN - 0734-189X

[23]. X. Bultel et al., 2018,"Security analysis and psychological study of authentication methods with PIN codes," 2018 12th International Conference on Research Challenges in Information Science (RCIS), pp. 1-11,

[24]. Tang, Jian, Terziyan, Vagan, Veijalainen, Jari, (2003), “Distributed PIN Verification Scheme for Improving Security of Mobile Devices” PP 159 – 175, VL – 8, JO - Mobile Networks and Applications

[25]. Lin Yen-Chun, (1993), "On balancing sorting on a linear array," in IEEE Transactions on Parallel and Distributed Systems, vol. 4, no. 5, pp. 566-571

[26]. Seung-Jo Han, Heang-Soo Oh and Jongan Park, (1996) "The improved data encryption standard (DES) algorithm," Proceedings of ISSSTA'95

International Symposium on Spread Spectrum Techniques and Applications, pp. 1310-1314 vol.3

[27]. R. Davis, (1978), "The data encryption standard in perspective," in IEEE Communications Society Magazine, vol. 16, no. 6, pp. 5-9

[28]. Md. Shamim Hossain Biswas , Dr. Md. Asraf Ali, Dr. Mostafijur Rahman, Mr. Md. Khaled Sohel, Mr. Md. Maruf Hasan, Kausik Sarkar, Abu Shamim Aminur razzaque, (2019). “A systematic study on classical cryptographic cypher in order to design a smallest cipher” Department of Software Engineering, Daffodil International University Bangladesh, PP 1 – 6

[29]. S. N. Gowda, (2016), "Innovative enhancement of the Caesar cipher algorithm for cryptography," 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall), pp. 1-4

[30]. Maurer, Ueli M, Wolf, Stefan, (2000) “The Diffie–Hellman Protocol” PP 147 – 171, VL – 19, JO - Designs, Codes and Cryptography.

[31]. P.Arul , Dr.A.Shanmugam (2009), “GENERATE A KEY FOR AES USING BIOMETRIC FOR VOIP NETWORK SECURITY”, PP 1 – 6, VL – 6.

[32]. Fakir Sharif Hossian , Ali Nawaz, Khan Md. Grihan, (2013) “Biometric Authentication Scheme for ATM Banking System Using Energy Efficient AES Processor”, Department of Electrical and Electronic Engineering, International Islamic University Chittagong, Dhaka, Bangladesh, PP 1 – 7 VL – 7.

[33]. **Disha Agarwal Amodini Vardhan and Pooja S (**2017) “AES BASED SYMMETRIC-BIOMETRIC CRYPTO SYSTEM USING USER PASSWORD” Department of Information and Communication, Technology Manipal Institute of Technology, Manipal, Karnataka, India.

[34]. R. Matsumura, T. Sugawara and K. Sakiyama, (2018), "A Secure LiDAR with AES-Based Side-Channel Fingerprinting," 2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW), pp. 479-482

[35]. N. E. Costea and E. V. Moisi, (2019), "Fingerprint Authentication for Budget Application," 2019 15th International Conference on Engineering of Modern Electric Systems (EMES), 2019, pp. 105-108

[36]. R. Guest and O. Miguel-Hurtado, (2011) "Enhancing off-line biometric signature verification using a fingerprint assessment approach," 2011 Carnahan Conference on Security Technology, pp. 1-4

[37]. F. Alonso-Fernandez, R. N. J. Veldhuis, A. M. Bazen, J. Fierrez-Aguilar and J. Ortega-Garcia, (2006), "Sensor Interoperability and Fusion in Fingerprint Verification: A Case Study using Minutiae-and Ridge-Based Matchers," 2006 9th International Conference on Control, Automation, Robotics and Vision, pp. 1-6

[38]. H. Xu and R. N. J. Veldhuis, (2010), "Complex spectral minutiae representation for fingerprint recognition," 2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition - Workshops, pp. 1-8

[39]. S. S. S. Priya, P. Karthigaikumar and N. M. S. Mangai, (2014) "Mixed random 128 bit key using finger print features and binding key for AES algorithm," 2014 International Conference on Contemporary Computing and Informatics (IC3I), pp. 1226-1230.

[40]. S. Cheepchol, W. San-Um, S. Kiattisin and A. Leelasantitham, (2014), "Digital biometric facial image encryption using chaotic cellular automata for secure image storages," The 4th Joint International Conference on Information and Communication Technology, Electronic and Electrical Engineering (JICTEE), pp. 1-5.

[41]. Jea, Tsai-Yang, Govindaraju, Venu (2005) “A minutia-based partial fingerprint recognition system” VL - 38, PP 1672 - 1684

[42]. Muthukumar Arunachalam, Kannan Subramanian,(2015) “AES Based Multimodal Biometric Authentication using Cryptographic Level Fusion with Fingerprint and Finger Knuckle Print” Vol. 12 PP 1-10

[43]. Journal of Physics: Conference Series, Volume 1916, 2021 International Conference on Computing, Communication, Electrical and Biomedical Systems (ICCCEBS) 2021 25-26 March 2021, Coimbatore, India.

[44]. Yousuf Janahi (2018) “Biometric Fingerprint Replaces PIN code on Point of Sale Machines in the Kingdom of Bahrain” International Business and Management Vol. 16, No. 2, pp. 48-51

[45]. Zhendong Wu, Zhengyin Lv, Jie Kang, Wenqian Ding, Jianwu Zhang, (2021) “Fingerprint bio-key generation based on a deep neural network” Volume37, PP 4329-4358

[46]. B. Chen and V. Chandran, (2007) "Biometric Based Cryptographic Key Generation from Faces," 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications (DICTA 2007), pp. 394-401

[47]. L. Wu, X. Liu, S. Yuan and P. Xiao, (2010) "A novel key generation cryptosystem based on face features," IEEE 10th INTERNATIONAL CONFERENCE ON SIGNAL PROCESSING PROCEEDINGS, pp. 1675-1678

[48]. Hua Yang, Zhendong Wu (2019),” A Biometric Key Generation Method for Fingerprint and Finger Vein Fusion” Cyberspace Safety and Security, 2019, Volume 11983, ISBN: 978-3-030-37351-1

[49]. M.Marimuthu, A.Kannammal (2015), “Dual Fingerprints Fusion for Cryptographic Key Generation” Assistant Professor Coimbatore Institute of Technology, Professor Coimbatore Institute of Technology, Volume 122

[50]. Panchal, Gaurang, Samanta, Debasis, (2018), “A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security” VL - 69, PP 461 – 478