International Journal of Emerging Technology and Innovative Engineering
Volume 5, Issue 3, March 2019 (ISSN: 2394 – 6598)

IMAGE ENCRYPTION APPLICATIONS: A SURVEY

I. Kalaimani
Assistant Professor
Mahendra Engineering College for Women
Kumaramangalam, India.
kalai.ilangovan@gmail.com

Abstract

Due to advances in the field of digital technology, Biometrics makes highest level of security over traditional methods like Passwords and PIN numbers. Biometric is the study of automated identification by use of physical (Fingerprint, Iris, Hand, DNA, Face) or behavioral (Voice, Signature, Keystroke) traits. Among all the Biometric traits, Fingerprint is an essential proven technology for verifying personal identity. In fact, Fingerprint patterns have stable, constant and distinctive features. For secure the biometrics fingerprint image from illegitimate users, many researchers have been proposed various techniques. In this paper survey of various reliable and robust fingerprint image encryption techniques has been discussed. From the survey, researchers have several fingerprint image encryption techniques which will show the way for enhancing the security.

Keywords: *Biometrics, Fingerprint, Image, Security, Encryption, Survey.*

1. Introduction:

Nowadays, Security is become very important issue in biometrics system [1]. Conventional security systems used knowledge based methods such as Passwords [3], pins [4] and token based methods such as key [14], license [15], smart card [16]. These methods are attacked by unauthorized person by using effective tools to crack the password or forged without permission of authorized holder [17]. So a biometrics system is needed for reliable, identification and authentication [18].

The word Biometrics with Greek origin meets “Life Measurement” which defines Bios as life and metric as a measurement [19]. Biometrics refers to science and technique for identifying/verifying the person by measuring and analyzing human characteristics [20]. It has the potential to distinguish between an authorized entity and faker [21]. Person to person have unique characteristics which are used to prevent threat [2]. Thus Biometrics has no risk of forgetting it, getting in stolen, getting it copied, being used by anyone else [22]. In general, biometric characteristics are divided in to two types [23]. One is Static (Physiological) that

refers shape of the body such as Fingerprints, Face, Iris, Hand geometry/ vein, Retinal pattern, DNA and the other is Dynamic (Behavior) that refers behavior of a person such as Signature, voice, keystroke, pulse [24-28]. The hardware captures the salient human characteristic. The software interprets the resulting data and determines acceptability [29-33].

3. Security of Fingerprint system:

Attacker tries to interpose digital thumb of authorized person in to the communications [34-36]. Therefore, Fingerprint images need to be protected from imposters before these images transmit over the communication channel [37-40]. In practice, there are two approaches for securing the image [41-45].

- Information Hiding(Water marketing)
- Encryption (Traditional-RSA, AES, DES, IDEA, others such as chaotic encryption methods) [46-77].

4. Literature Review

Fengling Han *et al.* [5] proposed a new effective method which use 2D Chaotic sequence obtained from multi scroll attractors for securing the fingerprint image. This method is based on asymmetric approach to enhance the security. A private key is generated from random pixel distribution of fingerprint images. In the encryption process, the fingerprint image is then XOR with 2D discrete chaotic sequence to get an encrypted image. In the decryption process, if valid private key is used then recover the original fingerprint, else different image exceptionally is produced.

Song Zhao *et al.* [6] proposed a novel fingerprint image encryption scheme in which the combination of shuttle operation and nonlinear dynamic filters chaotic map are used. In this scheme, the first step is to shuttle the fingerprint image and then performing exclusive-OR (XOR) with shuttled image and 8NDF chaotic sequence to get an encrypted image. It requires 10^{140} key space size to resist brute force attack.

Juan M. Vilardy *et al.* [7] have proposed Fractional Fourier Transform based fractional order as a key for fingerprint encryption/decryption. In this method, a grayscale fingerprint image is considered and it is placed as complex exponential. Then it is transformed 5 times and multiplied in intermediate steps by 4 random phase masks to get an encrypted image. The decryption is the inverse process of encryption. The key and masks in the decryption process must be equal key and the same masks used in encryption process to

recover the fingerprint image. Nevertheless, no fingerprint can be recovered. It requires $(95)^{10}$ possibilities to resist brute force attack.

A new method is introduced by Delong Cui *et al.* [8] in which the encryption process involves two steps. In First step, grayscale fingerprint image is considered and it is placed as complex exponential. Then it is transformed 2 times and multiplied in intermediate steps by 2 random phase masks to get an encrypted image. In second step, again that image is encrypted with the help of confusion matrix generated by a chaotic system. Decryption process is similar to an encryption process. In this method, fractional order is used as the key and also its size is reduced. Totally $(10)^{60}$ possibilities needed to succeed in brute force attack.

Rui liu *et al.* [9] have proposed a symmetric approach based on scrambling and confusion processes in the fingerprint image. In this algorithm, index values of the pixels are scrambled using chaotic map and then confuse the pixel using bit level permutation to enhance the security. This algorithm has large key space to resist various attacks and also time complexity is efficiently minimized. From analysis through experiment of the suggested model, verifying the strength by means of Histogram, spectrum, key space and sensitivity and various attacks.

P Devaki *et al.* [10] have proposed the finger print biometric security based on encryption and image slicing. In the encryption process, finger print image is encrypted using DES algorithm. In the slicing process, the encrypted image is sliced in to 'n' shares and stored on 'n' server. When all the slices are combined together only, the fingerprint image is recovered. To threat the fingerprint image, attacker not only requires key but also all the slices. This method has been deployed in various applications such as Finger print scanners and face recognition, etc.

G. Bhatnagar *et al.* **[**11**]** have been credited with proposing the new chaotic encryption model for enhancing the security for biometric data over the insecure channel in which fractional WPT, chaotic map and Hessenberg decomposition are used. This new method can be employed to other biometrics such as palm, iris, face, fingerprint, etc., In this frame work, shuffle the fingerprint image using affine transformation and the fractional wavelet packet transform (FrWPT) applied on it with transform orders which are chaotically generated. Then perform alteration on the FrWPT coefficient of every sub-band using the Hessenberg decomposition and chaotic map followed by perform inverse order FrWPT to obtain encrypted image. In order to show the security of new chaotic encryption technique, Key

space analysis, Edge similarity analysis, Randomness analysis, Histogram analysis, Correlation analysis, Numerical analysis was carried out.

F. Abundiz-P´erez *et al.* [12] have proposed the hyperchaotic Rössler map based fingerprint image encryption. The strength of the proposed method Rössler map is used to secure the fingerprint images; it is more complex behavior than a chaotic system. In the encryption process, the diffusion and permutation stages with assist of hyperchaotic Rössler map are involved. In the decryption process the inverse permutation stage and reverse diffusion stage with assist of hyperchaotic Rössler map are used.

Chander Kant *et al.* [13] have proposed a method by implementing RC4 algorithm to ensure the security of fingerprint image. RC4 is a stream cipher in which the same key is used for encryption and decryption process. Histogram test outcome of this method gives high security of the finger print images against statistical attacks. The result shown by them was higher than FISH, RABBIT, and SEAL cipher.

5. Conclusion

Since the authentication of biometrics techniques over open network occur more and more, security of such techniques is more important. In this literature survey, some important biometrics image encryption techniques have been discussed. The above all techniques are efficient for fingerprint image encryption and have their own advantages , disadvantages and give a perfect security. This survey paper very helpful for find the current trends of the fingerprint image security and next level of problem identification.

References

[1] Ashbourn, Julian. Biometrics: Advanced identity verification: the complete guide. Springer, 2014.

[2] Sharma, Monika. “Fingerprint Biometric System: A Survey.” International Journal of Computer Science & Engineering Technology (IJCSET) 5.07 (2014): 743-747.

[3] Sharma, Rahul, Nidhi Mishra, and Sanjeev Kumar Yadav. “Fingerprint Recognition System and Techniques: A Survey.” International Journal of Scientific & Engineering Research 4.6 (2013): 1670.

[4] Sravya. V, Radha Krishna Murthy,Ravindra Babu Kallam, Srujana B, “A Survey on Fingerprint Biometric System”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012.

[5] Han, Fengling, et al. “Fingerprint images encryption via multi-scroll chaotic attractors.” Applied Mathematics and Computation 185.2 (2007): 931-939.

[6] Song, Zhao, Li Hengjian, and Yan Xu. “A secure and efficient fingerprint images encryption scheme.” Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for. IEEE, 2008.

[7] Vilardy¹, Juan M., Cesar O. Torres, and Lorenzo Mattos. “FINGERPRINT ENCRYPTION USING FRACTIONAL FOURIER TRANSFORM.” (2008).

[8] Cui, Delong. “A novel fingerprint encryption algorithm based on chaotic system and fractional Fourier transform.” 2010 International Conference on Machine Vision and Human-machine Interface. IEEE, 2010.

[9] Liu, Rui. "Chaos-based fingerprint images encryption using symmetric cryptography." Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on. IEEE, 2012.

[10] P Devaki, Raghavendra Rao and Kumara swamy, “Securing the Biometric Image (finger print) through Encryption and Image slicing”, International Journal of Computer Science and Information Technology & Security (IJCSITS),Vol. 2, No.4, August 2012.

[11] Bhatnagar, Gaurav, and QM Jonathan Wu. “Enhancing the transmission security of biometric images using chaotic encryption.” Multimedia systems20.2 (2014): 203-214.

[12] Abundiz-Pérez, F., et al. “Fingerprint image encryption based on Rossler map”, Proceedings of the International Conference on Communications, Signal Processing and Computers, 2014.

[13] Chander Kant and Raksha, “Raising Security of Fingerprint Biometric Systems- using Advanced Encryption Scheme”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue. 5, May 2013.

[14] M. MUTHUKUMAR, Dr.T. RAVICHANDRAN,” Enhanced Database Compression and Decompression Techniques for Performance Improvement”, 2013, State Level Seminar on “EMERGING TRENDS AND ISSUES”, Kongu Arts and Science Collegs. ERODE

[15] K.Karthikeyan M Muthukumar, Senthil Pandian, “Analyzing and Improving the Performance of Decision Database with Enhanced Momentous Data Types”, Asia Journal of Information Technology, Volume: 16, Issue.9, Page(s): 699-705, 2017.

[16] Lakshmanaprabu, S. K., Shankar, K., Ilayaraja, M., Nasir, A. W., Vijayakumar, V., & Chilamkurti, N. (2019). Random forest for big data classification in the internet of things using optimal features. International Journal of Machine Learning and Cybernetics, 1-10. https://doi.org/10.1007/s13042-018-00916-z

[17] H. R. Boveiri, M. Elhoseny, A-COA: an adaptive cuckoo optimization algorithm for continuous and combinatorial optimization, Neural Computing and Applications, (2018). https://doi.org/10.1007/s00521-018-3928-9

[18] Haidi Rao, Xianzhang Shi, Ahoussou Kouassi Rodrigue, Juanjuan Feng, Yingchun Xia, Mohamed Elhoseny, Xiaohui Yuan, Lichuan Gu. Feature selection based on artificial bee colony and gradient boosting decision tree. Applied Soft Computing, 2018. https://doi.org/10.1016/j.asoc.2018.10.036

[19] Shankar, K., Lakshmanaprabu, S. K., Gupta, D., Khanna, A., & de Albuquerque, V. H. C. Adaptive optimal multi key based encryption for digital image security. Concurrency and Computation: Practice and Experience, e5122. https://doi.org/10.1002/cpe.5122

[20] Murugesan, M., & Ravichandran, T. (2012). Performance Enhancement Evaluation in Database Decompression Using HIRAC Algorithm. International Journal of Computer Science Issues (IJCSI), 9(6), 35.

[21] Elhoseny, M., Shankar, K., Lakshmanaprabu, S. K., Maseleno, A., & Arunkumar, N. (2018). Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural Computing and Applications, 1-15. https://doi.org/10.1007/s00521-018-3801-x

[22] Ambika Gopalakrishnan Unnikrishnan, Sanjay Kalra, Rakesh Kumar Sahay, Ganapathi Bantwal, Mathew John, Neeraj Tewari, "Prevalence of hypothyroidism in adults: An epidemiological study in eight cities of India", Indian Journal of Endocrinology and Metabolism, Vol.17, No.4, pp.647-653, 2017.

[23] Uthayakumar, J., Metawa, N., Shankar, K., & Lakshmanaprabu, S. K. (2018). Intelligent hybrid model for financial crisis prediction using machine learning techniques. Information Systems and e-Business Management, 1-29. https://doi.org/10.1007/s10257-018-0388-9

[24] Shankar, K., & Eswaran, P. (2015). ECC based image encryption scheme with aid of optimization technique using differential evolution algorithm. Int J Appl Eng Res, 10(55), 1841-5.

[25] Lydia, E. L., Kumar, P. K., Shankar, K., Lakshmanaprabu, S. K., Vidhyavathi, R. M., & Maseleno, A. (2018). Charismatic Document Clustering Through Novel K-Means Non-negative Matrix Factorization (KNMF) Algorithm Using Key Phrase Extraction. International Journal of Parallel Programming, 1-19.

[26] Shankar, K., Lakshmanaprabu, S. K., Gupta, D., Maseleno, A., & de Albuquerque, V. H. C. (2018). Optimal feature-based multi-kernel SVM approach for thyroid disease classification. The Journal of Supercomputing, 1-16.

[27] Dr.Muthukumar Murugesan, Dr. K. Karthikeyan, Dr.K. Sivakumar, "Analyzing Integral Components of SQL Server Databases Muthukumar Murugesan", International Journal of Applied Engineering Research (IJAER), Volume: 10, Issue.9, Page(s): 24189-24200, 2015.

[28] Maseleno, A., Tang, A. Y., Mahmoud, M. A., Othman, M., & Shankar, K. (2018). Big Data and E-Learning in Education 4.0. INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY, 18(5), 171-174.

[29] Amin, M. M., Maseleno, A., Shankar, K., Perumal, E., Vidhyavathi, R. M., & Lakshmanaprabu, S. K. (2018). Active Database System Approach and Rule Based in the Development of Academic Information System. International Journal of Engineering & Technology, 7(2.26), 95-101.

[30] Aminudin, N., Sundari, E., Shankar, K., Deepalakshmi, P., Fauzi, R. I., & Maseleno, A. (2018). Weighted Product and Its Application to Measure Employee Performance. International Journal of Engineering & Technology, 7(2.26), 102-108.

[31] Irviani, R., & Muslihudin, M. (2018). Nur algorithm on data encryption and decryption. International Journal of Engineering & Technology, 7(2.26), 109-118.

[32] Putra, D. A., Jasmi, K. A., Basiron, B., Huda, M., Maseleno, A., Shankar, K., & Aminudin, N. (2018). Tactical Steps for E-Government Development. International Journal of Pure and Applied Mathematics, 119(15), 2251-2258.

[33] Uthayakumar, J., Metawa, N., Shankar, K., & Lakshmanaprabu, S. K. (2018). Financial crisis prediction model using ant colony optimization. International Journal of Information Management. https://doi.org/10.1016/j.ijinfomgt.2018.12.001

[34] Muthukumar, M., & Ravichandran, T. (2012). Optimizing and enhancing parallel multi storage backup compression for real-time database systems. International Journal of Computer Technology and Applications, 3(4).

[35] Sugiyarti, E., Jasmi, K. A., Basiron, B., Huda, M., Shankar, K., & Maseleno, A. (2018). Decision support system of scholarship grantee selection using data mining. International Journal of Pure and Applied Mathematics, 119(15), 2239-2249.

[36] Susilowati, T., Jasmi, K. A., Basiron, B., Huda, M., Shankar, K., Maseleno, A., & Julia, A.(2018). Determination of Scholarship Recipients Using Simple Additive Weighting Method. International Journal of Pure and Applied Mathematics, 119(15), 2231-2238.

[37] Lydia, E. L., Shankar, K., Ilayaraja, M., & Kumar, K. S. Technological Solutions for Health Care Protection and Services Through Internet Of Things (IoT). International Journal of Pure and Applied Mathematics, 118(7), 277-283.

[38] Noura Metawaa, M. Kabir Hassana, and Mohamed Elhoseny. Genetic algorithm based model for optimizing bank lending decisions. Expert Systems with Applications, 2017, 80, pp, 75–82.

[39] Lydia, E. L., Shankar, K., Pamina, J., & Raja, J. B. Correlating NoSQL Databases With a Relational Database: Performance and Space. International Journal of Pure and Applied Mathematics, 118(7), 235-244.

[40] Muthukumar, M., & Ravichandran, T. Optimizing multi storage parallel backup for real time database systems. IJESAT, ISSN, 2250-3676.

[41] Tarek Gaber, Sarah Abdelwahab, Mohamed Elhoseny, Aboul Ella Hassanien, Trust-based secure clustering in WSN-based intelligent transportation systems, Computer Networks, (2018), 146, pp. 151-158.

[42] Muslihudin, M., Wanti, R., Hardono, N., Shankar, K., Ilayaraja, M., Maseleno, A., ... & Mukodimah, S. (2018). Prediction of Layer Chicken Disease using Fuzzy Analytical Hierarcy Process. International Journal of Engineering & Technology, 7(2.26), 90-94.

[43] K. Shankar and P.Eswaran. “A Secure Visual Secret Share (VSS) Creation Scheme in Visual Cryptography using Elliptic Curve Cryptography with Optimization Technique”. Australian Journal of Basic and Applied Sciences. Volume: 9, Issue.36, Page(s): 150-163, 2015.

[44] Ashraf Darwish, Aboul Ella Hassanien, Mohamed Elhoseny, Arun Kumar Sangaiah, Khan Muhammad, The Impact of the Hybrid Platform of Internet of Things and Cloud Computing on Healthcare Systems: Opportunities, Challenges, and Open

Problems, Journal of Ambient Intelligence and Humanized Computing, (2017), pp.1-16. https://doi.org/10.1007/s12652-017-0659-1

[45] Mohamed Elhoseny, Ahmed Abdelaziz, Ahmed Salama, AM Riad, Arun Kumar Sangaiah, Khan Muhammad, A Hybrid Model of Internet of Things and Cloud Computing to Manage Big Data in Health Services Applications, Future Generation Computer Systems, 86, (2018), pp.1383-1394.

[46] Shankar, K. (2017). Prediction of Most Risk Factors in Hepatitis Disease using Apriori Algorithm. RESEARCH JOURNAL OF PHARMACEUTICAL BIOLOGICAL AND CHEMICAL SCIENCES, 8(5), 477-484.

[47] I.S. Farahat, A.S. Tolba, Mohamed Elhoseny, Waleed Eladrosy, A secure real-time internet of medical smart things (IOMST), Computers & Electrical Engineering, (2018), 72, pp. 455-467.

[48] Mohamed Elhoseny, Gustavo Ramírez-González, Osama M. Abu-Elnasr, Shihab A. Shawkat, Arunkumar N, Ahmed Farouk, Secure Medical Data Transmission Model for IoT-based Healthcare Systems, IEEE Access, (2018), 6, pp. 20596 - 20608.

[49] Karthikeyan, K., Sunder, R., Shankar, K., Lakshmanaprabu, S. K., Vijayakumar, V., Elhoseny, M., & Manogaran, G. (2018). Energy consumption analysis of Virtual Machine migration in cloud using hybrid swarm optimization (ABC–BA). The Journal of Supercomputing, 1-17.

[50] Lakshmanaprabu, S. K., Shankar, K., Khanna, A., Gupta, D., Rodrigues, J. J., Pinheiro, P. R., & De Albuquerque, V. H. C. (2018). Effective Features to Classify Big Data Using Social Internet of Things. IEEE Access, 6, 24196-24204.

[51] Mohamed Elhoseny, Xiaohui Yuan, Hamdy K El-Minir, and AM Riad, " Extending self-organizing network availability using genetic algorithm", In 2014 International Conference on Computing, Communication and Networking Technologies (ICCCNT), (2014),pp, 11-13.

[52] Hamid Reza Boveiri, Raouf Khayami, Mohamed Elhoseny, M. Gunasekaran. An efficient Swarm-Intelligence approach for task scheduling in cloud-based internet of things applications, Journal of Ambient Intelligence and Humanized Computing, 2018. https://doi.org/10.1007/s12652-018-1071-1

[53] Shankar, K., Elhoseny, M., Lakshmanaprabu, S. K., Ilayaraja, M., Vidhyavathi, R. M., Elsoud, M. A., & Alkhambashi, M. (2018). Optimal feature level fusion based

ANFIS classifier for brain MRI image classification. Concurrency Computat Pract Exper, e4887.

[54] Mohamed Elhoseny, Noura Metawa and Aboul Ella Hassanien, An automated information system to ensure quality in higher education institutions, Proceedings of 12th International Computer Engineering Conference (ICENCO), IEEE, 2016, pp, 196 - 201, https://doi.org/10.1109/ICENCO.2016.7856468

[55] Murugesan, M., & Ravichandran, T. (2013). Evaluate database compression performance and parallel backup. International Journal of Database Management Systems, 5(4), 17.

[56] Mohamed Elhoseny, Noura Metawa, Ashraf Darwish, and Aboul Ella Hassanien, Intelligent Information System to Ensure Quality in Higher Education Institutions, Towards an Automated E-University, International Journal of Computational Intelligence Studies, (2017), 6(2/3), pp. 115-149.

[57] Gupta, D., Khanna, A., Shankar, K., Furtado, V., & Rodrigues, J. J. Efficient artificial fish swarm based clustering approach on mobility aware energy-efficient for MANET. Transactions on Emerging Telecommunications Technologies, e3524. https://doi.org/10.1002/ett.3524 e3524

[58] Mohamed Elhoseny, K. Shankar, S. K. Lakshmanaprabu, Andino Maseleno, N. Arunkumar. Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural Computing and Applications. 2018. https://doi.org/10.1007/s00521-018-3801-x

[59] Shankar, K., & Lakshmanaprabu, S. K. (2018). Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm. International Journal of Engineering & Technology, 7(1.9), 22-27.

[60] Ahmed E Hassan, Mohamed E Ibrahim, Designing quality e-learning environments for higher education, Educational Research, 1(6):186-197, 2010.

[61] Mahmud Kandel, Ahmed E Hassan, Aziza S Asem, Mohamed E Ibrahim, UML Analysis for Quality Assurance Management System for Higher Education, International Journal of Engineering Science and Technology, (2010), 2(4), pp. 417-432.

[62] Lakshmanaprabu, S. K., Mohanty, S. N., Shankar, K., Arunkumar, N., & Ramirez, G. (2019). Optimal deep learning model for classification of lung cancer on CT images. Future Generation Computer Systems, 92, 374-382.

[63] Ahmed Abdelaziza, Mohamed Elhoseny, Ahmed S. Salama, A.M. Riad, A Machine Learning Model for Improving Healthcare services on Cloud Computing Environment, Measurement, (2018), 119, pp. 117-128.

[64] Murugesan, C., & Ravichandran, T. (2013). Real time database compression optimization using iterative length compression algorithm. In Int. Conf. on Computer Science and Information Technology, USA (pp. 99-105).

[65] Shankar, K., Elhoseny, M., Chelvi, E. D., Lakshmanaprabu, S. K., & Wu, W. (2018). An Efficient Optimal Key Based Chaos Function for Medical Image Security. IEEE Access, 6, 77145-77154.

[66] Alaa Tharwat, Mohamed Elhoseny, AboulElla Hassanien, Thomas Gabel, and N. Arun kumar Intelligent Beziér Curve-based Path Planning Model Using Chaotic Particle Swarm Optimization Algorithm, Cluster Computing, (2018), pp. 1-22. https://doi.org/10.1007/s10586-018-2360-3

[67] Avudaiappan, T., Balasubramanian, R., Pandiyan, S. S., Saravanan, M., Lakshmanaprabu, S. K., & Shankar, K. (2018). Medical image security using dual encryption with oppositional based optimization algorithm. Journal of medical systems, 42(11), 208.

[68] El-Shorbagy MA, Elhoseny M, Hassanien AE, Ahmed SH. A novel PSO algorithm for dynamic wireless sensor network multiobjective optimization problem. Transactions on Emerging Telecommunications Technologies. (2018);e3523. https://doi.org/10.1002/ett.3523

[69] Mohamed Elhoseny, Khaled Elleithy, Hamdi Elminir, Xiaohui Yuan, and Alaa Riad. Dynamic Clustering of Heterogeneous Wireless Sensor Networks using a Genetic Algorithm, Towards Balancing Energy Exhaustion. International Journal of Scientific & Engineering Research, (2015), 6(8), pp, 1243-1252.

[70] Singhal, N., Sinha, P., Agarwal, N., & Murugesan, M. (2011). U.S. Patent Application No. 12/819,774.

[71] Shankar, K., Elhoseny, M., Kumar, R. S., Lakshmanaprabu, S. K., & Yuan, X. (2018). Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique. Journal of Ambient Intelligence and Humanized Computing, 1-13. https://doi.org/10.1007/s12652-018-1161-0

[72] Muthukumar Murugesan, D. K. K. (2016). Business intelligence market trends and growth in enterprise business. International Journal on Recent and Innovation Trends in Computing and Communication, 4(3), 188-192.

[73] Lakshmanaprabu, S. K., Shankar, K., Gupta, D., Khanna, A., Rodrigues, J. J., Pinheiro, P. R., & de Albuquerque, V. H. C. (2018). Ranking analysis for online customer reviews of products using opinion mining with clustering. Complexity, 2018.

[74] Xiaohui Yuan, Daniel Li, Deepankar Mohapatra, Mohamed Elhoseny. Automatic removal of complex shadows from indoor videos using transfer learning and dynamic thresholding. Computers and Electrical Engineering, 2017, 70, pp, 813-825.

[75] Farahat I.S., Tolba A.S., Elhoseny M., Eladrosy W. Data Security and Challenges in Smart Cities. In: Hassanien A., Elhoseny M., Ahmed S., Singh A. (eds) Security in Smart Cities: Models, Applications, and Challenges. Lecture Notes in Intelligent Transportation and Infrastructure. Springer, Cham, 2019. https://doi.org/10.1007/978-3-030-01560-2_6

[76] Murugesan, M., Karthikeyan, K., & Sivakumar, K. (2015). Novel investigation methodologies to identify the SQL server query performance. Indian Journal of Science and Technology, 8(27).

[77] Maseleno, A., Tang, A. Y., Mahmoud, M. A., Othman, M., Negoro, S. Y., Boukri, S.,& Muslihudin, M. The Application of Decision Support System by Using Fuzzy Saw Method in Determining the Feasibility of Electrical Installations in Customer's House. International Journal of Pure and Applied Mathematics, 119(16).

[78] Raja, J. Beschi, S. Chenthur Pandian, and J. Pamina. "Certificate revocation mechanism in mobile ADHOC grid architecture." Int. J. Comput. Sci. Trends Technol 5 (2017): 125-130.

[79] Lydia, E. Laxmi, K. Shankar, J. Pamina, and J. Beschi Raja. "Correlating NoSQL Databases With a Relational Database: Performance and Space." International Journal of Pure and Applied Mathematics 118, no. 7: 235-244.

[80] Raja, J. Beschi, and K. Vivek Rabinson. "Iaas for Private and Public Cloud using Openstack." International Journal of Engineering 5.04 (2016).

[81] Raja, J. Beschi, and V. Vetriselvi. "Mobile Ad Hoc Grid Architecture Based On Mobility of Nodes." International Journal of Innovative Research in Computer and Communication Engineering 2 (2014): 49-55.

[82] Deepa, V., A. Jenifa, and J. Pamina. "APPROACHES BASED ON DATA MINING IN NATURAL LANGUAGE PROCESSING." International Journal Of Emerging Technology And Innovative Engineering 4.2 (2018).

[83] Sree, GM Apurva, S. Ashika, S. Karthi, V. Sathesh, M. Shankar, and J. Pamina. "CHURN PREDICTION IN TELECOM USING CLASSIFICATION ALGORITHMS." International Journal of Emerging Technology and Innovative Engineering 5.2 (2019).

[84] Raja, Beschi & Jeyakumar, Pamina & Panchapakesan, Madhavan & Kumar, Sampath. (2018). MARKET BEHAVIOR ANALYSIS USING DESCRIPTIVE APPROACH. International Journal of Pure and Applied Mathematics. 118. 171-176.

[85] J.Pamina, J.Beschi Raja. “SURVEY ON DEEP LEARNING ALGORITHMS”. International Journal of Emerging Technology and Innovative Engineering 5.1 (2019).

[86] V Akhila, M Krithikaa, A.K Pavithra, K.G Adhipathy, J. Pamina."ANALYSING THE BEHAVIOUR OF CUSTOMERS TO PREDICT CHURN IN TELECOM SECTOR." International Journal of Emerging Technology and Innovative Engineering 5.2 (2019).