ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 9, No. 4, December 2021, pp.1159-1165

Secure wireless sensor network using cryptographic technique based hybrid genetic firefly algorithm

Iman Mohammed Burhan[1], Sura khalil Ibrahim[2], Zainab Taha Jebur[3], Musaddak Maher Abdul Zahra[4a ,b], Mohanad Ahmed Salih[5], Refed Adnan Jaleel[6]

[1] Dept. of Computer Science, College of Medicine, University of Babylon, Iraq
[2,3]Dept. of Computer Techniques Engineering, Al-Nisour University College, Iraq
[4a] Dept. of Computer Tech. Engineering, Al-Mustaqbal University College, Iraq
[4b] Dept. of Electrical Engineering, University of Babylon, Iraq
[5]Dept. of Computer Science, Al-Anbar University, Iraq
[6]Dept. of Information & Communication Engineering, Al-Nahrain University, Iraq

ABSTRACT

Wireless sensor networks (WSNs) are formed of self-contained nodes of sensors that are connected to one base station or more. WSNs have several primary aims one of them is to transport network node's trustworthy information to another one. As WSNs expand, they become more vulnerable to attacks, necessitating the implementation of strong security systems. The identification of effective cryptography for WSNs is a significant problem because of the limited energy of the sensor nodes, compute capability, and storage resources. Advanced Encryption Standard (AES) is an encryption technique implemented in this paper with three meta-heuristic algorithms which are called Hybrid Genetic Firefly algorithm, Firefly algorithm, and Genetic algorithm to ensure that the data in the WSNs is kept confidential by providing enough degrees of security. We have used hybrid Genetic firefly as a searching operator whose goal is to improve the searchability of the baseline genetic algorithm. The suggested framework's performance that based on the algorithm of hybrid genetic firefly is rated by using Convergence Graphs of the Benchmark Functions. From the graphs we have conclude that hybrid genetic firefly with AES is best from other algorithms.

Keywords: WSN, AES, Firefly algorithm, Genetic algorithm, Encryption

Corresponding Author:

Refed Adnan Jaleel
Information and Communication Engineering
Al-Nahrain University
Baghdad, Iraq
E-mail: Iraq_it_2010@yahoo.com

1. Introduction

One of the most rapidly developing technologies in the data processing and communication networks fields nowadays is wireless sensor networks. WSNs are made up of physically small nodes of sensors that communicate with one another primarily about the surroundings [1] [2]. Security, energy efficiency, size, scalability, energy efficiency, quality-of-service, processing power, and coverage and deployment are the primary challenges in WSNs [3] [4]. Security is a big issue in the wireless sensor networks, which is one of these challenges. Because the unguided data transmission medium is even more open to security attacks than the guided data transmission, wireless networks are more exposed to numerous security risks. The importance of secure data transmission via an unreliable channel is growing all the time. In order to secure wireless sensor networks, they must provide all four security properties: integrity, confidentiality, availability, and authenticity. In WSN, cryptography is a very basic data security mechanism. In all aspects, such as power

© The Author 2021. This work is licensed under a Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0/) that allows others to share and adapt the material for any purpose (even commercially), in any medium with an acknowledgement of the work's authorship and initial publication in this journal.

consumption, operating speed, and storage, it is best to select the most effective cryptographic method [5]. A metaheuristic protocol is similar to a heuristic protocol, but it is considered to be more effective because no compelled local lower limits are used. By running heuristic techniques across the search space, the metaheuristic can acquire superior results, bringing out its best capabilities. There are various instances where the heuristic method produces a solution that is sufficient. To identify better solutions, heuristic procedures rely on trial-and-error, learning, and adaptability. It is impossible to demand the optimum solution in every situation, but a good enough or optimal solution in a reasonable amount of time is acceptable [6]. When compared to other approaches that can be expensive when computing resources are considered, heuristic methods are particularly fast in computing [5 & 6]. The following are a few of the meta-heuristic protocols: The Firefly Algorithm (FA) is a metaheuristic protocol that was lately constructed. A Genetic Algorithm (GA) is a type of heuristic algorithm used in global search. It creates individuals who are dissimilar in order to determine the greatest potential solution. In GA, optimized fitness function is a technique [7] [8].

2. Material and methods

2.1. Wireless sensor network

Depending on the application, wireless sensors use a specific wireless protocol. 2.4 GHz radios based on standards either of IEEE 802.11/Wi-Fi or IEEE 802.15.4 among the standards available. In the measuring field, a sensor that is wireless is spread according to protocol [9] [10]. That sensor then runs in the background, continuously, recording, monitoring, categorizing, and pushing the obtained data to a central place. Gateway is the name of the central location [11]. The information gathered is recorded as numerical data. In addition, the Open Geospatial Consortium (OGC) has established interoperability standards that make it easier to integrate sensors into the internet and control them using a web browser [12]. To monitor the patient's health, these sensors were placed near or inside the patient. Wearable devices, for example, can assist in the monitoring of unwell patients within the hospital setting [13] [14]. Figure 1 shows an example for WSNs on the mine site.

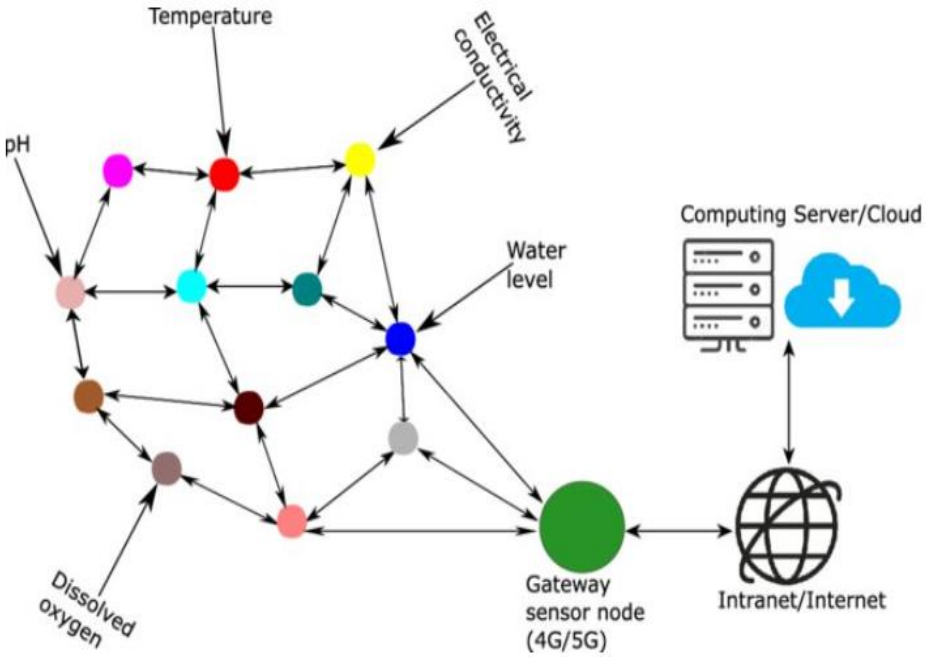


Figure 1. Deployment of WSNs on the mine site

2.2. Cryptographic technique

AES/Rijndael is a block cipher that is iterated, which means that the first input block and cipher key are transformed several times before the output is produced. A State is the name given to each intermediate

ciphering result [15]. The procedure of encryption appoint a set of key rounds, which are uniquely derived keys. These would be implemented on data array that have one data block to be encrypted, along with other processes. That array is referred to as the state array. The AES encryption method produces cipher text that is completely indecipherable conversion, unreadable plaintext data, which is the version of data that people could understand and read. The AES ciphertext, which is the result of the encryption process, couldn't be read unless a secure AES key is being used to decipher it [16] [17]. Figure 2 shows work of AES.

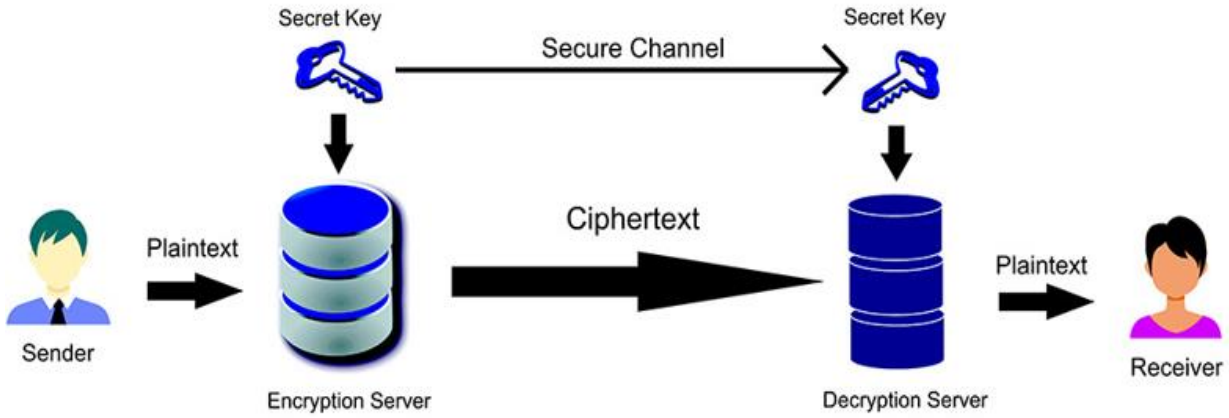


Figure 2. Working of AES

2.3. Genetic algorithm

Genetic Algorithm (GA) has been created by Holland J. and it is a model of biological evolution on the basis of Charles Darwin's nature selection theory [18]. The essential part of GA is formed from genetic operators such as the crossover, mutation, and selection. Individuals are stochastically selected from the population to create the basis of the next population. The fitter individuals have a more chance of selection than weaker one. To select the best individuals, many ways of selection are used such as Roulette Wheel, Rank, and Tournament Selections [19]. The crossover selects genes from parent, and creates a new offspring. Commonly, a process of taking two parent genes is used, such as uniform, and two point crossover. After performing the crossover, individuals are mutated. This process is to prevent falling into a local optima. Mutation changed the Genes of the offspring randomly [20]. Figure 3 shows Gentle introduction to Genetic Algorithm.

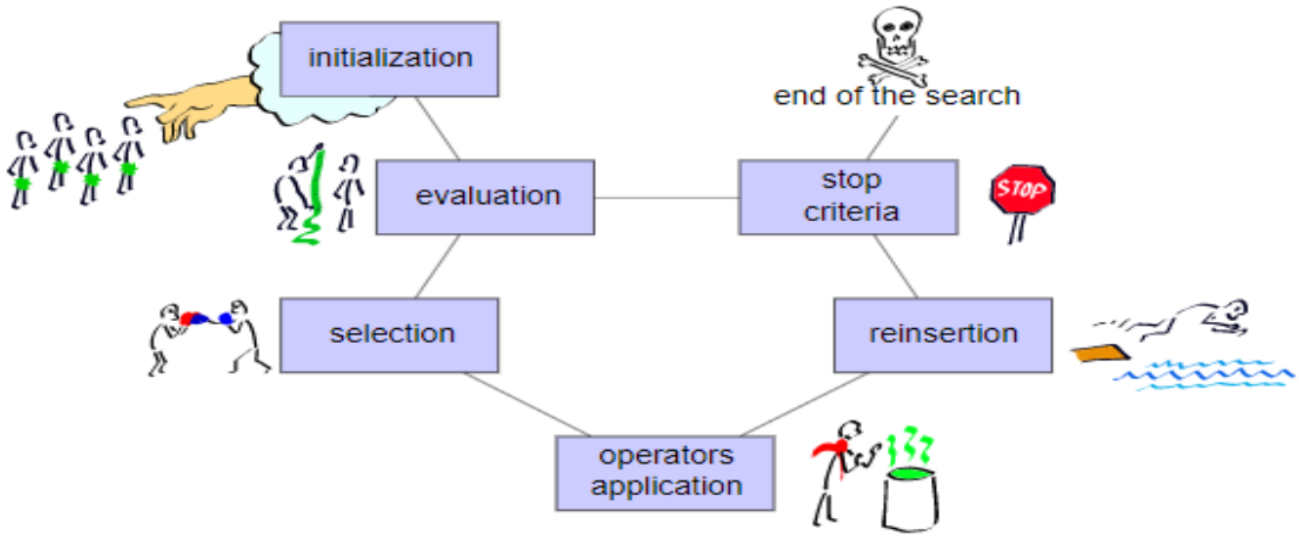


Figure 3. Gentle introduction to genetic algorithm

2.4. Firefly algorithm

Xin-She Yang created the Firefly algorithm in 2008 [4], which is an algorithm of metaheuristic that bases on fireflies' behavior, and the patterns of flashing. Regarding fireflies, Yang used the following hypotheses [21] [22]: For a more complete description of the firefly optimization, we turn to Yang, X. S [4], who proposed the firefly Pseudo code method [23] [24]. The fundamental steps of the firefly method are summarized in Figure 4.

• Because fireflies are unisexual, whatever firefly would be attracted with every other firefly [25].

• The less brilliant firefly would be attracted to the firefly that are brighter. However, as the distance between the fireflies grows, the light intensity drops [26].

• If there is no nearby fireflies that are brighter, the firefly would be migrate randomly.

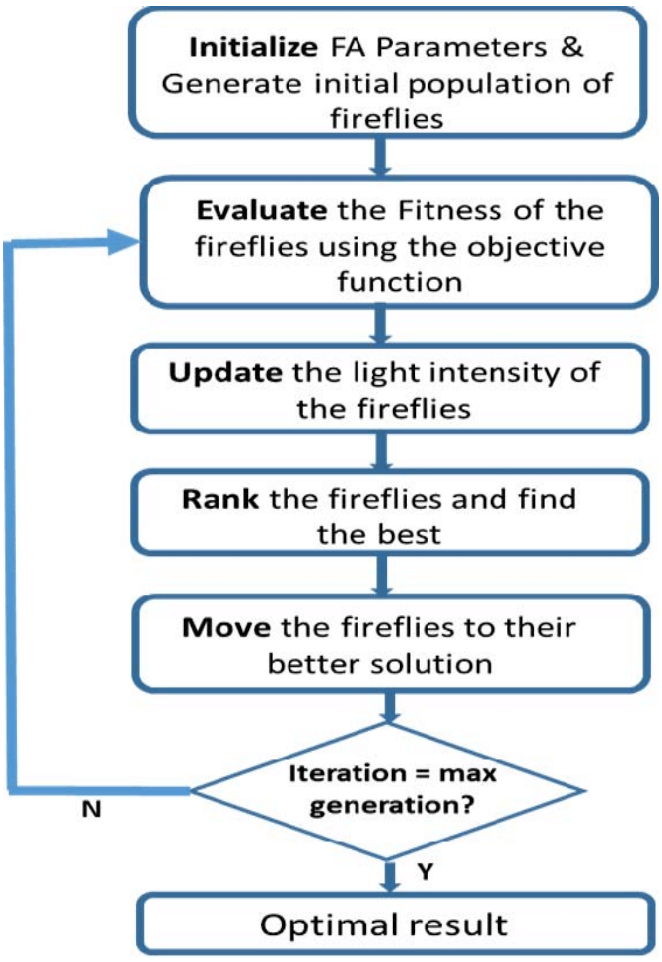
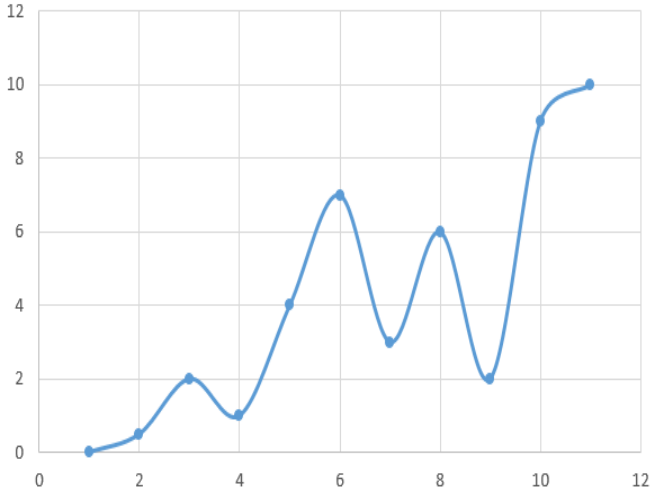


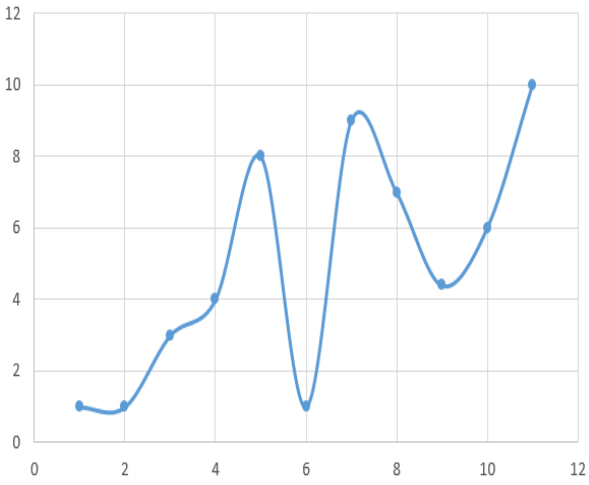
Figure 4. Flowchart of firefly algorithm

3. Results and discussion

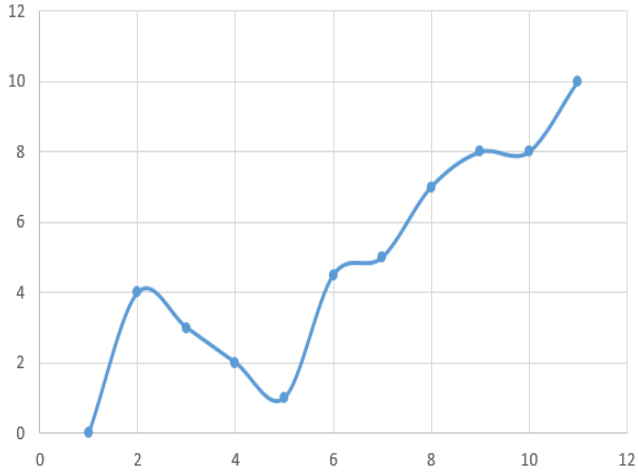
In this paper, we combine Firefly with AES, Genetic, and Hybrid between two algorithms to generate a solution to the problems and improve AES technique using matlab program on 4GB RAM and Intel CORE i3 platform specifications. The algorithm is tested on a datasets range to evaluate the recommended methods. These are two-dimensional Euclidean distance databases. On each dataset, we repeated the experiment 40-times in order to determine the minimum and the average length of the tour. The results have been compared to that of other proposed algorithms. Figure 5 shows the length of the tour as a result of using our proposed method (Hybrid genetic firefly with AES). In the majority of situations, combining hybrid genetic fireflies with AES creates perhaps a better or competitive tour. For the data sets, the proposed approach produces better results.



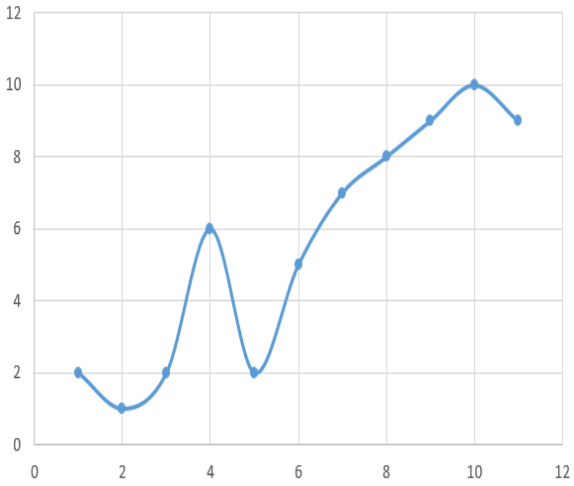
a) Genetic algorithm



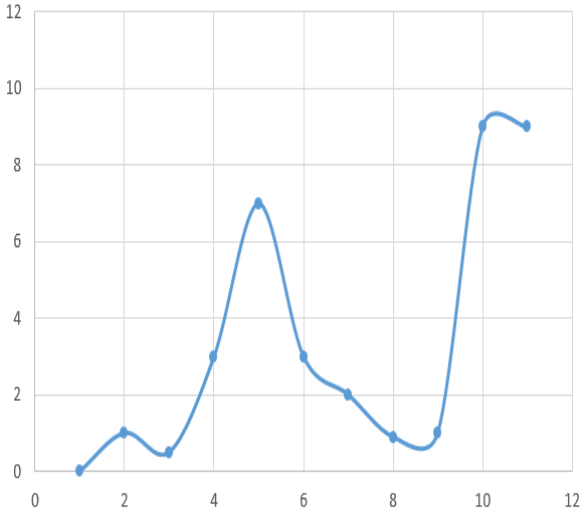
D) Genetic algorithm with AES



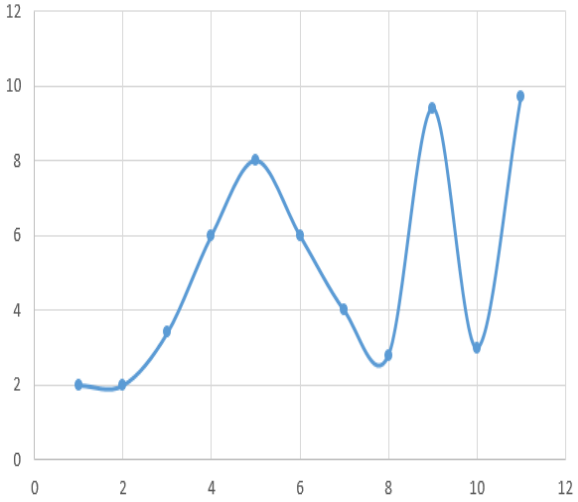
b) Firefly algorithm



E) Firefly algorithm with AES



c) Hybrid Genetic firefly



F) Hybrid Genetic firefly with AES

Figure 5. Average convergence graphs

4. Conclusions

We used the Firefly Algorithm in this research paper. In conjunction with the AES technique, the genetic algorithm and hybrid genetic firefly algorithm are used as a search operator. The proposed algorithm's main goal was to improve the basic genetic algorithm's global ability of search and level of security in WSNs. The suggested hybrid version of Genetic firefly algorithm with AES has addressed the majority of the problems that were tested and evaluated its effectiveness according to convergence towards the recognized solutions that are optimal of the benchmark's function against GA.

References

[1] A. S. Jaradat and S. B. Hamad, "Community Structure Detection Using Firefly Algorithm," *International Journal of Applied Metaheuristic Computing*, vol. 9, no. 4, pp. 52-70, 2018.

[2] L. Tan, Y. Tan, G. Yun and C. Zhang, "An improved genetic algorithm based on k-means clustering for solving traveling salesman problem," *Proceedings of the 2016 International Conference on Computer Science, Technology and Application (CSTA2016)*, pp. 334-343, 2017.

[3] R. Matai, S. Singh, and M. L. Mittal, "Traveling Salesman Problem: An Overview of Applications, Formulations, and Solution Approaches," 2012.

[4] M. P. Durisic, et al., "A survey of military applications of wireless sensor networks," in *2012 Mediterranean Conference on Embedded Computing (MECO)*, pp. 196–199, Bar, Montenegro, June 2012.

[5] N. K. Suryadevara, et al., "WSN-based smart sensors and actuator for power management in intelligent buildings," *IEEE/ASME Transactions on Mechatronics*, vol. 20, no. 2, pp. 564–571, 2015.

[6] R. Rodriguez, et al., "Process management in Iot operating systems: cross-influence between processing and communication tasks in end-devices," *Sensors*, vol. 19, no. 4, p. 805, 2019.

[7] M. Živković, et al., "A survey and classification of wireless sensor networks simulators based on the domain of use," *Adhoc and Sensor Wireless Networks*, vol. 20, 2014.

[8] Z. Kasiran, S. Abdullah, and M. Nor, "An advance encryption standard cryptosystem in iot transaction". *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, no. 3, pp. 1548-1554, 2020.

[9] I. Salih, A. Alabaich, and Y. Tuama, "Enhancing advance encryption standard security based on dual dynamic XOR table and mixcolumns transformation". *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 3, pp. 1574-1581, 2020.

[10] J. Madhloom, K. Ghani, and R. Baharon, "ECG Encryption Enhancement Technique with Multiple Layers of AES and DNA Computing. *INTELLIGENT AUTOMATION AND SOFT COMPUTING*, vol. 28, no. 2, pp. 493-512, 2021.

[11] B. K. Abdullah Ahmed, et al., '' A Novel secure artificial bee colony with advanced encryption standard technique for biomedical signal processing,'' *Periodicals of Engineering and Natural Sciences*, in press, 2021.

[12] A. Ezugwu, et al., "A Comparative Study of Meta-Heuristic Optimization Algorithms for 0 - 1 Knapsack Problem: Some Initial Results", *Digital Object Identifier 10.1109/ACCESS.2019.2908489*.

[13] S. Qian, Y. Liu, Y. Ye and G. Xu, "An enhanced genetic algorithm for constrained knapsack problems in dynamic environments", *Natural Computing*, vol. 18, pp. 913-932, 2019.

[14] S. Gupta and P. Poonam, "Solving travelling salesman problem using genetic algorithm", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 6, pp. 376-380, 2013.

[15] N. G. Ali, et al., '' Hybrid of K-Means and partitioning around medoids for predicting COVID-19 cases: Iraq case study'', *Periodicals of Engineering and Natural Sciences*, vol. 9, no. 4, pp. 569-579, October 2021.

[16] R. A. Jaleel, I. M. Burhan, and A. M. Jalookh , "A Proposed Model for Prediction of COVID-19 Depend on K-Nearest Neighbors Classifier: Iraq Case Study, " *Proc. of the 3rd International Conference on Electrical, Communication and Computer Engineering (ICECCE) 12-13 June 2021, Kuala Lumpur, Malaysia*, DOI: 10.1109/ICECCE52056.2021.9514171.

[17] M. R. Jawad, et al., "*Advancement of Artificial Intelligence Techniques based Lexicon Emotion Analysis for Vaccine of COVID_19*," *Periodicals of Engineering and Natural Sciences*, vol. 9, no. 4, pp. 580-588, October 2021.

[18] M. Fama, S. Lucarelli, and R. Orzi, "Rethinking Money, Rebuilding Communities: A Multidimensional Analysis of Crypto and Complementary Currencies". *Partecipazione e conflitto*, vol. 13, no. 1, pp. 337-359, 2020.

[19] Z. Rahaman, et al., "A novel structure of advance encryption standard with 3-dimensional dynamic S-Box and key generation matrix". *arXiv preprint arXiv:2005.00157*.2020

[20] A. Nadjia and A. Mohamed, "Aes ip for hybrid cryptosystem rsa-aes". *2015 IEEE 12th International Multi-Conference on Systems, Signals & Devices (SSD15)* (pp. 1-6). IEEE. 2015.

[21] H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", *arXiv preprint arXiv*: 2003.06557, 2020.

[22] C. Rego, et al., "Traveling salesman problem heuristics: Leading methods implementations and latest advances", *European Journal of Operational Research*, vol. 211, pp. 427-441, 2011.

[23] A. Jaradat, B. Matalkeh, and W. Diabat, '' Solving Traveling Salesman Problem using Firefly algorithm and K-means Clustering,'' *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, 2019.

[24] M.K. Ariyaratne, T.G. Fernando, and S. Weerakoon, "A Modified Firefly Algorithm to Solve Univariate Nonlinear Equations with Complex Roots", *Proceedings of the 2015 Fifteenth International Conference on Advances in ICT for Emerging Regions (ICTer); Colombo, Sri Lanka*, pp. 160–167, August 2015.

[25] S. K. Sarangi, et al., "A New Modified Firefly Algorithm for Function Optimization, *"Proceedings of the 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT),* Chennai, India, pp. 2944–2949, March 2016.

[26] M. K. Ariyaratne, T. G. Fernando, and S. Weerakoon," Solving systems of nonlinear equations using a modified firefly algorithm (MODFA)," *Swarm and Evolutionary Computation*, vol. 48, pp. 72-92, August 2019.