An enhanced fireworks algorithm to generate prime key for multiple users in fingerprinting domain

Hussein Ali Ismael[1], Jamal Mustafa Abbas[2], Salama A. Mostafa[3], Ali Hussein Fadel[4]
[1,2]Sollege of science, University of Diyala, Iraq
[3]Faculty of Computer Science and Information Technology, Universiti Tun Hussin Onn Malaysia, Malaysia
[4]Department of Computer Science, University of Diyala, Iraq

Article Info

Article history:

Received Mar 1, 2020
Revised May 12, 2020
Accepted Jun 30, 2020

Keywords:

3D logistic chaotic map
Convolution
Fireworks and camel algorithms
Otsu method
QRcode

ABSTRACT

This work presents a new method to enhance the performance of fireworks algorithm to generate a prime key for multiple users. A threshold technique in image segmentation is used as one of the major steps. It is used processing the digital image. Some useful algorithms and methods for dividing and sharing an image, including measuring, recognizing, and recognizing, are common. In this research, we proposed a hybrid technique of fireworks and camel herd algorithms (HFCA), where Fireworks are based on 3-dimension (3D) logistic chaotic maps. Both, the Otsu method and the convolution technique are used in the pre-processing image for further analysis. The Otsu is employed to segment the image and find the threshold for each image, and convolution is used to extract the features of the used images. The sample of the images consists of two images of fingerprints taken from the Biometric System Lab (University of Bologna). The performance of the anticipated method is evaluated by using FVC2004 dataset. The results of the work enhanced algorithm, so quick response code (QRcode) is used to generate a stream key by using random text or number, which is a class of symmetric-key algorithm that operates on individual bits or bytes.

Corresponding Author:

Salama A. Mostafa,
Faculty of Computer Science and Information Technology,
Universiti Tun Hussin Onn Malaysia,
Johor, Malaysia.
Email: salama@utm.edu.my

1. INTRODUCTION

The threshold is the least common method of image segmentation used to create parallel and binary images of colour segmented images. This article presents the Otsu image segmentation technique, which is the method for naming each pixel of the source image for at least two categories [1]. Otsu's strategy is used as a pre-made image to split images for further processing, for example, to highlight searches and metrics. Otsu's strategy seeks to set a threshold that limits the internal fluctuations of a segmented image [2].

Convolution technique is one of the basic operations that can be applied in an image. Feature extraction is the most important phase in the building of any pattern classification. The purpose of feature extraction is to extract information that is characterized by each image [3]. The histogram of image segmentation is used to find out the appropriate value of the thresholding. The histogram of the image is calculated by the number of pixels having the same grey level. Then it performs the normalization operation on the pixel which has the value between (0 and 1) [4]. Besides, the fireworks algorithm is a relatively new intelligence algorithm (SI). The important thought of the fireworks algorithm comes from the idea of fireworks in the evening sky. The explosion of fireworks in a single attempt brings a complete adjustment to the optimization algorithm [5]. Swarm intelligence (SI) is a subject that manages forged and distinctive frames that illustrate the general practices of beings. The camel herd algorithm (CHA) has been proposed as another swarm intelligence algorithm [6, 7]. Camel algorithm is a new recall algorithm based on the camel's travel behaviour in the wild in harsh environments. The hybrid algorithm is used to determine the ideal response for different measurement test functions [8].

The chaotic logistics map is considered one of the very important popular examples of chaos dynamics. The fundamental chaos theory creates a procedural structure and provides a distinctive device for exploring and knowing the complex behaviour in the installation of dynamic systems [9]. We briefly review some recent works concerning fingerprint authentication to find the best solution to overcome any problem by finding the threshold of each image by using the Otsu method. Moreover, the Otsu method is one of the effective processes that is employed for the selection of the threshold [10]. It is well known for being less time-consuming. The Otsu thresholding method involves iteration along with the all probable threshold values and evaluation of standard layout for the all4 pixel levels that occupy each side of the threshold. The first step in this method is segmenting the image into background and foreground parts [11, 12].

In this work, we propose a convolution technique for feature extraction, in which it is simple for a mathematical operation that it could be a fundamental part of many common image-processing operations. It is used to perform a diversity of image processing tasks, such as edge detection [13], smoothing [14], and blurring [15]. This work includes feature extraction by using convolution to find the best coordinates image. These coordinates are used to give optimal solutions by using the fireworks algorithm after segmentation the image into four regions, where each region of convolution is represented as one solution [16].

The algorithm of fireworks (FWA) involves the known algorithm of swarm intelligence by the explosion of real fireworks, which have drawn considerable speculation from analysts. It recreates the explosions more than once to look for firework in the neighbourhood around a specific location [17]. It evolves towards an ideal disposition. An updated FWA improves the comparative functionality of the first FWA and allows for better execution. Dynamic FWA (Dyn FWA) uses a unique explosive mode for extinguishing the current fire to make the study more intelligent and logical [18, 19].

The paper includes five sections; starting with Section 1 which represents the introduction. Section 2 describes the most common related works, whereas the proposed model of this work has been discussed in section 3. Section 4 concludes the paper.

2. RESEARCH METHOD

The proposed work creates a hybrid of fireworks and camel algorithms (HFCA) depending on the fingerprint biometric image. Fireworks algorithm (FWA) is based on the 3D logistic chaotic maps by creating a hybrid optimization to enhance the performance of the firework algorithm (FWA) by replacing the Gaussian sparks solution with the camel herds (CHA) solution. In biometric, each image of the fingerprint images has unique features which are extracted by using convolution techniques, to classify these features into two categories, max and min histogram convolution. These techniques aimed to find the best-coordinated position inside the image of fingerprint biometric. The results of enhanced FWA by hybrid optimization produce best coordinates position which is used by dropping these coordinate to (QRcode) to generate stream cipher key. Stream ciphers can encrypt a portion of the plaintext messages of variable length. This work consists of four stages, as shown in Figure 1. Each stage consists of several steps and each step has its procedures as illustrated in the following:

- Conversion of the original image is a step towards Grayscale image. The conversion process is based on (1). The (fingerprint) biometric image is uploading from the dataset. The image contains a three-colour band (R, G, and B) respectively. The intensity value can be obtained from each band and these values will be converted to grayscale value.

$$\text{Grayscale image }(i, j) = 0.2989 * R + 0.5870 * G + 0.1140 * B \tag{1}$$

- Conversion of the grayscale image step from grayscale to binary using Otsu's method. It includes finding the value of the threshold fingerprint images these images are dependent on the Otsu's method. Maximizing the variance between-class variance background and foreground regions of the input image specifies the optimal threshold.

$$Pi = ni/N,\ Pi > 0 \sum_{i=1.}^{L} Pi = 1 \tag{2}$$

Feature extraction step uses the convolution technique. Important and required features of the image are extracted by this technique. The extraction of features depends on the strength of the pattern of the mask, which is of a certain size, where the pattern of the mask is applied to the image. This stage consists of two algorithms, which are the fireworks algorithm (FWA) and camel herds algorithm (CHA). The FWA on 3D logistic chaotic maps is used to enhance the performance of fireworks. The CHA replaces part of the firework algorithm to form hybrid techniques.

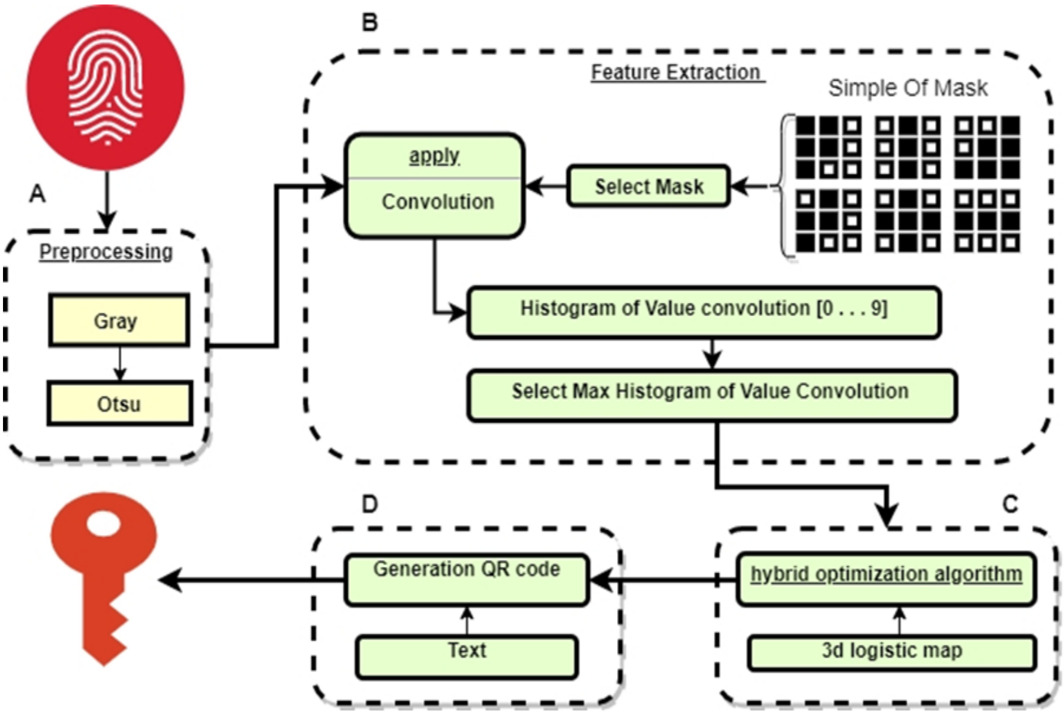


Figure 1. The impacts of choosing diverse switching in unique and dynamic conditions

2.1. Fireworks algorithm

Fireworks Algorithm (FWA) is working in four regions and takes from each region its coordinates (min coordinate as start and max coordinate as a goal). It aims to find three optimal solutions for the four regions of the fingerprint image: initial, spark, and Gaussian amplitude. Each one of the solutions must be evaluated based on the fitness function to know how FWA is close to the target [20]. The fitness function depends on the formula in equation:

$$\text{Fitness}^{n}_{\text{spark,Gaussian } and\ amplitude} = \text{Max (number of black feature locations)} \tag{3}$$

where n is the feature coordinate location [x, y] in four regions, the best solution is the maximum number of black locations, and the worst solution is the less minimum number of white locations.

The FWA always follows the edges of the fingerprint image. The initial solution is matching with an edge of a fingerprint image, so by default, it is considered the optimal solution as shown in Figure 2. The chaotic logistics map is one of the very important popular examples of chaos dynamics [21, 22]. The principles of chaos theory create a procedural structure and provide a distinctive device for exploring and knowing the complex behaviour in the installation of dynamic systems. The 3D logistic map is used to increase the security level of the encryption method [9, 23, 24].

2.2. Camel herds algorithm

The camel herds algorithm (CHA) relies on the behaviour of camels in the desert. Knowing that there is a leader for each herd, the major purpose of the herd is searching for food and water depending on factor humidity value (Hum). Furthermore, there is a neighbouring strategy that should be taken into consideration. Figure 3 shows the flowchart of CHA [25-30].

CHA arranges herds and each herd produces an arrangement. The herds take the number, choose one of the camels and turn it into a herd guide. The herd leader (LHC) is based on coordinates (min. Histogram folding). Each LHC begins with an alternative point to the space problem. This method offers different arrangements [13]. After setting the parameters, CHA presents the amount in study mode. The leader begins with his coordinate position [x, y].

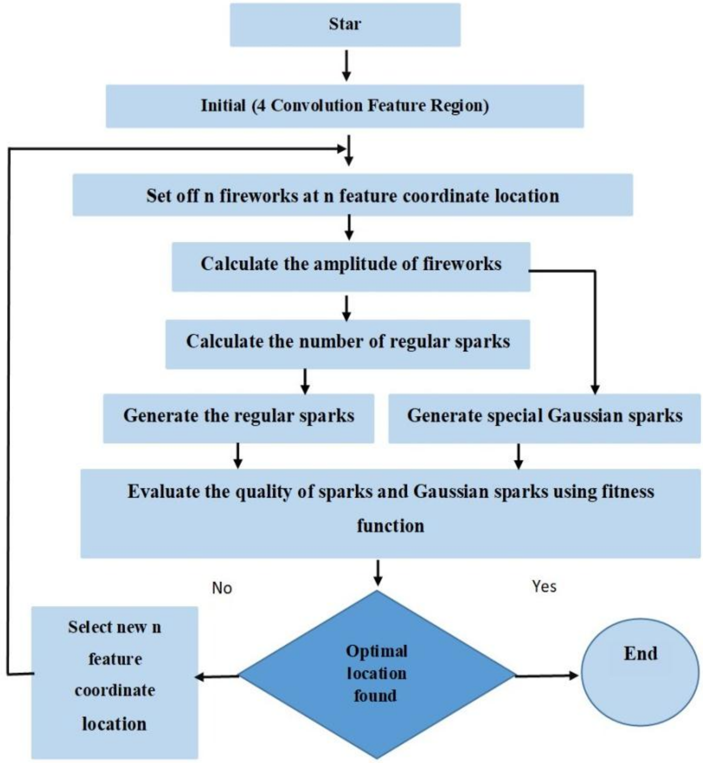

Star
Initial (4 Convolution Feature Region)
Set off n fireworks at n feature coordinate location
Calculate the amplitude of fireworks
Calculate the number of regular sparks
Generate the regular sparks
Generate special Gaussian sparks
Evaluate the quality of sparks and Gaussian sparks using fitness function
No
Yes
Select new n feature coordinate location
Optimal location found
End

Figure 2. The flowchart of FWA

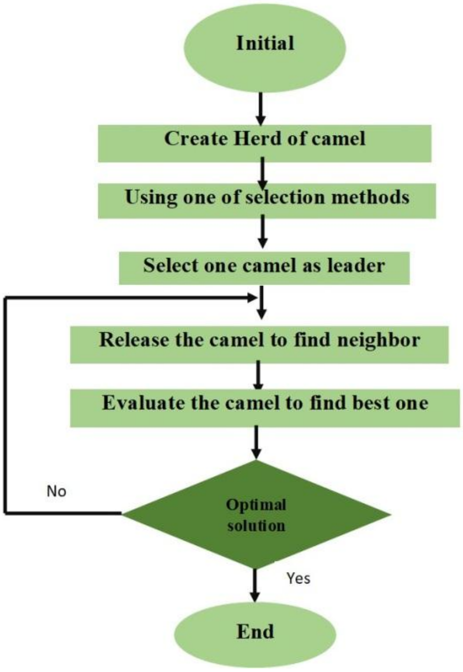

Initial
Create Herd of camel
Using one of selection methods
Select one camel as leader
Release the camel to find neighbor
Evaluate the camel to find best one
No
Optimal solution
Yes
End

Figure 3. The flowchart of the CHA

2.3. Hybrid optimization approaches

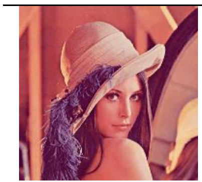
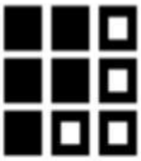
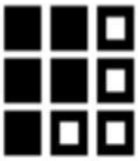
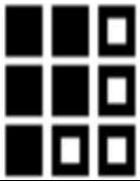
A hybrid optimization algorithm consists of firework and camel herd algorithms. The proposed hybrid aims to increase the speed of access to the best solution and thus reduce the access time that improves the performance of the optimization algorithm, as shown in Figure 3. Furthermore, as we discussed previously, this work aims to enhance the FWA based on the 3D logistic chaotic maps. The principle of the hybrid optimization algorithm is the enhancement performance of the firework algorithm (FWA) by replacing the Gaussian sparks solution by the camel herd solution. The reason for using the camel herd algorithm is giving perfect camels distribution over sample space to find the best solution.

Gaussian distributions are used to generate new sparks following Gaussian dissemination. Gaussian works ineffectively at the FWA for two reasons: First, it only affects the fireworks responsible for the blast caused by the person responsible for the blast for example; the operator, and then strengthens the connection between the sparks. Second, Gaussian sparks are unlikely to pass on to the next generation.

3. RESULTS AND DISCUSSION

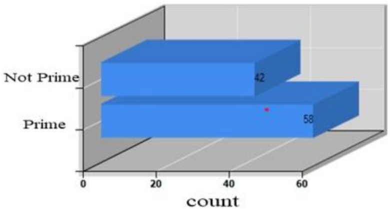
In Table 1, steganography is proposed to camouflage the data media. The technique of hiding information in the spatial field is one of the ways where data can be directly hidden on the image in a way that does not affect the hidden text visible in the cover image. The results are based on three samples of universal images, which are the image of Leena, the image of vegetables, and the image of fruit.

Table 1. The results of the hidden text

Image	Form mask (group box)	Key length	Mean square error	Peak signal to noise ratio	Image fidelity	Universal image quality index
		128	0.0000044321	101.6646758012	0.9999999717	0.9999999996
		256	0.0000099723	98.1428506201	0.9999999363	0.9999999992
		512	0.0000138504	96.7161755844	0.9999999115	0.9999999988
		1024	0.0000249307	94.1634505333	0.9999998407	0.9999999979
		128	0.0000055402	100.6955756711	0.9999999557	0.9999999996
		256	0.0000130194	96.9848970484	0.9999998960	0.9999999992
		512	0.0000191136	95.3173847204	0.9999998473	0.9999999988
		1024	0.0000379501	92.3386699562	0.9999996968	0.9999999977
		128	0.0000070363	99.6573555969	0.9999999505	0.9999999995
		256	0.0000129468	97.0091773668	0.9999999088	0.9999999991
		512	0.0000168871	95.8552431797	0.9999998811	0.9999999987
		1024	0.0000329299	92.9548970661	0.9999997681	0.9999999976

The proposed work generates a prime key that is derived from the stream key used for multiple users. A prime key is of a variable-length that depends on using the best coordinates of the fingerprint image as shown in Table 2. The prime key that is extracted is strong because it is checked by using a parameter namely Miller Rabin Test to get the highest percentage of the prime key. The extracted prime key depends on the concept of the one-time pad (OTP), which is also called the perfect cipher, or crypto algorithm. It means that each person has a simple space key. This simple space key works on the principle of one - time pad.

Table 2. Generation of a prime key

#	Key length	Number	Ch. prim	Check key by using the Miller Rabin test
1	00011111110101	13513115241254	True	
2	10001010110100	15628562541698	True	
3	01011110111101	30125615246852	False	
4	11110100110000	60241121254765	False	
5	11101111010101	12048221254782	False	
6	10000001110000	24097192014031	True	
7	10000001110000	22419510218737	False	
8	01110100100000	19313513215064	True	
9	00110101110010	62856121029547	False	
10	00011001010101	12561120014568	True	

The basic concept of stream cipher security is based on the concepts of Shannon's theory of secrecy systems and one time pad (OTP). Due to its immense contribution to the field of communication, the stream key is used to apply OTP with letters or numbers. In the first example, the use of letters is explained. The OTP keys are called OTLP (one-time letter pad) Encrypted text is always the conclusion of the encryption but only a ciphertext letter. This content framework is less adaptable to a number-based framework. It only needs one encrypted text letter for each plain text letter and one encryption step, which makes it very fast for a manual site as the results are presented in Table 1

4. CONCLUSION

This work aimed to present a new technique to generate stream cipher key by using a fingerprint biometric image and using the best coordinates is produced by a hybrid technique. The system used a random text to generate QRCode through which a stream key is produced. The generated key is of variable size, unique, and unpredictable. The system which generates a stream key depends on the points that were extracted during dropping a point of QRCode. The generated prime key derived from the stream key is used for multiple users and it is strong prime and unique because it is checked by using the parameter namely Miller Rabin Test to get the highest percentage of the prime key. In addition, it is flexible and more secure. This prime key depends on the principle of a One-time pad (OTP). It means that each person has a simple space key. This simple space key works on the principle of one - time pad. (Whatever new advancements may emerge in the future when encryption becomes an unusual and indelible framework that offers true long-term confidentiality. This key can be used in banks, emergency departments and numerous institutions).

ACKNOWLEDGEMENTS

This project is supported by the Directorate of Education in Diyala, Ministry of Education, Diyala, Iraq. It is also supported by Research Fund to E15501, Research Management Center, UTHM.

REFERENCES

[1] K. Bhargavi and S. Jyothi, “A survey on threshold-based segmentation technique in image processing,” *International Journal of Innovative Research & Development*, vol. 3, no. 12, pp. 234-239, 2014.

[2] N. Senthilkumaran and S. Vaithegi, “Image segmentation by using thresholding techniques for medical images,” *Computer Science & Engineering: An International Journal (CSEIJ)*, vol. 6, no. 1, pp. 1-13, 2016.

[3] G. Kumar and P. K. Bhatia, “A detailed review of feature extraction in image processing systems,” *2014 Fourth International Conference on Advanced Computing & Communication Technologies*, pp. 5-12, 2014.

[4] M. K. Tripathi and D. D. Maktedar, “A framework with OTSU’S thresholding method for fruits and vegetable image segmentation," *International Journal of Computer Applications*, vol. 179, no. 52, pp. 25-32, 2018.

[5] J. Yu, H. Takagi, and Y. Tan, “Accelerating the fireworks algorithm with an estimated convergence point,” *International Conference on Swarm Intelligence*, pp. 263-272, 2018.

[6] A. T. S. Al-Obaidi, H. S. Abdullah, and Z. O. Ahmed, “Camel herds algorithm: A new swarm intelligent algorithm to solve optimization problems,” *Int. Journal on Perceptive and Cognitive Computing*, vol. 3, no. 1, pp. 6-10, 2017.

[7] S. Selvaraj and E. Choi, “Survey of swarm intelligence algorithms,” *In Proceedings of the 3rd International Conference on Software Engineering and Information Management*, pp. 69-73, 2020.

[8] M. K. Ibrahim and R. S. Ali, “Novel optimization algorithm inspired by camel traveling behavior,” *Iraq Journal Electrical and Electronic Engineering*, vol. 12, no. 2, pp. 167-177, 2016.

[9] J. M. Al-Tuwaijari, “Image encryption based on fractal geometry and chaotic map,” *Diyala Journal for Pure Science*, vol. 14, no. 1, pp. 166-182, 2018.

[10] H. J. Vala and A. Baxi, “A review on otsu image segmentation algorithm,” *International Journal of Advanced Research in Computer Engineering &* Technology, vol. 2, no. 2, pp. 387-389, 2013.

[11] N. Kaur and R. Kaur, “A review on various methods of image thresholding,” *International Journal on Computer Science and Engineering*, vol. 3, no. 10, pp. 3441-3443, 2011.

[12] M. A. Jubair, S. A. Mostafa, R. C. Muniyandi, H. Mahdin, A. Mustapha, M. H. Hassan, M. A. Mahmoud, Y. A. Al-Jawhar, A. S. Al-Khaleefa, and A. J. Mahmood, “Bat optimized link state routing protocol for energy-aware mobile ad-hoc networks,” *Symmetry*, vol. 11, no. 11, pp. 1409, 2019.

[13] C. Yu, J. Li, and Y. Tan, “Improve enhanced fireworks algorithm with differential mutation,” *2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 264-269, 2014.

[14] S. Yeung, Rinaldo, J. Jopling, B. Liu, R. Mehra, N. L. Downing, M. Guo, G. M. Bianconi, A. Alahi, J. Lee, B. Campbell, K. Deru, W. Beninati, L. Fei-Fei, and A. Milstein, “A computer vision system for deep learning-based detection of patient mobilization activities in the ICU,” *NPJ digital medicine*, vol. 2, no. 1, pp. 1-5, 2019.

[15] N. K. Pawan and M. Narnaware, “3D chaotic functions for image encryption,” *International Journal of Computer Science Issues*, vol. 9, no. 3, pp. 323-328, 2012.

[16] J. Li and Y. Tan, “A comprehensive review of the fireworks algorithm,” *ACM Computing Surveys*, vol. 52, no. 6, pp. 1-28, 2019.

[17] S. He and L. Schomaker, “DeepOtsu: Document enhancement and binarization using iterative deep learning,” *Pattern Recognition*, vol. 91, pp. 379-390, 2019.

[18] A. B. Patil and J. A. Shaikh "OTSU thresholding method for flower image segmentation," *International Journal of Computational Engineering Research*, vol. 6, no. 5, pp. 1-6, 2016.

[19] M. A. Jubair, S. A. Mostafa, A. Mustapha, and H. Hafit, "A survey of multi-agent systems and case-based reasoning integration," *2018 Inte. Symp. on Agent, Multi-Agent Systems and Robotics (ISAMSR)*, pp. 1-6, 2018.

[20] M. Tuba, N. Bacanin, and A. Alihodzic, "Multilevel image thresholding by fireworks algorithm," *2015 25th International Conference Radioelektronika (RADIOELEKTRONIKA)*, pp. 326-330, 2015.

[21] T. Gao and Z. Chen, "Image encryption based on a new total shuffling algorithm," *Chaos, Solitons & Fractals*, vol. 38, no. 1, pp. 213-220, 2008.

[22] H. Nawata, "Coastal resource use by camel pastoralists," *Nilo-Ethiopian Studies*, vol. 7, pp. 23-43, 2001.

[23] Eerdunchaolu, K. Takehana, E. Yamamoto, A. Kobayashi, G. Cao, Baiyin, H. Ueda, and P. Tangkawattana, "Characteristics of dorsal lingual papillae of the Bactrian camel (*Camelus bactrianus*)," *Anatomia, Histologia, Embryologia*, vol. 30, no. 3, pp. 147-151, 2001.

[24] B. A. Khalaf, S. A. Mostafa, A. Mustapha, A. Ismaila, M. A. Mahmoud, M. A. Jubaira, and M. H. Hassan, "A simulation study of syn flood attack in cloud computing environment," *AUS Journal*, vol. 26, no. 1, pp. 188-197, 2019.

[25] S. A. Mostafa, A. Mustapha, P. Shamala, O. I. Obaid, and B. A. Khalaf , "Social networking mobile apps framework for organizing and facilitating charitable and voluntary activities in Malaysia," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 2, pp. 827-833, 2020.

[26] J. Yu, H. Takagi, and Y. Tan, "Fireworks algorithm for multimodal optimization using a distance-based exclusive strategy," *2019 IEEE Congress on Evolutionary Computation (CEC)*, pp. 2215-2220, 2019.

[27] E. Tuba, M. Tuba, and E. Dolicanin, "Adjusted fireworks algorithm applied to retinal image registration," *Studies in Informatics and Control*, vol. 26, no. 1, pp. 33-42, 2017.

[28] W. A. Mustafa, M. M. M. A. Kader, and Z. I. A. Khalib, "Improved wolf algorithm on document images detection using optimum mean technique," *Bulletin of Electrical Engineering and Informatics*, vol. 8, no. 2, pp. 551-557, 2019.

[29] S. Zheng, J. Li, A. Janecek, and Y. Tan, "A cooperative framework for fireworks algorithm," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 14, no. 1, pp. 27-41, 2017.

[30] M. Oktiana, F. Arnia, Y. Away, and K. Munadi, "Features for cross spectral image matching: A survey," *Bulletin of Electrical Engineering and Informatics*, vol. 7, no. 4, pp. 552-560, 2018.