



Secure Image Encryption Using Chicken Swarm Optimization-Based Key Generation

C. Swetha

Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India.

To Cite this Article

C. Swetha (2024). Secure Image Encryption Using Chicken Swarm Optimization-Based Key Generation, International Journal for Modern Trends in Science and Technology, 2024, 10(11), pages. 113-120.
<https://doi.org/10.46501/IJMTST1011013>

Article Info

Received: 29 October 2024; Accepted: 24 November 2024.; Published: 26 November 2024.

Copyright © C. Swetha ; This is an open access article distributed under the [Creative Commons Attribution License](#), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ABSTRACT

Today's world, image encryption is used to send interactive image data with the highest level of security and accuracy. There are a variety of picture encryption methods that can be used to transfer hidden pictures. Of these methods, Elliptic Curve Cryptography (ECC) is one of the most intriguing for keeping image data safe and private. The ECC approach generates the public and private key pair that is used to encrypt and decrypt a picture during the key generation phase. The public key is created randomly during the encryption phase. The private key (H) is developed using a Chicken Swarm Optimization (CSO) based optimization technique in the proposed method decryption procedure. The PSNR value is used to measure the image's performance and is used as a health value for optimization. In comparison to current approaches, the proposed approach has the best PSNR performance.

INTRODUCTION

Nowadays, mobile devices are now part of our daily life. They can be used for a variety of purposes including making Phone calls, listening to music, and browsing the Internet. They can be used for video conferencing or online transactions[1]. Therefore, security has become a major concern when accessing wireless networks through mobile devices. A mobile user typically accesses a wireless network by connecting to the nearest network access point with a strong signal [2][3]. These wireless connections must be authorized to block access. Mobile users can get free access: access the wireless network. Due to unstable radio signals from mobile devices in power saving mode, mobile devices may turn off when connecting to different access

points[4][5]. The need to restart when reconnecting creates a significant lag. This header increases as the mobile user surrounds the remote network, which increases line time because the remote network requires the user to be authenticated by the home network's authentication server[6].

Elliptic Curve Cryptography (ECC) computing is well known for its capabilities as enhanced encryption and labeling and is therefore enthusiastically recommended by the National Security Agency (NSA) [7]. The ECC hypothesis relies on the mathematics of elliptical loops, making it difficult to program the new logarithm of elliptical loops in an abelian bundle using reasonable tricks. ECCs is typically secure, more limited and faster than their exemplary counterparts such as

Ron Reeves, Adi Shamir Leonard Adleman (RSA), and the Digital Signature Algorithm (DSA) [8][9]. Therefore, ECC achieves zones such as confirmation, extended signature, secure correspondence and signature handling. The tests allowed in remote sensing organizations are an important issue. The confidentiality of some WSNs renders them unhelpful against bargaining power [10][11]. The security style of the WSN imposes many stringent requirements for the verification of various assets and organization and attacks. The plan of the remote sensor network for this overriding security or validation program must be powerful against attacks leading to sensor transactions and additional security concerns [12]. However, you often cannot find an effective remote security enhancement plan, which usually depends on the keys and encryption / encryption measures used. Likewise, longer cryptographic keys actually require higher baud rates, more memory, and preparation power.

An incredible opportunity to create cryptographic keys is ergonomics, vulnerability to input conditions and competence during long-term operation, used in a number of purposes [13]. There are many cryptographic calculations. The numerical hypothesis is central to any cryptographic technique. Each has a unique use case and solves a specific problem. This problem is evolving over time, and as it progresses, the current structure needs to be adjusted to implement this change. Portable data processing is the norm by which all advances in cryptography will be measured over the next decade [14]. Thanks to the approach of Apple Pay, Google Wallet and many other portable exchanges, they are common in most currency exchanges [15][16]. This requires strong cryptographic calculations for the assets, not benefits, but is an important precondition for the security of more beautiful structures. Legacy conditions, with their limited assets, fuzzy selection standards, and elliptical curvature cryptography, are the most predictable crypto strategies.

In this study, we reveal how to maintain IoT intermediate information security using ACECC strategy. We currently make series information bases largely dependent on usage. In this step, we perform an ACECC calculation based on organizational information to select the ideal hub. We have already defined the collection of information for all data in order to identify personal and non-confidential data. At

this point, we encrypt sensitive information using ECC and then store it with the cloud provider.

LITERATURE REVIEW

To deal with security issues in the IoT climate, experts have introduced different and different security arrangements using cryptography programs. This section depicts past and related works in the IoT security region.

Sethuraman *et al.* [17] Diffie Hellmann has introduced a fuzzy genetic elliptical curve to ensure correspondence between companies. The uniqueness of elliptical curve cryptography (ECC) lies in the ability to produce information using efficient limited keys to provide the RSA's long-standing key prerequisite. Intelligent guidelines are used for stabilization during key determination measurements, and many characteristic dynamic models with fuzzy reasoning to obtain keys and hereditary calculations to compulsorily improve computation in the ECC get the proposed FGECDH calculation.

Dharminder *et al.* [18] have provided a secure letter based on learning error on cell phones using fluffy extraction. The security verification of the proposed method ensures provable-security by learning the problem of errors at some point in the irregular prophecy. Besides, a simple security conversation and execution test shows that our LWESM conference is effective and can be used in many different applications. Joshi *et al.* [16] have implemented a lightweight verification conference for body territory networks based on elliptical-curve cryptography. This conference empowers the customer to refuse by immediately updating the time key. The proposed conference meets different security requirements, for example, non-connectivity, secrecy, forward security, shared confirmation and meeting key security. Experimental testing at AVISPA proved that the cost of verification conference calculation and efficiency on the part of the client was completely reduced compared to the existing arrangements, which are more suitable for property restricted remote body regional systems.

Sowjanya *et al.* [19] presented a guaranteed framework for WBAN using Ciphertext and Attribute-Based Elliptic Curve Elliptic Curve Encryption (CPABE) without implementing linear coordination. The proposed CPABE is provided under Diffie-Hellman's

assumption of elliptical curve determination and in addition has a customer / brand disclaimer segment. We investigated the light portion of the proposed CPABE, differentiating it from other ABE plans for WBAN.

Kumar *et al.*[20] have introduced a protected elliptic bend cryptography based common confirmation convention for cloud-helped TMIS. The proposed convention secure against man-in-the-center assault, understanding secrecy, replay assault, known-key security property, information classification, information non-disavowal, message confirmation, pantomime assault, meeting key security and patient unlink capacity. The proposed convention with existing related conventions in same cloud based TMIS. The proposed convention guarantees of all alluring security requirements and dealt with the productivity as far as calculation and correspondence costs for cloud-helped TMIS.

PROPOSED METHODOLOGY

The proposed method enhances the confidentiality and secrecy of original image between the sender and receiver. From the original image the RGB (Red-Green-Blue) values are taken and create a separate matrix for each component by using their pixel values[21]. Then the image is divided into blocks before the encryption and decryption process. Basically, the block size is 4×4 . The blocks of the each color component are encrypted by using the ECC method. The key generation process of the ECC method generates the private key randomly in the encryption and decryption process[22]. In the proposed method decryption process, the private key is generated by applying the optimization technique which integrates the CSO with it. The performance of the image is taken as a fitness value for the optimization process and here the peak signal-to-noise ratio (PSNR) value is considered[23]. After the encryption method, the encrypted image is decrypted by using the reverse process of the encryption. When the decryption process is completed, the output image compare with the original image for evaluating their performance using the peak signal-to-noise ratio (PSNR) value, Mean square error (MSE), and correlation coefficient (CC) as quality parameters.

3.1 Elliptical Curve Cryptography

ECC is one some kind procedure for applying public key cryptography in asymmetric key cryptography. Based on this procedure, the maximal limit is calculated with a fixed base point and the prime number function, and the encryption follows:[24] The basic ECC equation is shown in equation (1)

$$y^2 = x^3 + ax + b \quad (1)$$

Here, a and b are the integers

The intensity of encryption depends on the created key in every cryptographic operation. Two forms of key generation are available in the proposed process[25][26]. Firstly, public key is produced for encrypting the message from the receiver end and secondly, to create a private key to decrypt the original picture at the reception end. If the value " P " is any some point on the curve, select a random integer number " H ", which is a private key, in the area of " 1 to $n-1$ ", then the public key " Q " is generated as (2)

$$Q = H \times P \quad (2)$$

3.1.1. Encryption method

In the encryption part of the procedure, every color band of the input picture is divided into the blocks. These four blocks are encrypted by the proposed encryption method [27][28]. The total count of the blocks is presented as $F(i, j)$. Where i and j are the number of rows and columns of the blocks of the image. The pixels $P_x(i, j)$ and $P_y(i+1, j)$ and the point is obtained in (3) and (4)

$$C_1 = H \times P_e \quad (3)$$

$$C_2 = (P_x, P_y) + C_1 \quad (4)$$

3.1.2. Decryption method

In the decryption part of the procedure, the private key (H) is used to decrypt the information and the point C_3 of equation (5) is used to decrypt the pixel point

$$C_3 = H \times C_1 \quad (5)$$

$$C_{ij} = C_2 - C_3 \quad (6)$$

In this process the C_{ij} represents the final result. In the procedure of decryption, the secret key (H) is produced by the proposed CSO technique, which gives the best optimized values compared to the existing ECC technique.

3.2 CSO Optimization Technique

The CSO calculation is used to determine the best location for the main module. It usually mimics the mating pattern of chicken preservatives and its food requires action[29][30] In CSO calculations, the best fitness score is associated with the chicken and the worst health score is associated with the chicken coop. The rest of the qualities are given to a flock of chickens. The cycle for choosing the best hub is explained in the accompanying

Step1: Initialize the population of N chicken x and choose a 128-cycle key phrase set for ECC.

$$x_{i,j}^{t+1} = lb + Rand(ub - lb) \quad (7)$$

With lb and ub are lower bound and upper bound of the search space. This is done to ensure that subsequent placements are in a popular region.

Step2: To determine the fitness and start the best position N_{best} $t=1$

$$F = Min(Key_{space}) \quad (8)$$

The closest home furnishings among the roses were chosen using the irregular age subset technique, because the chick holding kit consists of a narrow set of key chains made from an elliptical ring. The primary way to use the subset generation technique is to reduce the focal space by controlling the rate of popularity.

Step3: Assess the reasonableness of the crowd of chickens and show the hierarchy in the group; Divide the chicken sword into many subgroups and evaluate the relationship.

$$x_{i,j}^{t+1} = x_{i,j}^t * S1 * Rand * (x_{i,j}^t - x_{i,j}^t) + S2 * Rand * t \quad (9)$$

$$(x_{i,j}^t - x_{i,j}^t) = t \quad (10)$$

Step4: Update the range of chickens, hens and chickens. Updates for roosters are done using the calculation below (11) and (12).

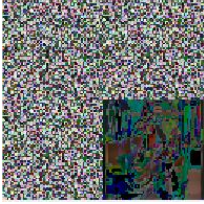
$$x_{i,j}^{t+1} = x_{i,j}^t * (1 + Rand(0, \sigma^2)) \quad (11)$$

$$\sigma^2 = \begin{cases} 1, & \text{if } f_i \leq f_k \\ \exp\left(\frac{f_k - f_i}{|f_i| + \varepsilon}\right) & \text{otherwise } k \in [1, N], k \neq i \end{cases} \quad (12)$$

4. Results and discussion

This section discusses the experimental findings about the proposed image encryption scheme. The image findings in this paper are based on five test images from the USC-SIPI image database[31]. The method of encrypting and decrypting two images is tabulated. Table 1 and 3 shows encryption and decryption of the original image. Table 2 and 4 shows the reconstruction process of decryption images. After decryption, the final output image is compared to the original image in order to determine their performance using quality parameters such as PSNR, MSE, and CC values. The PSNR value shows whether the resulting image's quality is improved or deteriorated. If the PSNR value is extremely high, the image's quality is excellent. 52.94 and 50.85 were the PSNR values obtained here. It is shown unequivocally that the suggested approach produces the original picture with the highest possible PSNR.

Table1: Results obtained for the proposed method

Input Image	Color band	Share creation	Combined Sharing	Encryption	Decryption
	R1				
	G1				

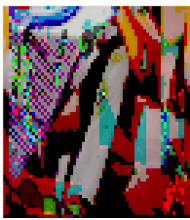
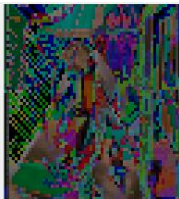
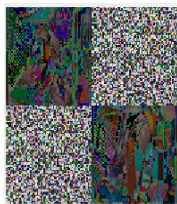
	B1				
	R2				
	G2				
	B2				

Table 2: Reconstruction images for the proposed method

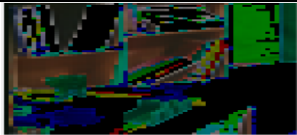
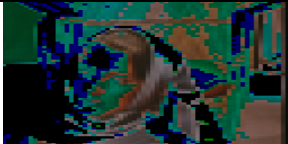
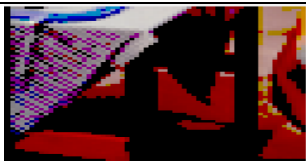
Input image	Reconstruction		Reconstructed image
	Upper left Quadrant	Upper right Quadrant	
			
			
	Lower left Quadrant1	Lower right Quadrant1	
			
			

Table 3:

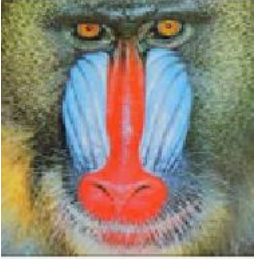
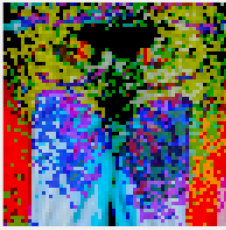
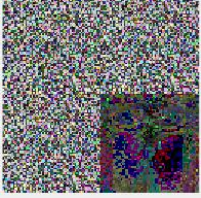
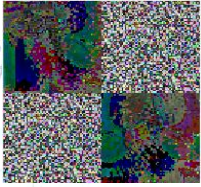
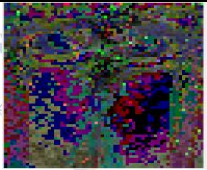
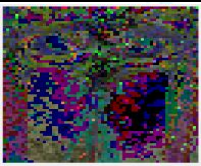
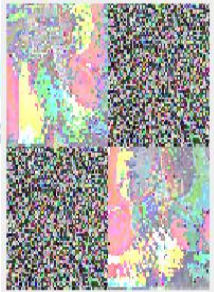
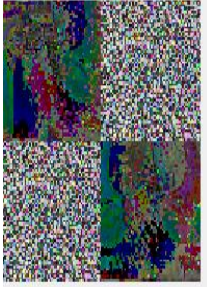
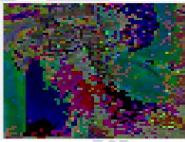
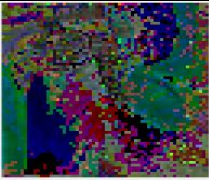
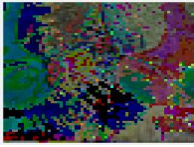
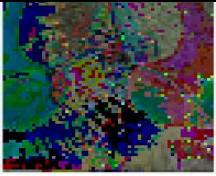
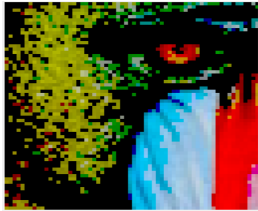
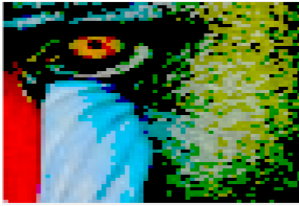
Input Image	Color band	Share creation	Combined Sharing	Encryption	Decryption
	R1				
	G1				
	B1				
	R2				
	G2				
	B2				

Table 4: Reconstruction results for baboon image

Input image	Reconstruction		Reconstructed image
	Upper left Quadrant	Upper right Quadrant	
			

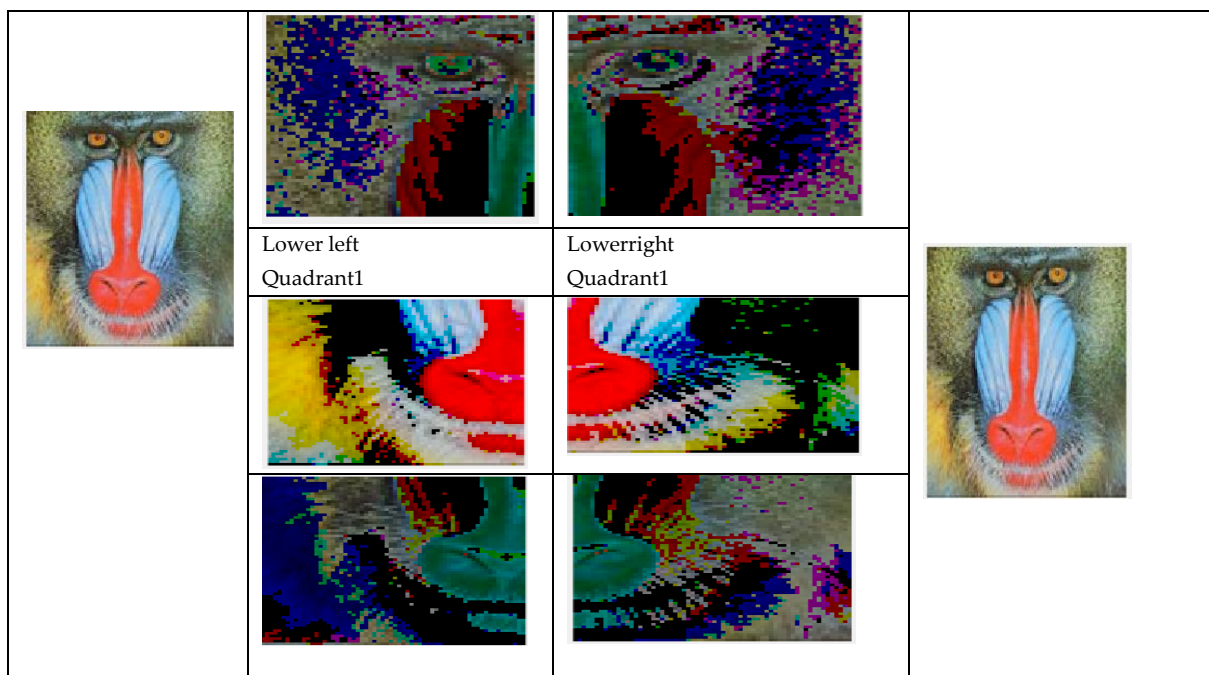


Table 5: Comparison of results obtained with the proposed method and ECC method

Input	Method	PSNR	MSE	CC
	ECC	45.94	1.67	0.9
	CSO	52.94	0.33	1
	ECC	46.07	1.62	0.9
	CSO	52.72	0.35	1
	ECC	46.23	1.56	0.9
	CSO	52.85	0.34	1
	ECC	46.61	1.43	0.9
	CSO	52.48	0.37	1
	ECC	46.35	1.52	0.9
	CSO	52.04	0.41	1

Table 5 compares the proposed ECC with CSO method to the ECC technique using several critical quality parameters such as PSNR, MSE, and CC values for images Barbara, Baboon, train, fingerprint and eye images. According to the table, the proposed method improved the image quality because its PSNR value is more than that of the ECC algorithm. The comparison study indicates that the suggested picture encryption

approach achieves an acceptable level of security. It clearly indicates that the proposed strategy outperforms the ECC approach.

CONCLUSION

The research presents an ECC-based picture encryption strategy that is optimized using CSO method. It is demonstrated unequivocally that the suggested method produces a higher-quality image with an average PSNR value of 52.94 between the original and final images. The mean square error is likewise minimized in all images, which means that almost all photos have a correlation coefficient of nearly 1. Histogram and correlation coefficient analyses make it abundantly evident that the encryption process remains unaltered and maintains the secret image's confidentiality. Comparative investigation demonstrates that the suggested technique outperforms ECC in terms of encryption quality and PSNR values. In the future, we will examine the suggested method's resilience to various forms of attacks such as salt and pepper, filtering, cropping, and blurring.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

- [1] B. Jyoshna and K. Subramanyam, "Time conserving secured cloud data storage solution based on keccak and elliptic curve

- cryptography," *Int. J. Adv. Res. Eng. Technol.*, vol. 10, no. 5, pp. 154–165, 2019, doi: 10.34218/IJARET.10.5.2019.016.
- [2] T. K. Goyal and V. Sahula, "Lightweight security algorithm for low power IoT devices," 2016 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2016, no. September, pp. 1725–1729, 2016, doi: 10.1109/ICACCI.2016.7732296.
 - [3] M. C. H. Kumar, S. Shahbaz, M. Varma, and T. Shri, "General survey on implementation of security in IOT," *Int. J. Mech. Eng. Technol.*, vol. 8, no. 12, pp. 529–535, 2017.
 - [4] D. R. Shashikumar, "Revisiting Security Aspects of Internet of Things for Self-Managed Devices," pp. 1652–1659, 2019.
 - [5] R. Shaik, N. K. Gudapati, N. K. Balijepalli, and H. R. Medida, "A Survey on Applications of Internet of Things," *Int. J. Civ. Eng. Technol.*, vol. 8, no. 12, pp. 558–571, 2017, doi: 10.1109/IS48319.2020.9200185.
 - [6] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," *Proc. 2017 Int. Conf. Eng. Technol. ICET 2017*, vol. 2018-January, pp. 1–7, 2018, doi: 10.1109/ICEngTechnol.2017.8308215.
 - [7] Z. Wang, Z. Ma, S. Luo, and H. Gao, "Enhanced Instant Message Security and Privacy Protection Scheme for Mobile Social Network Systems," *IEEE Access*, vol. 6, pp. 13706–13715, 2018, doi: 10.1109/ACCESS.2018.2813432.
 - [8] S. Kumar and R. K. Singh, "Secure authentication approach using Diffie-Hellman key exchange algorithm for WSN," *Int. J. Commun. Networks Distrib. Syst.*, vol. 17, no. 2, pp. 189–201, 2016, doi: 10.1504/IJCND.2016.079102.
 - [9] M. Arif, A. H. M. A. Habib, I. Rufat, and S. Azer, "Study and Implementation of Elliptic Curve Encryption Algorithm for Azerbaijan E-ID Card," 2015.
 - [10] A. Gopi and M. Kameswara Rao, "Survey of privacy and security issues in IoT," *Int. J. Eng. Technol.*, vol. 7, pp. 293–296, 2018, doi: 10.14419/ijet.v7i2.7.10600.
 - [11] P. Deshpande, S. Santhanalakshmi, P. Lakshmi, and A. Vishwa, "Experimental study of Diffie-Hellman key exchange algorithm on embedded devices," 2017 Int. Conf. Energy, Commun. Data Anal. Soft Comput. ICECDS 2017, pp. 2042–2047, 2018, doi: 10.1109/ICECDS.2017.8389808.
 - [12] A. Mullai and K. Mani, "Enhancing the security in RSA and elliptic curve cryptography based on addition chain using simplified Swarm Optimization and Particle Swarm Optimization for mobile devices," *Int. J. Inf. Technol.*, vol. 13, no. 2, pp. 551–564, 2021, doi: 10.1007/s41870-019-00413-8.
 - [13] A. Rawat and M. Deshmukh, "Tree and elliptic curve based efficient and secure group key agreement protocol," *J. Inf. Secur. Appl.*, vol. 55, p. 102599, 2020, doi: 10.1016/j.jisa.2020.102599.
 - [14] B. Bettoumi and R. Bouallegue, "Evaluation of Authentication Based Elliptic Curve Cryptography in Wireless Sensor Networks in IoT Context," 2018, pp. 1–5, doi: 10.23919/SOFTCOM.2018.8555745.
 - [15] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Processing*, vol. 155, pp. 391–402, 2019, doi: 10.1016/j.sigpro.2018.10.011.
 - [16] A. Joshi and A. K. Mohapatra, "A novel lightweight authentication protocol for body area networks based on elliptic-curve cryptography," *J. Inf. Optim. Sci.*, vol. 41, no. 7, pp. 1645–1672, 2020, doi: 10.1080/02522667.2020.1799511.
 - [17] P. Sethuraman, P. S. Tamizharasan, and K. Arputharaj, "Fuzzy Genetic Elliptic Curve Diffie Hellman Algorithm for Secured Communication in Networks," *Wirel. Pers. Commun.*, vol. 105, no. 3, pp. 993–1007, 2019, doi: 10.1007/s11277-019-06132-4.
 - [18] D. Dharminder and K. P. Chandran, "LWESM: learning with error based secure communication in mobile devices using fuzzy extractor," *J. Ambient Intell. Humaniz. Comput.*, vol. 11, no. 10, pp. 4089–4100, 2020, doi: 10.1007/s12652-019-01675-7.
 - [19] K. Sowjanya and M. Dasgupta, "A ciphertext-policy Attribute based encryption scheme for wireless body area networks based on ECC," *J. Inf. Secur. Appl.*, vol. 54, 2020, doi: 10.1016/j.jisa.2020.102559.
 - [20] V. Kumar, M. Ahmad, and A. Kumari, "A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS," *Telemat. Informatics*, vol. 38, no. September 2018, pp. 100–117, 2019, doi: 10.1016/j.tele.2018.09.001.
 - [21] L. D. Singh and K. M. Singh, "Image Encryption using Elliptic Curve Cryptography," *Procedia Comput. Sci.*, vol. 54, no. April, pp. 472–481, 2015, doi: 10.1016/j.procs.2015.06.054.
 - [22] K. Shankar and P. Eswaran, "Sharing a Secret Image with Encapsulated Shares in Visual Cryptography," *Procedia Comput. Sci.*, vol. 70, pp. 462–468, 2015, doi: 10.1016/j.procs.2015.10.080.
 - [23] A. M. Qadir and N. Varol, "A review paper on cryptography," 7th Int. Symp. Digit. Forensics Secur. ISDFS 2019, no. June, pp. 1–6, 2019, doi: 10.1109/ISDFS.2019.8757514.
 - [24] J. Wohllwend, "Elliptic Curve Cryptography: Pre and Post Quantum," pp. 1–17.
 - [25] A. K. Singh, "A Review of Elliptic Curve based Signcryption Schemes," *Int. J. Comput. Appl.*, vol. 102, no. 6, p. 8887, 2014.
 - [26] S. R., "Elliptic Curve Cryptography Based Security Protocol of MANET under Dynamic Cluster Head Selection Environment," *Int. J. Emerg. Trends Eng. Res.*, vol. 8, pp. 447–454, 2020, doi: 10.30534/ijeter/2020/32822020.
 - [27] R. Kaur and E. K. Singh, "Image Encryption Techniques: A Selected Review," *IOSR J. Comput. Eng.*, vol. 9, no. 6, pp. 80–83, 2013, doi: 10.9790/0661-0968083.
 - [28] B. Murali Krishna, H. Khan, and G. L. Madhumati, "Reconfigurable pseudo biotic key encryption mechanism for cryptography applications," *Int. J. Eng. Technol.*, vol. 7, no. 1.5 Special Issue 5, pp. 62–70, 2018, doi: 10.14419/ijet.v7i1.5.9124.
 - [29] A. Bouzidi, M. E. Riffi, and M. Barkatou, "Cat swarm optimization for solving the open shop scheduling problem," *J. Ind. Eng. Int.*, vol. 15, no. 2, pp. 367–378, 2019, doi: 10.1007/s40092-018-0297-z.
 - [30] A. M. Ahmed, T. A. Rashid, and S. A. M. Saeed, "Cat Swarm Optimization Algorithm - A Survey and Performance Evaluation Aram," *Comput. Intell. Neurosci.*, pp. 1–31.
 - [31] K. Shankar and P. Eswaran, "An Efficient Image Encryption Technique Based on Optimized Key Generation in ECC Using Genetic Algorithm," *Adv. Intell. Syst. Comput.*, vol. 394, pp. 1105–1111, 2016, doi: 10.1007/978-81-322-2656-7.