International Transactions on Electrical Engineering and Computer Science
Samat et.al., Vol: 4, No: 4, pp: 183-193, December 2025

Efficient ECC Image Encryption Technique using Whale Optimization

Samat Iderus[1], Nuramalina Bohari[1]

Abstract: IoT creates integrated communication scenarios for network elements and steps by bringing together the applied and widespread developments at the same time. This paper develops the studied the critical open challenges in reinforcing IoT security, which includes encryption technologies to provide security to transferred pictures among linked systems of both groups. The proposed method is built on a hybrid approach that employs encryption tactics as well as optimization approaches. The Whale Optimization approach was employed in this suggested image safety model encryption. The goal of using optimization procedures in the encryption developments is to choose the better favorable keys in encryption techniques, by using the proposed approach. The PSNR and MSE are used to assess the outcomes once they have been implemented and found that the recommended approach is better related to the remaining methods.

Keywords: Elliptic curve cryptography, Whale optimization, Image security, PSNR, MSE.

1. Introduction

Multicasting Internet Protocol (IP) is an excellent approach to deliver to many receivers from a single IP data system. The fast expansion of the Internet has boosted the demand for multicasting IP as an assembly announcement technology in submissions like the distribution of videos. However, there are several security issues [1] that may result in multicast IP liabilities and this is one of the factors driving the expansion of multicast IP-based data distribution organizations. Any server, for example, may join a multicast group by sending an IGMP message to its nearest router, making the operation tough.

History
Received: 03-07-2025; Revised: 28-08-2025;
Accepted: 10-09-2025

S. Iderus
samat.iderus@uts.edu.my

[1]Centre for Research of Innovation and Sustainable Development, University of Technology Sarawak, Sarawak - 96000, Malaysia

Using group keys for data encryption is one of the suggested techniques for preventing vulnerability [2-3]. Everyone in the group, including the sender, uses the same key, which is called the group key. Encryption of both the sender's and the recipient's communications relies on group keys. When handling group keys, it is important to adhere to security standards such as reverse secrecy [4] and call confidentiality [5-6]. This criterion is put in place to ensure that no one other than authorized team members may decipher the data. Unfortunately, encrypted communication is currently unavailable to those who have left the Multicast Group [7]. Upon joining the Multicast group, new members will not be able to see any messages that were sent before they did. In order to meet the requirements, group keys must be securely assigned to approved members and updated if there is a change in membership. This process is known as the lock or restart group. Calculations and communications overhead for rewriting after leaving a group are often higher than when joining a group. This is due to the fact that when a new member is added to a group, the members already part of the group may get the updated group key encrypted with the old key via multicast communication, while the new member can receive it encrypted with the private key through unicast

https://doi.org/10.62760/iteecs.4.4.2025.161

communication [8-10]. A variety of re-keying methods for secure multicast have been detailed up till now [11-12]. Departure group key distribution computational and communication cost reduction is a primary motivation for these techniques. Having said that, they've all had their share of problems. The majority of the approaches proposed in [8] center on how to provide group keys to members during joins. The group key is updated after a predetermined duration in references [13] and [14]. Thus, these methods do not provide true forward and backward secrecy. The multicast group is divided into several subgroups in the solutions given in [15]. Every subgroup has its own designated controller who is responsible for creating its own set of keys. The only subgroup that changes its local key upon joining or leaving is the one being discussed here. The difficulty of rekeying when a group member quits is one of the protocols' shortcomings. In consideration of this issue, this paper presents the following contributions. In order to encrypt data, the Elliptic Curve Cryptography (ECC) technique is used [16-17]. In this procedure, the private keys of all group members are selected using the WOA. This effective cryptographic method guarantees secure communication in a multicast group. The key server not only generates the private key but also its inverse value [18]. With the public keys of the group's controller and all members, the key server may create a shared key. As part of the joint process, the key server generates a new private key and its inverse value for the new member. After that, the updated group key is sent out to all members of the subgroup by multicast and, to new members, it is sent out through unicast. The key server does not generate a new group key but instead informs the remaining members of the subgroup of the inverse value of the deceased member. When one person leaves a group, the other members' group keys will be set to the opposite value of the leaving member. The computational cost of the rekeying operation will be reduced by following this technique [19].

The remaining paper is organized into various sections. Section 2 presents the literature survey about the recent works, Section 3 presents the proposed methodology, Section 4 talks about the results and conclusion in Section 5.

2. Related works

Secure group core management has been the focus of a number of earlier publications in this field. A mobile network comprises of several wirelessly communicating mobile devices. The complexity of security considerations is heightened by volatility. The topic of safe group key management for the ever-changing peer groups in mobile wireless networks is covered by Sukin et al. [20]. A major issue with secure group communication is people exchanging passwords. New team switching programs and efficient recording methods have been developed to accommodate the frequent changes in membership in network dynamics. Here we provide a way to set up the group key that is both flexible and able to handle dynamic group changes. The proposed project was a success in terms of independence of keys, validation of keys, forward or backward secrecy, and team secrecy. The proposed idea has the potential to greatly improve multicast security on mobile networks. A more effective central group centralized group key distribution (CGKD) that may reduce the cost of calculating the master key server (KS) during key updates was proposed by Kumar et al. [21]. Adding, multiplying, subtracting, playing a game, and making a picture all need less computer power when a member joins. In addition, KS storage becomes less complicated with the proposed technique. An expanding CGKD protocol based on dual policies has also been created to deal with significant changes in members. Results showed that the proposed method is superior based on KS overload and computational results from group members. A paradigm for effectively managing and deploying teams across various web technologies and ad hoc networks was laid forth by Veltri et al. [22]. Reducing network traffic and overheads generated by changes in team members due to user engagement or arrangement was the motivation for creating the recommended approach. Secure online data storage and encrypted communications in vehicle networks are only two of many potential applications for recommended mapping scenarios. In the proposed approach, a focal point is used. Clarity in communication between the KDC and the team member is only required in cases when several negative events have occurred. Consequently, the proposed method surpasses state-of-the-art content generation algorithms. The way confidentiality and authenticity are provided at the group level has been enhanced. Racking rises to new heights in an energetic team setting. This highlights the need of developing a solid team ethics agreement. A new method for identifying a significant group agreement using team members' official vectors was developed by Muhammad Bilal and Shin-Gak Kang [23]. There is no need for team synchronization to unlock or update keys in the proposed project, despite its division. In addition, the system utilizes the latest multicast keys to ensure that machine connections in subgroups are effectively secure. When it comes to compatibility and communication, the suggested protocols work like a charm. The two practical and provably safe techniques suggested by Yi-Ruei Chen and Wen-Guey Tzeng are KeyDer-GKM and ReEnc-GKM, respectively [24]. An individual may reduce the expense of finding the current group key for encryption using the ReEnc-GKM approach, which involves outsourcing protocol-N procedures. None of the proposed systems allow for joint attacks. Project success hinges on the trusted team manager's capacity to oversee the whole company and relinquish control. Because the structure, range, and dynamics of the network are unknown when the network is being built, the centralized method is not suited for big sensors and B2B networks. Since the proposed method requires just hash and XOR operations to execute, it outperformed earlier approaches. By re-entering user groups using a method for computing GCD based on the Euclidean algorithm, Alvarez et al. [25] presented a new approach to secure multicasting. The suggested technique shows that IT needs are lower than previous comparable methods and takes the user tree structure into account, which decreases bandwidth requirements as a single set of algorithms. Teams under the supervision of a manager have developed a distributed protocol to improve the security of distributed data and user verification while simultaneously reducing the number of incoming messages sent by a centralized technique. The presented methods have produced better results in regard to data breaches and IT requirements. S. Jabean Begum and T. Purushothaman devised a method for group communication [26]. A new decentralized multicast key management system that offers stability, scalability, and cost-effectiveness is introduced as the Cluster Optimal Cluster Hierarchical Tree (OCHT). The new decentralized OCHT-based solutions beat a number of more conventional systems in several metrics, including memory use, packet transfer speed, performance, power consumption, and end-to-end latency. The suggested strategy was perfect for moving the cluster head in the near future, therefore the reorganization time was much less than with conventional approaches. The importance of a robust verification scheme in protecting online communications has been investigated by Kumari et al. (2018) [27]. With the suggested ECC technique, attacks that impersonate clients or servers would fail. Their approach also does away with shared authentication and client confidentiality. There have been many proposals for picture encryption processes that aim to guarantee data secrecy. These limitations need to be considered by the suggested method. According to Shaheen et al. [28], traditional cryptosystems can't connect to the WSN since most of the methods aren't suitable for sophisticated pictures because of how they're structured and estimated.

3. Proposed method

In order to transmit an initial, secret picture from one party to another, the proposed image encryption technology is used. A distinct RGB matrix is created by extracting the pixel values of the source image's RGB pixels. Afterward, the picture is partitioned into blocks before starting the encryption process [8][29]. The individual matrices of each block are encrypted using the ECC method. Then, the new pixel value is used to replace the old one in every block. You may get the mangled picture while keeping the original one hidden by using this technique. The encrypted picture is decoded by using the reverse encryption method when the encryption process is finished [30]. Optimization of the private key generation technique was carried over into the decryption process via the WOA algorithm. The output of the picture is used as a health metric to determine the Peak Signal to Noise Ratio (PSNR) value after the optimized key generation phase is finished. Upon discovery of the maximum PSNR value, it is used as the optimal key value and state of the private key. Using the PSNR, MSE, and Correlation Coefficient (CC), we compare the original and decrypted images to determine the level of accuracy. This method ensures the secure transfer of the original picture while protecting the privacy of the original data.

3.1. Elliptical Curve Cryptography (ECC)

When it comes to asymmetric key cryptography, ECC is one method of using public key cryptography [31-33]. This method determines the upper bound by using a constant starting point and the prime number function; the encryption then follows: Equation (1) shows the fundamental ECC equation.

$$y^2 = x^3 + ax + b \tag{1}$$

In equation (1), *a* and *b* are the integers. The intensity of encryption depends on the key created in every cryptographic operation. There are two options for key generation in the proposed approach. At the receiving end, a public key is generated to encrypt the message, and at the sending end, a private key is generated to decode the original picture. If "*P*" is at any point on the curve, choose a private key, an integer between *"1 and n-1"*, and store it as "*H*", then produce the public key, "*Q*", according to (2).

$$Q = H \times P \tag{2}$$

3.1.1 Encryption method

Part of the process involves encrypting the input picture by dividing each color band into blocks. The suggested encryption technique encrypts these four blocks [34]. $F(i, j)$ represents the count of the total blocks. The number of rows and columns are mentioned with *i* and *j*. The pixels $P_x(i, j)$ and $P_y(i+1, j)$ the point is obtained in (3) and (4)

$$C_1 = H \times P_e \tag{3}$$

$$C_2 = (P_x, P_y) + C_1 \tag{4}$$

3.1.2 Decryption method

During the process of the decryption, the private key (*H*) is recommended for decrypting the information and the point C_3 of equation (5) is recommended for decrypting the pixel points

$$C_3 = H \times C_1 \tag{5}$$

$$C_{ij} = C_2 - C_3 \tag{6}$$

C_{ij} indicates the final outcome. During this process, the WOA is used [35].

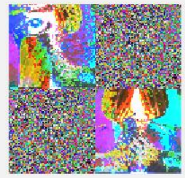
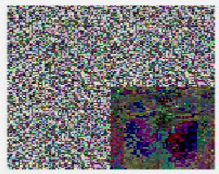
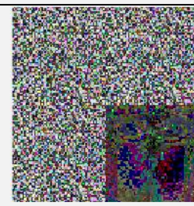
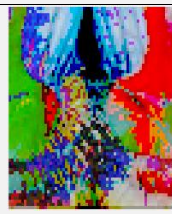
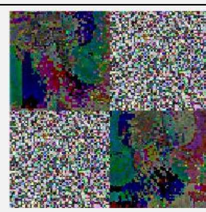
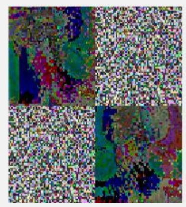
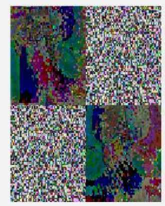
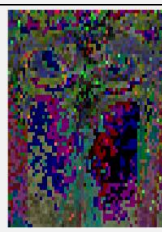
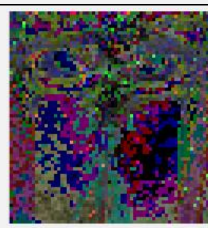
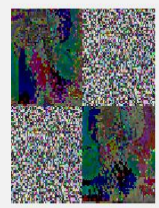
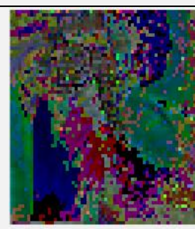
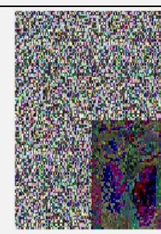
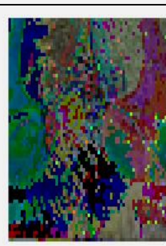
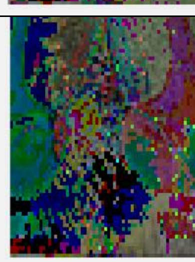
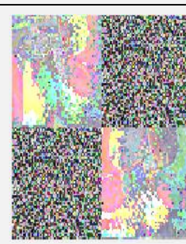
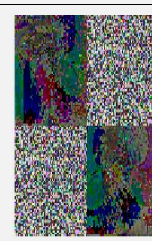
3.2 Whale Optimization Algorithm (WOA)

In 2024, Laith et.al created a heuristic approach called the whale optimization algorithm (WOA) [36] that accounts for biological processes. WOA is an optimization algorithm that mimics the specific humpback hunting approach. The exceptional worldwide search capability of WOA is a result of its unique optimization process. When choosing a bespoke key, it is best to use ECC that is based on the WOA [37]. The WOA takes its design cues from bubble-net predation, a hunting strategy used by humpback whales. The humpback whale can sense its surroundings and determine how far away its prey is. The humpback whale has been seen to spit up bubbles of varying sizes as it spirals up to a depth of around 15 meters. A network of cylindrical or tubular bubbles formed when the first and final spit bubbles reached the surface at the same time. Its favorite hunting technique is a huge web of spider knots that encircles its target and pulls it in toward its center. So, the almost vertical humpback whales swim into the bubble circle, open their jaws, and swallow the fish on the line. As mentioned earlier, there are three distinct phases to a humpback whale's hunting process: encircling prey, the spiral bubble-net feeding technique, and searching for prey [38].

3.2.1 Bubble-net attacking strategy

Humpback whales dovetail their attacks in a decreasing circle when they pinpoint the exact position of their victim. Since WOA couldn't determine the ideal answer when starting the optimization issue, it presumed that the prey or anything close by was the best contender at the moment. As a result, the other search agents compete to outdo the top search agent.

Table. 1: Encryption and decryption process with WOA for barbara image

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

The following equations are used to simulate the technique of encircling the prey

$$D = C.B - x^t$$

$$x^{t+1} = B - A.D$$

$$A = 2a.r - a$$

$$C = 2.r$$

The distance between the best search agent B at iteration t and the current search agent x^t is denoted by D. Keep in mind that if a better search agent becomes available, the best search agent gets changed throughout iterations. Since a declines from 2 to 0, where an is a randomly assigned value between a and a, the search agent's new position may be updated anywhere between its present location and the location of the best search agent. C stands for constant. A spiral-shaped journey may be modelled using these equations:

$$x^{t+1} = D'.e^{bl}.\cos(2\pi l) + B$$

$$D' = |B - x^t|$$

The value of the absolute distance between the current search agent and the best search agent at a particular iteration is represented by D'.

Table. 2: Encryption and decryption process with WOA for Lenna image

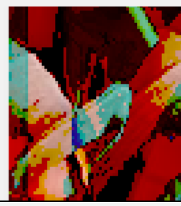
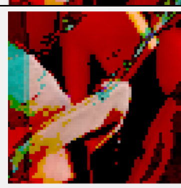
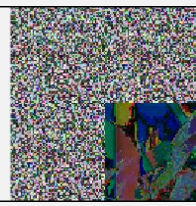
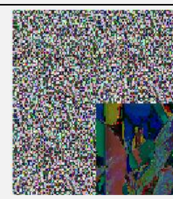
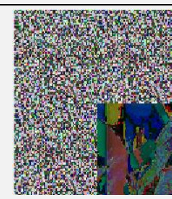
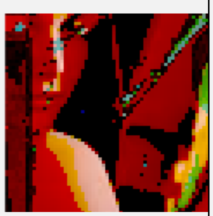
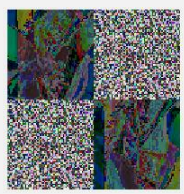
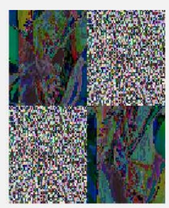
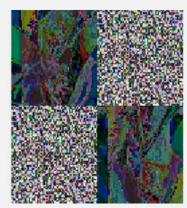
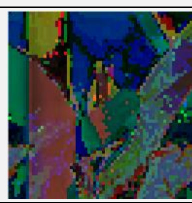
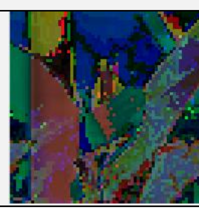
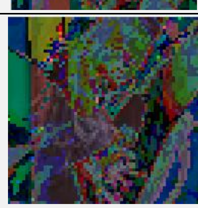
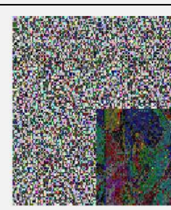
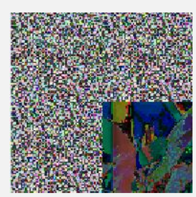
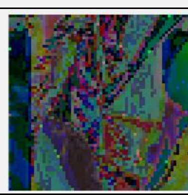
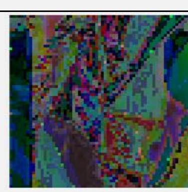
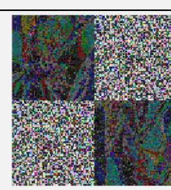
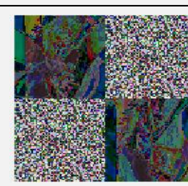
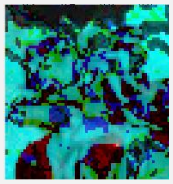
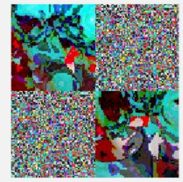
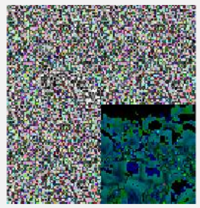
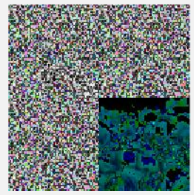
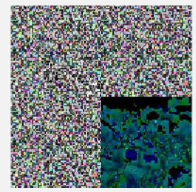
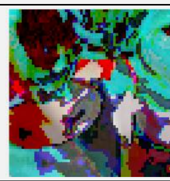
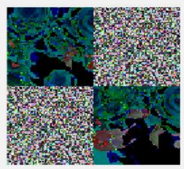
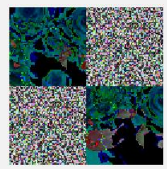
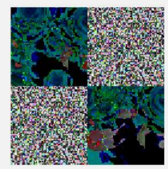
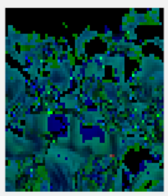
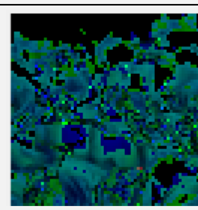
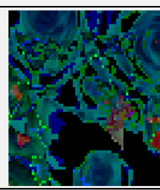
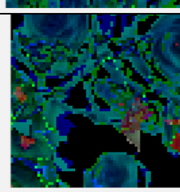
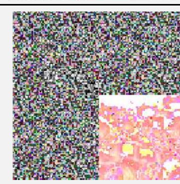
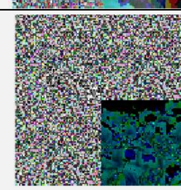
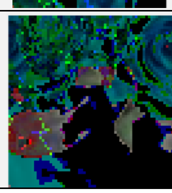
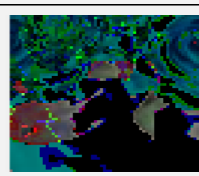
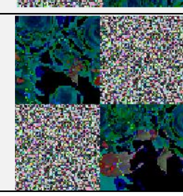
Input Image	Color band	Share creation	Combined Sharing	Encryption	Decryption	Re-Image
	R1					
	G1					
	B1					
	R2					
	G2					
	B2					

Table. 3: Encryption and decryption process with WOA for flower image

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

The shape of the logarithmic spiral is defined by the constant B. It may take on any value between -1 and 1. In the same way as humpback whales swim in a spiral pattern and a declining circle, WOA uses both behaviors equally.

$$x^{t+1} = \begin{cases} B - A.D & p < 0.5 \\ D'.e^{bl}.\cos(2\pi l) + B & p \leq 0.5 \end{cases}$$

3.2.2 Searching for the prey

Utilizing A with arbitrary values greater than 1 or less than 1 mimics the humpback whales' aimless pursuit of food. While a random search agent may be used for exploration, the bubble-net approach demonstrates how to utilize the optimum search agent for exploitation. Hunting for prey may be expressed mathematically as,

$$D = C.x_{rand} - x^t$$

$$x^{t+1} = x_{rand} - A.D$$

Where x_{rand} is a randomly picked search agent from the population. The pseudocode for WOA is shown in Fig. 1.

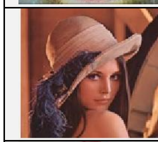
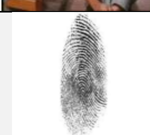
```
Whale Optimization Algorithm
Initialize a population of n random whales or search agents x_i(i = 1,2,...,n)
Evaluate each search agent
B = the best search agent
While (t < max _iter )
  for each search agent in the population
    Update WOA parameters (a, A, C, L, and p)
    if (p < 0.5 )
      if ( |A| < L)
        Update the current search agent by x^{t+1}=B − A.D
      else if ( |A| ≥ L )
        Select a random search agent (x_rand)
        Update the current search agent by x^{t+1} = x_rand − A.D
      end if
    else if ( p ≥ 0.5 )
      Update the current search agent by x^{t+1} = D'.e^{bl}.cos(2πl) + B
    end if
  end for
  Evaluate the search agent x^{t+1}
  Update B if there is a better solution in the population
  t = t + 1
end while
return B
```

Fig. 1: Whale optimization pseudocode

4. Results and Discussion

The proposed ECC-WAO-based image security procedure was developed in MATLAB 2018 using an Intel Core i5 CPU and 8 GB RAM configuration. The suggested model's results are compared to those of previous studies and generic optimization approaches in this article. This analysis model takes into account several standard images, including Lena, baboon, home, Barbara images and utilizes performance metrics such as PSNR, MSE, and CC. The suggested ECC-WOA based offer made encryption architecture is demonstrated in Tables. 1, 2 and 3. In hidden image, an RGB band was formed and each band included two scrambled and decoded offers. Security examinations include histogram analysis, correlation analysis, and entropy analysis [30]. This inquiry includes the highest severe PSNR value of 53.42 dB in unscrambled images, which corresponds to previous image exhibits. At any point, the correlation value is low, indicating that the encryption technique achieved a high degree of randomness between neighboring pixels in the scrambled image in CC. The data indicate that the image is more efficiently executed in terms of time since it is less fragmented. However, the PSNR suggested that a more original figure in primate image two-some to a greater number of squares, which results in an increase in the length of a number of chains, so achieving elite insecurity.

Table. 4: Comparison of the results for various images and algorithms

Input	Method	PSNR	MSE	CC
	ECC	46.541	1.53	0.9
	WOA	53.02	0.25	1
	ECC	43.2	1.67	0.9
	WOA	53.24	0.34	1
	ECC	46.96	1.4	0.9
	WOA	54.29	0.33	1
	ECC	45.07	1.61	0.9
	WOA	53.94	0.34	1
	ECC	45.23	1.58	0.9
	WOA	51.5	0.40	1
	ECC	47.61	1.43	0.9
	WOA	51.33	0.34	1
	ECC	45.34	1.59	0.9
	WOA	53.15	0.43	1

For the photos of Baboons, Lenas, flowers, boats, Barbara, fingerprints, and eyes, Table. 4 compares the ECC approach with the proposed ECC with WOA method based on CC values, PSNR, and MSE, among other important quality metrics. The table shows that the suggested technique outperformed the ECC algorithm in terms of picture quality due to its higher PSNR value. The proposed method of picture encryption delivers a satisfactory degree of security, according to the comparative analysis. Results show that compared to the ECC method, the suggested technique is much superior.

5. Conclusion

This study details an ECC-based picture encryption approach that makes use of the WOA optimization technique. An average PSNR value of

54.02 between the original and finished photos shows that the proposed technique delivers a higher-quality image. Similarly, every single picture has a correlation coefficient close to 1 when the mean square error is reduced. The analysis of histograms and correlation coefficients clearly shows that the encryption procedure is unaffected and protects the secret image's secrecy [39-40]. Based on the results of the comparison, the proposed method provides better encryption and higher PSNR values than ECC. We will test the proposed method's robustness against salt and pepper, filtering, cropping, and blurring assaults in the next steps.

Conflict of Interest

The authors declared "No conflict of Interest"

References

[1] Y.Yang et al ., "A Survey on security and privacy issues in IoT", *IEEE Internet of Things Journal,* Vol. 4, No. 5, pp. 1250-1258, 2017. https://doi.org/10.1109/JIOT.2017.2694844

[2] K. Gupta, S. Silakari, R. Gupta, and S. A. Khan, "An ethical way for image encryption using ECC", *2009 First International Conference on Computational Intelligence and Communication Systems and Networks,* pp. 342-345, 2009. https://doi.org/10.1109/CICSYN.2009.33

[3] L. D. Singh and K. M. Singh, "Image Encryption using Elliptic Curve Cryptography", *Procedia Computer Science*, Vol. 54, pp. 472–481, 2015. https://doi.org/10.1016/j.procs.2015.06.054

[4] K. Sowjanya and M. Dasgupta, "A ciphertext-policy Attribute based encryption scheme for wireless body area networks based on ECC", *Journal of Information Security Applications*, Vol. 54, art. no. 102559, 2020. https://doi.org/10.1016/j.jisa.2020.102559

[5] D. R. Shashikumar, "Revisiting Security Aspects of Internet of Things for Self-Managed Devices", *International Research Journal of Engineering and Technology*, Vol. 6, No. 10, pp. 1652–1659, 2019.

[6] U. Vijay Nikhil, Z. Stamenkovic, and S. P. Raja "A study of elliptic curve cryptography and its applications", *International Journal of Image and Graphics*, Vol. 25, No. 06, art. no. 2550062, 2025. https://doi.org/10.1142/S0219467825500627

[7] C. Pradeep, M. Rao, and B. Vikas, "Quantum Cryptography Protocols for Internet of Everything: General View", *Intelligent System Design*, pp. 211–218, 2020. https://doi.org/10.1007/978-981-15-5400-1_21

[8] K. Shankar and P. Eswaran, "RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique," *Journal of Circuits, Systems and Computers*, Vol. 25, No. 11, pp. 1–23, 2016. https://doi.org/10.1142/S0218126616501383

[9] R. Kaur and E. K. Singh, "Image Encryption Techniques: A Selected Review", *IOSR Journal of Computer Engineering,* Vol. 9, No. 6, pp. 80–83, 2013. https://doi.org/10.9790/0661-0968083

[10] R. Srilakshmi, "Dual Server based Security Protocol in MANET using Elliptic Curve Cryptography: A Cluster Head Selection Scenario", *International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 8, No. 4, pp. 1621–1629, 2019. https://doi.org/10.30534/ijatcse/2019/87842019

[11] K. Shah, A. Bhadauria, P. Thakkar, J. Shah and H. Kaur, "Advancements in Elliptic Curve Cryptography: A Review of Theory and Applications", *2024 Parul International Conference on Engineering and Technology (PICET)*, Vadodara, India, pp. 1-6, 2024. https://doi.org/10.1109/PICET60765.2024.10716041

[12] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve", *Signal Processing*, Vol. 155, pp. 391-402, 2019. https://doi.org/10.1016/j.sigpro.2018.10.011

[13] D. H. Je, J. S. Lee, Y. Park, and S. W. Seo, "Computation and storage efficient key tree management protocol for secure multicast communications", *Computer Communications,* Vol. 33, No. 2, pp. 136–148, 2010. https://doi.org/10.1016/j.comcom.2009.08.007

[14] N. Kettaf, H. Abouaissa, and P. Lorenz, "An efficient heterogeneous key management approach for secure multicast communications in ad hoc networks", *Telecommunication Systems,* Vol. 37, pp. 29–36, 2008. https://doi.org/10.1007/s11235-008-9074-4

[15] S. Toughi, M. H. Fathi, and Y. A. Sekhavat, "An

Image Encryption Scheme Based on Elliptic Curve Pseudo Random and Advanced Encryption System", *Signal Processing*, Vol. 141, pp. 217-227, 2017. https://doi.org/10.1016/j.sigpro.2017.06.010

[16] X. Zhang, K. Chen, J. Ding, Y. Yang, W. Zhang and N. Yu, "Provably Secure Public-Key Steganography Based on Elliptic Curve Cryptography," *IEEE Transactions on Information Forensics and Security*, Vol. 19, pp. 3148-3163, 2024. https://doi.org/10.1109/TIFS.2024.3361219

[17] A. Joshi and A. K. Mohapatra, "A novel lightweight authentication protocol for body area networks based on elliptic-curve cryptography", *Journal of Information and Optimization Sciences*, Vol. 41, No. 7, pp. 1645–1672, 2020. https://doi.org/10.1080/02522667.2020.1799511

[18] K. Sanjay, and D. Sharma "A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm", *Artificial Intelligence Review*, Vol. 57, No. 4, art. no. 87, 2024. https://doi.org/10.1007/s10462-024-10719-0

[19] B. Arpita, D. S. Laiphrakpam, A. Agrawal, and R. Patgiri "Secret image encryption based on chaotic system and elliptic curve cryptography", *Digital Signal Processing*, Vol. 129, art. no. 103639, 2022. https://doi.org/10.1016/j.dsp.2022.103639

[20] S. Kang, C. Ji, and M. Hong, "Secure collaborative key management for dynamic groups in mobile networks", *Journal of Applied Mathematics*, Vol. 2014, No. 1, art.no. 601625, pp. 1-10, 2014. https://doi.org/10.1155/2014/601625

[21] V. Kumar, R. Kumar, and S. K. Pandey, "A computationally efficient centralized group key distribution protocol for secure multicast communications based upon RSA public key cryptosystem", *Journal of King Saud University-Computer and Information Sciences*, Vol. 32, No. 9, pp.1081–1094, 2020. https://doi.org/10.1016/j.jksuci.2017.12.014

[22] L. Veltri, S. Cirani, S. Busanelli, and G. Ferrari, "A novel batch-based group key management protocol applied to the Internet of Things", *Ad Hoc Networks*, Vol. 11, No. 8, pp. 2724–2737, 2013. https://doi.org/10.1016/j.adhoc.2013.05.009

[23] M. Bilal and S. G. Kang, "A secure key agreement protocol for dynamic group", *Cluster Computing*, Vol. 20, pp. 2779–2792, 2017. https://doi.org/10.1007/s10586-017-0853-0

[24] Y. R. Chen and W. G. Tzeng, "Group key management with efficient rekey mechanism: A Semi-Stateful approach for out-of-Synchronized members", *Computer Communications*, Vol. 98, pp. 31–42, 2017. https://doi.org/10.1016/j.comcom.2016.08.001

[25] J. A. Á.Bermejo, N. Antequera, and J. A. L.Ramos, "Hierarchical approaches for multicast based on Euclid's algorithm", *The Journal of Supercomputing*, Vol. 65, No. 3, pp. 1164–1178, 2013. https://doi.org/10.1007/s11227-013-0923-x

[26] S. J. Begum and T. Purusothaman, "Hierarchical Tree Structure Based Clustering Schemes for Secure Group Communication", *Mobile Networks and Applications*, Vol. 21, pp. 550–560, 2016. https://doi.org/10.1007/s11036-015-0649-5

[27] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and V. Gupta, "Design of a secure anonymity preserving authentication scheme for session initiation protocol using elliptic curve cryptography", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 9, pp. 643–653, 2018. https://doi.org/10.1007/s12652-017-0460-1

[28] A. M. Shaheen, T. R. Sheltami, T. M. Al-Kharoubi, and E. Shakshuki, "Digital image encryption techniques for wireless sensor networks using image transformation methods: DCT and DWT", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 10, pp. 4733–4750, 2019. https://doi.org/10.1007/s12652-018-0850-z

[29] M. Kumar, D. C. Mishra, and R. K. Sharma, "A first approach on an RGB image encryption", *Optics and Lasers in Engineering*, Vol. 52, pp. 27–34, 2014. https://doi.org/10.1016/j.optlaseng.2013.07.015

[30] K. Shankar and P. Eswaran, "An Efficient Image Encryption Technique Based on Optimized Key Generation in ECC Using Genetic Algorithm", *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, Vol. 394, pp. 705 - 714, 2016. https://doi.org/10.1007/978-81-322-2656-7_64

[31] K. Shankar and P. Eswaran, "ECC based image encryption scheme with aid of optimization technique using differential evolution algorithm", *International Journal of Applied Engineering Research*, Vol. 10, No. 55, pp. 1841–1845, 2015.

[32] U. Shamsher, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey", *Computer Science Review*, Vol. 47, art. no. 100530, 2023. https://doi.org/10.1016/j.cosrev.2022.100530

[33] A. A. Khaliq, A. Anjum, A. B. Ajmal, J. L. Webber, A. Mehbodniya and S. Khan "A Secure and Privacy Preserved Parking Recommender System Using Elliptic Curve Cryptography and Local Differential Privacy", *IEEE Access*, Vol. 10, pp. 56410-56426, 2022. https://doi.org/10.1109/ACCESS.2022.3175829

[34] K. Shankar, M. Elhoseny, E. Perumal, M. Ilayaraja, and K. Sathesh Kumar "An efficient image encryption scheme based on signcryption technique with adaptive elephant herding optimization", *Cybersecurity and Secure Information Systems,* pp. 31-42, 2019. https://doi.org/10.1007/978-3-030-16837-7-3

[35] R. Srilakshmi, J. Muthukuru "Elliptic Curve Cryptography-Based Security Protocol of MANET under Dynamic Cluster Head Selection Environment", *International Journal of Emerging Trends in Engineering Research*, Vol. 8, No. 2, pp. 447–454, 2020. https://doi.org/10.30534/ijeter/2020/32822020

[36] A. Laith, R. A. Abualigah, A. M. Ikotun, R. A. Zitar, A. R. Alsoud, N. Khodadadi, A. E. Ezugwu, E. S. Hanandeh, and H. Jia "Whale optimization algorithm: analysis and full survey", *Metaheuristic Optimization Algorithms*, pp. 105-115. Morgan Kaufmann, 2024. https://doi.org/10.1016/B978-0-443-13925-3.00015-7

[37] M. A. Basset, D. E. Shahat, I. E.henawy, A. K. Sangaiah, and S. H. Ahmed, "A Novel Whale Optimization Algorithm for Cryptanalysis in Merkle-Hellman Cryptosystem", *Mobile Networks and Applications*, Vol. 23, No. 4, pp. 723–733, 2018. https://doi.org/10.1007/s11036-018-1005-3

[38] W. Z. Sun, J. S. Wang, and X. Wei, "An improved whale optimization algorithm based on different searching paths and perceptual disturbance", *Symmetry*, Vol. 10, No. 6, pp. 1–31, 2018. https://doi.org/10.3390/sym10060210

[39] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption", *Multidimensional Systems and Signal Processing,* Vol. 32, No. 1, pp. 281–301, 2021. https://doi.org/10.1007/s11045-020-00739-8

[40] 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", *International Journal of Information Technology*, Vol. 13, No. 2, pp. 551-564, 2021. https://doi.org/10.1007/s41870-019-00413-8

***