Whale Optimization Technique For ECC Image Encryption

V S Reddy Tripuram[1], Dr. Amit Singal[2], Dr. A. Ramaswami Reddy[3]

[1]Research Scholar, Computer Science and Engineering, Monad University, N.H.09, Delhi - Hapur Road, P.O Pilkhuwa, Distt. Hapur - 245304, (U.P), [2]Professor, Department of Computer Science and Engineering, Monad University, Hapur, (U.P.) India, [3]Professor, Computer Science and Engineering, Malla Reddy Engineering College, Maisammaguda, Secunderabad, India

Abstract: IoT creates integrated communication scenarios for network devices and stages by bringing together the practical and substantial worlds at the same time. The study's researchers identified and studied the critical open challenges in reinforcing IoT security, which includes encryption technologies to provide security to transferred images between linked networks of the two parties. The gadget is built on a hybrid algorithm 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 in encryption methods is to choose the most favorable keys in encryption algorithms, by using the proposed approach. The Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are used to assess the outcomes once they have been implemented and found that the suggested approach is better compared to the existing methods.

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

1. Introduction

Multicasting Internet Protocol (IP) is an excellent approach to deliver many receivers from a single IP datagram source. The fast expansion of broadband Internet has boosted demand for multicasting IP as a group communication technology in applications like real time video distribution. However, there are several security issues [1]that may result in multicast IP vulnerabilities and this is one of the factors driving the expansion of multicast IP-based information distribution organizations. Any server, for example, may join a multicast group by sending an IGMP message to its nearest router, making the operation tough. Using group keys

for data encryption is one of the suggested techniques for preventing vulnerability[2][3]. The group key is the key that the sender and all members of the group share. Group keys are important for encrypting communications sent by the sender as well as communications sent by group members. Security criteria such as call confidentiality and reverse secrecy[4]must be met while managing group keys[5][6]. The purpose behind this criterion is that only authorized team members will be able to appropriately decode the data. Recipients who have left the Multicast Group in the future will not be able to access secure communication at this time[7]. Any message made before joining the Multicast group cannot be seen in reverse for new members entering the group. To achieve the criteria, group keys must be updated with each change of members and securely given to only approve members. The lock or restart group is the name for this procedure. Rewriting after leaving a group often requires more calculations and communications overhead than entering a group. This is because, once a new member joins the group, the new group key may be sent to the existing group member through multicast communication, encrypted by the old group key, and to the new member through unicast communication, encrypted by the private key [8][9][10]. Until recently, a number of re-keying techniques for secure multicast have been described[11][12]. One of the main reasons for these methods is to reduce the computational and communicational cost of group key distribution upon departure. However, none of them has been without flaws. The suggested methods in [8] are mostly focused on group key distribution to members during joins. In [13] and [14], the group key is refreshed after a certain amount of time. As a result, these techniques do not provide forward and backward secrecy in the strict sense. In the solutions provided in [15], the multicast group is partitioned into many subgroups. A subgroup controller is assigned to each subgroup and is in charge of producing the keys for that subgroup. Only the subgroup in question changes its local key when it joins or leaves. One of these protocols' flaws is the difficulty of the rekeying process when a member leaves the group. The following contributions are offered in this study in light of this problem. The Elliptic Curve Cryptography (ECC) algorithm is used for encryption[16][17]. The Whale Optimization Algorithm (WOA) is used to pick the private key of each group member in this algorithm. In a multicast group, this efficient cryptography technique ensures safe communication. The key server also creates the inverse value of the private key along with the private key[18]. The key server generates a shared group key using the public keys of each member and group controller. The key server produces a new private key and its inverse value

for the new member during joint operation. The modified group key is then multicast broadcast to all sub-group members and unicast transmitted to new members. Instead of establishing a new group key, the key server notifies the surviving members of the sub-group of the inverse value of the departed member. The group keys of the remaining members in the group will be updated with the inverse value of the departing member. This procedure will lower the rekeying process's calculation overhead[19].

2. Related works

Several prior works in this area concentrate on research on secure group core management. A mobile network is made up of many mobile devices that communicate wirelessly with one another. Volatility adds to the complexity of security concerns. Sukin et al discuss secure group key management for mobile wireless networks' dynamic peer groups [20]. The sharing of passwords among group members is a critical problem for safe group communication. For frequent membership changes in network dynamics, new team switching programmes and efficient recording systems have been created. The method given here establishes the group key and allows for more flexibility in the event of dynamic group changes. In terms of team secrecy, forward or backward secrecy, key independence, and key validation, the suggested project produced successful outcomes. On mobile networks, the suggested concept may be leveraged to provide excellent multicast security. Kumar et al.[21] suggested a more efficient central group centralised group key distribution (CGKD) capable of lowering the cost of computing the master key server (KS) during key updates. When a member joins, the computing cost is reduced by adding a sum, multiplication, and a figure, removing, playing a game, and creating an image. Furthermore, the suggested solution reduces the complexity of KS storing. In addition, to cope with major changes in members, an extending CGKD protocol based on dual policies has been developed. Based on KS overload and group member calculations, the findings revealed that the suggested technique works better. Veltri et al.[22] established a paradigm for efficiently distributing and managing a team over a variety of ad hoc networks and online technologies. The suggested technique was created to decrease network traffic and overheads caused by changes in team members as a result of user interaction or arrangement. Recommended mapping scenarios may be utilised in a number of ways, including securely storing data on the Internet and communicating securely through automobile networks. A focus point is used in the suggested

method. Only when there are a large number of unfavourable occurrences does clear communication between the KDC and the team member become necessary. As a result, the suggested technique is able to outperform current content creation algorithms. The manner group-level privacy and integrity are offered has improved. In a dynamic team atmosphere, the racking process goes even farther. As a result, creating an effective team ethics pact is critical. Muhammad Bilal and Shin-Gak Kang [23]established a novel approach for determining a major group agreement based on the official vectors of team members. The proposed project is split, but it does not need team synchronization to unlock and update keys. Furthermore, the system employs the most up-to-date multicast keys for effectively safe machine connections in subgroups. In terms of communication and compatibility, the recommended protocols proven to be successful and efficient. KeyDer-GKM and ReEnc-GKM are two provably secure and practical schemes proposed by Yi-Ruei Chen and Wen-Guey Tzeng [24]. By outsourcing protocol-N operations, the ReEnc-GKM technique allows a member to lower the cost of determining the current group key for encryption. Joint assaults are not possible in any of the suggested systems. The success of the projects is dependent on the ability of the trusted team manager to manage the whole organization and hand over the keys. The centralized approach is not ideal for large sensors and B2B networks since network structure, range, and dynamics are unknown at the start of construction. It was more efficient than previous techniques since the suggested technique can only be implemented using hash and XOR operations. Alvarez et al. [25]proposed a novel technique to secure multicasting in which user groups are reentered using a technique for calculating GCD based on the Euclid algorithm. The proposed method considers user tree structure, which reduces bandwidth requirements as a single set of algorithms, and demonstrates that IT requirements are lower than other similar approaches. A distributed protocol has been created by teams with a team manager to assist minimize the quantity of incoming messages with a centralized method while also increasing the degree of security for dispersed information and user verification. In terms of data breaches and information technology needs, the approaches provided have yielded superior outcomes. An technique to group communication was presented by S. Jabean Begum and T. Purushothaman [26]. The Cluster Optimal Cluster Hierarchical Tree (OCHT) has been presented for a novel multicast key management system with decentralized design to provide stability, scalability, and cost-effectiveness. In terms of memory, packet transfer speed, performance, power consumption, and

end-to-end latency, the introduced decentralized OCHT-based designs outperformed several traditional systems. The time for reorganization was much shorter than with traditional methods because the proposed plan was ideal for shifting the cluster head in the short term. Kumari et al. (2018)[27] have explored how a strong verification conspire plays a critical role in safeguarding Internet communications. Client and server impersonation attacks are ineffective against the proposed ECC method. Similarly, their strategy foregoes client secrecy and shared authentication. Numerous image encryption procedures have been proposed to ensure the confidentiality of data. The proposed approach must take these constraints into account. However, the majority of the offered approaches are inapplicable to advanced images due to their structure and estimation; hence, conventional cryptosystems cannot be connected to the WSN by Shaheen et al [28].

3. Proposed method

The suggested image encryption system is used to transfer a secret initial image from the sender to the recipient. The RGB pixel values are extracted from the original image and a separate RGB matrix is generated using their pixel values. After that, the image is separated into blocks before the encryption phase begins[8][29]. The ECC technique is used to encrypt each block's separate matrix. Following that, each block's pixel value is substituted with the new pixel value. This method is used to obtain the scrambled image while still concealing the initial image. Following the completion of the encryption procedure, the encrypted image is decrypted using the reverse encryption technique[30]. The WOA algorithm's optimization strategy was extended to the private key generation method during the decryption process. The image's output is taken as a health value to be considered as the Peak Signal to Noise Ratio(PSNR) value after the optimized key generation phase is completed. When the highest PSNR value is found, it is used as the private key's optimum health and ideal key value. When the decryption step is complete, the final output image is compared to the original image to assess accuracy using the PSNR, MSE and Correlation Coefficient (CC). The original image is safely exchanged using this process, and the original information's confidentiality is retained.

3.1. Elliptical Curve Cryptography (ECC)

ECC is one some kind procedure for applying public key cryptography in asymmetric key cryptography[31][32][33]. Based on this procedure, the maximal limit is calculated with a fixed base point and the prime number function, and the encryption follows: 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. Firstly, public key is produced for encrypting the message from the receiver end and secondly, to create a private key to decrypt the original image 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 image is divided into the blocks. These four blocks are encrypted by the proposed encryption method[34]. The total count of the blocks is presented as $F(i, j)$. Where and *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)

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

$$C_2 = (P, P_{xy}) + C_1 \quad (4)$$

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 WOA technique, which gives the best optimized values compared to the existing ECC technique[35].

3.2 Whale Optimization Algorithm (WOA)

A heuristic method which takes biological processes into consideration has been developed by SeyedaliMirjalili and Andrew Lewis in 2016 and is referred to as the whale optimization algorithm (WOA)[36].WOA is a particular humpback hunting method optimization algorithm, which emulates the unique humpback hunting technique.The unique optimization methodology allows WOA to have a very good global search capacity. ECC based on the WOA is recommended for optimal custom key selection[37].The WOA is inspired by the humpback whale's distinctive hunting technique known as bubble-net predation. The humpback whale is capable of sensing the distance between himself and his prey and surrounding it. It is noticed that the humpback whale may ascend in a spiral pattern to a depth of around 15 meters and spit out a variety of different-sized bubbles. The last and initial spat out bubbles came to the surface simultaneously, forming a cylindrical or tubular bubble network. It prefers a massive spider-knotted web that closely surrounds the prey and draws it into the center of the net. Thus, the almost upright humpback whales open their mouths in the bubble circle and ingest the animals in the net. The humpback whale's hunting activity may be classified into three stages, as described above: surrounding prey, spiral bubble-net feeding maneuver, and looking for prey[38].

Bubble-net attacking strategy

Humpback whales are capable of determining their prey's location and attacking it in a diminishing circular fashion. Because the optimal solution is unknown at the outset of the optimization problem, WOA assumed that the current best candidate solution is the prey or something near to it. The other search agents attempt to improve their rankings in relation to the best search agent. To mimic the strategy of surrounding the prey, the following mathematical equations are used:

Where D is the distance between the current search agent and the best search agent at iteration. Note that, the best search agent is updated across iterations is there is a better search agent.A is a random value in the range [a, a], and a decreases from 2 to 0, indicating that the new location of the search agent can be updated anywhere between the current location and the location of the best search agent. C is a constant. The following equations are used to mimic the behavior of a spiral-shaped path:

Where denotes the absolute value of the distance between the current search agent and the best search agent at a given iteration. is a constant that specifies the logarithmic spiral's form. is a random number between . As humpback whales swim in a diminishing circle and in a spiral-shaped course, WOA employs both behaviors with an equal chance of 50%:

Searching for the prey

To simulate the humpback whales' random search for prey, A is employed with random values higher than 1 or less than -1.Exploration may be accomplished by the use of a random search agent, but exploitation may be accomplished with the use of the best search agent, as in the bubble-net technique. Mathematically, hunting for prey may be stated as:

Where is a randomly picked search agent from the population. The pseudocode for WOA is shown in Algorithm 1

Whale Optimization Algorithm

Initialize a population of n random whales or search agents $x_i(i = 1, 2, \ldots, n)$
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 ($|A| \geq L$)
        Select a random search agent (x_{rand})
        Update the current search agent by $x^{t+1} = x_{rand} - A.D$
      end if
    else if ($p \geq 0.5$)
      Update the current search agent by $x^{t+1} = D'.e^{bl}.\cos(2\pi l) + B$
    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

Results and Discussion

The proposed ECC-WAO-based image security procedure was built in MATLAB 2018 using an 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, barbaraimages 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 1

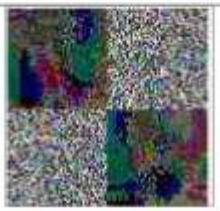
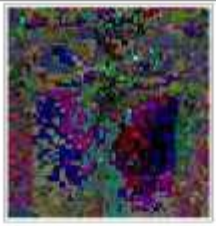
Input Image	Color band	Share creation	Combined Sharing	Encryption	Decryption	Reconstruct image
	R1					
	G1					
	B1					
	R2					
	G2					
	B2					

Table 2

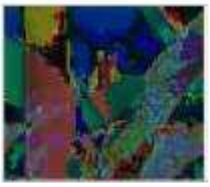
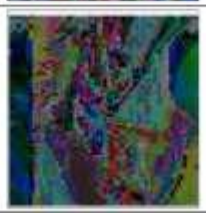
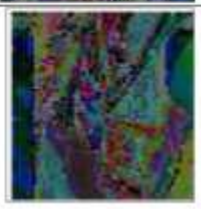
Input Image	Color band	Share creation	Combined Sharing	Encryption	Decryption	Reconstructed Output
	R1					
	G1					
	B1					
	R2					
	G2					
	B2					

Table 3

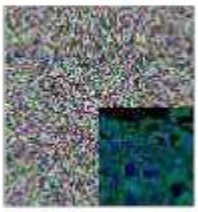
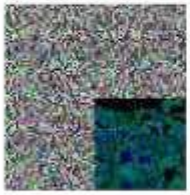
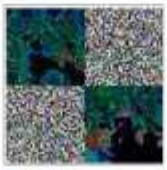
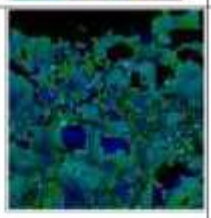
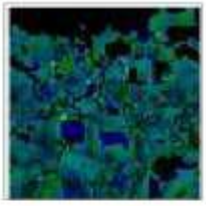
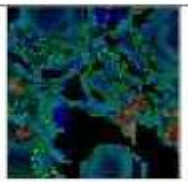
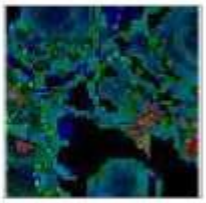
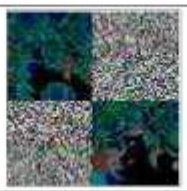
Input Image	Color band	Share creation	Combined Sharing	Encryption	Decryption	Reconstructed Output
	R1					
	G1					
	B1					
	R2					
	G2					
	B2					

Table 4

Input	Method	PSNR	MSE	CC
	ECC	46.54	1.54	0.9
	WOA	54.02	0.26	1
	ECC	45.94	1.67	0.9
	WOA	53.24	0.31	1
	ECC	46.96	1.36	0.9
	WOA	53.29	0.3	1
	ECC	46.07	1.62	0.9
	WOA	52.94	0.33	1
	ECC	46.23	1.56	0.9
	WOA	52.5	0.37	1
	ECC	46.61	1.43	0.9
	WOA	52.84	0.37	1
	ECC	46.35	1.52	0.9
	WOA	52.14	0.42	1

Table 4 compares the proposed ECC with WOA method to the ECC technique using several critical quality parameters such as PSNR, MSE, and CC values for images Baboon, Lena, flower, boat, Barbara, 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 image encryption approach achieves an acceptable level of security. It clearly indicates that the proposed strategy outperforms the ECC approach.

5. Conclusion

The research presents an ECC-based image encryption strategy that is optimized using WOA method. It is demonstrated unequivocally that the suggested method produces a higher-quality image with an average PSNR value of 54.02 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[39][40]. 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.

References

[1] 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.

[2] K. Gupta, S. Silakari, R. Gupta, and S. A. Khan, "An ethical way for image encryption using ECC," *2009 1st Int. Conf. Comput. Intell. Commun. Syst. Networks, CICSYN 2009*, pp. 342–345, 2009, doi: 10.1109/CICSYN.2009.33.

[3] 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.

[4] 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.

[5] D. R. Shashikumar, "Revisiting Security Aspects of Internet of Things for Self-Managed Devices," pp. 1652–1659, 2019.

[6] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maseleno, and N. Arunkumar, "Hybrid optimization with cryptography encryption for medical image security in Internet

of Things," *Neural Comput. Appl.*, vol. 32, no. 15, pp. 10979–10993, 2020, doi: 10.1007/s00521-018-3801-x.

[7] C. Pradeep, M. Rao, and B. Vikas, "Quantum Cryptography Protocols for Internet of Everything: General View," 2021, pp. 211–218.

[8] K. Shankar and P. Eswaran, "RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique," *J. Circuits, Syst. Comput.*, vol. 25, no. 11, pp. 1–23, 2016, doi: 10.1142/S0218126616501383.

[9] 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.

[10] S. R, "Dual Server based Security Protocol in MANET using Elliptic Curve Cryptography: A Cluster Head Selection Scenario," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 6, pp. 1621–1629, 2019, doi: 10.30534/ijatcse/2019/87842019.

[11] E. Babu, C. Raju, and M. Prasad, "Inspired pseudo biotic DNA based cryptographic mechanism against adaptive cryptographic attacks," vol. 18, pp. 291–303, 2016.

[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, doi: 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," *Comput. Commun.*, vol. 33, no. 2, pp. 136–148, 2010, doi: 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," *Telecommun. Syst.*, vol. 37, no. 1–3, pp. 29–36, 2008, doi: 10.1007/s11235-008-9074-4.

[15] T. Shahriyar, M. H. Fathi, and Y. A. Sekhavat, "An Image Encryption Scheme Based on Elliptic Curve Pseudo Random and Advanced Encryption System," *Signal Processing*, no. June, 2017, doi: 10.1016/j.sigpro.2017.06.010.

[16] V. S. Miller, "Use of Elliptic Curves in Cryptography," *Lect. Notes Comput. Sci.*

(including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 218 LNCS, pp. 417–426, 1986, doi: 10.1007/3-540-39799-X_31.

[17] 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.

[18] K. Vasundhara, Y. V S Sai Pragathi, and Y. Sai Krishna Vaideek, "A Comparative Study of RSA and ECC," *Int. J. Eng. Res. Appl. www.ijera.com*, vol. 8, no. 1, pp. 49–52, 2018, doi: 10.9790/9622-0801014952.

[19] 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.

[20] S. Kang, C. Ji, and M. Hong, "Secure collaborative key management for dynamic groups in mobile networks," *J. Appl. Math.*, vol. 2014, 2014, doi: 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," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 32, no. 9, pp. 1081–1094, 2020, doi: 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, doi: 10.1016/j.adhoc.2013.05.009.

[23] M. Bilal and S. G. Kang, "A secure key agreement protocol for dynamic group," *Cluster Comput.*, vol. 20, no. 3, pp. 2779–2792, 2017, doi: 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," *Comput. Commun.*, vol. 98, pp. 31–42, 2017, doi: 10.1016/j.comcom.2016.08.001.

[25] J. A. Álvarez-Bermejo, N. Antequera, and J. A. López-Ramos, "Hierarchical approaches for multicast based on Euclid's algorithm," *J. Supercomput.*, vol. 65, no. 3, pp. 1164–

1178, 2013, doi: 10.1007/s11227-013-0923-x.

[26] S. J. Begum and T. Purusothaman, “Hierarchical Tree Structure Based Clustering Schemes for Secure Group Communication,” *Mob. Networks Appl.*, vol. 21, no. 3, pp. 550–560, 2016, doi: 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,” *J. Ambient Intell. Humaniz. Comput.*, vol. 9, no. 3, pp. 643–653, 2018, doi: 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,” *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 12, pp. 4733–4750, 2019, doi: 10.1007/s12652-018-0850-z.

[29] M. Kumar, D. C. Mishra, and R. K. Sharma, “A first approach on an RGB image encryption,” *Opt. Lasers Eng.*, vol. 52, no. 1, pp. 27–34, 2014, doi: 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,” *Adv. Intell. Syst. Comput.*, vol. 394, pp. 1105–1111, 2016, doi: 10.1007/978-81-322-2656-7.

[31] K. Shankar and P. Eswaran, “ECC based image encryption scheme with aid of optimization technique using differential evolution algorithm,” *Int. J. Appl. Eng. Res.*, vol. 10, no. 55, pp. 1841–1845, 2015.

[32] K. Shankar, M. Elhoseny, R. S. Kumar, S. K. Lakshmanaprabu, and X. Yuan, “Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique,” *J. Ambient Intell. Humaniz. Comput.*, vol. 11, no. 5, pp. 1821–1833, 2020, doi: 10.1007/s12652-018-1161-0.

[33] V. K. Yadav, S. Singh, and G. Chandra, “Public Key Cryptosystem Technique Elliptic Curve Cryptography w ith Generator g for Image Encryption,” 2012.

[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*. Springer International Publishing, 2019.

[35] 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.

[36] C. Sivakumar and C. Nalini, "Efficient group key management using whale optimization algorithm based elliptic curve cryptography for dynamic multicast groups," *Int. J. Adv. Sci. Technol.*, vol. 29, no. 8 Special Issue, pp. 2415–2431, 2020.

[37] M. Abdel-Basset, D. El-Shahat, I. El-henawy, A. K. Sangaiah, and S. H. Ahmed, "A Novel Whale Optimization Algorithm for Cryptanalysis in Merkle-Hellman Cryptosystem," *Mob. Networks Appl.*, vol. 23, no. 4, pp. 723–733, 2018, doi: 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 (Basel).*, vol. 10, no. 6, pp. 1–31, 2018, doi: 10.3390/sym10060210.

[39] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimens. Syst. Signal Process.*, vol. 32, no. 1, pp. 281–301, 2021, doi: 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," *Int. J. Inf. Technol.*, vol. 13, no. 2, pp. 551–564, 2021, doi: 10.1007/s41870-019-00413-8.