



**International Journal of Multidisciplinary Engineering in Current Research**  
Volume 7, Issue 5, May 2022, <http://ijmec.com/>

## **ECC Image Encryption Scheme using Whale Optimization Technique**

**Tripuram Venkateswarlu Reddy<sup>1</sup>, A. Ramaswami Reddy<sup>2</sup>**

<sup>1</sup>Research Scholar, Computer Science Engineering, Arni University, Tanda, Himachal Pradesh <sup>2</sup>Professor, Computer Science Engineering, Malla Reddy Engineering College, Maisammaguda, Secunderabad, India

**Abstract:** IoT develops integrated communication possibilities for network devices and stages by bringing together the practical and substantial worlds at the same time. The study's authors uncovered and investigated the most pressing outstanding problems in bolstering IoT security, such as the need for encryption methods to safeguard photos being sent across connected networks. The algorithm used to construct the device is a hybrid, meaning that it makes use of both encryption and optimization strategies. This proposed picture security model encrypted using the Whale Optimization technique. Using optimization in encryption techniques allows one to choose optimal keys for use in encryption algorithms. Once the proposed technique has been applied, the results are evaluated using the Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) to determine whether or not the strategy was successful.

**Keywords:** Cryptography based on elliptic curves, optimization using whales, and protecting digital images.

### **1. Introduction**

Internet Protocol (IP) multicasting is a powerful method for sending IP datagrams to several recipients at once. Since the introduction of broadband Internet, multicasting IP has been more popular as a group communication tool

for uses such as real-time video delivery. However, the growth of multicast IP-based

information distribution organizations is complicated by a number of security concerns [1] that might leave such networks vulnerable. As an example, any server may join a multicast group by sending an IGMP message to the closest router, which makes the process more complicated. An approach recommended for avoiding exposure [2][3] is encrypting data using a group key. The

The sender's group key is a shared secret among all recipients in the group. Both the sender's and the receiver's communications may be encrypted using the group key. Group keys [5][6] must be managed in a way that satisfies security requirements such as confidentiality and reverse secrecy [4]. With this stipulation in place, only trusted team members will be able to correctly decipher the information. For the time being, those who have left the Multicast Group and want to continue receiving encrypted communications must join the group again [7]. New members of a Multicast group will not be able to see any messages sent before they joined in reverse. Group keys need to be kept up-to-date whenever members are added or removed, and sent securely to only authorized users, in order to meet the criterion. This operation is often referred to as a "lock" or "restart" group. It takes more time and effort to rewrite after leaving a group than it did to join the group first. Because the new group key may be sent to the current group member through multicast



## International Journal of Multidisciplinary Engineering in Current Research Volume 7, Issue 5, May 2022, <http://ijmec.com/>

---

communication using the old group key, and to the new group member via unicast communication using the private key, after the new group member has joined the group. [8][9][10]. Until recently, many re-keying methods for secure multicast have been described [11, 12]. These techniques are widely used to lessen the computational and telegraphic burden of distributing group keys before a trip. But there have been problems with each one. Group key distribution to members during joins is the primary emphasis of the approaches proposed in [8]. After some time has passed in [13] and [14], the group key is reset. Since this is the case, these methods cannot be considered "forward and backward secret" in the technical sense. The strategies presented in [15] divide the multicast group into several smaller groups. Each subgroup has a designated controller who generates the subgroup's keys. When a subgroup joins or quits, just that subgroup's local key changes. The rekeying procedure might be complicated if a member of the group quits, which is a weakness of these protocols. With this issue in mind, this research offers the following contributions. Encryption is performed using an Elliptic Curve Cryptography (ECC) algorithm [16][17]. Each individual's private key is selected using the Whale Optimization Algorithm (WOA). With this effective cryptography method, all conversations inside a multicast group may be taken into consideration to be secure. Along with the private key, the key server also generates the corresponding inverse value [18]. Using the public keys of all the members and the group controller, the key server creates a shared group key. During cooperative operation, the key server generates a new private key and its inverse for the participating node. Multicasting the updated group key follows.

to everyone in the subgroup through unicast transmission to new people joining the group. When a member of a subgroup dies, the key server does not generate a new group key but instead informs the other members of the subgroup of the inverse value of the deceased person's key. The leaving member's inverse value will be added to the group keys of the remaining members. The computational burden of the rekeying operation will be reduced thanks to this method [19].

Second, the works that are related

Secure group core management has been the focus of several earlier publications in this field. Many mobile devices are connected to one another wirelessly to form a mobile network. The uncertainty of the market increases the difficulty of addressing security issues. Group key management security for mobile wireless networks with changing peer groups is discussed by Sukin et al. [20]. A major threat to the security of group communication is the practice of participants exchanging passwords with one another. New team-switching programs and efficient recording systems have been developed to accommodate the frequent membership changes necessitated by the dynamic nature of networks. This approach to determining the group's key also provides greater leeway in the case of sudden shifts inside the group. The recommended project was effective in maintaining team confidentiality, forward or backward secrecy, key independence, and key validation. The proposed idea has the potential to be used in mobile networks to improve multicast security. A more effective central group centralised group key distribution (CGKD) was proposed by Kumar et al. [21], which may reduce the cost of calculating the master key server (KS) during key updates. Reduced computation time is achieved with the addition of a sum,



## International Journal of Multidisciplinary Engineering in Current Research Volume 7, Issue 5, May 2022, <http://ijmec.com/>

---

multiplication, and a figure, subtraction, a game, and an image when a new member joins. As an added bonus, the proposed technique simplifies KS archiving. In addition, a dual-policy based extended CGKD protocol has been created for dealing with large-scale membership shifts. The results of the KS overload and group member calculations show that the proposed method is superior. A paradigm for distributing and managing a team effectively over several ad hoc networks and digital tools was devised by Veltri et al.[22]. As a consequence of user input or arrangement, the proposed method was developed to lessen network traffic and associated overheads brought on by shifts in team members. Some potential applications of the suggested mapping scenarios include safe online data storage and encrypted in-car communication. The proposed strategy makes use of a central idea or concept. When there are several unfavorable events, only then does there have to be some kind of dialogue between the KDC and the team member. Since this is the case, the proposed method may provide better results than the best existing content generation algorithms. There has been a substantial improvement in the way confidentiality and security may be maintained in a group setting. The racking process advances much further in an energetic group setting. Therefore, it is crucial to establish a solid team ethics contract. By using the official vectors of team members, Muhammad Bilal and Shin-Gak Kang [23] developed a revolutionary method for establishing a significant group agreement. Although the planned project is in two parts, the teams do not have to be in sync in order to unlock and update keys. Moreover, the system makes use of modern multicast keys to securely join machines in smaller groups. The suggested protocols have been shown to be effective and efficient in terms of

communication and compatibility. Yi-Ruei Chen and Wen-Guey Tzeng [24] presented the KeyDer-GKM and the ReEnc-GKM, two systems that are both provably safe and practicable. The ReEnc-GKM method enables a user to reduce the cost of identifying the current group key for encryption by offloading protocol-N activities to another user. None of the proposed systems allow for coordinated attacks. One of the keys to project success is having a reliable team manager who can take charge and pass over the reins. Since network structure, range, and dynamics are unknown at the outset of creation, the centralized method is not optimal for big sensor and B2B networks. Due to the fact that the proposed method can only be achieved via the use of hash and XOR operations, it is more efficient than the methods that came before it. User groups are reentered using a GCD calculation method based on the Euclid algorithm, as suggested by Alvarez et al. [25]. The suggested technique takes into account the user tree structure, which decreases bandwidth needs as a collection of algorithms, and shows that the necessary IT resources are less than those for competing methods. Teams led by a manager have developed a decentralized protocol to improve the safety of distributed data and user authentication while decreasing the volume of incoming communications. The proposed methods have proven effective in addressing both data breaches and IT requirements. S. Jabeen Begum and T. Purushothaman [26] proposed a method for effective group conversation. An innovative decentralized multicast key management system, the Cluster Optimal Cluster Hierarchical Tree (OCHT), has been developed for achieving stability, scalability, and cost-effectiveness. The presented decentralized OCHT-based systems surpassed many others in memory, packet



**International Journal of Multidisciplinary Engineering in Current Research**  
**Volume 7, Issue 5, May 2022, <http://ijmec.com/>**

transfer speed, performance, power consumption, and end-to-end latency.

frameworks based on history. The suggested strategy was perfect for temporarily switching the cluster head, hence the reorganization time was significantly reduced compared to conventional approaches. Kumari et al. (2018)[27] have investigated the significance of a robust verification conspire in protecting online interactions. The suggested ECC approach is secure against both client and server impersonation threats. In a similar vein, their approach does not prioritize client anonymity or centralized authentication. Image encryption methods for protecting sensitive information have been presented several times. This is a requirement for the suggested method. Conventional cryptosystems cannot be linked to the WSN by Shaheen et al. [28] because to the inapplicability of the bulk of the available techniques to advanced pictures due to their structure and estimate.

## 2. The Approach Suggested

Using the proposed picture encryption technique, a sender may securely deliver a receiver a secret, initial image. It is possible to construct a distinct RGB matrix from the original picture by extracting the RGB pixel values. The next step, before encryption, is the partitioning of the picture into blocks[8][29]. Each block's matrix is encrypted independently using ECC. After that, the old pixel value in each block is replaced with the new one. The original picture is still hidden when this approach is utilized to get the scrambled image. Once the encryption process is complete, the encrypted picture is decrypted using the opposite encryption method[30]. To decrypt data, the WOA algorithm's optimization technique was used to the private key creation procedure. Once the optimal key generation process is complete, the image's output is used as a health metric,

specifically as the Peak Signal to Noise Ratio (PSNR) value. The best possible health and key value for the private key is determined by finding the PSNR value. After the decryption process is complete, the PSNR, MSE, and Correlation Coefficient are used to compare the final output picture to the original (CC). Using this method, the original picture may be sent without worrying about compromising the security of the data

Specifically, Cryptography Based on Elliptical Curves (ECC)

When it comes to asymmetric key cryptography, ECC is one method for implementing public key cryptography[31],[32],[33]. According to this method, the upper bound is determined using a constant value.

The encryption is based on the starting point and the prime number function: Standard ECC formula shown in equation (1)

$$y^2 = x^3 + ax + b$$

The numbers in this case are a and b. In every cryptographic process, the strength of encryption relies on the newly generated key. The suggested method offers two distinct ways to generate keys. The first step is to generate a public key that will be used to encrypt the message sent to the recipient, and the second is to generate a private key that will be used to decode the original picture upon its arrival. To produce the public key Q, if the private key H is an integer between 1 and n-1, and P is a point on the curve, we may perform the following: (2)

$$Q = H \cdot P$$

Method of Encryption, Version 3.1.1

The encryption process begins by segmenting the input picture into blocks based on each of the color channels. That's right, the suggested encryption method[34] encrypts all four of those chunks. F I j) represents the total number of blocks. If the rows and columns of are



## International Journal of Multidisciplinary Engineering in Current Research Volume 7, Issue 5, May 2022, <http://ijmec.com/>

numbered  $i$  and  $j$  respectively, then picture elements like squares, circles, and triangles. Each and every one of those pixels

It's  $P_x(i, j)$  and

Point found by squaring  $P_y(i, j)$  and solving (3)  
(4)

$C_1 \oplus H \oplus P_e$

(3) In other words,  $C_2(P_x, P_y) = C_1$ .

(4) Method 3.1.2 for Deciphering

Point  $C_3$  of equation (5) is utilized to decode the pixel coordinates using the private key ( $H$ ) in the decryption phase of the operation.

$C_3 \oplus H \oplus C_1$

$C_{ij} \oplus C_2 \oplus C_3$

Ultimately, it is the  $C_{ij}$  that indicates the outcome of this procedure. Decryption is a process whereby a secret key is used to

It is the suggested WOA method that generates ( $H$ ), since it provides the most optimal values when compared to the standard ECC method ([35]).

A Whale-Optimizing Algorithm, Version 3.2 (WOA)

In 2016, Seyedali Mirjalili and Andrew Lewis created the whale optimization algorithm (WOA) [36], a heuristic approach that considers biological dynamics.

The WOA algorithm is an optimization approach that was developed to simulate the special humpback hunting strategy.

WOA's exceptional worldwide search capability is the result of its novel optimization process.

When choosing a custom key, it's best to use ECC that's based on the WOA [[37]]. The WOA was created as a result of the humpback whale's unique hunting strategy, which is called bubble-net predation. The humpback whale is able to gauge its proximity to prey and encircle it with pinpoint accuracy. Spiral ascent to a depth of around 15 meters has been seen, at which point the humpback whale spits forth bubbles of varying sizes. The first and final

bubbles to be expelled rose to the surface at the same time, generating a network of bubbles that is cylindrical or tubular in shape. A gigantic spider web with knots in it is its preferred method of catching prey, since the prey is encircled before being drawn into the net's core. As a result, the almost upright humpback whales open their mouths in the bubble circle and swallow the netted creatures. As explained above, the humpback whale's hunting process consists of three phases: (1) encircling prey; (2) performing the spiral bubble-net feeding technique; and (3) searching for prey.

### Attacking using a Bubble Net

Using their keen sense of smell, humpback whales may zero in on their prey's position and launch a descending circle assault. Since the optimum solution to the optimization issue is unknown at the beginning, WOA believed that the best candidate solution at the time was the prey or very close to it. All the other search bots compete with the greatest one, trying to move up in the rankings. The following equations are used in math to simulate the strategy of encircling prey:

$$D = C \cdot B - xt$$

$$xt+1 = B - A \cdot D$$

$$A = 2a \cdot r - a$$



**International Journal of Multidisciplinary Engineering in Current Research**  
**Volume 7, Issue 5, May 2022, <http://ijmec.com/>**

$$C = 2 \cdot r$$

D = distance between current search agent  $x_t$  and best search agent B at iteration t. In the event that a better search agent becomes available, it will be used to replace the current best search agent in subsequent iterations. The new position of the search agent may be updated anywhere between the current location and the location of the best search agent, with a being a random number in the range [a, a] and a decreasing from 2 to 0. We can always count on C. To simulate a route with a spiral form, we may use the following equations.

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

$$D' = |B - x_t|$$

In this case,  $D'$  is the best search agent at the current iteration, and S is the current search agent. The shape of a logarithmic spiral is defined by the constant b. The range of l is negative one to one. Because humpback whales often choose both a decreasing circular path and a spiraling one, WOA uses both patterns with a probability of 50%.

$$x_{t+1}$$

$$B - A \cdot D \quad p < 0.5$$

$$= \{D' \cdot e^{bl} \cdot \cos(2\pi l) + B \quad p \leq 0.5$$

On the lookout for dinner

A is used with random values greater than 1 or less than -1 to represent the humpback whales' unpredictable hunt for food.

The bubble-net method is an example of an effective search agent being used for exploitation, whereas a random search agent is more appropriate for exploration. The pursuit of prey may be expressed mathematically as:

$$D = C \cdot x_{rand} - x_t$$

$$x_{t+1} = x_{rand} - A \cdot D$$

Where  $x_{rand}$  is a sample search agent chosen at random from the population. Algorithm 1 demonstrates the WOA pseudocode.

**Whale Optimization Algorithm**

```

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

**International Journal of Multidisciplinary Engineering in Current Research**  
**Volume 7, Issue 5, May 2022, <http://ijmec.com/>**

The aforementioned ECC-WAO based picture security technique was developed in MATLAB 2018 using an i5 CPU and 8 GB RAM setup. The outcomes of the proposed model are compared to those of prior research and standard optimization techniques in this paper. This analysis model uses efficiency measures including PSNR, MSE, and CC to consider many benchmark pictures. These photos include the Lena, baboon, house, and barbara images. Tables 1, 2, and 3 show the proposed ECC-WOA based offer offered encryption architecture. Each RGB color band in the concealed picture has two sets of jumbled and decoded deals. Histogram analysis, correlation analysis, and

entropy analysis are all used in security audits [30]. Unscrambled photos with a PSNR of 53.42 dB are included in this investigation, which is consistent with past displays of similar images. In CC, if the correlation value is low at any given instant, it means that the encryption method successfully produced a large amount of randomness between nearby pixels. According to the numbers, the picture is processed faster since it has less gaps. On the other hand, the PSNR proposed that a more novel figure in primate picture two-some to a larger number of squares would lead to an increase in the length of a number of chains, so accomplishing a state of elite insecurity.

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

	G2						
	B2						

**Table 1**

**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

Several essential quality characteristics, including PSNR, MSE, and CC values, are used in Table 4 to compare the proposed ECC with WOA approach to the ECC methodology for the pictures of a baboon, a flower, a boat, a Barbara, a fingerprint, and an eye. The PSNR value of the suggested technique is higher than that of the ECC algorithm, as shown in the table, indicating that the picture quality has been enhanced. Data from the investigation shows that the proposed method for encrypting images provides a sufficient degree of protection. As a result, it's evident that the suggested technique is superior than the ECC method.

### 5. Final Thoughts

This study introduces an ECC-based picture encryption solution that takes use of the WOA optimization technique. Finally, a PSNR of 54.02 is achieved on average between the original and final photos, proving beyond a reasonable doubt that the proposed technique yields a superior image. Statistical Mode

All pictures have a minimum mean square error, which indicates that the correlation coefficient is very close to 1 for virtually all of them. The integrity of the encryption and the security of the hidden picture are both confirmed by

statistical analysis using histograms and correlation coefficients[39][40]. Analysis shows that the proposed method has higher encryption quality and PSNR values than ECC. We want to investigate the proposed approach's resistance against assaults like salt and pepper, filtering, cropping, and blurring in the future.

### References

- [1] Int. J. Eng. Technol., vol. 7, pp. 293-296, 2018, doi: 10.14419/ijet.v7i2.7.10600, A. Gopi and M. Kameswara Rao, "Survey of privacy and security challenges in IoT."
- [2] "An ethical technique for picture 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] Image Encryption Using Elliptic Curve Cryptography, L. D. Singh and K. M. Singh, Procedia Comput. Sci., vol. 54, no. April 2015, pp. 472-481, 2015.
- [4] According to "A ciphertext-policy Attribute based encryption system for wireless body area networks based on ECC," K. Sowjanya and M. Dasgupta, J. Inf. Secur. Appl., vol. 54, 2020, doi: 10.1016/j.jisa.2020.102559.
- [5] Security considerations for IoT devices that are managed autonomously are revisited in D. R. Shashikumar's 2019 paper.
- [6] Neural Comput. Appl., vol. 32, no. 15, 2020, pp. 10979-10993, doi: 10.1007/s00521-



**International Journal of Multidisciplinary Engineering in Current Research**  
**Volume 7, Issue 5, May 2022, <http://ijmec.com/>**

- 018-3801-x; M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maselena, and N. Arunkumar, "Hybrid optimization with cryptography encryption for medical picture security in Internet of Things."
- [7] As cited in C. Pradeep, M. Rao, and B. Vikas, "Quantum Cryptography Protocols for Internet of Everything: General View," 2021, pp. 211-218.
- [8]
- [9] The following citation is for "RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique" by K. Shankar and P. Eswaran in *J. Circuits, Syst. Comput.*, volume 25, issue 11, pages 1–23, 2016, doi: 10.1142/S0218126616501383.
- [10] *IOSR J. Comput. Eng.*, volume 9, issue 6, pages 80-83, 2013, doi:10.9790/0661-0968083, R. Kaur and E. K. Singh, "Image Encryption Techniques:A Selected Review."
- [11] For example, see S. R., "Dual Server based Security Protocol in MANET using Elliptic Curve Cryptography: A Cluster Head Selection Scenario," in *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 6, pages 1621-1629, 2019, doi:10.30534/ijatcse/2019/87842019.
- [12] Inspired pseudo biotic DNA based cryptography technique against adaptive cryptographic assaults, by E. Babu, C. Raju, and M. Prasad, vol. 18, pp. 291-303, 2016.
- [13] "A new picture encryption technique based on an elliptic curve," [12] U. Hayat and N. A. Azam.
- [14] 2019; vol. 155, pages 391–402; DOI: 10.1016/j.sigpro.2018.10.011.
- [15] "Computation-and-storage-efficient key tree management protocol for secure multicast communications," *Comput. Commun.*, vol. 33, no. 2, pages 136-148, 2010, doi: 10.1016/j.comcom.2009.08.007. [13] D. H. Je, J. S. Lee, Y. Park, and S. W. Seo.
- [16] An efficient heterogeneous key management technique for secure multicast communications in ad hoc networks, by N. Kettaf, H. Abouaissa, and P. Lorenz, *Telecommun. Syst.*, vol. 37, no. 1-3, pp. 29-36, 2008, doi: 10.1007/s11235-008-9074-4.
- [17] "An Image Encryption Scheme Based on Elliptic Curve Pseudo Random and Advanced Encryption System," by T. Shahriyar, M. H. Fathi, and Y. A. Sekhavat, *Signal Processing*, no. June 2017, doi: 10.1016/j.sigpro.2017.06.010.
- [18] *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 218 LNCS, pages. 417-426, 1986; V. S. Miller, "Use of Elliptic Curves in Cryptography," doi: 10.1007/3-540-39799-X 31.
- [19] *J. Inf. Optim. Sci.*, vol. 41, no. 7, 2020, pp. 1645-1672, doi: 10.1080/02522667.2020.1799511. [17] A. Joshi and A. K. Mohapatra, "A new lightweight authentication technique for body area networks based on elliptic-curve cryptography."
- [20] "A Comparative Study of RSA and ECC," K. Vasundhara, Y. V S Sai Pragathi, and Y. Sai Krishna Vaideek, *Int. J. Eng. Res. Appl.* [www.ijera.com](http://www.ijera.com), vol. 8, no. 1, pp. 49-52, 2018, doi: 10.9790/9622-0801014952.
- [21] *Int. J. Civ. Eng. Technol.*, vol. 8, no. 12, pp. 558-571, 2017, doi: 10.1109/IS48319.2020.9200185, R. Shaik, N. K. Gudapati, N. K. Balijepalli, and H. R. Medida conducted a survey on the many uses of the Internet of Things.
- [22] *J. Appl. Math.*, vol. 2014, 2014, doi: 10.1155/2014/601625, cites [20] "Secure collaborative key management for dynamic groups in mobile networks" by S. Kang, C. Ji, and M. Hong.
- [23] *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 32, no. 9, pp. 1081-1094, 2020, doi:



**International Journal of Multidisciplinary Engineering in Current Research**  
**Volume 7, Issue 5, May 2022, <http://ijmec.com/>**

---

- 10.1016/j.jksuci.2017.12.014, "A computationally efficient centralized group key distribution algorithm for secure multicast communications based upon RSA public key cryptosystem."
- [24] A new batch-based group key management protocol applied to the Internet of Things, by L. Veltri, S. Cirani, S. Busanelli, and G. Ferrari, *Ad Hoc Networks*, volume 11, issue 8, pages 2724-2737, 2013, doi: 10.1016/j.adhoc.2013.05.009.
- [25] Based on the work of M. Bilal and S. G. Kang, "A secure key agreement mechanism for dynamic group," *Cluster Comput.*, volume 20, issue 3, pages 2779-2792, 2017, DOI: 10.1007/s10586-017-0853-0.
- [26] Group key management with efficient rekey mechanism: A Semi-Stateful technique for out-of-Synchronized members, by Y. R. Chen and W. G. Tzeng, *Comput. Commun.*, volume 98, pages 31-42, 2017, DOI: 10.1016/j.comcom.2016.08.001.
- [27] According to "Hierarchical techniques for multicast based on Euclid's algorithm," *J. Supercomput.*, volume 65, issue 3, pages 1164-1178, 2013, doi: 10.1007/s11227-013-0923-x.
- [28] *Mob. Networks Appl.*, vol. 21, no. 3, pp. 550-560, 2016, doi: 10.1007/s11036-015-0649-5, S. J. Begum and T. Purusothaman, "Hierarchical Tree Structure Based Clustering Schemes for Secure Group Communication."
- [29] Design of a safe blockchain network," by S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and V. Gupta,
- [30] session initiation protocol authentication approach utilizing elliptic curve cryptography for privacy preservation, *J. Ambient Intell. Humaniz. Comput.*, vol. 9, no. 3, pp. 643-653, 2018, DOI: 10.1007/s12652-017-0460-1.
- [31] "Digital image encryption techniques for wireless sensor networks using image transformation methods: DCT and DWT," by A. M. Shaheen, T. R. Sheltami, T. M. Al-Kharoubi, and E. Shakshuki, published in *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 12, pages 4733-4750, 2019, doi: 10.1007/s12652-018-0850-z.
- [32] *Opt. Lasers Eng.*, vol. 52, no. 1, 2014, pp. 27-34, doi: 10.1016/j.optlaseng.2013.07.015; M. Kumar, D. C. Mishra, and R. K. Sharma, "A first effort on an RGB picture encryption."
- [33] For example, see 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.
- [34] K. Shankar and P. Eswaran, "ECC based picture encryption strategy with assistance of optimization approach employing differential evolution algorithm," *Int. J. Appl. Eng. Res.*, vol. 10, no. 55, pp. 1841-1845, 2015.
- [35] In 2020, *J. Ambient Intell. Humaniz. Comput.* will publish "Secret picture sharing strategy with encrypted shadow images using optimum homomorphic encryption algorithm" by K. Shankar, M. Elhoseny, R. S. Kumar, S. K. Lakshmanaprabu, and X. Yuan (doi: 10.1007/s12652-018-1161-0).
- [36] Using Elliptic Curve Cryptography with a Random Number Generator for Image Encryption. V. K. Yadav, S. Singh, and G. Chandra. 2012.
- [37] To cite this entry: K. Shankar, M. Elhoseny, E. Perumal, M. Ilayaraja, and K. Sathesh Kumar. An effective picture encryption system using the signcryption method and the adaptive elephant herding optimization algorithm. Printed by Springer International Publishing in 2019.
- [38] To wit: S. R., "Elliptic Curve Cryptography Based Security Protocol of MANET under Dynamic Cluster Head Selection



**International Journal of Multidisciplinary Engineering in Current Research**  
**Volume 7, Issue 5, May 2022, <http://ijmec.com/>**

---

Environment," International Journal of Emerging Trends in Engineering Research, volume 8, pages 447-460.

[39] Reference: DOI: 10.30534/ijeter/2020/32822020, page number: 454, 2020.

[40] Group key management using whale optimization algorithm based elliptic curve cryptography for dynamic multicast groups, by C. Sivakumar and C. Nalini, Int. J. Adv. Sci. Technol., vol. 29, no. 8, 2020, pp. 2415-2431.

[41] Mob. Networks Appl., volume 23, issue 4, pages 723-733, 2018, doi: 10.1007/s11036-018-1005-3, authors M. Abdel-Basset, D. El-Shahat, I. El-henawy, A. K. Sangaiah, and S. H. Ahmed.

[42] An enhanced whale optimization method based on distinct searching pathways and perceptual disruption, Symmetry (Basel), vol. 10, no. 6, 2018, pp. 1-31, doi: 10.3390/sym10060210 [38].

[43] Multidimens. Syst. Signal Process., vol. 32, no. 1, pp. 281-301, 2021, doi: 10.1007/s11045-020-00739-8, features research by M. Kaur and D. Singh on "Multiobjective evolutionary optimization approaches based hyperchaotic map and its applications in image encryption."

[44] Int. J. Inf. Technol., vol. 13, no. 2, pp. 551-564, 2021, doi: 10.1007/s41870-019-00413-8, A. Mullai and K. Mani wrote about improving the safety of RSA and elliptic curve cryptography with addition chain utilizing simplified Swarm Optimization and Particle Swarm Optimization for mobile devices.