A ES

ISSN: 2096-3246
Volume 53, Issue 01, Jan, 2021

https://doi.org/10.5281/zenodo.12707087

ECC Image Encryption Scheme using WhaleOptimization Technique

K BALAJI SUNIL CHANDRA, JANGILI RAVI KISHORE, VIJAYA BHASKAR MADGULA

Assistant Professor [1,2,3]

hod.cse@svitatp.ac.in, jangiliravi.kishore1@gmail.com, vijaya.bhaskar2010@gmail.com
Department of Computer Science and Engineering, Sri Venkateswara Institute of Technology, N.H 44,

Hampapuram, Rapthadu, Anantapuramu, Andhra Pradesh 515722

Keywords:
Node Location, Cloud Safety, Data Deployment, and Throughput.

ABSTRACT

Through the simultaneous integration of the tangible and immaterial realms, the Internet of Things (IoT) generates integrated communication scenarios for network devices and stages. Encryption technologies that provide security to transmitted pictures across the connected networks of the two parties were one of the significant open difficulties in bolstering IoT security that the study's researchers recognised and analysed. The device is based on a hybrid algorithm that uses optimisation and encryption strategies. This proposed picture safety model encryption made use of the Whale Optimisation technique. By following the suggested strategy, optimisation in encryption techniques aims to choose the most advantageous keys for encryption algorithms. Following implementation, the results are evaluated using the Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). If the proposed technique outperforms the current approaches, then the recommendation is considered a success.

ISSN: 2096-3246
Volume 53, Issue 01, Jan, 2021

https://doi.org/10.5281/zenodo.12707087

Introduction

An outstanding method for delivering several recipients from a single IP datagram source is multicasting Internet Protocol (IP). With the proliferation of high-speed Internet, multicasting IP has become more popular as a means of group communication for uses such as real-time video delivery. Multicast IP vulnerabilities may be caused by a number of security flaws, which is why more and more organisations are relying on multicast IP to distribute information. Any server, for instance, may send an IGMP message to its closest router and join a multicast group, which makes the job difficult. One of the methods proposed to avoid vulnerabilities is encrypting data using group keys[2][3].

Every member of the group, including the sender, shares a single key, which is called the group key. For the purpose of encrypting both the sender's and the recipients' communications, group keys are crucial. Group key management must adhere to security standards such as reverse secrecy[4] and call confidentiality [5] [6]. This criteria is put in place to ensure that no one other than authorised team members may decipher the data. Secure communication is not available to those who have left the Multicast Group at this time [7]. New members joining the Multicast group will not be able to access messages made before they joined in reverse. 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. It usually takes more computations and communications overhead to rewrite after leaving a group compared to joining a group. This is due to the fact that when a new member is added to a group, the updated group key may be delivered to both the current members via multicast communication, encrypted with the old key, and to the new member through unicast using the private key. references [8] through [10]. There have been many descriptions of re-keying strategies for secure multicast up till recently[11][12]. Departure group key distribution computational and communication cost reduction is a primary motivation for these techniques. Having said that, there have been issues with each of them. Distribution of group keys to members during joins is the primary emphasis of the techniques proposed in [8]. The group key is updated after a predetermined duration in references [13] and [14]. Consequently, these methods do not provide true forward and backward secrecy. Multiple subgroups are created from the multicast group in the solutions given in [15]. It is the responsibility of a designated subgroup controller to generate keys for their own subgroup. When a subgroup enters or quits, just that subgroup modifies its local key. The troublesome rekeying procedure that occurs when a group member departs is one drawback of these protocols. This research offers the following contributions in response to this issue. To encrypt data, experts employ the Elliptic Curve Cryptography (ECC) technique. This approach selects the private key for every member of the group using the Whale Optimisation approach (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]. Using the public keys of all members and the group controller, the key server creates a shared group key. In order to facilitate cooperative operation, the key server generates a new private key and the inverse value for the new member. After then, the updated group key is sent out over multicast. to every member of the subgroup and broadcast to any new members via unicast. Key servers do not generate new group keys but instead inform the remaining members of the subgroup of the inverse value of the deceased member's value. When a member leaves a group, their inverse value is applied to the group keys of the other members who are still there. The computational cost of the rekeying operation will be reduced by following this technique [19].

ISSN: 2096-3246
Volume 53, Issue 01, Jan, 2021

https://doi.org/10.5281/zenodo.12707087

1. Related works

Secure group core management has been the focus of a number of earlier publications in this field. A mobile network is comprised of several wirelessly communicating mobile devices. Worries about security become more complicated when volatility is present. A discussion of safe group key management for the ever-changing peer groups in mobile wireless networks is given by Sukin et al. [20]. One of the biggest issues with secure group chat is people exchanging passwords. In order to accommodate the dynamic nature of networks and the frequent changes in membership, innovative team switching programmes and efficient recording systems have been developed. This technique provides greater leeway in case the group dynamically changes, while still establishing the group key. The proposed project was a success in terms of independence of keys, validation of keys, forward or backward secrecy, and team secrecy. Utilising the proposed idea might result in top-notch multicast security on mobile networks. In order to reduce the cost of calculating the master key server (KS) during key updates, Kumar et al.[21] proposed a more efficient central group centralised group key distribution (CGKD). The processing cost is decreased when a member joins by adding, multiplying, and subtracting, playing a game, and making an image, as well as by deleting. In addition, the proposed method simplifies KS storage. Furthermore, a dual-policy-based CGKD protocol extension has been created to deal with significant member turnover. Our results showed that the proposed method outperformed the control group in terms of KS overload and group participation. For effective team distribution and management over various internet technologies and ad hoc networks, Veltri et al.[22] laid forth a paradigm. Reduced network traffic and overheads due to user-induced changes in team composition are the goals of the proposed method. Some of the many possible uses for recommended mapping scenarios include safe online data storage and encrypted communications in vehicle networks. In the proposed approach, a focal point is used. When several adverse things happen at once, only then does 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 mannergroup-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 atechnique 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

https://doi.org/10.5281/zenodo.12707087

conventional methods. The suggested strategy was perfect for moving the cluster head in the near future, therefore the reorganisation time was far less than with conventional approaches. In order to ensure the security of Internet communications, Kumari et al. (2018)[27] investigated the crucial role that a robust verification scheme plays. With the suggested ECC technique, attacks that impersonate clients or servers would fail. Client confidentiality and shared authentication are also not part of their plan. 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. Shaheen et al. [28] state that traditional cryptosystems cannot be linked to the WSN since most of the presented methods are structurally and estimatively unsuitable for advanced pictures.

2. 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. Following this, the picture is partitioned into blocks prior to the encryption step[8][29]. The encryption method used to secure each block's matrix is the ECC approach. Then, the new pixel value is used to replace the old one in every block. The original picture may be hidden while the scrambled one is obtained using this procedure. After the encryption process is finished, the encrypted picture is decoded by using the opposite encryption method [30]. Optimisation of the private key generation technique was carried over into the decryption process via the WOA algorithm. Once the optimised key generation phase is over, the image's output is used as a health metric to determine the Peak Signal to Noise Ratio (PSNR) value. Finding the optimal PSNR value for a private key is the first step towards keeping it in top shape. After the decryption process is finished, the PSNR, MSE, and Correlation Coefficient (CC) are used to compare the original picture with the final output image in order to evaluate correctness. This method ensures the secure transfer of the original picture while protecting the privacy of the original data.

3.1. Elliptical Curve Cryptography (ECC)

Asymmetric key cryptography makes use of public key cryptography in several ways, and ECC is one of those ways[31][32][33]. Following this process yields the upper bound with a constant Cryptography, starting with the base point and working through the prime number function: Equation (1) shows the fundamental ECC equation.

Axe < b, where y2 < x3

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, tocreate 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) $Q = H \times P$(2)

A ES
https://doi.org/10.5281/zenodo.12707087
ISSN: 2096-3246
Volume 53, Issue 01, Jan, 2021

Whale Optimization Algorithm (WOA)

The whale optimisation algorithm (WOA)[36] is a heuristic approach that SeyedaliMirjalili and Andrew Lewis created in 2016 that accounts for biological processes.WOA is an optimisation algorithm that mimics the specific humpback hunting approach.The exceptional worldwide search capability of WOA is a result of its unique optimisation process. For the best bespoke key selection, use ECC based on the WOA [37].The unique hunting strategy of the humpback whale, called bubble-net predation, served as an inspiration for the WOA. The humpback whale can sense its surroundings and determine how far away its prey is. It has been observed that humpback whales may spit up bubbles of varying sizes after spiralling up to depths of around 15 metres. At the same time that the first and final bubbles emerged from the mouth, a network of cylindrical or tubular bubbles formed. Its preferred method of hunting is weaving a huge web like a spider's web around its prey and bringing it to the middle of the net. So, in the bubble circle, the almost upright humpback whales open their jaws and swallow the netted creatures. As mentioned earlier, there are three distinct phases to a humpback whale's hunting process: encircling prey, the spiral bubble-net feeding manoeuvre, and searching for prey [38].

Bubble-net attacking strategy

Humpback whales dovetail their attacks in a decreasing circle when they pinpoint the exact position of their victim. Because WOA doesn't know what the ideal solution is when they start the optimisation challenge, they presume that the prey or anything close by is the best candidate option right now. As a result, the other search agents compete to outdo the top search agent. Here are several mathematical equations that may be used to model the strategy of encircling the prey: \$$D$ = \$$\mathbf{O}.\ B - xb$ The formula for xb+1 is B minus A. $A = 2a.r - a$

$$C = 2.r$$

Where D is the distance between the current search agent x^t and the best search agent B at t 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 newlocation 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:

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

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

Where D' denotes the absolute value of the distance between the current search agent and thebest search agent at a given iteration. b is a constant that specifies the logarithmic spiral's form. l is a random number between $[-1,1]$. 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:

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

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

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

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.

ISSN: 2096-3246
Volume 53, Issue 01, Jan, 2021
https://doi.org/10.5281/zenodo.12707087

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 correlationvalue 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

<table>
<tr><th>Input Image</th><th>Color band</th><th>Share creation</th><th>Combined Sharing</th><th>Encryption</th><th>Decryption</th><th>Reconstruct image</th></tr>
<tr><td rowspan="5"></td><td>R1</td><td></td><td></td><td></td><td></td><td rowspan="5"></td></tr>
<tr><td>G1</td><td></td><td></td><td></td><td></td></tr>
<tr><td>B1</td><td></td><td></td><td></td><td></td></tr>
<tr><td>R2</td><td></td><td></td><td></td><td></td></tr>
<tr><td>G2</td><td></td><td></td><td></td><td></td></tr>
</table>

	B2					

Table 2

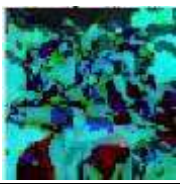
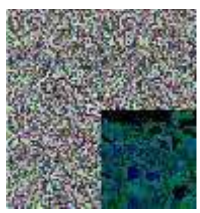
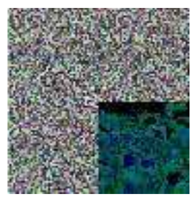
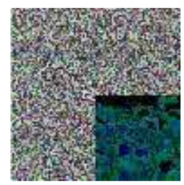
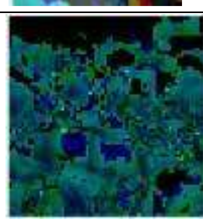
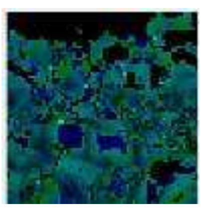
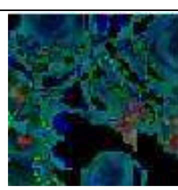
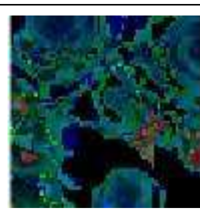
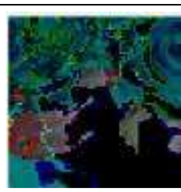
Input Image	Colo r band	Share creation	Combined Sharing	Encryption	Decryption	Reconstructed Output
	R1					
	G1					
	B1					
	R2					
	G2					

https://doi.org/10.5281/zenodo.12707087

ISSN: 2096-3246
Volume 53, Issue 01, Jan, 2021

	B2					

Table 3

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

https://doi.org/10.5281/zenodo.12707087
ISSN: 2096-3246
Volume 53, Issue 01, Jan, 2021

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 improvedthe 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 acceptablelevel of security. It clearly indicates that the proposed strategy outperforms the ECC approach.

5. Conclusion

Using ECC and the WOA approach, the paper presents an optimal image encryption strategy. With an average PSNR value of 54.02 between the first and final photographs, it is evident that the recommended technique produces a better picture. On whole, On top of that, the correlation coefficient is around 1 in most of the images since the square error is minimised across all photographs. The examination of correlation coefficients and histograms demonstrates unequivocally that the encryption process remains intact and safeguards the

ISSN: 2096-3246
Volume 51, Issue 01, Jan, 2019

confidentiality of the secret picture [39] [40]. The comparison shows that the suggested technique outperforms ECC in terms of encryption and PSNR values. Next, we'll see how well the suggested solution holds up under pressure from various editing techniques, such as salt & pepper, filtering, cropping, and blurring.

References

The article "Survey of privacy and security issues in IoT" was published in the International Journal of Engineering Technology in 2018. It can be found on pages 293-296 and has the DOI number 10.14419/ijet.v7i2.7.10600.

[2] "An ethical way for image encryption using ECC," 2009 1st Int. Conf. Comput. Intell. Commun. Syst. Networks, CICSYN 2009, pp. 342-345, doi: 10.1109/CICSYN.2009.33, written by K. Gupta, S. Silakari, R. Gupta, and S. A. Khan. "Image Encryption using Elliptic Curve Cryptography," published in Procedia Computer Science in 2015 (vol. 54, no. April, pp. 472-481, doi: 10.1016/j.procs.2015.06.054), was written by L. D. Singh and K. M. Singh. [4] "A ciphertext-policy Attribute based encryption scheme for wireless body area networks based on ECC," published in the Journal of Information Security and Applications in 2020, with the DOI 10.1016/j.jisa.2020.102559, is written by K. Sowjanya and M. Dasgupta.

[5] In his 2019 paper "Revisiting Security Aspects of Internet of Things for Self-Managed Devices," D. R. Shashikumar discusses issues related to the safety of smart home devices.

[6] "Hybrid optimisation with cryptography encryption for medical image security in Internet of Things," published in 2020 in Neural Comput. Appl., volume 32, issue 15, pages 10979-10993, with the DOI 10.1007/s00521-018-3801-x, is written by M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maseleno, and N. Arunkumar.In their 2021 article titled "Quantum Cryptography Protocols for Internet of Everything: General View," C. Pradeep, M. Rao, and B. Vikas discuss quantum cryptography on pages 211-218.

[8] "RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique," published in June 2016 by Journal of Circuits, Systems, and Computers, with the DOI number 10.1142/S0218126616501383.

"Image Encryption Techniques:A Selected Review" by R. Kaur and E. K. Singh appeared in the 2013 issue of the IOSR Journal of Computer Engineering, volume 9, issue 6, pages 80–83, with the DOI 10.9790/0661-0968083.

10. S. R. "Dual Server based Security Protocol in MANET using Elliptic Curve Cryptography: A Cluster Head Selection Scenario" (2019, vol. 6, pp. 1621-1629, doi: 10.30534/ijatcse/2019/87842019), International Journal of Advanced Computing Science and Engineering.

[11] "Inspired pseudo biotic DNA based cryptographic mechanism against adaptive cryptographic attacks," published in 2016, by E. Babu, C. Raju, and M. Prasad, vol. 18, pp. 291-303."A novel image encryption scheme based on an elliptic curve," published in Signal Processing in 2019, with the DOI 10.1016/j.sigpro.2018.10.011.

[12] U. Hayat and N. A. Azam. The authors of the article "Computation-and-storage-efficient key tree management protocol for secure multicast communications" (D. H. Je, J. S. Lee, Y. Park, and S. W. Seo, 2010, doi: 10.1016/j.comcom.2009.08.007.) discussed this topic in their 2010 publication in the Computer Communication and Signal Processing journal. "An efficient heterogeneous key management approach for secure multicast communications in ad hoc networks," published in 2008 in Telecommun. Syst., with the DOI 10.1007/s11235-008-9074-4, was written by N. Kettaf, H. Abouaissa, and P. Lorenz. An image encryption scheme based on an elliptic curve pseudo-random and advanced encryption system was published in Signal Processing in June 2017 by T. Shahriyar, M. H. Fathi, and Y. A. Sekhavat. The article may be accessed online at doi: 10.1016/j.sigpro.2017.06.010. Vol. 218 LNCS, pp. 417-426, 1986, doi: 10.1007/3-540-39799-X_31, V. S. Miller, "Use of Elliptic Curves in Cryptography," Lecture Notes in Computer Science (containing Supplementary Lecture Notes in Artificial Intelligence and Bioinformatics), vol.

[17] "A novel lightweight authentication protocol for body area networks based on elliptic-curve cryptography" by A. Joshi and A. K. Mohapatra appeared in the 2020 issue of the Journal of Industrial Optimisation Science, volume 41, issue 7, pages 1645–1672, with the DOI 10.1080/02522667.2020.1799511. In a 2018 article published

in the International Journal of Engineering Research and Applications, K. Vasundhara, Y. V. S. Sai Pragathi, and Y. Sai Krishna Vaideek compared RSA and ECC. The article can be found online at www.ijera.com and has the DOI of 10.9790/9622-0801014952. [19] "A Survey on Applications of Internet of Things," International Journal of Civil Engineering and Technology, volume 8, issue 12, pages 558–571, 2017, doi: 10.1109/IS48319.2020.9200185, by R. Shaik, N. K. Gudapati, N. K. Balijepalli, and H. R. Medida. The authors of the 2014 article "Secure collaborative key management for dynamic groups in mobile networks" (S. Kang, C. Ji, and M. Hong) published in the Journal of Applied Mathematics have the DOI: 10.1155/2014/601625.

[21] "A computationally efficient centralised group key distribution protocol for secure multicast communications based upon RSA public key cryptosystem," published in 2020 in the Journal of King Saud University - Computing and Information Science, with the DOI 10.1016/j.jksuci.2017.12.014.

[22] "A novel batch-based group key management protocol applied to the Internet of Things," published in Ad Hoc Networks in 2013, with the DOI 10.1016/j.adhoc.2013.05.009. The authors are L. Veltri, S. Cirani, S. Busanelli, and G. Ferrari. Cluster Computing, volume 20, issue 3, pages 2779–2792, 2017, with the DOI 10.1007/s10586-017-0853-0, was written by M. Bilal and S. G. Kang.

Y. R. Chen and W. G. Tzeng published an article titled "Group key management with efficient rekey mechanism: A Semi-Stateful approach for out-of-Synchronized members" in the Computer Communication magazine in 2017. The article can be found on pages 31–42 and has the DOI of 10.1016/j.comcom.2016.08.001. "Hierarchical approaches for multicast based on Euclid's algorithm," published by J. A. Álvarez-Bermejo, N. Antequera, and J. A. López-Ramos in [25]. Volume 65, Issue 3, Pages 1164–1178, Journal of Supercomputing, 2013, DOI: 10.1007/s11227-013-0923-x.

[26] "Hierarchical Tree Structure Based Clustering Schemes for Secure Group Communication" by S. J. Begum and T. Purusothaman appeared in the 2016 edition of Mobile Networks Applications, with the DOI 10.1007/s11036-015-0649-5. [27] "Design of a secure "An anonymity-preserving authentication scheme for session initiation protocol using elliptic curve cryptography," published in the Journal of Ambient Intelligence and Human-Centered Computing in 2018, with the DOI 10.1007/s12652-017-0460-1, is available online. [28] In a 2019 article published in the Journal of Ambient Intelligence and Human-Centric Computing, the authors discuss "Digital image encryption techniques for wireless sensor networks using image transformation methods: DCT and DWT." The article is available online at doi: 10.1007/s12652-018-0850-z. [29]"A first approach on an RGB image encryption" by M. Kumar, D. C. Mishra, and R. K. Sharma appeared in the 2014 edition of Opt. Lasers Eng., volume 52, issue 1, pages 27–34, with the DOI 10.1016/j.optlaseng.2013.07.015. [30] In 2016 they published an article titled "An Efficient Image Encryption Technique Based on Optimised Key Generation in ECC Using Genetic Algorithm" in the Adv. Intell. Syst. Comput. journal, with the DOI 10.1007/978-81-322-2656-7. The article can be found on pages 1105-1111 in print. "ECC based image encryption scheme with aid of optimisation technique using differential evolution algorithm," published in 2015 by Int. J. Appl. Eng. Res., was authored by K. Shankar and P. Eswaran. [32] "Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique," published in 2020 in the Journal of Ambient Intelligence and Human-Centered Computing, with the DOI 10.1007/s12652-018-1161-0, is written by K. Shankar, M. Elhoseny, R. S. Kumar, S. K. Lakshmanaprabu, and X. Yuan. Citation: "Public Key Cryptosystem Technique Elliptic Curve Cryptography with Generator g for Image Encryption" by V. K. Yadav, S. Singh, and G. Chandra, 2003 year 2012. [34] An effective picture encryption system developed by K. Shankar, M. Elhoseny, E. Perumal, M. Ilayaraja, and K. Sathesh Kumar using the signcryption method in conjunction with adaptive elephant herding optimisation. In 2019, Springer International Publishing was the publisher. An elliptic curve cryptography-based security protocol for MANETs operating in a dynamic cluster head selection environment was published in the International Journal of Emerging Trends in Engineering Research (vol. 8, pp. 447-448). DOI: .30534/ijeter/2020/32822020, 454, 2020. "Efficient group key management using whale optimisation algorithm based elliptic curve cryptography for dynamic multicast groups," International Journal of Advanced Scientific Technology, vol. 29, no. 8, special issue, 2020, pp. 2415-2431, proposed by C. Sivakumar and C. Nalini. [37] "A Novel Whale Optimisation Algorithm for

AES
https://doi.org/10.5281/zenodo.12707087
ISSN: 2096-3246
Volume 51, Issue 01, Jan, 2019

Cryptanalysis in Merkle-Hellman Cryptosystem," published in Mob. Networks Appl., volume 23, issue 4, pages 723-733, 2018, with the DOI 10.1007/s11036-018-1005-3, by M. Abdel-Basset, D. El-Shahat, I. El-henawy, A. K. Sangaiah, and S. H. Ahmed. This sentence is paraphrased from an article published in 2018 in the journal Symmetry (Basel) by W. Z. Sun, J. S. Wang, and X. Wei. The article is titled "An improved whale optimisation algorithm based on different searching paths and perceptual disturbance" and has the DOI 10.3390/sym10060210.
"Multiobjective evolutionary optimisation techniques based hyperchaotic map and their applications in image encryption" (M. Kaur and D. Singh, 2021) appeared in Multidimens. Syst. Signal Process., volume 32, issue 1, pages 281-301, with the DOI 10.1007/s11045-020-00739-8.
The authors of the essay "Enhancing the security in RSA and elliptic curve cryptography based on addition chain using simplified Swarm Optimisation and Particle Swarm Optimisation for mobile devices" (doi: 10.1007/s41870-019-00413-8), published in the International Journal of Information Technology in 2021, present their findings in the field.