As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology
Volume 10, Issue 01, pages 125-132.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol10issue01.html
DOI: https://doi.org/10.46501/IJMTST1001017

Gravitational Search Algorithm-Based Optimization of an ECC Image Encryption Scheme

Godina Amruthavani

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

To Cite this Article
Godina Amruthavani, Gravitational Search Algorithm-Based Optimization of an ECC Image Encryption Scheme, International Journal for Modern Trends in Science and Technology, 2024, 10(01), pages. 125-132. https://doi.org/10.46501/IJMTST1001017

Article Info
Received: 12 January 2024; Accepted: 28 January 2024; Published: 02 February 2024.

ABSTRACT

Image encryption enables users to safely transmit digital photographs via a wireless medium while maintaining enhanced anonymity and validity. Numerous studies are being conducted to strengthen picture encryption systems. Elliptical curve cryptography (ECC) is an effective tool for safely transferring images and recovering them at the receiver end in asymmetric cryptosystems. This method's key generation generates a public and private key pair that is used to encrypt and decrypt a picture. They use a public key to encrypt the picture before sending it to the intended user. When the receiver receives the image, they use their private key to decrypt it. This paper proposes an ECC-dependent image encryption scheme utilizing an enhancement strategy based on the Gravitational Search Algorithm (GSA) algorithm. The private key generation step of the ECC system uses a GSA-based optimization process to boost the efficiency of picture encryption. The image's output is used as a health attribute in the optimization phase, such as the PSNR value, which demonstrates the efficacy of the proposed approach. As comparison to the ECC Method, it has been discovered that the suggested encryption scheme offers better optimal PSNR values.

1. INTRODUCTION

The increased reliance on computers to process data and distribute it over virtually linked networks has heightened the need for protection. Information protection has become a concern as a result of developments in network technologies in today's modern environment. If the digital era progresses, we will be able to obtain knowledge explicitly and simply communicate it by photographs [1]. It was not done without any pitfalls, such as unauthorized access to these records and illicit copying. The importance of secret transmission in protecting classified information against risks and misuse cannot be overstated. In multimedia systems, image protection is a crucial and commanding problem [2][3]. Encryption and decryption of data have developed into the optimal method for ensuring the confidentiality and legitimacy of data. There will eventually be a significant test, when hazards and weaknesses develop in lockstep with advancements [4].Nowadays, various methods have been developed to provide security while also increasing the cost and utilization of computational resources [5]. Image encryption strategies enable us to alter a unique image to another (encoded) image that is not easy; consequently, to keep the image private between clients, or in other words, to ensure that no one can gain access to the substance without a decryption key [6]. Image encryption techniques attempt to turn an image into a difficult-to-understand image that is highly sensitive for users, implying that no one will access the content without a decryption key. Only the main identified individual has access to the initial picture magnitude. For cryptographic techniques, the majority of standards, such as hardware and applications, use the public key methodology. ECC is asymmetric key cryptography, which implies that the encryption and decryption keys are not the same [7][8]. A key pair is used in public key cryptography, with one serving as the private key and the other as the public key [9][10]. The public keys are distributed to all people, and only the person who is participating in the conversation recognizes the private key. ECC, unlike secret key cryptography, is ideal for systems where a protected channel to relay the private key is not available [11][12]. Elliptic Curve Cryptography is a nearly modern public key cryptosystem that offers higher security thresholds, lower mathematical difficulty, smaller key sizes, and greater computational efficiency [13][14]. The protection of such photos is becoming increasingly critical as digital products communicate over accessible networks. Some benefits of evolutionary optimization algorithms include the ability to optimize the fitness role of independent variables[15]. Essentially, these methods use iterative trial and error improvement, analogous to how living organisms adapt and evolve to find the best fitness under defined conditions [16][17]. Particle swarm optimization (PSO) is a simple-to-implement population-based stochastic optimization strategy that has seen a lot of success in solving real-world continuous optimization problems in recent years. Particle swarm optimization (PSO) and differential evolution (DE) are two population-based stochastic search methods that are commonly used to solve optimization problems in many research and engineering fields [18][19].

2. LITERATURE REVIEW

Prabir Kr. Naskar and Atal Chaudhuri [20] proposed a stable encryption strategy for digital images in 2014; it can also be used for any digital file (e.g. Text, image and audio, etc.). A block of hidden bytes is ciphered using bit-wise XORing and flipping, and then each ciphered byte is shuffled inside N locations (N is the size of secret byte). This is a method that combines substitution and transposition using dynamic SBOX and TBOX. The cryptosystem's key is very big, which makes it more secure against brute-force attacks. Furthermore, main sensitivity analysis, statistical analysis, and differential attack analysis demonstrate the author's established algorithm's high acceptability. Manish Kumar et al. [21] suggested the first two-stage random matrix affine cypher paired with discrete wavelet transformation for RGB picture encryption and decryption in 2013. The encryption process is simple in their system, but the decryption process is more difficult, particularly when there is no additional knowledge about the right keys or the possible correct RMAC parameter arrangement. The writers also offer a security overview as well as a study of their methodology to that of others. It reveals that their correctly decrypted picture has a very low MSE, indicating that the method decrypts with very little knowledge loss. This approach can be used to send RGB picture data over insecure channels easily and safely. Khaled Loukhaoukha et al [22] suggested a new picture encryption algorithm based on the Rubik's cube theorem in 2012. In this article, picture conservation is of special concern. The Rubik's cube theory is used to scramble the initial picture. The XOR operator is extended to rows and columns of the scrambled picture using two hidden keys as the first step in this principle. The same key is flipped and added to the hidden image's even rows and columns. The proposed algorithm's robustness against various forms of attacks, such as mathematical and differential attacks, was demonstrated by a systematic numerical study (visual testing). Randhir Kumar and Akash Anil[23]developed a system for developing ECC for file formats such as audio, video, and image in 2011. It's often used to compress files of the same kind. Security-constrained data may be hidden and retrieved using the software available. The protocols in the elliptic curve methodology are framed and thought to be impossible to find the discrete logarithm of a random elliptic curve element with respect to a publicly-known base point. The complexity of the issue is determined by the curve scale. In general, there are two people involved in the encryption and decryption processes, one on the encryption side and the other on the decryption side. Data is submitted not only in image form, but also in audio, video, and image form. Padma Bh et al.[24]addressedKoblitz's approach for representing a message as a point and vice versa in 2010. The execution time for encoding and decoding functions is unaffected by the values of a, b, and p. (domain parameters ECC). For various values of the ECC domain parameters, the encoding execution period varies. For various values of a, b, and p, the execution period for decoding is constant. As opposed to encoding, decoding takes a fraction of the time.

Elliptic Curve Cryptography (ECC) has established itself as a promising cryptographic technique [25]. The National Institute of Standards and Technology (NIST) defined the elliptic curve random generator as a method for grouping arbitrary numbers based on curves. The random age stage is determined by a publicly available key and a changing point G, which serves as the generator of a curve used to generate random configurations. AES is then coupled to these configurations, securing self-assertive keys for image encryption. AES in close proximity to widely spread random provides an illustrious encryption technology. Shankar and Lakshmanaprabu [26] proposed a homomorphic encryption scheme based on Ant Lion optimization (ALO).To increase the level of security, an algorithm called ALO is introduced. The best-encrypted image is displayed in terms of maximum entropy with this ALO. Ewees et al. [4]proposed OBLGOA, an upgraded form of the grasshopper optimization algorithm (GOA) that incorporates the opposition-based learning (OBL) methodology. The study examined the implementation of the proposed OBLGOA by conducting six test arrangements that included twenty-three benchmark capacities and four building difficulties. The experiments revealed that the proposed computation produced superior results than those frequently obtained through accurate calculations in this area. Finally, the researchers concluded that when compared to cutting-edge algorithms, OBLGOA calculation can produce aggressive results in optimization design problems.

3. PROPOSED METHODOLOGY

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 picture is separated into blocks before the encryption phase begins. The elliptical curve cryptography 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 picture is decrypted using the reverse encryption technique[27]. The GSA 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[28][29]. When the decryption step is complete, the final output picture is compared to the original image to assess accuracy using the PSNR, Mean Square Error (MSE), and Correlation Coefficient (CC). The original picture 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[30][7]. 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)

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

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 picture at the reception end. If the value "*P*" is any some point on the curve, select a random integer number "*H*", which is a private key, in the area of "*1 to n-1*", then the public key "*Q*" is generated as (2)

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

3.1.1 Encryption method

In the encryption part of the procedure, every color band of the input picture is divided into the blocks. These four blocks are encrypted by the proposed encryption method. 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[31][12]. The pixels $P_x(i,j)$ and $P_y(i+1,j)$ and the point is obtained in (3) and (4)

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

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

3.1.2 Decryption method

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

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

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

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

3.1.3 Gravitational Search Algorithm

GSA is an observational technique focused on Newton's laws of universal gravitation, which was first introduced in 2009[32][33]. The algorithm follows gravitational law's inductive reasoning: "For any two objects, a force is drawn to the other object that is directly proportional to their mass and inversely proportional to their square distance." The gravitational force of any two nodes is based on the gravity theorem as presented in equation (7)

$$F(t) = G(t)\frac{M_1 M_2}{D(t)^2} \quad (7)$$

Where, M_1 and M_2 are the mosses of the two nodes and $D$is the distance between the nodes. The gravitational constant G at the time of t instant is given by (8)

$$G(t) = G(t_0)\exp(-\alpha t / T_{final}) \quad (8)$$

In this expression $\alpha$is the positive constant, $G(t_0)$ is the gravitational constant at the time instant of t_0 and T_{final} is the total search time. The cost function value is heavily influenced by the gravitational constant at time t and the original masses. A node with a higher mass is a stronger node. Similarly, lighter mass denotes a weaker node. The new defined variable related to the j^{th}node is given by (9)

$$m_j(t) = \frac{C_j(t) - C_j^{worse}(t)}{C_j^{best}(t) - C_j^{worse}(t)} \quad (9)$$

Where $C_j(t)$ is the cost function of the jth node at the iteration instant of t. $C_j^{worse}(t)$ represents the worst cost function and $C_j^{best}(t)$ represents the best cost function. The mass and acceleration of the jth node are given by equations (10) and (11)

$$\overline{M}_j(t) = \frac{m_j(t)}{\sum_{j=1}^{n} m_j(t)} \quad (10)$$

$$a_{j,k}(t) = \frac{F_{j,k}(t)}{\overline{M}_j(t)} \quad (11)$$

For various values of k=1, 2, 3…. P and j=1, 2, 3…N, the variable N represents the number of nodes and the variable P represents the number of parameters to be optimized within the node. $F_{j,k}(t)$, indicates the force of the particles at the position of $x_{j,k}(t)$ and $\overline{M}_j(t)$ represents the mass of the jth particle. The velocity of kth parameter of jth node at $t+1$ iteration is given by (12)

$$v_{j,k}(t+1) = rand_j v_{j,k}(t) + a_{j,k}(t) \quad (12)$$

Where $rand_j$ represents a random number varying between 0 and 1. The final position of kthparameter in jthnode at the instant of $t+1$ is given by equation (13)

$$x_{j,k}(t+1) = x_{j,k}(t) + v_{j,k}(t+1) \quad (13)$$

The set of values k_{best} is used to obtain the best solution and in the every iteration it is updated. The complete process of obtaining best values are depicted in Fig. 1.

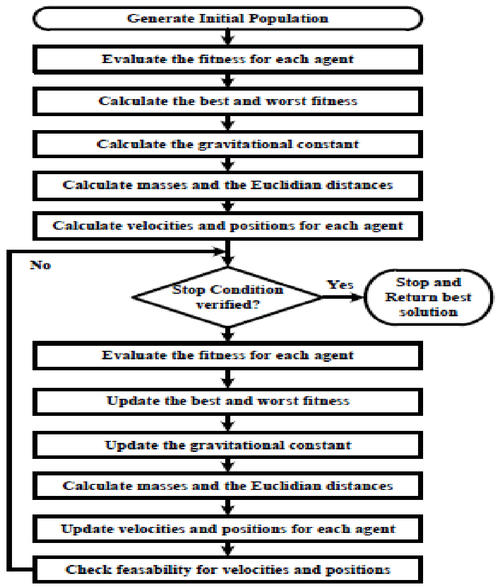


Fig.1: Flow chart representation of GSA

4. RESULTS AND DISCUSSION

This section discusses the experimental findings on the suggested image encryption and optimization technique. The proposed ECC Image Encryption with GSA Optimizationwas implemented in MATLAB 2018 using an i5 processor and 8 GB RAM system setup.The tables 1 and 2 illustrate two representative input images, namely Lena and boat.Encrypt the image of the relevant input images and then decrypt them. Following decryption, the final output image is compared to the original image to demonstrate the proposed algorithm's performance, using quality metrics such as PSNR, MSE, and CC values for each image.

Table1:ECC Image Encryption with GSA Optimization Technique for Lena image

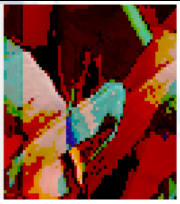
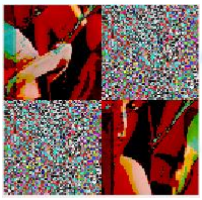
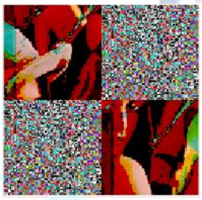
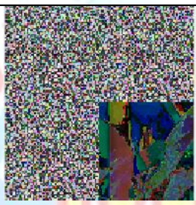
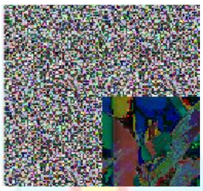
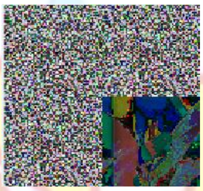
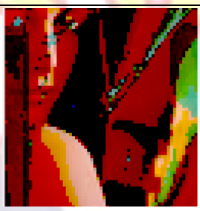
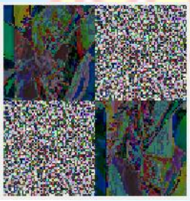
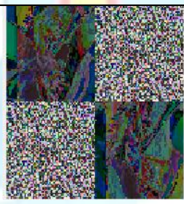
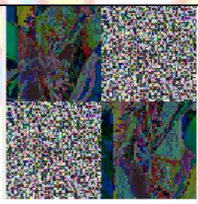
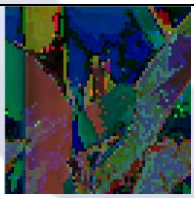
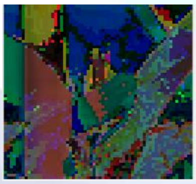
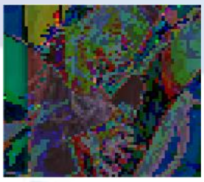
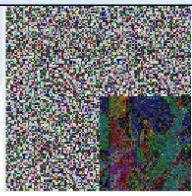
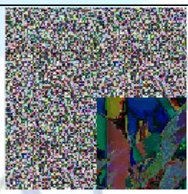
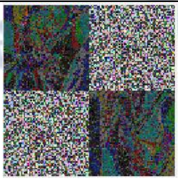
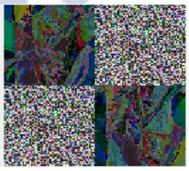
Input Image	Color band	Share creation	Combined Sharing	Encryption	Decryption	Reconstructed Output
	R1					
	G1					
	B1					
	R2					
	G2					
	B2					

Table 2: ECC Image Encryption with GSA Optimization Technique for boat image

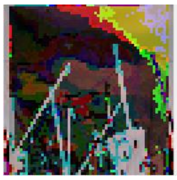
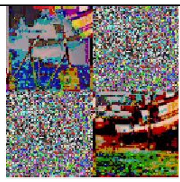
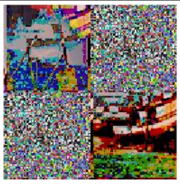
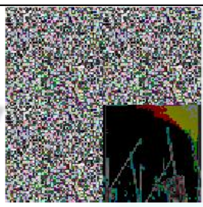
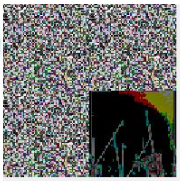
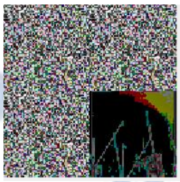
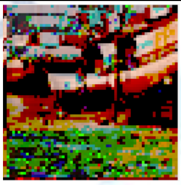
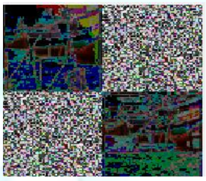
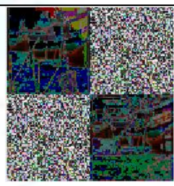
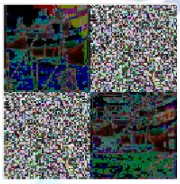
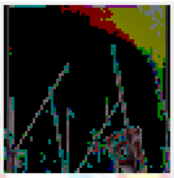
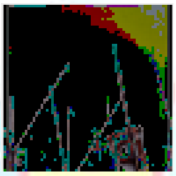
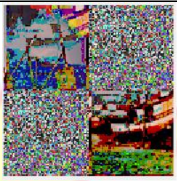
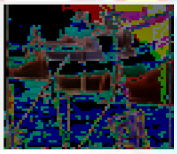
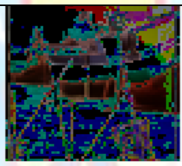
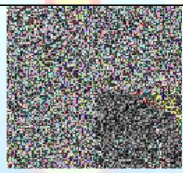
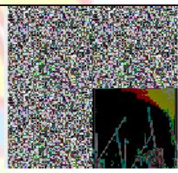
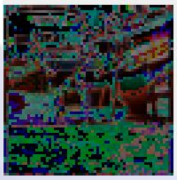
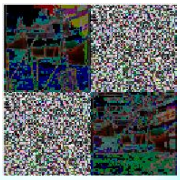
Input Image	Color band	Share creation	Combined Sharing	Encryption	Decryption	Reconstructed Output
	R1					
	G1					
	B1					
	R2					
	G2					
	B2					

Table 3 comparative analysis of ECC and proposed ECC with GSA method

Input	Method	PSNR	MSE	CC
	ECC	45.94	1.67	0.9
	GSA-ECC	60.04	0.065	1
	ECC	46.07	1.62	0.9
	GSA-ECC	59.24	0.078	1
	ECC	46.23	1.56	0.9
	GSA-ECC	59.3	0.077	1
	ECC	46.61	1.43	0.9
	GSA-ECC	58.64	0.87	1
	ECC	46.35	1.52	0.9
	GSA-ECC	57.91	0.105	1

Table 3 compares the proposed ECC with GSA method to the ECC technique using several critical quality parameters such as PSNR, MSE, and CC values for images Lena, 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 picture encryption approach achieves an acceptable level of security. It clearly indicates that the proposed strategy outperforms the ECC approach

Table 4 provides the comparative results analysis of the presented WSA-ECC modelwith existing CSO-FFO-ECC. From the Table 4, itis evident that the GSA-ECC model has obtained better performance compared to CSO-FFO-ECC model. On the applied image 1 lena , the GSA- ECC model has resulted in a higher PSNR of 60.04 dB At the same time, on the applied image 2, the GSA-ECC model has resulted in a higherPSNR of 59.3dB.

Table 4:Comparison of the Proposed GSA-ECC Method to Existing MethodCSO-FFO-ECC in Terms of MSE and PSNR

Input Image	ProposedGSA-ECC		CSO-FFO-ECC [1]	
	MSE	PSNR	MSE	PSNR
	0.065	60.04	0.088	58.68
	0.077	59.3	0.092	58.49

5. CONCLUSION

The research presents an ECC-based picture encryption strategy that is optimized using GSA method. It is demonstrated unequivocally that the suggested method produces a higher-quality image with an average PSNR value of 60.04 between the original and final images. The mean square error is likewise minimized in all images, which means that almost all photos have a correlation coefficient of nearly 1. Histogram and correlation coefficient analyses make it abundantly evident that the encryption process remains unaltered and maintains the secret image's confidentiality. Comparative investigation demonstrates that the suggested technique outperforms ECC in terms of encryption quality and PSNR values. In the future, we will examine the suggested method's resilience to various forms of attacks such as salt and pepper, filtering, cropping, and blurring.

Conflict of interest statement

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

REFERENCES

[1] S. Kaliswaran and M. Y. M. Parvees, "An Efficient Hybrid Optimization Algorithm with Elliptic-Curve Cryptography for Image Encryption," Eur. J. Mol. Clin. Med., vol. 07, no. 07, pp. 4753–4764, 2020.

[2] 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.

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

[4] A. A. Ewees, M. Abd Elaziz, and E. H. Houssein, "Improved grasshopper optimization algorithm using opposition-based learning," Expert Syst. Appl., vol. 112, pp. 156–172, 2018, doi: 10.1016/j.eswa.2018.06.023.

[5] T. K. Goyal and V. Sahula, "Lightweight security algorithm for low power IoT devices," 2016 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2016, no. September, pp. 1725–1729, 2016, doi: 10.1109/ICACCI.2016.7732296.

[6] 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.

[7] V. Kapoor, V. S. Abraham, and R. Singh, "Elliptic Curve Cryptography," ACM Ubiquity, vol. 9, no. 20, pp. 1–8, 2008.

[8] 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.

[9] A. Oad, H. Yadav, and A. Jain, "A Review : Image Encryption Techniques and its Terminologies," Int. J. Eng. Adv. Technol., vol. 3, no. 4, pp. 373–376, 2014.

[10] 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.

[11] M. S. N. G. K. Mounika, A. Yadav, S. L. Anand, and P. Satyannarayana, "Upgrade of GSM security using elliptic curve cryptography algorithm," Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 7, pp. 487–491, 2019.

[12] B. Jyoshna and K. Subramanyam, "Time conserving secured cloud data storage solution based on keccak and elliptic curve cryptography," Int. J. Adv. Res. Eng. Technol., vol. 10, no. 5, pp. 154–165, 2019, doi: 10.34218/IJARET.10.5.2019.016.

[13] 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.

[14] M. Al Saadi and B. Kumar, "A Review on Elliptic Curve Crytography," Int. J. Futur. Gener. Commun. Netw., vol. 13, no. 3, pp. 1597–1601, 2020.

[15] N. Yang, "Digital image encryption algorithm design based on Genetic-hyperchaos," Chinese J. Liq. Cryst. Displays, vol. 32, no. 6, pp. 474–481, 2017, doi: 10.3788/YJYXS20173206.0474.

[16] 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.

[17] A. Rawat and M. Deshmukh, "Tree and elliptic curve based efficient and secure group key agreement protocol," J. Inf. Secur. Appl., vol. 55, p. 102599, 2020, doi: 10.1016/j.jisa.2020.102599.

[18] 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.

[19] D. P. Rajesh, D. M. Alam, D. M. Tahernezhadi, T. Ravi Kumar, and V. P. Rajesh, "Secure communication across the internet by encrypting the data using cryptography and image steganography," Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 10, pp. 454–458, 2020, doi: 10.14569/IJACSA.2020.0111057.

[20] P. Kr. Naskar and A. Chaudhuri, "A Secure Symmetric Image Encryption Based on Bit-wise Operation," Int. J. Image, Graph. Signal Process., vol. 6, no. 2, pp. 30–38, 2014, doi: 10.5815/ijigsp.2014.02.04.

[21] 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.

[22] K. Loukhaoukha, J. Y. Chouinard, and A. Berdai, "A secure image encryption algorithm based on Rubik's cube principle," J. Electr. Comput. Eng., vol. 2012, 2012, doi: 10.1155/2012/173931.

[23] R. Kumar and A. Anil, "Implementation of Elliptical Curve Cryptography," vol. 8, no. 4, pp. 544–549, 2011.

[24] P. Bh, D. Chandravathi, P. P. Roja, and A. Professor, "Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method," IJCSE) Int. J. Comput. Sci. Eng., vol. 02, no. 05, pp. 1904–1907, 2010.

[25] 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.

[26] K. Shankar and S. K. Lakshmanaprabu, "Optimal key based Homomorphic Encryption for color image security aid of Ant Lion Optimization algorithm," Int. J. Eng. Technol., vol. 7, no. 1, pp. 22–27, 2018, doi: 10.14419/ijet.v7i1.9.9729.

[27] K. Shankar and P. Eswaran, "RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography," China Commun., vol. 14, no. 2, pp. 118–130, 2017, doi: 10.1109/CC.2017.7868160.

[28] 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.

[29] B. Murali Krishna, H. Khan, and G. L. Madhumati, "Reconfigurable pseudo biotic key encryption mechanism for cryptography applications," Int. J. Eng. Technol., vol. 7, no. 1.5 Special Issue 5, pp. 62–70, 2018, doi: 10.14419/ijet.v7i1.5.9124.

[30] Sujith Narayan, "a Review on Elliptic Curve Cryptography," Int. J. Emerg. Technol. Innov. Eng., vol. 4, no. 12, pp. 132–138, 2018.

[31] K.Shankar and P.Eswaran, "An Efficient Image Encryption Technique Based on Optimized Key Generation in ECC Using Genetic Algorithm," Adv. Intell. Syst. Comput., vol. 394, pp. 1105–1111, 2016, doi: 10.1007/978-81-322-2656-7.

[32] N. M. Sabri, M. Puteh, and M. R. Mahmood, "A review of gravitational search algorithm," Int. J. Adv. Soft Comput. its Appl., vol. 5, no. 3, 2013.

[33] H. Hu, X. Cui, and Y. Bai, "Two Kinds of Classifications Based on Improved Gravitational Search Algorithm and Particle Swarm Optimization Algorithm," Adv. Math. Phys., vol. 2017, 2017, doi: 10.1155/2017/2131862.