

Elliptical curve cryptography image encryption scheme with aid of optimization technique using gravitational search algorithm

Ramireddy Navatejareddy¹, Muthukuru Jayabhaskar¹, Bachala Sathyanarayana²

¹Department of Computer Science Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India

²Department of Computer Science and Technology, Sri Krishnadevaraya University, Ananthapur, India

Article Info

Article history:

Received Jun 21, 2021

Revised Oct 6, 2021

Accepted Nov 23, 2021

Keywords:

Elliptical curve cryptography

Gravitational search

Optimization

Image encryption

MSE

PSNR

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 peak signal to noise ratio (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.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Ramireddy Navatejareddy

Department of Computer Science Engineering, Koneru Lakshmaiah Education Foundation

Vaddeswaram, Guntur, Andhra Pradesh, 522502, India

Email: rnavateja2233@gmail.com

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 amount and usage of computing 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 hide among customers, or in other words, to ensure that no one can gain access to the substance without a decryption key [6]. Image encryption strategy 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. Elliptical curve cryptography (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]. ECC is a nearly modern public key cryptosystem that offers higher 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 strategy that has seen a lot of success in solving real-world continuous optimization problems in present years. PSO and differential evolution (DE) are two strength based stochastic search methods that are commonly used to solve optimization problems in many research and engineering fields [18], [19].

2. LITERATURE REVIEW

Naskar and Chaudhuri [20] proposed a stable encryption strategy for digital images in 2014; it can also be used for any digital data images (e.g. audio, image, and text). A block of hidden bytes is ciphered using bit-wise XORing and flipping, and then each ciphered byte is moved inside N locations (N is the secret byte size). This is a method that combines replacement and carrying using dynamic substitution box (SBOX) and transcription box (TBOX). The cryptosystem's key is very big, which makes it more secure against brute-force attacks. Furthermore, main statistical analysis, sensitivity analysis and differential attack analysis demonstrate the author's established strategies high acceptability. Kumar *et al.* [21] suggested the first double stage arbitrary matrix affine cypher paired with digital 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 remote monitoring and control (RMAC) parameter settings. 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 mean square error (MSE), indicating that the method decrypts with very little knowledge loss. Proposed strategy can be used to send RGB picture data over insecure channels easily and safely. Loukhaoukha *et al.* [22] suggested a new picture encryption strategy 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 columns and rows 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 images 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). Kumar and 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 recognize the discrete strategy of random ECC peaces with respect to a public recognized 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 area and the other on the decryption area. Data is submitted not only in image form, but also in audio, video, and image form. Bh *et al.* [24] addressed Koblitz'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.

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 random digits 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. Advanced encryption standard (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] suggested a homomorphic encryption scheme based on ant lion optimization (ALO). To increase the level of security, an approach called ALO is announced. The strong encrypted image is displayed in terms of maximum entropy with this ALO. Ewees *et al.* [4] proposed onset of blood lactate accumulation (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 suggested OBLGOA by conducting six test strategies that included 23 benchmark capacities and 4 building difficulties. The results revealed that the suggested computation produced superior results than those frequently obtained through accurate recommendations 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 utilized to transfer a private initial image from the sender to the recipient. The RGB pixel values are recognized from the base image, and a different RGB matrix is produced using their pixel parameters. After that, the picture is separated into blocks earlier 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 yield picture is compared to the base image to assess accuracy using the PSNR, correlation coefficient (CC) and mean square error (MSE). 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 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 (1).

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

Here a and b are the integers. The intensity of encryption depends on the created key in every cryptographic operation. Two forms of key generation are available in the proposed process. Firstly, public key is produced for encrypting the message from the receiver end and secondly, to create a private key to decrypt the original 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).

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

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 i and j are the number of rows and columns of the blocks of the image [12], [31]. 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 (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 cat swarm optimization (CSO) technique, which gives the best optimized values compared to the existing ECC technique.

3.1.3. Gravitational search algorithm

Gravitational search algorithm (GSA) is an observational technique focused on Newton's laws of universal gravitation, which was earlier recognized in 2009 [32], [33]. The strategy 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 (7).

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

Where, M_1 and M_2 are the masses of the two nodes and Dis 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 α 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 j^{th} 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 j^{th} node are given by (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 $k=1, 2, 3 \dots P$ and $j=1, 2, 3 \dots N$, 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 j^{th} particle. The velocity of k^{th} parameter of j^{th} 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 k^{th} parameter in j^{th} node at the instant of $t+1$ is given by (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 every iteration it is updated. The complete process of obtaining best values is depicted in Figure 1.

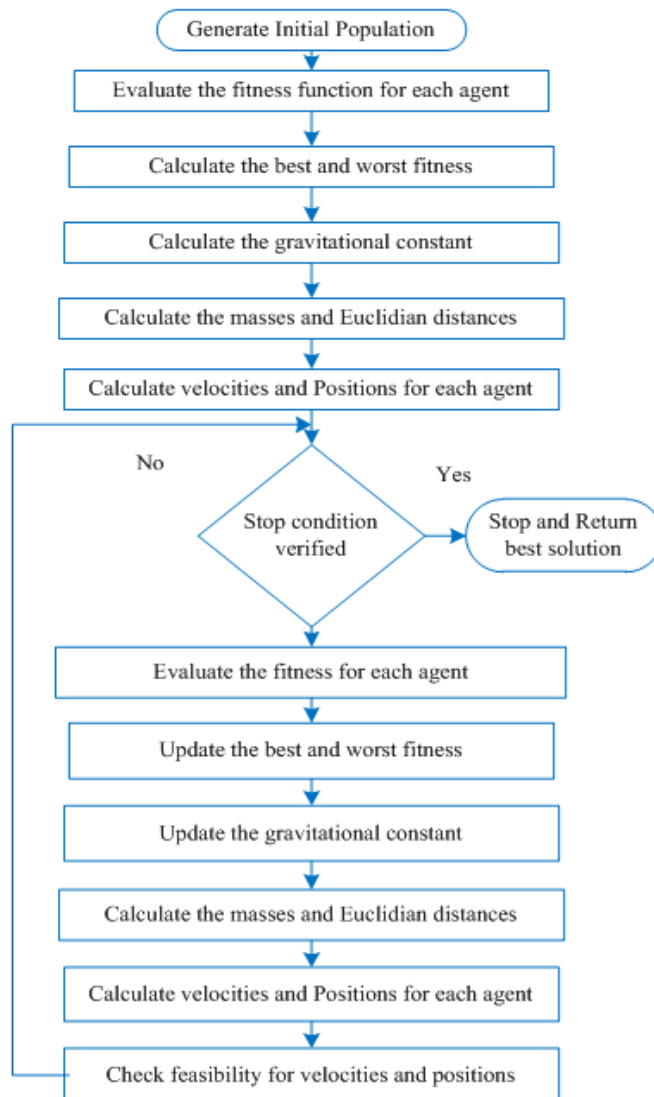


Figure 1. Flow chart representation of GSA

3 RESULTS AND DISCUSSION

This part of paper presents the experimental findings on the suggested image encryptions and optimization technique. The suggested ECC Image Encryption with GSA Optimization was 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 yield image is compared against to the genuine image to demonstrate the proposed algorithm's performance, using quality metrics such as MSE, CC and PSNR values for each image.

Table 1. ECC image encryption with GSA optimization technique for Lena image







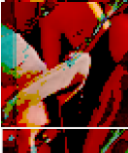

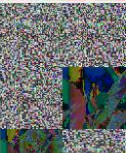
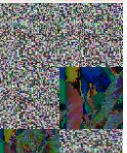
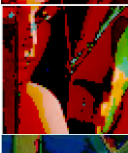
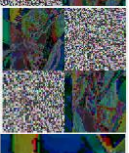
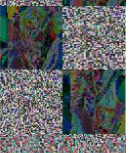

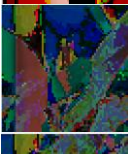
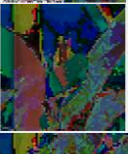


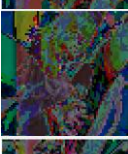



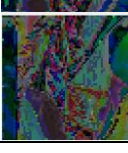
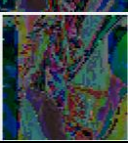
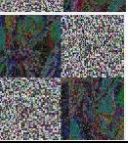
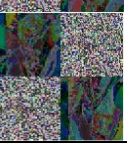
Input Image	Color band	Share creation	Combined Sharing	Encryption	Decryption	Reconstructed Output
	R1					
	G1					
	B1					
	R2					
	G2					
	B2					

Table 2. ECC image encryption with GSA optimization technique for boat image








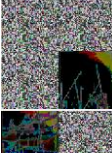
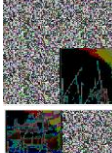
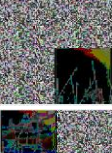
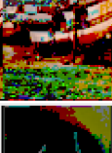
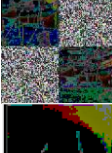

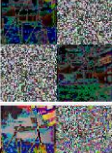
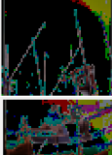
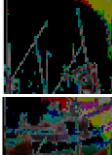

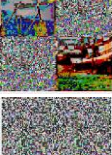
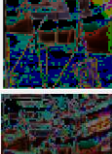
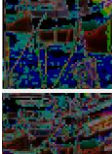
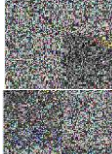
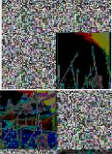




Input Image	Color band	Share creation	Combined Sharing	Encryption	Decryption	Reconstructed Output
	R1					
	G1					
	B1					
	R2					
	G2					
	B2					

Table 3 compares the proposed ECC with GSA method to the ECC technique using several critical quality indicators such as MSE, CC and PSNR 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 model with existing CSO-fruit fly optimization (FFO)-ECC. From the Table 4, it is 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 higher PSNR of 59.3 dB.

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 4. Comparison of the proposed GSA-ECC method to existing Method CSO-FFO-ECC in terms of MSE and PSNR

Input Image	Proposed GSA-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




4 CONCLUSION

The research presents an ECC-based picture encryption strategy that is optimized using GSA methodology. It is demonstrated unequivocally that the suggested approach produces a higher-quality image with an average PSNR value of 60.04 between the genuine and output images. The mean square error is likewise reduced 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 strategy outperforms ECC in terms of encryption quality and PSNR values. In the future, we will examine the suggested method's resilience to various forms of attacks such as salt and pepper, filtering, cropping, and blurring.




REFERENCES

- [1] S. Kaliswaran and M. Y. M. Parvees, "An Efficient Hybrid Optimization Algorithm with Elliptic-Curve Cryptography for Image Encryption," *European Journal of Molecular & Clinical Medicine*, vol. 07, no. 07, pp. 4753–4764, 2020, [Online]. Available: https://ejmcm.com/pdf_8322_17b371ea5a2b55a155c1f0a4e3128056.html
- [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] T. T. Ramanathan, J. Hossen, S. Sayeed, and J. E. Raja, "Survey on computational intelligence based image encryption technique," *Indonesian Journal of Electrical Engineering and Computer Science* 19, no. 3, PP. 1428-1435, 2020, doi: 10.11591/ijeecs.v19.i3.pp1428-1435.
- [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. Journal of Engineering Research and Application*, 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, [Online]: Available: <file:///C:/Users/JEC-07/Downloads/1386853.1378356.pdf>
- [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] S. R. M. Zeebaree, "DES encryption and decryption algorithm implementation based on FPGA," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 2, pp. 774-781, 2020, doi:10.11591/ijeecs.v18.i2.pp774-781.
- [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] R. K. Rao, G. Aithal, S. Shetty, and B. Kallapu, "Image Encryption Scheme in Public Key Cryptography Based on Cubic Pell's Quadratic Case," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, no. 1, pp. 385-394, 2020, doi: 10.11591/ijeecs.v20.i1.pp385-394.
- [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.
- [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 Cryptography," *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. Tahemezhadi, 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/IACSA.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," *IJCSI International Journal of Computer Science*, 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, [Online]. Available: <https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2014-2015/IJCSE10-02-05-08.pdf>
- [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," *Cybersecurity and Secure Information Systems*, pp 31-42, 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, pp. 62–70, 2018, doi: 10.14419/ijet.v7i1.5.9124.
- [30] S. 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.




BIOGRAPHIES OF AUTHORS

Ramireddy Navatejareddy    has obtained his B.Tech in information technology from Jawaharlal Nehru Technological University, Hyderabad, Andhra Pradesh, India in 2007 and M.Tech in Computer Science & Engineering from Visvesvaraya Technological University, Karnataka State, India in 2010. He has teaching experience of 10+ Years in the department of Computer Science & Engineering. Currently he is pursuing Ph.D in Koneru Lakshmaiah Education Foundation-KLEF. His research areas of interest are computer networks & security, IoT, cloud computing. He can be contacted at email: ramireddynavateja@gmail.com.



Muthukuru Jayabhaskar    has 7+ years of industry and 7+ years of teaching experience and has interests in real time issues in Networks which lead to research in Network and Data Security and further implementation of different security techniques like cryptography and signcryption. He published 20 papers in reputed journals. He completed his Ph.D on Elliptical Curve Cryptography Implementation Approaches for Efficient Smart Card Processing from Sri Krishnadevaraya University. He can be contacted at email: jayabhaskar@kluniversity.in.



Bachala Sathyanarayana    has 31 years of teaching experience and has interests in the area of security issues in Computer Networks and internet of things. He published 57 papers in reputed journals. He served as a chair. He guided 16 Ph.D, 5 M.Phil students and guiding 3 Ph.D students. Currently working as professor in the department of Computer Science and technology in Sri Krishnadevaraya University, Ananthapuramu, A.P, India. He can be contacted at email: bachalasadatya@yahoo.com.