iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 11 **Issue:** VIII **Month of publication:** Aug 2023

**DOI:** https://doi.org/10.22214/ijraset.2023.55220

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com*

# Analysis of Parameters Influencing the Performance of Digital Image Encryption using ECC

Farhan Ahmed Saleem[1], Vibhakar Mansotra[2]
[1]*M Tech Student,* [2]*Professor, Dept. of Computer science and IT, Jammu University, Jammu, India*

***Abstract:*** ***Digital images are widely used in various domains, including social media, military, and healthcare. However, the security of digital images is threatened by cyber-attacks and privacy concerns. Cryptography plays a crucial role in ensuring the privacy and integrity of data, including digital images. Encryption methods are employed to protect digital images from unauthorized access. Among these methods, elliptic curve cryptography (ECC) is particularly effective, offering robust security with shorter key lengths. This research paper analysis ECC-based encryption methods for digital image encryption, considering parameters that impact their performance.***
***Keywords: ECC, ASE, ECC, UACI, NPCR Entropy***

## I. INTRODUCTION

Billions of digital images are shared on messaging apps and social media every second. However, these images face security threats like alteration, illegal acquisition, and data disclosure. To minimize damages caused by malicious parties, encryption, steganography, and watermarking methods are used. Image encryption converts original images into unrecognizable encrypted versions, ensuring security and privacy.

This technique finds applications in medical imaging, communication, multimedia, and various other domains where data protection is crucial. The main objectives of encryption are confidentiality, integrity, and non-repudiation. These criteria play a crucial role in selecting an encryption method.

Encryption methods can be categorized into symmetric, asymmetric. Symmetric encryption employs a single private key, which is used by both the sender and receiver for encryption and decryption. Examples of symmetric encryption methods include AES, DES, and Hill cipher. While symmetric encryption is simple and fast, sharing the key securely among a large number of users can be challenging and inefficient. Asymmetric encryption, also known as public-key encryption, involves the use of two keys: a public key and a private key. Mathematical methods are used for key exchange. The Diffie-Hellman key exchange is an example of a solution to the key exchange problem. Public key encryption methods, such as RSA and ECC, utilize public and private keys for encryption and decryption. Digital image encryption differs significantly from text encryption, as there are additional parameters and considerations specific to image encryption these parameters are Entropy, PSNR, UACI etc.

## II. DEFINITION

### *A. Image*

A digital image is a collection of pixels arranged in a grid, with each pixel representing a small unit of colour or intensity. The image can be represented by a matrix, where rows and columns correspond to pixel values, capturing the colour or intensity information. There are three main types of digital images: binary, grayscale, and colour (RGB)

### *B. Elliptic Curve Cryptography (ECC)*

Elliptic Curve Cryptography (ECC) is a public key encryption method introduced by Koblitz and Miller in 1985. ECC has gained popularity due to its strong security and ability to achieve the same level of security with shorter key sizes compared to other encryption methods like RSA. ECC operations are performed on finite fields, which offer more precise and efficient results. To understand ECC, let's consider an elliptic curve denoted as E(a, b) on a finite field Fp. Here, 'a' and 'b' are integers that are smaller than a sufficiently large prime number 'p'. The equation defining the elliptic curve is given as follows: $y2 = x3 + ax + b(modp)$

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com*

*1) Point Addition*

Point addition is an operation that performs addition of two points J and K that lies on an elliptic curve to compute another point L on the same elliptic curve.

Geometrical Explanation

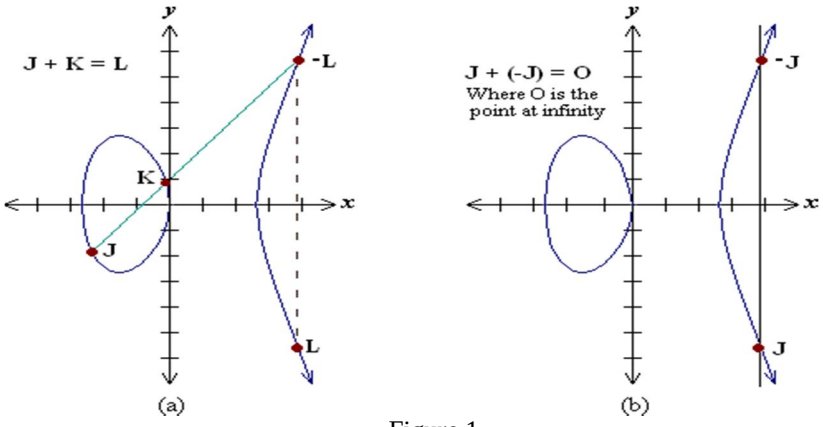



Figure 1

Intersect the elliptic curve at exactly one more point –L. The reflection of the point –L with respects to x-axis produces another point L, which contains the result of addition operation of points J and K.Thus on an elliptic curve L = J + K.

If K = -J the line through this point intersect at a point at infinity O. Hence J + (-J) = O. This is shown in figure (b). O is the additive identity of the elliptic curve group. A negative of a point is the reflection of that point with respect to x-axis.

*2) Point doubling*

Point doubling is an operation that performs addition of a point J to itself that les on the elliptic curve to produce another point L on the same elliptic curve.

Geometrical explanation

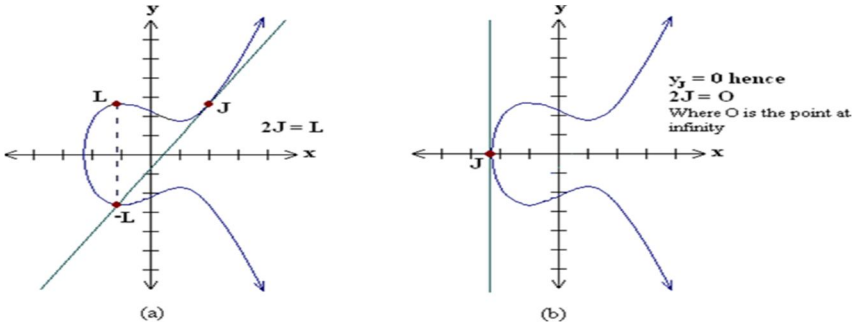



figure 2

To double a point J to get L, i.e. to find L = 2J, consider a point J on an elliptic curve as shown in fig2 (a). If y coordinate of the point J is not zero then the tangent line at J will intersect the elliptic curve at exactly one more point –L. The reflection of the point –L with respect to x-axis gives another point L, which contains the result of doubling the point J. Thus L = 2J

## III. ELLIPTIC CURVE DIFFIE–HELLMAN (ECDH) KEY EXCHANGE

*1)* User A generates its random secret key, $n_A$. A then computes the public key $P_A$ using his private key, nA. and generator point, G on the curve as,

PA = nA ∗ G

and sends it to user B.

*2)* User B generates its random secret key, nB. B then computes the public key PB using his private key, nB and generator point, G on the curve as,

PB = nB ∗ G

and sends it to user A

*3)* Both the users A and B compute the shared ECDH key,

*4)* User A

$U_A = nA * PB = nA * nB * G$ (8)

*5)* USER B

$U_B = nB * PA = nB * nA * G$

## IV. IMAGE ENCRYPTION

Image Encryption using ECIES

*1) Scheme 1 EC-AES Encryption*

The image data is encrypted using the AES encryption algorithm with the secret key derived from ECC.

*2) Scheme 2 XOR based Encryption*

*a) Original Message (Plaintext):* The message that needs to be encrypted is divided into individual bytes (groups of 8 bits). Each byte represents a character or data unit in the message.

*b) Secret Key:* The fixed-length secret key, obtained from the shared ECC key, is also divided into individual bytes.

*c) XOR Operation:* For each byte of the message, the corresponding byte of the secret key is used to perform the XOR operation. This means that each bit of the byte in the message is XORed with the corresponding bit in the byte of the secret key.

*d) Ciphertext (Encrypted Message):* The result of the XOR operation for each byte forms the encrypted byte of the ciphertext.

*e) Cyclic Use of Secret Key:* If the message is longer than the secret key, the secret key is used cyclically to ensure that the encryption process continues consistently. This means that once the secret key is used completely, it starts from the beginning, effectively forming a loop

## V. IMAGE DECRYPTION

*1) Scheme 1 (EC-AES) Decryption*

The image data is decrypted using the AES encryption algorithm with the secret key derived from ECC.

*2) Scheme 2 XOR Based Decryption*

*a) For Each Byte in the Ciphertext:* The decryption process loops through each byte of the encrypted message (ciphertext).

*b) XOR Operation with Secret Key:* For each byte of the ciphertext, the corresponding byte from the secret key is used in the XOR operation. This means that each bit of the byte in the ciphertext is XORed with the corresponding bit in the byte of the secret key.

*c) Decrypted Byte:* The result of the XOR operation for each byte produces the original byte of the plaintext message.

*d) Final Decrypted Message:* The decrypted bytes, obtained through the XOR operation, are combined to reconstruct the original plaintext message

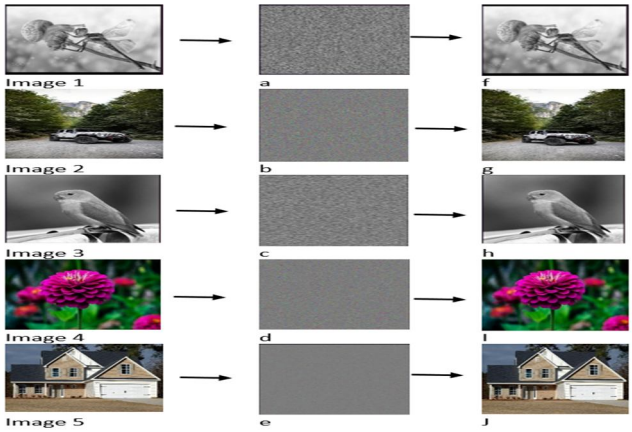
## VI. RESULT ANALYSIS

The implementation is performed on Ryzen 7 CPU 2.20 GHz hp laptop with 8 GB RAM using python. The Elliptic curve used here is the 256-bit Standard Elliptic curve given by ECC brainpoolP256r1

*A. Image description*

Table 1 (Image(1,3)—grayscale image , image(2,4,5) RGB image )

| | Image 1 | Image 2 | Image3 | Image 4 | Image 5 |
|---|---|---|---|---|---|
| size | 480, 360 | (1000, 1500) | (1286, 1500) | (6000, 4000) | (2974, 1950) |
| Resolution | 96dpi | (72)dpi | 72dpi | 72dpi | 72dpi |



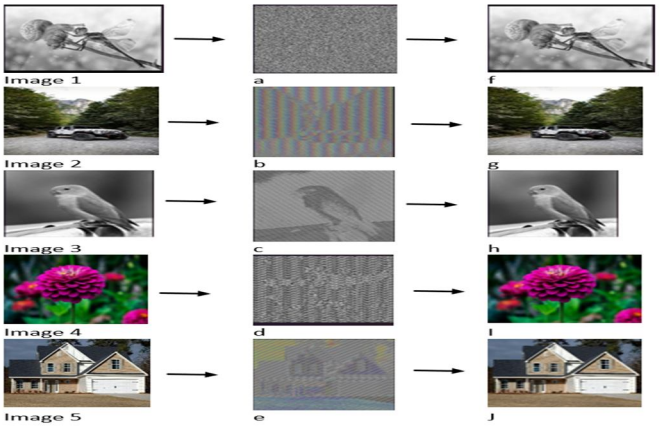




Figure 3 Image (1-5) plain image, (a-e) corresponding encrypted image, (f-j) decrypted image, using scheme1.
Figure 4 Image (1-5) plain image,(a-e) corresponding encrypted image,(f-j) decrypted image, using scheme 2.

### *B. Unified Average Changing Intensity (UACI)*

UACI is used to measure the average intensity of difference between two encrypted images which their plain images have one pixel difference.

| | Image 1 | Image 2 | Image3 | Image 4 | Image 5 |
|---|---|---|---|---|---|
| Schemes 1 | 33.38 | 35.7 | 33.12 | 37.85 | 33.56 |
| Schemes 2 | 29.90 | 34 | 30 | 35.26 | 32.81 |

Table 2

### *C. Normalized Pixel Change Ratio (NPCR)*

It is defined as different pixel numbers of two encrypted images which their plain images' whole pixels are same but one pixel is different

| | Image 1 | Image 2 | Image3 | Image 4 | Image 5 |
|---|---|---|---|---|---|
| Schemes 1 | 99.7 | 99 | 98 | 99.3 | 99.6 |
| Schemes 2 | 99 | 97 | 96 | 95 | 93 |

Table 3

### *D. Correlation coefficient (CC)*

Correlation coefficient (CC) is a statistical measure of the degree to which changes to the value of one variable predict change to the value of another.

| | Image 1 | Image 2 | Image3 | Image 4 | Image 5 |
|---|---|---|---|---|---|
| Schemes 1 | 0.0030 | 0.00029 | 0.0001 | 0.007 | 0.000105 |
| Schemes 2 | 0.04 | 0.05 | 0.1 | 0.08 | 0.03 |

Table 4

### *E. Information Entropy*

Information entropy is a measure of the uncertainty or randomness of a message

| | Image 1 | Image 2 | Image3 | Image 4 | Image 5 |
|---|---|---|---|---|---|
| Schemes 1 | 7.99 | 7.86 | 7.848 | 7.99 | 7.83 |
| Schemes 2 | 7.6 | 7.11 | 7.13 | 7.83 | 7.67 |

Table 5

*F. Bit Correct Ratio (BCR)*

BCR is used to calculate the difference pixels between a plain image and decrypted image

| | Image 1 | Image 2 | Image3 | Image 4 | Image 5 |
|---|---|---|---|---|---|
| Schemes 1 | 1.0000 | 1.0000 | 1.0000 | 1.0000 | 1.0000 |
| Schemes 2 | 1.0000 | 1.0000 | 1.0000 | 1.0000 | 1.0000 |

Table 6

*G. Mean Squares Error (MSE)*

MSE and RMSE is used to calculate the true pixel values of a plain image to decrypted image. The error is total of the plain image pixel values that different from the decrypted image

| | | Image 1 | Image 2 | Image3 | Image 4 | Image 5 |
|---|---|---|---|---|---|---|
| Schemes 1 | MSR | 0 | 0 | 0 | 0 | 0 |
| | RMSR | 0 | 0 | 0 | 0 | 0 |
| Schemes 2 | MSR | 0 | 0 | 0 | 0 | 0 |
| | RMSR | 0 | 0 | 0 | 0 | 0 |

Table 8

*H. Time complexity*

Encryption time(ET) Decryption time(DT)

| | | Image 1 | Image 2 | Image3 | Image 4 | Image 5 |
|---|---|---|---|---|---|---|
| Schemes 1 | ET | 0.08 | 0.05 | 0.06 | 0.05 | 0.078 |
| | DT | 0.04 | 0.03 | 0.07 | 0.06 | 0.04 |
| Schemes 2 | ET | 0.05 | 0.03 | 0.02 | 0.03 | 0.01 |
| | DT | 0.01 | 0.01 | 0.02 | 0.03 | 0.02 |

Table 9 All the time in seconds

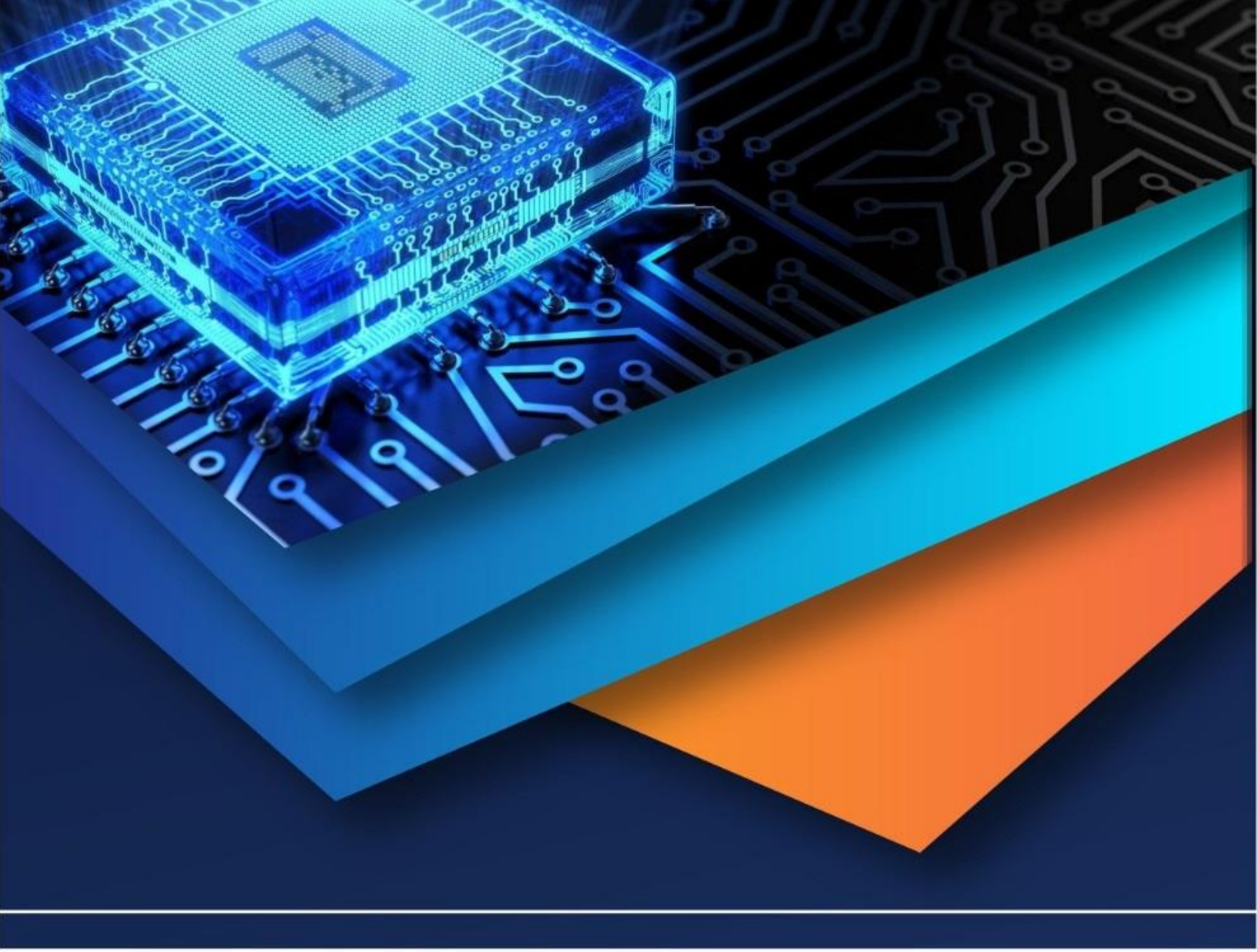
## VII. CONCLUSION

In the paper titled" Analysis of Parameters Influencing the Performance of Digital Image Encryption using ECC" the authors focus on the utilization of ECC (Elliptic Curve Cryptography) in image encryption. ECC has gained significant popularity due to its advantageous features, including short key sizes and low power consumption. As a result, it has found widespread use in various fields, particularly in image encryption. When evaluating the quality of digital image encryption, numerous parameters are considered. These parameters include entropy, NPCR (Number of Pixels Change Rate), and NPCR, ENTROPY etc. It is important for these parameters to exhibit optimal values in the encrypted image. In the paper, two techniques are explored for image encryption using ECC Schemes1 and schemes2. Scheme 2 offers better time complexity and both schemes successfully preserve the integrity of the decrypted images. Scheme 1's higher information entropy and weaker statistical relationship with the original images make it the preferable choice for achieving higher security in encryption.

## REFERENCES

[1] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," Archives of Computational Methods in Engineering 27.1, 15-43, 2020.
[2] F. Y. Shih, "Digital watermarking and steganography: fundamentals and techniques," CRC press, 2017
[3] G.Ye, M. Liu, and M. Wu. "Double image encryption algorithm based on compressive sensing and elliptic curve," Alexandria Engineering Journal 61.9, 6785-6795, 2022.
[4] Z. E. Dawahdeh, S. N. Yaakob, and R. R. bin Othman. "A new image encryption technique combining elliptic curve cryptosystem with hill cipher," Journal of King Saud University-Computer and Information Sciences 30.3, 349-355, 2018.
[5] M.Benssalah, Y. Rhaskali, and K. Drouiche. "An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography," Multimedia Tools and Applications 80.2, 2081- 2107, 2021.
[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982]. [7]Habek, M., Genc, Y., Aytas, N., Akkoc, A., Afacan, E., Yazgan, E. (2022, June 9). Digital Image Encryption Using Elliptic Curve Cryptography: A Review. 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)

[7] Singh, L. D., & Singh, K. M. (2015). Image Encryption using Elliptic Curve Cryptography. Procedia Computer Science, 54, 472–481. https://doi.org/10.1016/j.procs.2015.06.054
[8] Somaraj, S., & Hussain, M. A. (2015, December 29). Performance and Security Analysis for Image Encryption using Key Image. Indian Journal of Science and Technology, 8(35). https://doi.org/10.17485/ijst/2015/v8i35/73141
[9] Gupta, K., & Silakari, S. (2010, November). Performance Analysis for Image Encryption Using ECC. 2010 International Conference on Computational Intelligence and Communication Networks. https://doi.org/10.1109/cicn.2010.26
[10] Parida, P., Pradhan, C., Gao, X. Z., Roy, D. S., & Barik, R. K. (2021). Image Encryption and Authentication With Elliptic Curve Cryptography and Multidimensional Chaotic Maps. IEEE Access, 9, 76191–76204. https://doi.org/10.1109/access.2021.3072075



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY