ISSN: 2584-0495 Vol. 1, Issue 3, pp.156- 162

International Journal of Microsystems and IoT

ISSN: (Online) Journal homepage: https://www.ijmit.org

An Intelligent Secure Image Transmission System Using Elliptic Curve Cryptography

Shaik Hedayath Basha, C Arun, Jai Ganesh Sekar, N Nimitha, Sai Kiran Tatineni

Cite as: Shaik Hedayath Basha, C Arun, Jai Ganesh Sekar, N Nimitha, & Sai Kiran Tatineni. (2023). An Intelligent Secure Image Transmission System Using Elliptic Curve Cryptography. International Journal of Microsystems and IoT, 1(3), 156-162. https://doi.org/10.5281/zenodo.8359476

Published online: 21 August 2023.

DOI: https://doi.org/10.5281/zenodo.8359476

International Journal of Microsystems and IoT
Vol. 1, Issue 3, pp. 156-162; DOI: https://doi.org/10.5281/zenodo.8359476

An Intelligent Secure Image Transmission System Using Elliptic Curve Cryptography

Shaik Hedayath Basha[1], C Arun[1], Jai Ganesh Sekar[1], N Nimitha [1], Sai Kiran Tatineni[2]

[1]Department of Electronics and Communication Engineering, RMK College of Engineering and Technology, Chennai, India.

[2] Pharmaceutical Distribution Administrator, Cardinal Health, Dublin-Ohio-USA

ABSTRACT

In the fast-changing and developing world, it is very much essential to have a fast, secure intelligent communication system for data transmission. In the proposed work the author designed a traditional intelligent secured software-based digital image transmission system with elliptic curve cryptography and Diffie-Hellman key exchange protocol with smaller key size. Secret key is shared intelligently using the Diffie-Hellman key exchange protocol between the two end-users. The encryption process of the digital image is done on every pixel value of an image using an intelligent mapping table and hence it is very secure against an intruder. The decryption process is done pixel-wise using the same intelligent mapping table and secured shared keys by the authentic sender, the average process of image encryption and decryption takes 45.3210 seconds. The vulnerability of the intelligent communication system is verified using various active and passive attacks. Proposed work is robust to passive attacks like eavesdropping attack, network analysis, and traffic analysis also to the repudiation active attack. It is semi-fragile to active attacks like modification of messages, denial of service, and masquerade.

KEYWORDS

Attacks; Elliptic curve cryptography (ECC); Encryption; Decryption; Diffie-Hellman key exchange protocol (DHKEP); Intelligent mapping; Security.

1. INTRODUCTION

Intelligent technology is one of the promising subjects of research and development in the field of cybernetics and information science [9]. Elliptic curves were autonomously applied by Miller and Koblitz in 1985 [10].

ECC is a public key encryption technique used to compact and systematic cryptographic keys. ECC provides very good security to the digital content.

The elliptic curve is obtained from algebraic cubic equation with modular operation. Mainly ECC works by creating an equation from the arithmetic group derived from the points where the line intersects the axes.

Equations based on elliptic curves are very valuable as it can perform forward processes but extremely difficult to turnaround.

1.1 Elliptic Curve Computation

In mathematics, an elliptic curve is a plane algebraic curve defined by equation (1) of the form,

$$y^2 \text{ mod } P = (x^3+ax+b) \text{ mod } P \qquad (1)$$

'a' and 'b' are the constants satisfying the below condition,

$$4a^3 + 27b^2 \neq 0 \qquad (2)$$

The equation (2) is called the Weierstrass normal form for elliptic curves, which is non-singular, that is, the curve has no points or self-intersections.

Comparing security of RSA 3072-bit is almost equivalent to 256-bit ECC private key.

ECC is a trap door function, which is used in public-key cryptography, it means finding the secret keys from the sender 'A' to receiver 'B' is easy but finding the secret keys from the receiver 'B' to the sender 'A' is infeasible.

ECC relies on the concept of Point Multiplication, Q = nP. If 'P' is the point on the curve (1) then another point on the curve (1) is obtained from continues addition using (3), (4) and (6). If two points on the curve are different the third point is obtained using (3), (4) and (5).

The special addition operation 'O' is called point at infinity. If '3' points are on a line intersect an elliptic curve, the sum is equal to this point at infinity O. There are various operations performed on an elliptic curve the following major two operations called addition operation and doubling operation and it is given in the next section with the required equations and formulae. It is necessary to follow the mathematical steps to obtain the points in the defined elliptic curve [10]. Let the points P = (x_1, y_1) and Q = (x_2, y_2) be in the elliptic group E_p(a, b)and 'O' is the point at infinity.

The rules for addition over the elliptic group E_p (a, b) are as follows:

a) P + O = O + P = P

b) If x2 = x1 and y2 = –y1, that is P = (x_1, y_1) and Q =

(x_2, y_2) = (x_1, –y_1) = –P, then P + Q = O

c) If Q ≠ – P, then the sum, P + Q = (x_3, y_3), the values of x_3 and y_3 are calculated using (3), (4), (5), and (6)

$$x_3 = (\lambda^2 - x_1 - x_2) \text{ mod } P \qquad (3)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \text{ mod } P \qquad (4)$$

if $P \neq Q$,
$\lambda = (y_2 - y_1)/(x_2 - x_1)$ (5)
if P = Q,
$\lambda = (3x_1^2 + a)/2y_1$ (6)

1.2 Doubling Operation

Given the point P (x_1, y_1) on the elliptic curve here point doubling is the addition of a point ‘P’ itself to obtain another
point as ‘2P’ on elliptic curve. The tangent line at ‘P’ will intersect the elliptic curve at exactly one more point ‘–S’. The reflection of the point ‘–S’, gives the point ‘S’ as the doubling point of the point P only if the y-axis of the point ‘P’ is non-zero.
For $P \neq -P$, 2P is given by (x3, y3). The two users must be aware of the parameters related to the ECC. For one successful communication through ECC, it requires an elliptic curve which is chosen based on the three parameters ‘a’, ‘b’, and ‘P’. The values a and b need to satisfy equation 2. The value P (Prime number) decides the creation of the elliptic points table based on the above three parameters, the ECC curve is created, and the curve points are stored in the table Ep (a, b). This table is resized to the size of the image; the points are in cyclic order.

2. RELATED LITERATURE WORKS

In recent years many researchers have developed various techniques in the field of ECC for the security of data. K. Shankar and P. Eswaran [1] proposed image encryption using the Differential Evolution (DE) method and performed an optimization process.

Ali Soleymani [2] focuses on the various designs of image cryptosystem. Different techniques and security analysis methods for encrypted images are mentioned.

Kinani and Amounas proposed a mapping model method based on matrix properties used for the alphanumeric characters only [3].

There is an alternate method developed based on the matrix by Amounas for securing text data [4]. S. Gupta [5] provided image transmission in the medical field was the image act as plaintext after compression and then encrypted. Parma Nand Astya and Bhairvee Singh [6] performed image encryption and decryption by converting an image as a stream of bits and creating it as various grids which give pixel’s intensity. These are mapped into elliptic curve points. O.S. Rao and S.P. Setty [7] suggested on the plain message using two mapping methods.

The first method was very weak known to be static mapping another was that various steps were available for a single character to select as a point, but it increases complexity, usually Elliptic curve cryptography is compared with RSA algorithm based on the key size, time of execution, memory. Table1 shows the comparison of RSA, Elgamal and ECC with various important parameters.

Table. 1 Comparison – Key Sizes

Parameter	RSA	ELGAMAL	ECC
Key Generation (bits)	024 - 15360	024 - 15360	163 - 571
Security	Medium	High	Very High
Time Taken (sec)	166.078	166.078	0.522
Memory usage (bytes)	1091	1091	124.3
Latency (ms)	381	381	101.9

Ali S et al., [8] has proposed a new technique to use mapping method. They convert pixels of images to coordinates of the Elliptic curve. Larry [9] in a book by the name Hybrid Intelligent System explained about the development of intelligent technologies. Shaik Hedayath Basha and Jaison B in [10] explain a new method of message transmission system using a convolution wheel concept using ECC.
Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh [11] explain image encryption and decryption using ECC. Mehrabi [12] proposed residue number systems based ECC using two standard curves short weierstrar and twisted Edwards curves in Xilinx and reduced the time for the multiplication process in ECC. In [13] raw RGB images are encrypted by 15 different encryption keys.

K. Sowjanya in [14] uses 160 bits of ECC to provide security and strength for IoT applications. Almajed in [15] provides the several encryption schemes with the analysis.

In [16] efficient ECC was proposed with the throughput 60MBPS. Piljoo Choi in [17] proposed ECC processor - 180nm-CMOS technology to perform 256 bits multiplications and have better throughput.

In [18], backdoor concepts were discussed and implemented Secretely embedded Trapdoor with Universal protection.

In [19] Vijaykumar K proposed a method which provides continuous security to the applications entering in the cloud environment.

In [20, 21] RGB image encryption and decryption is done two times first time using 2D chaotic mapping and second time using ECC, the PSNR between encrypted and input color image values of 7 images ranges from 6.5454 to 9.2440.

As per the knowledge of the authors encryption and decryption of the color image is done using ECC in various ways. In the proposed work the main importance is given to reducing the key size with better security.

So, in this proposed work, the image encryption and decryption are based on the intelligent mapping model using ECC and DHKEP, in which every pixel of an input image is converted into elliptic curve points, that is every pixel is mapped to the elliptic point in the defined mapping table, the same is used for both encryption and decryption processes.

3. PROPOSED ECC IMAGE ENCRYPTION AND DECRYPTION

To overcome the challenges faced in the RSA algorithm and other methods used in ECC, we have proposed this method which is very efficient and fast compared to RSA. In the proposed work RSA and Diffie-Hellman key exchange algorithms are combined.

Suppose if two users want to communicate with each other through images first they follow the Diffie-Hellman key exchange to establish secure communication between them where the secret key is shared.

Let us consider two users as ‘X’ and ‘Y’, choose a number ‘P’ a prime number and, calculate ‘G’, which is a generator or primitive roots of ‘P’. ‘P’ and ‘G’ are shared in the public domain.

Let ‘X’ user select a private number secret number ‘a’ and user ‘Y’ select another private or secret number ‘b’ as it’s a secret integer.

Both users’ ‘X’ and ‘Y’ multiply their secret key with the generators and their shared key which in the public domain and is given in (7) and (8).

$$Q_x = (a * G) \bmod P \quad (7)$$

$$Q_y = (b * G) \bmod P \quad (8)$$

Where Q_x and $Q_y$are the shared keys exchanged between the two user’s ‘X’ and ‘Y’. Now ‘X’ and ‘Y’ exchange the computed values Qx and Qy to ‘Y’ and ‘X’.

Let Q_{x1} (9) and Q_{y1} (10) are the quantities at ‘X’ and ‘Y’.

$$Q_{x1} = a * Q_y \bmod P \quad (9)$$

$$Q_{y1} = b * Q_x \bmod P \quad (10)$$

Using equation (11) private keys of ‘X’ and ‘Y’ can be calculated at ‘Y’ and ‘X’.

$$M_{xy} = Q_{x1} = a * (b * G) = b * (a * G) = Q_{y1} \quad (11)$$

3.1 Elliptic Curve Points – Intelligent Mapping Table

The elliptic curve points are obtained using mathematical modeling, for example, let the prime number P = 19 and the constants ‘a’ and ‘b’ are –1 and 188.

Here first verify whether the constants ‘a’ and ‘b’ are satisfying equation ‘2’. Substituting the values of ‘a’ and ‘b’ in (2), the value is ‘9’ which is not equal to ‘0’.

The quadratic residues of Q_{19} are shown in table 2 and Table 3. The reduced set of is shown in the set of Z_{19} in (12).

$$Z_{19} = \{0, 1, 2, 3, . . . ,18\} \quad (12)$$

Therefore, the set of (P – 1) / 2 = 9, quadratic residues are shown in (13).

$$Q_{19} = \{1, 4, 5, 6, 7, 9, 11, 16, 17\} \quad (13)$$

Table. 2 Calculation of Quadratic residues of Q_{19}

$OUT_1 = X^2$Mod P	$OUT_2 = (P-X)^2$Mod P	$OUT_1 = OUT_2$
1^2 mod 19	18^2 mod 19	1
2^2 mod 19	17^2 mod 19	4
3^2 mod 19	16^2 mod 19	9
4^2 mod 19	15^2 mod 19	16
5^2 mod 19	14^2 mod 19	6
6^2 mod 19	13^2 mod 19	17
7^2 mod 19	12^2 mod 19	11
8^2 mod 19	11^2 mod 19	7
9^2 mod 19	10^2 mod 19	5

Table 3 shows the obtained Elliptic curve points.

Table. 3 Elliptic Curve Points

X	Y^2	Y2 cQ_{19}	Y_1	Y_2
0	17	yes	6	13
1	17	yes	6	13
2	4	yes	2	17
3	3	no	-	-
4	1	Yes	1	18
5	4	Yes	2	17
6	18	no	-	-
7	11	Yes	7	12
8	8	No	-	-
9	15	No	-	-
10	0	no	-	-
11	7	yes	8	11
12	4	yes	2	17
13	16	yes	4	15
14	11	yes	7	12
15	14	no	-	-
16	12	no	-	-
17	11	yes	7	12
18	17	yes	6	13

The group E_P (a, b) = E_{19}(1, 1) thus includes the points (10, 0). These points in (14) ultimately form the mapping table required for the elliptic curve cryptography of images, as these points are used to map the encrypted pixel values from the mapping table.

These mapping table values are intelligent based on the values of ‘P’, ‘a’, and ‘b’, where the values could be dynamically changing randomly depending upon the look-up table shared between the two entities.

$$E_P(-1,188) = \left\{\begin{matrix} (0,6) & (0,13) & (1,6) & (1,13) \\ (2,2) & (2,17) & (4,1) & (4,18) \\ (5,2) & (5,17) & (7,7) & (7,12) \\ (11,8) & (11,11) & (12,2) & (12,17) \\ (13,4) & (13,15) & (14,7) & (14,12) \\ (17,7) & (17,12) & (18,6) & (18,13) \end{matrix}\right\} \qquad (14)$$

Figure 1 shows the comparison of mapping with [15].

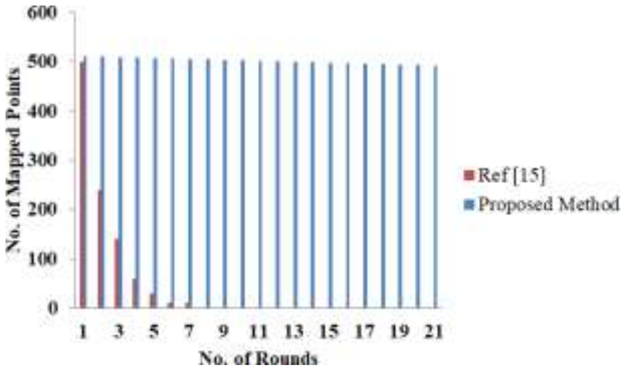

Fig. 1 Comparison of Mapping Points with existing work

3.2 Image Encryption

Consider a grayscale image of size (M x N). Every pixel of image is used to obtain a message point (say P_M). For example, if the pixel intensity value is 225 corresponding point for this pixel in the mapping table of E_{2789} (–1, 88) is given by P_M = (130, 1779). The obtained point is now encrypted using the (15) of ECC.

$$P_C = [(kG), (P_M + kP_B)] \qquad (15)$$

‘k’ is a random number, G is the generator point it is any point in the elliptic group commonly shared between two parties,‘P_B’ is the private key of receiver or Bob key in general.In the above example k = 113, G = (0, 150) and P_B = (247, 1095), then P_C value is obtained by substituting above values in (13), P_C = [446, 1984]. The obtained point $P_C$is mapped in the intelligent mapping table and the corresponding pixel is obtained in the original image, the pixel value for the above example is 231. Therefore, the original image intensity value 225 is replaced with 231 using the intelligent mapping table. The process is done for every pixel value of the image and the image encryption algorithm is explained in the next preceding section with which the encryption process gets completed successfully.

3.2.1 *Image Encryption Algorithm*

Step 1 Select the prime number, constants ‘a’ and ‘b’ satisfying (2).

Step 2 Determine the quadratic residues QP for all x, such that $0 \leq x \leq P$

Step 3 Compute (16)

$$y^2 \bmod P = (x^3+ax+b) \bmod P \qquad (16)$$

Determine y^2 is in the QP, if so, append the points to the elliptic group E_P (a, b).

Step 4 Resize the elliptic group E_P (a, b) to generate the mapping table containing the size of the original image M x N.

Step 5 Every pixel in the image, map a point in the intelligent mapping table, say as P_M.

Step 6 The point P_M is now encrypted by using (15).

Step 7 The encrypted point (PM + kPB) is now searched in the intelligent mapping.

Step 8 Table using jump search algorithm for optimization and its corresponding pixel value is taken and the new point is the corresponding encrypted pixel intensity value.

Step 9 Repeat Step 5 to Step 7 for all the pixels in the original image until the entire pixel values gets encrypted using the intelligent mapping table.

3.3 Image Decryption

The Encrypted image is obtained, and each pixel is mapped to the corresponding point in the table, says P_M as per the above example the encrypted pixel intensity value is 231 and the corresponding point in the intelligent mapping table is P_C = [446, 1984]. The point P_M is now decrypted by using (17).

$$P_D = [(P_M + k\,P_B) - [nB(kG)]] \qquad (17)$$

Where P_M is the point obtained from the encrypted image, $P_B$is the Public key of Bob (receiver), n is the private of Bob (receiver).

The same example and solve P_D point using the above (15). After calculating the value of P_D is [130, 1779]. The obtained point is now mapped to the corresponding pixel in the elliptic group table. Continuing with the same example the point P_D is mapped to the pixel value of 135. Hence the encrypted pixel is decrypted successfully.

3.3.1 Image Decryption Algorithm

Step 1 Take the encrypted image and select a pixel from it (encrypted pixel).

Step 2 Select the point corresponding to that pixel from the Mapping Table which is of the form (P_M + kP_B).

Step 3 Obtain the message point P_M by using (17).

Step 4 The point PM is now mapped in the table and the corresponding pixel value is taken which is the original pixel value.

Step 5 Repeat step 1 to step 4 for all the pixels of the encrypted image, till we get the decrypted image or the original image.

The Encrypted and decrypted images using the above algorithms is shown in Figure2.

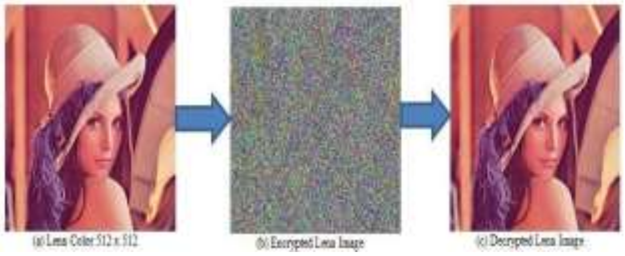

Fig. 2 Input Lena Color Image (512 x 512), (b) Encrypted Image and (c) Decrypted Image

4. RESULTS

In this proposed work an image is first converted into pixels and then encrypted using ECC mapping technique. It has been implemented in Python language. Thus, the decryption algorithm completely retrieves the original image from the encrypted image. The PSNR (Peak Signal to Noise Ratio) was found to be infinity decibels. So, there is no loss in the recovery of the original input image during the decryption process.

Figure 1(a) shows the input Lena original image of size 512 x 512 pixels, Figure 1 (b) is the encrypted image with same sizes as the input image, and Figure 1(c) shows the decrypted image. Table 4 shows that, with less key size, the entropy is attained is near to '8' which is reasonably very good.

Table. 4 Comparison of Parameters with the existing works

Parameters	[11]	[20]	Proposed Work
Key Size	512 bits	1111 (Values)	113 (Value) 8 bits
Entropy Analysis	7.99986	7.9887	7.988
Encryption time (sec)	2.47	5.1559 (encryption and decryption)	17.523
Decryption time (sec)	1.58		19.560

The processing time was very high compared with the existing method because the encryption and the decryption track the intelligent table and replace the input image intensity value with the cipher value for every pixel.

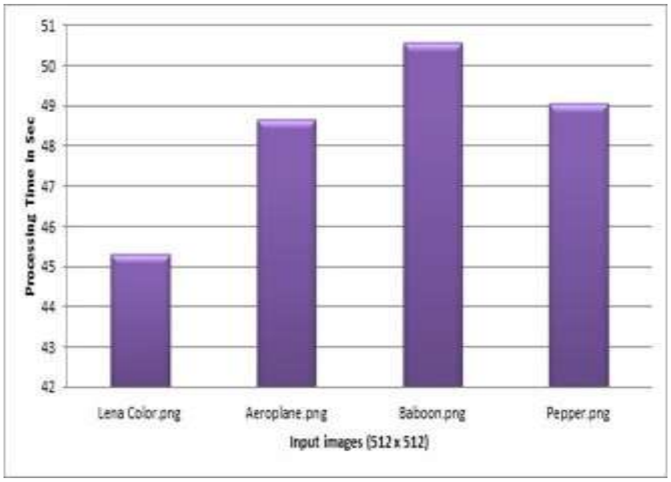

Fig. 3 Processing time of 4 standard RGB images in seconds

5. CONCLUSION

Raw color images are encrypted and decrypted using ECC and DHKEP. The PSNR of the original image and encrypted image is around 8.978. The SSIM of the original and the decrypted image is 1.

The proposed work uses very few key sizes with greater security with the intelligent mapping table. The latency of the proposed work is more compared with the other proposed work due to the complexity in the mapping table. The encrypted image is secured with the DHKEP and with the private key of ECC. It offers double security compared with the other works.

REFERENCES

1. K. Shankar and P. Eswaran, (2015), ECC based Image Encryption Scheme with aid of Optimization Technique using Differential Evolution Algorithm, International Journal of Applied Engineering Research, Vol. 10, No. 55.
2. Ali Soleymani, et. al. (2012), A Survey on Principal aspects of Secure Image Transmission, World Academy of Science, Engineering and Technology, International Journal of Computer and Information Engineering, Vol. 6, No.6.
3. E.H.E. Kinani and F. Amounas, (2012), Fast mapping method based on matrix approach for elliptic curve cryptography, International Journal of Information Network Security, Vol. 1, No. 2, pp. 54 – 59.
4. E.H.E. Kinani and F. Amounas, (2012), An efficient elliptic curve cryptography protocol based on matrices, International Journal of Engineering and Invent., Vol. 1, No. 9, pp. 49 – 54.
5. S. Guptha, P.S. Gill et. al. (2012), A scheme for secure image transmission using ECC over the fraudulence network, International Journal of Advance Research Computer Science Software Engineering, Vol. 2, No. 4, pp. 67 -70.

6. Parmanand Astya, et. al. (1998), Image encryption and decryption using elliptic curve cryptography, International Journal of Advance Research In Science And Engineering, Vol. No.3, Issue No.10, October 2014 on BRCA1, Breast Disease 10 (1998), 3–10.
7. O.S. Rao and S.P. Setty, (2010), Efficient mapping method for elliptic curve cryptosystems, International Journal of Engineering and Science and Technology, Vol. 2, pp. 3651-3656.
8. Ali Soleymani et. al. (2013), An Image Encryption Scheme Based on Elliptic Curve and a Novel Mapping Method, International Journal of Digital Content Technology and its Applications(JDCTA), Vol. 7, No. 13.
9. Larry R. Medsker, (1995) Hybrid Intelligent Systems by Department of Computer Science and Information Systems, The American University, Springer Science + Business Media, LLC, Page. No: 2.
10. Shaik Hedayath Basha and Jaison B, (2020), A Novel Secure Message Transmission using Elliptic Curve Diffie Hellman Key Exchange Protocol, International Journal of Scientific & Technology Research Vol. 9, issue 02, ISSN 2277-8616.
11. Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh, (2015), Image Encryption using Elliptic Curve Cryptography, Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015), Procedia Computer Science 54 (2015) 472 – 481.
12. Mohamad Ali Mehrabi et. al. (2020), Elliptic Curve Cryptography Point Multiplication Core for Hardware Security Module, IEEE transactions on Computers, Vol. 1, issue 1, doi:10.1109/tc.2020.3013266.
13. E. Hernandez Diaz et. al. (2020), Encryption of RGB Images by means of a Novel Cryptosystem using Elliptic Curves and Chaos, IEEE Latin America Transactions, Vol. 18, issue 08, pp. 1407 – 1415, doi:10.1109/tla.2020.9111676.
14. K. Sowjanya et. al. (2019), An efficient Ellipitic Curve Cryptography-Based without paring KPABE for IoT, IEEE Systems Journal, pp.1-10, doi:10.1109/jsyst.2019.2944240.
15. Hisham N. Almajed and Ahmad S. Almogren (2019), SE-Enc: A secure and Efficient Encoding Scheme using Elliptic Curve Cryptography, IEEE Access, Vol. 7, DOI:10.1109/ACCESS.2019.2957943.
16. Saleh Ibrahim and AymanAlharbi (2020), Efficient Image encryption scheme using Henon Map, Dynamic S-Boxes and Elliptic curve cryptography, IEEE Access, Vol. 8, DOI:10.1109/ACCESS.2020.3032403.
17. Piljoo Choi et. al. (2017), Low-Complexity Elliptic Curve Cryptography Processor based on Configurable Partial Modular Reduction over NIST Prime fields, IEEE Transactions on Circuits and Systems – II, Express Briefs, Vol. 1 and issue.1 doi:10.1109/tcsii.2017.2756680.
18. AnumSajjad et. al. (2020), Kleptographic Attack on Elliptic Curve based Cryptographic Protocols, IEEE Access, Vol. 8, 2020, DOI: 10.1109/ACCESS.2020.3012823.
19. Vijayakumar K and Arun C (2019) “Continuous Security Assessment of cloud-based applications using distributed hashing algorithm in SDLC”, Cluster Computing, 22, 10789-10800. https://link.springer.com/article/10.1007/s10586-017-1176-x
20. Joshi, A. B. et. al. (2020), Security of Digital Images Based on 3D Arnold Cat Map and Elliptic Curve, International Journal of Image and Graphics, 2020. doi:10.1142/s0219467821500066.
21. T. S. Reddy, Y. D. S. Raju (2021), “Implementation of Data Security with Wallace Tree Approach Using Elliptical Curve Cryptography on FPGA,” Turkish Journal of Computer and Mathematics Education, Vol. 12, pp. 1546-1553. Doi:10.17762/turcomat.v12i6.2693

AUTHORS

Shaik Hedayath Basha working as Assistant Professor in RMK College of Engineering and Technology, Department of Electronics and Communication Engineering, Chennai, having 15 years of teaching Experience. He completed bachelor’s degree under Madras University, Chennai. Bagged two master’s degrees, one in Applied Electronics from Satyabama University, Chennai and the other from JNTU, Anantapuramu, Anantapur, Andhra Pradesh. He completed Ph.D. at Anna University, Chennai. His Area of interest are Image and Video Watermarking, Image Encryption, Image Analysis, Image Processing, and IoT.

Corresponding Author E-mail: shaikhedaythbasha@mkcet.ac.in

C Arun working as a Professor in RMK College of Engineering and Technology, Department of Electronics and Communication Engineering. Chennai, India, having 20 years of teaching Experience. Area of interest are VLSI, Image and Video Watermarking, Image Encryption, Image Analysis, Image Processing, AI and ML.

E-mail: arun.c@mkcet.ac.in

S Jai Ganesh working as Assistant Professor in RMK College of Engineering and Technology, Department of Electronics and Communication Engineering, Chennai, having 14 years of teaching Experience. Area of interest is Cyber Security, Communication Networks, Cryptography, and AI and ML

Email id: jaiganeshece@mkcet.ac.in

Nimitha N is working as Assistant Professor in RMK College of Engineering and Technology, Department of Electronics and Communication Engineering, Chennai, having 14 years of teaching Experience. Area of interest is Medical Image Processing, Signal Processing, and AI and ML.
Email id: nimithaece@mkcet.ac.in

Sai Kiran T. Pharmaceutical Distribution Administrator, Cardinal Health, Dublin-Ohio- USA.
Email id: sri.tatineni@cardinalhealth.com