Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Digital Image Encryption Algorithm Based on Elliptic Curve Public Cryptosystem

[1]D S V Prasad, [2*]Dr. P. Sudam Sekhar, [3]Arigela Veera Venkata Prasanth,

[4]Kasina Naga Sai Ganesh, [5]Kovvuri Ramya Madhuri, [6]Thota Veera Venkata Durga Prasad

[1]Asst Professor,[3,4,5,6] Student
[1,3,4,5,6]Department of CSE, BVC Engineering College, Odalarevu, AP
[2]Associate Professor of Mathematics,
[2]Vignans Foundations for Science Technology and Research, Guntur
Corresponding Author: sudamshekhar@gmail.com

Article Info
Page Number: 644-655
Publication Issue:
Vol. 71 No. 4 (2022)

Article History
Article Received: 25 March 2022
Revised: 30 April 2022
Accepted: 15 June 2022
Publication: 19 August 2022

Abstract
The content security of digital images is a hot topic in both academics and business because to the growing usage of media in communications. In the meanwhile, users of symmetric cryptosystems must manage and transmit keys. This study suggests an elliptic curve-based asymmetric image encryption technique (ECC). The Diffie-Hellman public key sharing method is used to determine an elliptic curve point that is agreed upon by both the sender and the recipient. The sender first puts pixel data together and turns them into large numbers to shorten the encryption timings. Second, the sender uses the chaotic system and ECC to encrypt large integers. Finally, huge integers that have been encrypted are used to create the encrypted image. The suggested technique makes key management and transmission comparatively easy and secure. The suggested algorithm displays excellent security and great efficiency, according to simulation data.

Keywords: DNN, ECC, and the CHA-CHA algorithm

Introduction

The Internet, which is utilised extensively in virtually every industry, uses digital images as one of its primary ways of information delivery. Business secrets and even national security are frequently depicted in digital photographs. The growth of the internet and the widespread use of multimedia make image content security a crucial concern for scientists and engineers.

Because of the chaotic system's great sensitivity to initial values and parameters, ergodicity, pseudorandomness, etc., it is frequently utilised in the field of picture encryption [1]. Recently, a number of chaotic system-based picture encryption techniques have been proposed [2]–[7]. Low-dimensional chaotic sequences, however, have the issues of a short code period and low accuracy, which cannot ensure the security of the algorithm. The high-dimensional chaotic encryption algorithms [8]–[13] are being studied more.

Elliptic Curve Cryptosystem (ECC), which is based on the Elliptic Curve Discrete Logarithm Problem's complexity, is a superb asymmetric encryption technique (ECDLP). Manish et al. suggested an image encryption technique based on DNA encoding and ECC to encrypt the colour image [14]. Using the DNA encoding theory, the plain image is first encoded, and then

ECC executes the image encryption procedure. Although the encryption algorithm functions well, it might be made better. When every pixel is dark (pixel value 0), the associated encrypted picture is the image itself. In general, a good picture encryption method should turn every plain image into an unreadable encrypted image. A 4-dimensional cat map and ECC-based colour image encryption technique was put out by Wu et al. [15]. For the compression algorithm employed during the encryption process, the decrypted image of this algorithm is lossy. A colour image encryption technique based on ECC and Advanced Encryption System was proposed by Toughi et al. [16]. The random sequence is produced by their algorithm using ECC. A colour image encryption technique based on DNA encoding and ECC was proposed by Zhao and Zhang [17]. ECC is only utilised in their approach to encrypt the key data during encryption; it is not used to encrypt the pixel values of the plain image. A proposed image encryption technique based on ECC was made by Singh and Singh [18]. In order to simplify the cryptographic operations in their technique, the authors first group the pixel values into relatively large numbers before encrypting them with ECC. However, there are also a lot of cryptographic processes being performed. A chaotic system and ECC-based picture encryption technique were proposed by Laiphrakpam and Khumanthem [19]. ECC is employed in their technique to produce the random sequence that will spread the simple image. A mixed picture element encryption technique based on ECC was proposed by Zhu and Zhang [20]. They employ ECC in their approach to encrypt the filenames of mixed image components. Overall, the efficiency or security of the majority of these algorithms can be increased.

This work suggests an asymmetric picture encryption technique based on ECC and chaotic system to safeguard the content of digital photos. The proposed algorithm is deemed desirable in terms of security and effectiveness based on experimental findings and algorithm assessments.

1.1 ECC

The method of public key cryptography used for data encryption is called elliptic curve cryptography (ECC). Ellipstic curves were proposed by Neal Koblitz and Victor Miller in 1985 for the creation of public key cryptography systems. Elliptic curves are cubic curves of the form, not ellipses. The characteristics of ECC make it stronger against different attacks in wireless sensor networks and many other wirelessly suited situations. This provides high level security with a shorter key length, resolving the primary problem with public key cryptography.

1.2 CHAOS SYSTEM

The Piece-Wise Linear Chaotic Map (PWLCM) system can produce great random sequences for encrypting images because it has uniform invariant distribution, excellent ergodicity, confusion, and determinacy.

ENCRYPTION OF MIXED IMAGE ELEMENTS WITH ECC

The ECC algorithm will be used to encrypt the original image, three disguised images, and the mixture of the original image and the three camouflaged images.

1.3 Inspiration

In order to secure media content, image encryption techniques were introduced using symmetric algorithms. However, these algorithms work with a single key and require that key to be distributed before sending or receiving content. This key distribution will increase network load and make the network more vulnerable to attack if keys were compromised. Asymmetric encryption, which uses public and private keys to encrypt and decode data, was developed as a solution to this issue. Instead of publishing any keys, users just need to have a set of common ECC parameters that can produce public and private keys for data encryption and decryption.

1.4 Problem Description

The author has introduced a secure and more effective technique called Digital Image Encryption with ECC to address this issue. Many encryption techniques have been introduced using ECC, such as DNA encoding with ECC and colour images with ECC, among others. However, these techniques are not very secure and are computationally intensive.

1.5 Purpose:

The practice of secret writing known as cryptography is used to protect messages and conceal information. Encryption and decryption are two separate techniques used to keep the information secure. These are the principles of cryptography, which are both very important and quite basic. It is a method for maintaining information security, including data integrity, data secrecy, authentication, and non-repudiation, in the face of adversaries. In cryptography, the process of transforming common information or plain text into cypher text is known as encryption. In cryptography, decryption is the opposite of encryption, which transforms cypher text into plain text.

1.6 Work's scope:

In recent years, elliptic curve encryption has gone from being a fascinating theoretical concept to being widely used by businesses. This new development is due to two factors: First, ECC has endured a generation of assaults and is no longer novel. Second, its benefits over RSA have made it a desirable security in the emerging cellular market. Major wireless industry players like Motorola, DoCoMo, RIM, IBM, Sun Microsystems, Microsoft, and Hewlett-Packard are all making investments in ECC. The NSA developed the security standards for wireless devices connected to the military, and NIST offers standardised curves for use in a variety of ECC applications. The U.S. government is also permitted to employ ECC. ECC is also used by smartcard manufacturers like Gem Plus to increase the security of their goods.

1.8 Report organisation:

Five chapters make up the remaining portion of the report. Following this introduction chapter, chapter 2 goes on to detail the survey of the current system. This provides context for the research that has been done so far in the areas of existing image encryption methods using ECC, existing DNA encoding methods using ECC, and digital image encryption using the PWLCM System.

The suggested system is described in Chapter 3. The introduction of the dataset and the models employed in the report serves as the first step in this process. The suggested system's architecture is then covered. explains the procedures, techniques, and specifics of the software utilised for the research. Additionally, it describes the study's evaluation criteria.

The experiment and its findings are presented in Chapter 4. The comparison graph and each model's confusion network are apparent. This aids in determining the model that uses ML and DL algorithms to anticipate stock market trends is the most effective.

The conclusion of all the models used in this research work is given in Chapter 5, along with advice on when to utilise each model. It provides future work with a fresh orientation.

2.2 Contribution to Research:

Security features like the capacity for secure email, encrypted web surfing, and virtual private networking to corporate networks are gradually becoming more and more important for wireless devices. The cellular sector obscures the growing demand for security. For secure (authenticated, private) Web transactions as well as for secure messaging, a complete and effective public key infrastructure is required (signed, encrypted). ECC performs more effectively the implementation of all of these security features, which are increasingly employed on wireless devices for secure email, secure web surfing, and virtual private networking to corporate networks.

3. The suggested system

Create chaotic images using binary values and the PWLCM (Piece-Wise Linear Chaotic Map) to create a technique that can jumble images more securely and improve picture security. By grouping together and converting the values of the pixels into large integers, the proposed work first speeds up the encryption process. Second, the sender uses the chaotic system and ECC to encrypt large integers. Finally, huge integers that have been encrypted are used to create the encrypted image. The suggested technique makes key management and transmission comparatively easy and secure.

3.1 Methods:

We employ cryptography, DNN, and ECC in this study.

3.1.1 Cryptanalysis

For the purposes of secure communication and password management, cryptography is frequently utilised. It has mechanisms for both encryption and decryption. A plaintext is

transformed into cypher text using the encryption technique, and a secure key is used to decode the encrypted communication back into plain text during decryption.

3.1.2 DNN:

Machine learning techniques like DNN (deep neural networks) imitate how the brain learns. It has been employed for a number of purposes.

3.1.3 ECC:

Data encryption using elliptic curve cryptography (ECC), a key-based method For the purposes of decrypting and encrypting online traffic, ECC focuses on pairs of public and private keys. ECC has smaller ciphertexts, keys, and signatures, as well as faster key and signature generation. It decrypts and encrypts data at a reasonably quick rate.

3.1.4 The CHACHA

D. J. Bernstein created the stream cypher [CHACHA] in 2008. It is a development of Salsa20 and served as the foundation for BLAKE, a finalist for the SHA-3 award. This document uses the ChaCha version with 20 rounds and a 256 bit key.

3.3 Architecture/Framework:

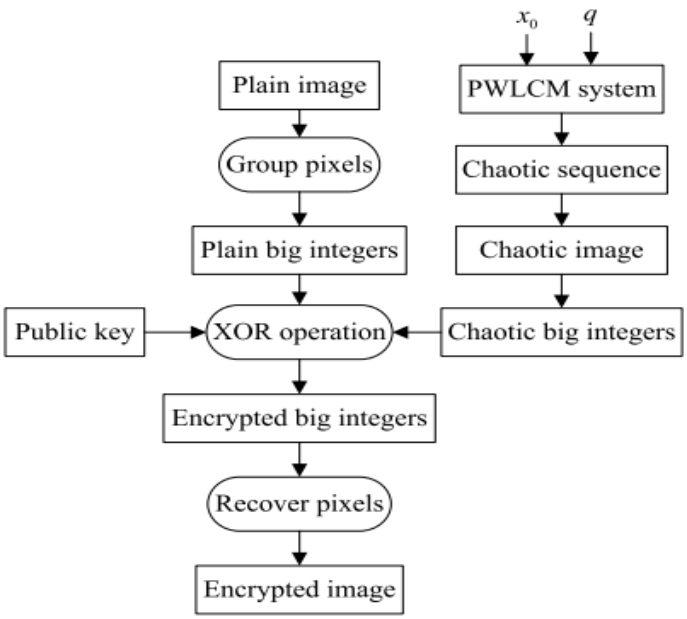

Fig.1. Architecture

3.4 Algorithm and Process Design:

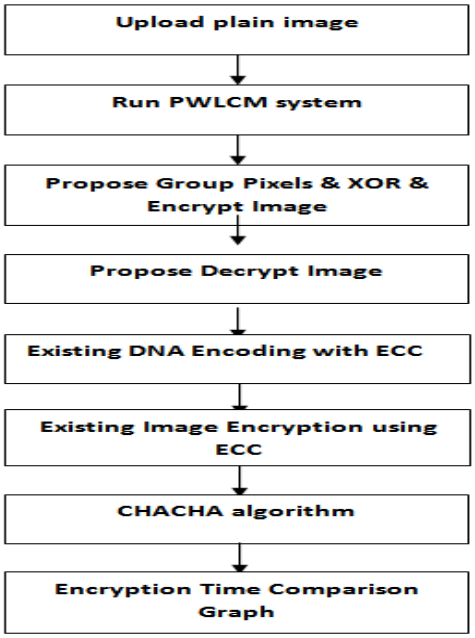

Fig.2. Process Design

Modules

• Upload a plain image: We'll upload a plain image using this module.

• Run the PWLCM system: The PWLCM model is run using this module.

• Use the module "Propose Group Pixels & XOR & Encrypt Image" to encrypt the image.

• Offer to Decrypt Image: Image is decrypted using this module.

Using this module, we can see how DNA sequence elements are used to encode the pixel values of images.

Existing Image Encryption Using ECC: We can check the time it takes ECC to encrypt an image as well as encrypted and decrypted images.

Using this module, we can see an encryption time comparison graph where the x-axis indicates the name of the algorithm and the y-axis represents the encryption time, and all algorithms proposed The proposed encryption technique is faster and more secure than the existing algorithms, according to the analysis, which required less time.

IV. Implementation and Outcome

4.1 Data collection

Input Plain Image

Fig. 3. Input Image

The technique of converting a plain image into an unintelligible form is known as image encryption.

4.2 Assessment Metrics:

The characteristics and structure of the CPU, memory space, text size, the type of software being used, and other factors all have an impact on how quickly an algorithm runs.

The execution time of the text to picture algorithm is referred to as this. It is the total of the runtime and compilation times.

For text-to-image encryption to be used in practise, the execution time should be as short as possible. Typically, it is measured in minutes, milliseconds, or seconds.

Layer by layer, the image was processed, which sped up the process. In comparison to others, the capacity was four times greater.

Encryption time for all of those algorithms, which we can see. Extension CHA-CHA executed more quickly than previous algorithms since it required less time.

4.3 Outcome:

Once a plain image is uploaded and instruct to generate ‘PWLCM’ values and in old diagram shots you can read in depth about this values

PWLCM X0 : 0.047058823529411764
PWLCM Q : 0.1843137254901961

The PWLCM values are generated and now one can encrypt image with ECC Chaotic algorithm

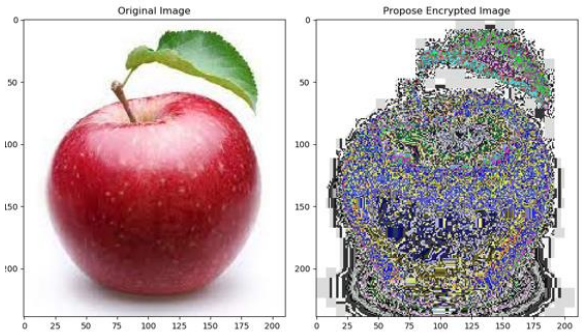

Fig.4. encrypted image using ECC

In above diagram first image is the original image and second one is encrypted image using ECC chaotic image and now close above and then to decrypt image and to get below output

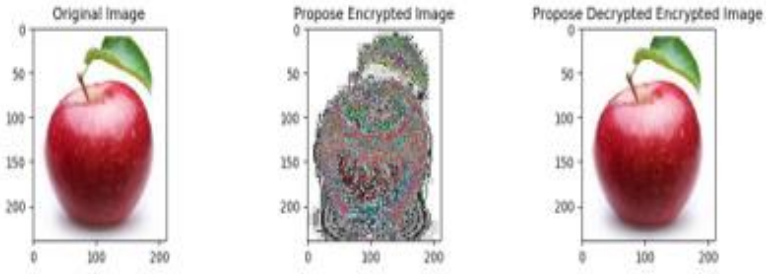

Fig.5. decrypted image and the histogram

In above diagram first is the original image and second is the encrypted image and 3rd one is the decrypted image and 4th one is the histogram generated from propose chaotic encrypted image and we can see histogram is almost uniform as describe in paper and we can conclude that propose chaotic encryption is more secure. Now close above image and then click on 'Existing DNA Encoding with ECC' button to encrypt image using DNA ECC Encoding and to get below output

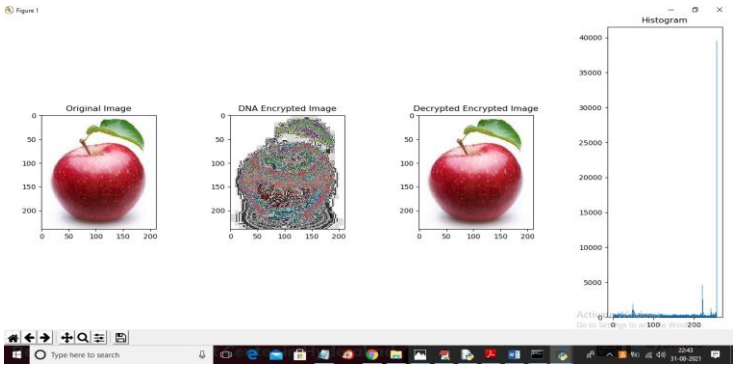

Fig.6. image encryption with DNA ECC Encoding

In above diagram we can see image encryption with DNA ECC Encoding and we can see histogram is not much uniform compare to propose algorithm. Now close above image and then click on 'Existing Image Encryption using ECC' button to encrypt image using ECC and to get below output

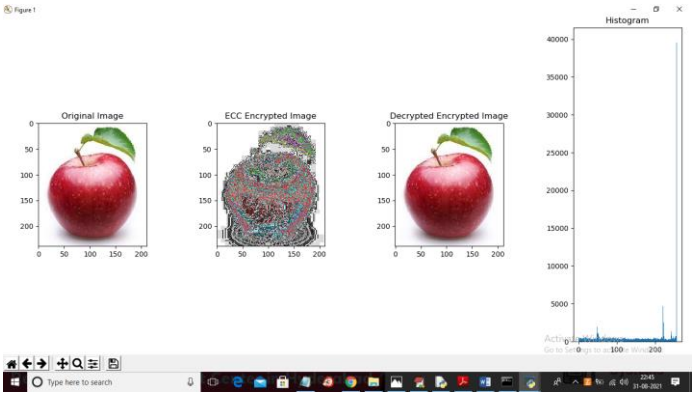

Fig.7. ECC algorithm

In above diagram with ECC algorithm also histogram is not much uniform compare to propose algorithm and now close above image and then click on 'Mixed Image Element Encryption using ECC' button to encrypt image using Mixed Image encryption and to get below output

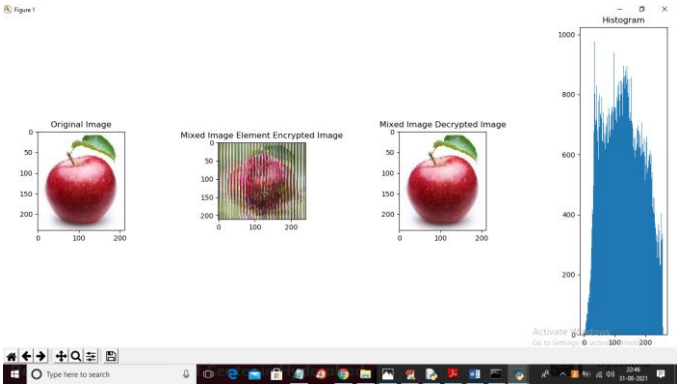

Fig.8. histogram

In above diagram first is the original image and second is the mixed encryption image and 3rd is the decrypted image and 4th is histogram which is not uniform compare to propose work. By seeing all algorithms output we can conclude that propose chaotic histogram is more uniform. Now close above image and then click on 'Encryption Time Comparison Graph' to get below encryption speed time graph

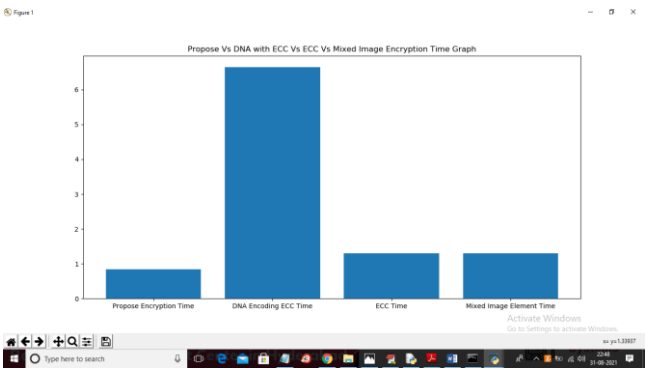

Fig.9. represents algorithm name and encryption time

In above graph x-axis represents algorithm name and y-axis represents encryption time and in all algorithms propose encryption took less time.

Extension Outcomes:

In this paper as extension we have used advance CHACHA algorithm and then compare performance with propose and existing ECC algorithm and the experiment prove that CHACHA is efficient than propose and existing algorithms. In below diagram we have done coding for CHACHA algorithm

In below diagram we are showing code to encrypt and decrypt image with CHACHA algorithm

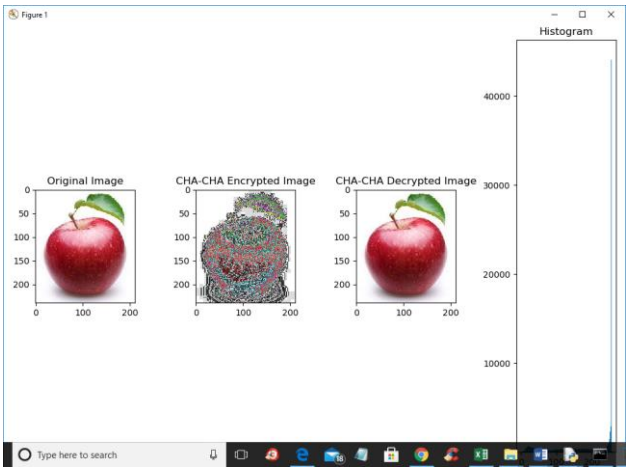

Fig.10. decrypted with CHA-CHA algorithm

In above diagram you can see image encrypted and decrypted with CHA-CHA algorithm and below is the Execution Time graph for all algorithms

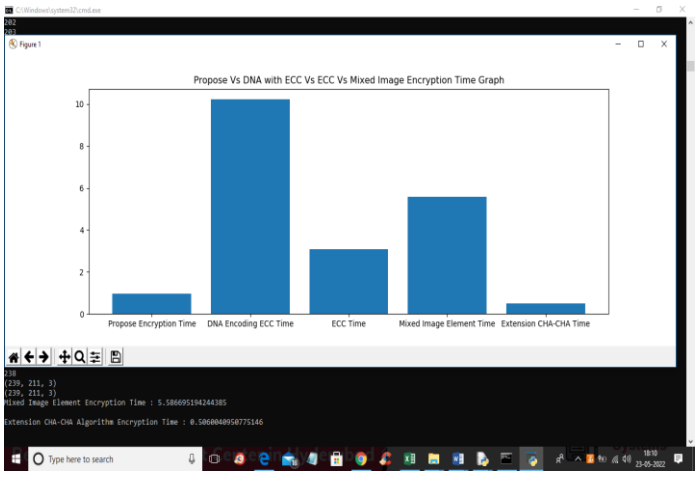

Fig.11. algorithm names and encryption time

In above graph x-axis represents algorithm names and y-axis represents encryption time for those algorithms and in above diagram we can see in all algorithms Extension CHA-CHA took less execution time so it's faster than other algorithms

CONCLUSION

This study provides an asymmetric picture encryption technique based on ECC and chaotic system to safeguard the content of the digital image. The suggested technique makes key management and transmission comparatively easy and secure. The proposed algorithm is secure enough to withstand, as demonstrated by experimental findings and algorithm analysis. The proposed approach is the fastest in terms of encryption speed when compared to three other similar algorithms that are already in use.

REFERENCES

[1] X. Huang and G. Ye, ‘‘An image encryption algorithm based on hyper chaos and DNA sequence,’’ Multimedia Tools Appl., vol. 72, no. 1, pp. 57–70, 2014.

[2] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, ‘‘An image encryption algorithm based on chaotic system and compressive sensing,’’ Signal Process., vol. 148, no. 7, pp. 124–144, 2018.

[3] R. Lan, J. He, S. Wang, T. Gu, and X. Luo, ‘‘Integrated chaotic systems for image encryption,’’ Signal Process., vol. 147, no. 6, pp. 133–145, 2018.

[4] R. Parvaz and M. Zarebnia, ‘‘A combination chaotic system and application in color image encryption,’’ Opt. Laser Technol., vol. 101, no. 5, pp. 30–41, 2018.

[5] L. Teng, X. Wang, and J. Meng, ‘‘A chaotic color image encryption using integrated bit-level permutation,’’ Multimedia Tools Appl., vol. 77, no. 6, pp. 6683–6896, 2018.

[6] L. Liu, S. Hao, J. Lin, Z. Wang, X. Hu, and S. Miao, ‘‘Image block encryption algorithm based on chaotic maps,’’ IET Signal Process., vol. 12, no. 1, pp. 22–30, 2018.

[7] C. Pak and L. Huang, ‘‘A new color image encryption using combination of the 1D chaotic map,’’ Signal Process., vol. 138, no. 9, pp. 129–137, 2017.

[8] Q. Ran, L. Wang, J. Ma, L. Tan, and S. Yu, ‘‘A quantum color image encryption scheme based on coupled hyper-chaotic Lorenz system with three impulse injections,’’ Quantum Inf. Process., vol. 17, no. 8, pp. 1–30, 2018.

[9] L. Gong, C. Deng, S. Pan, and N. Zhou, ‘‘Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform,’’ Opt. Laser Technol., vol. 103, no. 7, pp. 48–58, 2018.

[10] N. Zhou, W. Chen, X. Yan, and Y. Wang, ‘‘Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyperchaotic system,’’ Quantum Inf. Process., vol. 17, no. 6, pp. 1–24, 2018.

[11] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, ‘‘An image encryption algorithm based on compound homogeneous hyper-chaotic system,’’ Nonlinear Dyn., vol. 89, no. 1, pp. 61–79, 2017.

[12] X. Zhang, W. Nie, Y. Ma, and Q. Tian, ‘‘Cryptanalysis and improvement of an image encryption algorithm based on hyper-chaotic system and dynamic S-box,’’ Multimedia Tools Appl., vol. 76, no. 14, pp. 15641–15659, 2017.

[13] M. Kaur and V. Kumar, ‘‘Efficient image encryption method based on improved Lorenz chaotic system,’’ Electron. Lett., vol. 54, no. 9, pp. 562–563, 2018.

[14] M. Kumar, A. Iqbal, and P. Kumar, ‘‘A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography,’’ Signal Process., vol. 125, pp. 187–202, Aug. 2016.

[15] J. Wu, X. Liao, and B. Yang, ‘‘Color image encryption based on chaotic systems and elliptic curve ElGamal scheme,’’ Signal Process., vol. 141, pp. 109–124, Dec. 2017.

[16] S. Toughi, M. H. Fathi, and Y. A. Sekhavat, ‘‘An image encryption scheme based on elliptic curve pseudo random and advanced encryption system,’’ Signal Process., vol. 141, no. 12, pp. 217–227, 2017.

[17] Z. Zhao and X. Zhang, ‘‘ECC-based image encryption using code computing,’’ Amer. J. Eng. Technol. Res., vol. 11, no. 9, pp. 1399–1405, 2011.

[18] L. D. Singh and K. M. Singh, ‘‘Image encryption using elliptic curve cryptography,’’ Procedia Comput. Sci., vol. 54, pp. 472–481, 2015.

[19] D. S. Laiphrakpam and M. S. Khumanthem, ‘‘A robust image encryption scheme based on chaotic system and elliptic curve over finite field,’’ Multimedia Tools Appl., vol. 77, no. 11, pp. 8629–8652, 2018.

[20] G. Zhu and X. Zhang, ‘‘Mixed image element encryption algorithm based on an elliptic curve cryptosystem,’’ J. Electron. Image., vol. 17, no. 2, pp. 1–5, 2008.