IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 10 July 2023, accepted 7 August 2023, date of publication 14 August 2023, date of current version 29 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3305271

RESEARCH ARTICLE

EGCrypto: A Low-Complexity Elliptic Galois Cryptography Model for Secure Data Transmission in IoT

MANJIT KAUR[1], (Senior Member, IEEE), AHMAD ALI ALZUBI[2], TARANDEEP SINGH WALIA[3], VAISHALI YADAV[4], NARESH KUMAR[5], DILBAG SINGH[6,7], (Senior Member, IEEE), AND HEUNG-NO LEE[8], (Senior Member, IEEE)

[1]School of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana 506371, India
[2]Department of Computer Science, Community College, King Saud University, Riyadh 11421, Saudi Arabia
[3]School of Computer Application, Lovely Professional University, Phagwara, Punjab 144411, India
[4]Department of Computer and Communication Engineering, Manipal University Jaipur, Jaipur 303007, India
[5]Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, Janakpuri, New Delhi 110058, India
[6]Center of Biomedical Imaging, Department of Radiology, New York University Grossman School of Medicine, New York City, NY 10016, USA
[7]Blockchain Intelligence Convergence Center, Gwangju Institute of Science and Technology, Gwangju 61005, South Korea
[8]School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju 61005, South Korea

Corresponding author: Heung-No Lee (heungno@gist.ac.kr)

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2023-2021-0-00118, Development of decentralized consensus composition technology for large-scale nodes) and This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2023-2021-0-01835) supervised by the IITP (Institute of Information & Communications Technology Planning & Evaluation) and in part by the Researchers Supporting Project (RSP2023R395), King Saud University, Riyadh, Saudi Arabia.

ABSTRACT In recent years, data security has been a challenging endeavor, especially when the data is being transmitted every second. Internet of Things (IoT) involves continuously sending data over public networks, making the data vulnerable to various security threats. Therefore, ensuring the secure end-to-end communication of IoT data is critical. Cryptography and steganography have proven effective in providing secure connectivity for IoT devices. However, challenges in existing approaches include scalability, computational complexity, implementation, key management, trade-offs, evolving threats, and hyperparameter tuning. Therefore, in this paper, we propose EGCrypto, an efficient and secure model for IoT networks. EGCrypto utilizes a low-complexity elliptic Galois cryptography approach along with matrix XOR steganography to enhance security. To optimize its performance, we employ the zoning evolution of control attributes and adaptive mutation based self-adaptive differential evolution with fitness and diversity ranking. These techniques are utilized to fine-tune the hyperparameters of EGCrypto, enhancing its effectiveness and efficiency. The confidential IoT data is encrypted using low-complexity elliptic Galois cryptography. Following encryption, the encrypted data is embedded or hidden into cover blocks of an image, which are selected using the optimization algorithm. This ensures secure data communication in IoT architectures, as the encrypted data is transferred safely and can be easily recovered and decrypted at the receiving end. The experimental results demonstrate that EGCrypto outperforms competitive models with improvements of 1.8473% in peak signal to noise ratio (PSNR), 1.5490% in strutural similarity index metric (SSIM), 1.7682% in normalized root mean square error (NRMSE), 1.3829% in carrier capacity, and 1.9372% in embedding efficiency.

INDEX TERMS Data security, the Internet of Things, secure communication, cryptography, steganography, elliptic Galois, differential evolution, hyperparameters, encryption.

The associate editor coordinating the review of this manuscript and approving it for publication was Ramakrishnan Srinivasan.

I. INTRODUCTION

Internet of Things (IoT) refers to an environment where various physical resources, electronic gadgets, vehicles, and

software are interconnected, facilitating data transmission between these devices [1]. Initially, IoT was used for integrating Radio-frequency Identification (RFID) tags, sensors, and various communication devices. Its primary purpose is to provide a reliable and secure framework for exchanging ''Things'' [2]. These ''Things'' in the context of IoT are small items and devices that collaborate to accomplish tasks. The concept of IoT enables the association of different devices over the internet, allowing them to cooperate and achieve common goals [3]. However, the implementation of IoT poses challenges such as computational power limitations, connectivity issues, and energy constraints.

One challenge that often receives insufficient attention is secure communication in IoT networks. While developers focus on enhancing the potential of IoT devices, the security aspect is sometimes overlooked [4], [5]. Insufficient security measures during data communication leave the entire system vulnerable to security attacks, including data theft, manipulation, and other threats [6]. Without proper data security, personal user information becomes susceptible to hacking [7]. Therefore, it is crucial to implement user authentication and identification approaches to verify the authenticity of users accessing the data and ensure that data is transferred to the correct devices from trusted sources [8].

The personal data needs to be encrypted (i.e., transformed into a meaningless form) when sent from one device to another over an IoT network. Data encryption provides security and protects it from attackers [9]. Cryptographic techniques can be used to encrypt data, ensuring authentication, integrity, confidentiality, and non-repudiation [10]. This paper utilizes Elliptic Curve Cryptography (ECC), which is based on the algebraic structure of elliptic curves over finite fields. ECC offers smaller key sizes compared to other cryptographic techniques [11], [12].

It is found that the competitive approaches face challenges in scalability, complexity, implementation, key management, trade-offs, evolving threats, and hyperparameter tuning. Therefore, to enhance data security, this paper employs steganography alongside cryptography. Specifically, Matrix XOR steganography is utilized, embedding encrypted data into irrelevant file data, such as images. The selection of the block for hiding the encrypted data is achieved through an efficient method called Zoning evolution of control attributes and adaptive mutation based self-adaptive differential evolution with fitness and diversity ranking (ZSADE). The proposed approach operates as follows: the data is initially encrypted using ECC, then the ZSADE algorithm optimizes the image block, and finally, the encrypted data is concealed within the selected block using matrix XOR steganography. Consequently, potential intruders remain unaware of the existence of the hidden message.

The main contributions are as follows:

- A secure end-to-end communication model called EGCrypto is designed specifically for IoT networks.
- The sensed data is initially encrypted using the low complexity elliptic Galois cryptography (LCEGC) approach.
- Matrix XOR steganography is utilized to embed the ciphered data into the cover image.
- Zoning evolution of control attributes and adaptive mutation based self-adaptive differential evolution with fitness and diversity ranking (ZSADE) is designed to optimally embed the encrypted data in the cover image.

The remaining organization of the paper is as follows: Section II discusses the literature work in the field. Section III presents the methodology used. Section IV covers the experimental setup and results. Finally, Section V concludes the paper.

II. RELATED WORK

In an era dominated by the IoT, the importance of securing communication cannot be overstated. Various approaches have been devised to ensure end-to-end encryption and protect sensitive data. This section delves into recent advancements in end-to-end encryption techniques and their significance in safeguarding valuable information.

In [1], an elliptic Galois cryptography and matrix XOR steganography (EGMX) approach was designed to achieve secure end-to-end communication over IoT networks. Adaptive firefly optimization was used to obtain optimal blocks for hiding the encrypted image in the cover image. In [13], a secure IoT-enabled surveillance model was designed by applying a probabilistic and lightweight approach (PLA) for the encryption of key frames prior to communication. The designed model minimized the communication cost, bandwidth, and storage of surveillance data. In [14], an optical ghost steganography (OGS) approach was designed by embedding the intensity signals of one image into signals, with RSA asymmetric encryption used for the intensity signals encoding.

In [15], an advanced encryption system was integrated with bit matching steganography (IAEBM) to enhance the security of data packets. The bit matching approach evaluated the location of matching pixels and acquired a key to recover the secret packet. In [16], a bit mask-oriented genetic algorithm (BMOGA) was implemented to minimize the redundancy of medical reports communicated across organizations. Boolean-based mask-fill operators were utilized to overcome premature convergence. In [17], DNA steganography based hyper-elliptic curve cryptography (DHECC) was implemented to improve security, albeit with lower embedding capacity.

In [8], homomorphic encryption (HomEnc) were implemented for secure end-to-end communication in their proposed secure IoT architecture with lattice-based encryption. In [18], a hybrid cloud solution (HCS) for secure storage and communication of large images was proposed. Encryption was implemented on sensitive data prior to storing it on the private cloud. Compressive sensing and encryption-then-subsampling were applied to insensitive data stored on the

public cloud. In [19], a secure model for image transmission in IoT using compressive sensing (SCS) was implemented. The model combined diffusion and quantization operations utilizing chaotic maps to improve transmission security while meeting requirements of low storage, minimum energy consumption, and low computational cost.

In [10], the security of multimedia-based IoT applications was improved using compressive sensing-based encryption (CSEn). Artificial noise was utilized for quantization of compressive sensing measurements to resist ciphertext-plaintext attacks. In [20], image cryptography keys were secured using a random phase key exchange approach (RPKE) for Fourier optics image encryption. In [21], an encryption system was proposed for securing information sensed through IoT sensor nodes. Homomorphic encryption with collective matrix factorization and locality-sensitive hashing (HCL) were employed to provide significant security and privacy-preserving index structure.

In [22], a secure cryptographic hardware was built to increase the side-channel security and reduce the energy consumption of IoT-edge nodes. The hardware implemented an optimal datapath architecture (ODA) to resist power-based side-channel analysis attacks. In [23], the security was improved by selectively obtaining vehicle details without revealing sensitive details. A convolutional neural network (CNN) was utilized to recognize encrypted images based on the type of vehicle in real-time, captured by cameras placed on road-side units as part of an intelligent transportation system. In [24], an asymmetric broadcast encryption approach (ABE) was designed for securing various kinds of images in an efficient manner with minimum transmission/computation overhead. In [25], a lightweight break-glass access control model (LBAC) was implemented, allowing dual ways of retrieving encrypted data, namely break-glass and attribute-based retrieval. This model demonstrated significantly lesser communication and storage overheads.

In [26], a highly efficient cryptographic hardware, called EC-Crypto, was developed to optimize area and delay for ECC. This hardware aimed to enhance side-channel security and reduce energy consumption in IoT-edge nodes by implementing an optimal datapath architecture. In [27], a lightweight authentication scheme (LAS) was proposed for IoT devices based on elliptic curve El Gamal using ephemeral encoding parameters. This scheme aimed to provide secure authentication while minimizing computational overhead, making it suitable for resource-constrained IoT environments. In [28], an intrusion detection model (IDM) was presented that combined an optimized quantum neural network with elliptic curve cryptography for data security. This model aimed to detect and prevent intrusions by leveraging the strengths of both techniques, ensuring robust protection of sensitive data. In [29], a hybrid Advanced Encryption Standard (AES) model was designed for IoT in telemedicine. This model integrated ECC and ID-based key generation to provide secure communication in telemedicine applications. The hybrid approach aimed to enhance the security of data transmission and storage in IoT-based telemedicine systems.

Table 1 presents various approaches to enhance IoT security, including cryptographic algorithms, steganography, and optimization methods. Secure hardware architectures and lightweight authentication schemes improve device security, while advanced encryption systems, genetic algorithms, and compressive sensing techniques ensure secure data transmission. Despite these advancements, challenges remain in scalability, computational complexity, and implementation. Key management, trade-offs, and evolving threats also pose significant challenges. Furthermore, hyperparameter tuning in ECC and homomorphic encryption lacks standardized guidelines and automated tools, requiring expertise and research to develop efficient optimization algorithms and establish best practices.

III. METHODOLOGY

We propose EGCrypto, a model motivated from [1], which combines low-complexity elliptic Galois cryptography (LCEGC) [30], optimal matrix-based XOR (OM-XOR), and Zoning Evolution of Control Attributes with Adaptive Mutation-based Self-Adaptive Differential Evolution with Fitness and Diversity Ranking (ZSADE) to address IoT security issues. Our EGCrypto model ensures secure data exchange between IoT devices, as shown in Figure 1. LCEGC serves as the controller for data exchange, encrypting the data within the controller using LCEGC and embedding it in a cover image via Matrix XOR steganography. The ZSADE optimization algorithm selects the optimal image block for inserting the encrypted data. The resulting image, with hidden encrypted data, is transmitted over the Internet, ensuring confidentiality and preventing unauthorized detection of sensitive information. Table 2 presents the nomenclature used in this paper.

A. LOW COMPLEXITY ELLIPTIC GALOIS CRYPTOGRAPHY

As mentioned previously, ECC is a public key cryptography that utilizes the properties of elliptic curve equations for key generation. This process distinguishes it from other cryptography techniques. The use of an elliptic curve over a Galois field ($GF()$) enhances computational efficiency and reduces complexities related to rounding errors [31]. $GF(Q)$'s values must exceed 1. $GF(Q)$ elements are defined as [30]:

$$GF(Q) = S_0 \cup S_1 \cup S_2 \cup \ldots \cup S_{n-1} \tag{1}$$

Here,

$$S_0 = (0, 1, 2, \ldots, Q-1) \tag{1a}$$
$$S_1 = (Q, Q+1, Q+2, \ldots, Q+Q-1) \tag{1b}$$
$$S_2 = (Q^2, Q^2+1, Q^2+2, \ldots, Q^2+Q-1) \tag{1c}$$
$$S_{n-1} = (Q^{n-1}, Q^{n-1}+1, \ldots, Q^{n-1}+Q-1) \tag{1d}$$

TABLE 1. Pros and cons of competitive approaches.

Ref.	Model	Pros	Cons
[1]	EGMX	Improved data hiding capacity and embedding efficiency	Complexity in finding optimal blocks for image hiding
[13]	PLA	Minimized communication cost, bandwidth, and storage in IoT-enabled surveillance	Specific to surveillance data
[14]	OGS	Used optical ghost steganography for secure signal embedding	Limited embedding capacity
[15]	IAEBM	Enhanced data packet security using bit matching steganography	Dependent on matching pixel locations
[16]	BMOGA	Minimized redundancy in medical reports using a genetic algorithm	Requires careful parameter tuning
[17]	DHECC	Improved security with DNA steganography-based hyper-elliptic curve cryptography	Lower embedding capacity
[8]	HomEnc	Enabled secure communication in IoT architecture with lattice-based encryption	Potential performance overhead
[18]	HCS	Provided secure storage and communication for large images using a hybrid cloud	Encryption-then-subsampling may affect image quality
[19]	SCS	Utilized compressive sensing with low resource requirements for secure image transmission	Complexity in implementing chaotic maps
[21]	CSEn	Enhanced security in multimedia-based IoT applications using compressive sensing-based encryption	Increased complexity due to artificial noise
[20]	RPKE	Utilized random phase key exchange approach to secure the keys	Dependency on key exchange protocol
[21]	HCL	Ensured security and privacy in IoT sensor nodes using homomorphic encryption	Computational overhead in collective matrix factorization
[22]	ODA	Built secure cryptographic hardware for enhanced side-channel security in IoT-edge nodes	Complexity in implementing optimal datapath architecture
[23]	CNN	Improved security by selectively obtaining vehicle details using a convolutional neural network	Specific to vehicle recognition
[24]	ABE	Employed asymmetric broadcast encryption to secure different types of images	Specific to image encryption
[25]	LBAC	Reduced communication and storage overheads	Limited to break-glass and attribute-based retrieval
[26]	EC-Crypto	Designed highly efficient cryptographic hardware for ECC optimization	Complexity in parameter optimization
[27]	LAS	Implemented lightweight authentication scheme for resource-constrained IoT devices	Trade-off between security and computational overhead
[28]	IDM	Achieved better security using quantum neural network and ECC	Computational complexity in implementing quantum neural network
[29]	AES	Provided a fast encryption solution with a shorter key length for IoT-based telemedicine applications	Complexity in integrating ECC and ID-based key generation

Here, $Q \in \mathbb{Q}$ and $n \in \mathbb{Z}_+$. Q represents the characteristic of the field, and Q^n represents the order of the Galois field. Each polynomial's degree is maximum $n-1$ [30].

In ECC, a user generates two keys: a public key and a private key. The public key is used for data encryption and is accessible to everyone, while the private key is kept only by the user and is used for data decryption. The key generation process is essential as both keys are derived using the same process.

An elliptic curve in the Galois field $GF(Q)$, where $Q > 3$, is defined by variables i and j and elements (a, b), resulting in the following equation [30]:

$$b^2 = a^3 + j \; mod \; Q + ia \tag{2}$$

Different elliptic curve points with a and b persist for different values of inputs, i, and j. Consequently, the elliptic curve serves as the foundation for the public key, while the private key is generated through a random process. The public key is obtained by multiplying the private key with the generator point, represented as G, on the curve.

Let there be two points on the elliptic curve represented as Q and R, such that:

$$P_U = GP_R \tag{3}$$

Here, P_U and P_R represent the public and private keys, respectively. Using a generator point G, an elliptic curve can be computed as long as there are no repeated factors in $27j^2 + 4i^3 \equiv 0 \pmod{Q}$ and $a^3 + ia + j$.

Under these conditions, the addition over $GF(Q)$ can be expressed as follows: If $Q = (a_1, b_1)$ and $R = (a_2, b_2)$ are elliptic curve components, then:

$$Q + R = (a_3, b_3) \tag{4}$$

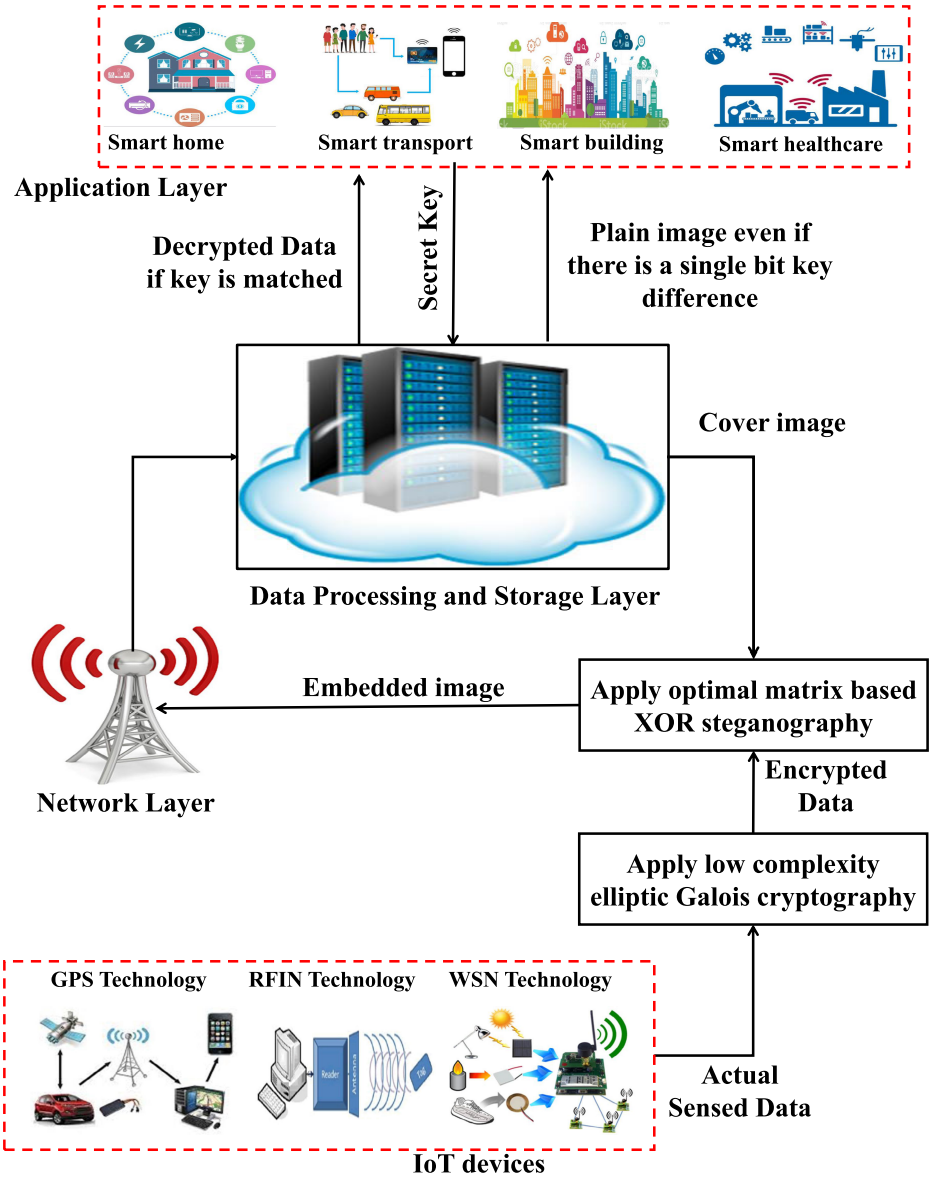

FIGURE 1. Diagrammatic flow of the proposed EGCrypto model.

where a_3 and b_3 are given as

$$a_3 = \lambda^2 - a_1 - a_2 \tag{5}$$

$$b_3 = \lambda(a_1 - a_3) - b_1 \tag{6}$$

Here, λ is given as

$$\lambda = \begin{cases} \dfrac{3a_1^2 + c}{2b_1} & \text{if} \quad Q = R \\ \dfrac{b_2 - b_1}{a_2 - a_1} & \text{if} \quad Q \neq R \end{cases} \tag{7}$$

After completing the key generation process, the data is encrypted using a chaotic neural network (ChNN), as described in the subsequent section.

B. CHAOTIC NEURAL NETWORK-BASED ENCRYPTION

ChNN encrypts the input plain data and generates the cipher data using the Galois field. The sensed data is represented as $(I_1, I_2, \ldots, I_n)$, and the encrypted data is represented as $(E_1, E_2, \ldots, E_n)$. ChNN with n inputs and outputs performs encryption using the following steps:

Step 1: Firstly, a chaotic sequence, known as the encrypted data, is generated and represented as:

$$(c(n), c(n+1), \ldots, c(n+n+1)) \tag{8}$$

Step 2: The ChNN takes plain data as input and converts it into a sequence of binary data represented as $(s_1, s_2, \ldots, s_n)$. This computation can be expressed as:

$$s(8n-8)s(8n-7)\ldots s(8n-2)s(8n-1) \tag{9}$$

TABLE 2. Nomenclature.

Symbol	Description
$GF()$	Galois Field
Q	Key Aspects of Field
a, b	Elements of the Elliptic Curve
i, j	Variables for Elliptic Curve
Q, R	Points on the Elliptic Curve
n	Order of the Galois Field
G	Generator Point
P_U, P_R	Public and Private Keys
λ	Slope Parameter
I	Plain Data
E	Encrypted Data
s	Binary Sequence
W	Weight Factors
b'	Bias Function
c	Chaotic Sequence
$OM-XOR$	Optimal Matrix based XOR
NP	Population Size
$FitR$	Fitness Rank
$DivR$	Diversity Rank
$Rank$	Final Rank
$r1, r2, r3$	Random Variables
F	Mutation Scaling Factor
W	Mutant Vector

Step 3: In this step, weight factors are generated based on the binary sequence from Step 2. The weight factors are dependent on the input values, meaning that different inputs result in different weight factors, as illustrated below:

$$W_x = \begin{cases} 1 & \text{if} \quad s(x+8\times n)=0 \\ -1 & \text{if} \quad s(x+n\times 8)=1 \end{cases} \tag{10}$$

Here x varies from 0 to 7.

Step 4: A bias function is generated for all chaotic values using the weight factors generated in Step 3. This bias function, denoted as b'_x, is designed to address the singularity problem. The generation of the bias function, incorporating the weight factor W_x and input b_x, can be described as follows:

$$b'_x = f(W_x \times b_x) \tag{11}$$

Step 5: Finally, the encrypted sensed data is generated using the input and the weight factor, according to the following procedure:

$$c(i) = a_n(n)\text{`}(1-b_n) + b'_x \tag{12}$$

Here, (a_n, b_n) represents a value pair on the elliptic curve, which serves as the secret key. Subsequently, the Matrix XOR technique of steganography is employed to store the cipher data generated in Step 5 on a cloud platform, as elaborated in the subsequent section.

C. OPTIMAL MATRIX BASED XOR

The encrypted data is hidden using the Optimal Matrix based XOR (OM-XOR) technique [32]. The image blocks are optimized through the ZSADE optimization algorithm, which selects the block from the complete image to conceal the data [31]. The following steps are involved in completing the process.

1) PERMUTATIVE STRADDLING

In certain cases, the complete image may not be utilized to hide the encrypted text, resulting in unused image blocks. To address this issue, permutative straddling can be employed to scatter the encrypted message throughout the entire image. A key-based password is utilized to perform the permutation, and the permutation can be repeated if the user possesses the correct key.

2) ENCODING

Among the various algorithms available for embedding encrypted data in an image block, Matrix XOR is utilized. Matrix XOR converts the triple $(m, k, c(i))$ to a quad $(d, k, c(i))$ and compresses the encrypted message, thereby enhancing the embedding efficiency. The secret data or chaotic sequence $c(i)$ is embedded into the cover block, which is the optimized image block, using Matrix XOR. The encrypted data block is substituted for one bit of the cover block during embedding. The process of embedding a single bit is performed as follows, with M representing the binary data bit and N is the block of binary image bits.

$$E_d = M \oplus N \tag{13}$$

The embedding procedure is conducted based on the following two conditions:

1) If the result of the XOR operation between two blocks is zero, the last bit position remains unchanged.
2) If the result of the XOR operation between two blocks is non-zero, bit position in cover block is modified, either from one to zero or from zero to one.

After verifying these conditions, the embedding is performed according to the following rule.

$$E_d = \left\{ \left((m(i) \oplus n(i)) n'(i) \right) + ((m(i) \oplus n(i))' n'(i)) \right\} \tag{14}$$

The image blocks are optimized using the ZSADE algorithm, as explained below.

D. OPTIMIZATION

Zoning evolution of control attributes and adaptive mutation based self-adaptive differential evolution with fitness and diversity ranking (ZSADE) algorithm introduces a modified mutation operation based on fitness and diversity ranking. It aims to arrange individuals effectively for the mutation operation, considering both fitness and diversity. This approach balances exploitation, considering the fitness value, and exploration, emphasizing diversity.

The ZSADE algorithm operates as follows:

Step 1: Initialize generation G to 0 and randomly initialize the population in generation 0 as follows:

$$I_1^0, I_2^0, \ldots, I_{NP}^0 \tag{15}$$

where NP represents the size of the population.

Step 2: Calculate the fitness value $f(I_i^0)$ for $i = 1$ to NP using the following equation:

Repeat the following steps until the termination condition is met.

Step 3: Assign the fitness rank $FitR_i$ to each individual using the following:

$$FitR_i = i \tag{16}$$

Step 4: Calculate the deviation $f_{dv,i}$ and the diversity rank $DivR_i$ of an individual i using:

$$f_{dv,i} = |f_i - f_{mid}| \tag{17}$$

Considering $FitR_i$ as the median individual with a value of $NP/2$, where f_{mid} represents its fitness value and f_i represents the fitness of I_i^G.

$$DivR_i = NP - i \tag{18}$$

Step 5: Determine the final rank $Rank_i$ using:

$$Rank_i = v \times DivR_i + (1 - v) \times FitR_i \tag{19}$$

where

$$v = \frac{G}{M} \tag{20}$$

Here, M shows maximum number of generations.

Step 6: For all individuals, i.e., for $i = 1$ to NP, select three random variables $r1$, $r2$, and $r3$ such that $i \neq r1 \neq r2 \neq r3$.

Step 7: Arrange I_{r1}^G, I_{r2}^G, and I_{r3}^G according to their final ranks, i.e., $Rank_{r1}$, $Rank_{r2}$, and $Rank_{r3}$. Represent the newly sorted individuals as I_{r1*}^G, I_{r2*}^G, and I_{r3*}^G.

Step 8: Perform the mutation operation to obtain the mutant vector W_i^G as:

$$W_i^G = I_{r1*}^G + F \times (I_{r2*}^G - I_{r3*}^G) \tag{21}$$

Step 9: Perform the crossover and selection operations based on the zoning evolution of control attributes and adaptive mutation of self-adaptive differential evolution [33].

Step 10: Increment the generation, i.e., $G = G + 1$.

E. DATA RETRIEVAL

The OM-XOR retrieval method is employed to retrieve the encrypted data stored in the cloud at the receiving end. This retrieval process involves decrypting the data using the user's private key and ChNN decryption. Decryption is accomplished using private key of user whose public key was initially used to encrypt the data.

IV. PERFORMANCE ANALYSIS

In this section, we present the experimental results and comparative analysis of EGCrypto. For experimentation, we have selected five cover images and five sensed data strings. EGCrypto is compared against five competitive encryption models as well as five steganography approaches to assess its effectiveness and performance.

A. VISUAL ANALYSIS

The visual analysis of EGCrypto is depicted in Figure 2. The first row displays the cover images, while the second row shows the obtained sensed data (strings). The third row illustrates the encrypted sensed data, and the fourth row showcases the final embedded stego images. The visual comparison demonstrates that there is no apparent correlation between the original sensed data and the encrypted data. Furthermore, the embedded stego images closely resemble their corresponding cover images, indicating the effectiveness of EGCrypto.

B. QUANTITATIVE ANALYSIS

To evaluate the performance of EGCrypto against competing approaches, performance measures such as peak signal-to-noise ratio (PSNR), strutural similarity index metric (SSIM), normalized root mean square error (NRMSE), execution time, carrier capacity, and embedding efficiency are utilized.

Table 3 presents PSNR analysis comparing EGCrypto with existing steganography approaches. The results demonstrate that EGCrypto achieves significantly better performance compared to the existing approaches, outperforming them by 1.8473%.

TABLE 3. PSNR analysis among EGCrypto and competitive approaches.

Models	Room	Parking	Store	Hospital	Patient
DHECC [17]	36.69	35.45	34.62	33.01	35.25
BMOGA [16]	36.28	38.84	34.91	35.87	35.34
IAEBM [15]	37.66	37.94	35.46	38.78	35.88
OGS [14]	35.65	34.79	37.55	38.38	38.26
EGMX [1]	34.95	38.51	37.91	38.13	33.65
EGCrypto	**38.98**	**40.16**	**39.23**	**40.13**	**39.58**

Figure 3 illustrates the results of the Structural Similarity Index (SSIM) analysis conducted among EGCrypto and other competitive models. The quantitative analysis reveals that EGCrypto consistently achieves the highest SSIM values across various scenarios. This indicates a strong similarity between the cover image and the embedded stego image, highlighting the effectiveness of EGCrypto in ensuring accurate and secure data transmission within IoT networks. SSIM values obtained for EGCrypto range from 0.9898 to 0.9919, further emphasizing its ability to maintain the integrity and fidelity of the transmitted data. EGCrypto outperforms existing approaches by 1.5490%, ensuring robust and reliable protection for Internet of Things network communications.

Figure 3 illustrates the analysis of Normalized Root Mean Square Error (NRMSE) conducted among EGCrypto and other competitive models. The NRMSE values are computed between the cover image and the resulting stego image, where text is embedded within the cover image. Lower NRMSE values indicate better quality and a closer resemblance between the cover and stego images. Among the evaluated models, EGCrypto achieves the lowest NRMSE values across various images, including Room, Parking, Store, Hospital, and

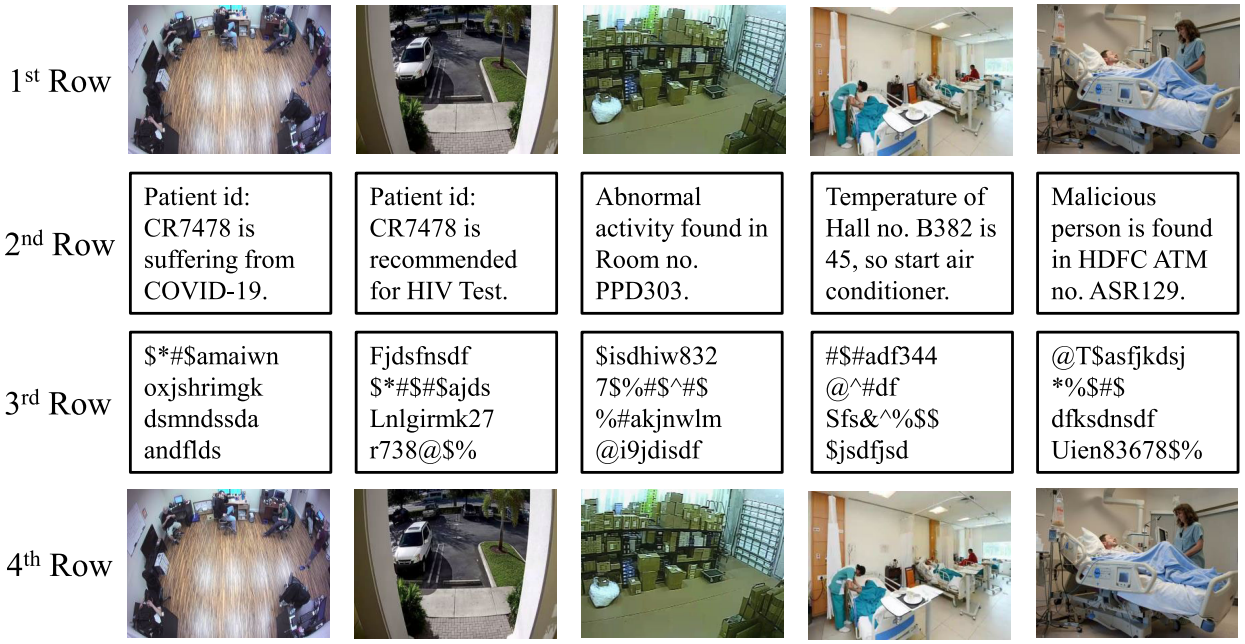

FIGURE 2. Visual analysis of EGCrypto: 1st row- Cover images, 2nd row- obtained sensed data (i.e., strings), 3rd row- encrypted sensed data, and 4th row- final embedded stego images.

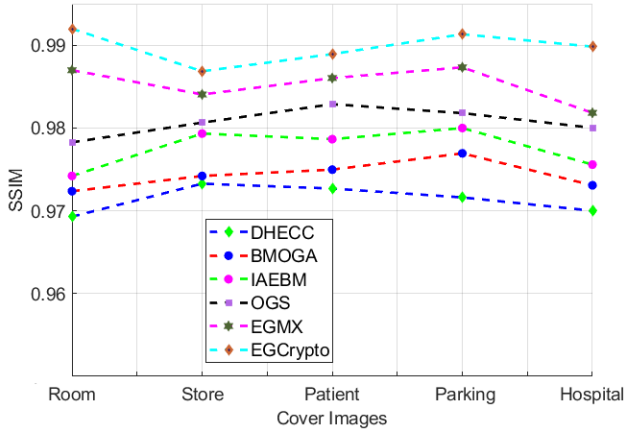

FIGURE 3. SSIM analysis among EGCrypto and competitive approaches.

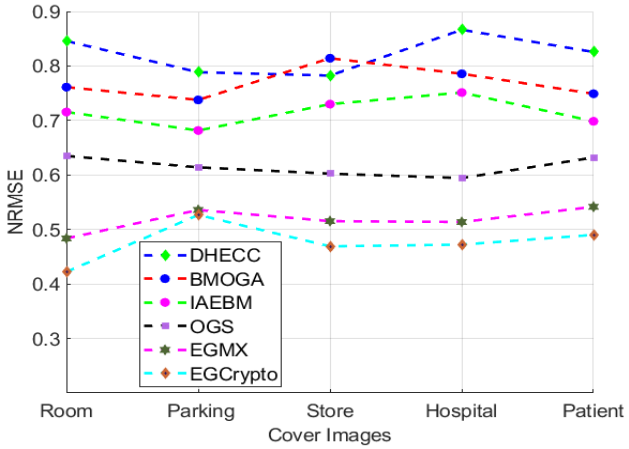

FIGURE 4. NRMSE analysis among EGCrypto and competitive approaches.

Patient. This indicates that EGCrypto performs well in preserving the content of the cover image while embedding the text, resulting in high-quality stego images. Other models such as DHECC, BMOGA, IAEBM, OGS, and EGMX also demonstrate relatively low NRMSE values, indicating their effectiveness. However, EGCrypto consistently outperforms them in terms of NRMSE values by 1.7682%, suggesting its superior ability to maintain image quality while embedding text.

Table 4 shows the carrier capacity analysis of EGCrypto. It is found that EGCrypto has significantly better carrier capacity values as compared to the existing steganography approaches. EGCrypto shows an average improvement in carrier capacity as 1.3829%.

TABLE 4. Carrier capacity analysis among EGCrypto and competitive approaches.

Models	Room	Parking	Store	Hospital	Patient
DHECC [17]	12.02	11.34	11.97	12.09	12.06
BMOGA [16]	13.31	12.81	13.68	11.89	12.97
IAEBM [15]	12.23	13.35	13.21	12.35	13.56
OGS [14]	12.03	12.88	13.31	12.49	13.24
EGMX [1]	14.02	14.17	14.91	14.27	14.34
EGCrypto	**14.83**	**14.95**	**15.69**	**15.05**	**15.12**

Figure 5 shows the embedding efficiency analysis. It should be maximum. EGCrypto obtains significantly better embedding efficiency values as compared to the competitive

approaches. EGCrypto has shown 1.9372% improvement over the existing approaches.

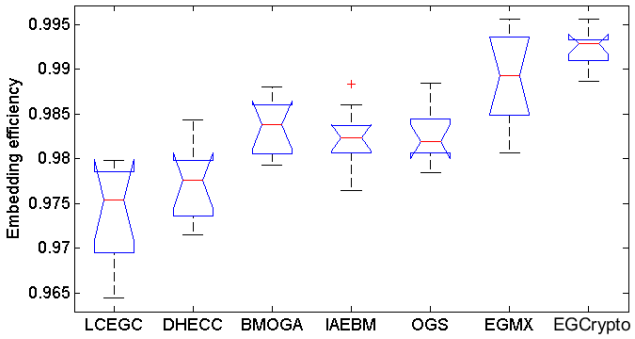

FIGURE 5. Embedding efficiency analysis among EGCrypto and competitive approaches.

Table 5 illustrates the execution time analysis (in seconds) of EGCrypto, including encryption and embedding. The results show that EGCrypto requires less time compared to existing approaches, reducing execution time by 0.9382%. This highlights the efficiency of EGCrypto for implementation in IoT networks.

TABLE 5. Execution time analysis (in seconds) among EGCrypto and competitive approaches.

Models	Room	Parking	Store	Hospital	Patient
DHECC [17]	1.34	1.42	1.47	1.21	1.37
BMOGA [16]	1.32	1.29	1.07	1.17	1.39
IAEBM [15]	0.99	1.05	1.04	0.92	0.92
OGS [14]	0.89	0.95	0.92	0.95	0.87
EGMX [1]	0.83	0.93	0.92	0.82	0.82
EGCrypto	**0.79**	**0.89**	**0.88**	**0.78**	**0.78**

Figure 6 show the recovery message's (i.e., secret message extracted from stego image) accuracy analysis. EGCrypto demonstrates a significantly higher accuracy compared to existing models, outperforming them by 1.2831%.

C. DISCUSSION

From the comparative analysis, it is found that DHECC [17] achieved a maximum PSNR of 36.69, maximum carrier capacity of 12.09, and maximum embedding efficiency of 86.64. BMOGA [16] obtained a maximum PSNR of 38.84, maximum carrier capacity of 13.68, and maximum embedding efficiency of 85.97. IAEBM [15] achieved a maximum PSNR of 38.78, maximum carrier capacity of 13.56, and maximum embedding efficiency of 83.92. OGS [14] achieved a maximum PSNR of 38.38, maximum carrier capacity of 14.91, and maximum embedding efficiency of 88.37. Although DHECC, BMOGA, IAEBM, and OGS achieved good results, EGMX [1] outperformed them with a maximum PSNR of 38.51, maximum carrier capacity of 14.91, and maximum embedding efficiency of 88.37.

EGCrypto achieved a maximum PSNR of 40.16, maximum carrier capacity of 15.69, and maximum embedding efficiency of 89.16. Thus, EGCrypto demonstrated significantly better performance compared to the existing approaches. Additionally, EGCrypto could encrypt and embed images in 0.78 seconds, which was significantly faster than the existing approaches. Therefore, EGCrypto could be efficiently utilized in IoT networks to provide secure data transmission.

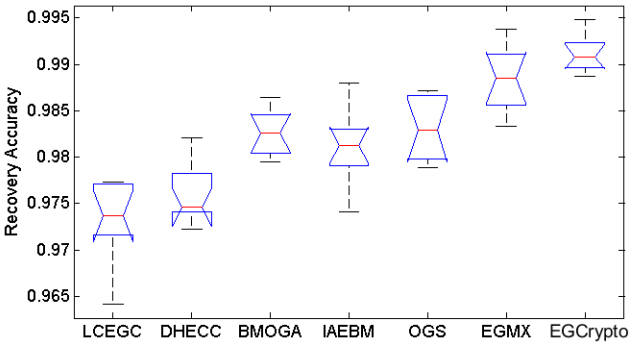

FIGURE 6. Recovery message's accuracy analysis among EGCrypto and existing secure IoT models.

V. CONCLUSION

A novel cryptography and steganography model was designed using low-complexity elliptic Galois cryptography and matrix XOR steganography. ZSADE was employed to tune the hyperparameters of EGCrypto. The IoT data was initially encrypted using low-complexity elliptic Galois cryptography and then embedded into optimal cover blocks of the cover image. This approach achieved secure communication in IoT architecture, ensuring the safe transfer and easy recovery of encrypted data. Extensive experimental results demonstrated that EGCrypto outperformed competitive models in terms of PSNR, SSIM, NRMSE, carrier capacity, and embedding efficiency by 1.8473%, 1.5490%, 1.7682%, 1.3829%, and 1.9372%, respectively. Furthermore, the improved computational speed of EGCrypto indicated its efficient implementation in securing IoT networks.

In the future, there are key areas to focus on for advancing EGCrypto in securing data transmission within IoT networks. First, optimization techniques and algorithms can be explored to enhance EGCrypto's efficiency and security. Efforts should also be made to strengthen its resilience against advanced attacks. Scalable solutions are needed to handle the growing data volume in large-scale IoT networks. Real-world implementation and validation of EGCrypto, along with standardization efforts, will contribute to its practical viability and widespread adoption.

REFERENCES

[1] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, "Securing data in Internet of Things (IoT) using cryptography and steganography techniques," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 73–80, Jan. 2020.

[2] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1646–1685, 3rd Quart., 2020.

[3] J. Cheng, Z. Pan, H. Liang, Z. Gao, and J. Gao, "Differential evolution algorithm with fitness and diversity ranking-based mutation operator," *Swarm Evol. Comput.*, vol. 61, Mar. 2020, Art. no. 100816.
[4] R. L. Rosa, M. J. De Silva, D. H. Silva, M. S. Ayub, D. Carrillo, P. H. J. Nardelli, and D. Z. Rodríguez, "Event detection system based on user behavior changes in online social networks: Case of the COVID-19 pandemic," *IEEE Access*, vol. 8, pp. 158806–158825, 2020.
[5] B. Yuan, C. Lin, H. Zhao, D. Zou, L. T. Yang, H. Jin, and C. Rong, "Secure data transportation with software-defined networking and k-n secret sharing for high-confidence IoT services," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 7967–7981, Sep. 2020.
[6] A. Waheed, M. Goyal, D. Gupta, A. Khanna, F. Al-Turjman, and P. R. Pinheiro, "CovidGAN: Data augmentation using auxiliary classifier GAN for improved COVID-19 detection," *IEEE Access*, vol. 8, pp. 91916–91923, 2020.
[7] M. J. Horry, S. Chakraborty, M. Paul, A. Ulhaq, B. Pradhan, M. Saha, and N. Shukla, "COVID-19 detection through transfer learning using multimodal imaging data," *IEEE Access*, vol. 8, pp. 149808–149824, 2020.
[8] L. Jiang, L. Chen, T. Giannetsos, B. Luo, K. Liang, and J. Han, "Toward practical privacy-preserving processing over encrypted data in IoT: An assistive healthcare use case," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10177–10190, Dec. 2019.
[9] S. Sakib, T. Tazrin, M. M. Fouda, Z. Md. Fadlullah, and M. Guizani, "DL-CRC: Deep learning-based chest radiograph classification for COVID-19 detection: A novel approach," *IEEE Access*, vol. 8, pp. 171575–171589, 2020.
[10] A. S. Unde and P. P. Deepthi, "Design and analysis of compressive sensing-based lightweight encryption scheme for multimedia IoT," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 1, pp. 167–171, Jan. 2020.
[11] Z. Liu, R. Azarderakhsh, H. Kim, and H. Seo, "Efficient software implementation of ring-LWE encryption on IoT processors," *IEEE Trans. Comput.*, vol. 69, no. 10, pp. 1424–1433, Oct. 2020.
[12] M. I. Mihailescu and S. L. Nita, "Elliptic-curve cryptography," in *Proc. Cryptography Cryptanalysis with C++ 23, Creating Program. Adv. Algorithms*. Cham, Switzerland: Springer, 2023, pp. 207–243.
[13] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, and S. W. Baik, "Secure surveillance framework for IoT systems using probabilistic image encryption," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3679–3689, Aug. 2018.
[14] H.-C. Liu and W. Chen, "Optical ghost cryptography and steganography," *Opt. Lasers Eng.*, vol. 130, Jul. 2020, Art. no. 106094.
[15] H. Antonio, P. W. C. Prasad, and A. Alsadoon, "Implementation of cryptography in steganography for enhanced security," *Multimedia Tools Appl.*, vol. 78, no. 23, pp. 32721–32734, Dec. 2019.
[16] H. M. Pandey, "Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography," *Future Gener. Comput. Syst.*, vol. 111, pp. 213–225, Oct. 2020.
[17] P. Vijayakumar, V. Vijayalakshmi, and G. Zayaraz, "An improved level of security for DNA steganography using hyperelliptic curve cryptography," *Wireless Pers. Commun.*, vol. 89, no. 4, pp. 1221–1242, Aug. 2016.
[18] Y. Zhang, H. Huang, Y. Xiang, L. Y. Zhang, and X. He, "Harnessing the hybrid cloud for secure big image data service," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1380–1388, Oct. 2017.
[19] L. Li, G. Wen, Z. Wang, and Y. Yang, "Efficient and secure image communication system based on compressed sensing for IoT monitoring applications," *IEEE Trans. Multimedia*, vol. 22, no. 1, pp. 82–95, Jan. 2020.
[20] Y. Kim, M. Sim, I. Moon, and B. Javidi, "Secure random phase key exchange schemes for image cryptography," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10855–10861, Dec. 2019.
[21] C. Guo, J. Jia, Y. Jie, C. Z. Liu, and K. R. Choo, "Enabling secure cross-modal retrieval over encrypted heterogeneous IoT databases with collective matrix factorization," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3104–3113, Apr. 2020.
[22] A. Singh, N. Chawla, J. H. Ko, M. Kar, and S. Mukhopadhyay, "Energy efficient and side-channel secure cryptographic hardware for IoT-edge nodes," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 421–434, Feb. 2019.
[23] V. M. Lidkea, R. Muresan, and A. Al-Dweik, "Convolutional neural network framework for encrypted image classification in cloud-based ITS," *IEEE Open J. Intell. Transp. Syst.*, vol. 1, pp. 35–50, 2020.
[24] J. Y. Kim, W. Hu, H. Shafagh, and S. Jha, "SEDA: Secure over-the-air code dissemination protocol for the Internet of Things," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 6, pp. 1041–1054, Nov. 2018.
[25] Y. Yang, X. Liu, and R. H. Deng, "Lightweight break-glass access control system for healthcare Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3610–3617, Aug. 2018.
[26] K. Javeed, A. El-Moursy, and D. Gregg, "EC-crypto: Highly efficient area-delay optimized elliptic curve cryptography processor," *IEEE Access*, vol. 11, pp. 56649–56662, 2023.
[27] S. Baccouri, H. Farhat, T. Azzabi, and R. Attia, "Lightweight authentication for IoT devices based on elliptic curve el gamal using ephemeral encoding parameters," in *Proc. IEEE Int. Conf. Adv. Syst. Emergent Technol. (IC_ASET)*, Apr. 2023, pp. 1–7.
[28] H. Kadry, A. Farouk, E. A. Zanaty, and O. Reyad, "Intrusion detection model using optimized quantum neural network and elliptical curve cryptography for data security," *Alexandria Eng. J.*, vol. 71, pp. 491–500, May 2023.
[29] A. Subashini and P. Kanaka Raju, "Hybrid AES model with elliptic curve and ID based key generation for IoT in telemedicine," *Measurement: Sensors*, vol. 28, Aug. 2023, Art. no. 100824.
[30] P. Choi, M.-K. Lee, J.-H. Kim, and D. K. Kim, "Low-complexity elliptic curve cryptography processor based on configurable partial modular reduction over NIST prime fields," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 65, no. 11, pp. 1703–1707, Nov. 2018.
[31] S. Bartolini, I. Branovic, R. Giorgi, and E. Martinelli, "Effects of instruction-set extensions on an embedded processor: A case study on elliptic curve cryptography over GF(2/sup m/)," *IEEE Trans. Comput.*, vol. 57, no. 5, pp. 672–685, May 2008.
[32] H. Tian, J. Qin, Y. Huang, Y. Chen, T. Wang, J. Liu, and Y. Cai, "Optimal matrix embedding for voice-over-IP steganography," *Signal Process.*, vol. 117, pp. 33–43, Dec. 2015.
[33] Q. Fan and X. Yan, "Self-adaptive differential evolution algorithm with zoning evolution of control parameters and adaptive mutation strategies," *IEEE Trans. Cybern.*, vol. 46, no. 1, pp. 219–232, Jan. 2016.