Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques

Manju Khari, Aditya Kumar Garg, Amir H. Gandomi, *Senior Member, IEEE*, Rashmi Gupta, *Member, IEEE*, Rizwan Patan, and Balamurugan Balusamy

***Abstract*—Internet of Things (IoT) is a domain wherein which the transfer of data is taking place every single second. The security of these data is a challenging task; however, security challenges can be mitigated with cryptography and steganography techniques. These techniques are crucial when dealing with user authentication and data privacy. In the proposed work, the elliptic Galois cryptography protocol is introduced and discussed. In this protocol, a cryptography technique is used to encrypt confidential data that came from different medical sources. Next, a Matrix XOR encoding steganography technique is used to embed the encrypted data into a low complexity image. The proposed work also uses an optimization algorithm called Adaptive Firefly to optimize the selection of cover blocks within the image. Based on the results, various parameters are evaluated and compared with the existing techniques. Finally, the data that is hidden in the image is recovered and is then decrypted.**

***Index Terms*—Confidential data, cryptography, data security, Internet of Things (IoT), steganography, user authentication.**

I. Introduction

THE INTERNET of Things (IoT) is a network of connected vehicles, physical devices, software, and electronic items that facilitate data exchange. The purpose of IoT is to provide the IT-infrastructure for the secure and reliable exchange of "Things" [1]. The foundation of IoT mainly consists of the integration of sensors/actuators, radio frequency identification (RFID) tags, and communication technologies. The IoT explains how a variety of physical items and devices can be integrated with the Internet to permit those objects to cooperate and communicate with each other to reach common goals. The IoT consists mostly of little materials that are associated together to facilitate collaborative calculating situations. Constraints of the IoT include energy budget, connectivity, and computational power [2].

Although IoT devices have made life easier, little attention has been given to the security of these devices. Currently, the focus of developers is to increase the capabilities of these devices, with little emphasis on the security of the devices. The data that is transferred over the IoT network is vulnerable to attack. This data is needed to be secured to protect the privacy of the user. If there is no data security, then there is a possibility of data breach and thus, personal information can be easily hacked from the system. Some of the important concepts of IoT involve identification and authentication. These concepts are inter-related to each other as cryptographic functions that are necessary to ensure that the information is communicated to the correct device and if the source is trusted or not. With the lack of authentication, a hacker can easily communicate to any device.

Whenever two devices communicate with each other, there is a transfer of data between them. The data can also be very sensitive and personal. Therefore, when this sensitive data is moving from device to device over the IoT network, then there is a need for encryption of the data. Encryption also helps to protect data from intruders. The data can be easily encrypted with the help of cryptography, which is the process of converting simple text into unintelligible text. The primary objectives of cryptography are confidentiality, integrity, nonrepudiation, and authentication. Elliptic curve cryptography (ECC) is one of the cryptographic algorithms that is used in the proposed work. ECC is a public key cryptographic technique based on the algebraic structure of elliptic curves over finite fields.

In addition, to the cryptographic techniques, another method, named steganography is used in the proposed work which helps to provide additional security to the data. Steganography hides encrypted messages in such a way that no one would even suspect that an encrypted message even exists in the first place. In modern digital steganography, encryption of data occurs using typical cryptographic techniques. Next, a special algorithm helps to insert the data into redundant data that is part of a file format, such as a JPEG image. The proposed work uses Matrix XOR steganography to provide additional security. The image block is optimized with the help of Adaptive Firefly algorithm in which the encrypted data is hidden in a selected block from a huge image block.

The remaining part of this paper is organized as follows. Section II discussed work that relates to the security of IoT communication. Section III proposes methodology for

Manuscript received July 22, 2018; revised October 16, 2018; accepted February 20, 2019. Date of publication March 27, 2019; date of current version December 31, 2019. This paper was recommended by Associate Editor Y. Yuan. *(Corresponding author: Amir H. Gandomi.)*

M. Khari, A. K. Garg, and R. Gupta are with the Department of CSE, Ambedkar Institute of Advanced Communication Technology and Research, New Delhi 110031, India (e-mail: manjukhari@yahoo.co.in; adityagarg2607@gmail.com; rashmig71@yahoo.com).

A. H. Gandomi is with the Analytics and Information Systems, School of Business, Stevens Institute of Technology, Hoboken, NJ 07030 USA (e-mail: a.h.gandomi@stevens.edu).

R. Patan and B. Balusamy are with the School of Computing Science and Engineering, Galgotias University, Greater Noida 201310, India (e-mail: prizwan5@gmail.com; kadavulai@gmail.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSMC.2019.2903785

improvements in medical data security. Section IV describes the experimental setup and results. Section V concludes this paper.

II. Related Work

This section presents an overview of existing studies of healthcare data security within the IoT network.

Daniels *et al.* [3] introduced security microvisor (SμV) middleware, which uses software virtualization and assembly level code verification to provide memory isolation and custom security. Banerjee *et al.* [4] presented energy-efficient datagram transport layer security (eeDTLS), which is a low-energy variant of datagram transport layer security (DTLS) that had the same security strength but a lower energy requirement.

Manogaran *et al.* [5] proposed a system in which medical sensor devices are embedded in the human body to collect clinical measurements of patients. Significant changes in respiratory rate, blood pressure, heart rate, blood sugar, and body temperature that exceed standard levels are detected by the sensors, which generate an alert message containing relevant health information that is sent to the doctor, with the help of a wireless network. This system uses a vital management security mechanism to protect large amounts of data in the industry.

There is an urgent need for the securing the data that is transmitted every second over the IoT network. Some of the existing studies for data security are shown below.

Sun *et al.* [6] proposed CloudEyes, a cloud-based anti-malware system. The proposed system provided efficient and trusted security services to the devices in the IoT network. Ukil *et al.* [2] studied the requirements of embedded security, provided methods and solutions for resisting cyber-attacks, and provided technology for tamper proofing the embedded devices based on the concept of trusted computing.

Chervyakov *et al.* [7] provided a data storage scheme for the least probability of data redundancy, data loss, and the speed of encoding and decoding, that can cope with different objective preferences, workloads, and storage properties. This analysis showed that if the selection of redundant residue number system (RRNS) parameters is accurate, then it not only allows increased safety and reliability but it also helps to increase the speed of processing the encrypted data. The applications used on IoT platforms generally require more data than traditional applications. Raza *et al.* [8] presented lightweight secure CoAP for the IoT (Lithe), which helped in the development of a novel DTLS header compression scheme designed to reduce energy consumption with the help of 6LoWPAN. Moreover, security is not compromised with the DTLS header compression scheme. Vučinić *et al.* [9] proposed object security architecture (OSCAR), which is the architecture for end-to-end security in the IoT. OSCAR is based on the concept that the security of an object is related to the security of the application payload.

Yang *et al.* [10] proposed the lightweight break-glass access control (LiBAC) system in which medical files can be encrypted in two ways: 1) attribute-based access and 2) break-glass access. In standard situations, a medical worker can decrypt and access data if the attribute set satisfies the access policy of a medical file. In an emergency, a break-glass access mechanism is used that can bypass the access policy of the medical file so that emergency medical care workers or rescue workers can access the data in a timely fashion.

Safety and confidentiality of information sent over the IoT network is a priority for the healthcare and medical industries. Bairagi *et al.* [11] developed three methods for hiding information so that communication over the IoT network can be preserved with the help of steganography. Information is hidden in the deepest layer of the image with the help of minimal distortion in the least significant bit (LSB) and the sign of the information can also be utilized. This technique improved imperceptibility and ability when compared to the actual method.

Huang *et al.* [12] presented a steganography scheme that employs vector quantization (VQ) transformation in which LSB embeds secret data into a cover image. In the first level, the pixels of a 4×4 VQ-transformed image block are separated into two different groups: 1) the LSB group and 2) the secret data group. In the second level, VQ indexes are embedded in the LSB group and secret data are embedded in the secret group. Shanableh *et al.* [13] proposed the flexible macro-block ordering (FMO) feature of H.264/AVC to hide message bits. The macroblocks are assigned to arbitrary slice groups with reference to the content of the message bits to be hidden. In the proposed method, a maximum payload of three message bits per macroblock is achieved.

Liao *et al.* [14] proposed a new medical JPEG image steganographic scheme that is based on the dependencies of interblock coefficients. The basic strategy that is used in this paper consists of preserving the differences among discrete cosine transform (DCT) coefficients at the same position in adjacent DCT blocks as much as possible.

The development of IoT was related to the security of end-user's privacy and communication. However, the technical heterogeneity, materials, and asymmetric nature of communication between the Internet and sensor nodes created challenging security issues.

III. Proposed Approach

A. Elliptic Galois Cryptography and Steganography Protocol

This paper proposes the elliptic Galois cryptography (EGC) protocol for protection against data infiltration during transmission over the IoT network. In the proposed work, different devices in the IoT network transmit data through the proposed protocol as a part of the controller. The encrypted algorithm within the controller encrypts the data using the EGC protocol and then the encrypted and secured message is hidden in layers of the image, with help from the steganography technique. The image can then be easily transferred throughout the Internet such that an intruder cannot extract the message hidden inside the image. Initially, the EGC technique encrypts confidential data. Subsequently, the encoded secret message is inserted within the image by the XOR steganography

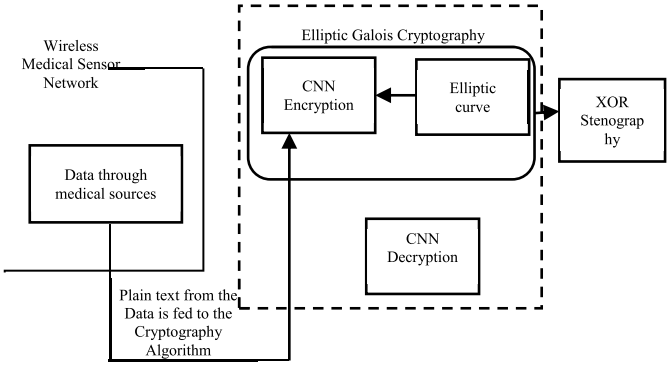


Fig. 1. EGC.

technique. Next, an optimization algorithm called the Adaptive Firefly algorithm is used to select a block in the image.

1) Elliptic Galois Cryptography: ECC, commonly known as the public key encryption technique, is based on elliptic curve theory. The keys are generated by using the properties of elliptic curve equations instead of traditional methods.

The proposed work uses EGC (Fig. 1). For improving the efficiency of calculations and to reduce the complexities of rounding errors, the elliptic curve over the Galois field (F_a) is used. The value of the Galois field must be greater than one. The elements of a Galois field GF(P) are as follows:

$$\begin{aligned}\mathrm{GF}(P) = {} & (0, 1, 2, \ldots, P-1)U \\ & (P, P+1, P+2, \ldots, P+P-1)U \\ & \left(P^2, P^2+1.P^2+2, \ldots, P^2+P-1\right)U \cdots U \\ & \left(P^{n-1}, P^{n-1}+1, P^{n-1}+2, \ldots, P^{n-1}+P-1\right)\ [15]\end{aligned}$$

where $P \in \mathbb{P}$ and $n \in Z_+$. The order of the Galois field is given by P^n and P is called the characteristic of the field. GF stands of Galois Field. The degree is at most $n-1$ for each polynomial [15].

The secret key/public key is generated by the owner of the medical data and is used to access the authorized data. The generation of the key is crucial as both the public key and the private key need to be generated. The message will be encrypted by the user's public key and the message can only be decrypted with the help of a private key. Every user on the network develops key pairs that are used for encryption and decryption.

An elliptic curve over a Galois field GF (P) greater than three ($P > 3$) that was formed with the help of variables g and h within the field GF (P) and elements such as (x, y) gives the following equation [15]:

$$y^2 = x^3 + h \bmod P + gx. \tag{1}$$

For different inputs and values of h and g, different elliptic curve points with values x and y exist that are within the range of the Galois field [x, y belongs to GF (P)]. The public key thus generated is a random point that lies on the elliptic curve and the random number generated is the private key. Multiplication of the private key by the generator point G in the curve provides the public key.

Let P and Q be two points on an elliptic curve such that [15]

$$U = GR \tag{2}$$

where U is the public key, R is the private key, and G is the generator point. An elliptic curve group is formed with the help of this point only if no repeated factors are contained in $27h^2 + 4g^3 = 0(\mathrm{mod}P)$ and $x^3 + gx + h$.

The mathematical structure for addition over GF (P), emulating the conditions are given by the following equation.

Let $P(x_1,\ y_1)$ and $Q(x_2, y_2)$ be components of the elliptic curve graph. Then, $P + Q = (x_3,\ y_3)$ where

$$x_3 = \lambda^2 - x_1 - x_2 \text{ and } y_3 = \lambda(x_1 - x_3) - y_1. \tag{3}$$

Then, λ resolves as

$$\lambda = \begin{cases} \frac{3x_1^2+a}{2y_1} & \text{if } P = Q \\ \frac{y_2-y_1}{x_2-x_1} & \text{if } P \neq Q. \end{cases} \tag{4}$$

After the completion of the key generation step, encryption can be performed with the chaotic neural network, as described below.

a) Encryption based on the chaotic neural network: Suppose there is a chaotic neural network with n inputs and outputs. The input to this network is the plain text that is converted into cipher text with the help of ECC-based Galois field. The input text is denoted as $(P_1, P_2, \ldots, P_n)$ and the cipher text is denoted as $(C_1, C_2, \ldots, C_n)$.

Step 1: Generate a chaotic sequence

$$(g(n),\ g(n+1), \ldots, g(n+n+1)).$$

This chaotic sequence is known as the cipher text.

Step 2: The plain text is input into the network $(P_1, P_2, \ldots, P_n)$ and is then converted into the chain of binary data. The binary sequence thus generated is denoted by $(b_1, b_2, \ldots, b_n)$ and the formula used to generate this binary data is as follows:

$$b(8n-8)b(8n-7)\cdots b(8n-2)b(8n-1)$$

where

$$n = 1, 2, \ldots, n.$$

Step 3: The binary sequence that was generated in the previous step helps to perform weight factor generation, which varies based on input functions. The equation for weight factor generation is as follows:

$$W_j = \left\{ \begin{matrix} 1 & \text{if } b(j + 8 \times n) = 0 \\ -1 & \text{if } b(j + 8 \times n) = 1 \end{matrix} \right\}. \tag{5}$$

According to the above equation, there are different weight factors for different inputs and the value of j varies from zero to seven.

Step 4: After the creation of weight factors, a bias function is introduced for every chaos, which is generated by using weight factors. The problem of singularity is avoided with the help of this bias function.

The equation for the bias function is as follows:

$$d_j' = f\left(W_j \times d_j\right) \tag{6}$$

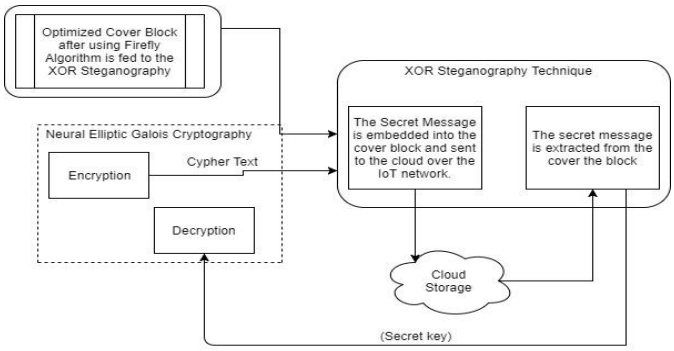


Fig. 2. Proposed Matrix-XOR steganography technique.

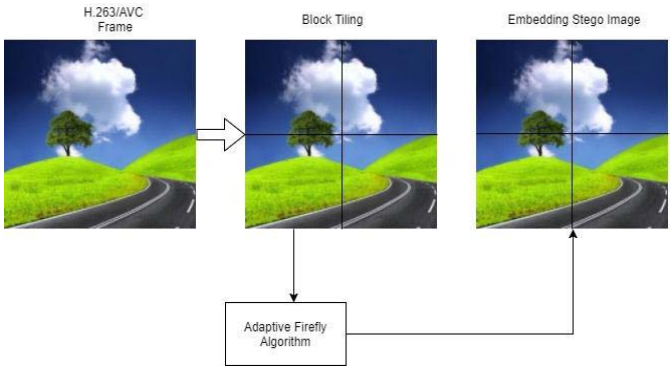


Fig. 3. Adaptive Firefly optimization.

d'_j is the bias function, W_j is the weight factor, and d_j is the input function.

Step 5: The cipher text is generated, based on the weight factor and the input function

$$g(i) = x_n(n) \times (1 - y_n) + d'_j. \tag{7}$$

In the above equation, (x_n, y_n) are the points on the elliptic curve (secret key). After creation of the cipher text, this text is stored on a cloud platform with the help of the Matrix XOR Encoding steganography technique.

b) Matrix XOR: Matrix XOR is a technique for hiding encrypted data in which the encrypted data is hidden inside the H.264 video file [16]. For this technique, the Firefly optimization technique is used to optimize the blocks of the image. With the help of this optimization technique, block selection among the whole image is possible.

The proposed OM-XOR steganography technique is shown in Fig. 2. The initial image is tiled and the secret data is hidden on the cover block with the help of Adaptive Firefly optimization. The tiled image is recombined and decoded. Finally, the encrypted message is decoded by using the secret key.

Step 1 (Permutative Straddling): When there is no need to use the full size to hide the encrypted message, the fragment of the image remains unused. Permutative straddling is used to eliminate this problem. This technique scatters the secret message over the complete carrier medium; i.e., over the complete image. Permutation depends on a key-based password. If the user has the correct key, the same permutation can be repeated.

Step 2 (Encoding): There are many algorithms for embedding secret information into an image block. By introducing the Matrix XOR encoding technique, the proposed work enhances the embedding efficiency. The conversion of triple(f, k, $g(i)$) to quad(e, k, $g(i)$) and the compression of the encrypted message enhances the efficiency of this technique.

The Matrix XOR technique embeds the $g(i)$ chaotic sequence (secret data) in the optimized image block (cover block). In this process, the one-bit block from the cover block is replaced with the encrypted information block. The one-bit embedding process is carried out using the following equation:

$$M_e = D \oplus C \tag{8}$$

where the binary data bit is D and C is the binary image bit block. Two conditions must be satisfied to carry out this embedding process.

Condition 1: For the two blocks, if the XOR operation results in a zero, then there is no requirement to change the last bit position.

Condition 2: For the two blocks, if the XOR operation does not result in zero, then there is a change of the cover block (i.e., zero to one or one to zero).

After deciding the bit position for the cover block, the embedding process is executed based on the following equation:

$$M_e = \left\{\left((d(i) \oplus c(i))c'(i)\right) + (d(i) \oplus c(i))' c'(i)\right)\right\}. \tag{9}$$

Optimization of the cover block is handled with the help of the Firefly algorithm, as discussed below.

Step 3 (Adaptive Firefly Optimization): The Adaptive Firefly algorithm (Fig. 3) is described by these three standard rules.

1) All the fireflies are unisex so that all fireflies are attracted to each other.
2) Attractiveness between the fireflies is proportional to their brightness; thus, a less bright firefly will move toward a brighter one. With increased distance between fireflies, both the attractiveness and brightness decrease.
3) The brightness of a firefly is determined by the landscape of the objective function. Two important issues persist in the Firefly algorithm: a) formulation of the attractiveness and b) the variation of light intensity [17].

The main motive is to reduce the count of the pixel blocks. For this, some control parameters are initialized, such as:

1) initial brightness $b = 0.4$;
2) randomization parameter $\eta = 0.5$;
3) coefficient of light absorption $\gamma = 0.5$.

The following equation is used to calculate multiobjective functions [17]:

$$f(x) = [\min\{(c)\}]. \tag{10}$$

For a given medium with a fixed light absorption coefficient, the light intensity I varies with the distance c, according to the following equation [17]:

$$I = I_0 e^{-\gamma c} \tag{11}$$

where I_0 is the original light intensity, In (10), the cost function "c" should be minimal in order to optimize the number of blocks of an image. As attractiveness of fireflies is directly related to LI with a neighboring firefly, β is defined as follows [17]:

$$\beta(r) = \beta_0 e^{-\gamma c^k}; \quad k \geq 1 \tag{12}$$

where β_0 is defined as attraction per $c = 0$ and γ is defined as the illuminated saturation immersion coefficient. $\gamma = [0, \infty]$ and $\gamma = 1$. In certain circumstances, β_0 is expressed as $\beta_0 = 1$ and $k = 2$ since most fireflies are visible due to a constrained separation.

Suppose that, for two fireflies i and j, room arrangement is n-dimensional. The distance between the x_i and y_i, the individual count can be create using Cartesian (c) count calculation, as follows:

$$c = \sqrt{\left(\sum_{k=1}^{d} \left(x_j - x_i\right)^2\right) + \left(y_i - y_j\right)}. \tag{13}$$

Next, a time-varying AW is developed to update the position of the fireflies. Over the period, the AW diminishes. The AW value is updated with the following equation:

$$S_{\text{new}}(t+1) = f(x) + \beta_0 e^{-\gamma c^m}\left(x_j - x_i\right) + \alpha\varepsilon_i. \tag{14}$$

Equation (14) shows that the ith firefly moves toward the jth firefly, which is more attractive in the optimization.

Where location of the ith firefly is $S_{\text{new}}(t+1)$, after $t+1$th interchange; randomization parameter is α; $\alpha \in [0, 1]$ in place of major difficulties $\alpha = 0.1$. The random numbers vector is ε_i. Thus, the ith element is updated as follows:

$$S_{\text{new}} = S_{\text{old}} + S_{\text{new}}(t+1). \tag{15}$$

Thus, complexity is reduced with the help of the Firefly optimization algorithm and helps to achieve better performance and results in the case of block selection.

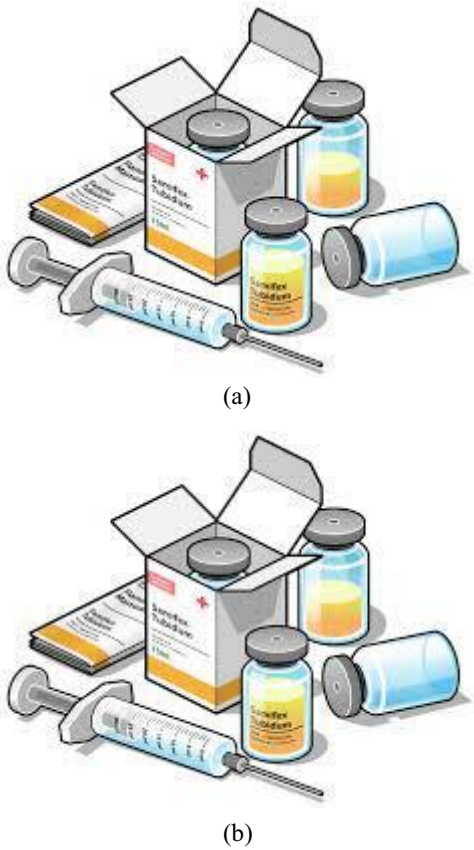
c) Data retrieval: On the receiver side, data is retrieved with the help of the OM-XOR retrieval process. Encrypted data that was stored in the cloud is retrieved with the OM-XOR decoding process. Finally, the decoded information that was encrypted using the steganography technique is then decrypted with the help of CNN decryption using the private key of the user.

IV. Experimental Results and Discussion

The MATLAB simulation tool is used for implementation of the proposed work. The proposed work uses H.264/AVC video standards.

A. Database Description

Some official videos, such as MPEG 2 and MPEG 4 help to achieve a high compression ratio. Although high-performance efficiency is achieved, there is a loss in the compression ratio [18]. This problem is solved with supreme progressive film coding model up-to-date. H.264 MPEG-4 is similarly used for this process and the video quality of this H.264/AVC is



(a)

(b)

Fig. 4. Matrix XOR stegno image and cover image. (a) Cover image. (b) Stegno image.

H.264, and each video has 30 frames/s. Video resolution is 304 × 204 pixels.

The cover block image, which is the converted frame for the H.264/AVC video, is depicted in Fig. 4(a). Fig. 4(b) corresponds to the stegno image in which medical data is hidden in the profound layer of the cover block. Thus, with the help of the proposed method, the medical data of the patient is securely hidden within the image.

The data that is hidden with the proposed method cannot be extracted by any unauthorized person since only the ECC secret key can retrieve the original data.

B. Parameter Evaluation

For showing the efficiency of the proposed EGC system, embedding efficiency, carrier capacity, peak signal to noise ratio (PSNR), mean square error (MSE), and time complexity were evaluated. The results of all these parameters were compared to some of the existing methods, such as LSB steganography, FMO steganography, and optimized modified matrix encoding (OMME) steganography. Various graphs have been put-up to efficiently show the comparison between the proposed work and the existing methods. The parameters are evaluated as follows.

1) Embedding Efficiency (E_η): Embedding efficiency is defined as the rate of the amount of secrets bits stored and embedded in an image block, which helps to show the

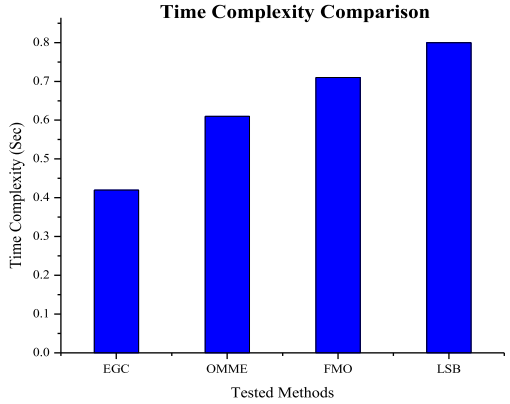


Fig. 5. Time complexity comparison analysis.

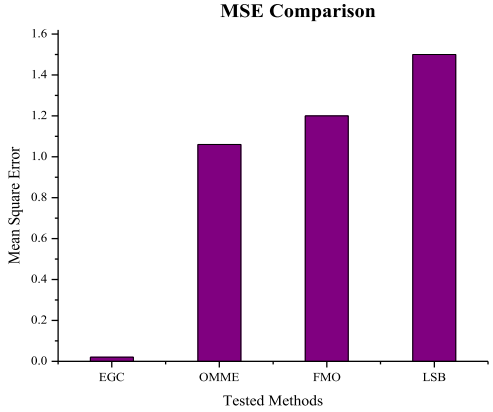


Fig. 6. MSE comparison analysis.

effectiveness of the system

$$E_\eta = \frac{k+1}{k} n \tag{16}$$

where k is the bit in the cover block and n is the total quantity of secret bits within the embedding technique.

2) Carrier Capacity (C): Carrier capacity is the ability of the system to hide encrypted data inside the cover block. The value of carrier capacity is directly proportional to the performance

$$C = \frac{\text{Total number of secret bits}}{\text{Number of bits in the cover block}}. \tag{17}$$

Carrier capacity is the other name for hiding capacity and is measured in terms of bits per pixel (BPP).

3) Mean Square Error: MSE is the amount of similarity and the range of distortion in an image and it also helps in the measurement of the amount of reliability

$$\text{MSE} = \frac{1}{N} \sum_{i=X,Y}^{n} (X - Y)^2. \tag{18}$$

N is the total pixel within the image, X is the initial image, and Y is the final Stegno image.

4) Peak Signal to Noise Ratio: PSNR calculates the invisibility of the image. PSNR can also be used for dynamic range images

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}}. \tag{19}$$

Time Complexity: Time complexity is the amount of time taken between the encryption and decryption process. To increase the efficiency of the system, time complexity must be lowered.

Comparative analyses are shown in Figs. 4–6.

The EGC protocol gave better performance regarding embedding efficiency, carrier capacity, PSNR, MSE, and time complexity as compared to other techniques, such as LSB steganography, FMO steganography, and OMME steganography. As depicted in Figs. 5 and 6, the MSE and time complexity of the proposed EGC protocol is very low, as compared to existing methods. The proposed protocol yielded better PSNR performance as compared to LSB, FMO, and OMME (32.42%, 45.62%, and 52.24% better performance,

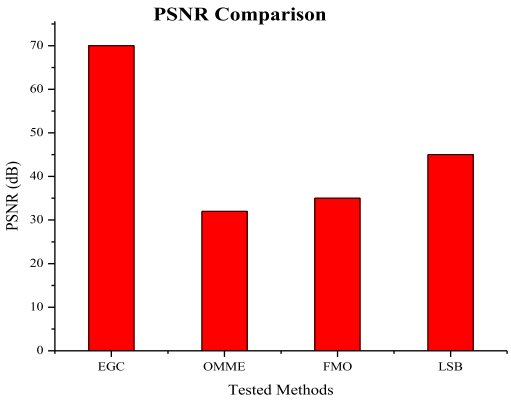


Fig. 7. PSNR comparison analysis.

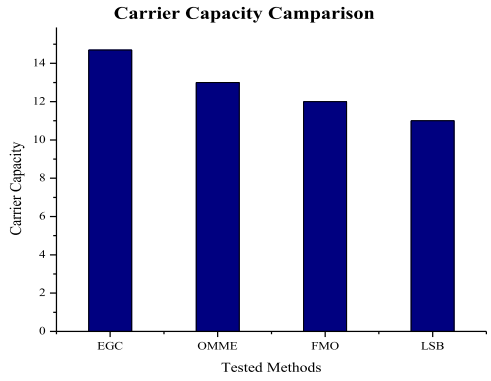


Fig. 8. Carrier capacity analysis.

respectively), as depicted in Fig. 7. Fig. 8 shows that the proposed protocol yielded better carrier capacity performance as compared to LSB, FMO, and OMME (0.33%, 16.35%, and 9.36% better performance, respectively). As shown in Fig. 9, the proposed protocol yielded better embedding efficiency performance as compared to LSB, FMO, and OMME (31%, 21%, and 1.16% better performance, respectively). Therefore, overall the proposed method is well optimized and yielded better results when compared to the existing protocols.

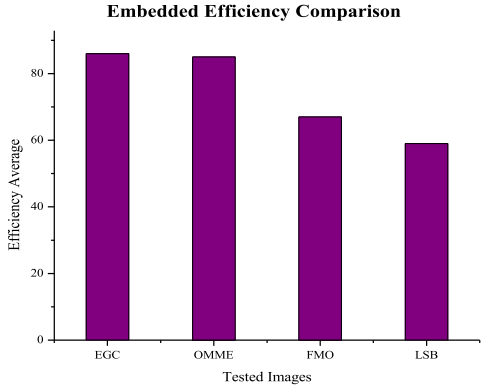


Fig. 9. Embedding efficiency analysis.

V. Conclusion

The EGC protocol generated high levels of data security to serve the purpose of protecting data during transmission in the IoT. With the novel ECC over Galois field, the proposed EGC protocol provided better security. Due to the enhanced embedding efficiency, advanced data hiding capacity can be achieved. With the help of the proposed protocol and Adaptive Firefly optimization, any amount of data can be easily transmitted over the IoT network securely hidden within the profound layers of images. Performance is evaluated with parameters, such as embedding efficiency, PSNR, carrier capacity, time complexity, and MSE. Finally, the proposed work is implemented in a MATLAB simulator, and approximately 86% steganography embedding efficiency was achieved. Results from this proposed protocol were compared to existing methods, such as OMME, FMO, and LSB.

References

[1] R. H. Weber, "Internet of Things—New security and privacy challenges," *Comput. Law Security Rev.*, vol. 26, no. 1, pp. 23–30, 2010.

[2] A. Ukil, J. Sen, and S. Koilakonda, "Embedded security for Internet of Things," in *Proc. 2nd Nat. Conf. Emerg. Trends Appl. Comput. Sci. (NCETACS)*, Mar. 2011, pp. 1–6.

[3] W. Daniels *et al.*, "SμV-the security microvisor: A virtualisation-based security middleware for the Internet of Things," in *Proc. ACM 18th ACM/IFIP/USENIX Middleware Conf. Ind. Track*, Dec. 2017, pp. 36–42.

[4] U. Banerjee, C. Juvekar, S. H. Fuller, and A. P. Chandrakasan, "eeDTLS: Energy-efficient datagram transport layer security for the Internet of Things," in *Proc. GLOBECOM IEEE Glob. Commun. Conf.*, Dec. 2017, pp. 1–6.

[5] G. Manogaran, C. Thota, D. Lopez, and R. Sundarasekar, "Big data security intelligence for healthcare industry 4.0," in *Cybersecurity for Industry 4.0*. Cham, Switzerland: Springer, 2017, pp. 103–126.

[6] H. Sun, X. Wang, R. Buyya, and J. Su, "CloudEyes: Cloud-based malware detection with reversible sketch for resource-constrained Internet of Things (IoT) devices," *Softw. Pract. Exp.*, vol. 47, no. 3, pp. 421–441, 2017.

[7] N. Chervyakov *et al.*, "AR-RRNS: Configurable reliable distributed data storage systems for Internet of Things to ensure security," *Future Gener. Comput. Syst.*, vol. 92, pp. 1080–1092, Mar. 2019.

[8] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight secure CoAP for the Internet of Things," *IEEE Sensors J.*, vol. 1, no. 10, pp. 3711–3720, Oct. 2013.

[9] M. Vučinić *et al.*, "OSCAR: Object security architecture for the Internet of Things," *Ad Hoc Netw.*, vol. 32, pp. 3–16, Sep. 2015.

[10] 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. 2017.

[11] A. K. Bairagi, R. Khondoker, and R. Islam, "An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures," *Inf. Security J. Glob. Perspective*, vol. 25, nos. 4–6, pp. 197–212, 2016.

[12] C.-T. Huang, M.-Y. Tsai, L.-C. Lin, W.-J. Wang, and S.-J. Wang, "VQ-based data hiding in IoT networks using two-level encoding with adaptive pixel replacements," *J. Supercomput.*, vol. 74, no. 9, pp. 4295–4314, 2018.

[13] T. Shanableh, "Data hiding in MPEG video files using multivariate regression and flexible macroblock ordering," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 455–464, Apr. 2012.

[14] X. Liao, J. Yin, S. Guo, X. Li, and A. K. Sangaiah, "Medical JPEG image steganography based on preserving inter-block dependencies," *Comput. Elect. Eng.*, vol. 67, pp. 320–329, Apr. 2018.

[15] C. J. Benvenuto, *Galois Field in Cryptography*, Univ. Washington, Seattle, WA, USA, 2012.

[16] T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 7, pp. 560–576, Jul. 2003.

[17] A. H. Gandomi, X. S. Yang, and A. H. Alavi, "Mixed variable structural optimization using firefly algorithm," *Comput. Struct.*, vol. 89, nos. 23–24, pp. 2325–2336, 2011.

[18] R. Hegde and S. Jagadeesha, "An optimal modified matrix encoding technique for secret writing in MPEG video using ECC," *Comput. Stand. Interfaces*, vol. 48, pp. 173–182, Nov. 2016.

Manju Khari received the B.Tech. degree from the Indira Gandhi Institute of Technology under Guru Gobind Singh Indraprastha (GGSIP) University, New Delhi, India, in 2004, the M.Tech. degree in information security from the Ambedkar Institute of Technology under GGSIP University in 2010, and the Ph.D. degree in computer science and engineering from the National Institute of Technology Patna, Patna, India, in 2016.

She is an Assistant Professor with the Ambedkar Institute of Advanced Communication Technology and Research, Under Govt. of NCT Delhi affiliated with Guru Gobind Singh Indraprastha University. She is also the Professor-in-Charge of the IT Services of the Institute and has experience of over 12 years in Network Planning and Management. She has 70 published papers in refereed National/International Journals and Conferences, such as IEEE, ACM, Springer, Inderscience, and Elsevier, 6 book chapters in a Springer. She has also coauthored two books published by NCERT of XI and XII. Her current research interests include software testing, software quality, software metrics, information security, optimization, and nature-inspired algorithm.

Aditya Kumar Garg is currently pursuing the B.Tech. degree in computer science with the Ambedkar Institute of Communication Technologies and Research, New Delhi, India.

His current research interests include developing Web Applications, image processing, machine learning algorithms, and their applications.

Amir H. Gandomi (SM'19) received the Ph.D. degree in engineering from the University of Akron, Akron, OH, USA, in 2015.

He used to be a Lecturer in several universities. He was a Distinguished Research Fellow in headquarter of BEACON NSF Center located at Michigan State University, East Lansing, MI, USA. He is an Assistant Professor of Analytics and Information Systems with the School of Business, Stevens Institute of Technology, Hoboken, NJ, USA. He has published over 130 journal papers and four books. Some of those publications are now among the hottest papers in the field and collectively have been cited over 11 000 times with an H-index of 53. He has been named as Highly Cited Researcher (top 1%) for two consecutive years, 2017 and 2018, and One of the World's Most Influential Scientific Minds. He is currently ranked 19th in GP bibliography among over 11 000 researchers. He is part of a NASA Technology cluster on big data, artificial intelligence, and machine learning. His current research interests include global optimization and (big) data mining using machine learning and evolutionary computations in particular.

Dr. Gandomi has also served as an Associate Editor, an Editor, and a Guest Editor in several prestigious journals and has delivered several keynote/invited talks.

Rashmi Gupta (M'13) received the B.Tech. degree from the Institute of Electronics and Telecommunication Engineers under Delhi University, New Delhi, India, in 1997, and the M.E. and Ph.D. degrees in electronics and communication engineering from the Delhi College of Engineering under Delhi University, New Delhi, in 2005 and 2014, respectively.

He was a Senior Engineer with Calcom Group of companies from 1991 to 1999, a Lecturer with the Electronics and Communication Engineering Department, Hindu Institute of Technology, Sonipat, India, and a Senior Lecturer with the Maharaja Agrasen Institute of Technology, New Delhi, from 1999 to 2003. She is currently a Professor with the Electronics and Communication Engineering Department, Ambedkar Institute of Communication Technologies and Research (Govt. of NCT of Delhi). She has authored over 70 research papers in various renowned international journal and conferences. Her current research interests include machine learning, computer vision, and signal and image processing.

Dr. Gupta is a Fellow Member of IETE.

Rizwan Patan received the B.Tech. and M.Tech. degrees in computer science and engineering from Jawaharlal Nehru Technological University Anantapur, Anantapur, India, in 2012 and 2014, respectively, and the Ph.D. degree in computer science and engineering from the School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India, in 2017.

He is an Assistant Professor with the School of Computing Science and Engineering, Galgotias University, Greater Noida, India. He has published reputed 8 SCI journals and 20 free Scopus indexed journals, and also presented paper in National/International Conferences, published book chapters in CRC Press, IGI Global, Elsevier, and edited as books. He has two Indian patents.

Dr. Patan is a Guest Editor of the *International Journal of Grid and Utility Computing* (Inderscience), Recent Patents on Computer Science, and Information Medical Unlock (Elsevier).

Balamurugan Balusamy received the B.E. degree in computer science and engineering from Bharathidasan University, Tiruchirappalli, India, in 2001, the M.E. degree in computer science and engineering from Anna University, Chennai, India, in 2005, and the Ph.D. degree in computer science and engineering from VIT University, Vellore, India, in 2015.

He is a Professor with the School of Computing Science and Engineering, Galgotias University, Greater Noida, India. His current research interests include big data, network security, and cloud computing. He is pioneer researcher in the areas of big data and IoT and has published over 70 papers in various top international journals.