IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURING DATA IN INTERNET OF THINGS (IOT) USING CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES

1.D. Madhu,2.Munishankar,2.M.Priyadharshini,3.B.Rahulchand,4S.Nagaphanisri,5.G.Ranjitkumar

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

SIDDHARTH INSTITUTE OF ENGINEERING AND TECHNOLOGY

1 D. Madhu , M.Tech;(Ph.D) Associate professor, Department of ECE, SIETK

2 C.Munishankar

3 M. Priyadarshini

4 B. Rahul chand

5 S. Naga phanisri

6 G. Ranjitkumar

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.

Keywords: 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”. The foundation of IoT mainly con-sists 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.

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 withthe help of Adaptive Firefly algorithm in which the encrypted data is hidden in selected block from image block.

II. RELATED WORK

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

Chitra Biswas et al.[1] Proposed a Least significant bit Steganography strategy. Here cross breed Cryptography gives a superior security, Steganography expands security. An uncommon element of this calculation is the check of Message bits.

Jayati Bhadra et al.[2] This paper proposes and incorporates a calculation that utilizes the elliptic bend encryption plan to encode the information and the least critical calculation for embedding information into the grayscale picture.

Lipi Kothari et al.[3] This paper centers around various steganography strategies to conceal information on web. This technique they propose has more noteworthy security, bigger implanting capability, and preferred cognizance over others.

Roy Fisher et al.[4] DTLS for Lightweight Secure Data Streaming in the Internet of Things. This recommended that Data gram Transport Layer Security is a productive choice to layer security with regards to gushing information over the web from an associated remote sensor organize.

Chervyakov et al.[5] Provided an information stockpiling plan for minimal likelihood of information repetition, information misfortune, and the speed of encoding and interpreting, that can adapt to contrast target inclinations, remaining burdens, and capacity properties. This examination indicated that if the determination of excess buildup number framework boundaries is precise, at that point it not just permits expanded wellbeing and dependability however it additionally makes a difference to speed up handling the scrambled information. The applications utilized on IOT stages for the most part require more information than conventional applications.

Huang et al. [6] introduced a Steganography conspire that utilizes Vector Quantization (VQ) change in which LSB installs mystery information into a spread picture. In the first level, the pixels of a 4 × 4 VQ-changed picture square are isolated into two distinct gatherings: 1) the LSB gathering and 2) the mystery information gathering. In the subsequent level, VQ files are installed in the LSB gathering and mystery information are implanted in the mystery gathering.

Shanableh et al. [7] proposed the adaptable full scale square requesting (FMO) highlight of H.264/AVC to cover up message bits. The macro blocks are doled out to self- assertive cut bunches regarding the substance of the message bits to be covered middleware, which uses software virtualization and assembly level code verification to provide memory isolation.

Liao et al. [8] proposed another clinical JPEG picture steganographic plot that depends on the conditions of inter block coefficients. The essential system that is utilized in this paper comprises of safeguarding the at distinctions among discrete cosine change (DCT) coefficients a similar situation.

Daniels *et al.* [9] introduced security microvisor (SμV) 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.

Bairagi *et al.* [10] 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.

III. PROPOSED APPROACH

1. Elliptic Galois Cryptography*:*

This paper proposes the elliptic Galois cryptography (EGC) protocol for protection against data infiltration during trans-mission 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. Inti, the EGC technique encrypts the confidential data.

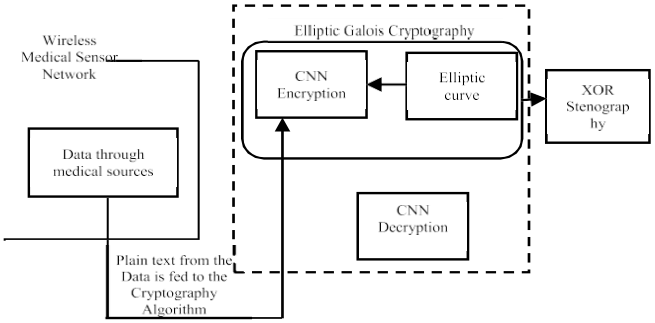

Fig1: EGC

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:

$$y^2 = x^3 + h \bmod P + gx.$$

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.

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:

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

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:

$$W_j = \begin{cases} 1 \text{ if } b(j + 8 \times n) = 0 \\ -1 \text{ if } b(j + 8 \times n) = 1 \end{cases}$$

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.

Step 5: The cipher text is generated, based on the weight factor and the input function $g(i) = x_n(n) \times (1 - y_n) + d^r$.

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.

2.Matrix XOR steganography technique:

Matrix XOR is a technique for hiding encrypted data in which the encrypted data is hidden inside the image. For this technique, the 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 (Permeative Straddling): When there is no need to use the full size to hide the encrypted message, the fragment of. the image remains unused. Permeative 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:

$$M_e = D \oplus C$$

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)

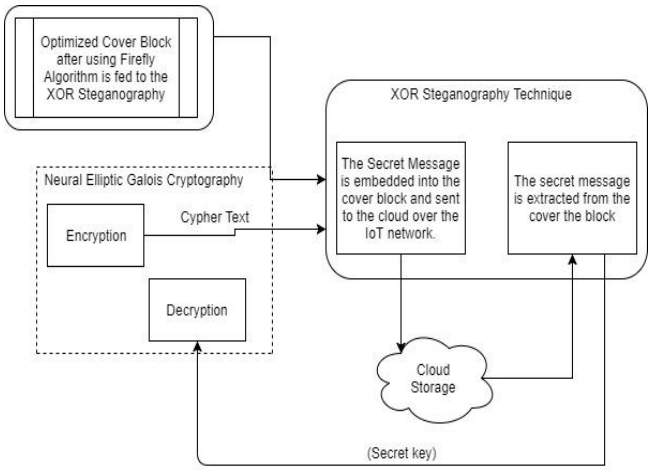

Fig2: Proposed matrix xor steganography techniques

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

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.

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 η = 0 .5
3. coefficient of light absorption $\gamma = 0.5$

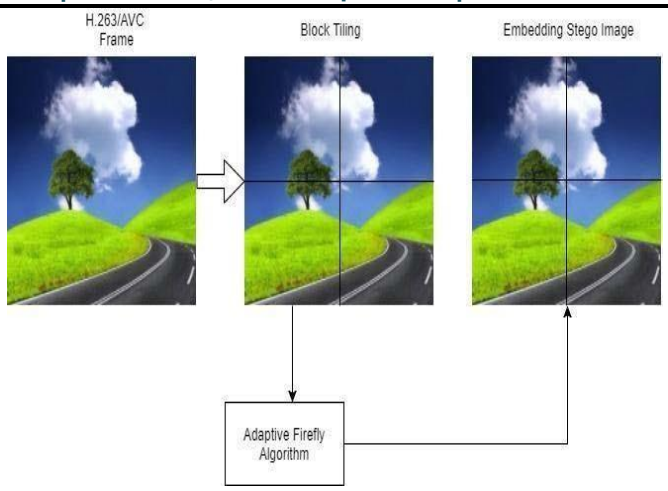

Fig 3: adaptive firefly optimization

4. 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.

1V. RESULTS AND DISCUSSION

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 complex- ity 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 number of secrets bits stored and embedded in an image block, which helps to show the effectiveness of the system.

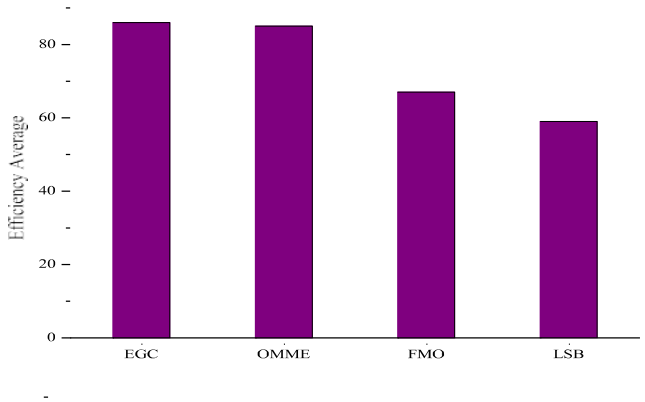

Fig 4: Embedding efficiency analysis

2. *Peak signal to noise ratio:* PSNR calculates the invisibility of the image. It can also be used for dynamic range of images.

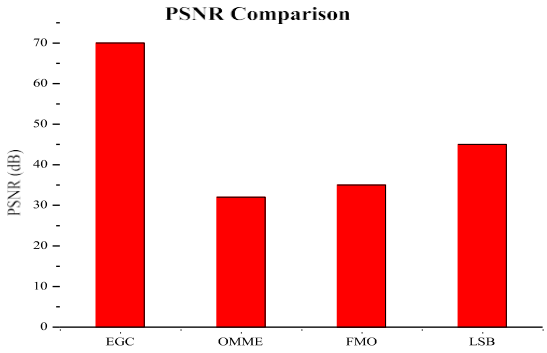

Fig 5: PSNR comparison analysis

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

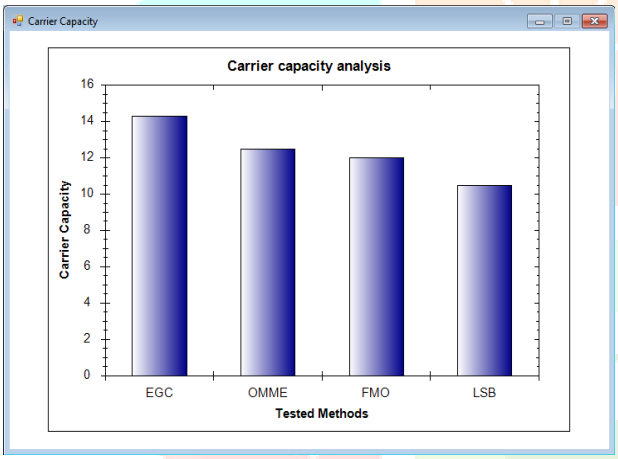

Fig 6: Carrier capacity analysis

4. *Time complexity analysis:* The amount of time taken between the encryption and decryption process. To increase efficiency of the system, time complexity must be lowered.

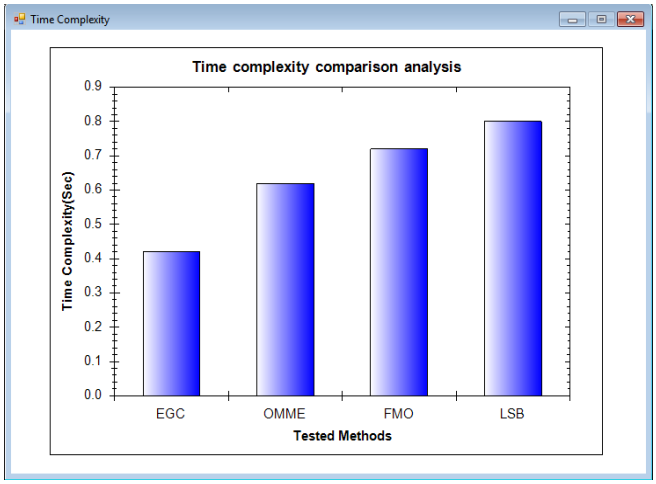

Fig 7: Time complexity analysis

embedding efficiency, carrier capacity, PSNR, and time complexity as compared to other techniques, such as LSB steganography, FMO steganography, and OMME steganography., 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. 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). 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.

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 visual studio, and approximately 86% steganography embedding efficiency was achieved. Results from this proposed protocol were compared to existing methods, such as OMME, FMO, and LSB.

Future Scope

In future work, we are hoping to apply the proposed strategies in sound and video, and anticipate improving the proposed strategy to expand the productivity by keeping same PSNR or higher. And also, we are hoping high payload capacity. The broadened idea of IOT innovation prompts greater security nonrecognition.

REFERENCES

[1]. Haque, An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography. 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), 7-9 February, 2019.

[2]. jayathi Bhadra, M.K.Banga, M.Vinayaka Murthy, Securing data using Elliptic Curve Cryptography and Least Significant Bit Steganography. 2017,IEEE.

[3]. Lipi Kothari ,Rikin Thakkar,Satvik Khara, Data hiding on web using combination of Steganography and Cryptography 2017 International Conference on Computer, Communications and Electronics (Comptelix) Manipal University Jaipur.

[4]. Roy Fisher,Dr GP Hancke, DTLS for Lightweight Secure Data Streaming in the Internet of Things,2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing.

[5]. N. Chervyakov et al., "AR-RRNS: Configurable reliable distributed datastorage systems for Internet of Things toensure security," Future Gener.Comput. Syst., vol. 92, pp. 1080–1092, Mar. 2019.

[6]. 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 encodingwith adaptive pixel replacements," J. Supercomput., vol. 74, no. 9,pp. 4295–4314, 2018.

[7]. T. Shanableh, "Data hiding in MPEG video files using multivariateregression and flexible macroblock ordering," IEEE Trans. Inf. ForensicsSecurity, vol. 7, no. 2, pp. 455–464, Apr. 2012.

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

[9]. 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.

[10]. 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.