Steganography Techniques for Data Protection in IOT

S.Jagadeesan[*1], P.Jaisankar[2], C.Navamani[3], E.Padma[4]

[*1]Assistant Professor, Department of CSE, Nandha Engineering College(Autonomous), Erode, Tamilnadu, India

[2] Assistant Professor, Department of Mathematics, Nandha Engineering, College (Autonomous), Erode, Tamilnadu, India

[3]Assistant Professor, Department of CSE, Nandha Engineering College(Autonomous), Erode, Tamilnadu, India

[4]Assistant Professor, Department of CSE, Nandha Engineering College(Autonomous), Erode, Tamilnadu, India

Abstract:

Internet of Things (IoT) is a domain wherein which the relocate of data is taking place every single second. The protection of these data is an exigent task; however, security challenges can be mitigated with cryptography and steganography techniques. These techniques are decisive when commerce with user verification and data isolation. Here the planned exertion, the elliptic Galois cryptography protocol plays an important role. In this protocol, a cryptography procedure is worn to encrypt confidential data that came from dissimilar medical sources. Next, a Matrix XOR encoding steganography system is use to embed the encrypted data into a low density representation. The proposed work also uses an optimization algorithm called Adaptive Firefly to optimize the assortment of envelop blocks within the image. Based on the results, various parameters are evaluated and compared with the obtainable techniques. Finally, the data that is secreted in the figure is recovered and is then decrypted.

Keywords: Internet of Things, Steganography, Cryptography, Authentication, Encryption, Encryption & Authentication.

DOI: 10.24297/j.cims.2023.1.1

1. Introduction

The Internet of Things (IoT) is a system of linked vehicle, substantial devices, software, and electronic substance that smooth the progress of data swap over. The reason of IoT is to make available the IT-infrastructure for the protected and dependable replace of "Things". The establishment of IoT largely consists of the incorporation of sensors/actuators, radio frequency identification (RFID) tags, and communication technology. The IoT details how a multiplicity of physical matter and plans can be included with the Internet to authorize individuals things to

collaborate and be in touch with every supplementary to attain frequent task. The IoT focus frequently of slight resources that is coupled collectively to make likely shared manipulative situation. Constraints of the IoT consist of energy budget, connectivity, and computational power. Even though IoT strategy have finished being smoother, slight concentration has been specified to the safety measures of these procedure. At present, the hub of designers is to augment the capability of these devices, with little prominence on the safety measures of the devices. The information that is transfer over the IoT set of connections is susceptible to assault. This information is desirable to be tenable to defend the isolation of the client. If there is no data protection, then there is a likelihood of data violate and thus, individual information can be with no trouble hacked from the structure. Some of the significant concepts of IoT engage classification and validation. These concepts are interconnected to every one other as cryptographic functions that are essential to make sure that the information is communicated to the accurate tool and if the basis is trust or not[1]. With the lack of verification, a hacker can simply converse to any mechanism. When two procedures converse with each other, there is a reassign of data stuck between them. The data can also be very responsive and private. Therefore, when this responsive data is transfer from machine to device over the IoT network, then there is a need for encryption of the data. Encryption also helps to defend information from intruder. The data can be without difficulty encrypted with the assist of cryptography, which is the procedure of converting easy text into incomprehensible text[2]. The major objectives of cryptography are confidentiality, reliability, no negation, and authentication. Elliptic curve cryptography (ECC) is one of the cryptographic algorithms that are used in the projected exertion. ECC is a public key cryptographic procedure base on the algebraic arrangement of elliptic curves over restricted field.

In adding together, to the cryptographic technique, an additional scheme, named steganography is used in the projected effort which helps to make obtainable supplementary protection to the data. Steganography hide encrypted messages in such a way that no one would even suppose that an encrypted Message even exists in the primary place. In contemporary digital steganography, encryption of data occurs with typical cryptographic technique. Next, a special algorithm helps to pop in the data into superfluous data that is fraction of a folder arrangement, such as a JPEG picture. The planned work uses Matrix XOR steganography to make available further security. The image chunk is optimized with the help of Adaptive Firefly algorithm in which the encrypted data is hidden in a preferred chunk from an enormous image block[3].

2. Literature Review

Cryptography and steganography are easily recognized and extensively used techniques that are essentially used for exploitation of information in arrange to cipher or secrete their continuation respectively. Steganography is a technique which allows group to converse and conceal the subsistence of statement. Cryptography scramble a communication so it cannot be unstated, in other words, cryptography is a technique of transform data so that only those for

whom it is anticipated can read and procedure it. Even though both methods make available safety, a cram is made to merge both cryptography and steganography methods into one system for improved privacy and protection.

Wide-ranging measurement of Steganography

• Hidden Data : The data that is to be entrenched or the data that must stay concealed from everybody other than future beneficiary.

• Cover Media : The media in which the information is to be entrenched. Cover/carrier media can be an figure file, or an audio file or it can be a video file.

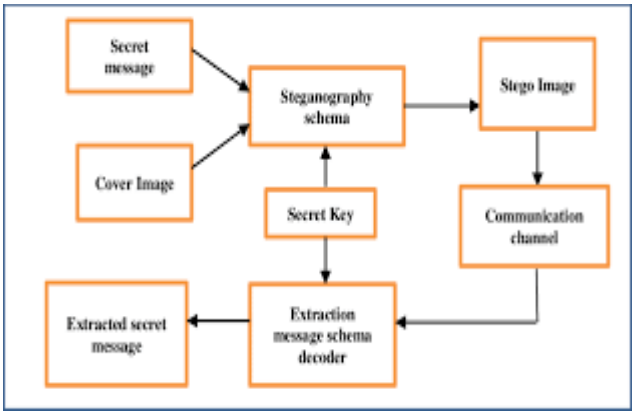

Fig.1. Basic stenography

2.1. Stego media: cover media contain the concealed information

Steganography is the discipline of indistinguishable message. This relocate of information takes place by hiding data within medium. As revealed in the figure, a variety of steganographic technique can be categorize into four main mechanism, they are as follow:

a. ***Image Steganography***. We utilize an picture folder as a cover medium to hide the secret communication. A digital representation is a mixture of low and high incidence stuffing. A low frequency region is robustly connected with its adjacent pixels while a high frequency region strongly deviates from its bordering pixels. By striking the benefit of individual apparition compassion the surreptitious message is entrenched within the image pixels depending on dissimilar renovate technique to hide the data in a representation. In recent times, a small amount of machine learning technique are also being used to enlarge the stoutness, embed capability etc .

b. ***Audio Steganography***. It is a system worn to broadcast a concealed message within an audio file. Embed message in an audio file is much extra tricky than hiding message in an image file as the human auditory system (HAS) is more responsive than human visual system (HVS). As the message is entrenched in audio signal, there are a variety of method used for embed procedure in an audio file like LSB coding, parity coding and echo data thrashing.

c. ***Text Steganography***. It deal altering with arrangement of an obtainable text within a file, altering the words within the text or generate arbitrary character sequence. Essentially here we

use the text folder as a cover media to entrench the secret information. It is extra susceptible for assault as it can be easy for an attacker to distinguish the pattern.

D. Video steganography : A video file is worn as a cover medium to secrete the secret message. it is a smaller amount prone for steganalysis as a video file is a amalgamation of text, image and audio. it is a compilation of convinced frame running at some invariable speed and is deliberate in frame per second. in arrange to embed a secret message in a video file first; we have to remove the frames from it. in organize to embed the message in video file first, frame exchange is completed. it is a procedure of convert a video to consequential images or frames and then each or one frame is used as transporter data to obscure the concealed information. following the embedding procedure, all frames are compound mutually to manufacture the stego video[4].

3. EXISTING SYSTEM

At the present time, quite a lot of method is used for communicate secret messages for protection purpose or in arrange to make sure the isolation of announcement among two party. So we go for hiding information in ways that avoid its discovery. A number of of the method used for privacy statement are the use of imperceptible links, underground channels are some of obtainable systems that are used to communicate the communication.

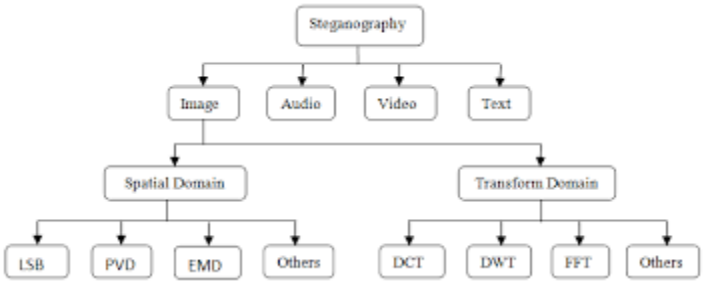

Fig.2.Classification of stegnography

At present, the prominence has been on a variety of form of digital steganography. Frequently there are a number of digital technologies that the community is concerned with, namely text files, still images, movie images and audio. The majority of other organizations using steganographic techniques involve individuals or corporations interested in protecting intellectual property[5].

4. Proposed System

The proposed system proposes the elliptic Galois cryptography (EGC) process for fortification alongside data penetration all through broadcast over the IoT network. In the considered exertion, dissimilar campaigns in the IoT system broadcast data from side to side the proposed protocol as a part of the controller[6]. 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 procedure. The image can then be easily

transferred throughout the Internet such that an intruder cannot extract the message concealed contained by the image. Initially, the EGC system encrypts private data. afterward, the encoded secret message is inserted within the image by the XOR steganography practice[7][8]. Subsequently, an optimization algorithm called the Adaptive.

Elliptic Galois Cryptography: ECC, usually known as the public key encryption technique, is base on elliptic curve hypothesis. The keys are generating by the means of the properties of elliptic curve equations as an alternative of conventional methods. The future work use EGC. For civilizing the competence of calculation and to diminish the complexity of rounding errors, the elliptic curve over the Galois field (Fa) is worn. Value of the Galois field must be greater than one. The attractiveness and b) the variation of light intensity[9][10].

5. Implementation

5.1. Sender

In this component, dispatcher has to login with suitable username and password. Following login successful user can do some operation such as Browse and encrypt image, Enter message to hide by secret encrypted key, Hide message into encrypted image using Cryptography and Steganography Techniques.

5.2. Receiver

In this component, there are n numbers of users are at hand and will do some operation like Browse and select encrypted image, Decrypt image and extract Hidden data by Cryptography and Steganography Techniques by inward bound data hidden key, save message or file .

5.3. IOT Router

The IOT Router acts as a middleware connecting sender and receiver to receive and re route the encrypted image to an suitable Receiver[11][12].

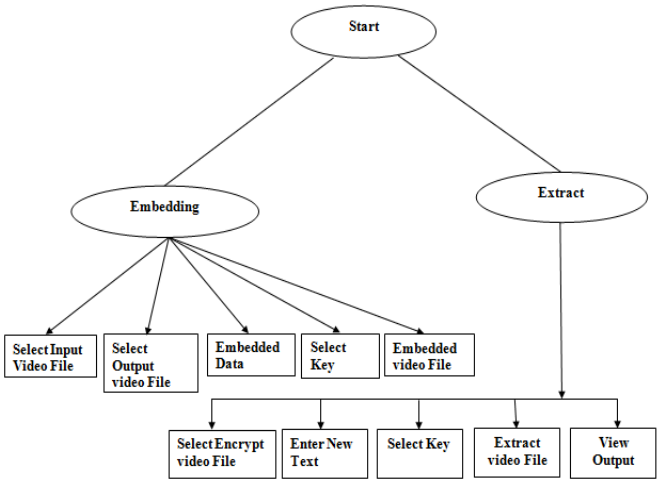

Fig.3. System Design

6. CONCLUSION

The EGC protocol generate elevated level of data safety to provide the function of defensive data throughout transmission in the IoT. With the novel ECC over Galois field, the projected EGC procedure provides healthier security. Due to the improved embed effectiveness; advanced data thrashing aptitude can be achieved. With the assist of the future procedure and Adaptive Firefly optimization, any quantity of data can be effortlessly transmit over the IoT system firmly hidden within the profound layers of descriptions. Presentation is evaluated with parameter, such as embedding competence, PSNR, carrier capacity, time complexity, and MSE. In conclusion, the projected work is implementing in a MATLAB simulator, and approximately 86% steganography embedding competence was achieved. Consequences from this planned protocol were compare to presented methods, such as OMME, FMO, and LSB.

References

1. S.Jagadeesan, C.Mani, R.Navin Kumar, S.Prabhakaran, " High Level Secure Message Based on Stegnography And Cryptography", International Journal of Engineering Trends and Technology (IJETT) – Volume 68 , pp.142-145,Issue 2- Feb 2020.
2. S.Jagadeesan, P.Jaisankar, " Fused Distortion Measurement For Securing RGB Steganography, "International Journal of Engineering Trends and Technology (IJETT) – Volume 68, pp.64-68, Issue 3 - March 2020".
3. S.Jagadeesan, R.Navin Kumar, K.E.Eswari, N.Zahira Jahan, "Multi phase Shelter using Pixel Assortment Practice for Enhancing Steganography", International Journal of Mechanical Engineering – Volume 3, No.03, pp.1164-1168, December-2021.
4. S.Jagadeesan, C.Mani, S.Sambasivam, P.Jaisankar, S.Sasikala, " The Role of AES and RC5 Algorithm: A Cryptosystem Model to Secure Information in the Image based Steganography along with Watermarking", Webology – Volume 18, Special Issue on Current Trends in Management and Information Technology, October, 2021. [5] 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.

5. 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.
6. 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.
7. 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.
8. 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.
9. G. Swain, and S.K. Lenka, "A novel steganography technique by mapping words with LSB array", Int. J. SignalImag. Syst. Eng, 8: pp. 115-122,2015.
10. C. N. Yang, C. Kim, and Y.-H. Lo, ''Adaptive real-time reversible data hiding for JPEG images,'' J. Real-Time ImageProcess., vol. 14, no. 1, pp. 147–157, Jan.2018.
11. Y. Shen and L. H. Huang, ''A data hiding scheme using pixel value differencing and improving exploiting modification directions,'' Comput. Secur., vol. 48, pp. 131– 141, Feb.2015.