IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURITY DATA IN INTERNET OF THINGS USING CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES

KOTA JAYA SRI [#1], B.SURYANARAYANA MURTHY [#2]
[#1] MCA Student, Master of Computer Applications,
D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.
[#2] Associate Professor, Master of Computer Applications,
D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

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 overcome 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. Here we try to encrypt the Image and send through network from sender to receiver.

Key Words:

Internet of Things, cryptography, steganography, Image, Encryption, Decryption

I. INTRODUCTION

The idea of making sure about messages through Steganography and Cryptography has long history. Cryptography is engrossed with the insurance of the substance of a message or data. Steganography originates from Greek and signifies "secured composing". Steganography is a strategy used to conceal data inside pictures. Utilizing transcription, watermarks and copyrights can be put on a picture to ensure the privileges of its proprietor without changing the presence of the picture. Practically like enchantment, pictures, executable projects, and instant messages can cover up in pictures. The spread picture doesn't seem, by all accounts, to be adjusted. Individuals take a gander at the spread picture and never presume something is covered up. Your data is covered up on display.

The way to conceal information is to gadget a covering up (encryption) system that is extremely hard to switch (i.e., to locate the first information) without utilizing the decoding key. Symmetric-key calculations are a class of calculations for cryptography that utilization the equivalent cryptographic keys for both encryption of plaintext and unscrambling of ciphertext. In uneven key one key is utilized for encryption and another key is utilized for decoding. All the more explicitly this Paper manages the Symmetric key cryptography. For the Steganography we are utilizing the idea of bit move calculation.

II. LITERATURE SURVEY

In this section we will mainly discuss about the background work that is carried out in order to prove the performance of our proposed Method. Now let us discuss about them in detail

MOTIVATION

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.

III. EXISTING METHODOLOGY

In the existing system we used to preserve text data by using primitive cryptography techniques and try to send the data over network in encrypted manner. But there is no technique which can give advance level of security for that primitive data sharing within the network. There is no concept ;like steganography which is used along with cryptography for privacy preserving of sensitive data in IOT or cloud.

LIMITATIONS OF THE EXISTING METHODOLOGY

1) Existing system failed in hiding one form of data in side another form of data and then tries to send that sensitive content to the receiver.

2) All the Existing system failed in achieving the principle of steganography.

3) In the existing system the text data is encrypted by using normal cryptography techniques and there is no utmost level of security from the attacker.

4) In the existing system there is more chance of data loss due to lack of proper security.

IV. PROPOSED METHODOLOGY

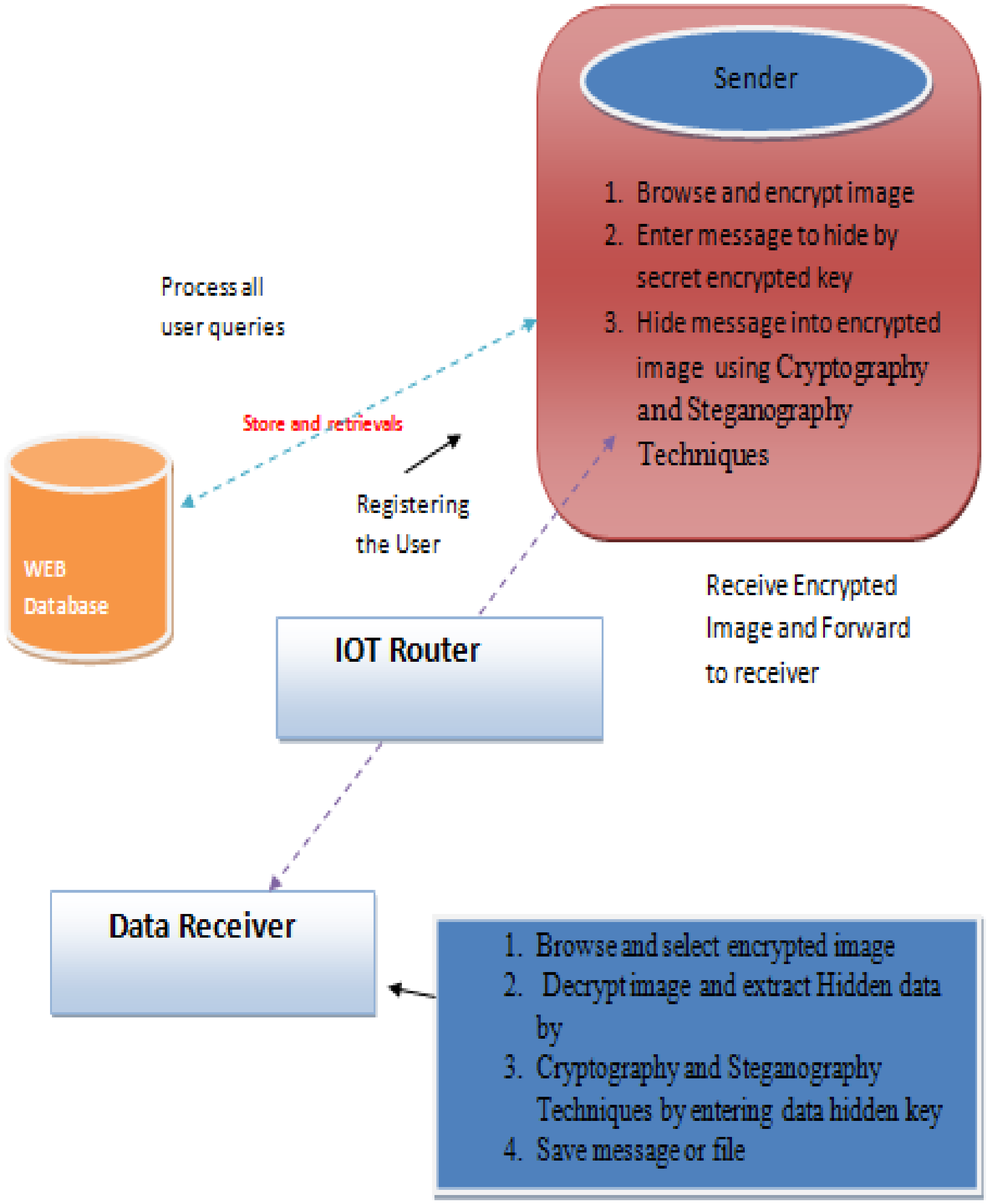
In the proposed work, the elliptic Galois cryptography protocol is introduced and discussed. In this protocol, a cryptography technique is used to encrypt confidential data that came from different medical sources. Here we try to encrypt the Image and send through network from sender to receiver.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system. They are as follows:

1. In this proposed system we can able to give high level of security for the data which is transmitted from one location to other location under a secure channel.
2. Here if any attacker who try to see the internal content during transmission he/she can only see the outer cover image but they cant able to see the hidden encrypted content.
3. The proposed system is less time complexity
4. The proposed system can easily transmit the sensitive information from sender to receiver under secure manner.

V. PROPOSED APPROACH


Sender
1. Browse and encrypt image
2. Enter message to hide by secret encrypted key
3. Hide message into encrypted image using Cryptography and Steganography Techniques
Process all user queries
Store and retrievals
Registering the User
WEB Database
IOT Router
Receive Encrypted Image and Forward to receiver
Data Receiver
1. Browse and select encrypted image
2. Decrypt image and extract Hidden data by
3. Cryptography and Steganography Techniques by entering data hidden key
4. Save message or file

VI. EXPERIMENTAL REPORTS

1) Main Window

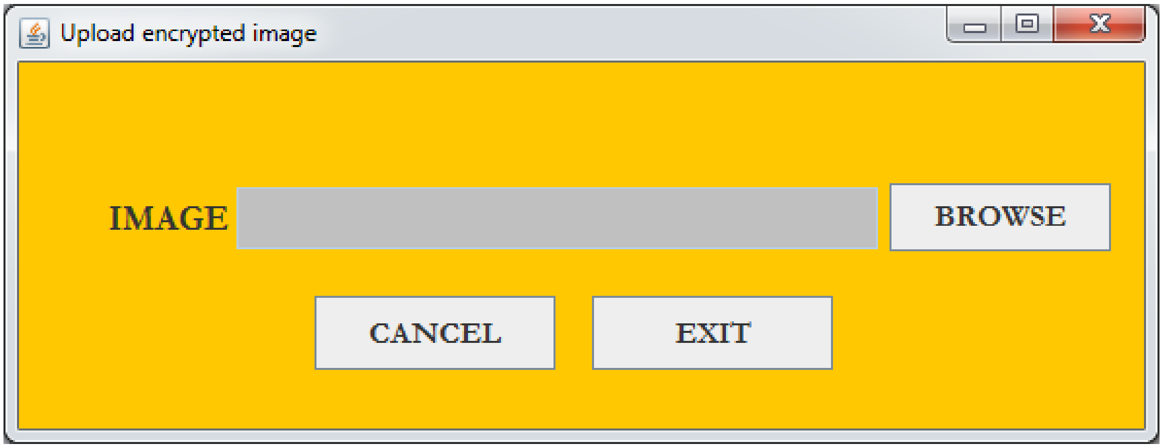
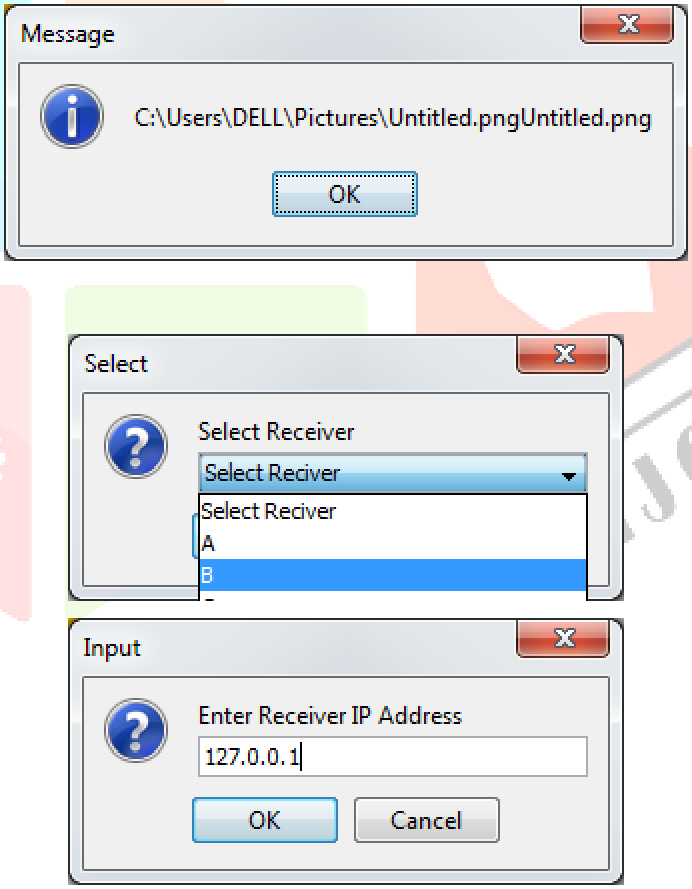


Figure Represents the Main Window for the Proposed Application

2) User Select a Image as Input



C:\Users\DELL\Pictures\Untitled.pngUntitled.png

Select Receiver

Select Reciver

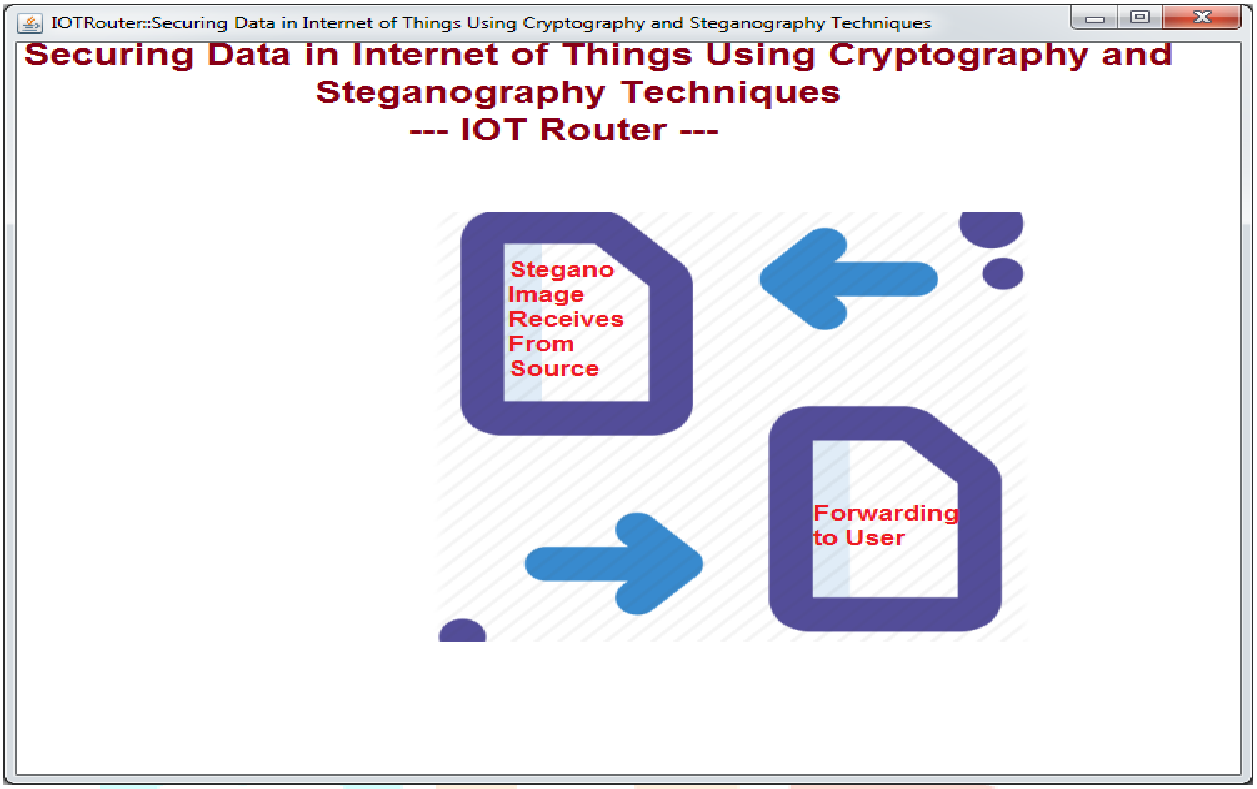
Select Reciver
A
B

Enter Receiver IP Address

127.0.0.1

Figure Embedding a Image with Sub Parameters

3) **Router Window**

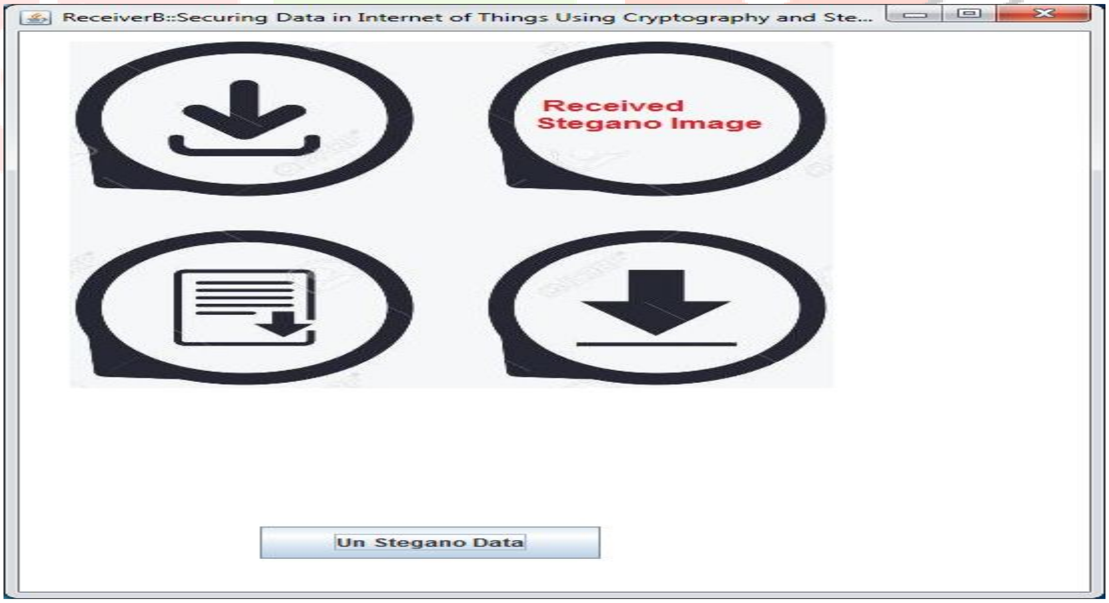


IOTRouter::Securing Data in Internet of Things Using Cryptography and Steganography Techniques

Securing Data in Internet of Things Using Cryptography and Steganography Techniques
--- IOT Router ---

Figure Router Window

4) **Receiver Will Receive the Data**



ReceiverB::Securing Data in Internet of Things Using Cryptography and Ste...

Figure Represents the Receiver Window

5) **Receiver Choose Un stegno Data**

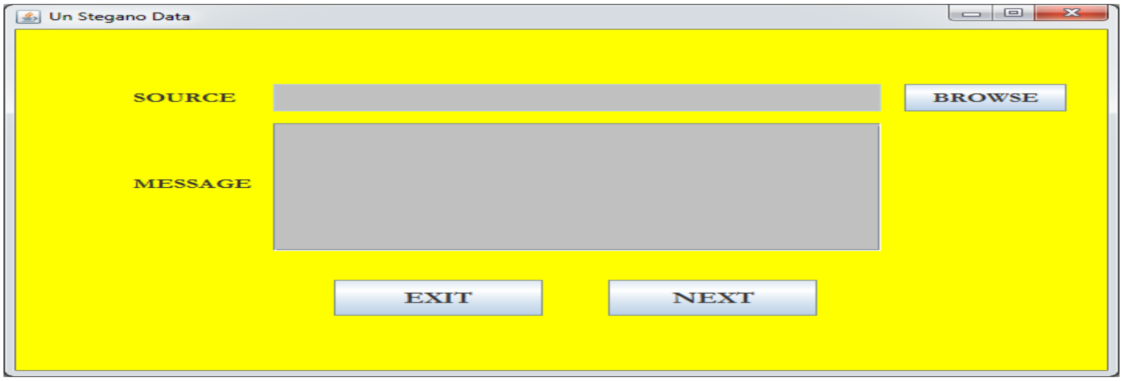
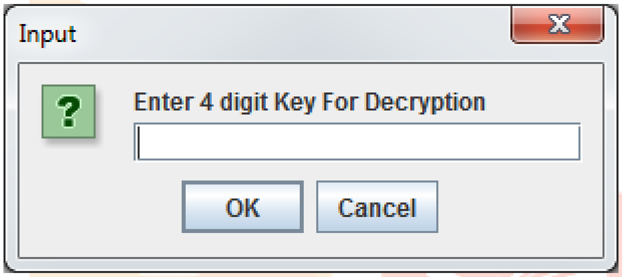


Figure . Receiver try to Decode the File

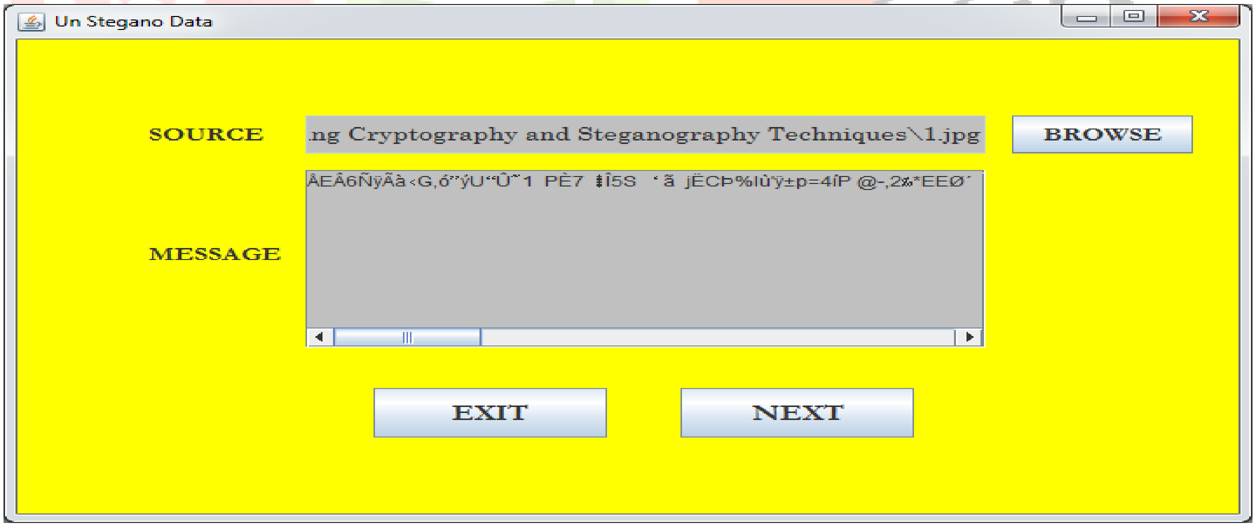
6) **User is asked Decryption Key**



Enter 4 digit Key For Decryption

Figure Represents the Decryption Key

7) **Retrieve Message File Information at the receiver side**



SOURCE: ng Cryptography and Steganography Techniques\1.jpg

MESSAGE: ÅEÂ6ÑÿÃà‹G,ő"ÿU"Û˜1 PÈ7 ‡Î5S ʻã jËCÞ%lůÿ±p=4íP @-,2‰*EEØ˝

Figure Represents the File Information

8) Decrypt the Original Image at receiver side

Figure . Represents the Decrypt Image at Receiver Node

VII. 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.

VIII. 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. Vuˇcini´c *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.