INTERNATIONAL JOURNAL ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

COPY RIGHT

ELSEVIER

SSRN

IJIEMR Transactions, online available on 30th Aug 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue 08

DOI: 10.48047/IJIEMR/V11/ISSUE 08/21

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

Volume 11, ISSUE 08, Pages: 169-175

Paper Authors

Dr. Mohammed Maqsood

International Journal for Innovative Engineering and Management Research

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

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

Dr. Mohammed Maqsood, Associate Professor, IT Department, University of Technology and Applied Sciences, Salalah, Sultanate of Oman. Email ID: maqsoodmsc@gmail.com

ABSTRACT

Data is transferred every second in the Internet of Things (IoT) sector of the economy. Steganography and cryptographic methods may be helpful in protecting sensitive data, notwithstanding their difficulty. These techniques are essential for protecting user identity and privacy. The elliptic Galois cryptography protocol is introduced and covered in the suggested reading. The encrypted data used in this protocol came from a variety of medical sources. The matrix XOR coding steganography method is then used to combine the encrypted data into a simple image. The suggested research improves the cover block selection via the application of the Adaptive Firefly optimization technique. Numerous parameters are assessed and contrasted with contemporary methods based on the findings. Then, the encrypted secret data in the picture is found and decoded.

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

1. INTRODUCTION

The Internet of Things (IoT) is a network of electronically and physically linked objects, including electrical and mechanical equipment, software, and vehicles. IoT's goal is to provide the IT infrastructure necessary for the interchange of "Things" in a safe and trustworthy manner [1]. Radio frequency identification (RFID) tags, communication technology, and sensors/actuators are the essential components that make up the IoT's basis. The Internet of Things (IoT) describes how various physical objects and devices may be connected to the Internet to enable cooperation and communication among them in order to accomplish shared objectives. The IoT mostly comprises of small components that are connected to one another to enable collaborative calculation scenarios.

Energy budget, connection, and processing capacity are some of the IoT's limitations [2]. Despite the fact that IoT gadgets have made life simpler, their security has received little consideration. At the moment, developers are primarily concerned with enhancing these devices' capabilities and place minimal attention on ensuring their security. The information sent via an IoT network is open to intrusion. To safeguard the user's privacy, this data must be safeguarded. Without data protection, there is a chance of a data breach, making it simple to hack into the system and steal personal data. IoT principles such as identity and authentication are crucial. These ideas are connected to one another as cryptographic operations that are required to make sure that information is sent to the proper device and to determine whether or not the source can be trusted. A hacker may simply connect with any device without authentication.

A data transfer occurs whenever two devices interact with one another. The information may also be very private and sensitive. Encryption of the data is thus required when this sensitive data is sent between devices through an IoT network. Data protection against hackers is made easier by encryption. With the use of cryptography, which is the act of turning plaintext into unreadable text, the data may be simply encrypted. Confidentiality, integrity, nonrepudiation, and authentication are the main goals of cryptography. One of the cryptographic techniques employed in the suggested study is elliptic curve cryptography

(ECC). The algebraic structure of elliptic curves over finite fields serves as the foundation for the public key cryptography method known as ECC. Steganography is a technique that is employed in the proposed work in addition to cryptographic approaches to assist further secure the data. Steganography conceals encrypted communications in a manner that makes it impossible for anybody to know that they exist at all. Data is encrypted in current digital steganography using standard cryptographic methods. The information is then inserted into redundant data that is a component of a file format, such a JPEG picture, with the use of a particular algorithm. The suggested approach adds more security by using Matrix XOR steganography. The Adaptive Firefly technique is used to optimise the picture block, hiding the encrypted data in a chosen chunk from a large image block.

2. LITERATURE REVIEW

W. Zhang et.al [1] Many picture encryption methods based on the pixel or bit plane have recently been created. Both pixel-level and bit-level interpolation have downsides, however. In this research, a brand-new cryptosystem is recommended as a remedy for these problems. The first step is a review and comparison of various permutation techniques. Since an image may be seen from the bitplane as a natural three-dimensional (3D) bitmatrix (width, height, and bitlength), a unique 3D bitmatrix permutation using a Chen system is presented to give a random visiting mechanism. A novel mapping technique is devised to shift a random site to another random position in the 3D matrix (i.e. double random position permutation) without necessitating conventional sequential visits by combining parts of the Chen system with a 3D cat map in the permutation phase. We run clear simulations, and the outcomes show how our new cryptosystem is both efficient and secure.

SghaierGuizni et.al [2] In recent years, the academic community has paid increasing attention to the information contained in multimedia data. These confidential information may be utilised for anything from attribution to copyright protection to private discussions. This article discusses using adaptive steganography in optical cryptography to encrypt and decrypt audio and video sequences (AS). The needed audio/video sequences in optical cryptography are encoded and decoded using a double random phase encoding method. The basic goal of steganography algorithms is to conceal as much information as possible in the cover material. The trade-off for steganography algorithms is how much stego data—hidden information—to implant and ensure that its nonexistence is camouflaged. Despite their aims seem to be distinct, recent advancements enable the collection of incredibly secret information using sophisticated watermarks.

Xu et.al [3] To ensure security and privacy, it has been suggested that digital photos sometimes be stored and processed in an encrypted format using B. cloud storage and cloud computing. Cloud servers must include some additional information directly into these encrypted images in order to annotate the content and/or manipulate the users' identities. A beneficial new idea in cloud computing is reverse data hiding in an encrypted domain since it might maintain anonymity. This study provides a novel, fault-free technique for concealing encrypted image data. The sampled pixels are stream encrypted after reviewing the features of the interpolation methods, and a specific encryption technique is used to encrypt the interpolation errors of the unsampled pixels. The data hider may then use a modified version of the histogram shift and variance expansion approach to inversely embed the hidden data in the interpolation errors without being aware of the original image content. Data extraction may be carried out either in the encrypted domain or the decrypted domain, depending on the needs of the application. Additionally, true reversibility is realised, enabling error-free data extraction and image recovery. Experimental results confirm the effectiveness and feasibility of the proposed strategy.

K. Kainth et.al [4] Encryption transforms data into ciphertext, restricting access to those with the proper authorization. When encrypting 2-D picture data, image encryption is mainly a substantial part of encryption; as a result, the whole encryption process is carried out on it. This paper presents a very simple implementation of the high-security SCAN pattern-based picture encryption technique. A special code known as a four-of-eight code is used in the SCAN process to create the carrier image, which is then mixed with the original picture to create a scrambled image. The technique for picture encryption proposed in this study separates the image into entirely distinct pieces, which are then combined to form a pattern that can only be deciphered and decrypted by authorised parties. The method described in this article offers a high level of security. In MATLAB, all encryption and decryption techniques are used, along with additional picture feature analyses.

M Pooyan et.al [5] developed a novel approach for encrypting sensitive data in audio signals and embedding in the wavelet coefficients of the host audio signal. Using a training wavelet transform prevents extraction mistakes. We determine the hearing threshold in the wavelet range to make the most of the audio signals' potential. The data bits are then included in the least significant bits of the lifting wavelet coefficients based on this threshold. The adjusted coefficients are passed via an inverse lifting wavelet transform to produce a time-domain stego signal. According to experimental findings, the suggested approach provides a big payload, good audio quality, and 100% recovery.

3. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM:

In order to provide memory isolation and adaptive security, Daniels et al. [3] proposed a Security Microvisor (SV) middleware that makes use of software virtualization and assembly-level code verification. according to Banerjee et al. The security level is the same, but it consumes less energy. [4]. Manogaran et al. developed a method that places medical sensor devices inside of people in order to collect clinical data from patients. Suggested. [5]. If the sensors detect significant differences in blood pressure, heart rate, blood sugar, and body temperature outside of the expected ranges, they generate an alert with essential health information and wirelessly broadcast it to the doctor's network. To protect most industrial data, the system uses essential management security measures.

A cloud-based anti-malware tool called CloudEyes was developed by Sun and colleagues. [6]. The recommended approach provided reliable and efficient security services for IoT network devices. On the idea of trusted computing, Ucilet et alresearch[2] .'s on embedded security requirements, vulnerability approaches for embedded systems, and rules and countermeasures to avoid cyberattacks is founded.

Medical data may be protected in two different ways using the broken-glass access control (LiBAC) technology developed by Yang et al. as stated by [10]. Break-glass access and attribute-based access are these two strategies. A healthcare professional may often decrypt and examine the data if the attribute set conforms with the medical records access policy. Emergency medical technicians (EMTs) may bypass the process of gaining access to medical records in an emergency by rapidly accessing data through a broken glass access mechanism.

PROPOSED SYSTEM:

- Elliptic Galois Cryptographic Protocol (EGC) is the solution put out by the suggested system to guard against data intrusion while being sent across the IoT network. As part of the controller in the proposed work, different IoT network devices transfer data using the suggested protocol. A controller-based encryption method uses the EGC protocol to encrypt data, and a steganographic approach is used to hide an encrypted and secure message behind picture layers.

- Since it is easy to send the image over the Internet, an invasive party cannot read the message hidden in the picture. Private data is initially encrypted using EGC technology. The encrypted secret message is inserted into the image using XOR steganography. The following is the adaptive optimization process.
- *Galois Elliptic Cryptography:* ECC, sometimes referred to as public key cryptography, is a cryptographic method that is based on the elliptic curves theory. Instead than utilising conventional techniques, elliptic curve equations' characteristics are used to produce keys. The planned project employs EGC. An elliptic curve is used to the Galois field to increase computation performance and decrease the complexity of rounding mistakes (Fa). The Galois field's value must be larger than 1.

❖ All the fireflies are unisex so that all fireflies are attracted to each other.

❖ 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.

4. SYSTEM DESIGN

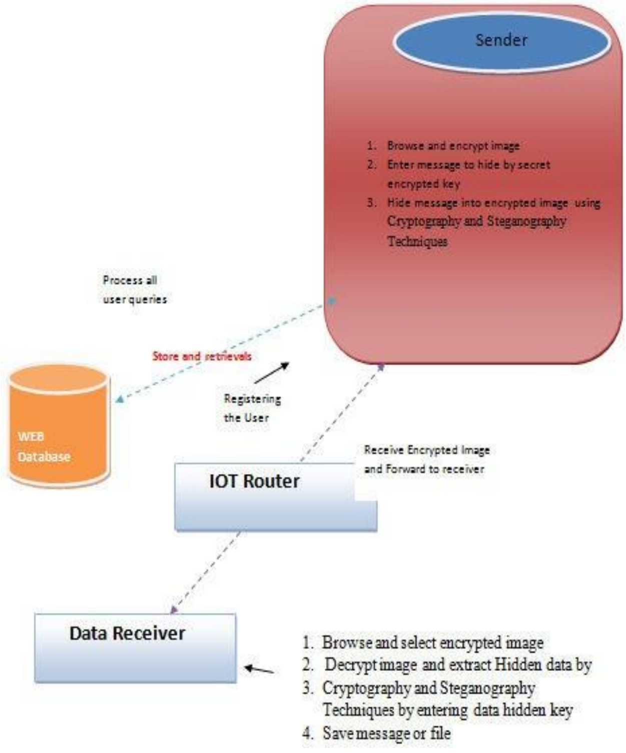

Sender
1. Browse and encrypt image
2. Enter message to hide by secret encrypted key
3. Hide message into encrypted image using Cryptography and Steganography Techniques
Process all user queries
Store and retrievals
Registering the User
WEB Database
Receive Encrypted Image and Forward to receiver
IOT Router
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

Fig 1.Architecture

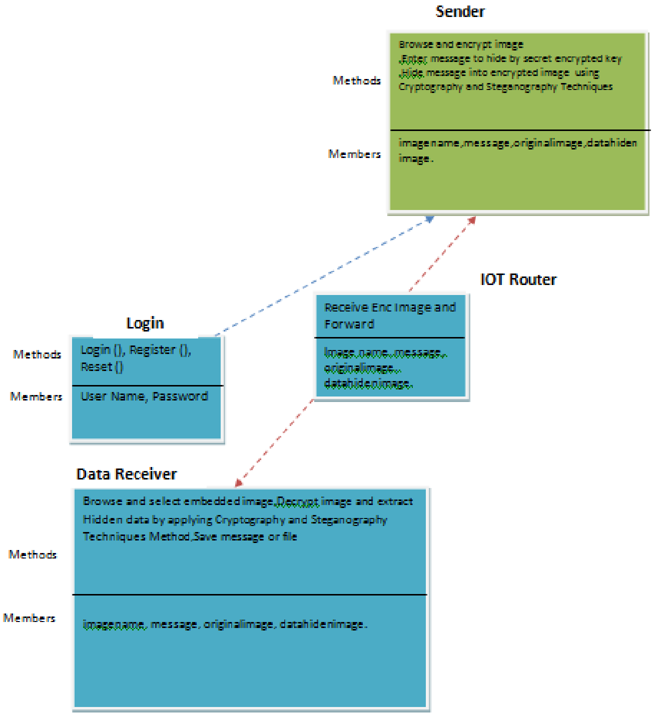

Sender
Methods
Browse and encrypt image
,Enter message to hide by secret encrypted key
,Hide message into encrypted image using Cryptography and Steganography Techniques
Members
imagename,message,originalimage,datahiden image.
IOT Router
Receive Enc Image and Forward
Image name, message, originalimage, datahidenimage.
Login
Methods
Login (), Register (), Reset ()
Members
User Name, Password
Data Receiver
Methods
Browse and select embedded image,Decrypt image and extract Hidden data by applying Cryptography and Steganography Techniques Method,Save message or file
Members
imagename, message, originalimage, datahidenimage.

Fig 2.Class Diagram

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

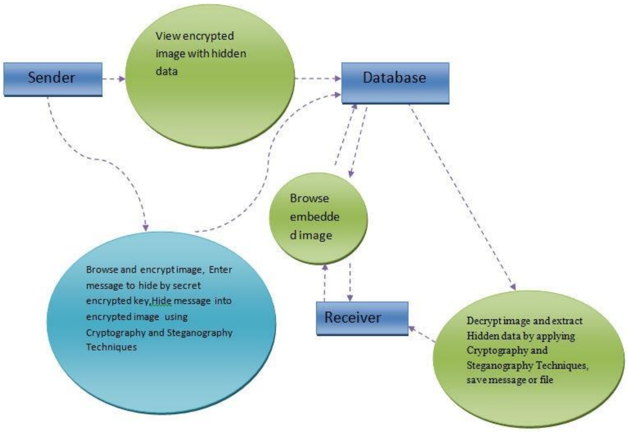

Sender
View encrypted image with hidden data
Database
Browse embedded image
Browse and encrypt image, Enter message to hide by secret encrypted key,Hide message into encrypted image using Cryptography and Steganography Techniques
Receiver
Decrypt image and extract Hidden data by applying Cryptography and Steganography Techniques, save message or file

Fig3.Flow chart

SEQUENCE DIAGRAM

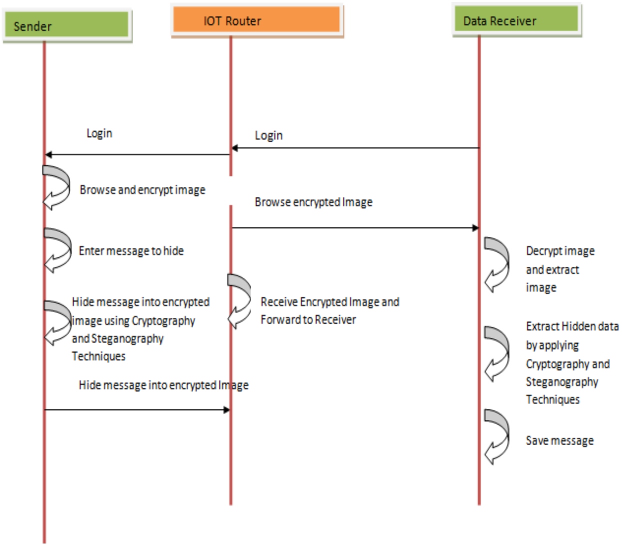

Sender
IOT Router
Data Receiver
Login
Login
Browse and encrypt image
Browse encrypted Image
Enter message to hide
Decrypt image and extract image
Hide message into encrypted image using Cryptography and Steganography Techniques
Receive Encrypted Image and Forward to Receiver
Extract Hidden data by applying Cryptography and Steganography Techniques
Hide message into encrypted Image
Save message

Fig 4. Sequence Diagram

5. IMPLEMENTATION

Sender

Sender must provide a valid account and password to log in to this module. After successfully logging in, he may do certain actions like browse and encrypt images. Using secret encryption key, enter the message to be concealed. Using cryptography and steganography, conceal a message in an encrypted picture.

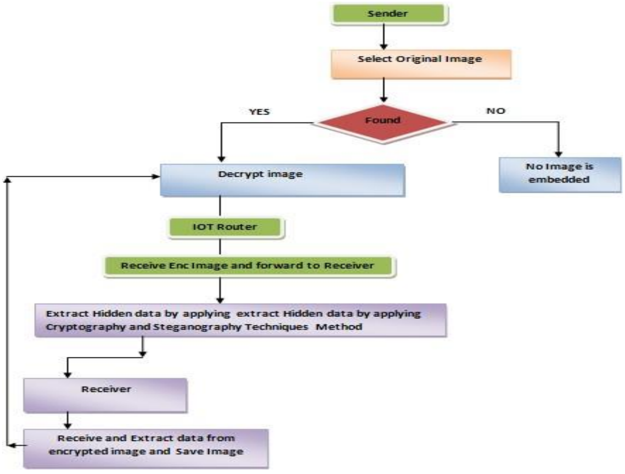

Sender
Select Original Image
YES
Found
NO
Decrypt image
No Image is embedded
IOT Router
Receive Enc Image and forward to Receiver
Extract Hidden data by applying extract Hidden data by applying Cryptography and Steganography Techniques Method
Receiver
Receive and Extract data from encrypted image and Save Image

Fig 5.Flow Chart: User

Receiver

There are n users in this module, and they will do activities like browse and choose encrypted images, decrypt images, and extract hidden data. Techniques for encrypting and hiding data by inputting a secret key, saving a message, or creating a file

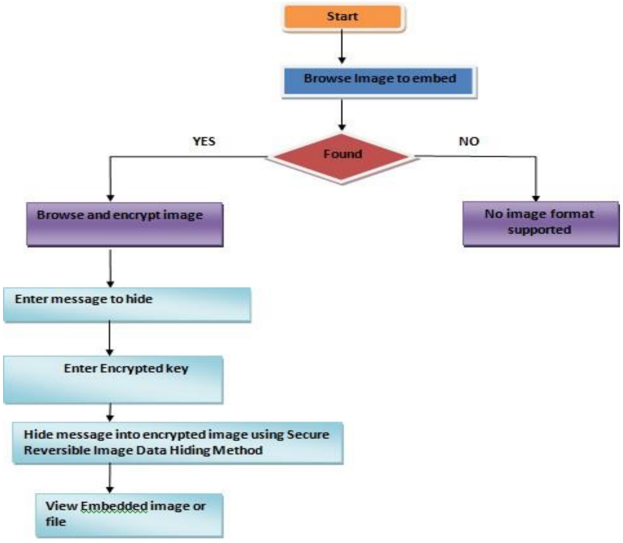
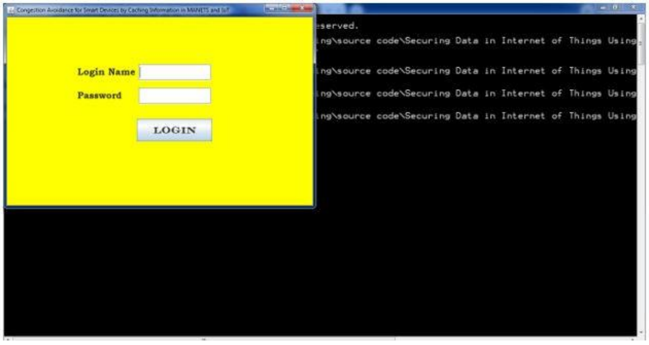

Start
Browse Image to embed
YES
Found
NO
Browse and encrypt image
No image format supported
Enter message to hide
Enter Encrypted key
Hide message into encrypted image using Secure Reversible Image Data Hiding Method
View Embedded image or file

Fig 6. Flow Chart: admin:

Results and Discussion :

IOT Router

In order to receive and reroute the encrypted picture to the proper recipient, the IOT Router serves as a middleman between the transmitter and receiver.

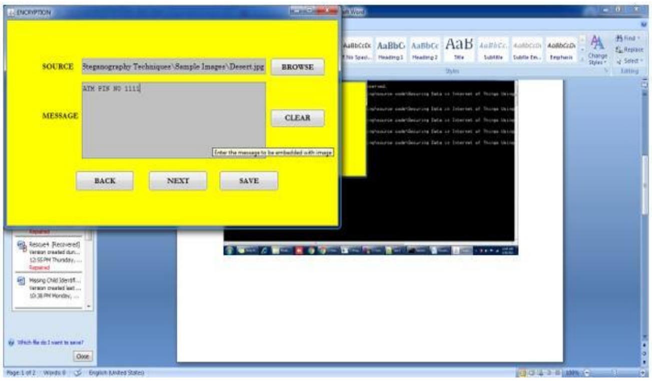


Congestion Avoidance for Smart Devices by Caching Information in MANETS and IoT

Login Name
Password
LOGIN

```
eserved.
ing\source code\Securing Data in Internet of Things Using
ing\source code\Securing Data in Internet of Things Using
ing\source code\Securing Data in Internet of Things Using
ing\source code\Securing Data in Internet of Things Using
```

Fig7.Login Home



ENCRYPTION

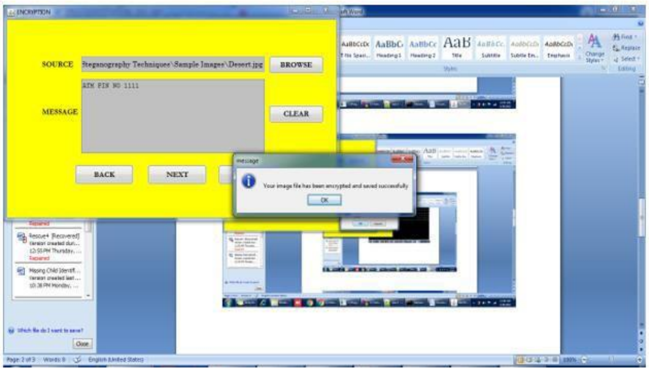
SOURCE: Steganography Techniques\Sample Images\Desert.jpg — BROWSE

MESSAGE: ATM PIN NO 1111 — CLEAR

Enter the message to be embedded with image

BACK — NEXT — SAVE

Fig8.Encript



ENCRYPTION

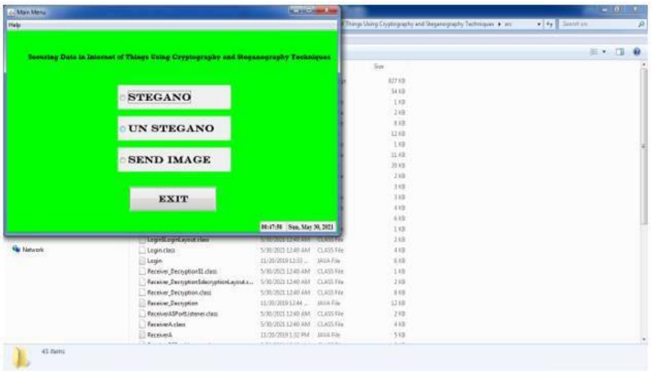
SOURCE: Steganography Techniques\Sample Images\Desert.jpg — BROWSE

MESSAGE: ATM PIN NO 1111 — CLEAR

BACK — NEXT

message: Your image file has been encrypted and saved successfully — OK

Fig9.Image uploaded



Main Menu

Help

Securing Data in Internet of Things Using Cryptography and Steganography Techniques

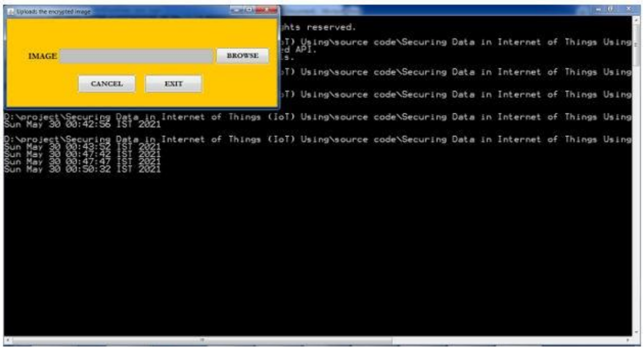
○ STEGANO
○ UN STEGANO
○ SEND IMAGE
EXIT

00:47:50 Sun, May 30, 2021

Login$LoginLayout.class	5/30/2021 12:40 AM	CLASS File	2 KB
Login.class	5/30/2021 12:40 AM	CLASS File	4 KB
Login	11/30/2019 12:33 ...	JAVA File	6 KB
Receiver_Decryption$1.class	5/30/2021 12:40 AM	CLASS File	1 KB
Receiver_Decryption$decryptionLayout.c...	5/30/2021 12:40 AM	CLASS File	2 KB
Receiver_Decryption.class	5/30/2021 12:40 AM	CLASS File	8 KB
Receiver_Decryption	11/30/2019 12:44 ...	JAVA File	12 KB
ReceiverA$PortListener.class	5/30/2021 12:40 AM	CLASS File	2 KB
ReceiverA.class	5/30/2021 12:40 AM	CLASS File	4 KB
ReceiverA	11/30/2019 1:32 PM	JAVA File	5 KB

43 items

Fig10.Main menu



Uploads the encrypted image

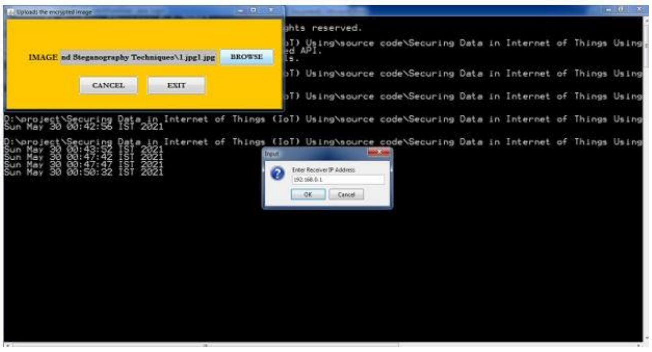
IMAGE — BROWSE

CANCEL — EXIT

```
ghts reserved.
oT) Using\source code\Securing Data in Internet of Things Using
ed API.
is.
oT) Using\source code\Securing Data in Internet of Things Using
oT) Using\source code\Securing Data in Internet of Things Using
D:\project\Securing Data in Internet of Things (IoT) Using\source code\Securing Data in Internet of Things Using
Sun May 30 00:42:56 IST 2021

D:\project\Securing Data in Internet of Things (IoT) Using\source code\Securing Data in Internet of Things Using
Sun May 30 00:43:52 IST 2021
Sun May 30 00:47:42 IST 2021
Sun May 30 00:47:47 IST 2021
Sun May 30 00:50:32 IST 2021
```

Fig11. Upload the encrypted image



Uploads the encrypted image

IMAGE: nd Steganography Techniques\1.jpg1.jpg — BROWSE

CANCEL — EXIT

```
ghts reserved.
oT) Using\source code\Securing Data in Internet of Things Using
ed API.
is.
oT) Using\source code\Securing Data in Internet of Things Using
oT) Using\source code\Securing Data in Internet of Things Using
D:\project\Securing Data in Internet of Things (IoT) Using\source code\Securing Data in Internet of Things Using
Sun May 30 00:42:56 IST 2021

D:\project\Securing Data in Internet of Things (IoT) Using\source code\Securing Data in Internet of Things Using
Sun May 30 00:43:52 IST 2021
Sun May 30 00:47:42 IST 2021
Sun May 30 00:47:47 IST 2021
Sun May 30 00:50:32 IST 2021
```

Input: Enter Receiver IP Address: 192.168.0.1 — OK — Cancel

Fig12.Reciever

CONCLUSION

The EGC protocol's high level of data security provides protection for data transfer in the Internet of Things. The proposed EGC protocol offers enhanced security for cutting-edge ECC in the area of galois. Due to improved embedding efficiency, data concealing efficiency may be improved. Any data may be safely delivered over an IoT network while being safely concealed in deep picture layers thanks to Firefly's suggested protocol and adaptive optimization. Variables including embedding efficiency, PSNR, carrier efficiency, temporal complexity, and MSE are used to assess performance. Finally, the suggested work is implemented in the MATLAB simulator, and a steganography embedding efficiency of roughly 86 percent is attained. The outcomes of this suggested methodology are contrasted with those of approaches now in use, 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 Internetof 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-basedsecurity middleware for the Internet of Things,” in *Proc. ACM 18thACM/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 ofThings,” in *Proc. GLOBECOM IEEE Glob. Commun. Conf.*, Dec. 2017,pp. 1–6.

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

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

[7] N. Chervyakov*et al.*, “AR-RRNS: Configurable reliable distributed datastorage 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 Internetof Things,” *Ad Hoc Netw.*, vol. 32, pp. 3–16, Sep. 2015.