© 2018 IJSRSET | Volume 4 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

# Secure Image Hiding using algorithm IOT and LSB

**Nidhi Chawade*, Priya Bisen , Ankita Makde, Priyanka Kawale**
B.E(CSE), Smt.Rajshree Mulak College of Engineering For Women, RTMNU, Nagpur ,India

## ABSTRACT

Internet of Things (IoT) is a common thing (object) in today's world, which serves as part of our routine life activities. Although it benefits the residential district in several ways, various challenges such as data confidentiality and privacy are created.Cryptography and Steganography are the two major techniques for secret communicationIn this paper we propose a lightweight encryption algorithm named as Secure internet of things (SIT). It is a 64-bit block cipher and requires 64-bit key to encrypt the data. Now this encrypted image is embedded with stego image by using LSB Approach of Steganography. Our proposed model gives two layers of security for secret data, which fully satisfy the basic key factors of information security system that includes: Confidentiality, Authenticity, Integrity and Non – Repudiation.

**Keywords:** Internet of Things, SIT

## I. INTRODUCTION

### 1.1 Cryptography

Any $n-1$ shares revealed no information about the original image. When all $n$ shares were overlaid, the original image would appear. There are several generalizations of the basic scheme including k-out-of-n visual cryptography.[2][3] Encryption is the process of transforming original image(which is readable original image file) into the cipher image(data which is unreadable).Whereas decryption is just opposite process of encryption process in which we retrieve the original image from cipher image. Cryptography is basically used to hide the original image into a coded image so that unauthorized access can be prevented. To encrypt the original image secure internet of things is used.

### 1.2 Steganography

The embedding process produces a stego medium by replacing the information with data from hidden message. To hide hidden information, Steganography gives a large opportunity in such a way that someone can't know the presence of the hidden message and thus they can't access the

Internet of Things (IoT) is among the emerging technologies that would be the greatest agents to change the modern world. It involves machine-to-machine communications with mobile, virtual and instantaneous connections. Not just typical computing devices, IoT system consists of household devices and many other data-gathering sensors. With IoT, people may control their household appliance with just a few touch on their smart devices. In addition, Cisco's Internet Business Solutions Group had predicted the amount of IoT devices to be double (50 billion devices) by 2020 [1]. The convenience and "smartness" of IoT devices helps in the growth of number of these devices. However, some people may still be afraid to have these devices in their homes. Although IoT devices may make people's life a whole lot easier, security experts had mentioned their concernson the potential security problems (The Insecurity of Things), which make the IoT devices among top five security threats in 2015 original message.

Steganography is the art of concealing a message in a cover without leaving a remarkable track on the original message.

There are 4 different types of Steganography:

1. Text
2. Image
3. Audio
4. Video

- TextSteganography:Theyhaveaverysmallamount ofredundantdata,therefore theyareveryoftenlyused.
- Audio/Video Steganography: They are very complex inuse.
- Image Steganography: It is mostly used for hiding process of data. It provides a secure and simple way to transfer the information over the internet.

It is categorized in varioustypes:

- ✓ Transform Domain: It includesJPEG.
- ✓ Spread Spectrum: It includes patchwork.
- ✓ Image Domain: It includes->LSB and MSB in BMP and LSB and MSB inJPG

## II. AIM AND OBJECTIVE

We have worked on two major techniques of data security i.e. Cryptography and Steganography. In our system these two techniques provides higher security to our data. Initially the information is encrypted by using Secure Internet of Things algorithm which is better than other encryption algorithms then the encrypted information is hidden by LSB approach . So it is very difficult for the unauthorized users to identify the changes in the stego image. The use of the Secure Internet of Things algorithm and LSB gives a way to secure the information from illegal user and provide better PSNR value. It is very difficult to recover the hidden image for the third party without knowing the bits of the frames.

This project comprehends the following objectives:

I. To produce security tool based on cryptography techniques.

II. To explore techniques of hiding data using Steganography

## III. EXISTING SYSTEM

Cryptography technique can convert the original text to encrypted text. The encrypted information can decrypt the intruder by get the key information. A single key is used for both contrast to Cryptography, where the enemy is allowed to encryption and decryption. The sender uses the key (or detect, intercept and modify messages without being able some set of rules) to encrypt the original image and sends them to violate certain security premises guaranteed by a cipher text to the receiver. The receiver applies the same cryptosystem, the goal of Steganography is to hide key (or rule set) to decrypt the message and recover the messages inside other harmless messages in a way that original image.

## IV. PROPOSED SYSTEM

Advantage of proposed technique is that it combines both cryptanalysis as well the steaganographic techiniques and hence we can declare it as more secure than any other algorithm. Hence it support secure transmission and also used for fast transmission. Bulk Size- In transmission it uses HTML file, size of which file is not bulky to transfer.

Assuring data security is a big dispute for computer users. Business men, professionals, and home users all have some important data that they want to secure from others.

The combination of these two methods will enhance the security of the data embedded.

Steganography is not the same as cryptography data hiding techniques have been widely used to broadcast of hiding secret message for long time.

Assuring data security is a big dispute for computer users. Business men, professionals, and home users all have some important data that they want to secure from others.

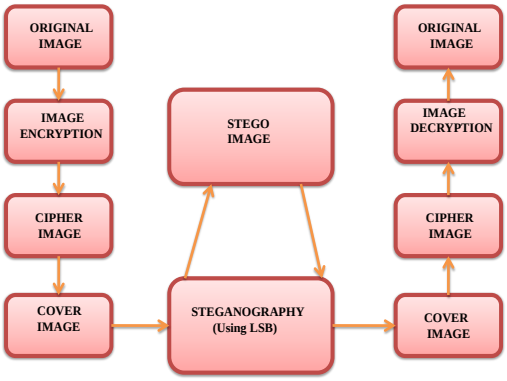



Fig:- Proposed Architecture

## V. METHODOLOGY USED

### 1) Lightweight encryption algorithm or Secure Internet of Things Algorithm:

IOT security is the area of endeavor concerned with safeguarding connected devices and networks in the internet of things(IoT).The cryptographic algorithms are usually designed to take on an average 10 to 20 rounds to keep the encryption process strong enough that suits the requirement of the system.. Some well known block cipher including AES (Rijndael), 3-Way , Grasshopper , PRESENT , SAFER , SHARK , and Square use Substitution-Permutation (SP) network. Other popular ciphers including SF, Blowfish ,Camelia and DES, use the feistel architecture.

The proposed algorithm is a hybrid approach based on feistel and SP networks. SIT is a symmetric key block cipher that constitutes of 64-bit key and original-text. The key generation process involves complex mathematical operations.

### 2) Least Significant Bit(LSB):

Image Steganography technique can be divided into two groups: Image Domain and Transform Domain. Image Domain technique embed message in the intensity of the pixel directly whereas in transform domain technique, images are first transformed and then the message is embedded in image. It is analogous to the least significant digit of a decimal integer, which is the digit in the right-most position.

The least significant bits have the useful property of changing rapidly if the number changes even slightly. By contrast, the three most significant bits stay unchanged (000 to 000).

## VI. MODULES

In our project there are mainly two modules.

1. Encryption module
2. Decryption module

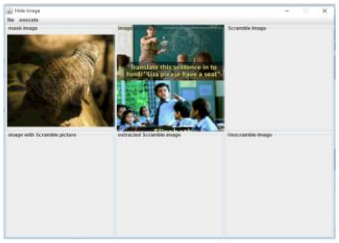
1. Encryption module:- This module is going to encrypt the image, which is commonly known as cryptography. Here we are using the symmetric key to encrypt the image.
2. Decryption module:- This module is going to decrypt the image. Here also we are using the symmetric key to decrypt the image.

- ❖ We are using the Secure internet of things algorithm for encrypting the image. Here we are also using the steganography technique to hide the encrypted image, by using the LSB algorithm, that means we are providing the double security to the image.
- ❖ Cryptography technique can convert the original text to encrypted text.

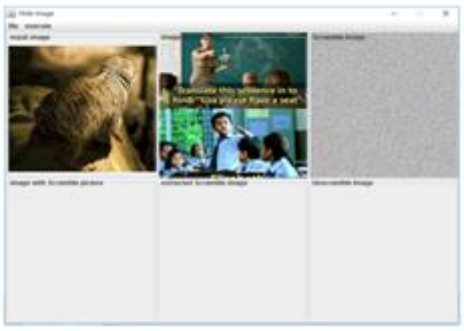
- ❖ In this module first user choose a image for send to receiver. After choosing a image ,secure internet of thing algorithm is used to perform a encryption. Original image is convert into encrypted image and encrypted image is known as cipher image.

- ➢ In our project as we run it, it asks for the image for encryption in such a way that we have to select an image for masking image.

- After that In encryption ,we have to select an image for scrambling of the secret image as shown below.



- After that the image which we select for scrambling that image is converted into scramble image as shown in below.



- Finally we get the encrypted image with hidden scramble image is as follows, which we have selected earlier.

- Now, At the receiver side there will be extraction of scramble image from encrypted image which is given by sender to receiver as shown in figure.

- Finally ,At the receiver side the image will be unscramble and the receiver get the original image

## VII. ADVANTAGE

1. In cryptography we easily hide the information using symmetric and asymmetric key .
2. Cryptography is most useful to secure data hiding or transmission.
3. Using LSB techniques providing strong encrypting key to secure data .
4. Encryptions of the message, so that who extracts it must also decrypt it before it make sense.

## VIII. APPLICATION

Cryptography and Steganography can be used for wide range of applications such as,

- ✓ In defense organizations for safe circulation of secret data.
- ✓ In military and intelligence agencies,.
- ✓ In smart identity cards where personal details are embedded in the photograph itself for

copyright control of materials.

- ✓ In online voting system so as to make the online election secure and robust against a variety of fraudulent behaviors.

  In tamper proofing so as to prevent or detect unauthorized modifications and other numerous applications.

## IX. CONCLUSION

We have worked on two major techniques of data security i.e. Cryptography and Steganography. In our system these two techniques provides higher security to our data. Initially the information is encrypted by using Secure Internet of Thing algorithm which is better than other encryption algorithms then the encrypted information is hidden by LSB approach . So it is very difficult for the unauthorized users to identify the changes in the stego image. The use of the Secure Internet of Thing algorithm and LSB gives a way to secure the information from illegal user and provide better PSNR value. It is very difficult to recover the hidden image for the third party without knowing the bits of the frames. Finally we can conclude that the proposed technique is effective for secret data communication.

## X. FUTURE SCOPE

In the future work, we are looking forward to try applying the proposed method on audio and video. Also, we are looking forward to enhance the proposed method to make the capacity higher than it while keeping the same PSNR or higher. In our work we propose a new approach which give good quality of the image after encoding the original image by using the LSB technique because LSB technique has a drawback it affects the resolution the original image after encoding, so that image quality go burst.The main intention of the project is to develop a steganographic application that provides good security.

## X. REFERENCES

[1]. Rajput A.S., Mishra N., and Sharma S., -Towards the growth of image Encryption and Authentication Schemes‖, International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2013.

[2]. BassemBakhache, Joseph M. Ghazal, and Safwan El Assad,‖Improvement of the Security of ZigBee by a New Chaotic Algorithm‖, IEEE Systems Journal 2013.

[3]. V.Sathyal, K.Balasuhramaniyam, N.Murali, M.Rajakumaran, Vigneswari,‖data hiding in audio signal, video signaltext and jpeg images‖,IEEE-International Conference on Advances in Engineering, Science and Management (ICAESM -2012)

[4]. Audio-video Crypto Steganography using LSB substitution and advanced chaotic algorithm‖.Praveen. P1, Arun. R2M.Tech, Asst. Prof, Dept of Computer Science and Engineering, Shree NarayanaGurukulam College of Engineering, Kadayiruppu, Ernakulam, Kerala.

[5]. K.A Navas, Vidya.V, Sonia.V.Dass,High security data embedding in video‖,Recent Advances in Intelligent Computational Systems (RAICS), 2011 IEEE.

[6]. FatihaDjebbar, BeghdadAyad, HabibHamamandKarimAbed-Meraim,‖A view on latest audio steganography techniques‖, International Conference on innovations in Information Technology 2011.

[7]. Yogita Verma1, Neerja Dharmale2, 1M Tech Scholar Digital Electronics RCET Bhilai, India 2Assistant Professor (ET&T) RCET Bhilai, India, A Survey Paper Based On Image Encryption and Decryption Using Modified Advanced Encryption Standard,International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013)

[8]. Sneha Ghoradkar, Aparna Shinde, Review on Image Encryption and Decryption using AES Algorithm,International Journal of Computer

Applications (0975 – 8887) National Conference on Emerging Trends in Advanced Communication Technologies (NCETACT-2015).

[9]. Muhammad Usman_, Irfan Ahmedy, M. Imran Aslamy, Shujaat Khan_ and Usman Ali Shahy,Faculty of Engineering Science and Technolog,SIT: A Lightweight Encryption Algorithm for Secure Internet of Things,(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, 2017.