

Implementing Information Security Techniques in Internet of Things (IoT) Devices

Prof. B.S.Panchbhai
R.C.Patel Arts, Commerce and Science College, Shirpur
E-mail: bharat.panchbhai@gmail.com

Abstract

The distribution of e-work is a regular occurrence among e-users. There are a number of organisations where all work is done without the use of paper. For such work, it is critical to provide security. Information will be secured in a variety of methods, but when we send data from one computer to another or from a server to a client utilising the Internet of Things (IOT) idea, we used two prominent information security techniques: cryptography and steganography.

Keywords: IoT, DES, AES and LSB

Introduction

Every country now has a growing number of Internet users. All of the computers are used to hold vast amounts of data, yet none of the data on them is secure. When a computer sends information to another computer, such data must be protected. In the field of information security, cryptography and steganography are particularly essential techniques. Almost all devices in today's society are connected via a network.

Many devices, including as tweets, iPhones, automated embedded machines, and manufacturing plants, are used in offices to do a variety of tasks. The number of linked devices is always increasing since new Internet-connected devices are being developed every day to assist consumers in making their daily lives easier and to provide a new digital experience. Smart cities, smart energy plants, automobiles, health services, retail stores, and transportation are all connected by existing and new Internet-based gadgets.

CCTV security cameras and refrigerators, smart city software to assist citizens in finding vacant parking spaces, and personal trainer equipment in the health services industry are examples of this area. [1]

The confidence and control needed to distribute and identify public encryption keys, secure data exchanges over networks, and verify identity are provided by the public key and private key, which establishes a secure infrastructure for better and secure communication between devices or IoT devices.

As we all know, IoT devices must operate at a faster rate, and standard encryption methods such as DES, 3DES, and AES are more difficult. These algorithms take a long time to run and work slowly whenever IoT devices exchange data. We must create a lightweight encryption technique for information security to ensure secure and speedy data transmission. The following is a simple encryption technique that is suitable for IoT devices. [5]

To begin, determine whether the communication is an image or text. The message is clear. The process of decoding, Use a simple symmetric Exclusive OR (XOR) encryption key to encrypt the message.

Table2: Encryption Process

Message Value	Encryption Key Value	Encrypted Value (XOR)
1	0	1
0	0	0
0	1	1
1	1	0

Table1: Decryption Process

Encrypted Value	Decryption Key Value	Decrypted Value
1	0	1
0	0	0
1	1	0
0	1	1

Steganography is the science and art of concealing a message or writing. People must keep their secrets hidden as long as there remain secrets. Steganography and cryptography are frequently confused, despite the fact that they are two distinct fields. Cryptography is a science that requires a password or key to read. Steganography, on the other hand, conceals the fact that there is a hidden message. Due to the absence of privacy in today's environment, steganography is a very essential field. Because no one knows that hidden messages are encoded, steganography allows people to interact without having to check with others.

Algorithm Proposed

Cryptography and Steganography are combined in the proposed lightweight encryption and information concealment technique. In cryptography, we employed symmetric encryption with Exclusive OR(XOR) for text encryption, and we used the LSB (Least Significant Bit) technique to hide the encrypted text in an image. Despite the fact that both techniques are fairly simple, this algorithm requires a key for encryption and the same for decryption. Because of the suggested cryptography and steganography algorithm, information can be transferred or sent from one device to another in a relatively short amount of time while maintaining security. Encoding and decoding in a sequential order

Process of encoding and decoding:

1. For hiding text or images, a JPG, BMP, PNG, or GIF file is required as a Cover Image.
2. Hiding requires a text or image file.
3. Encrypt plain text data with symmetric encryption and offer an encoding key value, as well as reverse the procedure for decryption.
4. Using the LSB technique, embed encrypted data in an image file. The data in a message is encoded from a beginning point.
5. The data in the message is then encoded /decoded in a consistent fashion.

Encoding and Decoding of Pseudo-Random Data

1. For hiding text or images, a JPG, BMP, PNG, or GIF file is required as a Cover Image.
2. Hiding requires a text or image file.
3. Encrypt plain text data with symmetric encryption and offer an encoding key value, as well as reverse the procedure for decryption.
4. Pseudo-Random Number Generator without Starting Point
5. Using the LSB technique, embed encrypted data in an image file. RNG determines the pixel location where message data is encoded/decoded.

Method of sequential steganography

The process of sequential steganography is easy and effective. It is a typical method for concealing secret information in an image. This method is used to conceal images that are 24-bit, 8-bit, or grayscale. The 8th bit of a byte of a cover picture is replaced with a secret message. We insist on picture Steganography exclusively, with a heavy emphasis on LSB approaches in image Steganography. [2]

Until the message is finished, the least significant bit of each pixel is substituted with the secret message bit. We can store three bits in each pixel using a 24-bit image by changing a bit of each colour component in the green, red, and blue colour components. [3]

There is no difference between the cover image and the stego image when the LSB of a pixel is changed. Only half of the bits in the LSB technique are swapped or altered on average. These alterations are invisible to the naked eye. [4].

A bit depth of 8 to 24 or greater is commonly used to express a colour image. The bits in a 24-bit image are commonly divided into three groups: eight for red, eight for green, and eight for blue. Other hues are represented by groupings of those bits. 16.7 Million (2²⁴) colour values are available in a 24-bit picture. Scanners are increasingly recording 10 bit images.

Pseudo-Random Steganography is a way of hiding text or images using a pseudo-random number generator. In this procedure, one random number is generated using the built-in rng function in MATLAB. Encryption is accomplished by combining a key and a random number. Decryption is also a part of the process. Like shown in

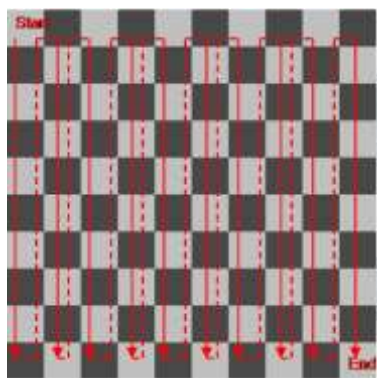


Figure1: Sequential Encoding



Figure2: Pseudo-Random Encoding

Sequential encoding is a simple and uncomplicated approach for encoding, although it has several drawbacks. Messages in similar samples, such as histogram analysis and other steganalysis systems, are always encoded, especially those that are particularly sensitive. Encoding is always used to make it easier for the intruder to access the sensitive message. The programme will have to run the programme again in Matlab, which will take a very long time.

Sequential encoding is pseudo-random encoding. It's extremely efficient and effective. Finding the hidden messages hidden in the cover is really challenging. Furthermore, we discovered that the pseudo-random decoding procedure was more efficient and time-consuming than utilising the changing counter during recovery because the set of pixel location sets was once counted during the process. Decoding requires less time than sequential encoding. [1]

Conclusion and analysis

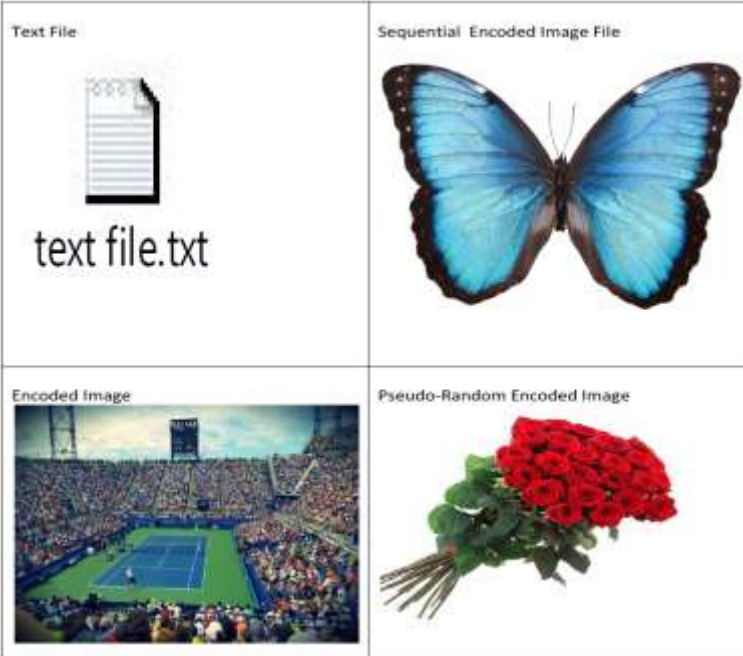
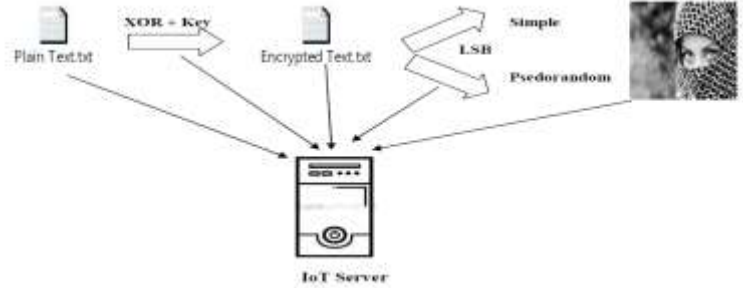
<p>After employing two IoT devices (computers) to execute the suggested algorithm for some small and large text files as a message and cover image, After embedding encrypted text in the BMP file, 100 percent of the same data was extracted without any data loss, and while sequential encoding takes less time to embed and extract data in the cover, psedo-random takes more time.</p>	
<p>Submission of Txt file and image file to IoT sever by applying Crypto-Stegno lightweight algorithm</p>	

Figure 3: Crypt-Stegno technique on IoT

Conclusion

IoT is one of the most important principles in moving secure and confidential data from one device to another. The lightweight technique described above will be useful in iPhones and other smart gadgets that can be used to share information.

References:

1. Steganography-The hidden message, David Pipkorn and Preston ,Weisbrot
2. Computational Photography (CS 534) Course Project - Fall 2012 .
3. Priyanka B. Kutade, Parul S. Arora Bhalotra, “ A Survey on Various Approaches of Image Steganography”, *International Journal of Computer Applications (0975 – 8887) Volume 109 – No. 3, January 2015, page 1-5.*
4. Manjinder Kaur and Varinder Kaur Attri, “Implementation of Steganographic Method based on Interpolation and LSB Substitution.
6. Digital Images with Watermarking and Visual Cryptography”, *International Journal of Computer Applications (0975 – 8887) Volume 121 – No.21, July 2015, page 7-12*
7. A Review of Data Security and Cryptographic Techniques in IoT based devices, Ghulam Mustafa, Rehan Ashraf, Muhammad Ayzed Mirza, ICFNDS’18, June 26–27, 2018, Amman, Jordan,