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

A Survey on Image Cryptography Using Lightweight Encryption Algorithm

Bhinal Chauhan[1], Shubhangi Borikar[1], Shamali Aote[1], Prof. Veena Katankar[4]
1Department of CSE, Smt.Rajshree Mulak College of Engineering For Women, RTMNU, Nagpur, India
[4]M.E.(WCC), Asst. Prof (CSE), Smt.Rajshree Mulak College of Engineering For Women, RTMNU, Nagpur, India

ABSTRACT

In the present scenario, any communication of internet and networks application requires security as it is very much crucial part over a network. Lots of data security and data hiding algorithms have been developed in the last decade for such purpose. Cryptography and steganography are the two techniques for secret communication over the network. In this paper we propose a lightweight encryption algorithm also known as secure internet of things (SIT) algorithm. 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 which includes: Confidentiality, Authenticity, Integrity and Non – Repudiation.
Keywords: Cryptography, steganography, stego image, cipher image, encryption, decryption.

I. INTRODUCTION

In the present era, communication through computer network requires the highest security. Attacks may affect the delicacy of the data. There are various numbers of approaches available for it. In this paper we are introducing a two major techniques for image security. We are providing security to image by using combination of cryptography and steganography mechanism.

Cryptography

Cryptography is the art and science of achieving security by encoding message to make them non-readable which means it is used to protect the user data .Cryptography consist of two basic functions that are encryption and decryption. 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.

Steganography

Steganography is a technique to hide information from the observer to establish an invisible communication. This steganography system consists of a cover media into which the secret information is embedded. 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 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

- ✓ Text Steganography: They have a very small amount of redundant data, therefore they are very oftenly used.
- ✓ Audio/Video Steganography: They are very complex in use.
- ✓ Image Steganography: It is the most widely used for hiding process of data. It provides a secure and simple way to transfer the information over the internet.

It is categorized in various types:

- ✓ Transform Domain: It includes JPEG.
- ✓ Spread Spectrum: It includes patch work.
- ✓ Image Domain: It includes->LSB and MSB in BMP and LSB and MSB in JPG

II. LITERATURE SURVEY

A. Review on Image Encryption and Decryption technique using AES Algorithm

This paper is based on the encryption and decryption of the image by using the Advanced Encryption Standard Algorithm.The Advanced Encryption Standard (AES) algorithm is a symmetric block cipher that processes image which is of blocks size 128 bits using three different cipher key sizes of lengths 128,192 or 256 bits. Based on the key size length used, the number of execution rounds of the algorithm is 10, 12 or 14 respectively. The proposed system consists of block size of 128 bits and key size of 256 bits. The algorithm is applied for both image encryption and decryption. As the key size is of 256 bits it will take 14 rounds. The use of the internet and wireless communications has been rapidly growing and occupying a wide area in everyday life. Millions of users generate and interchange large amount of electronic data on a daily basis in diverse domains. However, the issue of privacy and security is on the top of the crucial concerns which determine the diffusion of such applications into the daily life. Hence, cryptography turns to become the key for the reliability and effectiveness of the embedded. In this paper there uses the various rounds to encrypt an image.

B. SIT: A Lightweight Encryption Algorithm for Secure Internet of Things

In this paper the need for the lightweight cryptography have been widely discussed for securing an image, also the shortcomings of the IoT in terms of constrained devices are highlighted. In secure systems the confidentiality of the data is maintained and it is made sure that during the process of message exchange the data retains its originality and no alteration is unseen by the system. The IoT is composed of many small devices such as RFIDs which remain unattended for extended times, it is easier for the adversary to access the data stored in the memory. The proposed algorithm provides a simple structure suitable for implementing in IoT environment. Some well known block cipher including AES , 3-Way, Grasshopper PRESENT, SAFER, SHARK, and Square use Substitution-Permutation (SP) network. Several alternating rounds of substitution and transposition satisfies the Shannon's confusion and diffusion properties that ensues that the cipher text is changed in a pseudo random manner.

C. A Survey Paper Based On Image Encryption and Decryption Using Modified Advanced Encryption Standard

With the ever-increasing growth of multimedia applications, Important issue for communication and storage of images is security, and encryption is one the technique to ensure security. Their different encryption techniques are used to protect the confidential message from unauthorized user.

Cryptography is technique particularly used for secure communication, in this paper, it has been surveyed about the existing works on the encryption techniques such as AES, 3DES, Blowfish and DES.DES key size is too small as compare to other techniques. 3DES is slower than other block cipher methods and has poor performance. AES algorithm was considered to be the best algorithm than that of blowfish algorithm. The adjacent pixels in an image have close relation which cannot be easily removed by AES algorithm.

D. A review on Image encryption techniques

In this paper the author described about many traditional encryption techniques like DES, AES or IDEA etc for providing high security to the data that may be textual or image form. These techniques are difficult to use them directly in multimedia data because of some shortcomings on the key space, encryption speed and other aspects. On the other hand exchanging techniques for scrambling and transforming are used mainly for image encryption which are very simple and are easy to implement. But due to the simplicity of these techniques, the decryption process is also very simple so a third person can easily crack the algorithm. To provide high security this technique is combined with the other technique. In this paper we have learned that compression and encryption both are combined and formed a new technique which is effective but needs additional operating requirements. Every technique has its own advantages or disadvantages according to the way of its working.

III. 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. In our paper we used a LSB to hide encrypted image into stego image, which provides the new look to the image steganography. It is very difficult to recover the hidden image for the third party without knowing the bits of the frames. Finally we conclude that the proposed technique is effective for secret data communication.

IV. REFERENCES

[1]. Rajput A.S., Mishra N., and Sharma S.,-Towards the growth of image Encryption and Authentication Schemes‖, (ICACCI), 2013.

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

[3]. Audio-video Crypto Steganography using LSB substitution and advanced chaotic algorithm‖.Praveen. P1, Arun. NarayanaGurukulam College of Engineering, Kadayiruppu, Ernakulam, Kerala .

[4]. Abboud, G.; Marean, J.; Yampolskiy, R.V.;"Steganography and Visual Cryptography in Computer Forensics," Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 Binary Images," Innovative Computing, Information and Control,2006.ICICIC '06.

[5]. 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)

[6]. 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).

[7]. 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.

[8]. Bhinal Chauhan is a student of Final year B.E, department of Computer Science and Engineering, college of Smt. Rajshree Mulak College of Engineering for Women, Rashtrasanth Tukdoji Maharaj University Nagpur.

[9]. Shamali Aote is a student of Final year B.E, department of Computer Science and Engineering, college of Smt. Rajshree Mulak College of Engineering for Women, Rashtrasanth Tukdoji Maharaj University Nagpur.

[10]. Shubhangi Borikar is a student of Third year B.E, department of Computer Science and Engineering, college of Smt. Rajshree Mulak College of Engineering for Women, Rashtrasanth Tukdoji Maharaj University Nagpur.

[11]. Veena Katankar is a Asst. Prof. of Computer Science and Engineering department, college of Smt. Rajshree Mulak College of Engineering for Women, Rashtrasanth Tukdoji Maharaj University Nagpur.