ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152

www.ijmece .com

Vol 12, Issue 2, 2024

SECURE DATA TRANSFER THROUGH INTERNET USING CRYPTOGRAPHY AND IMAGE STEGANOGRAPHY

[1]M Sravanthi, [2]Reddeddy Kavya,[3]Alakuntla Poojitha,[4]Kota Harika

[1]Assistant professor in Department of Information Technology Bhoj Reddy Engineering College forWomen

[2,3,4] UG Scholars in Department of Information Technology Bhoj Reddy Engineering College for Women

Abstract

Hacking became a big problem these days. Transmission of secure Data or communication through internet turns to be challenging due to security concerns. In order to forestall these security obstacles, we used Cryptography, Image Steganography. Over the centuries, there are numerous advancements in information security. Steganography and cryptography are the two emerging techniques for secure data transmission over years. Cryptography is the art of encrypting the text whereas Steganography is used to hide the text inside any multimedia element that appears to be nothing. Steganography makes the data secure as if any person views the file, he/she cannot sense that there is some secret message hide in that, human senses cannot detect or sense the data inside the multimedia element. In this paper, we proposed a system that uses both cryptography and steganography to ensure two levels of security to the data. The purpose of this paper is to develop new methodology using XOR operation for encrypting the data and embedding the encrypted data into the image pseudo randomly using user chosen key

I INTRODUCTION

Internet is no longer safe to transfer sensitive information. The dependence of the people made the hackers to monitor the network and attack for sensitive information. The data is securely saved in our system might not be safe when we transfer it over the internet.

Also, the system itself can be affected with virus, trojans and malwares in variety of ways. This leads to intrusion into the system and again loss of data. Therefore, security is the most important thing for the people since evolution of hacking. Steganography is the method of embedding the data into object where human sense cannot sense it [1]. This means the communication is accomplished in such a way that the message existence cannot be identified. The word cryptography in Greek can be shown as ‘Krypto’ means hidden and ‘graphene’ means to writing.

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

Image Steganography A digital image is most secure way to carry the sensitive information through the internet using steganography. The image is captured using the camera, the light of the camera will sense the object which should be captured, and the will be displayed on the screen of the camera. Image is combination of the pixels; the resolution of the picture depends upon the pixel. Pixel is the minute are of illumination on a display screen. Human eyes cannot sense the pixels in the image.Pixel is made of three components. Three components of the pixel are Red, Green and Blue (R, G and B). Each pixel has depth of 24 bits that is 3 bytes [2]. Each component is of size one byte. Any color is formed by the combination of these three components. The byte value varies from 0 to 255. The color will be displayed based on the value of the bits, 0 is the darkest and 255 is the brightest. The size of the picture is given in the pixels, for example the size of the picture is 600*450, then the image is the combination of 2,70,000 pixels. pixel is made of three components which of each component is size of 8 bits, for example 11111111 00000000 00000000 is the pixel bits then the pixel will red in color. Depending upon the RGB values the pixel color will be changed.

II LITERATURE SURVEY

The image protection in wireless channel is proposed in [7]. After embedding the data using LSB, the image is divided into blocks which is size of 8*8. The blocks are encrypted using double random phase encoding which converts into stationary noise. Using Fourier transformation, the image multiplied by random phase mask is converted to frequency domain from time domain and random phase mask is applied.

presented an enhanced safe data transfer scheme in smart Internet of Things (IoT) environment. They proposed a technique that employ an integrated approach of steganography and cryptography during data transfer between IoT device & home server and home server & cloud server. The sensed data from IoT device is encrypted and embedded in the cover image along with message digest of sensed data and send to the home server for authentication purpose. At the home server the embedded message digest and encrypted data version is extracted. The received digest is compared with newly computed digest to ensure data integrity and authentication. The same procedure is carried out between home server and cloud server.

the data to be transferred is encrypted using RSA algorithm. Using LSB the encrypted data is hidden inside audio object which provided high security to the data.

The secret message is encrypted using Vernan cipher according to [10]. The data is embedded into the image using LSB. The authors used grayscale images.

S-DES algorithm is used in [11] to encrypt the secret message to produce an array. The elements of the array are divided into 2 parts where first part contains 4 MSB's and other contains LSB's. The value of each pixel is transformed into alphabets from A to P which is from 0000 to 1111. Using XOR operation the data is embedded

III EXISTING SYSTEM

The data is used more widely in present days and authenticity is becoming a much problem while sharing or transmitting through medium. In order to securely transmitting the data through internet there were several methodologies developed using image steganography and cryptography.

visual cryptography and neural networks. Using AES algorithm, the data is encrypted. Neural network is used to find the best location in the image blocks generated by the visual cryptography and to embed the data using LSB. The application of inverse cryptography is accomplished during decryption.

The image protection in wireless channel is proposed. After embedding the data using LSB, the image is divided into blocks which is size of 8*8. The blocks are encrypted using double random phase encoding which converts into stationary noise. Using Fourier transformation, the image multiplied by random phase mask is converted to frequency domain from time domain and random phase mask is applied.

Existing approaches presented an enhanced safe data transfer scheme in smart Internet of Things (IoT) environment. They proposed a technique that employ an integrated approach of steganography and cryptography during data transfer between IoT device & home server and home server & cloud server. The sensed data from IoT device is encrypted and embedded in the cover image along with message digest of sensed data and send to the home server for authentication purpose. At the home server the embedded message digest and encrypted data version is extracted. The received digest is compared with newly computed digest to ensure data integrity and authentication. The same procedure is carried out between home server and cloud server.

the data to be transferred is encrypted using RSA algorithm. Using LSB the encrypted data is hidden inside audio object which provided high security to the data.

The secret message is encrypted using Vernan cipher. The data is embedded into the image using LSB. The authors used grayscale images.

S-DES algorithm is used to encrypt the secret message to produce an array. The elements of the array are divided into 2 parts where first part contains 4 MSB's and other contains LSB's. The value of each pixel is transformed into alphabets from A to P which is from 0000 to 1111. Using XOR operation the data is embedded.

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

it has introduced has given a hybrid approach for the security if the data that enhances the quality if the encryption. Used blowfish algorithm to encrypt the image to cipher image. Then the encrypted image is embedded using LSB technique in the cover image. Blowfish algorithm is lossless and highly secured encryption technique.

Mp3 file is used as a cover object. The secret message is encrypted using AES algorithm with the key generated by MD5 hash function. The encrypted data is embedded into mp3 files along with key code.

The author uses space domain steganography. One image is embedded into another image. Using a key as a seed pseudo randomness is generated in the images. The pixel is selected and using column sequence and row sequence, the plane of secret image is divided into 16 pixels.

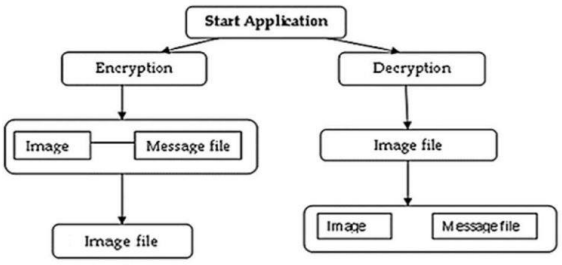
IV PROPOSED SYSTEM

The technique to hide the data inside an image is called image steganography. Humans cannot make a difference in the image when the data is embedded in it. It takes quite knowledge and tool practice to identify the image. We are using cryptography and steganography to provide high security to the data over a network.

V IMPLEMENTATION

A private key is used as seed to randomly generate the sequence of number of pixels which can be used to store the secret message. Using the same private key, the message is encrypted and then used to embed into the pixels. Since noise will be generated after embedding the bits, instead we use pictures where each pixel has a noise before using it. It is helpful because, since all the pixels has noise, the hacker will have hard time to find the pixels with embedded information. A system is created in such a way that the image can be viewed only with the person login credentials which is shared with. Instead of embedding each bit in 3 components of pixel (RGB) we replace one component (Either R, G or B) which is a byte with secret message byte. By doing this, hacker cannot know how many bits are hidden in a pixel and in which component the message bits are stored.

VI ARCHITECTURE



VIII CONCLUSION

In this paper, we concluded that using crypto-steganography, one can achieve two levels of security. There will be no thirdparty interruption

by using this technique because no one can even know that data is embedded into the image as there will be no noise created in the cover image. It provides high level of integrity and confidentiality of messages. There are numerous numbers of algorithms are developing to overcome the lags in the existing algorithms and enhancing the level of security of the data transmitted through the internet. Whereas there are many message detection techniques are developing simultaneously, still detection doesn't guarantee retrieving all the information. Crypto steganography is the technique where we encrypt the data using the key and using that key, we are embedding the data in the pixels of the cover image pseudo randomly. Even though we are changing the bits of the components of the pixels of the image there will not be more distortion in the stego image, however there will be some distortion created that cannot be seen by human eyes. Furthermore, we are hiding the data in the noisy picture and transmitting so that data will be more secure. By this way the stego image will be same as the cover image. Numerous application areas are developing like the cloud security, online communication sites etc., the vision into the crypto steganographic principles will make us find vivid areas of application.

REFERENCES

[1] SREELAKSHMI (2015, NOV 9). "Image steganography using LSB," https://www.slideshare.net/SreelekshmiSree1/image- steganographyusing-lsb (accessed: February 27, 2019).

[2] K. Curran and K. Bailey, "An Evaluation of Image Based Steganography Methods," Multimedia Tools and Applications, Vol. 30 Issue 1, pp. 55 – 88, July 2006.

[3] Osuolale and A. Festus, "Secure Data Transfer Over the Internet Using Image Crypto Steganograph y." in International Journal of Scientific & Engineering Research, 8(12), pp. 6-9, December 2017.

[4] S. Singh and V. K. Attri, "Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm ", in International Journal of Signal Processing, Image Processing and Pattern Recognition,Vol. 8, No. 5, pp. 259-266, 2015. [5] R. Böhme, "Advanced Statistical Steganalysis information security and cryptography," in New York, NY: Springer. DOI: 10.1007/978- 3- 642-14313-7, May 2010.

[6] K.S. Seethalakshmi, Usha. B, and Sangeetha. K. N, "Security Enhancement in Image Steganography Using Neural Networks and Visual Cryptography," in IEEE Int. Conf. Computation System and Information Technology for Sustainable Solutions (CSITSS), 2016.

[7] S. Bukhari, M. S. Arif, M.R. Anjum and S. Dilbar, "Enhancing security of images by

Steganography and Cryptography techniques", in IEEE Int. Conf. Innovative Computing Technology (INTECH), 2016.

[8] R. Das, I. Das, "Secure Data Transfer in IoT environment: adopting both Cryptography and Steganography techniques", in IEEE Int. Conf. on Research in Computational Intelligence and Communication Networks (ICRCICN), 2016.

[9] A. Gambhir and S. Khara, "Integrating RSA Cryptography & Audio Steganography", in IEEE ICCCA, 2016.

10] K. Joshi, R. Yadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication," in IEEE ICIIP, 2015.

[11] V. Shanna and Madhusudan, "Two New Approaches for Image Steganography Using Cryptography" in IEEE Int. Conf. Image Information Processing, 2015.

[12] M. Mukhedkar, P. Powar and P. Gaikwad, "Secure non-real- time image encryption algorithm development using cryptography & Steganography", in IEEEINDICON,2015.

[13] R. Indrayani, H. A. Nugroho, R. Hidayat, I. Pratama, "Increasing the Security of MP3 Steganography Using AES Encryption and MD5 Hash Function," in International Conference on Science and TechnologyComputer (ICST), IEEE, 2016.

[14] N. Patel, S. Meena, "LSB Based Image Steganography Using Dynamic Key Cryptography", in International Conference on Emerging Trends in Communication Technologies (ETCT), 2016.