International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in; editorijoer@gmail.com

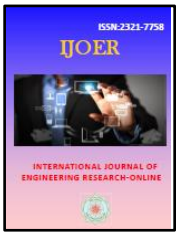
Vol.6., Issue.6, 2018
Nov-Dec

REVIEW ARTICLE

ISSN: 2321-7758

An Enhanced Image Encryption Technique for Effective Transmission in IoT Devices: An Overview

SWATHY.K.SHAJI
M G University



ABSTRACT
The paper proposes a novel method of image encryption that can be used in areas like the geographical boundary of a country, other geographically inaccessible areas and other confidential areas that is most prone to attacks. The paper uses a motion detection sensor to effectively detect the physical movement in a given area, and then capture the image and send it to the receiver after encrypting it. The proposal is based on the use of Voronoi Tessellation [4] to transform the image captured into a vector, that represents less than 1% of the raw image volume. The content confidentiality of the image can be preserved by keeping secret the positions behind the generation of the vector. This enhanced encryption method effectively encrypts the image and sent it to the receiver.

I. INTRODUCTION

In the last years, the Internet of Things is turning out to be an emerging discussion in the research domains. The IoT is taking the mobile network, conventional internet and sensor network to another level as everything will be connected to the internet. The matter of concern with the devices is the issues related with the data integrity, confidentiality and authenticity[1].

IoT is expected to connect millions of devices and is expected to generate a huge amount of data as well. One of the serious challenge faced by the devices were the threat of data security. The IoT systems suffer from different limitations, and were constrained in terms of energy and computational power, which renders them extremely vulnerable to attacks. As a matter of concern the need of a secure environment is vital in order to secure the transmission of data from the device over the network. The paper proposes a novel method of image encryption that can be used in areas like the geographical boundary of a country, other geographically inaccessible areas and other confidential areas that is most prone to attacks. The paper uses a motion detection sensor to effectively detect the physical movement in a given area, and then capture the image and send it to the receiver after encrypting it. The proposal is based on the use of Voronoi Tessellation [4] to transform the image captured into a vector, that represents less than 1% of the raw image volume. The content confidentiality of the image can be preserved by keeping secret the positions behind the generation of the vector. This enhanced encryption method effectively encrypts the image and sent it to the receiver.

Applications of IoT Devices

With the revolution of telecommunication, more and more devices are getting connected to the Internet. A great number of devices such as personal computer, tablets, laptops, smart phones, smart TVs, video game consoles even the refrigerators and air conditioners have the ability to communicate with each other or over Internet[1].

Security Challenges of IoT Devices

The biggest security related threat of IoT systems from the traditional IT systems is that the devices can become a target of cyberattacks[3]. To adopt the IoT technology it is essential to build confidence among the users about its security and

privacy[1]. From a high level perspective, IoT is composed of three components namely, Hardware, Middleware and Presentation [1]. Hardware consists of sensors and actuators, the Middleware provides storage and computing tools and the presentation provides the interpretation tools accessible on different platforms[1]. In IoT the sensor nodes themselves are considered as the Internet nodes making the authentication process even more significant[2].

II. Objectives

A recent study by HP reveals that 70% of the devices in IoT are vulnerable to attacks[5]. An attack can be performed by sensing the communication between two nodes which is known as man-in-the-middle attack. No reliable solution has been proposed to cater such attacks. The paper proposes an image encryption method to effectively reduce the data volume and ensures the content confidentiality. The major objectives of the study is to :

1. Reduce the transmitted data volume
2. Ensures Content confidentiality
3. Reduce the attacks
4. Ensures Integrity and Authenticity to the data transmitted.

III. Review of Literature

Mourad Talbi et.al [1]proposes a lightweight encryption algorithm named as Secure IoT (SIT) to a quantized speech image for Secure IoT. It is a 64-bit block cipher and requires 64-bit key to encrypt the data. This quantized speech image is constructed by first quantizing a speech signal and then splitting the quantized signal into frames. Each of these frames is transposed for obtaining the different columns of this quantized speech image.

Muhammed Usman et.al[2] proposes a lightweight encryption algorithm named as Secure IoT (SIT). It is a 64-bit block cipher and requires 64-bit key to encrypt the data. The architecture of the algorithm is a mixture of fiestal and a uniform substitution permutation network. Simulations result shows the algorithm provides substantial security in just five encryption rounds. The hardware implementation of the algorithm was done on a low cost 8-bit micro controller and the results of code size, memory utilization and encryption/decryption execution cycles are compared with benchmark encryption algorithms.

Saurabh Singh et.al discusses a state-of-art of lightweight cryptographic primitives which include lightweight block ciphers, hash function, stream ciphers, high performance system, and low resources device for IoT environment. The paper analyze many lightweight cryptographic algorithms based on their key size, block size, number of rounds, and structures. In addition, the work discuss the security architecture in IoT for constrained device environment, and focus on research challenges, issues and solutions.

Mostefaoui et.al[4] proposes a novel integrated approach, specifically tailored to significantly reduce the size of the transmitted multimedia data whilst ensuring its content confidentiality. In opposition to traditional approaches, based on cryptographic systems which inquire a huge overhead when applied to multimedia data, their approach makes use of Voronoi tessellation to transform the input data. This transformation is performed on a random fashion basis, allows both significant data reduction and content confidentiality as well, while it exhibits a very low complexity.

Light Weight Encryption Algorithms: A light weight encryption algorithm may differ in key size, block size and the number of rounds for performing the encryption task. The light weight cryptographic algorithms that is used is indicated in the table.1 below:

Table.1. Light Weight Cryptographic Algorithms

Algorithm	Keysize	BlockSize	Structure	No. Of Rounds
AES	128/192/256	128	SPN	10/12/14
HEIGHT	128	64	GFS	32
PRESENT	80/128	64	SPN	31
TEA	128	64	Feistel	64
LEA	128, 192, 256	128	Feistel	24/28/32
DES	54	64	Feistel	16
Seed	128	128	Feistel	16
Twine	80/128	64	Feistel	32

DESL	54	64	Feistel	16
3DES	56/112/168	64	Feistel	48
Iceberg	128	64	SPN	16
Pride	128	64	SPN	20

Light weight cryptographic primitives is summarized in Figure.1. indicated as below:

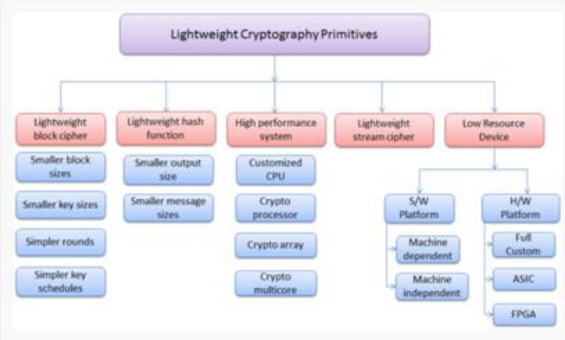


Fig.1. Light weight cryptography Primitives

Light Weight block Ciphers : Light weight block ciphers are light weight cryptographic primitives. A good block cipher must be fast and secure. Block Ciphers has two designs namely: Substitution permutation network and Feistel network.

Substitution permutation network aims to provide both confusion and diffusion using two distinct operation. Confusion aims at making relationship between plain text, key and cipher text. Diffusion must focus on the fact that a small modification on plaintext must spread to cipher text as well.

A festal network is used in the construction of block cipher based algorithm. It implement a series of iterative ciphers on a block of data. It is widely be used for encrypting large quantity of data. The festal network works by splitting the data block into two equal pieces and apply the encryption method in multiple rounds. Each of the round implement permutation and combination derived from primary key.

Light Weight Stream Ciphers: Light weight Steam ciphers are light weight cryptographic primitives. To build a stream cipher, we have to use a regular block cipher in counter mode. It is a symmetric cipher in which each character of plain text is transformed into a symbol of cipher text. It uses a different approach to image encryption, rather than a block cipher.

Methodology Adopted: The proposed paper uses a motion detection sensor that can detect the physical movement in a given area. The work discusses a novel method of image encryption that can be used in areas like the geographical boundary of a country, geographically inaccessible areas and other confidential areas which is most prone to attacks. The motion detection sensor is incorporated on a camera that eventually captures the image whenever the sensor detects the physical movement. The captured image is then transmitted to the receiver after encrypting it using the method of cell substitution.

Motion detection sensors: A motion detector is an electronic device which is used to detect the physical movement(motion) in a given area and it transforms motion into an electric signal. Motion detection plays an important role in the security industry. Businesses utilize these sensors in areas where no movement should be detected at all times, and it is easy to notice anybody's presence with these sensors installed. These are primarily used for intrusion detection systems, Automatics door control, Boom Barrier, Smart Camera (i.e motion based capture/video recording),Toll plaza, Automatic parking systems, Automated sinks/toilet flusher,Hand dryers, energy management systems(i.e. Automated lighting, AC, Fan, Appliances control) etc.

Image sensors: Image sensors is instruments which is used to convert optical images into electronic signals for display or storage files electronically. The major use of image sensor in Digital camera & modules, medical imaging and night vision equipment, thermal imaging devices, radar, sonar, media house, Biometric & IRIS devices.

Encryption method: The captured image were divided into multiple cells (or convex poltgons) and the cell colour is replaced with the mean color of all pixels belonging to that cell. Thus the image is converted into a color vector and is transmitted to the receiver after encrypting the message using secret key.

Source Side: Voronoi Tessellation [4] is the partioning of a plane with a set of N points into convex polygons known as Voronoi cells, where each cell contains exactly one generating point is

called a site. The paper uses the Voronoi tessellation on the captured image at the source, where N sites are generated using a common generator shared between source and destination. These generated points are used for Voronoi tessellation[4].The color of each cell in the captured image is replaced with the mean color of all pixels belonging to that cell. This process significantly reduces the image size. After the mean color computation the image is replaced with a color vector and sents it to the destination.

Destination side: In the destination side upon receiving the color vector, regeneration of the same Voronoi tessellation is performed, to reconstruct the original image correctly. Each source has its own unique secret key and is later used for the generation of dynamic key which is generated with the help of a random generator shared between source and destination. The dynamic key generated along with the color vector is transmitted to the receiver. The destination side performs the same operation in the reverse order.

IV. Conclusion

The paper proposes a novel method of image encryption that can be used in areas like the geographical boundary of a country, other geographically inaccessible areas and some confidential areas that is mostly prone to attacks. In the paper we are using a motion detection sensor to effectively detect the physical movement in a given area and then capture the image and send it to the receiver after encrypting it. The work employs an enhanced encryption method to effectively encrypt the image captured and thus effectively transmit the one captured to the receiver. The proposed work significantly reduces the data volume and ensures the content confidentiality as well.

References

[1]. IoT Mourad Talbi, Med Salim Bouhlel on “Application of a light weight Encyption algorithm to a quantized speech image for secure IoT”, in 2017 Sixth International Conference on Advances in Computing, Electronics and Communication.

[2]. Muhammad Usman, Irfan Ahmed , M. Imran Aslam, Shujaat Khan and Usman Ali Shah on “SIT: A lightweight encryption algorithm for secure Internet of Things”, in *2017 International Journal of Advanced Computer Science and Applications*, Vol. 8, No. 1.

[3]. Saurabh Singh, Pradip Kumar Sharma, Set Yeon Moon, Jong Hulk Park on “Advanced lightweight Encryption algorithms for IoT devices: survey, challenges and solutions”, in *2017 Journal of Ambient Intelligence and Humanized Computing,* pp 1-18.

[4]. Mostefaoui, H Noura, Z Fawaz on “An integrated multimedia data reduction and content confidentiality approach for limited networked devices”, *in 2015 Journal on Adhoc Networks,* Vol 32 Issue C.

[5]. S.A Kumar, T. Vealey, and H.Srivastava, “Security in Internet of Things: Challenges, solutions and future directions”, in *2016 49th Hawai International Conference on System Sciences(HICSS)*. IEEE, 2016, pp. 5772-5781