IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 5, Issue 10, October 2018

Instigating Improved Steganography Scheme for Internet of Things

Manikandan.C[1], Dr.S.Prema[2]

M. Phil Research Scholar, Department of Computer Science (PG),

K. S. Rangasamy College of Arts and Science (Autonomous), Tiruchengode, Tamilnadu, India[1]

Associate Professor, Department of Computer Science (PG),

K. S. Rangasamy College of Arts and Science (Autonomous), Tiruchengode, Tamilnadu, India[2]

Abstract: The evolution of the IoT and pervasive computing creates a significant impact in the information and commination. The growth rate of the devices seems to be hiked in exponential manner. The overall objective seems to be providing better services for the end user with the emergence of the new age gadgets. Steganography exist the complete of conceal a file, message, image, or video within another file, message, image, or video. The benefit of steganography in overload of cryptography alone be to the planned secret communication doing not attract attention to itself as an object of scrutiny. Plainly able to be alive see encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be there incriminating in countries in which encryption is illegal. IoT is one such technology, which holds many promising aspects in networking and communication. In another perspective the nature of the data handled in the IoT is more open and vulnerable for hacking. Since the data handled through the IoT technology is sensitive and almost deals with personal privacy, industry needs to cater the security concerns in IoT.

Keywords: Steganography, IoT**,** Least Significant Bit, Network

I. INTRODUCTION

IoT is the technology of the decade which also in turn has lots of potential points for breach of information. This research addresses the problem of security concern and proposes enhanced steganography scheme for the IoT devices. The evolution of the IoT and pervasive computing creates a significant impact in the information and communication. The growth rate of the devices seems to be hiked in exponential manner. The overall objective seems to be providing better services for the end user with the emergence of the new age gadgets. Steganography exist the complete of conceal a file, message, image, or video within another file, message, image, or video. The benefit of steganography in overload of cryptography alone be to the planned secret communication doing not attract attention to itself as an object of scrutiny. Plainly able to be alive see encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be there incriminating in countries in which encryption is illegal. This research proposes a technique, which can hide the secret data in image layers, and steganography for IoT. The proposed strategy is LSB substitution ciphers for the IoT. Experiments are conducted with different aspect ratio images, which show that the proposed algorithms seem to work better. The proposed method performs well in specifically in RGB mode. The simple LSB method seems to have a lack which is rectified with the proposed method Vacillating LSB in terms of the MSE and PSNR.

II. LITERATURE REVIEW

A. Secure Quantum Steganography Protocol for Fog Cloud Internet of Things: Ahmed a. abd el-latif et.a1 [3] the security of sensitive information is an urgent need in today's message, principally in cloud and Internet of Things (IoT) environments. Then a well-designed security device should be carefully considered. This paper presents a fresh framework for safe information in fog cloud IoT.

B. A New Audio Steganography with Enhanced Security based on Location Selection Scheme Sweat Vinayakarao Jadhav et.a1 [4] Data transmission in public communication system is not secure because of interception and improper manipulate ion by eavesdropper. There for eat active solution for this problem is Steganography, which is the painting and science of writing hidden communications in such a way that no one, separately from the sender and aim recipient, suspects the existence of the message, a form of security through obscurity.

C. Secure Image Hiding using algorithm IOT and LSB: Xinyi Zhou et.a1 [11] an developed LSB information hiding algorithm of color image by secret key is be future, combining information hiding and cryptography, increasing the

DOI 10.17148/IARJSET.2018.51011

human eye visual features, and the self-authentication based on digital signature and encryption technology to improve the security of information hiding. On the other hand, by by digital signature and encryption technology of cryptography, we can make the unauthorized users can not know the location of the embedded secret information.

D .Lightweight Noise Resilient Steganography Scheme for Internet of Things: Fatiha Djebbaret.a1 [9] now this paper, we address these issues by proposing a light-weight, noise-resilient, high payload audio steganography scheme capable of securing communication in IoT networks. The proposed technique is based on partial modification of well-selected phase frequencies leading to a smoother transition while preserving the phase continuity and the naturalness of the altered signal.

E. A Semantic IoT Early Warning System for Natural Environment Crisis Management: Stefan poled et.a1 [5] An early warning system (EWS) is a core type of data driven Internet of Things (IoTs) system used for environment disaster risk and effect management. The potential beneath of using a semantic-type EWS include easier sensor and data source plug-and-play, simpler, richer, and more dynamic metadata-driven data analysis and easier service interoperability and orchestration.

Table I: Summary of Literature Review

S. No	Title	Author, Publisher and Year	Working Platform	Objective	Future Scope
1	Secure Image Hiding using algorithm IOT and LSB	Nidhi Chawade et.a1[1] IEEE [2018]	Secure internet of things (SIT)	To save the information as of illegal user with provides better PSNR value.	Erich provide first-class quality of the image after encoding the original image by the LSB technique because LSB.
2	A New Audio Steganography with Enhanced Security based on Location Selection Scheme	Shweta Vinayakarao Jadhav et.a1[4] IEEE[2016]	Chaotic Encryption	Data transmission in public communication system is not secure because of interception and manipulation by Eavesdropper.	The secrete message will be embedded at selective positions within the audio carrier also we had used secret key to increase the security.
3	Secure Image Hiding using algorithm IOT and LSB	Nidhi Chawade Et.a1[3] IEEE [2018]	Computing Network, SIT	Two major techniques for secret communication In this paper we propose a lightweight encryption algorithm named as Secure internet of things (SIT).	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.
4	Lightweight Noise Resilient Steganography Scheme for Internet of Things	Fatiha Djebbar et.a1[9] IEEE [2007]	IOT network	Light-weight, noise resilient, high payload audio steganography scheme capable of securing communication in IoT networks.	Hides data in a cover-signal to generate a stego-signal which then modulated using$OFDM/QPSK$then sent on $AWGN$channel.
5	A Semantic IoT Early Warning System for Natural Environment Crisis Management	Stefan poslad et.a1[13] IEEE [2015]	Early warning system, W3CWeb Ontology Language	EWS include easier sensor and data source plug-and-play, simpler, richer, and more dynamic metadata-driven data analysis.	These potential applications include financial and banking systems, health and physiological signal acquisition and monitoring, and smart transport and utility management in smart cities.

DOI 10.17148/IARJSET.2018.51011

III. IDENTIFIED PROBLEM FROM EXISTING SYSTEM

Pervasive computing creates a significant impact in the information and commination. The growth rate of the devices seems to be hiked in exponential manner. The overall objective seems to be providing better services for the end user with the emergence of the new age gadgets. IoT is one such technology, which holds many promising aspects in networking and communication. In another perspective the nature of the data handled in the IoT is more open and vulnerable for hacking. Since the data handled through the IoT technology is sensitive and almost deals with personal privacy, industry needs to cater the security concerns in IoT.

A. Existing scenario

The selection of bits in the data hiding is the major part of the steganography process. The available scenario makes use of the static selection of bits. The fixed bit pattern is selected and the data will be hide on the predicted pattern. Mean while the space for the intruders is more obvious that they can interpret the data from the sensor pathway to the home network and manipulate the content if they have the uniform pattern. Hence the proposed method makes a vacillating method in the bit pattern selection.

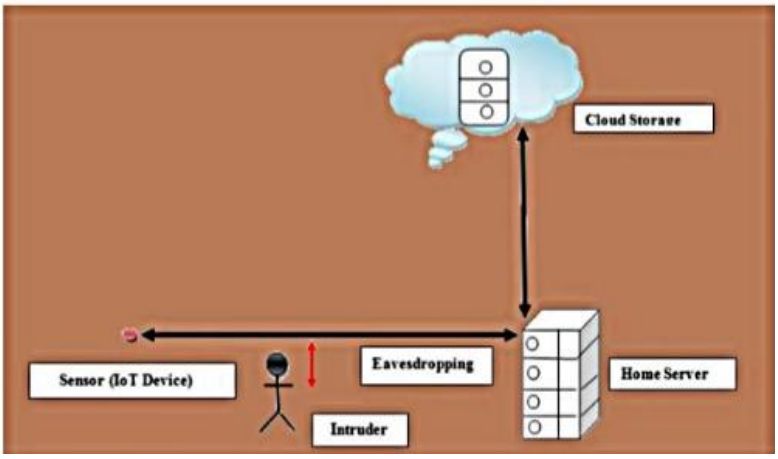
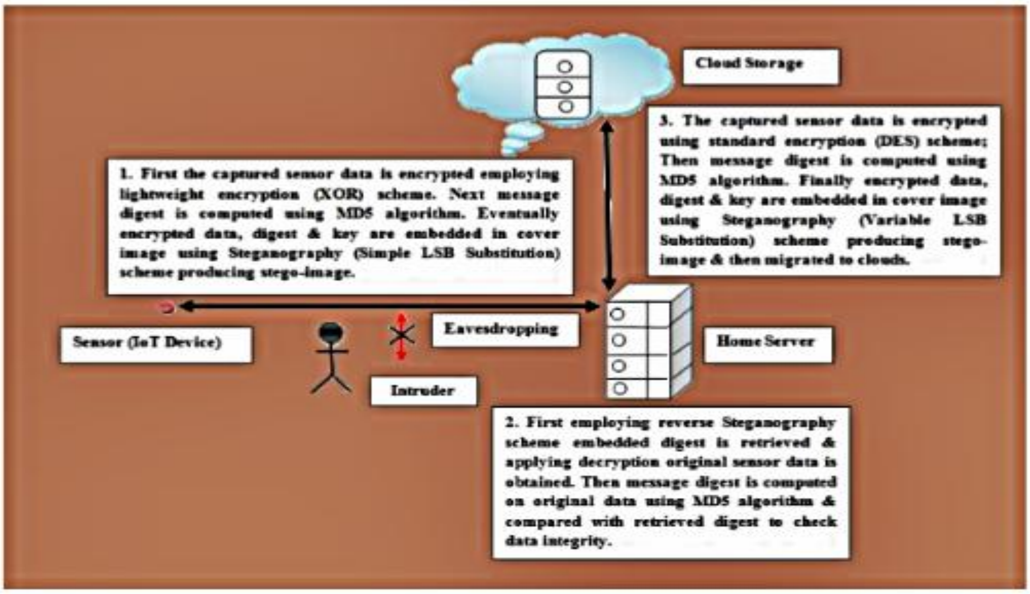


Figure 2: Existing scenario

IV. PROPOSED WORK: STEGANOGRAPHY SCHEME FOR INTERNET OF THINGS



1. First the captured sensor data is encrypted employing lightweight encryption (XOR) scheme. Next message digest is computed using MD5 algorithm. Eventually encrypted data, digest & key are embedded in cover image using Steganography (Simple LSB Substitution) scheme producing stego-image.

2. First employing reverse Steganography scheme embedded digest is retrieved & applying decryption original sensor data is obtained. Then message digest is computed on original data using MD5 algorithm & compared with retrieved digest to check data integrity.

3. The captured sensor data is encrypted using standard encryption (DES) scheme; Then message digest is computed using MD5 algorithm. Finally encrypted data, digest & key are embedded in cover image using Steganography (Variable LSB Substitution) scheme producing stego-image & then migrated to clouds.

Figure 2: Proposed Method

This research proposes a technique, which can hide the secret data in image layers, and steganography for IoT. The proposed strategy is LSB substitution ciphers for the IoT. Experiments are conducted with different aspect ratio images, which show that the proposed algorithms seem to work better. IoT seems to rule the world for the next decade. The

DOI 10.17148/IARJSET.2018.51011

diverse natre of the IoT technology leads to much more security breaches. This research provides an enhanced novel strategy to secure the information using steganography. This research addresses the quality of the image as aconcern. Addressing high quality images and images with huge compression ratio would be the further enhancements added for the research.

V. THE LEAST SIGNIFICANT BIT ALGORITHMS

A. Least Significant Bits

A simple approach for embedding information in cover image is using least significant bit .The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover image in a deterministic sequence . Modulating the least significant bit does not result in human perceptible different because the amplitude of the change is small.
00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
When the character A, Which binary value equals 10000001, is inserted the following gird results:
(0010011**1** 1110100**0** 1100100**0**)
(0010011**0** 1100100**0** 1110100**0**)
(1100100**0** 0010011**1** 1110100**1**)

B. Least Significant Bit algorithm

1. The pixels selected for the embedding of the secure data through the hashing algorithm.
2. The hash key generated would be having an index
3. The bit position changing would help in prevention and counter attacks and reply orca knowledgement of the intruders to concern privacy protectors.
4. The random selection of bits helps much more in protection of data
5. The proposed method address the RGB or grey scale image hidden within another image
6. The rows and column values are extracted
7. If it is RGB extract any on channel
8. Get rows and column values of the mage to be hide and map the data

VI. IMAGE ENCODING TECHNIQUES

Information can be hidden a lot of different ways in images. Straight message insertion be able to be done, which will simply encode every bit of information in the image. More complex encoding can be done to embed the message only in ``noisy" areas of the image, that will attract less attention. The message may also be scattered randomly throughout the cover image.

The most common approaches to information hiding in images are,

- Least significant bit (LSB) insertion
- Masking and filtering techniques
- Algorithms and transformations

A. Security Concerns in IoT
IoT is one such technology, which holds many promising aspects in networking and communication. In another perspective the nature of the data handled in the IoT is more open and vulnerable for hacking. Since the data handled through the IoT technology is sensitive and almost deals with personal privacy, industry needs to cater the security concerns in IoT.

CONCLUSION

This research proposes a technique, which can hide the secret data in image layers, and steganography for IoT. The proposed strategy is LSB substitution ciphers for the IoT. Experiments are conducted with different aspect ratio images, which show that the proposed algorithms seem to work better. The proposed method performs well in specifically in RGB mode. The simple LSB method seems to have a lack which is rectified with the proposed method Vacillating LSB in terms of the MSE and PSNR.

DOI 10.17148/IARJSET.2018.51011

FUTURE WORK

IoT seems to rule the world for the next decade. The diverse nature of the IoT technology leads to much more security breaches. This research provides an enhanced novel strategy to secure the information using steganography. This research addresses the quality of the image as concern. Addressing high quality images and images with huge compression ratio would be the further enhancements added for the research.

REFERENCES

[1]. Wojciech Mazurczyk and Luca Caviglione "Steganography in Modern Smartphone and Mitigation Techniques" steganography in modern Smartphone and mitigation techniques communication surveys & tutorials, vol. 17, 2015 on 334 -357 IEEE, 2015.

[2]. Shweta Vinayakarao Jadhav "A New Audio Steganography with Enhanced Security based on Location Selection Scheme"International Journal of Engineering Science and Computing, August 2016 on 2280 -2283 IEEE 2016.

[3]. Amitava Nag "An Image Steganography Scheme based on LSB++ and RHTF for Resisting Statistical Steganalysis" Transactions on Smart Processing and Computing, vol. 5, no. 4, August 2016 on 250 – 255 IEEE 2106.

[4]. A.m.negrat & A.kumar "Secure steganography for audio signals" new aspects of signal processing, computational geometry and artificial vision Steganography, Cryptography, RSA and pseudorandom 1792-4618 IEEE 2001.

[5]. Nidhi Chawade*, Priya Bisen , Ankita Makde, Priyanka Kawale "Secure Image Hiding using algorithm IOT and LSB" International Journal of Scientific Research in Science, Engineering and Technology (ijsrset.com) 2018 IJSRSET | Volume 4 | Issue 4 | Print ISSN: 2395-1990" IEEE 2018.

BIBLIOGRAPHIES

Dr. S. Prema, currently working as an Associate Professor in K.S.R. College of Arts & Science has received Ph.D., from the Bharathiar University in 2015. She has been involved in the teaching for the past 13 years. She secured the 1st Rank in B.Sc under Periyar University, Salem. She has totally 52 publications and one of her research paper entitled "An NLP based Approach for Facilitating Efficient Web Search Results using BSDS" received the **best paper award**. Her papers are cited at various publications (IEEE Xplore, Elsevier, Springer and International Conference Proceedings). She has h-index value: 5, i-10 index: 3, Citations: 125 and her profile is listed in Marquis Who is Who in World, International Biography Center, London, UK, 2011.She has been awarded "Innovative Research & Dedicated Women Academician Award" at International Awards & Honors Convocation 2018 Conducted by The Society of Innovative Educationalist & Scientific Research Professional, Malaysia. She has produced 5 M.Phil scholars and currently guiding 4 M.Phil and 1 Ph.D Scholars for doing their research. She has been involved in generating funds for R&D.

Mr. Manikandan.C is pursuing M.Phil (Computer Science) in K.S.Rangasamy College of Arts and Science (Autonomous), Tamilnadu, India. He has attented 5 workshops related to Network and 5 Seminar related to Network. His areas of interest are Network, Data Structure.

DOI 10.17148/IARJSET.2018.51011