International Journal of Engineering & Technology, 7 (2.7) (2018) 433-435

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Optimized and secured data collection and recovery for IoT applications

M. Tanooj Kumar, T. Praveena, T. Lakshman, M. Sai Krishna

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India
**Corresponding author Email: praveena.chinni97@gmail.com*

Abstract

This paper proposes a new compressive sensing based method for data collection and recovery related to IoT based systems. It performs data capturing, its compression and encryption at the same time, transmission, storage and its recovery. The measurement matrix, used in compressive sensing, is generated based on the user private key and is utilized for encrypting the captured data. Basis Pursuit is used for reconstruction of the data. The results shows that it is very suitable for the IoT based applications by considering data security, transmission cost and storage cost.

Keywords*:* Basis Pursuit; Compressive sensing; Internet of Things (IoT); Measurement matrix;

1. Introduction

The style from these instructions will adjust your fonts and line spacing. Please do not change the font sizes or line spacing to squeeze more text into a limited number of pages . Compressed sensing (CS) is a developing field which has allured considerable research fascination from the last couple of years. Compressed sensing (also called as compressive sampling) is a technique used in signal processing for effective obtaining and restoring a signal, by detecting solutions for indecipherable linear systems. We use compressed sensing for securing data through cryptographic techniques. It enables us to perform signal catching, size minimization and encryption simultaneously. The resultant matrix obtained is used as a private user key and is treated for performing encryption. Conventionally, signals carried through a public medium are first received and compressed by minimizing the size and encrypted so that an intruder is not able to reveal the actual information i.e., even when attacked actual information cannot be obtained. In contrary, compressed sensing consists of three steps which are data capturing, size minimization and encryption simultaneously. In this case, the resultant matrix is obtained with the help of a key. Traditional cryptographic techniques are not fitting for encoding the images, due to big unwanted blocks in images. Any signals received are inspected and then compression is done so that the size is minimized. Next, this data is encoded using a user’s private key and sent by a transmission medium to the destination. At destination, decryption of the text is carried out using the user’s private key used for encryption by the sender. We will concentrate on the feasibility of using compressed sensing as a cryptographic technique. Resultant matrix is obtained based on the user’s private key and encryption is carried out. We carry out this technique for the voice to text conversion systems data storage and its processing.

2. Background

IOT (Internet of Things) has many techniques for encryption and enormous number of applications. But according to our survey Compressed sensing is a technique that is generally not associated with IOT until recent days. In modern times, compressed sensing (CS) has captured noticeable attention in applied mathematics, electrical engineering and computer science, by predicting that it can be viable to exceed the conventional limits of the theory of sampling. Compressed Sensing is build on the rudimentary fact that we can foretell signals by utilizing only fewer coefficients that are non-zero in a acceptable dictionary. Then, the Nonlinear optimization is ability of recovering signals with fewer measurements.

Compressed sensing is a way to deal with signal processing which performs restoring of the signals and images with minimum sampling rates. This makes signal processing and restoring significantly less complex and has a wide assortment of utilizations in reality, including photography, holography and facial acknowledgment. Compressed sensing is otherwise called compressive sensing, compressive sampling and sparse sampling. The developing compressed sensing techniques can hypothetically diminish the number of samplings indicates that directly indicates the volume of information gathered, which implies that part of the redundant information is never obtained. It makes it feasible to create independent and net-driven applications with a handful of resources in Internet of Things (IOT).

The most ideal approach to describe Compressed sensing is in layman's terms ,i.e., to utilize the case of group experimenting(testing). Envision you have a flawed object set among an extensive arrangement of many related yet non-defective objects. You also likewise have a sensor that could identify whether any object is imperfect yet keeping in mind the end goal to discover which one it is, you'd need to execute the same number of estimations as there are things in the full (and vast) set. Envision now the likelihood of performing estimations on groupings of things: Instead of calculating one thing at any given moment, one gauges a few things at any given moment and acquire single estimation for each gathering being measured. Compressed sensing gives you methods for outlining what these groupings are, i.e. you get the opportunity to have leads on the most proficient methods to combine the distinctive things in various groupings. Utilizing strategies created in Compressed sensing, the quantity of estimations expected to locate that one inadequate thing is currently substantially less if you were measuring entire object set, each one in turn. This is the reason the articulation has "Compressed" or "compressive" in it. "Sensing" alludes to the demonstration of measuring these grouping of things. Compressed Sensing is an evolving concept in Internet of Things. By this technique we can establish Compressed Sensing as a cryptography technique.

The word encryption is originated from the Greek word kryptos, which means covered up. The usage of encryption is almost as historic as the specialty of correspondence itself. In 1900 BC, just writing a message was enough, when most people couldn't read, but encryption techniques soon developed to convert messages into unreadable and un-understandable grouping of figures to assure the message's security while it was carried out starting from one place to another. In present days providing security for data that is to be stored or transmitted is very important. The Encryption technique is used for converting a simple plain text into cipher text by using a key. This cipher text to be understood should be decrypted, which is possible only if key is known. So, it prevents the data from third-party attacks.

The encryption technique’s key role is to assure privacy of the data stored on PC or carried on through the Internet or other PC’s. The most progressive encrypting systems are required to give confidentiality, and assisting key elements of security.

Authentication: To provide access to only authorised users.

Integrity: the source of a message can be known.

Non-repudiation: the sender of a message can't contradict sending it.

Encryption is utilized to guard the information that is transmitted from a wide ranging of appliances over a vast range of system networks. Every time someone utilizes a cash machine for purchasing something on the internet through a mobile phone ,it influences the mobile to call or presses a key to unlock a car, encryption is brought to play to ensure the security of the data being handed-off. There are many security concerns and threats that we are facing in IOT such as Multi-tenancy, Denial of services, Velocity of attack, Data privacy, Information Assurance etc.

Sparsity relates to frameworks which are closely coupled. Sparsity in compressed sensing is used for checking if the given matrix is a sparse or a dense matrix. Sparse matrix is a framework in which the vast majority of the components are zero. On the other hand, if the vast majority of the components are non-zero, at that point the matrix is viewed as dense. To compress a given matrix, the matrix should be a sparse matrix. If not i.e., on the off chance that there is total number of zeros is less than the non-zero components then it is known as a dense matrix. If the given matrix is a dense matrix, then it is to be converted into a sparse matrix by adding zeroes.

3.Proposed Method

The proposed method is shown in Algorithm1.

```
Algorithm1 : CS based Encryption
Input : File selected
Output : File Uploaded
Begin cs-based-encryption
Generate Sparse matrix (of the file selected) of order 1 x i
Generate measurement matrix of order i x j based on user key
Multiply measurement matrix with spare matrix with measurement matrix
Generate the measurement vector and upload it
end
```

The Proposed method is tested on the message received. To encrypt a message, we use extended ASCII code to illustrate the data as a 8-digit binary number. The binary code sequence sets a sparse vector so that we can encode it utilizing compressed sensing.

Let us consider a voice signal and the message given is,

SWITCH ON FAN

Now, the message converted into the binary format is shown below:

S	W	I	T	C	H	
1000 0011	1000 0111	0111 0011	1000 0100	0110 0111	0111 0010	0011 0010

Matrix : [10000011 10000111 01110011 10000100 01110010 00110010 00110010 01111001 01111000 00110010 01110000 01100101 01111000 00110010]

O	N		F	A	N	
0111 1001	0111 1000	0011 0010	0111 0000	0110 0101	0111 1000	0011 0010

The obtained binary numbers are considered in a 1*i matrix form. This matrix is the plain text and to encrypt and get a cipher text we need a key. To generate a key, we generate random numbers using gaussian random number generator. The chaotic pseudo random number generator enables you to create random numbers based on the private key chosen by the user. This generated number series is written in the form of a i*j matrix, such that m is less than n (i<j). Now by performing the encryption

i.e., **(plain-text)*key = cipher-text.**

[1*i]*[i*j] = [1*j]

The obtained 1*j matrix is the resultant matrix after encryption is done. By using this technique the dimensionality of the matrix is reduced from i to j, where (j << i). For the reconstruction of the original plain text, Basis Pursuit (BP) algorithm is used and successfully recovered.

4. Conclusion

This paper presents a possibility of using compressed sensing for simultaneous compression and encryption in IoT based applications. The user’s private key is used to generate the measurement matrix. In turn, it is used to reduce the dimensionality of the cipher text compared with plain text. So, we can say that Simultaneous Encryption with Compression is done and this method can provide good security and compression performance.

References

[1] ENCRYPTION OF MESSAGES AND IMAGES USING COMPRESSED SENSING by Marie Dankova.

[2] Compressed Sensing for IOT Application by Mayur Mhaske, Sayali Shelke,Bhakti Kulkarni, Ravindra Salunke, Dept. of Information Technology, Sinhgad Institute of Technology & Science.

[3] Structured Compressed Sensing From Theory to Applications By Marco F. Duarte, *Member, IEEE*, and Yonina C. Eldar, *Senior Member, IEEE.*

[4] D. L. Donoho, “Compressed sensing,” *IEEE Trans. Inf. Theory*, vol.52, no. 4, pp. 1289–1306, Sep. 2006.

[5] R. G. Baraniuk, “Compressive sensing,” *IEEE Signal Process. Mag.*,vol. 24, no. 4, pp. 118–120, 124, Jul. 2007.

[6] Candes, E. J.; Wakin, M. B.: An introduction to compressive sampling. Signal Processing Magazine, IEEE, vol.25, no.2, pp.21,30, March 2008, doi: 10.1109/MSP.2007.914731.

[7] Sreedhanya, A.V.; Soman, K. P.: Secrecy of Cryptography with Compressed Sensing. 2012 International Conference on Advances in Computing and Communications. IEEE, 2012, p. 207-210. DOI: 10.1109/ICACC.2012.48.

[8] M.Tanooj Kumar, Dr.M.Babu Reddy, compressive sensing based simultaneous data compression and convergent encryption for secure deduplication, International Journal of computer science and Information security, Vol. 15,No. 9.,2017, pp 144-147.

[9] Mayiami, M. R.; Seyfe, B.; Bafghi; H. G.: Perfect Secrecy via Compressed Sensing. Communication and Information Theory (IWCIT), 2013 Iran Workshop on , vol., no., pp.1,5, 8-9 May2013. doi: 10.1109/IWCIT.2013.6555751/

[10] Orsdemir, A.; Altun, H. O.; Sharma, G.; Bocko, M. F.: On the Security and Robustness Encryption via Compressed Sensing. MILCOM 2008-2008 IEEE Military Comm Conference. 2008. DOI: 10.1109/milcom.2008.4753187.

[11] Sreedhanya , A.V.; Soman , K. P.: Secrecy of Cryptography with Compressed Sensing. 2012 International Conference on Advances in Computing and Communications. IEEE, 2012, p. 207-210. DOI: 10.1109/ICACC.2012.48.

[12] ANNABATTULA, J., KOTESWARA RAO, S., SAMPATH DAKSHINA MURTHY, A., SRIKANTH, K.S. and DAS, R.P., 2015. Underwater passive target tracking in constrained environment. Indian Journal of Science and Technology, 8(35), pp. 1-4.

[13] HUSSAIN, S.N. and KISHORE, K.H., 2016. Computational Optimization of Placement and Routing using Genetic Algorithm. Indian Journal of Science and Technology, 9(47),.

[14] Vudatha, C.P., Nalliboena, S., Jammalamadaka, S.K.R., Duvvuri, B.K.K., Reddy, L.S.S., Automated generation of test cases from output domain of an embedded system using Genetic algorithms, ICECT 2011 - 2011 3rd International Conference on Electronics Computer Technology 5,5941989, pp. 216-220

[15] Sastry, J.K.R., Suresh, A., Bhanu, S.J., Building heterogeneous distributed embedded systems through rs485 communication protocol, ARPN Journal of Engineering and Applied Sciences, 2015, 10(16), pp. 6793-6803