International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 06 | June 2019 www.irjet.net p-ISSN: 2395-0072

Enhanced Security using DNA Cryptography

Aishwarya R U[1], Dr. M N Sreerangaraju[2]

[1]Student, Electronics and Communication Department
[2]Professor, Electronics and Communication Department, Bangalore Institute of Technology, V.V Puram, Bengaluru-560004, India

---

Abstract - *This paper proposes a secure and lightweight compressive sensing of stream cipher based on DNA encoding and decoding method. This method encrypts text and data generated by image sensors. The proposed method combines the compressive sensing technique with DNA encoding and decodin g based stream cipher to implement the secure compressive sensing. To have the security objective, the overhead should be minimal which is achieved by using of stream cipher for generating the measurement matrix. The proposed system is implemented using Verilog HDL and simulated using Modelsim 6.4 c and synthesized using Xilinx tool.*

Key Words: *DNA encoding and decoding, compressive sensing, stream cipher.*

1. INTRODUCTION

The continuous rapid progress in the innovation of the electronics and telecommunication industry has spread throughout leading to sensor-infested smart infrastructures. Due to the growth in smart sensors and other devices the bandwidth for communication and storage is becoming a scarce resource and moreover communication of secured and private information over the channels can raise the possibility of the security. Therefore security of sensory data is a challenging concern.

To combat these problems, Cryptographic systems are being used where the process of cryptography involves processing of plain text information using a key to form a cipher text and decrypting the cipher text to get back the original plain text where third party will not be having any knowledge of the key being used for cryptography process.

Compressive Sensing (CS) is an emerging technology in the signal processing technology for efficiently acquiring and reconstructing a signal, by finding solutions to underdetermined linear systems. The principle on which it is based is through the optimization of the signal [1]. It is the method of compressing the signals with the help of fewer resources.

The compressive sensing uses a measurement matrix called φ-matrix [3] which is used for compressing the original signal. This matrix is considered to be the secret key as it is known only known to the sender and recipient which is used for encrypting and compressing the signals or images.

Stream cipher is a type of symmetric encryption and decryption algorithm. Stream ciphers are much faster than any block cipher. The encryption and decryption of plaintext with a stream cipher will result in the same when the same key is used.

In this paper, we propose a new technique for secure encryption and decryption by combining both stream cipher and compressive sensing. Firstly, the paper discuss about the measurement matrix used for compressive sensing. Secondly, LFSR method [2] along with stream cipher is being used to generate the above matrix. Third, the same stream cipher is used for performing the encryption process.

2. STREAM CIPHER

Stream ciphers are symmetric-key ciphers. In this cipher, the plain text is encrypted along with the corresponding key-stream digit, one at a time to obtain the corresponding one digit cipher text stream. As the each digit obtained from the encryption depends on the current state of the cipher, this cipher is also known as state cipher. The cipher text is obtained by XOR- ing the individual bit of the key-stream with the input message bits.

Stream ciphers executes at a faster rate when compared to block ciphers. These ciphers have lower hardware complexity. As these ciphers have lower resource requirements and due to the faster operations, stream ciphers are preferred as lightweight cryptographic primitive over block ciphers. The block diagram of stream cipher encryption is as shown in Fig 1.

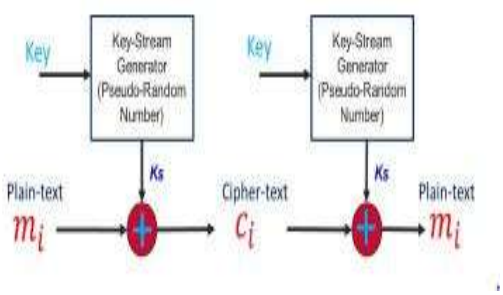

Fig 1: Stream Cipher Encryption and Decryption

3. COMPRESSIVE SENSING ARCHITECTURE

Compressive Sensing (CS) is a signal processing technique for effectively acquiring and reconstruction of signals using fewer resources. The secure compressive sensing is done by implementation of CS encoder using the stream cipher based φ-matrix which is referred to as CS using Stream Cipher (CSSC).

The proposed architecture of CSSC based on φ-matrix is as shown in Fig 2. The numbers of adders/ subtractors used are based on accumulators used in the system. The X_i is subtracted from the previous accumulator value Y_1^{i-1} if φ_1(i) =1 otherwise X_i is added to the previous value. The accumulator is implemented using only added with input carry and XOR gates as defined by the Eq. (1).

$$Y_1^i = Y_1^{i-1} + \varphi_1(i) \oplus X_i + \varphi_1(i) \quad (1)$$

Firstly, the stream cipher generates the one column of φ- matrix. Then to the accumulator each input signal X_i is taken at a time and it subtracts or adds from the previous accumulator value depending on the φ-matrix elements. This process continues till the completion of the whole block of the input data being processed.

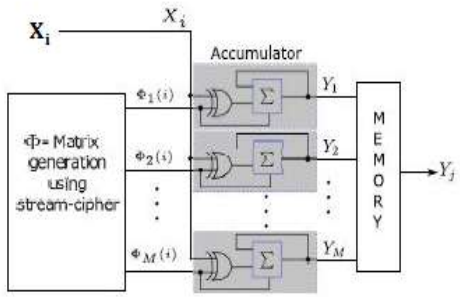

Fig 2. Proposed Architecture of Compressive Sensing with Stream Cipher based φ-matrix

To generate a random sequence, stream cipher requires a secret key. Without the use of same secret key, the reconstructed data generated from the φ-matrix will not be same as that of the original data. Therefore, for the synchronous stream cipher same key should be used for both encryption and decryption.

4. DNA ENCODING AND DECODING

DNA (Deoxy ribo Nucleic Acid) cryptography is the process of hiding data in terms of DNA sequence. DNA has a great cryptographic strength and its binding properties between its nucleotide bases offer the possibility of create a self-assembly structures which are the effective means of executing parallel molecular computations.

DNA has many properties like vast parallelism, exceptional energy storage capability. There are four classes of nucleotides, Adenine, Guanine, and Cytosine, Thymine (A, C, G, and T). These nucleotides are stranded into polymer chains (DNA strands). DNA is basically used to store genetic information. This information cannot be duplicated or copied. The advantages of DNA computing are: it has faster speed of computation, minimal storage requirements and minimal power requirements.

In the proposed system, the user gives the key input for the generation of key to encrypt and decrypt the information. And then the key is represented using the DNA bases format using lookup table (Table 1). These bases representation will become the cipher text. To decode this cipher text, the eavesdropper must have access to lookup table and the key which is stored in the DNA bases, which is more or less impossible. The cipher text is now secured and can securely transmit over any channel. At the receiver side, key which is known to the receiver and along with the lookup table, the cipher text is decrypted to its original text. The block diagram for the DNA cryptography process is shown in Fig 3.

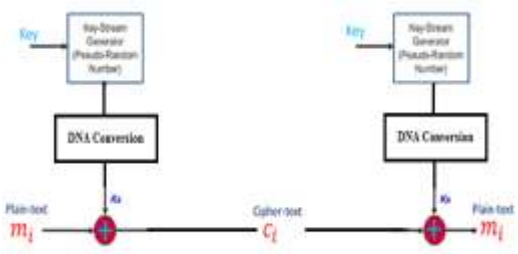

Fig 3: DNA Encoding and Decoding

5. PROPOSED SYSTEM

The proposed method for secure encryption using the combination of stream cipher and compressive sensing. Firstly, the properties of measurement matrix used in the CS are being studied. Secondly, LFSR-based stream cipher is used to generate measurement matrix. Third, we reuse the stream cipher for performing encryption.

Lastly the system is extended for the encryption of data using DNA cryptography. The DNA encryption starts with the message that contains alphabets, numerals and some special characters. The key which is used for encryption is being changed to DNA base triplets and this triplet key is XOR-ed with the input bit to get the cipher text and is send to the receiver over a public channel. This cipher text will be the input to the decryption process which is simply the reverse of encryption. For the decryption, the same key is used and with the lookup table, the cipher is decoded and original data is obtained.

Table 1: Triplet code table for DNA encryption and Decryption

A=CGA	K=AAG	U=CTG	0=ACT
B=CCA	L=TGC	V=CCT	1=ACC
C=GTT	M=TCC	W=CCG	2=TAG
D=TTG	N=TCT	X=CTA	3=GCA
E=GGC	O=GGA	Y=AAA	4=GAG
F=GGT	P=GTG	Z=CTT	5=AGA
G=TTT	Q=AAC	=ATA	6=TTA
H=CGC	R=TCA	,=GAT	7=ACA
I=ATG	S=ACG	.=GAT	8=AGG
J-AGT	T=TTC	;=GCT	9=GCG

6. RESULTS AND DISCUSSIONS

The output for the CSSC based φ-matrix is as shown in the Fig 4. The waveform of input which is used for the encryption and the corresponding output is shown in the Fig 4.

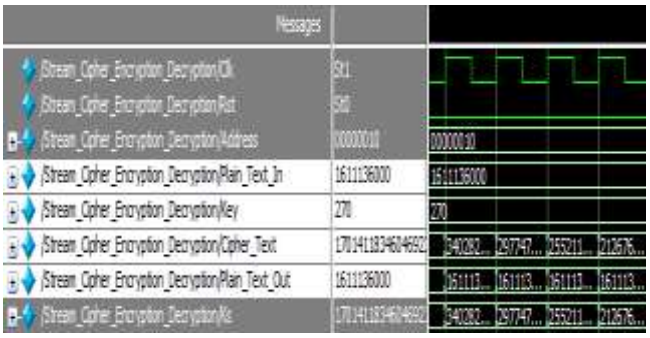

Fig 4. Output for CSSC Encryption and Decryption

A specific waveform for the DNA encrypted key will be generated due to a user DNA key and the following figure (Fig 5) illustrates the same.

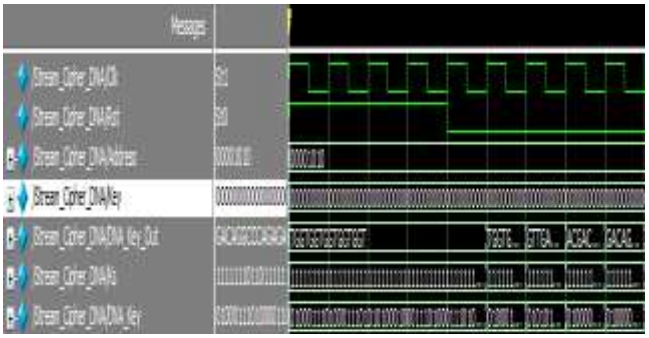

Fig 5. Output for DNA key generation

The output waveform for the DNA Cryptography is as shown in the Fig 6. Here in this output, the DNA triplet for each character is shown as per the encoding table and also the encrypted and decrypted data is also shown.

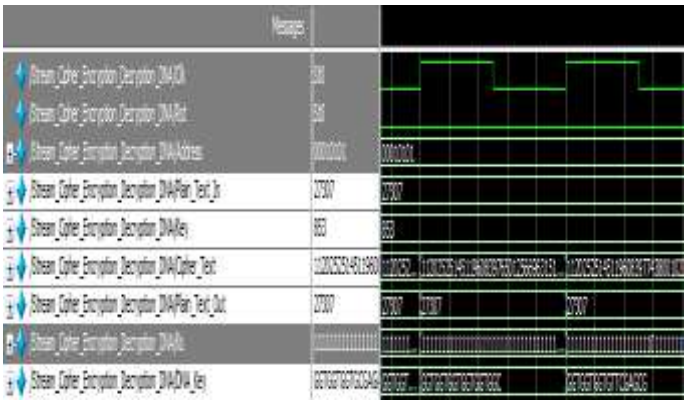

Fig 6. Output for DNA Encoding and Decoding

7. CONCLUSION

In this paper, the idea of compressive sensing of stream cipher using DNA cryptography for 128-bit text is proposed. As the LFSR method used for the generation of stream cipher does not provide confidentiality of the data. Therefore the proposed method of DNA cryptography provides data security and faster speed of operation. The applications of our proposed method includes, among others, real-time monitoring systems, secure transmission of medical data (like ECG signals, MR images), traffic videos, environmental monitoring, Unmanned Arial Vehicles (UAVs) and IoT sensors.

REFERENCES

[1] N. Zhou, A. Zhang, F. Zheng, and L. Gong, "Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing," *Opt. Laser Technol.,* vol. 62, pp. 152–160, Oct. 2014.

[2] R. Dautov and G. R. Tsouri, "Establishing secure measurement matrix for compressed sensing using wireless physical layer security," in *Proc.Int. Conf. Comput. Netw. Commun. (ICNC),* San Diego, CA, USA, 2013, pp. 354–358.

[3] G. Zhang, S. Jiao, X. Xu, and L. Wang, "Compressed sensing and reconstruction with Bernoulli matrices," in *Proc. IEEE Int. Conf. Inf. Autom. (ICIA),* Harbin, China, 2010, pp. 455–460.