Chaotic Encryption Scheme using 3D Multi Scroll Hyperbolic Functions for IoT Applications

G. Gugapriya, B. Lakshmi

Abstract: With the advent of Internet of Things (IoT), security breaches increases day by day which remain the major threat for an effective data communication. Nearly 14.4 million devices will be interconnected with each other by 2022, cyber -security threats will be the real challenge among the developers and researchers. In this paper, an effective framework for chaotic encryption based on 3D multi scroll hyperbolic functions are presented together with the dynamic quad tier architecture and electroencephalogram (EEG) signals. The dynamic characteristics of EEG signals and MAC parameters make the proposed system more suitable for the transmission of an effective data transmission. The test bed has been developed using Raspberry Pi 3 -Cortex A-7 Quad Core architectures and the performance of the proposed architecture has been evaluated on the above test bed. Furthermore, experimental implementation and result analysis shows that the proposed architecture can provide more secure and high confidential data transmission.

Index Terms: EEG, Internet of Things, Multi Scroll, Hyperbolic Functions, Received Signal Strength Indicator (RSSI).

I. INTRODUCTION

Data encryption methods which uses symmetric key encryption uses confusion or/and diffusion processes. For achieving better encryption quality, substitution techniques are used in many literatures. But these methods are not more reliable for the secured data transmission in an IoT environment. Chaos based data encryption methods are emerging rapidly as they are very sensitive to initial conditions and are having high degree of randomness. Based on the iterative chaotic map with infinite collapse (ICMIC), a fast image encryption algorithm was proposed in [1].

To promote the efficiency of the permutation-diffusion type X. Huang proposed an efficient self-adaptive model for chaotic image encryption algorithm [2]. A. Kanso used a 3D chaotic map to design a novel image encryption algorithm [3]. To reduce the transmission burden and to overcome the security risk, N. Zhou proposed an efficient image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing[4].Various image encryption algorithms are proposed in the literature [5]-[8]. A novel image encryption scheme based on reversible cellular automata (RCA) combining chaos is also reported [9]. A chaotic image encryption scheme based on permutation and one round of XOR operation is explored [10].Various hyperchaotic systems are used to generate secret keys for providing better encryption scheme.[11]-[14]. A novel image encryption scheme combining chaotic system, DNA sequence operations, and SHA 256 hash is discussed [15].

After the detailed study, major problems in achieving the secured data transfer are fixed key generation, permutation only structures, low security and key dependent. The proposed methodology overcomes the above mentioned drawbacks and by integrating the 3D multi scroll chaotic functions as described in by introducing a hyperbolic function in state 3 and integration of the EEG signals to generate the initial conditions [16].

The rest of the paper is organized as follows: Section-II deals with the proposed architecture for data encryption systems which includes 3D multi scroll chaotic system. Validation analysis and comparative analysis are presented in Section III and IV respectively. Finally the conclusion is given in Section-V.

II. PROPOSED ARCHITECTURE FOR DATA ENCRYPTION SYSTEMS

To solve the shortcomings of the fixed key encryptions, proposed architecture does not use the keys which are generated by the sender and receiver. The proposed architecture integrates the EEG signals of the person to generate the initial conditions of the proposed chaotic systems. This proposed methodology produces the most efficient random keys with the integration of EEG signals. Also to increase in the strength of the encryption, proposed architecture also implements the XOR permutation with the dynamic MAC parameters such as the Received Signal Strength Indicator (RSSI), distance and channel ID and integrates the diffusion mechanism between the data and cipher keys. The proposed algorithm has been integrated in the Raspberry pi 3 in an IoT environment to test the sensitivity of the proposed algorithm.

After getting the input data from IoT Sensor node, the input data streams are divided into eight bytes length which is scaled in accordance with the application. Then 3D multiscroll chaotic system is implemented. Initial conditions are determined using the EEG signal with travelling filters.

Manuscript published on 30 June 2019.
***** Correspondence Author (s)

G. Gugapriya, School of Electronics Engineering, VIT Chennai, India.
B. Lakshmi, School of Electronics Engineering, VIT Chennai, India.

The next step is the determination of MAC parameters such as RSSI, distance and channel ID.'G' vector is formulated by 3D multiscroll systems with EEG based initial conditions. New complex key is formed by doing XOR operation of the obtained G vector with MAC parameters. Data is re-arranged as data matrix d (i) and G matrix which is scaled to up to 256. Finally the diffusion process is performed between the odd selected key and data along with the constant β which is given in equation (3).

The following subsection discusses the implementation of 3D multi scroll chaotic system, generation of initial conditions from EEG, data encryption and diffusion process.

A. 3D Multi scroll Chaotic System

Dynamical systems with multiscroll attractors have more complex dynamics than general chaotic systems with mono-scroll attractors. An autonomous chaotic system is modified by adding p1tanh (y+g) in the third state which is given in Eqn. 1[16].

$$\dot{x} = -ax + byz$$
$$\dot{y}=-cy3+dxz \qquad (1)$$
$$\dot{z} = ez- fxy + p1\tanh (y+g)$$

Initial conditions are randomly chosen as 0.1, 0.1, and 0.6. From the chaotic system given in Eqn(1). a, b, c, d, e, f, p1 and g are the parameters whose values are 2, 6, 6, 3, 3, 1, 1 and 2 respectively which is already discussed [16] . By varying the value of 'g' different scrolls can be obtained. The next step is the generation of EEG signals using the EEG LAB open source software on MATLAB platform.

B. Generation of Initial Conditions

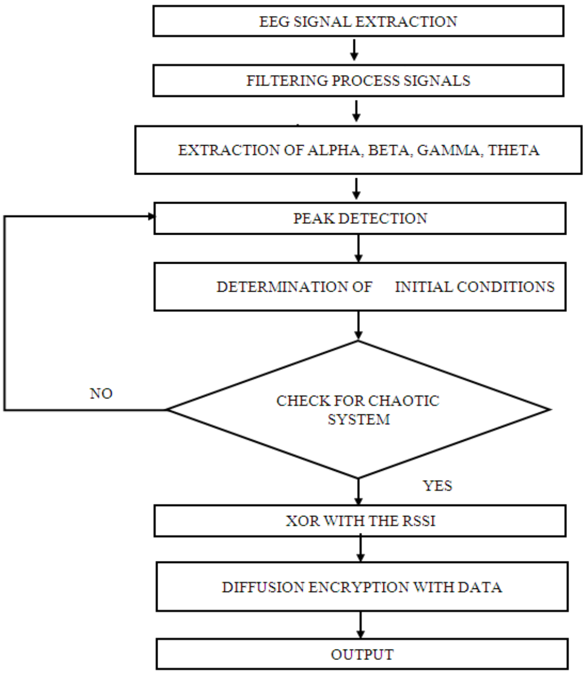
EEG SIGNAL EXTRACTION
FILTERING PROCESS SIGNALS
EXTRACTION OF ALPHA, BETA, GAMMA, THETA
PEAK DETECTION
DETERMINATION OF INITIAL CONDITIONS
CHECK FOR CHAOTIC SYSTEM
NO
YES
XOR WITH THE RSSI
DIFFUSION ENCRYPTION WITH DATA
OUTPUT

Figure 1 Flow chart for the Overall Encryption Process

Figure 1 shows the overall proposed encryption process. EEG signals are the most complex and non-linear signals which are used to analyze the different parts of the human brain. Since the human body is the most complex machine in the world, extraction of EEG signals is used to generate the initial conditions of chaotic systems, thereby the problem of fixed key encryption can be fixed. As the EEG signals have time-varying and non-deterministic property, it can lead to the most complex pseudo generators in the encryption process. EEGLAB 1.15.3 version which works on the MATLAB V2018 is used for the generation of the EEG Signals with the different iterations. EEGLAB consists of data sets which are extracted using 32 electrodes placed on human head. These EEG signals are integrated in the 3D multi scroll system to generate the chaotic system.

The extraction of the EEG signals are shown in Figure 2.The different features from the EEG signals such as alpha (8Hz < f < 12Hz), beta (12Hz < f < 30Hz) and gamma (30Hz < f) bands were extracted using the travelling filter using the different combinations of the notch filters. The spike detection methodology is used for the final extractions of integers from the EEG signal frequencies. These integers were used as the initial conditions for the above mentioned chaotic systems.

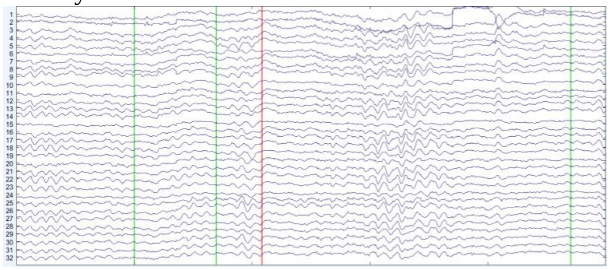

Figure 2 Generation of EEG Signals using the EEG LAB open source software on MATLAB Platform

Extraction of constant values from the EEG signals using the travelling filters and peak detection mechanism, are shown in Figure 3 and initial conditions are formulated by using the above mentioned values and phase portraits of 3D multi scroll chaotic system has been analyzed with EEG initial conditions which are given in Figure 4

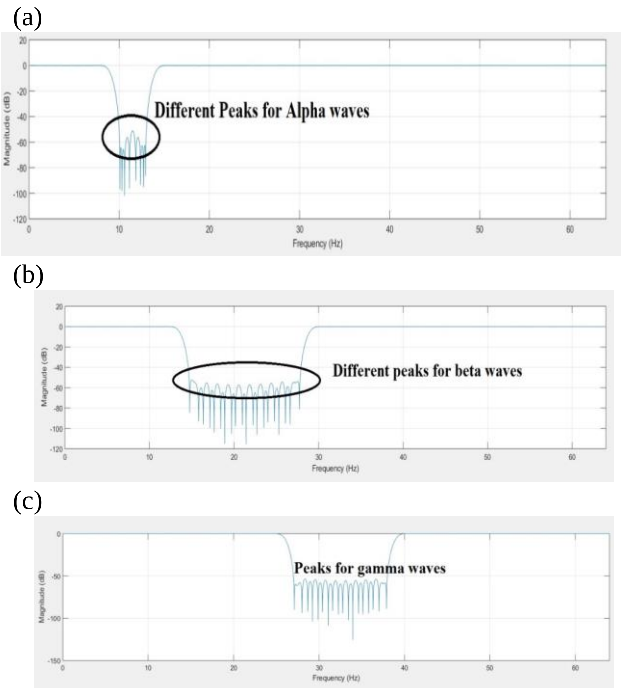

Figure 3 (a) to (c) extraction of alpha, beta, delta waves using the travelling filters along with threshold peak detection mechanism.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

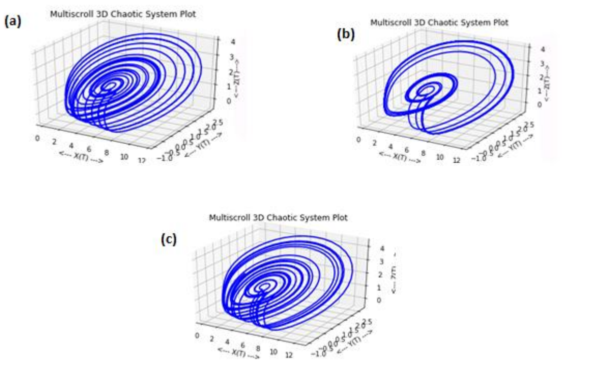

Figure 4. (a), (b), (c) Phase portraits with EEG initial conditions for 3D multi-scroll systems

C. Encryption Process

Normal Encryption process deals with XOR operation, permutation and diffusion process in a single step. This leads to the insecurity of the data encryption when the system is connected in an IoT environment. For producing the high randomness in the key, the proposed architecture uses the new technique of using dynamically varying MAC parameters such as RSSI and distance, to provide the secure data transmission [17].

The XOR operation is employed by the proposed architecture to generate the new key which can acts as the dynamic pseudo random generator. The MAC parameters which are measured for the encryption process are as follows

RSSI (R): The RSSI is the most predominant term which is calculated between the nodes and gateways.

Distance (D) : The distance between the node and gateways is calculated by using RSSI in which the expression is given as

$$D_{(N_s,BS)} = 10\left[\frac{(P_o - F_m - P_r - 10n\ log(f) + 30n - 32.44)}{10n}\right] \quad (2)$$

Where P_o is the power of the signal (dBm) in the zero distance, P_r is the signal power (dBm) in the distance d, f is the signal frequency in MHz, F_m is the fade margin and n is the path-loss exponent.

Channel ID: Channel ID of the user transceivers interfaced with the nodes.

After calculating the MAC parameters, new high complex key is generated which is used to encrypt the data streams .Table I gives the parameter values along with RSSI and distance to produce the keys.

Table I Parameter values along with the RSSI and distance (D) for the choatic system to produce the high complexity keys.

A	B	C	D	E	F	RSSI	D
2	6	6	3	3	1	-43	1
2	6	6	3	3	1	-71	1
2	6	6	3	3	1	-88	1
2	6	6	3	3	1	-86	1
1	6	6	3	3	1	-78	1
2	6	6	3	3	1	-86	1
2	6	6	3	3	1	-70	1
2	6	6	3	3	1	-50	1
2	6	6	3	3	4	-48	1

Figure 5 shows the chaotic behavior of the proposed 3D chaotic system with EEG initial conditions and RSSI, D values of the networks.

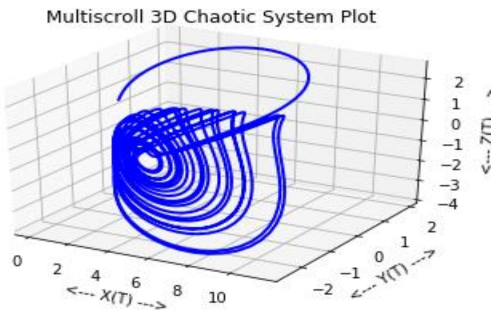

Figure 5. Choatic Behavoiur of the Proposed 3D chaotic system using EEG initial conditions and RSSI, D values of the Networks

D. Diffusion Process

To ensure the security of the data, diffusion process is employed between the new encrypted key and the input data streams. For diffusion process, newly generated keys are iterated for 'N' times and 'G' vector is formed by selection of keys at the odd iteration. Subsequently, 'G' vector is arranged into the matrix F which has the same size as of the input data streams. Before diffusion, all the elements in F matrix should be scaled to 0 to 255.The new dynamic constant β has been introduced in the diffusion process and the diffusion operator μ for the input data streams are given in Eqns. (3) and (4).

$$B = \sum d(i) mod256 \text{ where } i =,1,2,3,\ldots 255 \quad (3)$$

$$\mu = Fi + \beta + d(i) mod256 \quad (4)$$

The final new cipher data is obtained after the diffusion process.

III. VALIDITY ANALYSIS

The proposed encryption algorithm has been tested with the number of negative permutation of data bits by changing the input data bits with the gradual change of 5%, 25%, 50% and 100% changes and Number of Pixel Change rate (NPCR) is calculated by using Eqn. (5) [23]

$$NPCR = \{[\sum i\ d\ (i)]/m\}\ x100\% \quad (5)$$

where d (i) is the data matrix

m is the no. of bits changed

The NPCR is calculated for the above said cases and tabulated in the Table II.

Table II. NPCR values for test cases

Sl.No	Changes in data position bit	NPCR
01	5%	99.8%
02	10%	99.75%
03	25%	99.8%
04	50%	99.8%
05	75%	99.8%
06	100%	99.8%

Table 2. clearly shows that NPCR has been maintained at constant rate of 99.8% even though the bit values are changed at the different proportions.

IV. COMPARITIVE ANALYSIS

The proposed encryption algorithm is compared with the existing algorithms and the results are given in Table III.

Table III. Comparative analysis between the proposed algorithm and other existing algorithm

Sl.No	DIFFERENT ALGORITHMS	NPCR
01	Guodong Ye et al., [18]	99.6%
02	Manish Kumar et al.,[19]	99.568%
03	Proposed Algorithm	99.8%

Table III. clearly depicts that the NPCR of the proposed encryption algorithm is found to be 99.8% which outperforms other existing encryption algorithms.

V. CONCLUSION

To enhance the data security in an IoT environment, dynamic chaos models are used for the data encryption. The proposed architecture employs the 3D multi scroll chaotic systems. To make the randomness in the key and data, the proposed architecture uses the different peaks from EEG signals to generate the initial conditions of the proposed chaotic systems .The key has strong randomness since the obtained values are again doing XOR operation with the MAC parameters such as the RSSI distance and channel ID. Also 3D chaotic systems are implemented in Raspberry pi -3 in an IoT environment and EEGLAB is used for extracting the different peaks from the EEG signals. The proposed encryption algorithm has been tested at different scenarios and NPCR is found to be 99.8 % and it clearly outperforms the other existing algorithms.

REFERENCES

1. W. Liu, K. Sun, and C. Zhu, “A fast image encryption algorithm based on chaotic map,” Optics and Lasers in Engineering, vol. 84, pp. 26–36, 2016.
2. X. Huang and G. Ye, “An efficient self-adaptive model for chaotic image encryption algorithm,” Communications in Nonlinear Science and Numerical Simulation, vol. 19, no. 12, pp. 4094–4104, 2014.
3. A. Kanso and M. Ghebleh, “A novel image encryption algorithm based on a 3D chaotic map,” Communications in Nonlinear Science and Numerical Simulation, vol. 17, no. 7, pp. 2943–2959, 2012.
4. N. Zhou, S. Pan, S. Cheng, and Z. Zhou, “Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing,” Optics & Laser Technology, vol. 82, pp. 121–133, 2016.
5. G. Zhou, D. Zhang, Y. Liu, Y. Yuan, and Q. Liu, “A novel image encryption algorithm based on chaos and Line map,” Neurocomputing, vol. 169, pp. 150–157, 2015.
6. S. El Assad and M. Farajallah, “A new chaos-based image encryption system,” Signal Processing: Image Communication, vol. 41, pp. 144–157, 2016.
7. S. Mohammad Seyedzadeh and S. Mirzakuchaki, “A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map,” Signal Processing, vol. 92, no. 5, pp. 1202–1215, 2012.
8. I. Hussain, T. Shah, and M. A. Gondal, “Application of S-box and chaotic map for image encryption,” Mathematical and Computer Modelling, vol. 57, no. 9-10, pp. 2576–2579, 2013.
9. X. Wang and D. Luan, “A novel image encryption algorithm using chaos and reversible cellular automata,” Communications in Nonlinear Science and Numerical Simulation, vol. 18, no. 11, pp. 3075–3085, 2013.
10. S.-J. Xu, J.-Z. Wang, and S.-X. Yang, “An improved image encryption algorithm based on chaotic maps,” Chinese Physics B, vol. 17, no. 11, pp. 4027–4032, 2008.
11. B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, and M. R. Mosavi, “A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos,” Multimedia Tools and Applications, vol. 74, no. 3, pp. 781–811, 2013.
12. Y. Liu, X. Tong, and J. Ma, “Image encryption algorithm based on hyper-chaotic system and dynamic S-box,” Multimedia Tools and Applications, vol. 75, no. 13, pp. 7739–7759, 2016.
13. Y. Zhang, D. Xiao, W. Wen, and M. Li, “Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process,” Nonlinear Dynamics, vol. 76, no. 3, pp. 1645–1650, 2014.
14. R. Rhouma and S. Belghith, “Cryptanalysis of a new image encryption algorithm based on hyper-chaos,” Physics Letters A, vol. 372, no. 38, pp. 5973–5978, 2008.
15. X. Chai, Y. Chen, and L. Broyde, “A novel chaos-based image encryption algorithm using DNA sequence operations,” Optics Lasers in Engineering, vol. 88, pp. 197–213, 2017.
16. Mei Zhang, Qingtao Han, “Dynamic analysis of an autonomous chaotic system with cubic nonlinearity”, Optik, 0030-4026, Published by Elsevier GmbH. 2016. http://dx.doi.org/10.1016/j.ijleo.2016.01.142
17. Lisheng XU1,2, Feifei Yangl, Yuqi Jiangl, Lei Zhang 1, Cong Fengl and Nan Bao,” Variation of Received Signal Strength in Wireless Sensor Network”, 3rd International Conference on Advanced Computer Control (ICACC 2011)-2011
18. Guodong Ye, Kaixin Jiao, Chen Pan, and Xiaoling Huang “An Effective Framework for Chaotic Image Encryption Based on 3D Logistic Map”, Security and CommunicationNetworksVolume 2018, Article ID 8402578, 11pages https://doi.org/10.1155/2018/8402578
19. Manish Kumar, Sunil Kumar, M.K. Das and Sanjeev Singh,” Lightweight Data Security Model for IoT Applications: A Dynamic Key Approach”, 978-1-5090-5880-8/16 $31.00 © 2016 IEEE DOI 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.100

AUTHORS PROFILE

G.Gugapriya is pursuing her doctoral degree in Electronics and Communication Engineering in Vellore Institute of Technology, Chennai. She received her ME (Embedded Systems Technology) from Anna University, Chennai in 2007 and BE (EEE) from Bharathiyar University in 2002. Her research interests includes non-linear dynamics, embedded systems and real time operating systems.

B.Lakshmi obtained her doctoral degree in Information and Communication Engineering from Anna University, Chennai, in the year 2013. She received her ME (Applied Electronics) from Anna University, Chennai, in 2005 and BE (ECE) from Madras University in 2000. She is currently working as an Associate Professor in the school of Electronics Engineering, VIT, Chennai. Her research interests include VLSI, nano-scale transistors, and micro/nano-electronics. She successfully completed a project for DST- SERB titled, “Process Variational Study and Performance Analysis of Nano-scale MOSFETs and Tunnel FETs: Tunnel FETs based Mixed Signal Integrated Circuits for System-on-Chip Applications" in the year 2017. To her credit, she has 25 journal papers and 10 conference papers.