**Dynamics of Memristive Autapse-Synapse Chaotic Neuron Model and its Application to Medical Cryptography**

**Abstract:**

With the advent of physical memristor, various memristive neuron models have been designed and analyzed to mimic some human brain functions. However there exist a realistic issue given that many works reported the coupling of neuron model using either memristive synapse or memristive autapse while a neuron in the real brain can interact both with another neuron and with itself. Two main ideas are developed in this work. First we investigate the dynamics of two different neurons coupled via memristive synapse and memristive autapse. The analyses indicate that the global dynamics of the model is highly sensitive to the memristive coupling strength. Second the chaotic sequences generated from the proposed model are exploited to construct a nonlinear and pseudorandom random substitution box (s-box). The s-box is then exploited to construct the measurement matrix useful in the compressive sensing process. The whole algorithm is used to compress and secure medical images. The results indicate that the coupling strength of the proposed model can be adjusted to increase or decrease the security of medical data. In addition the compressive sensing method is hardware-friendly that is it results can be exploited for practical applications including Wireless Boby Area Network (WBAN).

**Keywords:** Memristive synapse; Memristive autapse; Neuron model; s-box; Compressive sensing; image encryption.

**1. Introduction**

Neurons are brain cells that are used to transmit information. They are all interconnected and communicate with each other by electrical and chemical messages through branches called dendrites on which the axons end to transmit information. Neurons are responsible of several functions of the human brain. The complexity of the brain has encouraged scientists to study neuronal models dynamics. Thus, in the early 1980s, artificial neuron models and artificial neural network models emerged including Hodgkin–Huxley neuron model (HH) [3], FitzHugh–Nagumo(FHN) neuron model [4,5], Morris–Lecar neuron model (ML) [6], Hindmarsh–Rose neuron model (HR) [7], Chay neuron model [8], Hopfield neural network(HNN) [9], Cellular neural network (CNN) model [10]. The analysis of the dynamics of these models made it possible to reveal several electrical activities in the brain dynamics such as periodic spiking [12], periodic bursting [13], and mode transition [14]. Although these classical models have allowed the demonstration of some dynamic behaviors of the brain, it is quite obvious that the human brain is very complex. Some researchers believe that the coupling of neurons may be more realistic in highlighting the dynamic behaviors of the human brain. Mohammad and collaborators exploited gap junction with different coupling strength to link type I and type II excitability neurons [ref1]. The investigations indicated that the coupling strength considerably affects the dynamics of the neurons. The discovery of the physical memristor reactivated the interest on neural networks dynamic analysis. It should be noted that the memristor has several properties including its programmability, its memorability, its nonlinearity... These properties can be exploited to reproduce the synaptic functions of the brain such as plasticity. It is also important to stress that the memristor can also be exploited to describe the effect of electromagnetic radiation on the electrical activity of the neuron. Consequently, several researchers believe that with the memristor as a neuronal synapse and/or autapse, the dynamics of the artificial neuron are more realistic and many researches can be identified in this line. A review on chaos in the dynamics of coupled neurons has been investigated by Hairong and collaborators [ref2]. In this review it is obvious that memristive autapse can be exploited to interconnect the dendrites and the axon of the same neuron. On the other way memristive synapse is used to couple two identical neurons or two different neurons. Note that the analysis of couple neurons using both memristive autapse and memristive synapse is not yet reported. Tabekoueng and coworkers exploited memristive synapse to couple 2D FitzHugh–Nagumo neuron and 3D Hindmarsh–Rose neuron. The dynamics reveals the coexistence of infinite patterns in the state space. Ref3 exploited a new locally active memristor as synapse to couple neurons. It can be observed that with the advent of memristor the field of neurodynamics has made significant progress. However it is obvious to note that none of the most recent works has investigated the dynamics of coupled neurons using both memristive synapse and memristive synapse. This limitation is our main motivation in the design of the new neuronal model presented in this work.

Security in communication channels is one of the primary concerns of a very large scientific community. One of the most affected areas is the medical field where highly sensitive medical information can pass from sender to receiver. These confidential data must be secured. In this perspective, several algorithms for securing medical images can be identified in the literature [ref…]. [Ref4] exploited SCAN technique and Ten map in chaotic windows to secure medical image. The method decomposes the image plane into bit first, follows with a pixel rearrangement and finally a diffusion process. Njitacke and collaborators recently studied the electromagnetic effect of two coupled neurons on the security of medical images. A compressed sensing algorithm is used to compress the image to fit its size with the communication channel bandwidth. The results provided secured and compressed output images. It should be noted that the compression performance in compressive sensing mainly rely on the construction of measurement matrix. In this work the measurement matrix is constructed using the nonlinear and pseudorandom properties of S-box generated from the sequences of the memristive autapse-synapse neuron model. The main objective of this work can be summarized in the sequel:

1. Using memristive autapse and synapse couple two different neurons and analyze its dynamics in term of coupling strength. The idea of coupling neurons using both memristive synapse and autapse is completely new.
2. Exploit the sequence of the memristive autapse-synapse neuron model construct a new S-box with strong nonlinearity and pseudo-random properties.
3. Build a strong and hardware-friendly (fast and useful for practical application) compressed sensing algorithm using the generated S-box in the process of measurement matrix construction. Note that this idea is not yet reported in the literature.
4. Propose a compression-encryption algorithm for medical data using both the designed compressed sensing method and the sequence of the memristive autapse-synapse neuron model in the chaotic range.
5. Evaluate the effect of the neuron synapse-autapse coupling strength of the neuron on the security of the medical image.

The remainder of this paper is arranged as follows:

***Ref1:*** *Emergence of bursting in two coupled neurons of different types of excitability*

***Ref2:*** *Review on chaotic dynamics of memristive neuron and neural network*

***Ref3:*** *A simple locally active memristor and its application in HR neurons*

***Ref4:*** *Medical Image Encryption Using SCAN Technique and Chaotic Tent Map System*

*[3] Hodgkin, A.L., Huxley, A.F.: A quantitative description of membrane current and its application to conduction and excitation in nerve. J. Physiol. 117(4), 500–544 (1952)*

*[4] Fitzhugh, R.: Impulses and physiological states in theoretical models of nerve membrane. Biophys. J. 1(6), 445–466 (1961)*

*[5] Nagumo, J., Arimoto, S., Yoshizawa, S.: An active pulse transmission line simulating nerve axon. Proc. IRE 50(10), 2061–2070 (1962)*

*[6] Morris, C., Lecar, H.: Voltage oscillations in the barnacle giant muscle fiber. Biophys. J. 35(1), 193–213 (1981)*

*[7] Hindmarsh, J.L., Rose, R.M.: A model of the nerve impulse using two first-order differential equations. Nature 296(5853), 162–164 (1982)*

*[8] Chay, T.R.: Chaos in a three-variable model of an excitable cell. Physica D 16(2), 233–242 (1985)*

*[9] Hopfield, J.J.: Neurons with graded response have collective computational properties like those of 2-state neurons. Proc. Natl. Acad. Sci. USA 81(10), 3088–3092 (1984)*

*[10] Chua, L.O., Yang, L.: Cellular neural networks: theory. IEEE Trans. Circuits Syst. 35(10), 1257–1272 (1988)*

*[11] Maass, W.: Networks of spiking neurons: the third generation of neural network models. Neural Netw. 10, 659–1671 (1997)*

*[12] Izhikevich, E.M.: Neural excitability, spiking and bursting. Int. J. Bifurcat. Chaos 10(6), 1171–1266 (2000)*

*[13] González, J.M.: Complex bifurcation structures in the Hindmarsh–Rose neuron model. Int. J. Bifurcat. Chaos 17(9), 3071–3083 (2007)*

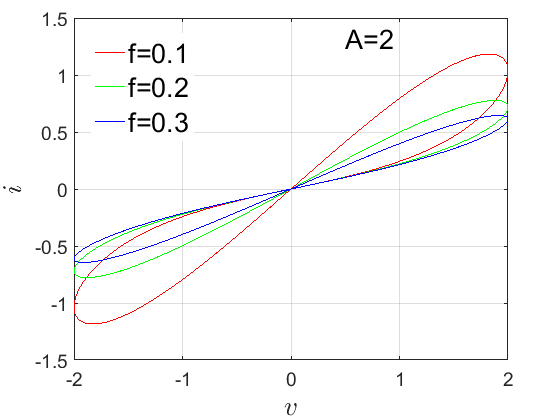
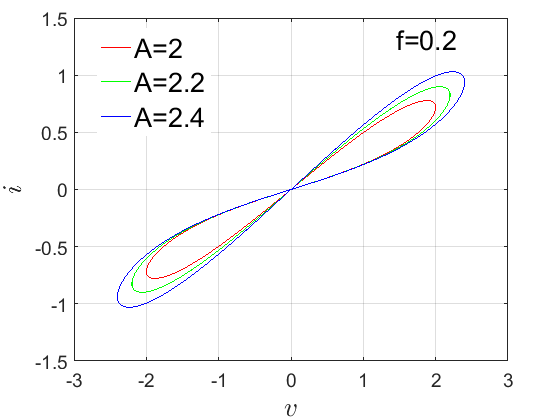
*[14] Yang, Z., Lu, Q.: Different types of bursting in Chay neuronal model. Sci. China Phys.Mech.51(6), 687–698(2008)*

**2.** **The memristive autapse-synapse neuron model**

The memristor is the fourth missing electronic component, beside the inductor, the capacitor, and the resistor. It is mainly characterized by its capability to save information, given that its resistance changes from a very large value to a very low value, which is interpreted as ‘1' and ‘0' logics. As such, the memristor is a suitable tool to reproduce the dynamics of the human brain. A novel memristor model is introduced in this work to couple neurons, and the corresponding mathematical equation is defined by Eq.1.

 (Eq.1)

In Eq.(1), the term  represents the memductance of the memristor, while the evolution of that inner variable of the memristor. By applying various sinusoidal excitation of the form  on the designed memristor with , , , the pinched hysteresis loop in the voltage–current plane of the memristor is established (Fig.2). Consequently the memristor model is suitable to design memristive synapse-autapse neuronal models.



**Fig.1:** Hysteresis representation of the proposed memristor exploited for autapse-synapse.

Neuronal models that are able to reproduce human brain dynamics have greatly improved the field of neurodynamics. Various models have been introduced and analyzed to show some common dynamics in the human brain. Hindmarsh and Rose (HR) designed one of the most simple and single neuron model capable to display most of firing activities in the human brain. The mathematical description of Hindmarsh-Rose neuron model includes both 2-D and 3-D models. 2-D model is described by Eq.2.

 (2)

Another classical neuronal model presented and analyzed in the literature is the FitzHugh–Nagumo (FHN) model. This model is introduced by simplifying the Hodgkin and Huxley (HH) neuronal model. The FHN neuron model (presented in Eq.3) also reflects some well-known dynamical behavior present in the human brain.

 (3)

Human brain is made of different interconnected neurons. However most of the recent works in the literature proposed and analysed the interconnection of identical neurons. Also note that the recent works in the literature shows the interconnection of neurons using either memristive autapse or memristive synapse. In this work the 2-D HR model described by Eq.2 and the 2-D FHN model described by Eq.3 are exploited to design the memristive autapse-synapse neural network model as described by Eq.4.

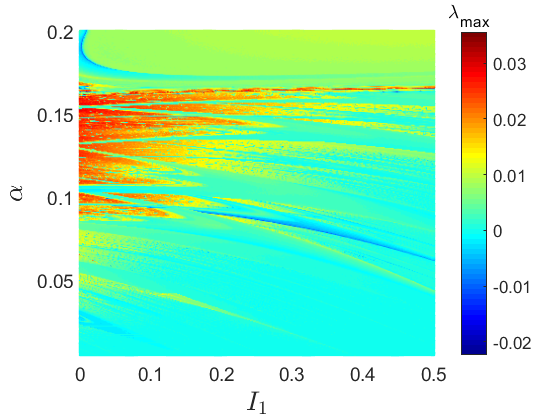
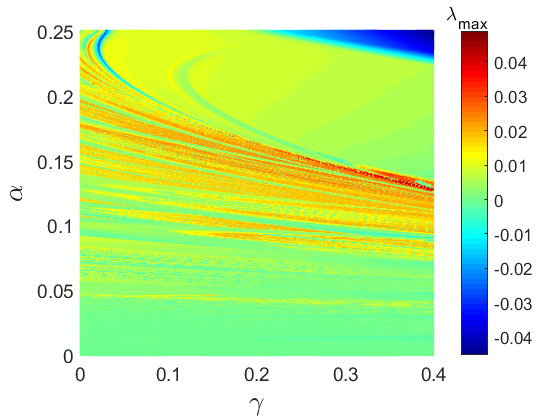
 (4)

Note that such model better reflects the real dynamics of the neurons in human brain. The coupling method of the neurons follows the Campbell and Waite principle [[1](#_ENREF_1)]. In this model  represent the fast variable or the potential membrane and  indicate the slow variable or the ion current (Na+ or K+).  stand for the inner variable of the memristive autapse as well as the memristive synapse. ,  and  represent the parameters of the memristive synapse and autapse. , , ,  and  are traditional parameter of the neuron model defined by Eq.5 for invariant parameters

 (5)

**3. Dynamics of the memristive autapse-synapse neural network model**

Remember that a brain-like complex system is made up of a large number of neurons that are linked together. These neurons are important in a variety of biological processes, including hearing, speech, memory, emotions, learning, transport, and information processing/coding, to name a few [[2](#_ENREF_2)]. Based on a global bifurcation analysis, the complex behaviors of the introduced model can be easily investigated.



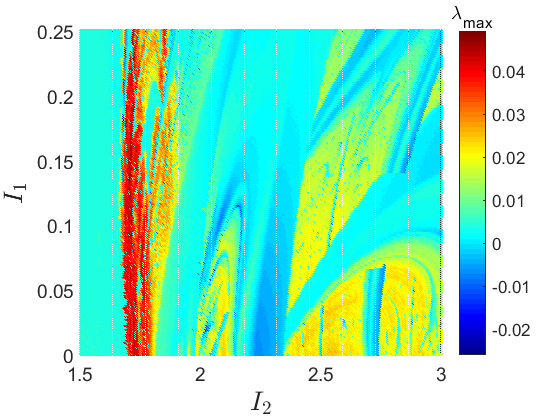
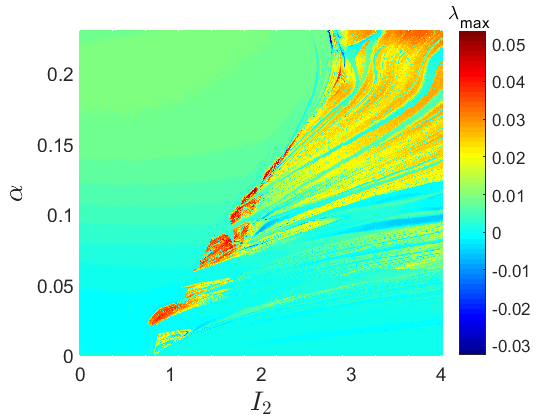


Fig.2.

Two-parameter diagrams obtained when two parameters of the coupled neurons are simultaneously varied. The is obtained for , . The is obtained for , . The is obtained for , . And the is obtained for , . Initial conditions are .

Lyapunov exponent graphs with two parameters are used to quickly explore the global dynamics of the coupled neurons. These graphs are created by simultaneously varying two parameters of the coupled neurons from a minimum to a maximum value. The maximum

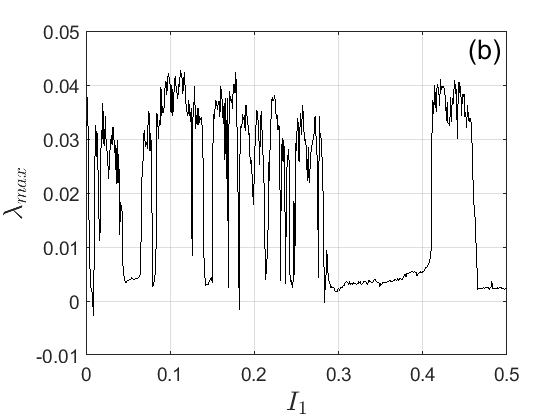
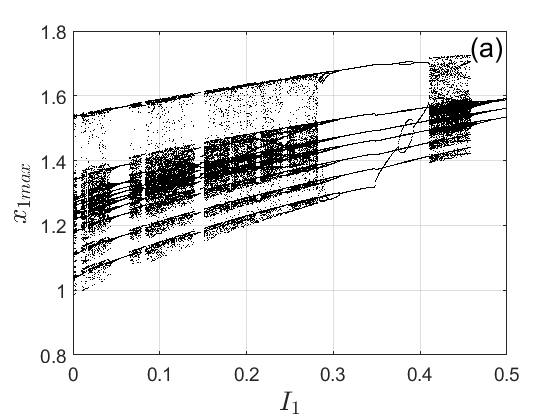


Fig.3.

(a) Bifurcation diagram showing the local maxima of the state variable of the membrane potential of the first neuron versus the external current . The corresponding graph of the maximum Lyapunov exponent is present in (b). These diagrams are obtained for , , . Initial conditions are .

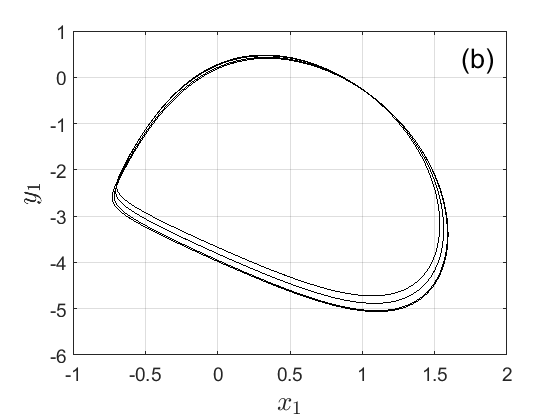
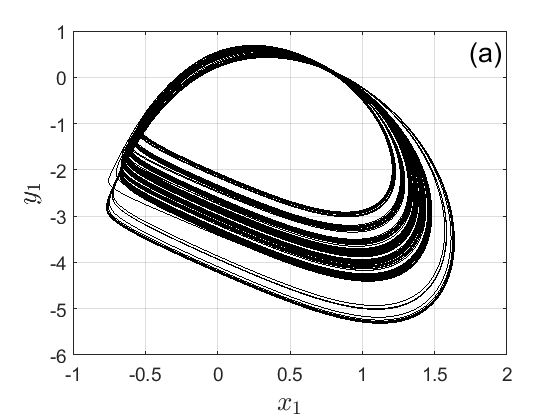


Fig.4.

(a) Chaotic phase portrait obtained for while (b) represents the periodic phase portrait obtained for 

Lyapunov exponent is estimated with the Wolf algorithm [[3](#_ENREF_3)] at each step of the variation and plotted on the same graph as the two parameters. The two-parameter Lyapunov diagrams of Fig. 2 are obtained using the computational method described above. According to the diagrams, several firing activities can be developed by the coupled neurons via the memristive autapse synapse. Among them, it can be found regular behaviors with , and irregular behaviors with . Using the parameters of the fourth two-parameter diagrams as argument (the plane ) the bifurcation diagram of Fig. 3 as well as its corresponding graph of the maximum Lyapunov exponent have been computed.

From that bifurcation diagram, it is obvious that the dynamic behavior of the coupled neuron when the external current  of the neuron is varied changes from chaotic to periodic behavior through several chaotic and periodic windows. For some discrete values of  the chaotic and periodic phase portrait of Fig.4 have been computed to further supported the irregular and the regular of patterns found in the coupled neurons via a memristive autapse synapse.

**3.** **Fundamental knowledge and related works**

**3.1 S-box introduction**

In symmetric cryptography, to obscure the relationship between cipher text and plain text and to hold the properties of confusion and diffusion suggested by C E Shannon, Look-up table like components are employed. Such look-up tables are known as the Substitution-boxes or simply S-boxes. S-boxes are the only non-linear components of symmetric cryptographic system and act as the basic building blocks of symmetric cryptosystems which provide substitution [1]. Cryptographic strong S-boxes are credible to provide resistance against differential and linear cryptanalysis. S-boxes play a significant role in the security of the symmetric cryptosystems. An S-box of size  nonlinearly transforms the n-bit plain-text to m-bit ciphertext *i.e*. it is mathematically mapping from {0, 1}*n* to {0, 1}*m*, where  [2]. Traditional block cipher algorithms like (DES, AES, IDEA, etc.) aren’t that effective for the security of image and video data [3]. Therefore, the chaos based cryptography has been lately used to ensure the security of graphic data, because basic cryptosystems requirements like sensitivity to the block and cipher text, randomness, and the confusion and diffusion processes are well fulfilled by chaotic maps [4]. These S-boxes are formed using the parts of the given key of a cryptosystem to increase its cryptographic strength and are more in demand than the static S-boxes. If a block cipher employs such key-dependent dynamic S-boxes, it becomes difficult for an attacker to unveil the sensitive plain-text data fully or partially [5]. The construction of strong S-boxes using chaotic maps has gained much attention. Additionally, the applications of S-boxes have been increasing its domain for the past many years. Apart from its usage and application in block ciphers design, the S-boxes have been also incorporated for the design of image encryption [5-7], image watermarking [8, 9], image and video steganography [10-12], pseudo-random number generation [13, 14], etc.

**4. Description of newly designed S-box**

**4.1 S-box generation algorithm**

This section deals with the description of the proposed method with which the optimized S-box gets generated as an outcome. The proposed S-box method involves two phases. In the first phase, an initial random chaotic S-box is constructed with the help of the proposed memristive synapse-autapse neuron model in Eq. 4. Initial phases make use of random chaotic values to extract integer values lying the domain of  S-box*.* The first occurrence of such integer values is saved in an array. The procedure is repeated until the array has unique 256 elements in . The random nature of S-boxes generation doesn’t guarantee the yielding of strong components [15]. Hence, it is advisable to have some mechanism which can evolve the S-boxes in terms of its security performance. Therefore, an intelligent heuristic is suggested which has the credibility to evolve the composite fitness function in the second phase. The complete method for the optimized S-box generation is presented as **Algorithm 1**. The fitness function is constructed with an aim to be maximized. The fitness function is composite in the sense that it is based on nonlinearity and differential uniformity of the anticipated S-box. Hence, the maximized fitness value tends to produce S-box with higher nonlinearity and lower differential uniformity as desired. The anticipated fitness function is unique and different as it involves two performance parameters instead of just one. In practice, only nonlinearity is adopted for the performance optimization of the S-box. The fitness function  considered in the proposed work to evolve the S-box *S* for better security performance has the following form.



|  |
| --- |
| **Algorithm 1**. The generation of S-box with optimized fitness |
| **Input:** Initial states initial parameters and synapse-autapse neuron model parameters; positive integers ; maximum number of passes |
| **Output:** S-box |
| **Initialization:** |
| (1): Take empty array ; set flag |
| (2): Using initial parameters and synapse-autapse neuron model parameters and the Runge-Kutta method, solve the memristive autapse synapse neuron model in the chaotic range to obtain with *T* elements and discard all but keep the last state. |
| (3): **while** **do** |
| (4): Using initial parameters and model parameters and the Runge-Kutta method, solve the memristive autapse synapse neuron model in the chaotic range to obtain. |
| (5): Compute |
| (6): **if** (value  doesn’t belong to array ) **then** |
| (7): append value  in array |
| (8): **end if** |
| (9): **if** (array  contains 256 elements) **then** |
| (10): Set , and |
| (11): **end if** |
| (12): **end while** |
| **Fitness Refinement:** |
| (13): **for**  to  **do** |
| (14): Using initial parameters and model parameters and the Runge-Kutta method, solve the memristive autapse synapse neuron model in the chaotic range to obtain. |
| (15): Compute |
| (16): Compute |
| (17): Compute |
| (18): Find  such that |
| (19): Exchange  with |
| (20): Set |
| (21): Evaluate fitness of as: |
| (22): **if** is greater than or equal to **then** |
| (23): and |
| (24): **end if** |
| (25): **end for** |
| (26): Final S-box is  with fitness |

**3.2 S-box performance analysis**

The security assessment of the proposed S-box is crucial to judge the performance against some well accepted parameters. The proposed S-box method is implemented for the settings of  . The S-box obtained after executing the proposed S-box **Algorit-hm 1** is shown in Table 1. The cryptographic strength of the obtained S-box is assessed by quantify the performance param-eters such as nonlinearity (high is better), differential uniformity (lower is better), SAC (ideal is 0.5), bits independence criterion (higher is better for NL), and linear approximation probability (lower is better). The following subsections are prepared to analyze these parameters for security evaluation.

**Table 1:** Generated optimized 8×8 S-box using **Algorithm 1**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **R/C** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **A** | **B** | **C** | **D** | **E** | **F** |
| **0** | 187 | 228 | 125 | 50 | 25 | 51 | 150 | 103 | 91 | 136 | 40 | 49 | 121 | 113 | 159 | 153 |
| **1** | 202 | 235 | 176 | 70 | 253 | 24 | 152 | 138 | 243 | 185 | 54 | 248 | 219 | 207 | 241 | 102 |
| **2** | 105 | 38 | 168 | 211 | 236 | 5 | 116 | 229 | 88 | 22 | 147 | 14 | 13 | 71 | 80 | 148 |
| **3** | 36 | 245 | 154 | 66 | 239 | 48 | 162 | 143 | 64 | 142 | 233 | 157 | 193 | 63 | 165 | 220 |
| **4** | 42 | 21 | 158 | 130 | 39 | 250 | 133 | 244 | 112 | 234 | 173 | 32 | 206 | 114 | 30 | 221 |
| **5** | 218 | 86 | 124 | 0 | 240 | 52 | 61 | 3 | 180 | 203 | 169 | 84 | 82 | 99 | 177 | 199 |
| **6** | 126 | 224 | 184 | 255 | 232 | 117 | 144 | 9 | 249 | 31 | 167 | 8 | 4 | 226 | 89 | 155 |
| **7** | 181 | 123 | 175 | 69 | 118 | 79 | 67 | 194 | 145 | 182 | 23 | 237 | 205 | 238 | 96 | 104 |
| **8** | 172 | 198 | 188 | 65 | 191 | 179 | 171 | 37 | 18 | 149 | 254 | 15 | 230 | 216 | 214 | 7 |
| **9** | 58 | 156 | 183 | 72 | 87 | 98 | 46 | 146 | 11 | 197 | 33 | 81 | 75 | 222 | 17 | 16 |
| **A** | 108 | 120 | 29 | 76 | 45 | 44 | 247 | 213 | 60 | 59 | 106 | 95 | 209 | 231 | 164 | 57 |
| **B** | 137 | 41 | 174 | 2 | 56 | 77 | 68 | 242 | 192 | 140 | 34 | 210 | 195 | 215 | 1 | 132 |
| **C** | 119 | 212 | 151 | 178 | 111 | 139 | 85 | 201 | 115 | 131 | 246 | 93 | 12 | 189 | 141 | 97 |
| **D** | 128 | 6 | 47 | 135 | 19 | 78 | 186 | 129 | 94 | 10 | 73 | 62 | 160 | 161 | 166 | 90 |
| **E** | 26 | 43 | 225 | 170 | 20 | 204 | 100 | 107 | 127 | 27 | 35 | 208 | 223 | 163 | 74 | 83 |
| **F** | 252 | 110 | 134 | 101 | 122 | 92 | 196 | 109 | 28 | 55 | 251 | 190 | 53 | 227 | 200 | 217 |

3.2.1 Nonlinearity

To offer sufficient nonlinearity transformation of data from the plain-text to the encrypted data is the primary task for an S-box in block cryptosystems. The nonlinearity measure is considered as the most fundamental piece which defines the security and strength of whole system [16]. The strong confusion capability of block cryptosystems is primarily associated with the large nonlinearity to mitigate linear cryptanalysis. Practically, the nonlinearity for 8-bit Boolean function , utilizes Walsh spectrum for function *f*, is evaluated as [16].



where  is the Walsh spectrum of function *f*,which is figured as



Here, *u.w* is the bitwise dot product of two 8-bit vectors. The nonlinearity scores of eight Boolean functions comprises the proposed S-box are found as 110, 112, 110, 112, 110, 112, 112, and 112. The same has been also presented in Table 2. The proposed S-box showed a decent nonlinearity behavior as the it has minimum(*NL*), maximum(*NL*) and average (*NL*) values as 110, 112, and 111.25, respectively. It is evident that all nonlinearity scores are very upright and larger than or equal to 110. This implies that the proposed S-box which is evolved on considered fitness function has admirable ability to bring high nonlinear transformation to oppose related assaults from attackers.

**Table 2:** Nonlinearities of Boolean functions of optimized S-box

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | 110 | 112 | 110 | 112 | 110 | 112 | 112 | 112 | 110 | 112 | 111.25 |

3.2.2 Differential uniformity

The resistivity of S-Box against the differential cryptanalysis (DC) is estimated by differential uniformity. Biham and Shamir gave the procedure to execute the DC. The attack analysis is connected with existing imbalance on the input or output scattering to attack block ciphers and S-boxes [12]. If the EX-OR of each output has identical uniformity with the value of EX-OR of each input contradictorily the cryptanalysis can be perfect [17]. On the off chance that an S-box is uniform in input or output distribution, it is supposed to be good resistant to the anticipated differential attack. Therefore, EX-OR table it is favored that the highest value of differential uniformity (DU) ought to be just about as little as could really be expected. Meaning, a smaller value of DU indicates the decent ability of the S-box to withstand the DC. For an S-box *S*, the differential uniformity is measured as:



Here, set *X* holds all probable input values and the size of this set is 256 for an 8×8 S-box. The EX-OR distribution obtained for the proposed S-box is shown in Table 3. Table 3 shows that biggest value of EX-OR distribution for the propo-sed S-box is 8 which is ought to be as sufficiently little to oppose the differential cryptanalysis.

**Table 3:** EX-OR distribution for proposed S-box

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6 | 6 | 8 | 6 | 6 | 6 | 6 | 8 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 8 |
| 6 | 6 | 6 | 8 | 6 | 8 | 6 | 6 | 8 | 6 | 6 | 6 | 6 | 8 | 6 | 6 |
| 6 | 8 | 6 | 6 | 6 | 4 | 8 | 6 | 6 | 6 | 6 | 6 | 8 | 6 | 6 | 6 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 8 | 6 | 6 | 6 | 6 | 8 |
| 6 | 6 | 8 | 6 | 6 | 8 | 8 | 6 | 8 | 6 | 6 | 8 | 4 | 6 | 8 | 8 |
| 6 | 8 | 6 | 8 | 6 | 8 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 8 | 6 |
| 8 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 8 | 6 |
| 6 | 6 | 6 | 6 | 8 | 8 | 8 | 8 | 6 | 6 | 8 | 6 | 8 | 6 | 6 | 6 |
| 8 | 6 | 8 | 8 | 4 | 6 | 8 | 8 | 6 | 6 | 8 | 6 | 8 | 8 | 6 | 6 |
| 6 | 6 | 6 | 8 | 8 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 6 | 6 | 8 | 8 | 6 | 6 | 6 | 6 | 6 | 4 | 6 | 6 | 8 | 6 | 6 | 6 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 8 | 6 | 6 | 6 | 6 | 6 |
| 8 | 6 | 8 | 6 | 6 | 6 | 6 | 8 | 8 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 6 | 8 | 6 | 8 | 8 | 6 | 6 | 6 | 6 | 8 | 6 | 6 | 6 | 6 | 6 | 6 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 4 | 6 | 8 | 6 | 6 | 6 | 8 | 6 | 6 |
| 6 | 6 | 6 | 6 | 6 | 8 | 6 | 8 | 8 | 8 | 8 | 8 | 6 | 8 | 6 | - |

3.2.3 Strict avalanche criterion

The strict avalanche standard as imperative for strong S-boxes was acquired by Webster and Tavares [18]. To fulfill SAC criteria in S-boxes, the reversing of one bit of vector which gives input must prompt fifty percent of change in the vector which gives out. Because half avalanche is important to lessen any sort of correlation between I/O mix and neglects to spill the sensitive data. A SAC value nearer to 0.5 is constantly seen as respectable. To confirm SAC, Webster and Tava-res gave a procedure for computing the dependency matrix as mentioned in [18]. The dependency matrix for the proposed S-box shown in Table 4 is obtained. The dependency matrix reveals that every entry of the table is quite close to 0.5. This matrix has an average score of 0.500488 which signifies the proposed S-box fulfills the strict avalanche criterion well as it is very close to ideal score of 0.5 with just a deviation of 0.000488.

**Table 4:** Dependency matrix for SAC of proposed S-box

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0.5156 | 0.5 | 0.4843 | 0.5156 | 0.4843 | 0.5 | 0.4843 | 0.5312 |
| 0.5 | 0.5468 | 0.5312 | 0.5 | 0.5156 | 0.5 | 0.4531 | 0.4687 |
| 0.5156 | 0.4375 | 0.5 | 0.4687 | 0.4531 | 0.4687 | 0.4843 | 0.4687 |
| 0.5156 | 0.4062 | 0.4375 | 0.4687 | 0.4843 | 0.4375 | 0.5156 | 0.5 |
| 0.5156 | 0.4531 | 0.5781 | 0.5 | 0.5312 | 0.5 | 0.4843 | 0.5156 |
| 0.5 | 0.5312 | 0.5625 | 0.5 | 0.5625 | 0.4843 | 0.5156 | 0.5781 |
| 0.5156 | 0.5 | 0.4843 | 0.4687 | 0.5 | 0.5 | 0.5312 | 0.5 |
| 0.5312 | 0.5312 | 0.4843 | 0.5312 | 0.5156 | 0.5312 | 0.5468 | 0.4531 |

3.2.4. Bits independence criterion

One of the equally critical criterions for strong S-boxes is bits independence criterion. A strategy to test BIC was recommended by Adams and Tavares [19]. Supposing, the Boolean function’s component of an 8×8 S-box are *f*0, *f*1, …, *f*7. It is said that if the S-box meets BIC, the Boolean function *bitxor*(*f*j, *f*k) (where, *j* ≠ *k* and 0 ≤ *j*, *k* ≤ 7) ought to be exceptiona-lly nonlinear and fulfills avalanche criterion nicely. Thus, BIC is confirmed by computing SAC and nonlinearity of each of the 56 combination Boolean functions *bitxor*(*f*j, *f*k) for an 8×8 S-box. The potential scores of nonlinearities of all 56 fun-ctions *bitxor*(*f*j, *f*k) for proposed S-box are evaluated which are displayed in Table 5. The average score of BIC as for nonlinearities are found as 104.357 which appears to be high and excellent. The score for the proposed S-box verifies the fantastic performance as far as satisfaction of bits independent criterion is concern.

**Table 5:** BIC-NL performance of proposed S-box

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *f*j / *f*k | ­*f*0 | *f*1 | ­*f*2 | *f*3 | ­*f*4 | *f*5 | ­*f*6 | *f*7 |
| *f*0 | - | 106 | 100 | 104 | 106 | 104 | 104 | 108 |
| *f*1 | 106 | - | 106 | 106 | 106 | 104 | 104 | 104 |
| *f*2 | 100 | 106 | - | 98 | 106 | 98 | 104 | 102 |
| *f*3 | 104 | 106 | 98 | - | 104 | 108 | 102 | 102 |
| *f*4 | 106 | 106 | 106 | 104 | - | 108 | 104 | 104 |
| *f*5 | 104 | 104 | 98 | 108 | 108 | - | 108 | 106 |
| *f*6 | 104 | 104 | 104 | 102 | 104 | 108 | - | 106 |
| *f*7 | 108 | 104 | 102 | 102 | 104 | 106 | 106 | - |

3.2.5 Linear approximation probability

The strategy for linear approximation probability (LAP) is useful in computing the imbalance of an event. Matsui in [20] presented the largest probability showing the imbalance of an event measured with the assistance of the examination. There should be no distinction of bits uniformity among output and input. Every one of the input bits along its outcomes in output bits is analyzed independently. On the off chance that every one of the input components are 28, *D* is the class of all potential inputs and the masks applied on the correspondence of output and input bits are individually *w*x and *w*y, then, at that point, most extreme linear guess is the greatest number of similar outcomes which is determined as shown in Eq. .



The fact that that S-box is more competent to resist against linear cryptanalysis attack is because of the lower value of LAP. Following the definition of LAP, the proposed S-box found to have an LAP score of 0.1328.

**3.3 S-box performance comparison**

This section provides comparison analysis of the proposed S-box with other recent and state of the art S-boxes methods. Table 6 is maintained to have a view of scores of all significant performance parameters of some recently investigated S-boxes. The proposed S-box is the results of evolution of S-box based on a composite fitness function which optimizes nonlinearity as well as the differential uniformity measure. As can be seen from the comparison table that the proposed S-box shows excellent nonlinearity and differential uniformity as compared to all other S-boxes. The average NL of our S-box is 111.25 which is considerably higher than all the S-boxes of the table. This is also the case for the differential uniformity as well since it is the lowest (*i.e.* better) compared to the S-boxes. Additionally, the proposed S-box satisfies the SAC criterion in quite better manner compared to the SAC scores of S-boxes investigated in [21, 11, 22, 24, 27, 28, 30]. The bits independence criterion is also gets satisfied as the BIC-NL for proposed S-box is 104.357 which is better than score found in S-boxes of [21, 11, 22, 23, 25, 26, 28-30]. Similarly, our linear approximation probability is 0.1328 which is comparable to many S-boxes of the table in robustness against withstanding the Matsui’s linear cryptanalysis. Hence, the proposed S-box has better security and robustness strength compared to many recent S-boxes and it is well suitable for its usage in cryptographic applications.

**Table 6:**  Performance comparison of proposed S-box

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| S-box | Nonlinearity | | | DU | SAC | BIC-NL | LAP |
| min | max | average |
| Proposed S-box | 110 | 112 | 111.25 | 8 | 0.5004 | 104.357 | 0.1328 |
| Garcia *et al.* [21] | 105 | 107 | 106 | 12 | 0.5066 | 103 | 0.1445 |
| Latif *et al.* [11] | 96 | 106 | 102.5 | 10 | 0.5037 | 103.9 | 0.1250 |
| Çavuşoğlu [12] | 104 | 110 | 107 | 12 | 0.5004 | 102.85 | 0.1328 |
| Zhang *et al.* [22] | 108 | 110 | 108.75 | 10 | 0.4946 | 102.28 | 0.1328 |

**4. Proposed image cryptosystem using 6-D memristive FHN model and block CS**

**4.1 Image encryption scheme**

This section will provide an application of newly designed 6-D memristive FHN model in privacy data protection with assistance of block compressed sensing technology. And the workflows of proposed image encryption and corresponding decryption schemes are drawn in Fig. 1. Then, the whole technical details are listed as hereunder mentioned.

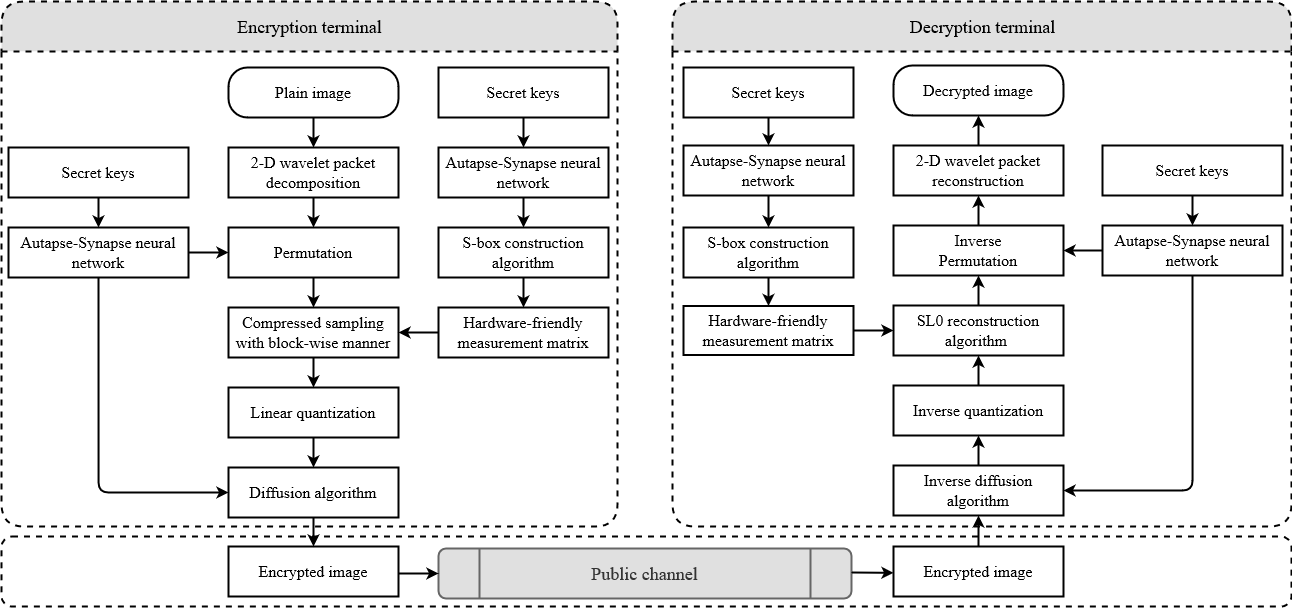


Fig.1 Workflow of the proposed image cryptosystem.

**Step 1.** First, to be capable of performing compressed sampling on the plain image  through 2-D measurement matrix, it is sparsely represented using the multi-layer wavelet packet decomposition algorithm1. And the corres-ponding sparse coefficient matrix is denoted as .

**Step 2.** Then, to relax the restricted isometry property (RIP) [31], the coefficient matrix  is shuffled by the fast 2-D Cat transform with good scrambling effect, thereby spreading its principal components uniformly to each column. In addition, this process can be elaborated into Eq. , where the symbols  and  are the index sequences generated by sorting the output values of new 6-D synapse-autapse memristive FHN model under condi-tions of initial state . And the symbol “mod” means the modulus operator.



**Step 3.** Next, the 3-D generalized chaotic map (GCM), whose mathematical definition is displayed in Eq. , is adopted to construct the initial state of the S-box, where the symbols . Afterward, acc-ording to **Algorithm 1**, the small-scale measurement matrix  consisting of  and 1 is obtained.



**Step 4.** The matrix  is partitioned into several non-overlapping blocks of size . Wherein, the variate  is arranged to be  in this paper. Then, each block is linearly projected onto the measurement matrix  and the resulting values are concatenated to obtain the compressed matrix . Later, it is linearly quantized to the interval  for subsequent processing. This process can be expressed as Eq. .



**Step 5.** Under the control of sequences  constructed by new 6-D synapse-autapse memristive FHN model, the compressed image  is subjected to the bidirectional diffusion algorithm to acquire the final snowflake-like encrypted image  with strong avalanche feature. This process can be expressed as Eq. and Eq. , where the vectors .





**Remark:**

1. For sake of obtaining the higher level of data security, different measurement matrices can be constructed for each sub-block using the counter mode [31] according to the actual application scenarios.
2. The S-box is first proposed to construct measurement matrix for compressed sampling in this paper. Moreover, the measurement matrix generated by **Algorithm 2** is more hardware friendly than the chaotic measurement matrix [32] and the randomly structured measurement matrix [33], etc.

|  |
| --- |
| **Algorithm 2:** The construction of hardware-friendly measurement matrix |
| **Input:** Private key  and matrix dimension . |
| **Output:** Measurement matrix . |
| (1): Initialize an unsigned 8-bit integer variate *pt* with size of , whose elements are all equal to zero. |
| (2): Initialize a floating-point variate *phi*, whose elements are all equal to zero. |
| (3): ; |
| (4): **for** *i* = 1 : 256 **do** |
| (5): ; |
| (6): *num* = 1; |
| (7): **for**  *j* = 7 :  : 0 **do** |
| (8): ; |
| (9): ; |
| (10): **end** |
| (11): **end** |
| (12): Initialize  and rearrange it as size  with column-wise manner. |
| (13): Arrange the element value equal to zero in matrix  to be . |

**4.2 Corresponding decryption scheme**

As for the corresponding decryption process, it is the inverse process of encryption process mentioned earlier, as plotted in Fig. 1. Later, with the aid of the resolution of plain image  and the secret keys, the encrypted image can be decrypted and decompressed to acquire the accurately reconstructed image. In the following, test objects with different sizes will be randomly selected to evaluate the performance of image cryptosystem proposed above from the aspects of security, com-pression, robustness and execution efficiency.

**5. Performance analyses**

This section is devoted the analysis of the performances of the proposal. First it is important to note that all simulations are performed using a laptop with Intel CoreT M i7 – 4600M, 3.00GHz, 64 bits central processing unit, 8GB RAM. The environment is equipped with MATLAB 2014 running under 64-bits operating system. To analyze the performances of the proposed algorithm three medical images (each of size ) are selected from the free medical images data base *MedPix* (<https://medpix.nlm.nih.gov/home>). The proposed autapse-synapse model is solved with the following parameters using the fourth-order Runge-Kutta algorithm to yield chaotic sequences useful in the compression-encryption-decryption stages: ,  , , . Initial conditions are . The algorithm is applied on the test images (each of size ) and the results of compression-encryption-decryption-reconstruction is presented on Fig.X where the first column contains the original input medical data (each of size ). The second column contains the compressed encrypted medical data (each of size ) . The third column contains the results of decryption-reconstruction. Three observations can emerge from these results. (1) The output of the compression provide images each of size when each inputs images is of size . This simply indicates that the images are compressed along the row dimension. (2) The Output of the encryption process (second column) provides images with no profitable information. This simply indicates that the algorithm is capable to secure the input medical data. (3) The output of the compression-encryption-decryption-reconstruction is identical to the input image with few errors.

|  |  |  |
| --- | --- | --- |
| G:\Jiang 5\Code\med9.bmp  Original med1 | Compressed-cypher med1 | G:\Jiang 5\Code\med9.bmp  Decompressed-decypher med1 |
| G:\Jiang 5\Code\med2.bmp  Original med2 | Compressed-cypher med2 | G:\Jiang 5\Code\med2.bmp  Decompressed-decypher med2 |
| G:\Jiang 5\Code\med7.bmp  Original med3 | Compressed-cypher med1 | G:\Jiang 5\Code\med7.bmp  Decompressed-decypher med3 |

Fig.X: Results of compression-encryption-decryption-reconstruction processes.

**5.1. Histogram analysis**

In image processing, histogram of image refers to the representation of each pixel density with respect to the corresponding gray value. This tool is very useful in image encryption to evaluate some statistical properties of both the plain input data and the output data. The histogram of the plain input image is randomly distributed. A given encryption algorithm is required to make uniform the distribution of the pixels. Consequently the histogram of the encrypted image is almost uniform. In the present case the first row of Fig.xx shows the plain image, the compressed-encrypted image and the corresponding histograms. From this result and the above comments it is seen that the proposed algorithm produces output image with uniformly distributed pixels. Consequently the algorithm is secured against statistical attacks.

Fig.xx:

|  |  |  |  |
| --- | --- | --- | --- |
| G:\Jiang 5\Code\med9.bmp  Original med1 |  | Compressed-cypher med1 |  |
| G:\Jiang 5\Code\med2.bmp  Original med2 |  | Compressed-cypher med2 |  |

**5.2. Correlation coefficients analyses**

Another efficient tool to evaluate the capability of an algorithm to resist statistical attacks is correlation coefficient. This metric evaluate how strong is the resemblance between two neighboring pixels in three directions: (horizontal-H, vertical-V and diagonal-D). The results yield a value between -1 and +1 going through 0. When the results approach the extreme values (-1 or +1) this simply indicate very strong correlation between the pixels of the images. Whereas the results close to 0 indicates very poor correlation between the pixels of the image. The distribution of the correlation between pixels can also be represented along various directions. When the distribution is linear this indicates very high correlation between pixels while there is very poor correlation when the distribution is random. The correlation is computed in cryptography using Eq.x.

 (x)

Tab.x provides the correlation coefficients of the plain input medical images and the corresponding ciphers. It is observed that for the plain medical images the correlation coefficients are very close to the extreme values (-1 or +1). This indicates very high correlation between the pixels of the considered data images. In contrast the correlation of the output cipher images are very close to zero indicating that the proposed algorithm has destroyed the correlation between the pixels of the plain images. Consequently the proposed algorithm produces data that can resist statistical attacks.

**5.3. Compression performances analyses**

Structural Similarity Index Measure (SSIM) and Peack Signal to Noise Ratio (PSNR) are two important metrics exploited to compare the output data of any compression algorithm with respect to its input data. This helps to evaluate the performance of the considered compression algorithm. NPCR measures in decibels (dB) the ratio between the maximum power of the input signal and the noise introduced by the considered compression operation. Considering 8-bits images in image and video compression the PSNR should belong to the set  to allow human perception. SSIM measures the degradation of the plain input data in terms of luminance and contrast. Tab.x presents the results of PSNR and MSSIM (Mean SSIM) for the proposed compression algorithm. It is observed that the results are within the threshold values. Consequently the compression-reconstruction processes are effective.

**5.4. Entropy analysis**

Entropy is a statistical tool exploited to evaluate the degree of randomness in a given data. In cryptography this metric is exploited to check if the diffusion step of the algorithm is efficient. There exist various type of entropy but global entropy is the most used in cryptography and this type will be exploited in this work. Given an 8-bits image the global entropy is exploited using Eq.xx.

 xx

For 8-bits image the threshold value of the entropy is 8. Eq.xx has been exploited to compute the entropy values for the three medical plain images and the corresponding ciphers. The results are presented in Tab.x. From these results it is observed that the entropy values of cipher are very close to the threshold value 8 compare to the entropy values of the plain input images. Consequently the proposed algorithm can resist unauthorized intrusion.

**5.5. NPCR and UACI analyses**

NPCR and UACI are two metrics exploited to evaluate the capability of an encryption algorithm to resist differential attacks. In such intrusion unauthorized party create one pixel difference in the image and exploit this difference to obtain the relationship between the plain input and the corresponding cipher image. Considering a plain image and the corresponding cipher,  can be obtained as the cipher of the same plain image with just one different pixel. And these metrics are usually computed using Eq.xxx and Eq.xxxx.

 Eq.xxx

 Eq.xxxx

 represents the size of the image. The threshold value of the NPCR is 100% while the threshold value of the UACI is 33.6%. Eq.xxx and Eq.xxxx have been exploited in this work to compute both NPCR and UACI. The results are shown in Tab.x from where the results are very close to the threshold values. This simply indicates that the proposed algorithm can resist differential attack.

Tab.x

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Test images | Correlation coefficients | | | Entropy | NPCR (%) | UACI (%) |
| H | V | D |
| Original med1 | 0.9025 | 0.9000 | 0.8614 | 6.4263 | 99.9771 | 33.4012 |
| Compressed-cypher med1 | 0.0004 | -0.0002 | -0.0007 | 7.9946 |
| Original med2 | 0.9015 | 0.8256 | 0.8125 | 7.0011 | 99.9901 | 33.5107 |
| Compressed-cypher med2 | -0.0037 | 0.0019 | -0.0069 | 7.9947 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Test images | Correlation coefficients | | | Entropy | NPCR (%) | UACI (%) | PSNR | MSSIM |
| H | V | D |
| Original med1 | 0.9025 | 0.9000 | 0.8614 | 6.4263 | 99.9771 | 33.4012 | 38.1747 | 0.8990 |
| Compressed-cypher med1 | 0.0004 | -0.0002 | -0.0007 | 7.9946 |
| Original med2 | 0.9015 | 0.8256 | 0.8125 | 7.0011 | 99.9901 | 33.5107 | 37.4525 | 0.9716 |
| Compressed-cypher med2 | -0.0037 | 0.0019 | -0.0069 | 7.9947 |
| Original med3 | 0.7264 | 0.6984 | 0.9804 | 7.9851 | 99.8612 | 33.5820 | 38.2963 | 0.9278 |
| Compressed-cypher med3 | 0.0005 | -0.0009 | -0.0025 | 7.9018 |

**5.6. Comparative analysis**

**5.6.1. Comparing the model**

**5.6.2. Comparing the compression-encryption**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Test images | MSSIM | PSNR | Entropy | NPCR (%) | UACI (%) | Enc. Time | Dec. Time |
| Ref x | 0.9903 | 31.7986 | 7.9884 | 99.8700 | 33.4027 | 0.1544 | 2.2489 |
| Ref y | 0.9853 | 38.2045 | 7.9245 | 99.2410 | 33.1542 | 1.5308 | 3.5124 |
| Ref z | 0.9970 | 35.4988 | 7.9896 | 99.0589 | 33.3571 | 2.1296 | 6.7961 |
| Ref w | 0.9950 | 38.2105 | 7.9900 | 99.9854 | 33.4602 | 0.260829 | 3.0218 |
| This work | 0.9971 | 38.2963 | 99.9901 | 99.9901 | 33.5820 | 0.1384 | 1.5144 |

**Conclusion**

The dynamics of two different neurons coupled with both memristive synapse and memristive autapse was considered in this work. Using Lyapunov exponent, bifurcation analysis and phase portrait as dynamical analysis methods, it was established that the model is capable to display various windows of both chaotic and periodic attractors with the variation of the coupling strength. The sequences of the model have been exploited in chaotic windows to construct a measurement matrix a compressive sensing for medical image compression followed by an encryption algorithm. The simulation results show that the proposed algorithm is secured and is friendly-hardware and can be useful in real applications.

**Ref x:** H. Wang, D. Xiao, M. Li, Y. Xiang, and X. Li, “A visually secure image encryption scheme based on parallel compressive sensing,” Signal Processing, vol. 155, pp. 218–232, 2019

**Ref y:** Zhang, Y., Zhao, R., Zhang, Y., Lan, R., & Chai, X. (2022). High-efficiency and visual-usability image encryption based on thumbnail preserving and chaotic system. *Journal of King Saud University-Computer and Information Sciences*.

**Ref z:** Ren, H., Niu, S., Chen, J., Li, M., & Yue, Z. (2022). A Visually Secure Image Encryption Based on the Fractional Lorenz System and Compressive Sensing. *Fractal and Fractional*, *6*(6), 302.

**Ref w:** Huang, X., Dong, Y., Zhu, H., & Ye, G. (2022). Visually asymmetric image encryption algorithm based on SHA-3 and compressive sensing by embedding encrypted image. *Alexandria Engineering Journal*, *61*(10), 7637-7647.

**References**

[1] Makarim, R.H.; Tezcan, C. Relating Undisturbed Bits to Other Properties of Substitution Boxes; Lecture Notes in Computer Science Lightweight Cryptography for Security and Privacy; Springer: Cham, Switzerland, 2015, pp. 109–125.

[2] Ahmad, M., Haleem, H., & Khan, P. M. (2014, February). A new chaotic substitution box design for block ciphers. In 2014 International Conference on Signal Processing and Integrated Networks (SPIN) (pp. 255-258). IEEE.

[3] Azam, N. A., Hayat, U., & Ayub, M. (2021). A substitution box generator, its analysis, and applications in image encryption. Signal Processing, 187, 108144.

[4] Knudsen, L.R.; Robshaw, M.J. The Block Cipher Companion; Information Security and Cryptography; Springer: Berlin/Heidelberg, Germany, 2011.

[5] Deb, S., & Behera, P. K. (2022). Design of key-dependent bijective S-Boxes for color image cryptosystem. Optik, 253, 168548.

[6] Brahim, A. H., Pacha, A. A., & Said, N. H. (2021). A new image encryption scheme based on a hyperchaotic system & multi specific S-boxes. Information Security Journal: A Global Perspective, 1-17.

[7] Gan, Z., Chai, X., Yuan, K., & Lu, Y. (2018). A novel image encryption algorithm based on LFT based S-boxes and chaos. Multimedia Tools and Applications, 77(7), 8759-8783.

[8] Rafiq, A., & Khan, M. (2019). Construction of new S-boxes based on triangle groups and its applications in copyright protection. Multimedia Tools and Applications, 78(11), 15527-15544.

[9] Khan, J. S., Kayhan, S. K., Ahmed, S. S., Ahmad, J., Siddiqa, H. A., Ahmed, F., & Al Dubai, A. (2022). Dynamic S-Box and PWLCM-Based Robust Watermarking Scheme. Wireless Personal Communications, 1-18.

[10] Shah, D., Shah, T., Naseer, Y., Jamal, S. S., & Hussain, S. (2022). Cryptographically strong SP boxes and their application in steganography. Journal of Information Security and Applications, 67, 103174.

[11] A. A. A. El-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, “A novel image steganography technique based on quantum substitution boxes,” Optics & Laser Technology, vol. 116, pp. 92–102, 2019.

[12] Çavuşoğlu, Ü. (2022). S-Box-based video stenography application of variable-order fractional hopfield neural network (VFHNN). The European Physical Journal Special Topics, 1-19.

[13] Girija, R., & Singh, H. (2018). Design of a novel pseudo random generator based on Walsh Hadamard transform and Bi S-boxes. Procedia computer science, 132, 795-804.

[14] Álvarez, R., Martínez, F., & Zamora, A. (2022). Improving the Statistical Qualities of Pseudo Random Number Generators. Symmetry, 14(2), 269.

[15] Ahmad, M., & Ahmad, Z. (2018). Random search based efficient chaotic substitution box design for image encryption. International Journal of Rough Sets and Data Analysis (IJRSDA), 5(2), 131-147.

[16] Cusick, T.W.; Stanica, P. Cryptographic Boolean Functions and Applications; Elsevier: Amsterdam, The Netherlands, 2009.

[s17] Biham, E.; Shamir, A. Differential Cryptanalysis of DES-like Cryptosystems; Advances in Cryptology-CRYPT0’ 90 Lecture Notes in Computer Science; Springer: Heidelberg/Berlin, Germany, 1991; pp. 2–21.

[18] Webster, A.F.; Tavares, S.E. On the Design of S-Boxes; Lecture Notes in Computer Science Advances in Cryptology—CRYPTO ’85 Proceedings; Springer: Heidelberg/Berlin, Germany, 1985; pp. 523–534.

[19] Adams, C.; Tavares, S. The structured design of cryptographically good s-boxes. J. Cryptol. 1990, 3, 27–41.

[20] Matsui, M. Linear Cryptanalysis Method for DES Cipher; Advances in Cryptology—EUROCRYPT ’93 Lecture Notes in Computer Science; Springer: Heidelberg/Berlin, Germany, 1993; pp. 386–397.

[21] V. M. Silva-García, R. Flores-Carapia, C. Rentería-Márquez, B. Luna-Benoso, and M. Aldape-Pérez, ``Substitution box generation using Chaos: An image encryption application,'' Appl. Math. Comput., vol. 332, pp. 123-135, Sep. 2018.

[22] Zhang, T., Chen, C. P., Chen, L., Xu, X., & Hu, B. (2018). Design of highly nonlinear substitution boxes based on I-Ching operators. IEEE Transactions on Cybernetics, 48(12), 3349-3358.

[23] Ibrahim, S., & Abbas, A. M. (2021). Efficient key-dependent dynamic S-boxes based on permutated elliptic curves. Information Sciences, 558, 246-264.

[24] Zamli, K. Z. (2021). Optimizing S-box generation based on the adaptive agent heroes and cowards algorithm. Expert Systems with Applications, 182, 115305.

[25] Alhadawi, H. S., Majid, M. A., Lambić, D., & Ahmad, M. (2021). A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm. Multimedia Tools and Applications, 80(5), 7333-7350.

[26] Zhou, P., Du, J., Zhou, K., & Wei, S. (2021). 2D mixed pseudo-random coupling PS map lattice and its application in S-box generation. Nonlinear Dynamics, 103(1), 1151-1166.

[27] Wang, Y., Zhang, Z., Zhang, L. Y., Feng, J., Gao, J., & Lei, P. (2020). A genetic algorithm for constructing bijective substitution boxes with high nonlinearity. Information Sciences, 523, 152-166.

[28] Jamal, S.S.; Khan, M.U.; Shah, T. A Watermarking Technique with Chaotic Fractional S-Box Transformation. Wireless Personal Communication. 2016, 90, 2033–2049.

[29] Artuğer, F., & Özkaynak, F. (2021). An effective method to improve nonlinearity value of substitution boxes based on random selection. Information Sciences, 576, 577-588.

[30] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, “Secure data encryption based on quantum walks for 5G internet of things scenario,” IEEE Transactions on Network and Service Management, vol. 17, no. 1, 118131, 2020.

[31] H. Wang, D. Xiao, M. Li, Y. Xiang, X. Li, A visually secure image encryption scheme based on parallel com-pressive sensing, Signal Processing. 155 (2019) 218-232. https://doi.org/10.1016/j.sigpro.2018.10.001.

[32] L. Yu, J.P. Barbot, G. Zheng, H. Sun, Compressive sensing with chaotic sequence, IEEE Signal Processing Letters 17 (2010) 731-734. https://doi.org/10.1109/LSP.2010.2052243

[33] T.N. Canh, B. Jeon, Restricted structural random matrix for compressive sensing. Signal Processing: Image Communication, 90 (2021) 116071. <https://doi.org/10.1016/j.image.2020.116017>.

|  |  |  |  |
| --- | --- | --- | --- |
| G:\Jiang 5\Code\med9.bmp  Original med1 |  | Compressed-cypher med1 |  |
| G:\Jiang 5\Code\med2.bmp  Original med2 |  | Compressed-cypher med2 |  |
| G:\Jiang 5\Code\med7.bmp  Original med3 |  | Compressed-cypher med1 |  |
| G:\Jiang 5\Code\med9.bmp  Original med1 |  | Compressed-cypher med1 |  |
| G:\Jiang 5\Code\med2.bmp  Original med2 |  | Compressed-cypher med2 |  |
| G:\Jiang 5\Code\med7.bmp  Original med3 |  | Compressed-cypher med1 |  |