Dynamics of a Memristive Autapse-Synapse Neural Network: Application to Medical Image Encryption

Xi Zhang, Donghua Jiang, Jean De Dieu Nkapkop, Zeric Tabekoueng Njitacke, Musheer Ahmad, Aliya Zhu, Nestor Tsafack,

***Abstract*—With the advent of the physical memristor, various memristive neural network models have been designed and analyzed to mimic some human brain functions. However, there is a realistic issue because many works reported the coupling of neuron models using either memristive synapse or memristive autapse, whereas in the real brain, a neuron can interact with both another neuron (memristive synapse) and with itself (memristive autapse). 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 this highly relies on the neuron's coupling strength. Second, a cryptographic scheme based on both S-box driven block compressive sensing and the memristive autapse synapse model is proposed. Performance analyses indicate that the coupling strength of the proposed neural network model can be adjusted to increase or decrease the security of medical data**

***Index Terms*—Memristive synapse; Memristive autapse; Neural network model; Compressive sensing; Image encryption.**

I. 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 dynamics [1]. Thus, in the early 1980s, artificial neuron models and artificial neural network models emerged, including but not limited to the Hodgkin-Huxley neuron model (HH) [2], FitzHugh-Nagumo (FHN) neuron model [3], Morris-Lecar neuron model (ML) [4], Hindmarsh-Rose neuron model (HR) [5], Chay neuron model [6], Hopfield neural network (HNN) [7] and the Cellular neural network (CNN) model [8]. The analysis of the dynamics of these models made it possible to reveal several electrical activities in the brain dynamics such as periodic spiking, periodic bursting, and mode transition [9]. 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 strengths to link type I and type II excitability neurons [10]. The investigations indicated that the coupling strength considerably affects the dynamics of the neurons. The discovery of the physical memristor reactivated interest on neural networks dynamic analysis. It should be noted that the memristor has several properties including, programmability, memorability, and its nonlinearity. These properties can be exploited to reproduce the synaptic functions of the human brain, such as plasticity. It is important to stress that the memristor can also be exploited to show the effect of electromagnetic radiation on the electrical activity of the neuron. Consequently, several researchers believe that with the memristor as a neuronal synapse or autapse, the dynamic of the artificial neuron is more realistic and much research can be identified in this line [11]. A review on chaos in the dynamics of coupled neurons has been investigated by Hairong and collaborators [11]. 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 hand, a memristive synapse is used to couple two identical neurons or two different neurons. Note that the analysis of coupled neurons using both memristive autapse and memristive synapse has not yet been reported. Tabekoueng and colleagues used a memristive synapse to connect a FitzHugh-Nagumo (2-D) neuron to a Hindmarsh-Rose (3-D) neuron [12]. The dynamics reveals the coexistence of infinite patterns in the state space. [13] exploited a new locally active memristor as synapse to couple neurons. It can be observed that with the advent of the 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 autapse. 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

Manuscript received ****; revised ****

Xi Zhang is with the chool of Aeronautics Engineering, Air Force Engineering University, Xi'an 710038,China

Donghua Jiang is with the School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou 511400, China

Jean De Dieu Nkapkop is with the Department of Electrical Engineering and Industrial Computing, University Institute of Technology, P.O. Box 8698 Douala, Cameroon

Zeric Tabekoueng Njitacke is with the Department of Electrical and Electronic Engineering, College of Technology (COT), University of Buea, P.O. Box 63, Buea, Cameroon and Department of Automation, Biomechanics and Mechatronics, Lodz University of Technology, Lodz, Poland

Musheer Ahmad is with the Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India

Nestor Tsafack is with the Research Unit of Laboratory of Energy and Artificial Intelligence (RU-LEAI), Electrical Engineering Department and Industrial Computing of ISTAMA, University of Douala, P.O. Box 3223, Douala, Cameroon

Xingyuan Wang is with the School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China

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 [14, 15]. [14] exploited the SCAN technique and Tent map in chaotic windows to secure medical images. The method decomposes the image planes into bit first, followed by 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 [15]. The compressed sensing technology 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 relies on the construction of measurement matrix. In this work, the measurement matrix is constructed using the S-box with nonlinear and pseudorandom properties generated from the sequences of the memristive autapse-synapse neural network model. This idea is completely new. The main objective of this work can be summarized in the sequel:

1) Couple two different neurons to form a neural network and analyze its dynamics in terms of coupling strength using memristive autapse and synapse.The most noteworthy point is that the idea of coupling neurons using both memristive synapse and autapse is completely new and not yet studied in the literature.
2) Exploit the output of the memristive autapse-synapse neural network model to construct a new S-box with strong nonlinearity and pseudo-random properties.
3) Using the generated S-box, create a robust and hardware-friendly compressive sensing model (suitable for practical application). It should be noted that this concept has not yet been reported in previous works. Meanwhile, it opens up a new application scenario for the S-box.
4) Develop a compression-encryption scheme for medical data that incorporates the designed compressive sensing model as well as the memristive autapse-synapse neuron model; and evaluate the effect of the memristive synapse-autapse neural network coupling strength on the security of the medical data.

This paper is arranged in the following sections in addition to the introductive Section I. The construction method of the proposed memristive autapse-synapse neural network is presented in Section II. Its dynamics is analyzed with the help of some well-known tools. Section III describes the designed method of the s-box using the memristive autapse-synapse neural network. In Section IV the compressive sensing encryption based on the memristive autapse-synapse neural network is presented with the results. Finally, the work is summarized in Section V.

II. The Memristive Autapse-Synapse Neuron Model

A. Model description

The memristor is the fourth missing electronic component, beside the inductor, the capacitor, and the resistor. It is mainly

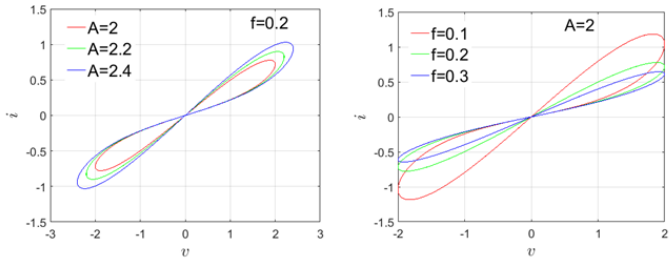

Fig. 1: Hysteresis representation of the proposed memristor exploited for autapse-synapse.

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.

$$\begin{cases} i = G(w)v = \alpha w v \\ \frac{dw}{dt} = g(w,v) = \gamma v + \beta \cos(w) \end{cases} \tag{1}$$

In Eq.1, the term $G(w)$ represents the memductance of the memristor, while $g(w,v)$ the evolution of that inner variable of the memristor. By applying various sinusoidal excitation of the form $v = A\sin(2\pi Ft)$ on the designed memristor with $\alpha = 0.1$, $\beta = 1$, $\gamma = 0.2$, the pinched hysteresis loop in the voltage-current plane of the memristor is established (Fig.1). Consequently the memristor model is suitable to design memristive synapse-autapse neuronal models.

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 and is quite simple than the 3-D model.

$$\begin{cases} \dot{x}_1 = y_1 - a_1 x_1^3 + b_1 x_1^2 + I_1 \\ \dot{y}_1 = c_1 - d_1 x_1^2 - y_1 \end{cases} \tag{2}$$

Another classical neuronal model presented and analyzed in the literature is the FitzHughNagumo (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.

$$\begin{cases} \dot{x}_2 = x_2 - d_2 x_2^3 - y_2 + I_2 \\ \dot{y}_2 = c_2(a_2 + x_2 - b_2 y_2) \end{cases} \tag{3}$$

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

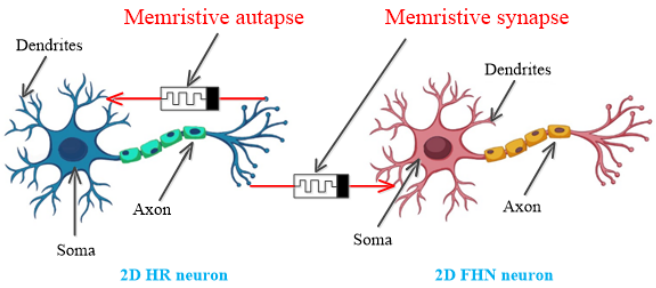

Fig. 2: Synoptic representation of the coupling principle though memristive synapse and autapse.

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 following the synoptic representation of Fig2.

$$\begin{cases} \dot{x}_1 = y_1 - a_1 x_1^3 + b_1 x_1^2 + I_1 - \alpha w_2 (x_1 - x_2) - \alpha w_1 x_1 \\ \dot{y}_1 = c_1 - d_1 x_1^2 - y_1 \\ \dot{w}_1 = \gamma x_1 + \beta \cos(w_1) \\ \dot{x}_2 = x_2 - d_2 x_2^3 - y_2 + I_2 + \alpha w_2 (x_1 - x_2) \\ \dot{y}_2 = c_2 (a_2 + x_2 - b_2 y_2) \\ \dot{w}_2 = \gamma (x_1 - x_2) + \beta \cos(w_2) \end{cases} \tag{4}$$

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]. In this model x_i represent the fast variable or the potential membrane and indicate the slow variable or the ion current (Na+ or K+). w_i stand for the inner variable of the memristive autapse as well as the memristive synapse. α, β and γ represent the parameters of the memristive synapse and autapse. a_i, b_i, c_i, I_i and d_i are traditional parameter of the neuron model defined by Eq.5 for invariant parameters.

$$\begin{cases} a_1 = 1; b_1 = 3; c_1 = 1; d_1 = 5 \\ a_2 = 1; b_2 = 0.1; c_2 = 0.1; d_2 = 1/3 \end{cases} \tag{5}$$

B. 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 [11]. Based on a global bifurcation analysis, the complex behaviors of the introduced model can be easily investigated. It should be noted that the investigation of stability of the model revealed that it is equilibrium free, therefore the considered neuron models exhibits hidden Dynamic.

Lyapunov exponent graphs with two parameters are used to quickly explore the global dynamics of the coupled neurons. These graphs are created by jointly increasing two parameters of the coupled neurons from a minimum to a maximum value. The maximum Lyapunov exponent is estimated with the Wolf algorithm [12] at each step of the variation and plotted on the same graph. The two-parameter Lyapunov diagrams of Fig. 3

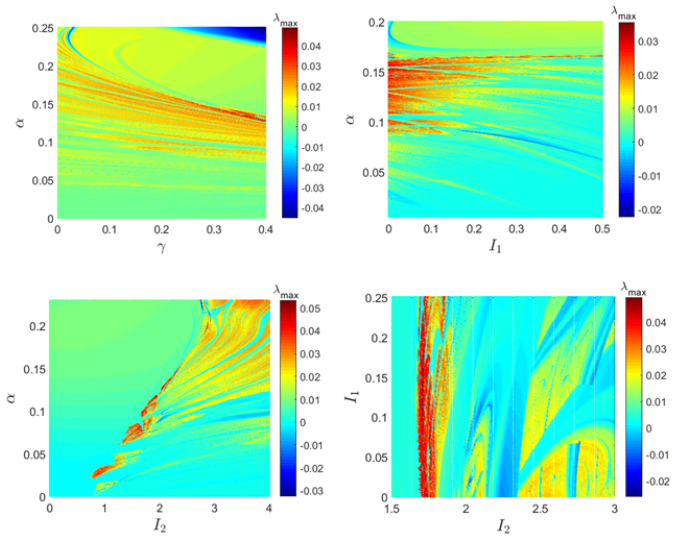

Fig. 3: Two-parameter diagrams obtained when two parameters of the coupled neurons are simultaneously varied. The (γ, α) is obtained for $I_1 = 0.1, I_2 = 2.5$. The (I_1, α) is obtained for $\gamma = 0.2, I_2 = 2.5$. The (I_2, α) is obtained for $\gamma = 0.2, I_1 = 0.1$. And the (I_2, I_1) is obtained for $\gamma = 0.2, \alpha = 0.1$. Initial conditions are $(0.1, 0.1, 0.1, 0.1, 0.1, 0.1)$.

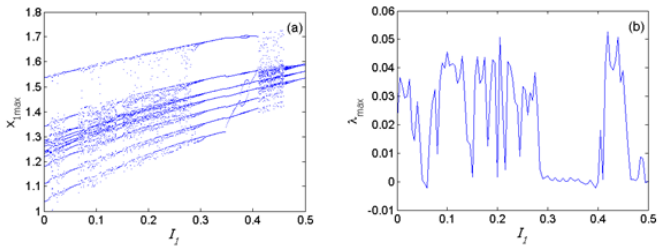

Fig. 4: (a) Bifurcation diagram showing the local maxima of the state variable of the membrane potential of the first neuron versus the extemal current I_1. The corresponding graph of the maximum Lyapunov exponent is present in (b). These diagrams are obtained for $I_2 = 1.75, \gamma = 0.2, \alpha = 0.1$. Initial conditions are $(0.1, 0.1, 0.1, 0.1, 0.1, 0.1)$.

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 $\lambda_{\max} \leq 0$, and irregular behaviors with $\lambda_{\max} > 0$. Using the parameters of the fourth two-parameter diagrams as argument (the plane (I_2, I_1)), the bifurcation plot of Fig. 4 and the corresponding plot of the maximum Lyapunov exponent have been evaluated.

From that bifurcation diagram, it is obvious that the dynamic behavior of the coupled neuron when the external current I_1 of the neuron is varied changes from chaotic to periodic behavior through several chaotic and periodic windows. For some discrete values of I_1 the chaotic and periodic phase portrait of Fig.5 have been computed to further support the irregularity and the regularity of the patterns found in the coupled neurons via a memristive autapse-synapse. The Lyapunov exponents corresponding to the chaotic state of Fig.5-a have been computed. The outcome shows the following values $\lambda_1 = 0.0525859$, $\lambda_2 = -0.00174098$, $\lambda_3 = -0.227193$, $\lambda_4 = -0.867789$, $\lambda_5 = -1.06122$, $\lambda_6 = -2.98989$. From these values we computed the Kaplan-York dimension (KY) as $DK = 2 + (\lambda_1 + \lambda_2)/\lambda_3$ and the result produces $DK =$

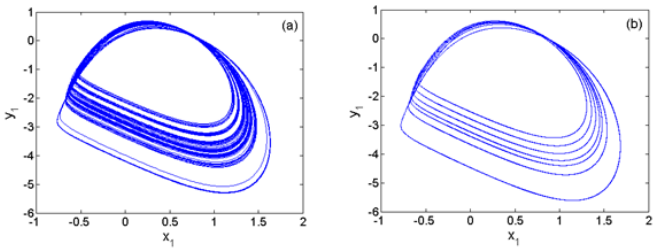

Fig. 5: (a) Chaotic phase portrait obtained for $I_1 = 0.2$ while (b) represents the periodic phase portrait obtained for $I_1 = 0.5$

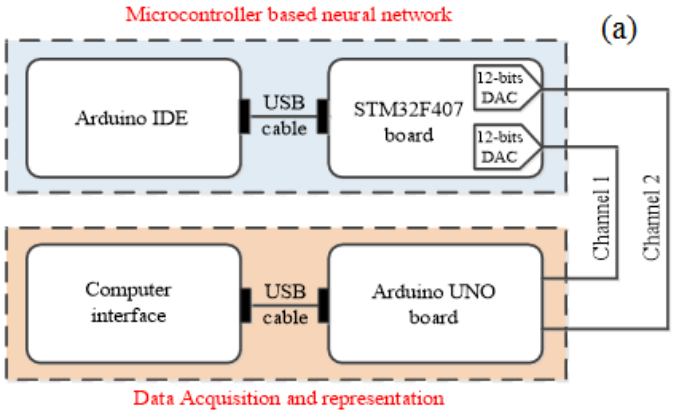

Fig. 6: (a) The topology of the Microcontroller implementation. (b) Experimental setup of the proposed neural network model.

2.2237. This value simply shows that, the attractor in Fig.5-a presents chaotic state of the memristive autapse-synapse neural network.

C. Microcontroller Implementation of the neural network

Two main techniques are usually exploited to implement neural network model namely analogue techniques and digital techniques. Analogue techniques exploit some off-the shell electronic component such as resistors, capacitors, inductors and operational amplifiers to reproduce the dynamics of neural network models. Analogue techniques are very sensitive to temperature variation of the components used. In addition, noise significantly affects the results in this case. Digital techniques use some numerical environment to implement neural network models. Some of the well-known environments include STM board, Arduino board, FPGA board just to name few. In this work STM32F407 and Arduino UNO to implement

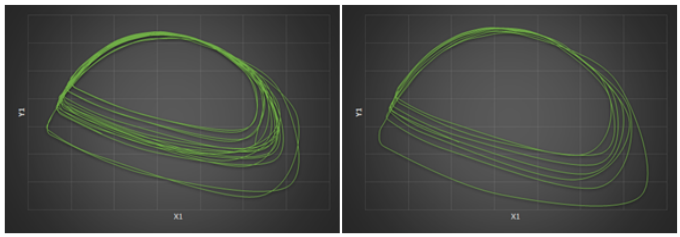

Fig. 7: Experimental phase portrait obtained from the microcontroller implementation of the proposed neural network. These results are obtained using the same values that enable to obtain the results in Fig.3.

the neural network model following the synoptic diagram of Fig.6-(a) These boards are low cost and open source microcontroller environments for digital electronic systems and applications. The experimental configuration is given in Fig.6-(b). STM32F407 is used jointly with the Runge-Kutta algorithm to solve the neural network model. Arduino UNO which is connected to the DAC (digital to analogue) pins of the STM32F407 to construct the data acquisition system. A computer interface is used jointly with the acquired data to plot the corresponding phase portrait in real time (Fig.7).

III. Description of newly designed S-box

A. S-box generation algorithm

This section is concerned with the description of the proposed method with which the optimized S-box gets generated. 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 8×8 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 $[0, 2^8 - 1]$. The random nature of S-boxe generated doesnt guarantee the yielding of strong components [16]. 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 Fit_S considered in the proposed work to evolve the S-box for better security performance has the form of Eq.6.

$$Fitness function : Fit_S = NL(S) + 256 - DU(S) \quad (6)$$

Algorithm 1: Generation of S-box with optimized fitness

Data: Initial parameters of memristive synapse-autapse neuron model parameters; positive integers T, C_1, C_2; maximum number of passes $PASS_{max}$.
Result: S-box S_{optm}.

Initialization:
1. Take empty array $SB = [\,]$; set flag $yes = 1$.
2. Solve the memristive autapse synapse neuron model in the chaotic range to obtain $x_1, y_1, w_1, x_2, y_2, w_2$ with T elements and discard all but keep the last state.
while yes **do**
  3. Solve the memristive autapse synapse neuron model in the chaotic range to obtain $x_1, y_1, w_1, x_2, y_2, w_2$.
  4. Compute $u = [\text{floor}(x_1 \times 10^{14})] \text{mod}\,(256)$
  if *value* u *doesn't belong to array* SB **then**
    append value u in array SB
  end
  if *array* SB *contains* 256 *elements* **then**
    5. Set $yes = 0$, and $Fit_{SB} = Fitness\,(SB)$
  end
end

Fitness Refinement:
for $i = 1$ *to* $PASS_{max}$ **do**
  6. Solve the memristive autapse synapse neuron model in the chaotic range to obtain $x_1, y_1, w_1, x_2, y_2, w_2$.
  7. Compute $C_1 = [C_1 + \text{floor}(x \times 10^{14})] \text{mod}\,(256) + 1$
  8. Compute $C_2 = [\text{floor}((x_1 + y_1) \times 10^{14})] \text{mod}\,(256)$
  9. Compute $C_3 = bitxor\,(SB\,(C_1), C_2)$
  10. Find C_4 such that $SB\,(C_4) = C_3$
  11. Exchange $SB\,(C_4)$ with $SB\,(C_1)$
  12. Set $S_{optm} = SB$
  13. Evaluate fitness of S_{optm} as: $Fit_{optm} = Fitness\,(S_{optm})$
  if $(Fit_{optm} \geq Fit_{SB})$ **then**
    14. $SB = S_{optm}$ and $Fit_{SB} = Fit_{optm}$
  end
end
15. Final S-box is S_{optm} with fitness Fit_{optm}

B. S-box performance analysis

The security evaluation of the above described S-box is crucial to judge the performance against some well accepted parameters. The S-box method is implemented with the following settings: $e_0 = 0.123, f_0 = 0.234, g_0 = 0.345, a = 3.72, b = 0.98$, $t = 0.00001, T = 100, C_1 = C_2 = 34, PASS_{max} = 100,000$. The S-box obtained after executing the Algorithm 1 is presented in Table I. The cryptographic properties of the S-box are assessed by quantifying the performance parameters 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 the most important of these metrics (Nonlinearity and Differential uniformity) for security evaluation [16].

TABLE I: 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	203	235	176	70	253	24	152	138	243	185	54	248	219	207	241	102
2	105	38	168	211	36	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

TABLE II: Nonlinearities of Boolean functions of optimized S-box.

f_i	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	min	max	$average$
$NL\,(f_i)$	110	112	110	112	110	112	112	112	110	112	111.25

1) Nonlinearity: Evaluating the nonlinearity transformation of data from the plaintext 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. The nonlinearity is usualy evaluated with the help of Eq.7.

$$NL(f) = 128 - 0.5\left(\max_{w \in \{0,1\}^8} |S_f(w)|\right) \tag{7}$$

$S_f\,(z)$ indicates the Walsh spectrum of the 8-bit boolean function f, which is provided on Eq.8

$$S_f(w) = \sum_{u \in \{0,1\}^8} (-1)^{f(u) \oplus u.w} \tag{8}$$

Here, $u.w$ is the bitwise dot product of two 8-bit vectors. In this work the results of nonlinearity are presented in Table II. The proposed S-box showed a decent nonlinearity behavior as it has minimum NL value (110), maximum NL value (112) and average NL value (111.25). It is evident that all nonlinearity scores are all greather than 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.

2) Differential uniformity: The resistivity of S-Box against the differential cryptanalysis (DC) is estimated by differential uniformity. The attack analysis is connected with existing imbalance on the input or output scattering to attack block ciphers and S-boxes. If the EX-OR of each output has identical uniformity with the value of EX-OR of each input contradictorily the cryptanalysis can succeed. 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 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

TABLE III: 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
[17]	108	110	108.75	10	0.4946	102.28	0.1328
[18]	105	107	106	12	0.5066	103	0.1445
[19]	104	110	107	12	0.5004	102.85	0.1328
[20]	96	106	102.5	10	0.5037	103.9	0.1250

DC. For an S-box S, the differential uniformity is measured with Eq.9:

$$DU(S) = \max_{\delta m \neq 0, \delta n} \left(\# \left\{ w \in X | S(m) \oplus S(m \oplus \delta m) = \delta n \right\} \right) \tag{9}$$

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 result shows that the biggest value is 8 indicating the capbility of the S-box presented in this work to oppose the differential cryptanalysis.

3) S-box performance comparison: This section provides comparison analysis of the proposed S-box with other recent methods. Table III is maintained to have a view of scores of all significant performance parameters of some recent works. The superiority of the proposed S-box is both based on the utilization of a memristive synapse-autapse neural network with a composite fitness function which optimizes nonlinearity as well as the differential uniformity measure. As can be seen from the comparison Table III that the proposed S-box shows excellent nonlinearity and differential uniformity as compared to all other S-boxes. The average NL of the memristive autapse-synapse based S-box is 111.25 which is considerably above the values presented in some recent works [17, 18, 19, 20].This is also the case for the differential uniformity as well since it is the lowest (i.e. better) compared to the S-boxes methods cited in the same table (Table III). Additionally, the memristive autapse-synapse based S-box satisfies the SAC criterion in quite better manner compared to the SAC results in some top works cited in Table III. The bits independence criterion is also gets satisfied as the BIC-NL for memristive autapse-synapse based S-box is 104.357 which is better than the scores found in S-boxes of [17, 18, 19, 20]. Similarly, our linear approximation probability is 0.1328 which is comparable to many S-boxes of Table III in robustness against withstanding the linear cryptanalysis. Hence, the memristive autapse-synapse based S-box has better security and robustness cryptographic properties compared to many recent S-boxes and it is well suitable for its usage in cryptographic applications.

IV. Image Cryptosystem Using Both the Memristive Autapse-Synapse Neural Network and S-box Based Block Compressive Sensing

A. Proposed method

This section will provide an application of newly designed autapse-synapse neural network model in privacy data protection with the assistance of S-box based block compressed sensing technology. The workflows of proposed image encryption and corresponding decryption schemes are drawn in Fig. 8. Then, the whole technical details are listed as hereunder mentioned.

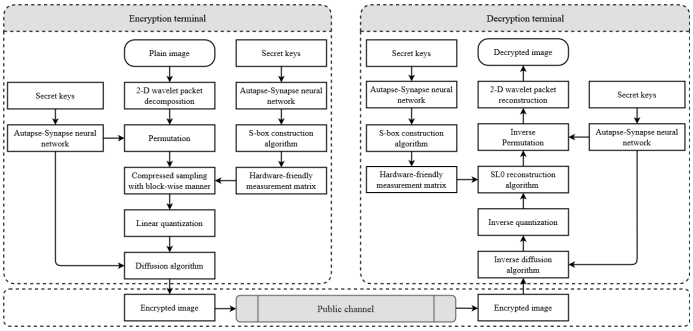

Fig. 8: Workflow of the proposed image cryptosystem

Step 1. First, to be capable of performing compressed sampling on the plain image $P1 \in \mathbb{N}^{n \times n}$ through 2-D measurement matrix, it is sparsely represented using the multi-layer wavelet packet decomposition. And the corresponding sparse coefficient matrix is denoted as $P2 \in \mathbb{R}^{n \times n}$.

Step 2. Then, the coefficient matrix $P2$ is shuffled with good scrambling effect, thereby spreading its principal components uniformly to each column. This process can be elaborated into Eq.10, where the symbols $z_1 \in \mathbb{N}^{n \times n}$ and $z_2 \in \mathbb{N}^{n \times n}$ are the index sequences generated by sorting the output values of new synapse-autapse memristive neural network model. And the symbol "mod" means the modulus operator.

$$\begin{cases} \begin{bmatrix} k \\ t \end{bmatrix} = \mathrm{mod}\left(\begin{bmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{bmatrix} \times \begin{bmatrix} i \\ j \end{bmatrix}, \begin{bmatrix} n \\ n \end{bmatrix} \right) \\ P_3(i,j) = P_2(k,t) \end{cases} \tag{10}$$

with z_{ij} $(i = 1...2\,;\, j = 1...2)$ defined as $z_{11} = 1$; $z_{12} = z_1$; $z_{21} = z_2$; $z_{22} = z_1.z_2 + 1$.

Step 3. Next, the proposed memristive autapse-synapse neural network is adopted to construct the S-box following Algorithm 1. Afterward, according to Algorithm 2, the small-scale measurement matrix Φ consisting of -1 and 1 is obtained. The measurement matrix generated is more hardware friendly than some chaotic measurement matrix and the randomly structured measurement matrix [21].

Step 4. The matrix $P3$ is partitioned into several non-overlapping blocks of size $n/N \times n/N$. Where, $N = n/64$. Then, each block is linearly projected onto the measurement matrix Φ and the resulting values are concatenated to obtain the compressed matrix $P4$. Later, it is linearly quantized to the interval $[0, 255]$. This process can be expressed as Eq.11.

$$P5 = 255 \cdot (P_4 - \min(P_4)) \cdot (\max(P_4) - \min(P_4))^{-1} \tag{11}$$

Step 5. Under the control of sequences $\{d_i\}_{i=1}^{2}$ constructed by new memristive synapse-autapse neural network model, the compressed image $P5$ is subjected to the bidirectional diffusion to obtain the final encrypted image $C \in \mathbb{N}^{0.5n \times n}$.

This process can be expressed as Eq.12 and Eq.13, where the vectors $\{s_i\}_{i=1}^{2} = \left(\left(\{d_i\}_{i=1}^{2} + 10\right) \times 10^{10}\right) \bmod 256$.

$$P6(i) = (P6(i-1) + P5(i) + s_1(i)) \bmod 256 \quad (12)$$

$$C(i) = (C(i+1) + P6(i) + s_2(i)) \bmod 256 \quad (13)$$

Algorithm 2: Construction of the measurement matrix

Data: Memristive synapse-autapse neuron model parameters; measurement matrix dimension $(n/2N, n/N)$.
Result: Measurement matrix Φ.
1. Initialize an unsigned 8-bit integer variate pt with size of *(1,256)*, whose elements are all equal to zero.
2. Initialize a floating-point variate phi, whose elements are all equal to zero.
3. $pt = SB\,([e_0, f_0, g_0])$
for $i = 1{:}256$ **do**
  4. $tmp = dec\,2\,bin(pt(i), 8)$;
  5. $num = 1$
  for $i = 7{:}{-}1{:}0$ **do**
    6. $phi\ (8i - j) = \mathrm{str}\,2\,num(tmp(\ num\ ))$;
    7. $num = num + 1$;
  end
end
8. Initialize $\Phi = phi$ and rearrange it as size $(n/2N, n/N)$ with column-wise manner.
9. Arrange the element value equal to zero in matrix Φ to be -1.

The encrypted image can be decrypted and decompressed to acquire the accurately reconstructed image with the reverse encryption method as shown in Fig. 8.

B. Performance evaluation

This section is devoted to 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 256×256) are selected from the free medical images data base *MedPix* (*https://medpix.nlm.nih.gov/home*). The proposed memristive autapse-synapse neural network model is solved (with the parameters of Fig.5-a) using the fourth-order Runge-Kutta algorithm to yield chaotic sequences useful in the compression-encryption-decryption stages. The algorithm is applied on the test images (each of size 256×256) and the results of compression-encryption-decryption-reconstruction is presented on Fig.9 where the first column contains the original input medical data (each of size 256×256). The second column contains the compressed encrypted medical data (each of size 128×256) . The third column contains the results of decryption-reconstruction. Three observations can emerge from these results. **(1)** The output of the compression provides

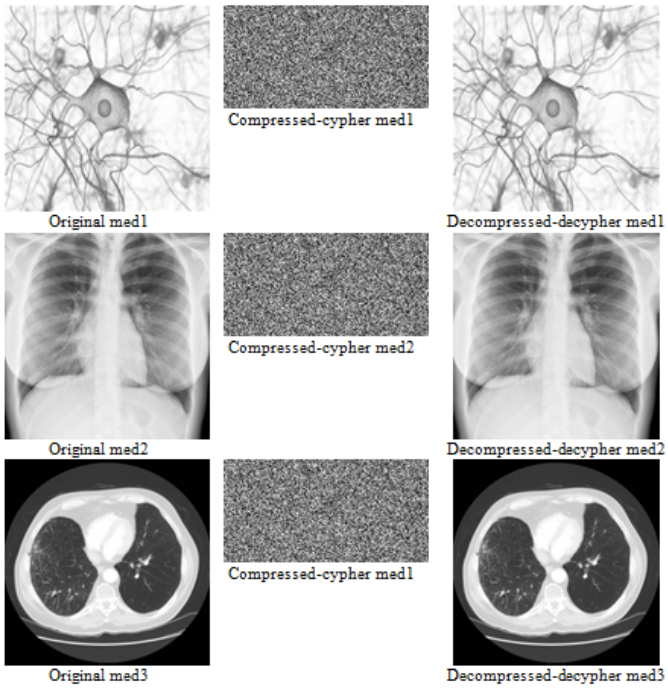

Fig. 9: Results of compression-encryption-decryption-reconstruction processes

images each of size 128×256 when each inputs images is of size 256×256. 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.

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 [15]. 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.10 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.

2) Correlation coefficients analysis: Another efficient tool to evaluate the capability of an algorithm to resist statistical attacks is correlation coefficient [22]. 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 $+1$. 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

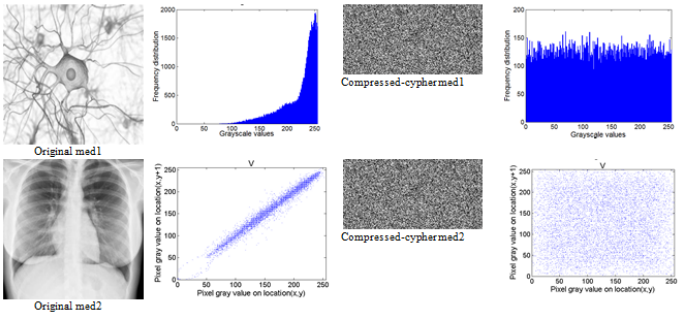

Fig. 10: Original input data with respectve ciphers and the corresponding histograms

TABLE IV: Security performances of the proposed work.

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	33.5107	38.2963	0.9278
Compressed-cypher med3	0.0005	−0.0009	−0.0025	7.9018				

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.14.

$$C_{i,j} = \frac{A[(i-A(i))(j-A(j))]}{\sqrt{B(i)}\sqrt{B(j)}}$$
$$with\ \ A(i) = \frac{1}{n}\sum_{x=1}^{n} i_x\ ,\ \ B(i) = \frac{1}{n}\sum_{x=1}^{n}(i_x - A(i))^2 \tag{14}$$

Table IV 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 data are close to zero indicating that the method has destroyed the correlation between the pixels of the plain images. Consequently the proposed algorithm produces data that can resist statistical attacks.

3) Compression performance analysis: 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 [23]. 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. In image and video compression, considering 8-bits data, the PSNR should belong to the set $[30\,;\,50]$ to allow human perception. SSIM measures the degradation of the plain input data in terms of luminance and contrast. Table IV 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.

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 [24]. 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.15.

$$GE(i) = \sum_{x=1}^{2^n-1} p(i_x)\log_2\frac{1}{p(i_x)} \tag{15}$$

For 8-bits image the threshold value of the entropy is 8. Eq.15 has been exploited to compute the entropy values for the three medical plain images and the corresponding ciphers. The results are presented in Table IV. From this table it is observed that the entropy scores of cipher is around the threshold value 8 compare to the entropy values of the plain input images. Consequently the proposed algorithm can resist unauthorized intrusion.

5) NPCR and UACI analyses: NPCR and UACI are two metrics exploited to quantify the capability of the memristive autapse-synapse based method to resist differential attacks [24]. In such intrusion unauthorized party create one pixel difference in the image and exploit this difference to obtain the acquaintance between the plain input and the corresponding cipher image. Considering a plain image and the corresponding cipher, The $NPCR$ and the $UACI$ can be obtained as the cipher of the same plain image with just one different pixel. And these metrics are usually computed using Eq.16 and Eq.17.

$$UACI = \frac{100}{xy}\sum_{i=1}^{x}\sum_{j=1}^{y}\frac{|C_{r_2}(i,j) - C_{r_1}(i,j)|}{255} \tag{16}$$

$$NPCR = \frac{100}{xy}\sum_{i=1}^{x}\sum_{j=1}^{y} Diff(i,j)\ ;$$

$$where\ Diff(i,j) = \begin{cases} 1 & for\ C_{r_1}(i,j) \neq C_{r_2}(i,j) \\ 0 & for\ C_{r_1}(i,j) = C_{r_2}(i,j) \end{cases} \tag{17}$$

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.16 and Eq.17 have been exploited in this work to compute both $NPCR$ and $UACI$. The outcomes are shown in Table IV from where the results are very close to the threshold values. This simply indicates that the proposed algorithm can resist differential attack.

V. Conclusion

The dynamics of two different neurons, coupled with both memristive synapse and memristive autapse, was first considered in this work. Then using Lyapunov exponent, bifurcation, Kaplan-York dimension and phase portrait as dynamical analysis methods, it was established that the model is capable of displaying various windows of both chaotic and periodic attractors with the variation of the coupling strength. Afterward, the S-box controlled by the coupled memristive neuron model has been exploited in chaotic windows to construct a hardware-friendly measurement matrix for medical image compression, followed by a series of encryption procedures. Ultimately, it can be concluded from the extensive experimental results and analysis that the proposed medical data protection scheme is secure enough and can be useful in real applications.

REFERENCES

[1] S. H. Sung, T. J. Kim, H. Shin, T. H. Im, and K. J. Lee, "Simultaneous emulation of synaptic and intrinsic plasticity using a memristive synapse," *Nature Communications*, vol. 13, no. 1, pp. 1–12, 2022.

[2] L. F. Abbott and T. B. Kepler, "Model neurons: from hodgkin-huxley to hopfield," in *Statistical mechanics of neural networks*. Springer, 1990, pp. 5–18.

[3] M. Nouri, G. R. Karimi, A. Ahmadi, and D. Abbott, "Digital multiplierless implementation of the biological fitzhugh–nagumo model," *Neurocomputing*, vol. 165, pp. 468–476, 2015.

[4] X. Song, H. Wang, and Y. Chen, "Autapse-induced firing patterns transitions in the morris–lecar neuron model," *Nonlinear Dynamics*, vol. 96, no. 4, pp. 2341–2350, 2019.

[5] J. Cai, H. Bao, Q. Xu, Z. Hua, and B. Bao, "Smooth nonlinear fitting scheme for analog multiplierless implementation of hindmarsh–rose neuron model," *Nonlinear Dynamics*, vol. 104, no. 4, pp. 4379–4389, 2021.

[6] Q. Xu, X. Tan, D. Zhu, H. Bao, Y. Hu, and B. Bao, "Bifurcations to bursting and spiking in the chay neuron and their validation in a digital circuit," *Chaos, Solitons & Fractals*, vol. 141, p. 110353, 2020.

[7] B. Bao, C. Chen, H. Bao, X. Zhang, Q. Xu, and M. Chen, "Dynamical effects of neuron activation gradient on hopfield neural network: Numerical analyses and hardware experiments," *International Journal of Bifurcation and Chaos*, vol. 29, no. 04, p. 1930010, 2019.

[8] E. Tlelo-Cuautle, A. M. González-Zapata, J. D. Díaz-Muñoz, L. G. de la Fraga, and I. Cruz-Vega, "Optimization of fractional-order chaotic cellular neural networks by metaheuristics," *The European Physical Journal Special Topics*, pp. 1–7, 2022.

[9] Z. T. Njitacke, S. D. Isaac, T. Nestor, and J. Kengne, "Window of multistability and its control in a simple 3d hopfield neural network: application to biomedical image encryption," *Neural Computing and Applications*, vol. 33, no. 12, pp. 6733–6752, 2021.

[10] M. R. Razvan and S. Yasaman, "Emergence of bursting in two coupled neurons of different types of excitability," *Chaos, Solitons & Fractals*, vol. 132, p. 109482, 2020.

[11] H. Lin, C. Wang, Q. Deng, C. Xu, Z. Deng, and C. Zhou, "Review on chaotic dynamics of memristive neuron and neural network," *Nonlinear Dynamics*, vol. 106, no. 1, pp. 959–973, 2021.

[12] Z. T. Njitacke, C. N. Takembo, J. Awrejcewicz, H. P. E. Fouda, and J. Kengne, "Hamilton energy, complex dynamical analysis and information patterns of a new memristive fitzhugh-nagumo neural network," *Chaos, Solitons & Fractals*, vol. 160, p. 112211, 2022.

[13] Y. Tan and C. Wang, "A simple locally active memristor and its application in hr neurons," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 30, no. 5, p. 053118, 2020.

[14] B. Parameshachari, H. Panduranga *et al.*, "Medical image encryption using scan technique and chaotic tent map system," in *Recent Advances in Artificial Intelligence and Data Engineering*. Springer, 2022, pp. 181–193.

[15] Z. T. Njitacke, N. Tsafack, B. Ramakrishnan, K. Rajagopal, J. Kengne, and J. Awrejcewicz, "Complex dynamics from heterogeneous coupling and electromagnetic effect on two neurons: Application in images encryption," *Chaos, Solitons & Fractals*, vol. 153, p. 111577, 2021.

[16] M. Ahmad and Z. Ahmad, "Random search based efficient chaotic substitution box design for image encryption," *International Journal of Rough Sets and Data Analysis (IJRSDA)*, vol. 5, no. 2, pp. 131–147, 2018.

[17] T. Zhang, C. P. Chen, L. Chen, X. Xu, and B. Hu, "Design of highly nonlinear substitution boxes based on i-ching operators," *IEEE transactions on cybernetics*, vol. 48, no. 12, pp. 3349–3358, 2018.

[18] V. Silva-García, R. Flores-Carapia, C. Rentería-Márquez, B. Luna-Benoso, and M. Aldape-Pérez, "Substitution box generation using chaos: An image encryption application," *Applied Mathematics and Computation*, vol. 332, pp. 123–135, 2018.

[19] Ü. Çavuşoğlu, "S-box-based video stenography application of variable-order fractional hopfield neural network (vfhnn)," *The European Physical Journal Special Topics*, pp. 1–19, 2022.

[20] A. A. Abd 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.

[21] T. N. Canh and B. Jeon, "Restricted structural random matrix for compressive sensing," *Signal Processing: Image Communication*, vol. 90, p. 116017, 2021.

[22] Y. Ding, G. Wu, D. Chen, N. Zhang, L. Gong, M. Cao, and Z. Qin, "Deepedn: a deep-learning-based image encryption and decryption network for internet of medical things," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1504–1518, 2020.

[23] D. Tellez, G. Litjens, J. van der Laak, and F. Ciompi, "Neural image compression for gigapixel histopathology image analysis," *IEEE transactions on pattern analysis and machine intelligence*, vol. 43, no. 2, pp. 567–578, 2019.

[24] Y. Xu and J. Zhang, "Invertible resampling-based layered image compression," in *2021 Data Compression Conference (DCC)*. IEEE, 2021, pp. 380–380.

[25] 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.

[26] Y. Zhang, R. Zhao, Y. Zhang, R. Lan, and X. Chai, "High-efficiency and visual-usability image encryption based on thumbnail preserving and chaotic system," *Journal of King Saud University-Computer and Information Sciences*, 2022.

[27] H. Ren, S. Niu, J. Chen, M. Li, and Z. Yue, "A visually secure image encryption based on the fractional lorenz system and compressive sensing," *Fractal and Fractional*, vol. 6, no. 6, p. 302, 2022.

[28] X. Huang, Y. Dong, H. Zhu, and G. Ye, "Visually asym-

metric image encryption algorithm based on sha-3 and compressive sensing by embedding encrypted image," *Alexandria Engineering Journal*, vol. 61, no. 10, pp. 7637–7647, 2022.