applied sciences

MDPI

Article

S-Box Based Image Encryption Application Using a Chaotic System without Equilibrium

Xiong Wang [1], Ünal Çavuşoğlu [2], Sezgin Kacar [3], Akif Akgul [4], Viet-Thanh Pham [5,*], Sajad Jafari [6], Fawaz E. Alsaadi [7] and Xuan Quynh Nguyen [8]

1 Institute for Advanced Study, Shenzhen University, Shenzhen 518060, Guangdong, China; wangxiong8686@szu.edu.cn
2 Department of Computer Engineering, Faculty of Computer and Information Sciences, Sakarya University, 54187 Serdivan, Turkey; unalc@sakarya.edu.tr
3 Department of Electrical and Electronics Engineering, Faculty of Technology, Sakarya University, 54187 Serdivan, Turkey; skacar@sakarya.edu.tr
4 Department of Electrical and Electronics Engineering, Faculty of Technology, Sakarya University of Applied Sciences, 54187 Serdivan, Turkey; aakgul@sakarya.edu.tr
5 Nonlinear Systems and Applications, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam
6 Biomedical Engineering Department, Amirkabir University of Technology, Tehran 15875-4413, Iran; sajadjafari@aut.ac.ir
7 Department of Information Technology, Faculty of Computing and IT, King Abdulaziz University, Jeddah 21589, Saudi Arabia; fesalsaadi@kau.edu.sa
8 National Council for Science and Technology Policy, Hanoi, Vietnam; Quynhnx@hactech.edu.vn
* Correspondence: phamvietthanh@tdtu.edu.vn

Received: 21 December 2018; Accepted: 19 February 2019; Published: 22 February 2019

Abstract: Chaotic systems without equilibrium are of interest because they are the systems with hidden attractors. A nonequilibrium system with chaos is introduced in this work. Chaotic behavior of the system is verified by phase portraits, Lyapunov exponents, and entropy. We have implemented a real electronic circuit of the system and reported experimental results. By using this new chaotic system, we have constructed S-boxes which are applied to propose a novel image encryption algorithm. In the designed encryption algorithm, three S-boxes with strong cryptographic properties are used for the sub-byte operation. Particularly, the S-box for the sub-byte process is selected randomly. In addition, performance analyses of S-boxes and security analyses of the encryption processes have been presented.

Keywords: chaos; equilibrium; entropy; circuit; S-box; image encryption

1. Introduction

Previous researches have focused on chaotic systems, which have rich dynamics [1–5]. Chaos is useful for providing mixing and spreading features in cryptography [6–8]. Recent developments have shown an increasing interest in many chaos-based cryptosystems such as chaos-based watermarking [9,10], encryption algorithm over TCP data packets [11], digital image encryption [12], steganography [13], and so on [14–18].

There is a large volume of published works relating to the role of S-box in encryption algorithms [19,20]. S-box is an important unit to provide higher security properties. S-box construction has been the subject of many studies [21–23]. Especially, chaos-based S-boxes have received critical investigation [24–29]. Chaotic S-box has attractive features and is an interesting research topic [30–35]. Based on chaotic maps, Tang et al. designed S-boxes [25]. S-boxes based on tent maps were reported

in [26] while S-boxes based on chaotic Boolean functions was presented in [28]. Strong S-boxes were constructed by using a chaotic Lorenz systems [32]. Hussain et al. proposed a novel approach for designing S-boxes with a nonlinear chaotic algorithm [33]. A chaotic scaled Zhongtang system was applied to generate strong a S-box algorithm [30]. Moreover, by using a time-delay chaotic system, Özkaynak and Yavuz introduced chaotic S-boxes [29].

In this work, we investigate a non-equilibrium system, which attracts interest because its attractor is "hidden" [36–39]. A hidden attractor cannot be localized numerically by a standard computational procedure [38,39]. Because there is no limitation of equilibrium, such a chaotic system without equilibrium is appropriate for the area of information encryption [40]. Chaotic time-series obtained from the proposed system are used to construct S-boxes and develop an image encryption application. In this study, unlike the S-box based encryption algorithms in the literature, S-box production with high randomness bit sequences and strong cryptographic properties is performed using chaotic system based random number generator (RNG) with rich dynamical properties. An algorithm has been proposed that performs pixel-based encryption on image files and uses a different S-box in each cycle with random selection of S-boxes.

2. A Nonequilibrium System with Ten Terms and Its Feasibility

Recently, there has been considerable critical attention on nonequilibium systems with chaos [40–44]. Such chaotic systems are totally different from common chaotic ones, in which there are some unstable equilibrium points. Investigating new chaotic systems without equilibria is a continuing concern [45]. For studying new nonequilibrium systems, we consider a general three-dimensional form:

$$\begin{cases} \dot{x} = a_1 y, \\ \dot{y} = a_2 x + a_3 z + a_4 xz, \\ \dot{z} = a_5 x + a_6 y + a_7 z + a_8 xy + a_9 xz + a_{10}, \end{cases} \tag{1}$$

in which parameters are denoted as a_i $(i = 1, \ldots, 10)$, and $a_i \neq 0$. The origin of the system (1) is based on the published work [42].

By used a search procedure [42], we have found the parameter set (2), for which there is no any real equilibrium in the three-dimensional form (1),

$$\begin{cases} a_1 = a, \\ a_2 = a_7 = a_8 = -1, \\ a_3 = b, \\ a_4 = a_5 = a_{10} = 1, \\ a_6 = c, \\ a_9 = d, \end{cases} \tag{2}$$

with $a, b, c, d > 0$.

Thus, form (1) becomes the following system:

$$\begin{cases} \dot{x} = ay, \\ \dot{y} = -x + bz + xz, \\ \dot{z} = x + cy - z - xy + dxz + 1. \end{cases} \tag{3}$$

It is trivial to confirm that for $a = 2$, $b = 2.5$, $c = 0.2$, and $d = 0.3$ system (3) does not have any real equilibrium. It is noted that there are some sets of values which make a system without real equilibria. We have selected such a set of values because in this case the system is elegant [46–48]. Especially, the system exhibits chaos (see Figure 1). Chaotic dynamics was verified by calculated Lyapunov exponents $L_1 = 0.2376$, $L_2 = 0$, $L_3 = -0.5231$ as presented in Figure 2. For calculating the Lyapunov exponents, we applied the known Wolf's algorithm [49]. Entropy was used to estimate the transfer rate of information in a particular system [50]. Moreover, entropy indicates the level of

chaos in a dynamical system [51,52]. Here we measured the approximate entropy (ApEn) [53,54] for system (3). The calculated approximate entropy of the system without equilibrium (3) is 0.1503, which presents the level of chaotic behavior.

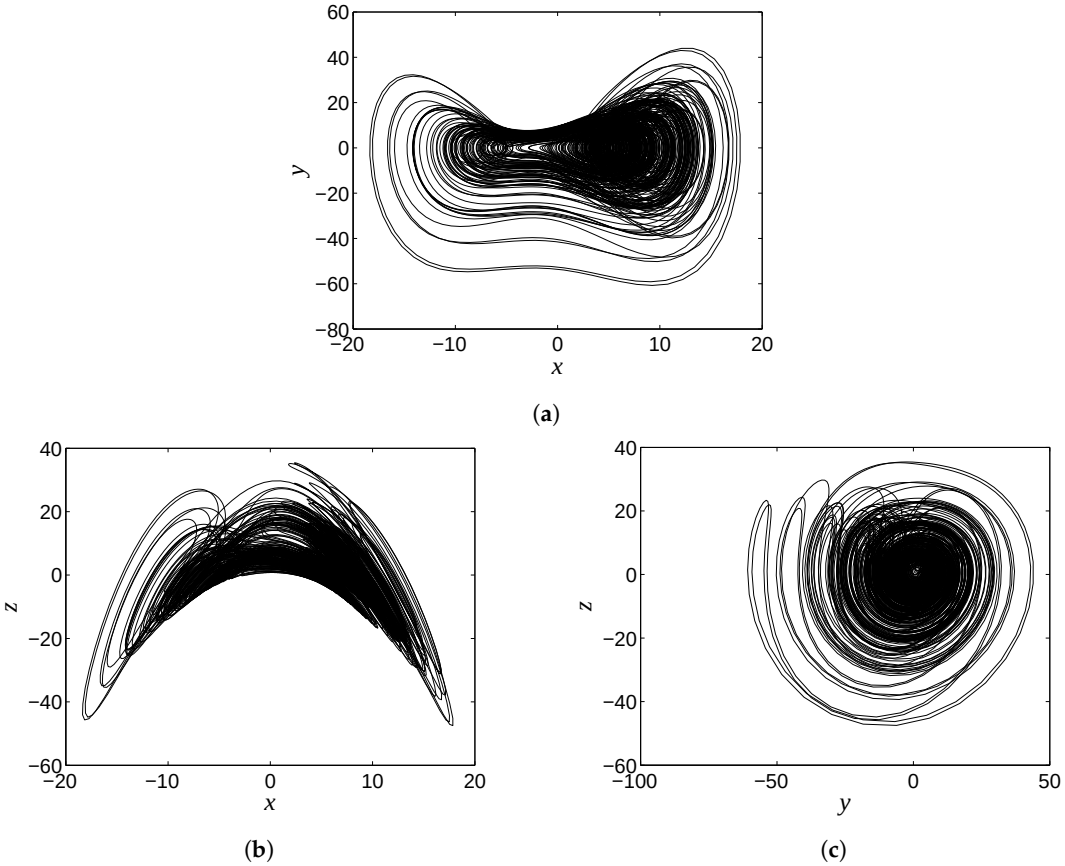


Figure 1. Different attractors without equilibrium in (**a**) $x-y$ plane, (**b**) $x-z$ plane, and (**c**) $y-z$ plane. The parameter set is $a=2$, $b=2.5$, $c=0.2$, $d=0.3$ and initial conditions are $(x(0),y(0),z(0))=(1,1,1)$.

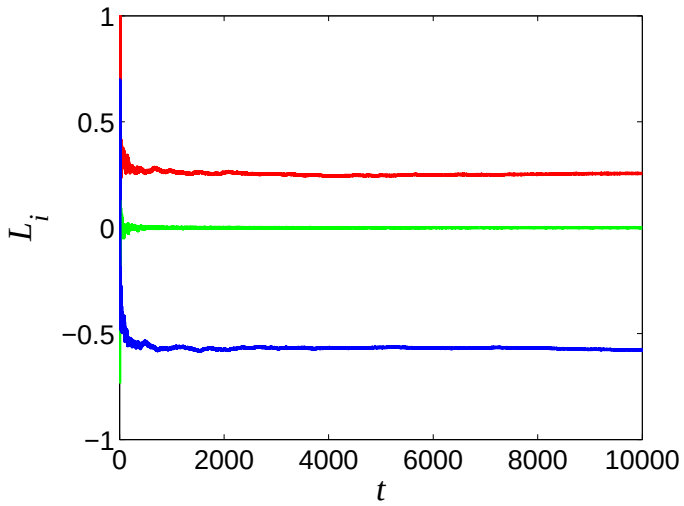


Figure 2. Calculated Lyapunov exponents (L_1 (red), L_2 (green), and L_3 (blue)) of the system when $a=2$, $b=2.5$, $c=0.2$, $d=0.3$ and $(x(0),y(0),z(0))=(1,1,1)$. It is noted that chaos of the system is indicated by $L_1>0$.

Circuit implementation provides an effective tool for verifying the feasibility of theoretical models [55–59]. Therefore, we have designed and realized the nonequilibrium system via a real circuit as shown in Figures 3 and 4. The circuit was implemented with selected components: R1 = 200 kΩ, R2 = R3 = R7 = R8 = R15 = R16 = 100 kΩ, R4 = R9 = R11 = 400 kΩ, R5 = 160 kΩ, R6 = R14 = 8 kΩ, R10 = 2 MΩ, R12 = 30 MΩ, R13 = 26.6 kΩ, and C1 = C2 = C3 = 1 nF. The phase portraits are displayed by the oscilloscope as reported in Figure 5. Figure 1 is a theoretical figure obtained by solving the system at noequilibrium conditions, while Figure 5 was obtained experimentally by using the implemented electronic circuit.

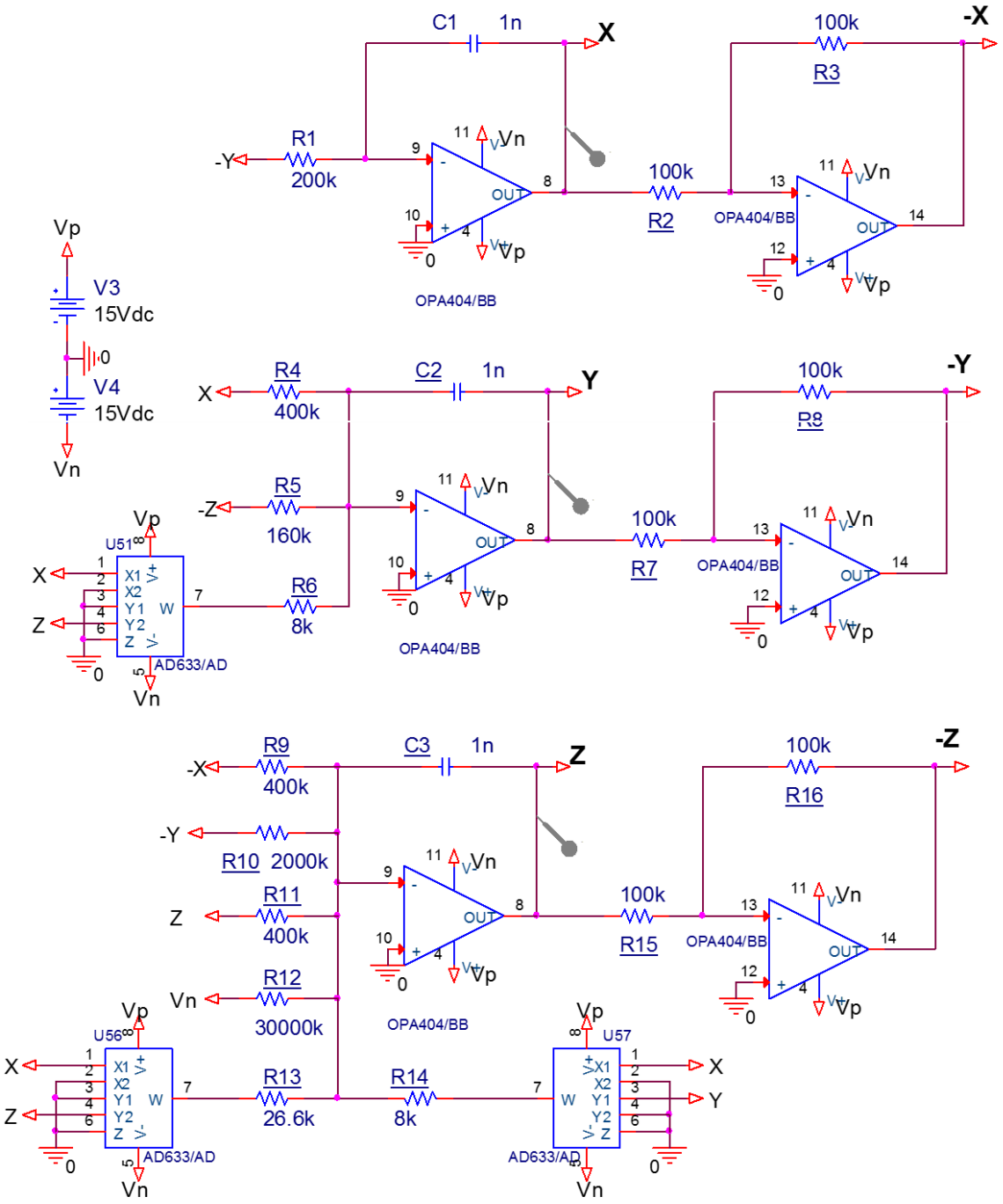
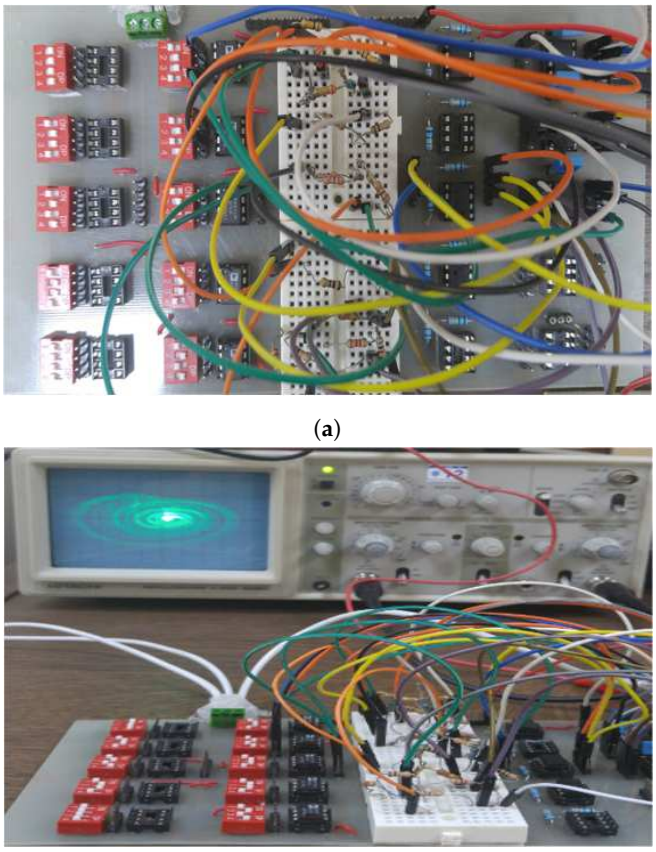


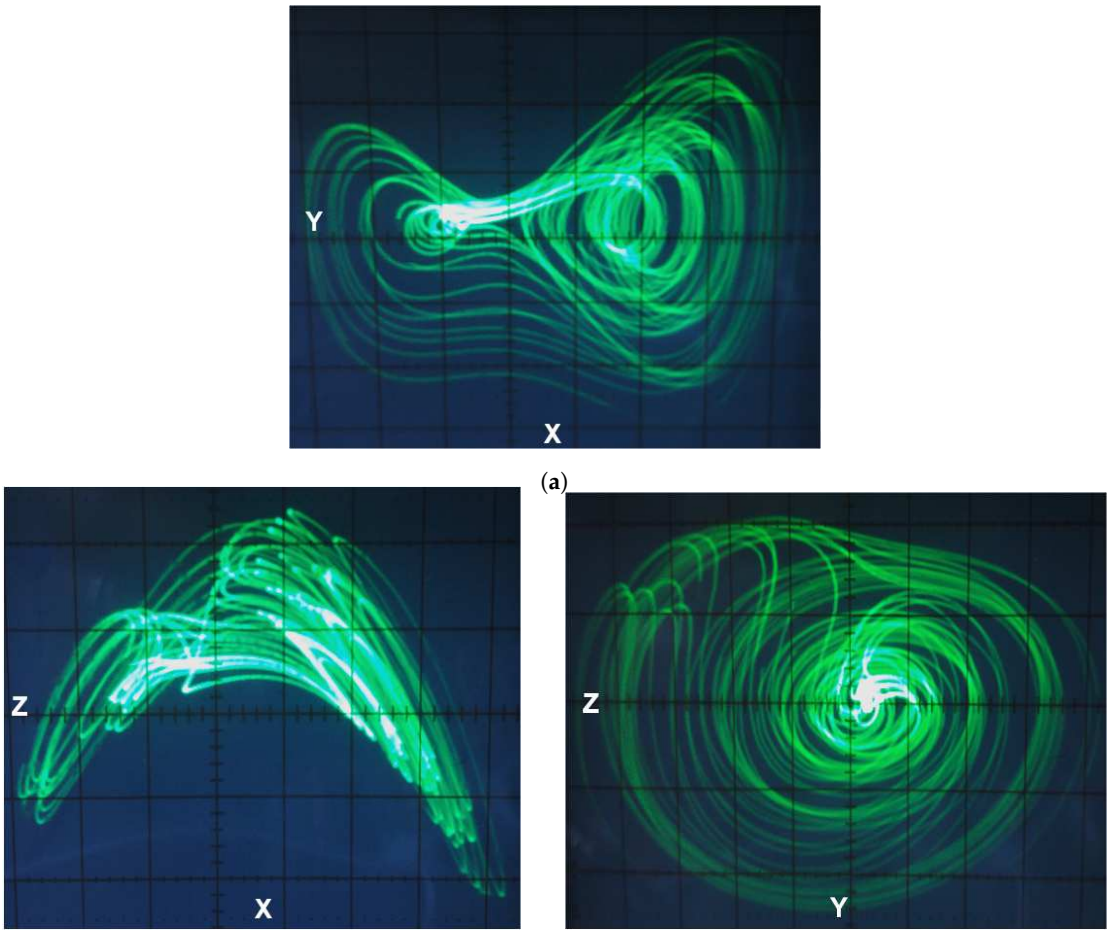
Figure 3. Circuit schematic including electronic components.



(**a**)

(**b**)

Figure 4. Real electronic circuit implemented using a board. (**a**) the electronic board, (**b**) the measurement of the circuit by using the oscilloscope.



(**a**)

(**b**) (**c**)

Figure 5. Experimental attractors displayed by using an oscilloscope in (**a**) $X-Y$ plane, (**b**) $X-Z$ plane, and (**c**) $Y-Z$ plane.

3. The S-Box Generation Algorithm Design and Performance Analysis

S-box is one of the most basic structures used in block encryption algorithms. S-box structures in encryption algorithms are used for byte change operations. In this section, a new S-box production algorithm is designed using the developed chaotic system and new S-box productions are realized. Performance analyses of the produced S-boxes are made and compared with the S-boxes in the literature.

3.1. The S-Box Generation Algorithm Design

In this section, the S-box production algorithm is designed to be used in the encryption algorithm. Three different S-box generations are realized with the S-box production algorithm developed in the study. In the algorithm design, a chaotic system with rich dynamic characteristics introduced to the model is used. The pseudo code block for the algorithm design is shown in Algorithm 1. Firstly, the system parameters (a, b, c, d) and initial conditions $(x(0), y(0), z(0))$ of the chaotic system are entered. Then, in order to obtain a more random output, the appropriate sampling step range is determined. This value is set at 0.001. The chaotic system RK-4 (Runge–Kutta 4) algorithm is solved with the specified sampling step interval. The float values from each phase are obtained from the RK-4 algorithm. The generated float values are taken from the first three digits after the decimal point, and mod-256 operation is applied. Remain and round operations have also been applied to obtain the first three steps after the decimal point. As a result of this process, 0–256 values are obtained from each phase. The values obtained from the x and y phases for the proposed S-box1, x, y and z phases for

S-box2, y and z phases for S-box3 bitxor operation are applied. It is then checked whether the values produced are on the S-box, in other words whether it has been produced before. If produced, this value is discarded, otherwise it is added to the S-box. In this way a 256 element S-box is produced. Subsequently, S-box performance tests are conducted to test the produced S-boxes.

Algorithm 1 S-box generation algorithm pseudo code.

Start
i = 1; SBox=[];
Entering system parameters (a, b, c, d) and initial conditions $(x(0), y(0), z(0))$ of chaotic system
Determination of the appropriate value of Δh (0.001)
Sampling with determination Δh value
Solving the chaotic system using RK4 algorithm and obtaining output time series (ys)
ys → Calculated current values $(ys(1), ys(2), ys(3))$ from RK4 algorithm
while (i<257) **do**
  $x = mod(round2int(remain(ys(1), 1) * 10^3), 256);$
  $y = mod(round2int(remain(ys(2), 1) * 10^3), 256)$
  $z = mod(round2int(remain(ys(3), 1) * 10^3), 256)$
  $xorvalue = bitxor(x, y) \ \ for \ \ SBox1$
  $xorvalue = bitxor(x, y, z) \ \ for \ \ SBox2$
  $xorvalue = bitxor(y, z) \ \ for \ \ SBox3$
  if (Is there xorvalue in SBox = yes) **then**
    Go step 8.
  else {Is there xorvalue in SBox = no}
    SBox[i] ← xorvalue
    i++;
  end if
end while
sbox ← reshape(SBox,16,16) (outputs: SBox1, SBox2, SBox3)
Implementation of SBox Performance Tests (outputs: Nonlinearity, BIC-SAC, BIC-Nonlinearity, SAC, DP)
End

3.2. Performance Analysis Results of Proposed S-Boxes

In order to be able to use the generated S-boxes in the encryption process, performance tests are required. S-box structures with strong cryptographic properties play a major role in encryption. By using the developed S-box generation algorithm, three different S-boxes have been proposed to be used in image encryption processes and the performance tests of these S-boxes have been carried

out. The performance results of the proposed S-boxes are compared with the S-box structures in the literature. The proposed S-box that uses the cryptography process are shown in Tables 1–3. S-box productions are realized using different phases of chaotic systems.

Table 1. The proposed S-box1.

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

Table 2. The proposed S-box2.

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

Table 3. The proposed S-box3.

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

Performance tests have been applied to show the cryptographic performance values of the produced S-boxes. Nonlinearity [21] is one of the most important features in the S-box value evaluation criteria. The min. and max. nonlinearity values of produced S-boxes are found as follows: min. value of 104, max. value of 110 for S-box1; min. value of 104, max. value of 108 for S-box2; min. value of 106, max. value of 108 for S-box3. The min., avg. and max. nonlinearity values of the S-boxes suggested in Table 4 are given. It shows the best values after the Advanced Encryption Standard (AES) algorithm application for the max., min. and avg. nonlinearity values of proposed S-box1, 2 and 3 respectively. The strict avalanche criterion (SAC) is a another important performance measure method that calculates the probability of change in output bits based on the change in input bits. This method was developed by Webster and Tavares [22]. The optimum value for the calculated coefficient is 0.5. This method calculates the probability of a change in half of the output bits when a single change occurs from the input bits. Table 4 shows that the SAC values of the proposed S-boxes are very close to the ideal value of 0.5. The bit independence criteria (BIC) is a performance criterion recommended by Webster and Tavares [22] and is evaluated in two different ways. In these tests, it is tested whether the vector set generated with the plaintext inverse bit is independent of all the avalanche variable sets. BIC-SAC and BIC-nonlinearity values of S-boxes are calculated in BIC performance evaluation. BIC-SAC and BIC-nonlinearity values of the S-boxes suggested in Table 4 are shown. Suggested S-boxes have been found to have good values. Differential approximation probability (DP) [23] is a differential cryptanalysis evaluation criterion that examines the the exclusive or XOR distribution balance between the input and output bits of an S-box. Each output XOR value must have equal probability when compared to input values. The close XOR distribution between the input and output bits and the low DP value suggests that the S-box is more resistant to differential cryptanalysis. As shown in Table 4, the AES S-box has the lowest DP value. Compared to all the S-boxes given in Table 4, it is seen that the proposed S-boxes have the lowest DP values. As a result, as shown in Table 4, the proposed S-boxes have good nonlinearity and DP values after AES S-box construction compared to the S-boxes presented in the literature. SAC, BIC-SAC and BIC-nonlinearity values of proposed S-boxes were found to be close to optimum values. When examining the S-box studies in the literature, it is seen that the S-box produced by the AES algorithm has the best values. The studies in the literature are trying to realize S-box production with low load processing and high cryptographic properties by using different methods.

Table 4. The comparison of chaos-based S-box.

S-Box	Nonlinearity			BIC-SAC	BIC-Nonlinearity	SAC			DP
	Min	Avg	Max			Min	Avg	Max	
Proposed S-Box1	104	106	110	0.4988	103.857	0.4018	0.4946	0.5781	10
Proposed S-Box2	104	107	108	0.4997	103.357	0.4218	0.5029	0.5937	10
Proposed S-Box3	106	106	108	0.5058	104.14	0.3918	0.4916	0.5781	10
Jakimoski [24]	98	103.2	108	0.5031	104.2	0.3761	0.5058	0.5975	12
Tang [25]	99	103.4	106	0.4995	103.3	0.4140	0.4987	0.6015	10
Wang [26]	102	104	106	0.5070	103.8	0.4850	0.5072	0.5150	12
Çavuşoğlu [27]	104	106	108	0.49763	103.857	0.3906	0.5063	0.5937	12
Khan [28]	84	100	106	0.4962	101.9	0.3712	0.4825	0.6256	16
Ozkaynak [29]	100	104.2	109	0.4988	103.3	0.3906	0.4931	0.5703	12
Chen [60]	100	103	106	0.5024	103.1	0.4218	0.5000	0.6093	14
Çavuşoğlu [30]	104	106	110	0.5058	103.4	0.4218	0.5039	0.5937	10
Khan [31]	98	105	110	0.4994	105.7	0.4062	0.4926	0.5937	12
Khan [32]	96	103	106	0.5010	100.3	0.3906	0.5039	0.6250	12
Liu [61]	102	104	106	0.5019	103.5	0.4825	0.5018	0.5175	10
Hussain [33]	102	105.2	108	0.5053	104.2	0.4080	0.5050	0.5894	12
Skipjack S-Box [34]	104	105.7	108	0.4994	104.1	0.3986	0.5032	0.5938	12
AES S-Box [35]	112	112	112	0.5046	112	0.4531	0.5048	0.5625	4

4. Design, Implementation and Analysis Results of the Image Encryption Algorithm

In this section, a S-box based encryption algorithm is proposed for image encryption. In the developed algorithm, the S-box structures generated by the chaos-based S-box algorithm described in the previous section are used. First, the design of the S-box based encryption algorithm has been presented, then the image encryption process has been performed and the performance and security analysis results of the encryption processes have been given.

4.1. Design of Image Encryption Algorithm

In the algorithm developed for image encryption, encryption is realized by performing sub-byte operations with S-box structure used for confusion in block encryption algorithms. An S-box structure with strong cryptographic features makes the encryption process very robust and resistant to attacks. In this study, by using the developed S-box generation algorithm, three S-boxes with strong cryptographic properties have been generated and the performance results of S-boxes are given in the previous section. The block diagram for the designed encryption algorithm is shown in Figure 6.

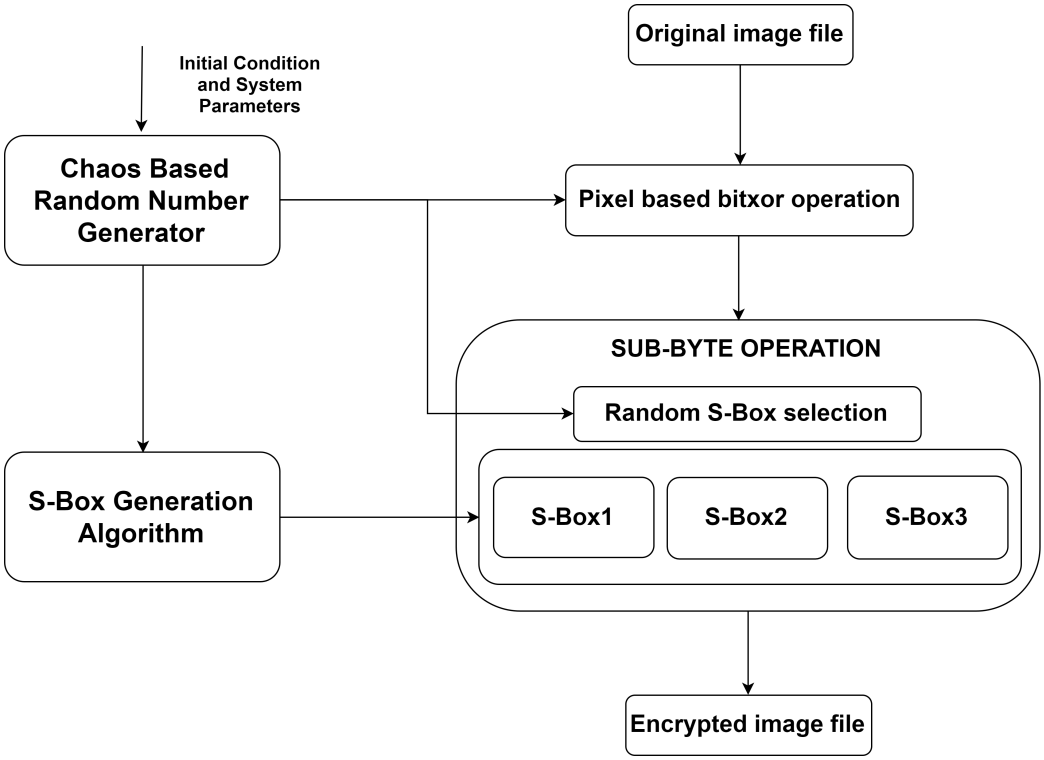


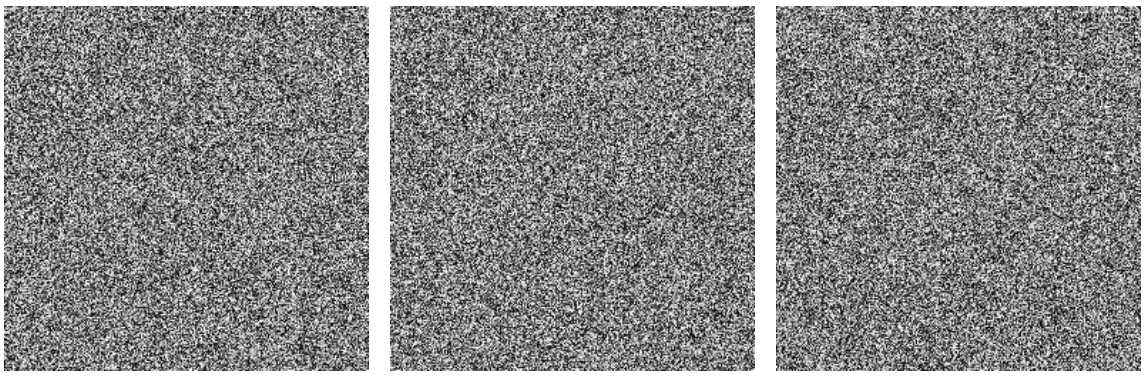
Figure 6. The proposed new encryption algorithm.

In the encryption algorithm, first, the random number obtained from the random bit sequences generated by the chaos-based RNG and the image file are subjected to "bitxor" process over pixels. Number generation by chaos-based RNG is performed as described in the S-box generation algorithm. Then, sub-byte process is performed on the image with S-boxes having strong cryptographic properties generated by the S-box generation algorithm. In the sub-byte process, row and column positions of pixels of the image are replaced with the eight-bit value on the S-box. The S-box to be used during this replacement is also determined by mod-3 operation over the numbers in the random number array generated from the x-phase of the chaos-based RNG. In this way, the S-box for sub-byte process is randomly selected. After sub-byte process, an encrypted image file is obtained. By applying the reverse of these operations for decryption, the original image is obtained.

4.2. Image Encryption Application and Security Analysis

In this section, by using the developed image encryption algorithm, encryption and decryption processes have been performed on three different images. Also, security analyses of encryption processes have been realized. Original image files, 256×256, that were used in encryption can be seen in Figure 7a–c encrypted images are in Figure 7d–f and decrypted image files are located in Figure 7g–i. When the original and decrypted image files are compared, it appears that the encryption process has been successful.

(**a**) Original Image (**b**) Original Image (**c**) Original Image

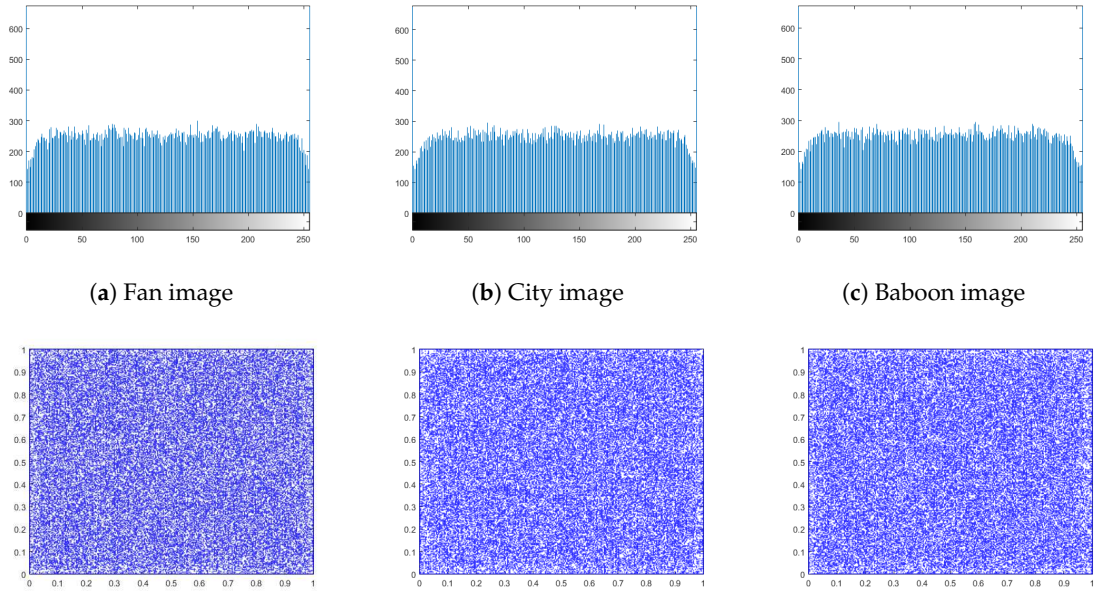


(**d**) Encrypted Image (**e**) Encrypted Image (**f**) Encrypted Image

(**g**) Decrypted Image (**h**) Decrypted Image (**i**) Decrypted Image

Figure 7. The result of image encryption. (**a**) original fan image, (**b**) original city image , (**c**) original baboon image, (**d**) encrypted fan image, (**e**) encrypted city image , (**f**) encrypted baboon image, (**g**) decrypted fan image, (**h**) decrypted city image , (**i**) decrypted baboon image.

Following the encryption process, performance analyses have been performed to determine the quality of the encryption process. First, a histogram analysis of the encryption process has been performed. In Figure 8a–c, histogram distribution graphs of the encrypted image files are shown. Histogram distribution shows the distribution of pixel values in the image file. The more balanced the distribution, the more successful the encryption has been performed. Correlation coefficient and correlation analysis [62] shows the independence of the relation of the two random variables. When the correlation distribution is linear, there is strong relation between variables and the encryption is not good. So, the distribution should be nonlinear. Correlation distribution graphs are shown in Figure 8d–f, and the calculated correlation coefficients are located in Table 5. When the correlation distribution graphs are examined, it is seen that the encryption processes had a good correlation distribution and the correlation coefficients are close to zero in Table 5.



(**a**) Fan image (**b**) City image (**c**) Baboon image

(**d**) Fan image (**e**) City image (**f**) Baboon image

Figure 8. The result of Histogram and Correlation Analysis. (**a**) histogram of fan image, (**b**) histogram of city image, (**c**) histogram of baboon image, (**d**) correlation analysis of fan image, (**e**) correlation analysis of city image, (**f**) correlation analysis of baboon image.

Table 5. The security and performance analysis results.

	Fan Image	City Image	Baboon Image
Correlation Analysis (r_{xy})	0.0054	0.0039	0.0061
NPCR	99.6167	99.5232	99.5845
UACI	31.7543	35.2089	32.0312
Information Entropy	7.9563	7.9514	7.9572
Encryption Quality	35.8046	45.3828	61.4676
Total Time (encryption+decryption) (sec)	1.0540	1.0520	1.0485

Other analyses performed on the encryption process is the number of pixels change rate (NPCR) and unified average changing intensity (UACI) [23]. They are cryptanalysis methods to determine resistance of encryption against differential attacks. They are used for detection of effects of small changes in the original images to encrypted images. Table 5 shows the calculated NPCR and UACI values of the performed encryption processes. It has been found that the NPCR values are very close to the results in [63]. That means the pixel values of the images have been changed because of the encryption. Also UACI values are very close to optimum. Information entropy [64] is used to measure randomness and complexity of encrypted data. Encrypted data should be very complex and there must not be any information about the original data. Optimum value of information entropy is eight for an gray scale information. When the entropy values of the encryption processes in Table 5 are examined, it is seen that they are very close to eight. This means that the encryptions in this study are good. Encryption quality is obtained by calculating the differences of the pixel values between the encrypted and original images. If the difference values are greater, the encryption quality is higher. In Table 5, the values of encryption quality are given as 35.8046, 45.3828 and 61.4676 for three images. From the results, it can be seen that the baboon image has the best encryption quality. The encryption and decryption time of the algorithm is very important for performance and usefulness. To show performance of the developed encryption algorithm, encryption and decryption times have been determined as in Table 5. As seen from the results, all of the encryption and decryption processes are performed in approximately 1 s totally. In Table 6, the comparison of the encryption times of

the proposed algorithm and some studies in the literature is given. When Table 6 is examined, it is seen that the proposed algorithm completes the encryption processes in a shorter time than studies in the literature.

Table 6. Encryption time and comparisons (256 × 256 image).

	Encryption Time (sec)
Proposed Algorithm	0.5554
Ref. [65]	1.6764
Ref. [66]	0.5699
Ref. [67]	7.6418
Ref. [68]	0.7124

5. Conclusions

A no-equilibrium system exhibiting chaos has been studied in our work. Experimental results of the implemented circuit verify the system's feasibility. We have designed an S-box generation algorithm using a system without equilibrium. Using the developed S-box algorithm, three different S-boxes are produced. The outputs of the different phases of the chaotic system are used in the S-box generation algorithm. The performance tests of the generated S-boxes are performed. They are compared with the studies in the literature. Then a new image encryption algorithm is developed using the generated S-boxes. With the random S-box selection in the encryption algorithm, each pixel has been encrypted with different S-box. This is the most important specificity aspect of the developed encryption algorithm. With the developed encryption algorithm, encryption operations are performed on different images, and security and performance analyses are performed. According to the analysis results, the developed encryption algorithm has been shown to have good correlation, NPCR, UACI, information entropy, encryption quality and encryption time. As a result, it is proven that S-box based encryption algorithm can be used safely in image encryption operations.

Author Contributions: conceptualization, X.W. and U.C.; formal analysis, U.C.; funding acquisition, X.Q.N.; investigation, X.W. and S.K.; methodology, S.K.; project administration, F.E.A.; resources, A.A. and V.–T.P.; software, A.A. and V.–T.P.; supervision, S.J.; visualization, S.J.; writing—original draft, F.E.A.; writing—review and editing, X.Q.N.

Funding: The author Xiong Wang was supported by the National Natural Science Foundation of China (No. 61601306) and Shenzhen Overseas High Level Talent Peacock Project Fund (No. 20150215145C).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lorenz, E. Deterministic nonperiodic flow. *J. Atmos. Sci.* **1963**, *20*, 130–141. [CrossRef]
2. Rössler, O. An equation for continuous chaos. *Phys. Lett. A* **1976**, *57*, 397–398. [CrossRef]
3. Sprott, J. Some simple chaotic flows. *Phys. Rev. E* **1994**, *50*, R647–R650. [CrossRef]
4. Gotthans, T.; Petržela, J. New class of chaotic systems with circular equilibrium. *Nonlinear Dyn.* **2015**, *73*, 429–436. [CrossRef]
5. Gotthans, T.; Sportt, J.C.; Petržela, J. Simple chaotic flow with circle and square equilibrium. *Int. J. Bifurc. Chaos* **2016**, *26*, 1650137. [CrossRef]
6. Baptista, M.S. Cryptography with chaos. *Phys. Lett. A* **1998**, *240*, 50–54. [CrossRef]
7. Alvarez, G.; Li, S. Some basic cryptographic requirements for chaos–based cryptosystems. *Int. J. Bifurc. Chaos* **2006**, *16*, 2129–2151. [CrossRef]
8. Amigo, J.M.; Kocarev, L.; Szczepanski, J. Theory and practice of chaotic cryptography. *Phys. Lett. A* **2007**, *366*, 211–216. [CrossRef]
9. Zhao, D.; Chen, G.; Liu, W. A chaos–based robust wavelet–domain watermarking algorithm. *Chaos Solitons Fractals* **2004**, *22*, 47–54.
10. Wu, Y.; Shih, F.Y. Digital watermarking based on chaotic map and reference register. *Pattern Recognit.* **2007**, *40*, 3753–3763. [CrossRef]

11. Cavusoglu, U.; Akgul, A.; Kacar, S.; Pehlivan, I.; Zengin, A. A novel chaos based encryption algorithm over TCP data packet for secure communication. *Secur. Commun. Netw.* **2016**, *9*, 1285–1296. [CrossRef]
12. Shen, Q.; Liu, W. A novel digital image encryption algorithm based on orbit variation of phase diagram. *Int. J. Bifurc. Chaos* **2017**, *27*, 1750204. [CrossRef]
13. Ghebleh, M.; Kanso, A. A robust chaotic algorithm for digital image steganography. *Commun. Nonlinear Sci. Numer. Simul.* **2014**, *19*, 1898–1907. [CrossRef]
14. Grassi, G.; Mascolo, S. A system theory approach for designing cryptosystems based on hyperchaos. *IEEE Trans. Circuits Syst.–I: Fund. Theory Appl.* **1999**, *46*, 1135–1138. [CrossRef]
15. Wong, K.W. A combined chaotic cryptographic and hashing scheme. *Phys. Lett. A* **2003**, *307*, 292–298. [CrossRef]
16. Arumugam, G.; Praba, V.L.; Radhakrishnan, S. Study of chaos functions for their suitability in generating message authentication codes. *Appl. Soft Comput.* **2007**, *7*, 1064–1071. [CrossRef]
17. Zhao, D.; Chen, G.; Liu, W. Image scrambling encryption algorithm of pixel bit based on chaos map. *Pattern Recognit. Lett.* **2010**, *31*, 347–354.
18. Liu, Q.; Li, P.; Zhang, M.; Sui, Y.; Yang, H. A novel image encryption algorithm based on chaos maps with Marlov properties. *Commun. Nonlinear Sci. Numer. Simul.* **2015**, *20*, 506–515. [CrossRef]
19. Stinson, D.R. *Cryptography: Theory and Practice*; CRC Press: Boca Raton, FL, USA, 1995.
20. Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed.; Wiley: New York, NY, USA, 1996.
21. Adams, C.; Tavares, S. The structured design of cryptographically good S-boxes. *J. Cryptol.* **1990**, *3*, 27–41. [CrossRef]
22. Webster, A.; Tavares, S.E. On the design of S-boxes. In *Conference on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1985; pp. 523–534.
23. Biham, E.; Shamir, A. Differential cryptanalysis of DES-like cryptosystems. *J. Cryptol.* **1991**, *4*, 3–72. [CrossRef]
24. Jakimoski, G.; Kocarev, L. Chaos and cryptography: Block encryption ciphers based on chaotic maps. *IEEE Trans. Circuits Syst. I: Fundam. Theory Appl.* **2001**, *48*, 163–169. [CrossRef]
25. Tang, G.; Liao, X.; Chen, Y. A novel method for designing S-boxes based on chaotic maps. *Chaos, Solitons Fractals* **2005**, *23*, 413–419. [CrossRef]
26. Wang, Y.; Wong, K.W.; Liao, X.; Xiang, T. A block cipher with dynamic S-boxes based on tent map. *Commun. Nonlinear Sci. Numer. Simul.* **2009**, *14*, 3089–3099. [CrossRef]
27. Çavuşoğlu, Ü.; Kaçar, S.; Pehlivan, I.; Zengin, A. Secure image encryption algorithm design using a novel chaos based S-Box. *Chaos, Solitons Fractals* **2017**, *95*, 92–101. [CrossRef]
28. Khan, M.; Shah, T.; Batool, S.I. Construction of S-box based on chaotic Boolean functions and its application in image encryption. *Neural Comput. Appl.* **2016**, *27*, 677–685. [CrossRef]
29. Özkaynak, F.; Yavuz, S. Designing chaotic S-boxes based on time-delay chaotic system. *Nonlinear Dyn.* **2013**, *74*, 551–557. [CrossRef]
30. Çavuşoğlu, Ü.; Zengin, A.; Pehlivan, I.; Kaçar, S. A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. *Nonlinear Dyn.* **2017**, *87*, 1081–1094. [CrossRef]
31. Khan, M.; Shah, T. A novel image encryption technique based on Hénon chaotic map and S8 symmetric group. *Neural Comput. Appl.* **2014**, *25*, 1717–1722. [CrossRef]
32. Khan, M.; Shah, T.; Mahmood, H.; Gondal, M.A.; Hussain, I. A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. *Nonlinear Dyn.* **2012**, *70*, 2303–2311. [CrossRef]
33. Hussain, I.; Shah, T.; Gondal, M.A. A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm. *Nonlinear Dyn.* **2012**, *70*, 1791–1794. [CrossRef]
34. Brickell, E.F.; Denning, D.E.; Kent, S.T.; Maher, D.P.; Tuchman, W. *SKIPJACK Review: Interim Report. Building in Big Brother*; Springer-Verlag Inc.: New York, NY, USA, 1995; pp. 119–130.
35. Rijmen, V.; Daemen, J. Advanced encryption standard. In *Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology*; NIST: Gaithersburg, MD, USA 2001; pp. 19–22.
36. Leonov, G.A.; Kuznetsov, N.V.; Vagaitsev, V.I. Localization of hidden Chua's attractors. *Phys. Lett. A* **2011**, *375*, 2230–2233. [CrossRef]

37. Leonov, G.A.; Kuznetsov, N.V.; Vagaitsev, V.I. Hidden attractor in smooth Chua system. *Phys. D* **2012**, *241*, 1482–1486. [CrossRef]
38. Leonov, G.A.; Kuznetsov, N.V. Hidden attractors in dynamical systems: From hidden oscillation in Hilbert-Kolmogorov, Aizerman and Kalman problems to hidden chaotic attractor in Chua circuits. *Int. J. Bifurc. Chaos* **2013**, *23*, 1330002. [CrossRef]
39. Dudkowski, D.; Jafari, S.; Kapitaniak, T.; Kuznetsov, N.; Leonov, G.; Prasad, A. Hidden attractors in dynamical systems. *Phys. Rep.* **2016**, *637*, 1–50. [CrossRef]
40. Wang, Z.; Cang, S.; Ochala, E.; Sun, Y. A hyperchaotic system without equilibrium. *Nonlinear Dyn.* **2012**, *69*, 531–537. [CrossRef]
41. Wei, Z. Dynamical behaviors of a chaotic system with no equilibria. *Phys. Lett. A* **2011**, *376*, 102–108. [CrossRef]
42. Jafari, S.; Sprott, J.C.; Golpayegani, S.M.R.H. Elementary quadratic chaotic flows with no equilibria. *Phys. Lett. A* **2013**, *377*, 699–702. [CrossRef]
43. Wang, X.; Chen, G. Constructing a chaotic system with any number of equilibria. *Nonlinear Dyn.* **2013**, *71*, 429–436. [CrossRef]
44. Wei, Z.; Wang, R.; Liu, A. A new finding of the existence of hidden hyperchaotic attractor with no equilibria. *Math. Comput. Simul.* **2014**, *100*, 13–23. [CrossRef]
45. Rajagopal, K.; Karthikeyan, A.; Srinivasan, A.K. FPGA implementation of novel fractional–order chaotic systems with two equilibriums and no equilibrium and its adaptive sliding mode synchronization. *Nonlinear Dyn.* **2017**, *87*, 2281–2304. [CrossRef]
46. Sprott, J.C. *Elegant Chaos Algebraically Simple Chaotic Flows*; World Scientific: Singapore, 2010.
47. Jafari, S.; Sprott, J.C. Simple chaotic flows with a line equilibrium. *Chaos Solitons Fractals* **2013**, *57*, 79–84. [CrossRef]
48. Sprott, J.C. A proposed standard for the publication of new chaotic systems. *Int. J. Bifurc. Chaos* **2011**, *21*, 2391–2394. [CrossRef]
49. Wolf, A.; Swift, J.B.; Swinney, H.L.; Vastano, J.A. Determining Lyapunov exponents from a time series. *Phys. D* **1985**, *16*, 285–317. [CrossRef]
50. Eckmann, J.; Ruelle, D. Ergodic theory of chaos and strange attractors. *Rev. Mod. Phys.* **1985**, *57*, 617. [CrossRef]
51. Xu, G.; Shekofteh, Y.; Akgul, A.; Li, C.; Panahi, S. New chaotic system with a self-excited attractor: Entropy measurement, signal encryption, and parameter estimation. *Entropy* **2018**, *20*, 86. [CrossRef]
52. Wang, C.; Ding, Q. A new two-dimensional map with hidden attractors. *Entropy* **2018**, *20*, 322. [CrossRef]
53. Pincus, S. Approximate entropy as a measure of system complexity. *Proc. Natl. Acad. Sci. USA* **1991**, *88*, 2297–2301. [CrossRef]
54. Pincus, S. Approximate entropy (ApEn) as a complexity measure. *Chaos Interdiscipl. J. Nonlinear Sci.* **1995**, *5*, 110–117. [CrossRef]
55. Volos, C.K.; Kyprianidis, I.M.; Stouboulos, I.N. A chaotic path planning generator for autonomous mobile robots. *Robot. Auton. Syst.* **2012**, *60*, 651–656. [CrossRef]
56. Bouali, S.; Buscarino, A.; Fortuna, L.; Frasca, M.; Gambuzza, L.V. Emulating complex business cycles by using an electronic analogue. *Nonl. Anal.: Real World Appl.* **2012**, *13*, 2459–2465. [CrossRef]
57. Volos, C.K.; Kyprianidis, I.M.; Stouboulos, I.N. Image encryption process based on chaotic synchronization phenomena. *Signal Process.* **2013**, *93*, 1328–1340. [CrossRef]
58. Zhou, W.; Wang, Z.; Wu, M.; Zheng, W.; Weng, J. Dynamics analysis and circuit implementation of a new three–dimensional chaotic system. *Optik* **2015**, *126*, 765–768. [CrossRef]
59. Lai, Q.; Yang, L. Chaos, bifurcation, coexisting attractors and circuit design of a three–dimensional continuous autonomous system. *Optik* **2016**, *127*, 5400–5406. [CrossRef]
60. Chen, G. A novel heuristic method for obtaining S-boxes. *Chaos Solitons Fractals* **2008**, *36*, 1028–1036. [CrossRef]
61. Liu, H.; Kadir, A.; Niu, Y. Chaos-based color image block encryption scheme using S-box. *AEU-Int. J. Electron. Commun.* **2014**, *68*, 676–686. [CrossRef]
62. Pareek, N.K.; Patidar, V.; Sud, K.K. Image encryption using chaotic logistic map. *Image Vis. Comput.* **2006**, *24*, 926–934. [CrossRef]

63. Wu, Y.; Noonan, J.P.; Agaian, S. NPCR and UACI randomness tests for image encryption. *Cyber J.* **2011**, *1.2*, 31–38.
64. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
65. Zhou, Y.; Cao, W.; Chen, C.P. Image encryption using binary bitplane. *Signal Process.* **2014**, *100*, 197–207. [CrossRef]
66. Liao, X.; Lai, S.; Zhou, Q. A novel image encryption algorithm based on self–adaptive wave transmission. *Signal Process.* **2010**, *90*, 2714–2722. [CrossRef]
67. Wu, Y.; Noonan, J.; Yang, G.; Jin, H. Image encryption using the two–dimensional logistic chaotic map. *J. Electron. Imag.* **2012**, *21*, 013014. [CrossRef]
68. Wong, K.; Kwok, B.; Law, W. A fast image encryption scheme based on chaotic standard map. *Phys. Lett. A* **2008**, *372*, 2645–2652. [CrossRef]