Wireless Pers Commun (2015) 82:1497–1503
DOI 10.1007/s11277-015-2295-4

A Technique for Designing Substitution Box Based on Van der Pol Oscillator

Amir Anees · Zeeshan Ahmed

Published online: 22 February 2015

Abstract Chaos is the impromptu behavior exhibited by some nonlinear dynamical systems and has been applied extensively in secure communication over the last decade. In this paper, the chaotic behavior of Van der Pol oscillator is studied and proposed a method to generate Substitution Box (S-box) from it. The generated S-box have some good statistical properties such as PSNR, MSE, correlation, energy, Homogeneity, entropy and contrast. The performance of proposed S-box is compared with other S-boxes like AES, gray, APA, Lui J and S8 to show the strength of anticipated technique.

Keywords Chaos · Secure communication · Substitution box · Statistical analysis

1 Introduction

In the modern world, today's society is tightly surrounded by the sphere of information era, which is classified by scholar assets and utilizable inside data being considered exceptionally precious. Furthermore, information is electronically processed and conveyed through public networks. The safety of this information during transfer, saving and in routine practice is very important. To ensure the safety of this information, the field of secure communication plays an important role and overcome this issue. Secure communication can be broadly classified in to three subjects, namely, cryptography, steganography and watermarking. The purpose of cryptography and steganography is same, i.e. to conceal the information message but the methodologies employed in these techniques are different. The methodology of watermarking and steganography is same but the purposes of these techniques are different. Watermarking deals with copyright protection of digital data while steganography concerns about the hiding of digital data. One of the most sophisticated cryptographic algorithms used

A. Anees (✉) · Z. Ahmed
Department of Electrical Engineering, HITEC University, Taxila, Pakistan
e-mail: amiranees@yahoo.com

Z. Ahmed
e-mail: zeeshan.ahmed@hitecuni.edu.pk

today for encrypting digital data is Advanced Encryption Standards (AES) [3]. AES is a well known block cipher. The block cipher is a type of symmetric-key encryption algorithm that transforms a fixed-length plaintext data into cipher text data of the same dimension. This transformation takes place under the action of a user provided secret key. The decryption is performed by applying the reverse transformation to the cipher text block using the same secret key. AES consists of four steps, which are: byte sub, shift row, mixed column and add round key, the first step is an important one, also known as substitution step performed by the help of S-box. The byte sub step plays a pivotal role in the encryption process because it creates confusion that is reflected in the encrypted data and is the only nonlinear component in AES. S-box is a bijective mapping relation which holds one to one and onto relations; in which a message symbol is replaced with only one unique symbol/element of S-box. S-box can be thought of as a bijective function, $f(x)$, that is [1],

$$S : GF(2)^n \rightarrow GF(2)^m \tag{1}$$

Equation (1) represents an $n \times m$ S-box which takes n bits as the input and gives m bits as the output, such that

if

$$x_1 = x_2 \tag{2}$$

then

$$f(x_1) = f(x_2) \tag{3}$$

A major performing criterion of the S-box in encryption techniques is its non-linearity. A foremost research development in the past few years for the construction of S-boxes has been done mainly to increase the non-linearity of these S-boxes [2]. There are many methods proposed in literature for the construction of S-boxes, some of them are AES [3], gray [4], APA [5], Lui J [6] and S8 [7]. In this paper, we proposed a technique of generating S-box from a chaotic map and then compare the performance analysis of anticipated S-box with some of the existing proposed S-boxes.

2 Van der Pol and Proposed Algorithm

In dynamics, the Van der Pol oscillator is a non-conservative oscillator with non-linear damping. It evolves in time according to the second order differential equation, defined as [8]:

$$\ddot{x} - \mu(1 - x^2)\,\dot{x} + x = 0 \tag{4}$$

In which, $\dot{x}$ represents the derivative of x with respect to time. As it is a nonlinear system with the nonlinearity x^2, so there is no analytical solution to it. The iterative solution of (4) is a chaotic solution obtained after initializing it with some initial conditions. The solution of Van der Pole along with the phase trajectory are plotted in Fig. 1. The solution of Van der Pole will be used for designing the S-box as mentioned in the following algorithm.

The flow chart of the proposed algorithm is shown in Fig. 2. The methods involve in the proposed technique are:

- M.1: The iterative solution of chaotic map is obtain via applying numerical technique.
- M.2: Apply the ceiling function on the chaotic values to map the real values to the smallest integers, defined as:

$$\lceil y \rceil = min\{n \in \mathbb{Z} \mid n \geq y\} \tag{5}$$

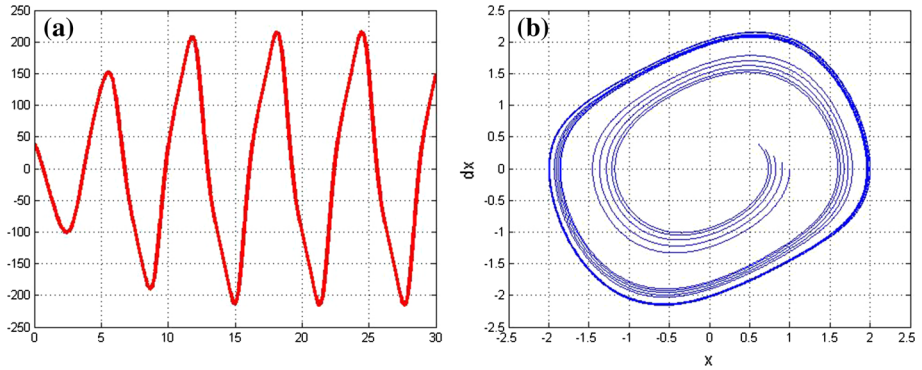

Fig. 1 **a** Solution of Van der Pole **b** Phase trajectory plot between x and its derivative

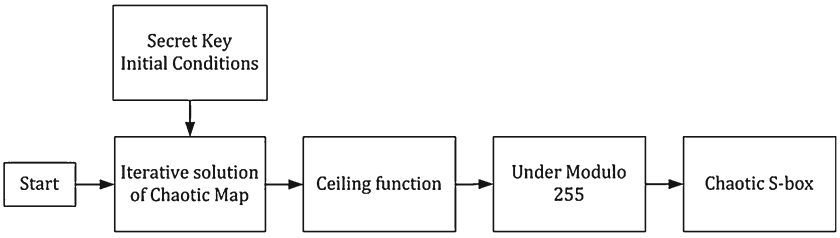

Fig. 2 Proposed chaotic S-box designing technique

where y is the real value obtain from chaotic map, n is the nearest integer to y and $\mathbb{Z}$ is the set of integers.

- M.3: Scale the solution of chaotic map between 0 to 255 by applying modulo operation denoted by %, i.e. take n modulo 255, which is remainder on division of n by 255 resulted in x, defined as:

$$x = n\%255$$
$$n = 255 \times m + x \Rightarrow x = n - 255 \times m \tag{6}$$

In terms of ceiling function,

$$x = n - 255 \times \left\lceil \frac{n}{255} \right\rceil \tag{7}$$

where

$$m \in \mathbb{Z}, \lceil m \rceil = \left\lceil \frac{y}{255} \right\rceil$$

- M.4: Pick the first 256 distinct integers to make strong chaotic S-box as shown in Table 1

3 Stimulated Results and Statistical Analysis

The proposed S-box is applied on the Lena plain image to substitute with it. The plain and substituted images are shown in Fig. 3. To demonstrate the strength of proposed technique, few security statistical analysis have been done defined below:

Table 1 Proposed chaotic S-box

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

(a) **(b)**

Fig. 3 **a** Plain Lena image, **b** Substituted image with the proposed chaotic S-box

3.1 Correlation

The most fundamental method used in determining the similarity between two images is the correlation analysis. The correlation of an image is given as:

$$Corr = \sum \frac{(i - \mu i)(j - \mu j)p(i, j)}{\sigma_i \sigma_j} \tag{8}$$

where i, j corresponds to image pixels positions, $p(i, j)$ is pixel value at *ith* row and *jth* column of digital image, μ is the variance and σ is the standard deviation.

3.2 Entropy

Entropy is a magnitude of the uncertainty of a random variable to come in a random process and can be use to show the randomness of the digital image as well. Entropy is defined as:

$$H = -\sum p(x_i) \log_2 p(x_i) \tag{9}$$

where $p(x_i)$ is the probability of random variable x at *ith* index.

3.3 Contrast

The contrast analysis of the image enables the viewer to vividly identify the objects in texture of an image. The contrast of an image is given as:

$$C = \sum |i - j|^2 p(i, j) \tag{10}$$

3.4 Homogeneity

The homogeneity analysis processes the closeness of the distribution in the gray level cooccurrence matrix (GLCM) to GLCM diagonal. The GLCM shows the measurements of combinations of pixel brightness values or gray levels in tabular form. The frequency of the patterns of gray levels can be inferred from the GLCM table. The homogeneity can be determined as:

$$Hom = \sum \frac{p(i, j)}{1 + |i - j|} \tag{11}$$

3.5 Energy

The energy of the image gives the sum of squared values of gray pixels of a digital image defined as:

$$E = \sum p(i, j)^2 \tag{12}$$

3.6 Mean Squared Error

Mean Squared Error (MSE) is used to measure the difference between two digital images. It can be defined as:

$$MSE = \frac{1}{n} \sum (X_i - X_i^*)^2 \tag{13}$$

where X_i corresponds to original image pixel at *ith* position, X_i^* corresponds to resulted image pixel at *ith* position.

3.7 Peak Signal to Noise Ratio

Pick Signal to Noise Ratio (PSNR) has the same function as MSE, but it takes the signal strength and divided it by noise strength or the difference between the images (MSE), thus gives the better comparative statistical analysis. It is given as:

$$PSNR = 10 \log_{10} \frac{MAX^2}{MSE} \tag{14}$$

where MAX represents the maximum pixel value in the image.

Table 2 Statistical security analysis of proposed and existing techniques

Statistical analysis	Plain	AES [3]	Gray [4]	APA [5]	Lui [6]	S8 [7]	Proposed
Correlation	0.8771	0.0815	0.1014	0.1258	0.1311	0.0734	0.0732
Entropy	6.6733	7.9325	7.9299	7.8183	7.9325	7.9447	7.9448
Homogeneity	0.9334	0.4701	0.4567	0.0193	0.4701	0.0190	0.0189
Contrast	0.2455	7.2240	7.7961	8.9114	7.2240	8.1274	8.1201
Energy	0.2917	0.0211	0.0198	0.0193	0.0211	0.0190	0.0188
MSE	N/A	72.1541	71.2514	68.2532	70.2578	72.5847	72.0145
PSNR	N/A	9.2154	8.1421	9.0014	9.2541	9.2611	9.2751

These analysis are done on the proposed technique, as well as on some of the existing S-boxes like AES [3], gray [4], APA [5], Lui J [6] and S8 [7] to show the strength of proposed technique. The results of these analysis, as well as in comparison are listed in Table 2. We can see that the results of proposed technique are much better than the existing techniques.

4 Conclusion

S-box is the most important component in the encryption algorithm, combine in the substitution-permutation network to play a pivotal role. In this paper, a method for designing strong chaotic S-box is presented based on Van der Pole oscillator. The generated S-box shows good results as compared to some existing S-boxes, as evident from the statistical analysis done in this paper.

References

1. Anees, A. (2014). *Design of security systems based upon nonlinear dynamics*. MS Thesis, MIlitary College of Signals, NUST.
2. Anees, A., Siddiqui, A. M., & Ahmed, F. (2014). Chaotic substitution for highly autocorrelated data in encryption algorithm. *Communications in Nonlinear Science and Numerical Simulations*, *19*(9), 3106–3118.
3. Daemen, J., & Rijmen, V. (2002). *The design of Rijndael: AES–the advanced encryption standard*. Springer, Berlin.
4. Tran, M. T., Bui, D. K., & Doung, A. D. (1998). Gray S-box for advanced encryption standard. In *International Conference on Computational Intelligence and Security*, pp. 253–256.
5. Cui, L., & Cao, Y. (2007). A new S-box structure named Affine- Power-Affine. *International Journal of Innovative Computing, Information and Control*, *3*(3), 45–53.
6. Lui, J., Wai, B., Cheng, X., & Wang, X. (2005). An AES S-box to increase complexity and cryptgraphic analysis. *International Conference on Advanced Information Networking and Applications*, *1*, 724–728.
7. Hussain, I., Shah, T., & Mehmood, H. (2010). A new algorithm to construct secure keys for AES. *International Journal of Contemporary Mathematical Sciences*, *5*(26), 1263–1270.
8. Cartwright, M. L. (1960). Balthazar van der Pol. *Journal of the London Mathematical Society*, *35*, 367–376.

Amir Anees received his BS degree in Electrical Engineering from HITEC University, Taxila-Cantt Pakistan in 2011 and MS degree in Electrical Engineering from Military College of Signals, National University of Sciences and Technology, Pakistan in 2014. He has six journal publications with a cumulative impact factor of 9.5 and four conference publications in which two of them got the best research paper awards at national and international levels. His research interests include image encryption, image hashing and chaos-based encryption.

Zeeshan Ahmed got his degree of Bachelors in Electronics Engineering in 2008 from International Islamic University Islamabad, Pakistan and did Masters in Electrical Engineering with specialization in control systems from HITEC University, Taxila Cantt, Pakistan in 2013. Currently he is serving as a Lecturer in the Department of Electrical Engineering at HITEC University. His area of research involves Control Systems, Wireless Communication, and Secure Communication.