A NEW SERIES-WOUND FRAMEWORK FOR GENERATING 1D CHAOTIC MAPS

Zhongyun Hua, Yicong Zhou and C. L. Philip Chen*

Department of Computer and Information Science, University of Macau, Macao, China
*yicongzhou@umac.mo

ABSTRACT

This paper introduces a series-wound framework to generate a large number of new one-dimensional (1D) chaotic maps using a combination of two different 1D chaotic maps (called seed maps). Examples and experimental analysis demonstrate that the newly generated chaotic maps have more parameters, larger chaotic ranges, and better chaotic behaviors than their corresponding seed maps.

Index Terms— series-wound, chaotic system, chaotic map.

1. INTRODUCTION

The chaotic map generally has several significant properties such as ergodicity and unpredictability. It can generate random-like sequences. And it is extremely sensitive to its initial value and control parameters. Chaotic maps have been widely used in spread spectrum communication [1], data compression [2], image encryption [3] and so on. For image encryption, chaotic maps are used to generate pseudo-random sequences with specific settings for their initial values and control parameters. These random sequences are then used to encrypt a digital image into a random-like one such that the original image information is protected with a high level of security. Recent application examples of chaotic maps in image encryption can be found in [4][5].

There are two problems with the existing chaotic maps. The first one is that their trajectories are easy to be predicted [6]. The other is that traditional 1D chaotic maps based encryption algorithms have been reported to be vulnerable for low computational attacks [7]. Therefore, developing new chaotic maps with more complex structures, more parameters and better chaos performance becomes significative.

In this paper, we propose a new series-wound framework of 1D chaotic map. It can generate many new 1D chaotic maps from different combinations of two seed maps. The new 1D chaotic maps generated by this framework have more complex structures, more parameters and better chaos performance. Examples and experimental analysis are provided.

The rest of this paper is organized as follows: in Section 2, three traditional 1D chaotic maps and their properties will be reviewed as background. In Section 3, the new series-wound framework of 1D chaotic map will be introduced. In Section 4, three examples of new chaotic maps using this framework will be introduced and their chaos performance will be discussed in Section 5. Section 6 will give a conclusion.

2. BACKGROUND

This section reviews three traditional 1D chaotic maps which will be used as seed maps to generate new 1D chaotic maps in the series-wound framework proposed in Section 3.

2.1. Logistic map

The Logistic map is one of the most popular chaotic maps used in many fields. Its good chaos performance has been verified [4]. Mathematically, the Logistic map is defined as Eqn. (1)

$$x_{n+1} = a x_n (1 - x_n) \tag{1}$$

where a is a parameter and $a \in$[0, 4], x_n is the n^{th} output and $(n+1)^{th}$ input with range the of [0, 1].

It is well known that the Logistic map has chaotic behavior when $a \in$[3.57, 4]. Its bifurcation diagram is shown in Fig. 1(a). As can be seen, when the parameter a is close to 4, the output of the Logistic map dynamically changes in the entire data range. Its chaotic behaviors become better.

2.2. Sine map

The Sine map is another useful chaotic map that is similar to the Logistic map, but its mathematic function is totally different, as shown in Eqn. (2)

$$x_{n+1} = r \cdot \sin(\pi x_n) \tag{2}$$

where r is a parameter between 0 and 1, x_n is the iteration output/input with a range of [0, 1].

When the parameter $r \in$[0.867, 1], the Sine map has chaotic behaviors. Its bifurcation diagram is shown in Fig. 1(b). We can see that the Sine map shows better chaotic behaviors when the parameter r is close to 1.

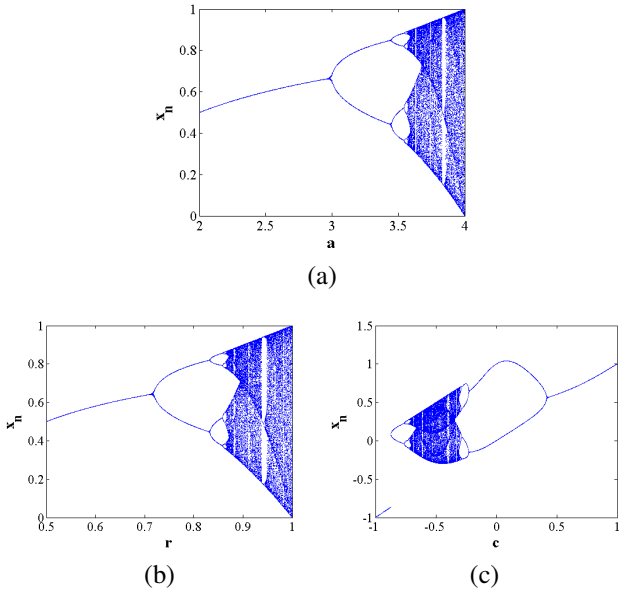
2.3. Gaussian Map

The Gaussian map is an 1D chaotic map that is based on the 1D Gaussian function. It is defined as Eqn. (3)

$$x_{n+1} = \exp(-bx_n^2) + c \tag{3}$$

where b and c are two parameters and x_n is the output/input of the Gaussian map.

When b = 6.2 and $c \in [-0.71, -0.3]$, the Gaussian map has chaotic behaviors. Its bifurcation diagram is shown in Fig. 1(c). The chaotic ranges of the Gaussian map are clearly shown.



(a) (b) (c)

Fig. 1: Bifurcation diagrams of three traditional 1D chaotic maps. (a) the Logistic map; (b) the Sine map; (c) the Gaussian map with the parameters b = 6.2.

3. THE NEW SERIES-WOUND FRAMEWORK

In this section, a series-wound framework is proposed. Using this framework, new 1D chaotic maps can be generated from any two existing 1D chaotic maps. The proposed framework is shown in Fig. 2. $G(x)$ and $F(x)$ are two 1D chaotic maps which are considered as seed maps. The output of G(x) is fed into the input of F(x). The output of F(x) is then fed back into the input of G(x) for recursive iterations and is also the output of the proposed framework, generating new chaotic maps.

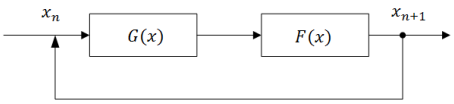


Fig. 2: The proposed series-wound framework for generating 1D chaotic maps.

The mathematic representation is defined in Eqn. (4), where $G(x)$ and $F(x)$ are two 1D chaotic maps.

$$x_{n+1} = F(G(x_n)) \tag{4}$$

The proposed framework links two chaotic maps G(x) and F(x) in series. Its output chaotic sequences have the structure of G(x), F(x), or both. In the hardware implementation, a time compensation circuit may be required in its feedback path to eliminate the time delay in the series connection of G(x) and F(x). Using a different pair of seed maps G(x) and F(x), the proposed framework generates a completely different chaotic sequence, and thus becomes a new chaotic map. These sequences have chaotic behaviors in a larger dynamic range than those of their corresponding seed maps. The parameters of the proposed framework include all parameters in two seed maps. This offers new chaotic maps more complicate properties than their corresponding seed maps, and thus more suitable for security applications.

4. EXAMPLES OF NEW CHAOTIC MAPS

The output of the proposed framework is dependent on the combination of two seed maps. Using different seed maps G(x) and F(x), the proposed framework is able to generate new chaotic maps. This section provides three examples to demonstrate robustness of the proposed framework and excellent properties of its newly generated chaotic maps.

4.1. The Logistic-Sine map

When the Logistic and Sine maps are selected as the seed maps, the proposed framework becomes a new chaotic map, called the Logistic-Sine map. Its block diagram is shown in Fig. 3, in which the output of the Logistic map is used as the input of the Sine map, and the output of the Sine map is the output of the new Logistic-Sine map.

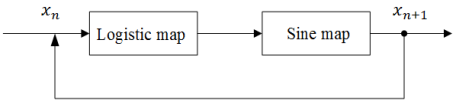


Fig. 3: The structure of the Logistic-Sine map.

Mathematically, the Logistic-Sine map is defined as Eqn. (5)

$$x_{n+1} = r \cdot \sin(\pi a x_n(1 - x_n)) \tag{5}$$

where r and a are parameters, and $r \in$[0, 1], $a \in$[0,4].

The bifurcation diagram is a straightforward way to show the characteristics of a chaotic map. It plots the output sequence of a chaotic map versus its parameter changes.

The bifurcation diagrams of the Logistic-Sine map are shown in Fig. 4. From these bifurcation diagrams, we can

see that the Logistic-Sine map has a large chaotic ranges on both parameters a and r, especially on the parameter a.

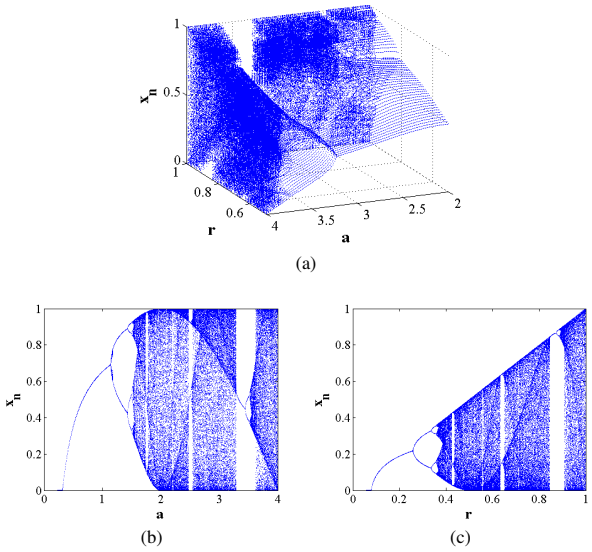


Fig. 4: The bifurcation diagrams of the Logistic-Sine map with different parameter settings. (a) the 3D bifurcation diagram with parameters r ∈[0.5, 1] and a ∈[2, 4]; (b) r = 1, a ∈[0, 4]; (c) a = 4, r ∈[0, 1].

4.2. The Gaussian-Logistic map

Here we use the Logistic map and Gaussian map as two seed maps to generate a new 1D chaotic map, called the Gaussian-Logistic map. Its structure is described in Fig. 5. The output of the Gaussian map is used as the input of the Logistic map, and the output of the Logistic map is the output of the Gaussian-Logistic map.

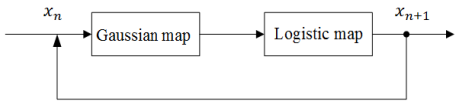


Fig. 5: The structure of the Gaussian-Logistic map.

Its mathematic representation is defined by Eqn. (6)

$$x_{n+1} = a(\exp(-bx_n^2) + c)(1 - (\exp(-bx_n^2) + c)) \quad (6)$$

where a, b, and c are parameters, and a ∈[0, 4], c ∈[-1, 1], and for parameter b, we usually set b = 6.2, where the map keeps good chaos performance.

Fig. 6 shows the bifurcation diagrams of the Gaussian-Logistic map both in the 2D and 3D spaces. From these bifurcation diagrams, we can see that the Gaussian-Logistic map has a much larger dynamic ranges than its seed maps, the Gaussian and Logistic maps.

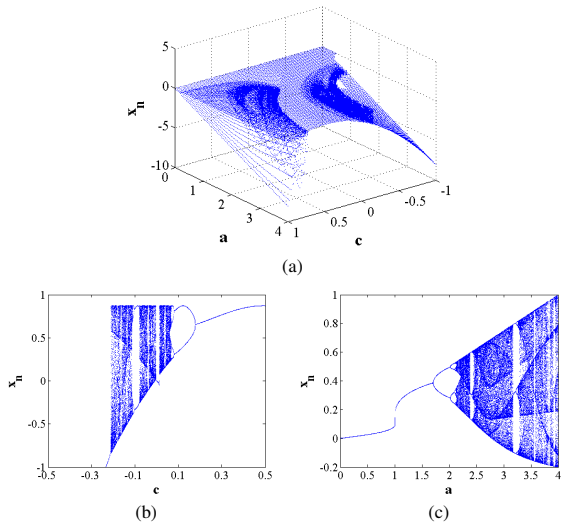


Fig. 6: The bifurcation diagrams of the Gaussian-Logistic map with different parameter settings. (a) the 3D bifurcation diagram with parameters a ∈[0, 4], c ∈[-1, 1] and b = 6.2; (b) a = 3.49, b = 6.2, c ∈[-0.5, 0.5]; (c) c = -0.05, b = 6.2, a ∈[0, 4].

4.3. The Gaussian-Sine map

Here is another example of the series-wound framework where the Sine and Gaussian maps are used as seed maps. The new chaotic map is called the Gaussian-Sine map. Its structure is shown in Fig. 7. The output of the Gaussian map is used as the input of the Sine map, and the output of the Sine map is the output of the Gaussian-Sine map.

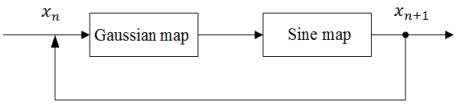


Fig. 7: The structure of the Gaussian-Sine map.

The Gaussian-Sine map is defined as Eqn. (7)

$$x_{n+1} = r \cdot \sin(\pi(\exp(-bx_n^2) + c)) \quad (7)$$

where r, b, c are parameters and b = 6.2, r ∈[0, 1], and c is a real number.

The 2D and 3D bifurcation diagrams of the Gaussian-Sine map are shown in Fig. 8. These plots give us straightforward representations about chaos performance of the Gaussian-Sine map. There is an interesting observation that its chaotic behaviors along with the parameter c are periodic as shown in Fig. 8(a) and (b).

5. PERFORMANCE COMPARISONS AND ANALYSIS

This section discusses some properties of three new chaotic maps introduced in Section 4. Comparisons and analysis

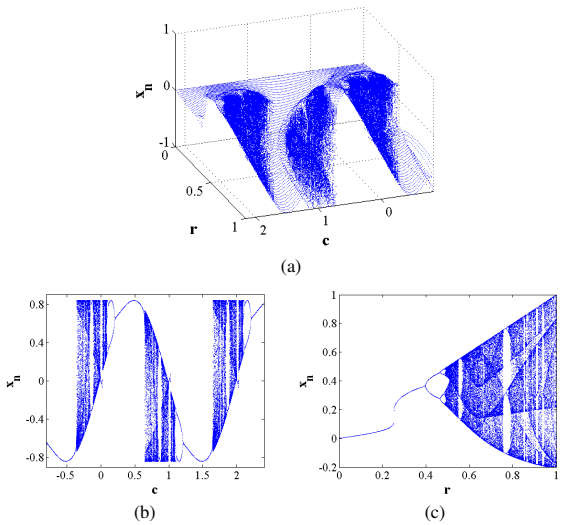


Fig. 8: The bifurcation diagrams of the Gaussian-Sine map with different parameter settings. (a) the 3D bifurcation diagram with parameters r ∈[0, 1], c ∈[-0.8, 2.2] and b = 6.2; (b) r = 0.84, b = 6.2, c ∈[-0.8, 2.2]; (c) c = -0.07, b = 6.2, r ∈[0, 1].

show that these new chaotic maps have better chaos performance than their corresponding seed maps.

5.1. Lyapunov Exponent

The Lyapunov exponent [8] is an important quantitative standard to evaluate the chaos feature of a dynamical system. It denotes the exponential divergences between two infinitesimally close trajectories in the phase space. A positive Lyapunov exponent value means that the differences between two trajectories, no matter how small differences their initial values are, will increase exponentially along the time and thus make their trajectories unpredictable. In other words, a system with one or more positive Lyaponov exponents is chaotic.

The Lyapunov exponent for a 1D discrete time system $x_{n+1} = f(x_n)$ is defined as Eqn. (8)

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)| \tag{8}$$

where n denotes the total number of iterations and $f'(x)$ is the first-order derivative of $f(x)$.

The Lyapunov exponent values of three new chaotic maps are shown in Fig. 9. As can be seen in Fig. 9(a) and (b), the Lyapunov exponent distributions of the Logistic-Sine map along with parameter a and with parameter r are similar. This is because chaotic behaviors of the Logistic and Sine maps are similar as shown in Fig. 1(a) and (b). In Fig. 9(d), the Lyapunov exponent distribution of the Gaussian-Sine map along with the parameter c is periodic. Compared with its Lyapunov exponent distribution in Fig. 9(d) with its bifurcation diagram in Fig. 8(b), the Gaussian-Sine map has the same chaotic behaviors in the parameter ranges c ∈[-0.5, 0.5] and c ∈[0.5, 1.5].

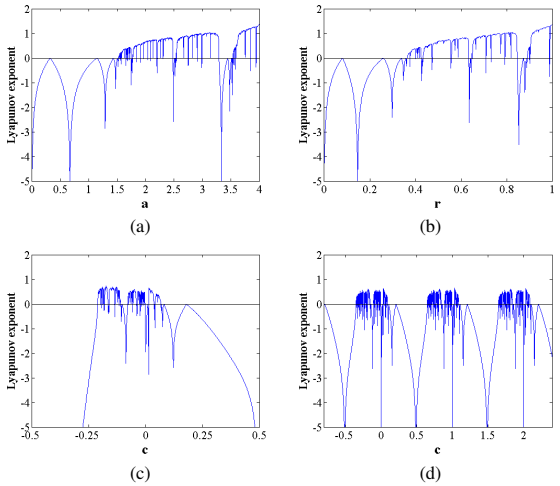


Fig. 9: The Lyapunov exponent values of the newly generated chaotic maps. (a) the Logistic-Sine map: r = 1, a ∈[0, 4]; (b) the Logistic-Sine map: a = 4, r ∈[0, 1]; (c) the Gaussian-Logistic map: a = 3.49, b = 6.2, c ∈[-0.5, 0.5]; (d) the Gaussian-Sine map: r = 0.84, b = 6.2, c ∈[-0.8, 2.2].

5.2. Iteration function diagram

For an iteration map $x_{n+1} = f(x_n)$, the iteration function diagram is to show the iteration outputs x_{n+1} along with different inputs x_n.

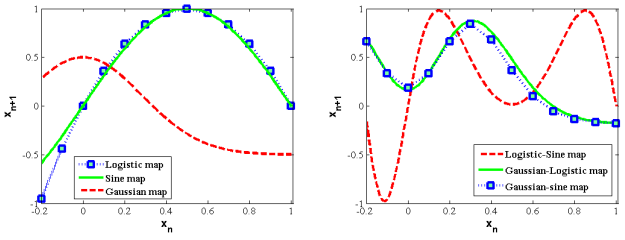


Fig. 10: The iteration function diagrams. (a) the Logistic, Sine and Gaussian maps; (b) the Logistic-Sine, Gaussian-Logistic and Gaussian-Sine maps.

The iteration function diagrams of newly generated maps are shown in Fig. 10(b). As can be seen, the iteration function diagram of the Gaussian-Logistic map is similar with that of the Gaussian-Sine map. This is because the Logistic and Sine maps have similar iteration function diagrams which can be seen in Fig. 10(a). The results in Fig. 10(b) show that the iteration functions of newly generated maps have more complex structures compared with their seed maps. It makes the output of new chaotic maps difficult to be predicted. This property is useful for security applications.

Table 1: The correlation comparisons of the output sequences generated by the new chaotic maps and their seed maps.

Parameters (r, a)	$(0.949, 3.64)$		$(0.981, 3.95)$	
	Correlation of S_1, S_2	Correlation of S_3, S_4	Correlation of S_1, S_2	Correlation of S_3, S_4
Logistic map (a)	0.811877	0.799098	-0.010366	-0.030699
Sine map (r)	-0.096664	-0.098244	-0.033337	-0.006322
Logistic-Sine map (r, a)	0.025092	0.001360	-0.001901	-0.001561
Parameters (a, b, c)	$(3.49, 6.2, -0.05)$		$(1.58, 6.2, -0.62)$	
Gaussian map (b, c)	1	0.993685	-0.060466	0.043801
Logistic map (a)	0.999999	0.995623	0.999816	0.045439
Gaussian-Logistic map (a, b, c)	-0.000757	-0.029911	0.033942	0.000725
Parameters (r, b, c)	$(0.88, 6.2, -0.07)$		$(0.5, 6.2, -0.6)$	
Gaussian map (b, c)	1	0.991556	-0.003322	0.040779
Sine map (r)	0.856123	0.889449	0.999898	-0.009045
Gaussian-Sine map (r, b, c)	0.022485	-0.005757	0.000801	0.000393

5.3. Correlation

The correlation is a measure that can reflect the distance between two sequences. It is defined as Eqn. (9)

$$Co = \frac{E[(X - \mu_X)(Y - \mu_Y)]}{\sigma_X \sigma_Y} \tag{9}$$

where X and Y are two sequences, μ is the mean value and σ is the standard deviation. From the definition we can see that, if the correlation value between two sequences, generated by a chaotic map with infinitesimally different settings of control parameters or initial values, is close to 0, the map will have chaotic behaviors, and smaller absolute correlation value indicates better chaos performance.

Experiments in Fig. 11 and Table 1 are to evaluate how the output sequences of a chaotic map are sensitive to its initial values and parameters. In Fig. 11, two sequences S_1 and S_2 in each plot are obtained by applying a tiny change to their initial values of the chaotic maps, and two sequences S_3 and S_4 are obtained by applying a tiny change to their parameters. As can be seen in Fig. 11, the correlations of all sequences dynamically change in the entire data range. This means that they all have no correlation with each other, and that these chaotic maps are extremely sensitive to their initial values and parameters.

Table 1 also shows the quantitative results of the correlation comparisons between the new chaotic maps and their corresponding seed maps. From Table 1, we can see that the absolute correlation scores of the new chaotic maps are smaller than those of their corresponding seed maps. This further verifies that the new chaotic maps are extremely sensitive to their initial values and parameters.

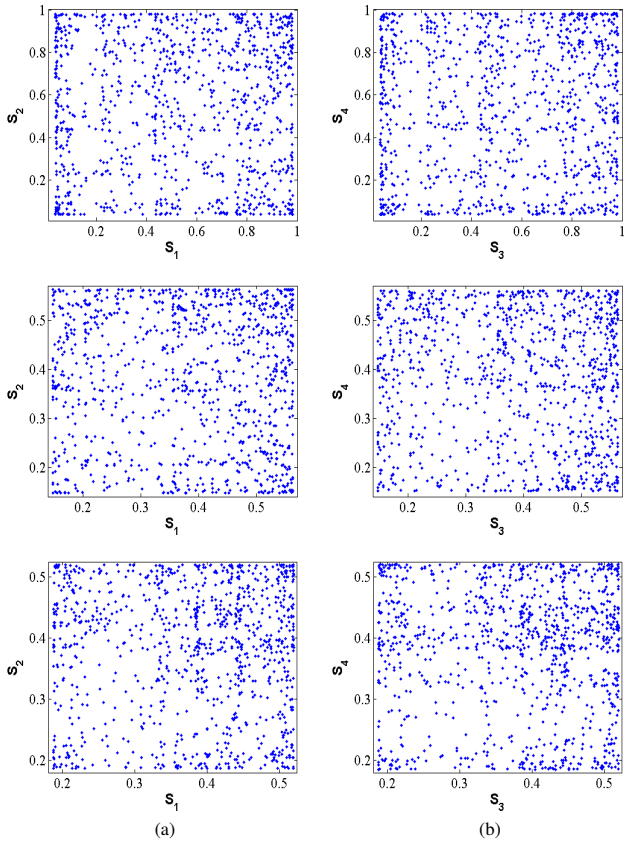


Fig. 11: The correlations of sequences generated by different chaotic maps. The first, second and third rows plot the corrections of sequences generated by the Logistic-Sine, Gaussian-Logistic and Gaussian-Sine maps, respectively, with a tiny change applied to (a) initial values; and (b) parameters.

5.4. Shannon entropy

Shannon entropy [9] is a quantitative measure of distributivity for a signal. It can be used to measure the distribution of

chaotic sequence. Mathematically, the Shannon entropy is defined as Eqn. (10)

$$H(X) = -\sum_{i=1}^{n} Pr(x_i) log_2 Pr(x_i) \quad (10)$$

where X represents a collection of data, x_i is the i^{th} possible value of the data and $Pr(x_i)$ is the probability of x_i. In our test, we set #Bin:256 means that we uniformly separate our testing data into 256 different levels. Table 2 shows the Shannon entropy results between the new chaotic maps and their seed maps. The bigger Shannon entropy value means that the chaotic sequence shows better randomness. We can see from Table 2 that the Shannon entropy values of the chaotic sequences generated by the new chaotic maps are bigger than those of their seed maps. This means that the newly generated chaotic maps have a better chaos performance than their corresponding seed maps.

Table 2: The Shannon entropy comparisons between the new chaotic maps and their seed maps (#Bins:256).

Parameters (r, a)	$(0.949, 3.64)$	$(0.981, 3.95)$
Logistic map (a)	6.6043	7.6714
Sine map (r)	6.8658	7.6720
Logistic-Sine map (r, a)	7.2120	7.7120
Parameters (a, b, c)	$(3.49, 6.2, -0.05)$	$(1.58, 6.2, -0.62)$
Gaussian map (b, c)	2	0
Logistic map (a)	1	6.9836
Gaussian-Logistic map (a, b, c)	7.6636	7.2466
Parameters (r, b, c)	$(0.88, 6.2, -0.07)$	$(0.5, 6.2, -0.6)$
Gaussian map (b, c)	6.4565	0
Sine map (r)	1	6.9521
Gaussian-Sine map (r, b, c)	7.5677	7.4743

6. CONCLUSION

In this paper, a new series-wound framework was proposed. Using this framework, a large number of new 1D chaotic maps can be generated from different pair of two seed maps. Three examples of the new 1D chaotic maps, the Logistic-Sine, Gaussian-Logistic and Gaussian-Sine maps, were also introduced to demonstrate the performance of the proposed framework.

Experimental analysis and quantitative measures between three presented chaotic maps and their seed maps have shown that new chaotic maps have better chaos performance and more complex structures than their corresponding seed maps. The proposed framework can be use for communication and security applications.

7. ACKNOWLEDGEMENT

This work was supported in part by the Macau Science and Technology Development Fund under Grant 017/2012/A1 and by the Research Committee at University of Macau under Grants SRG007-FST12-ZYC, MYRG113(Y1-L3)-FST12-ZYC and MRG001/ZYC/2013/FST.

8. REFERENCES

[1] D. S. Broomhead, J. P. Huke, and M. R. Muldoon, "Codes for spread spectrum applications generated using chaotic dynamical systems," *Dynamics and Stability of Systems*, vol. 14, no. 1, pp. 95–105, 1999.

[2] Qian Qinchun, Chen Zengqiang, and Yuan Zhuzhi, "Video compression and encryption based-on multiple chaotic system," in *Innovative Computing Information and Control, 2008. ICICIC '08. 3rd International Conference on*, 2008, pp. 561–561.

[3] J. C. Yeo and J. I. Guo, "Efficient hierarchical chaotic image encryption algorithm and its vlsi realisation," *Vision, Image and Signal Processing, IEE Proceedings -*, vol. 147, no. 2, pp. 167–175, 2000.

[4] Zhang Tong, Zhou Yicong, and C. L. P. Chen, "A new combined chaotic system for image encryption," in *Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on*, 2012, vol. 2, pp. 331–335.

[5] Bao Long, Zhou Yicong, C. L. P. Chen, and Liu Hongli, "A new chaotic system for image encryption," in *System Science and Engineering (ICSSE), 2012 International Conference on*, 2012, pp. 69–73.

[6] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, and V. Fernandez, *On the security of a new image encryption scheme based on chaotic map lattices*, Chaos: An Interdisciplinary Journal of Nonlinear Science, 18(2008) 033112. 7 pp.

[7] M. I. Sobhy and A. E. R. Shehata, "Methods of attacking chaotic encryption and countermeasures," in *Acoustics, Speech, and Signal Processing, 2001. Proceedings. (ICASSP '01). 2001 IEEE International Conference on*, 2001, vol. 2, pp. 1001–1004 vol.2.

[8] G. Jakimoski and K. P. Subbalakshmi, "Discrete lyapunov exponent and differential cryptanalysis," *Circuits and Systems II: Express Briefs, IEEE Transactions on*, vol. 54, no. 6, pp. 499–501, 2007.

[9] C. E. Shannon, "A mathematical theory of communication," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 5, no. 1, pp. 3–55, 2001.