

Controllable V-Shape Multi-Scroll Butterfly Attractor: System and Circuit Implementation

M. AFFAN ZIDAN

*Electrical Engineering, King Abdullah University of Science and Technology (KAUST),
Thuwal, Kingdom of Saudi Arabia 23955-6900
mohammed.zidan@kaust.edu.sa*

A. G. RADWAN*

*Electrical Engineering, King Abdullah University of Science and Technology (KAUST),
Thuwal, Kingdom of Saudi Arabia 23955-6900
agradwan@ieee.org*

K. N. SALAMA

*Electrical Engineering, King Abdullah University of Science and Technology (KAUST),
Thuwal, Kingdom of Saudi Arabia 23955-6900
khaled.salama@kaust.edu.sa*

In this paper, a new controllable V-shape multi-scroll attractor is presented, where a variety of symmetrical and unsymmetrical attractors with a variable number of scrolls can be controlled using new staircase nonlinear function and the parameters of the system. This attractor can be used to generate random signals with a variety of symbol distribution. Digital implementation of the proposed generator is also presented using a Xilinx Virtex[®] 4 Field Programmable Gate Array and experimental results are provided. The digital realization easily fits into a small area (< 1.5% of the total area) and expresses a high throughput (4.3Gbit/s per state variable).

Keywords: Controlled Chaos, Digital Chaos Generator, Multi-scroll Attractor

1. Introduction

Butterfly attractors, first introduced in [Lorenz, 1963], are among the mostly known chaotic systems. The original butterfly attractor was defined by three differential equations, with multiplication as the non-linear element. The attractors in [Elwakil & Kennedy, 2001; Chen & Lu, 2003], introduced modified versions of the system to create butterfly attractors without the need of multiplication. Rather, the sign and modulus functions are used as the nonlinear elements. Several other multi-scroll versions of the butterfly attractor were introduced based on variety of techniques [Yu *et al.*, 2010; Lu & Chen, 2006], such as using a pulse signal [Elwakil *et al.*, 2002a; Elwakil & Ozogus, 2008], a sawtooth wave function [Yu *et al.*, 2008], or a piecewise linear function [Zhang *et al.*, 2008].

Chaos control received increased research attention in the last two decades due to its useful engineering applications. For example, chaotic oscillators find applications in chaotic based digital communication systems [Chen *et al.*, 2010] such as chaos shift keying (CSK) [Galias & Maggio, 2001; Xia *et al.*, 2004] and chaotic pulse-position modulation [Chiang & Hu, 2010]. Moreover, chaos is used in cryptography [Guglielmi

*A. G. Radwan is also with the Department of Engineering Mathematics, Faculty of Engineering, Cairo University, Egypt

et al., 2009; Pareschi *et al.*, 2009], water marking and image encryptions [Sidiropoulos *et al.*, 2009; Mazloom & Eftekhari-Moghadam, 2009; Barakat *et al.*, 2011], and random number generation [Ergn & Ozoguz, 2010; Zidan *et al.*, 2011b]. In addition, multi-scrolls attractors are proven to have better properties, like having higher entropy for random number generation, compared to normal attractors [Yalcin, 2007]. The implementation of these generators ranges from using discrete elements and operational amplifiers [Lu *et al.*, 2006; Elwakil & Kennedy, 2001; Salama *et al.*, 2003], completely MOS based [Radwan *et al.*, 2004; Tavas *et al.*, 2010], to fully integrated [Elwakil *et al.*, 2002b]. Hybrid analog/digital implementation was introduced in [Radwan *et al.*, 2007]. In addition, several digital implementations have been presented recently, using logistic maps as in [Chen *et al.*, 2010] and the numerical solution of differential based chaotic equation as in [Zidan *et al.*, 2011b; Mansingka *et al.*, 2011a,b].

In this paper, a new multi-scroll attractor based on a staircase nonlinear function is presented. The system did not require external inputs to move from one scroll to another. Rather, the output shifts between the multiple scrolls in a chaotic scheme. The proposed attractor have the new scrolls aligned in a diagonally scheme rather than vertical or hormonal. These scrolls can be shaped into a variety of symmetrical and unsymmetrical shapes, including V- and Heart-shapes. The number of scrolls can be asymmetrically controlled using the parameters of the system. This controlled multi-scroll attractor can be used to generate random signals with a variety of symbol distributions which could find future applications.

The time series output of the system variable can be controlled to have either a shifting DC bias or a variable amplitude by moving between different scrolls. The proposed multi-scroll system is based on the modified Lorenz butterfly, which is defined in [Elwakil & Kennedy, 2001] as,

$$\dot{X} = a(Y - X) \quad (1a)$$

$$\dot{Y} = \text{sign}(X)(b - Z) \quad (1b)$$

$$\dot{Z} = |X| - cZ \quad (1c)$$

where \dot{X} , \dot{Y} and \dot{Z} are the differential equations defining the system, and a , b and c are the system's parameters. This system is transformed to multi-scroll using the new proposed nonlinear function. The introduced system is verified to be chaotic using its attractor and by having a positive Maximum Lyapunov Exponent (MLE). To implement chaotic generators on digital system, is also presented. For further validation purposes, the system is implemented on Xilinx Virtex[®] 4 XC4VSX35 Field Programmable Gate Array (FPGA), and experimental results are provided. The realization fits into a very small area, exhibits a high throughput, and allows introducing controllable version of the circuit.

2. Proposed Multi-Scroll Attractor

Based on the modified Lorenz attractor given in [Elwakil & Kennedy, 2001], we introduce a new multi-scroll attractor by adding additional nonlinear function to the system. The introduced system did not require external input for expressing the multi-scroll scheme. The original system given in equation (1) is modified as,

$$\dot{X} = Y - X \quad (2a)$$

$$\dot{Y} = \text{sign}(X)[1 - mZ + G(Z)] \quad (2b)$$

$$\dot{Z} = |X| - 0.5Z \quad (2c)$$

where m is an added parameter to the system and $G(Z)$ is the nonlinear function responsible to produce multi-scroll. The new proposed staircase nonlinear function, $G(Z)$ is defined as a step-piecewise function, such that,

$$G(Z) = \begin{cases} 0 & Z < S_0 \\ d_1 & S_0 \leq Z < S_1 \\ \vdots & \vdots \\ d_{N-1} & Z \geq S_{N-1} \end{cases} \quad (3)$$

where d_i is the additive coefficient and s_i is the limiting coefficient. The introduced piecewise nonlinear equation is a multiple-step function resembling the shape of stairs, and the number of scrolls of the attractor is $2N$. Fig 1(a) shows the proposed multi-scroll attractor.

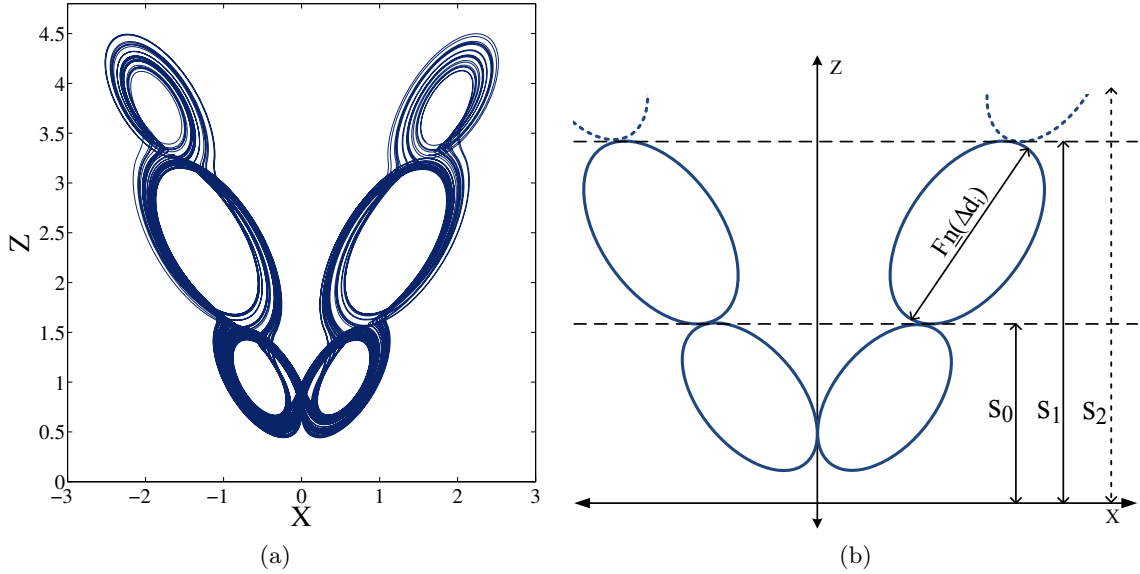


Fig. 1. (a) Multi-scroll attractor created using the proposed system. Used parameters: $N = 3$, $m = 1$, $d_1 = 1.4$, $d_2 = 2.8$, $s_0 = 1.555$, and $s_1 = 3.25$. (b) Illustration for the V-shape attractor showing the effect of Δd_k and s_i .

2.1. Controlling the attractor shape

The shape of the attractor is mainly controlled by the coefficients d_i , s_i , and m . Using these parameters a variety of attractors can be produced. The additive coefficients (d_i) control the size of the generated scrolls by following governing equation:

$$\Delta d_k = d_k - \sum_{i=1}^{k-1} d_i \quad (4)$$

where $k = \{1, 2, \dots, N - 1\}$. The limiting coefficients (s_i), however, define the boundaries at which the system shifts from one scroll to another. All these parameters should be selected to terminate each scroll at the correct position. Fig. 1(b) shows how the additive and the limiting coefficients affects the shape of the output. The figure also shows that the limiting coefficients should be set to limit the scrolls just at its upper edge.

Symmetrical V-shape attractor:

A V-shape multi-scroll attractor can be achieved by designing the system parameters such that all the scrolls possess the same size, as can be seen in Fig. 2(a). These equal sized scrolls are generated by setting the (d_i) coefficients to:

$$\Delta d_k = a, \forall k \quad (5)$$

where a is a constant that is set to produce scrolls of the same size of the original two scrolls. The parameters (s_i) will have in turn a constant difference between each two successive parameters, such that,

$$s_{k+1} - s_k = s_k - s_{k-1}, \forall k \quad (6)$$

Symmetrical heart-shape attractor:

The heart-shape is produced by setting the parameter $m = 2$. This amplifies of the effect of the variable Z in equations (2b), which changes the shape of the attractor significantly, and the attractor takes the shape of family of interconnected scroll-pairs, rather than a group of adjacent parabolic rings, as can be seen in Fig. 2(b).

Asymmetrical attractors:

An extra degree of freedom in shaping the attractor can be added by extending the nonlinearity to be function in X and Z simultaneously. In other words the system equation \dot{Y} changes to,

$$\dot{Y} = \text{sign}(X)(b - mZ + H(X, Z)) \quad (7)$$

and H is given by,

$$H(X, Z) = \begin{cases} G^-(Z) & X < 0 \\ G^+(Z) & X \geq 0 \end{cases} \quad (8)$$

where $G^+(Z)$ and $G^-(Z)$ are two instants of the equation (3). In the modified equation, a different control is defined for the scrolls lies on the positive and negative parts of the X -axis. The modifications introduced in equation (7) allow the attractor to have different scroll shapes and numbers on the opposite sides of Z -axis. Fig. 4 shows two asymmetrical V-shape attractors created using the proposed nonlinear function, and shows also that the asymmetrical V-shape is as smooth as the symmetrical one.

2.2. Mathematical Analysis*Equilibrium points:*

The equilibrium points of the system described by (2) are given by,

$$Y^* = X^* \quad (9a)$$

$$Z^* = 2|X^*| \quad (9b)$$

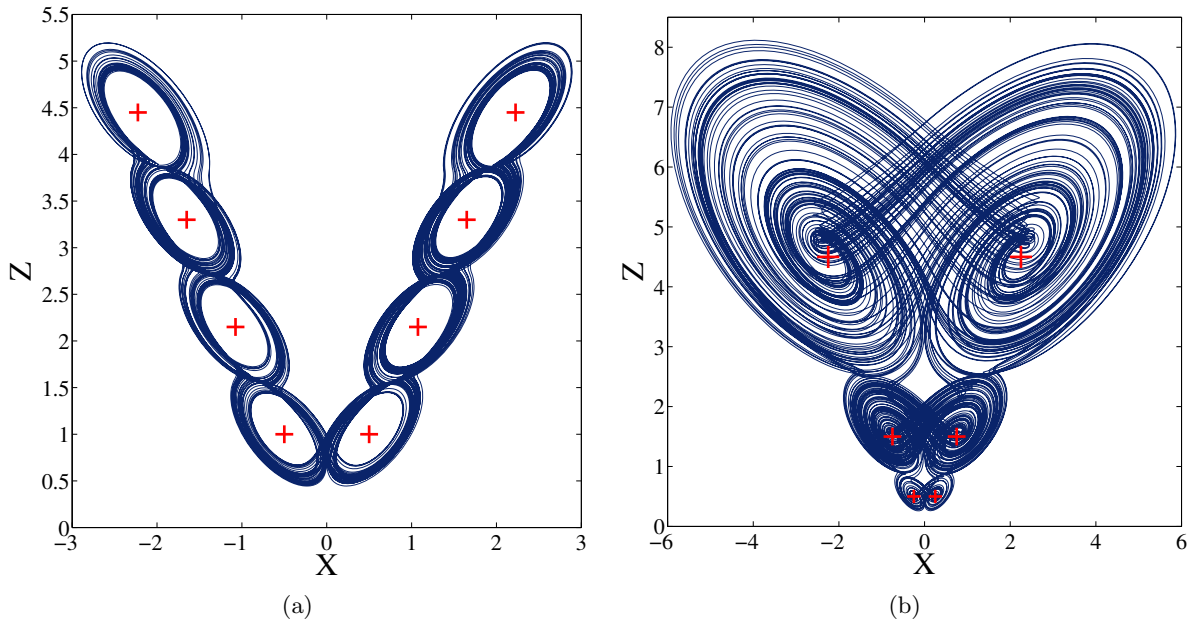


Fig. 2. (a) V-shape attractor, and (b) heart-shape attractor, created using the proposed system. Used parameters: (a) $N = 4$, $m = 1$, $d_1 = 1.15$, $d_2 = 2.3$, $d_3 = 3.45$, $s_0 = 1.56$, $s_1 = 2.7115$, and $s_2 = 3.863$; (b) $N = 3$, $m = 2$, $d_1 = 2$, $d_2 = 8$, $s_0 = 0.865$, and $s_1 = 2.53$. The red crosses marks the equilibrium points locations.

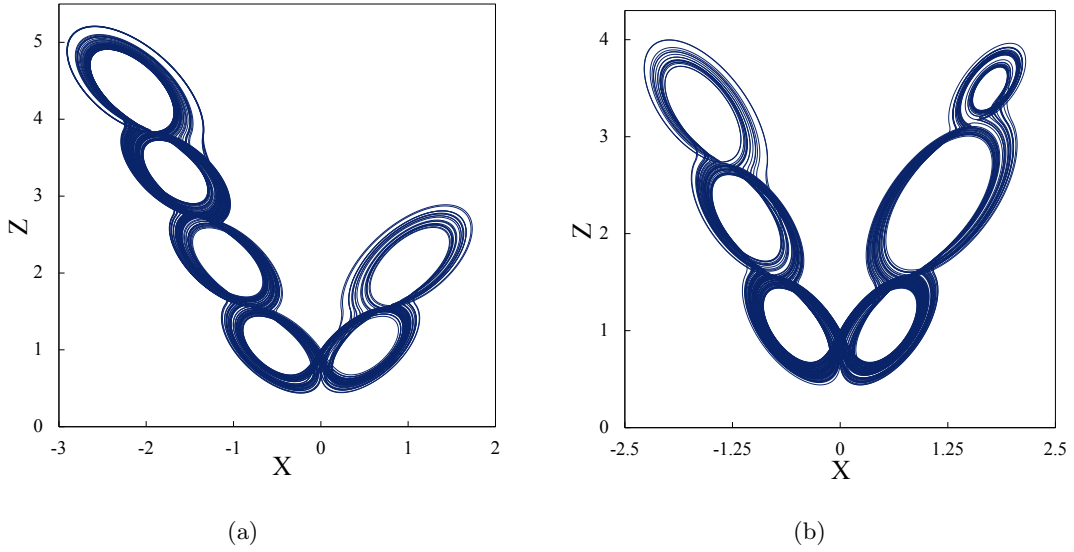


Fig. 3. Asymmetrical V-shape attractors. (a) Equal size scrolls, four on the negative X -axis part and two on the positive part. (b) Three equal size scrolls on the negative X -axis part and three different size scrolls on the positive direction.

$$G(Z^*) = mZ^* - 1 \quad (9c)$$

Based on equation (9c) we can get the following points,

$$Z_i^* = \frac{d_i + 1}{m}, \quad s_{i-1} < Z_i \leq s_i \quad (10a)$$

$$(X^*, Y^*, Z^*) = \left(\pm \frac{Z_i^*}{2}, \pm \frac{Z_i^*}{2}, Z_i^* \right) \quad (10b)$$

Fig. 2 shows the plot of the equilibrium points over the V- and Heart-attractors. In addition, a graphical method to obtain the equilibrium points is shown in Fig. 4(a).

Stability Analysis:

For each equilibrium point, the Jacobi matrix can be derived from,

$$J = \begin{pmatrix} -1 & 1 & 0 \\ 0 & 0 & \mp m \\ \pm 1 & 0 & -0.5 \end{pmatrix} \quad (11)$$

The upper sign is for positive X^* and the lower sign is for negative X^* . The trace of the Jacobi matrix is the sum of the eigenvalues, which equals to,

$$\text{trace}(J) = \nabla V = \frac{\partial f_x}{\partial X} + \frac{\partial f_y}{\partial Y} + \frac{\partial f_z}{\partial Z} = \sum_{i=1}^3 \lambda_i = -1.5 < 0 \quad (12)$$

and reflect that this is a dissipation system. Through the computation, the characteristic equation of this system is given by,

$$s^3 + 1.5s^2 + 0.5s + m = 0 \quad (13)$$

Therefore, the poles (eigenvalues) of this system are $(-1.5832, 0.0416 \pm 0.7937j)$ for $m = 1$, and $(-1.8260, 0.163 \pm 1.0338j)$ for $m = 2$. It is clear that in both cases, two poles exist in the right half plane while the other lies on the left half plane such that their summation is always negative. The poles versus the parameter m are shown in Fig. 4(b) where, the two conjugate poles are located on the $j\omega$ axis at $m = 0.75$ with eigenvalues $(-1.5, \pm 0.171j)$, and enter the unstable region at $m > 0.75$.

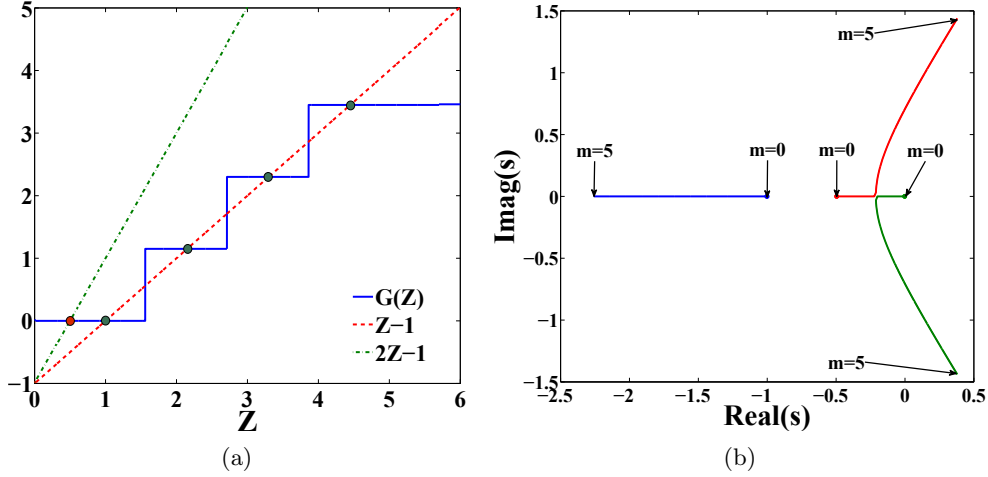


Fig. 4. (a) The locations of the equilibrium points for heart-shape with 2 scrolls ($2Z - 1$) and V-shape with $\{4, 4\}$ scrolls ($Z - 1$) (b) The poles of the system given in 2 for different values of m .

Symmetry:

It is clear from the system equations in (2) that the system is invariant under the transformation $(x, y, z) \rightarrow (-x, -y, z)$ with a symmetry plan at $Z = 0$.

2.3. Maximum Lyapunov Exponent (MLE)

While the output of the proposed system is in the shape of a chaotic attractor, the sufficient condition to prove chaos is to have a positive MLE [Pecora *et al.*, 1997]. Fig. 5 shows the calculated MLE for the original system and one of the proposed multi-scroll. Clearly, the figure shows that both of the systems have a positive MLE, saturating at 0.0288 and 0.0497 for the original and the multi-scroll systems respectively. The calculations are made using the tool provided in [Perc, 2010; Kodba *et al.*, 2005], with a time series containing more than 245,00 iterations.

3. A Digital Implementation Technique for Chaotic Generators

Differential based chaos generators are usually realized by implementing analog integrators that utilize big capacitors to store the system state. However, the initial condition of analog generators cannot be set precisely. Further more, the analog chaotic generators are sensitive to the running conditions, process

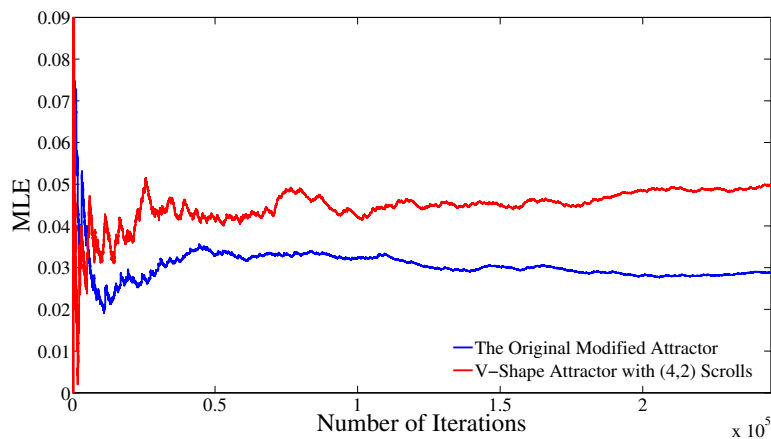


Fig. 5. The MLE versus number of iterations for the originally introduced modified system and asymmetrical V-shape attractor with four scrolls on the left size and two scrolls on the right side.

variations, and the operating temperature. On the other hand, a digital implementation does not require any capacitors, and registers are used to store the state of the system. The latter important characteristic of digital chaos generator is its extremely small areas. This approach enables us to generate the digital data directly in contrast to earlier methods where the continuous time chaotic circuit is used as the entropy source followed by a threshold function implemented using comparators [Yalcin *et al.*, 2004] or a successive approximation Analog to Digital Converter (ADC) [Tavas *et al.*, 2010].

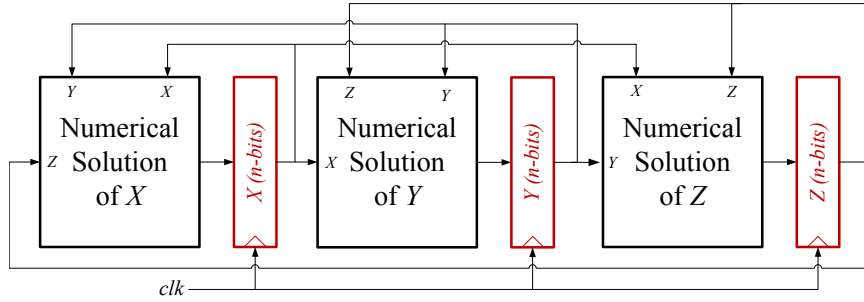


Fig. 6. The general schematic of the digital implementation for any third-order differential-based digital chaotic generator.

Any chaos generator can be implemented in a digital scheme by realizing the numerical solution of the nonlinear differential equation that describes the system. Explicitly, registers are used to store the state of the system, while the solution is implemented as combinational circuits [Zidan *et al.*, 2011b; Mansingka *et al.*, 2011a,b]. Fig. 6 shows the general architecture for any third-order differential-based digital chaotic generator. As can be seen, the system state variables X , Y and Z are stored into three n -bit registers. The numerical solution of the state variables X , Y and Z are realized as combinational blocks. A comparison for the chaotic response of different numerical solutions is discussed in [Zidan *et al.*, 2011a].

Realization of the proposed system:

The proposed system is implemented digitally by realizing its numerical solution. The system of equations given in (2) is solved using Euler method, such that,

$$F_x(X, Y) = X_{t+h} = X_t + h(Y_t - x_t) \quad (14a)$$

$$F_y(X, Y, Z) = Y_{t+h} = Y_t + h \text{sign}(X_t) [b - mZ_t + G(X_t)] \quad (14b)$$

$$F_z(X, Z) = Z_{t+h} = Z_t + h(|X_t| - 0.5Z_t) \quad (14c)$$

where t denotes the time and h denotes the time step.

The state variables X , Y and Z are realized as n -bit registers, where n is the number of bits used to represent numbers in the digital system. The registers are updated with the new state at each positive edge of a clock cycle. These registers are the sequential part of the system, and rather than that equations (14) are implemented in a combinational scheme. The effect of the bus-width (n) where studied in [Mansingka *et al.*, 2011b], where it was found that very small values for n is not sufficient for generating chaos. According to [Mansingka *et al.*, 2011b] the MLE peak is due to the added nonlinearity to the system by limited number of bits.

The area and the delay of the system were improved by using different techniques. Among these improvements is the elimination of multiplication by constant operation, by converting this operation into wired shift. This conversion is done by setting the values of the constants to be in the orders of two. The multiplication by the time step h is neutralized by setting its value as $h = 2^r$, where r is an integer and is set to 4 in the proposed implementations. The other constant multiplication m is eliminated natively, since m only takes the value of one or two.

Fig. 7 shows the schematic of the implementation. The function $F_x(X, Y)$ given in equation (14a) is implemented as a multi-input adder circuit, with X added to a shifted version of Y and $-X$. The bottleneck

of the system which describes the $F_y(X, Y, Z)$ function, is equation (14b), and includes the evaluation the proposed nonlinear function $G(Z)$. The calculated $G(Z)$ is then added to '1' and subtracted from a shifted version of Z . The output of this operation, *i.e.* the expression $[b - mZ_t + G(X_t)]$, is multiplied by $\text{sign}(X_t)$, which is equivalent to a two's complement circuit with the $\text{sign}(X_t)$ as "enable". Then, Y is added to a shifted version of the two's complement output. The last expression $F_z(X, Z)$, given in equation (14c), is finally evaluated by calculating the summation of Z , shifted version of Z , and the shifted version of $|X|$.

The asymmetrical attractors are implemented by realizing the nonlinear function $H(X, Z)$ in equation (8). The implementation of this expression was done by multiplexing two version of $G(Z)$ for the positive and negative values of X , where the MUX selection line is the sign bit of X .

The outputs of the chaotic generator are within bounded intervals, which saves the shape of the attractor. Therefore, fixed-point numbers representation is suitable for system realization. This selection will reduce the area required and delay significantly. Distribution of the 32 bits is used within the system. Selection was governed by the bounding interval of the multi-scroll output, the bounding interval of the intermediate results, and the effect of the negative shift of the parameter (h). The 32-bits are distributed such that the highest significant bytes are reserved for the two's complement integer and the rest of the bits are for the fraction part.

Nonlinear circuit realization:

The piecewise nonlinear function $G(Z)$, given in equation (3), can be simply implemented as a series of comparators along with a multiplexer (MUX). An optimized version on this technique is provided in Fig. 8(a), where parallel comparators are used and their outputs are encoded to drive the MUX selection lines. Based on the selection input, the MUX will select from the set of $\{0, d_1, \dots, d_{N-1}\}$.

The nonlinear function can be also redefined as,

$$G(Z) = \frac{1}{2} \sum_{l=0}^N \Delta d_l * (\text{sign}(Z - s) + 1) \quad (15)$$

where $\Delta d_0 = 0$. With equation (15), another implementation is provided in Fig. 8(b), where the Δd parameters are used to shape the attractor directly (rather than d). Since the usage of Δd eases the shaping of the attractor, since it is directly affect the size of each scroll as shown in Fig. 1(b). The implementation based on Δd is shown in Fig. 8(b).

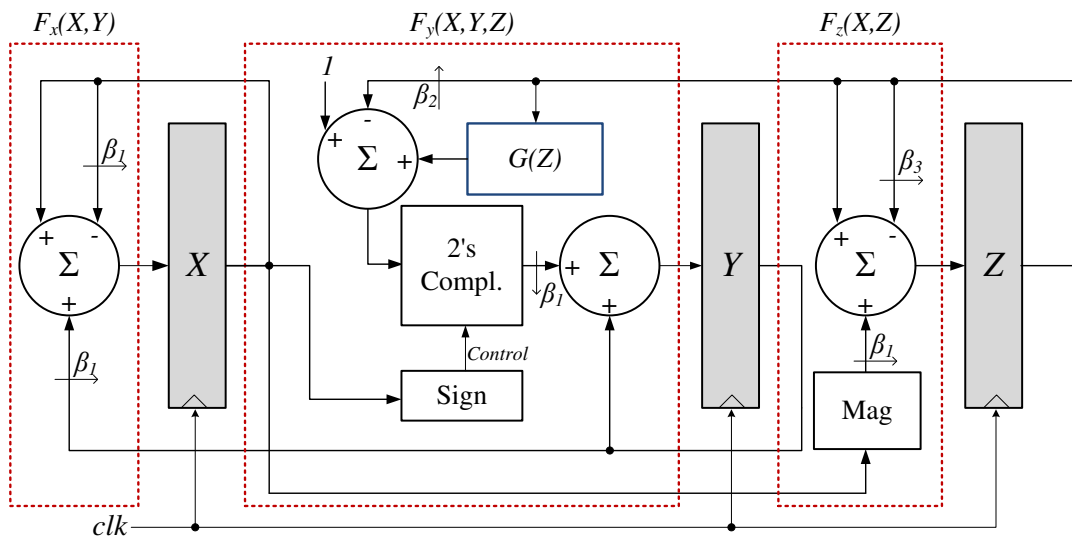


Fig. 7. Schematic diagram for the implementation of the proposed system. All the wires represent buses. The β_i is a wired shift, where $\beta_1 = \log_2(h)$, $\beta_2 = \log_2(mh)$, and $\beta_3 = \log_2(0.5h)$.

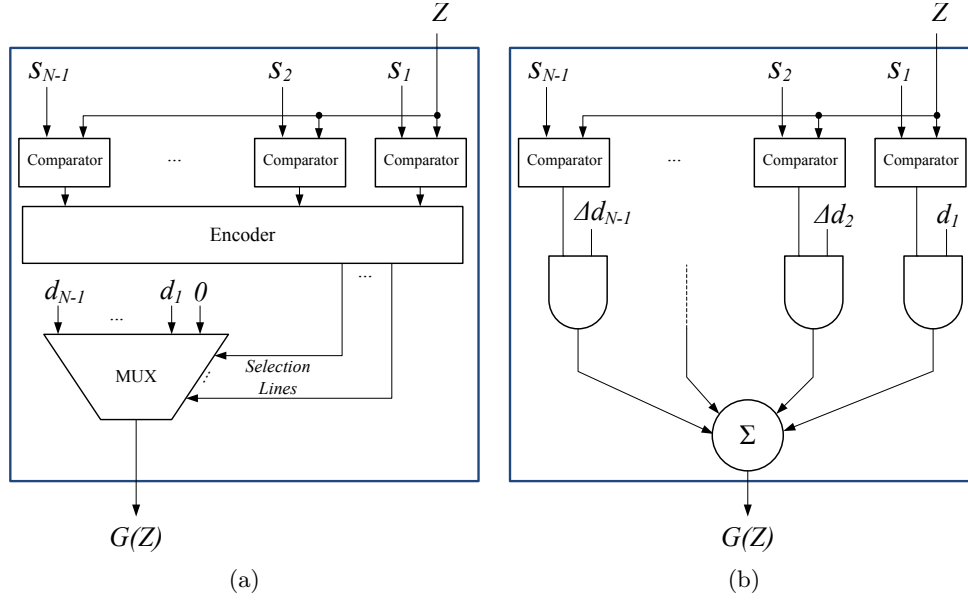


Fig. 8. Block diagram of the different realizations of the nonlinear function, $G(Z)$.

Real-time Controllable Circuit:

Controlling the shape of the scrolls was based on determining which scrolls are to be generated and the size of each scrolls. Fig. 9 shows a simple circuit that is capable of controlling the scrolls generation. The circuit is based on enabling or disabling the Δd variables based on an external input. By referring to equation (15), it could be concluded that the number of scrolls can be limited by setting the higher order Δd parameters to zero. The Δd enabling could be fully controlled by the user simply by using the control lines as shown in Fig. 9. Further, the used control can be limited to selecting the number of scrolls, and this number decoded internal to enable the control lines.

The control could be extended by registering the values of Δd from an external input. This scheme will enable controlling the size of scrolls beside its number. Despite this controlling privilege, it should be noted that changing the values of the additive coefficient, forces us to reset the limiting coefficient. Finally, the shape of the attractor selected from V- and heart-shapes by setting the value of the parameter m .

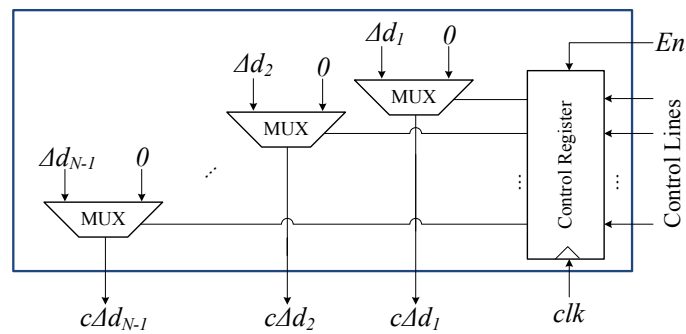


Fig. 9. Block diagram of the circuit used to control the scrolls of the attractor.

4. Experimental Results

The proposed multi-scroll system were written in Verilog VHDL and realized on Xilinx Virtex[®] 4 XC4VSX35 FPGA. Within the simulation phase, Xilinx ISE[®] 11 and the GNU iVerilog software were used. The attractors, the time diagrams, and the histograms are captured using the TekTronix[™] MSO

414 mixed signal oscilloscope. All the circuits were synthesized using Xilinx ISE[®] 11, with optimized for time (speed) option selected.

The introduced circuit exhibits small area and high throughput. Table 1 shows the occupied area and the maximum frequency and throughput for various implementations. The results shows the multi-scroll system can reach a maximum frequency of 134.7 MHz (4.3 Gbits/s per state variable) and less than 1.5% of the total area of the used FPGA. The area and speed were calculated with the variables X and Z used as the output ports. The achieved throughput exceeds the data reported by Intel in [Taylor & Cox, 2011]

Table 1. Detailed area utilization and the maximum frequency and throughput for different implementations on Xilinx Virtex 4[®] XC4VSX35 FPGA.

Attractor Type	Slice Flip-flops (30,720)	Look-Up-Tables (30,720)	Frequency (MHz)	Throughput (Gbit/s)
Original Attractor	97	255	130.1	4.2
Heart-Shape (6 scrolls)	97	235	134.7	4.3
V-Shape (12 scrolls)	105	359	99.3	3.2

4.1. *Attractors*

The attractor shape is the main property that differentiates between chaotic systems. Thus, Fig. 10 shows several snapshots from the oscilloscope for different system implementations of the attractors in the Z - X plane for comparison purposes. Figures 10(a-d) show the symmetric V-shape implementations for 4, 6, 8, and 12 scrolls respectively, the figures 10(e-h) show the generated asymmetrical V-shape attractors, figures 10(i-j) show a V-shape attractor with different scrolls' sizes, controlled using Δd , and finally, the figures 10(k-l) show the heart shape attractor, where the parameter $m = 2$.

4.2. *Time outputs and histograms*

Fig. 11 shows the time series output of the various implementations as captured from the oscilloscope, for the variable (X), where it is clearly shown the different time series for different implementation. The V-shape time response shows that the DC value of the oscillation changes as the attractor shifts from

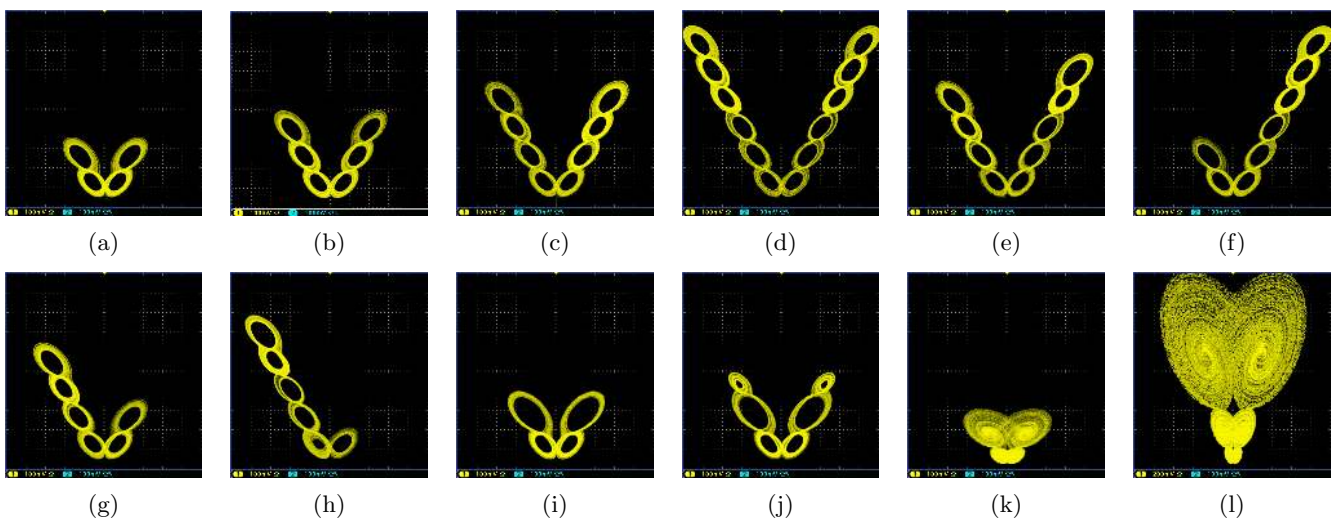


Fig. 10. Oscilloscope snapshots of the attractors' projection on the Z - X plane for different system implementations, (a-d) symmetric V-shape, (e-f) asymmetrical V-shape, (i,j) V-shape attractor with different scrolls' sizes, and (k,l) heart-shape. $Z, X = 100$ mV/div and each sub-figure is 10 divisions per axis.

one scroll to another, as shown in the figures 11(a-c). On the other hand, the amplitude of the oscillation changes when the attractor moves between scrolls in the heart-shape, as shown in figure 11(d). The time series reveals the number of scrolls within the system, as DC levels for V-shape, or different oscillations amplitude as in heart-shape. Figure 11(b) shows the time response for an unbalanced V-shape attractor, with different number of scrolls on the two sides of the Z-axis. The unbalanced V-Shape attractor has a nonzero total DC bias for the time series of the variable (X).

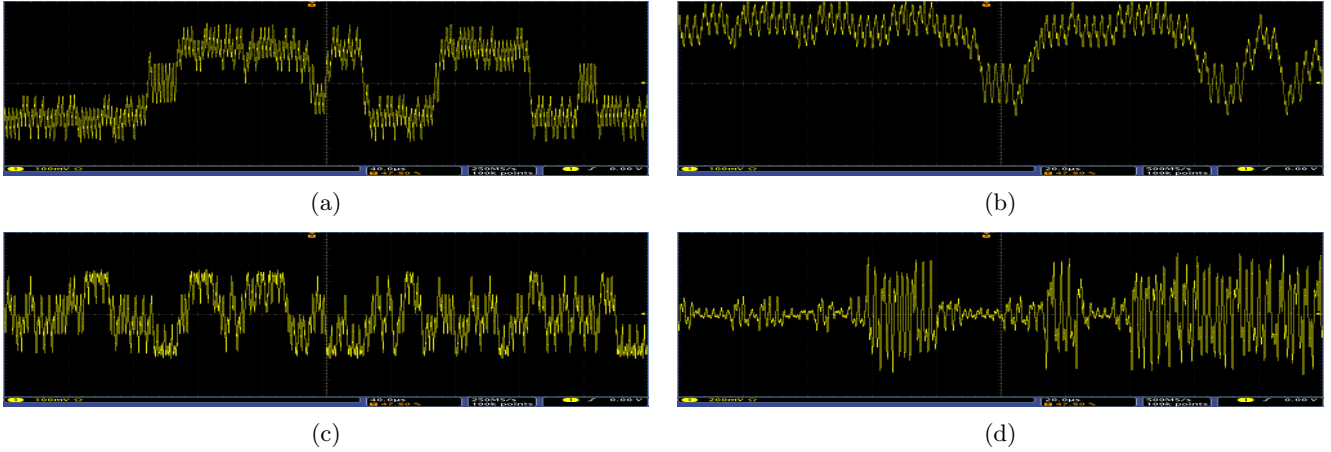


Fig. 11. Oscilloscope time series output of the various implementations for the variable (X). The sub-figures shows (a) 8-scrolls symmetric V-shape, (b) asymmetrical V-shape with two scrolls on the left side and six on the right, (c) 6-scrolls V-shape with different sized scrolls, and (d) 6-scrolls heart-shape. $X = 100$ mV/div and each sub-figure shows 10 divisions on X -axis.

The histogram or the output depends mainly on the shape of the generated attractor. Combining this property with the ease of control of the shape of the proposed attractor, shaping the histogram becomes possible. This property can be attractive for applications that require a special shape of histogram with a random output. Fig. 12 shows a comparison between the histogram of symmetric and asymmetrical attractors. Although the number of distinct histograms depends on many factors, including system parameters and the numbers of used bits, a rough estimate can be calculated using the number of scrolls. For a system consisting of $\{n, m\}$ maximum scrolls (V-shape), the total number of histograms is $n \cdot m$. Some of these histograms will be almost mirrored such as the cases $\{1, 2\}$ and $\{2, 1\}$. Thus the number of distinct histograms can be calculated using the following formula,

$$N_{histograms} = n \cdot m - \frac{\min(n, m) (\min(n, m) - 1)}{2} \quad (16)$$

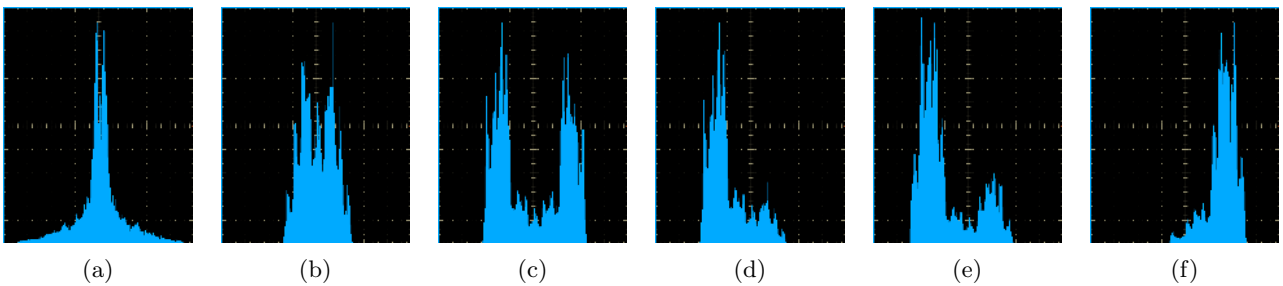


Fig. 12. Histogram oscilloscope snapshots of the variable X for (a) 6-scrolls heart shape attractor, (b) $\{3,3\}$ -scrolls symmetric V-shape attractor, (c) $\{4,4\}$ -scrolls symmetric V-shape attractor, (d) $\{5,3\}$ -scrolls asymmetrical V-shape, (e) $\{6,4\}$ -scrolls asymmetrical V-shape, and (f) $\{1,6\}$ -scrolls asymmetrical V-shape

5. Conclusion

In this paper a new controllable multi-scroll attractor is presented. A variety of symmetrical and asymmetrical attractors with controlled number of scrolls can be provided, including V- and heart-shapes. The introduced system is based on a proposed staircase nonlinear function, which is different from previously published nonlinear functions. The system is verified to be chaotic by calculating the Maximum Lyapunov Exponent (MLE). Further, the proposed system was implemented, in a digital scheme, on Xilinx Virtex[®] 4 XC4VSX35 FPGA, and experimental results are provided. The realization fits into a small area ($< 1.5\%$) and expresses a high throughput ($> 4.3\text{Gbit/s}$).

Acknowledgments

The authors would like to thank Dr. Amro Elshurafa, Hesham Omran, and Dr. Talal Bonny for their reviews and valuable suggestions.

References

- Barakat, M. L., Radwan, A. G. & Salama, K. N. [2011] "Hardware realization of chaos based block cipher for image encryption," *IEEE International Conference on Microelectronics (ICM'11)*.
- Chen, G. R. & Lu, J. H. [2003] "Dynamics of the Lorenz system family: Analysis, control and synchronization," *Beijing: Science Press* (in Chinese).
- Chen, S.-L., Hwang, T., Chang, S.-M. & Lin, W.-W. [2010] "A fast digital chaotic generator for secure communication," *International Journal of Bifurcation and Chaos* **20**, 3969–3987.
- Chiang, P. & Hu, C. [2010] "Chaotic pulse-position baseband modulation for an ultra-wideband transceiver in CMOS," *IEEE Transactions on Circuits and Systems II: Express Briefs* **57**, 642–646.
- Elwakil, A. S. & Kennedy, M. P. [2001] "Construction of classes of circuit-independent chaotic oscillators using passive-only nonlinear devices," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* **48**, 289–307.
- Elwakil, A. S. & Ozoguz, S. [2008] "A system and a circuit for generating multiple butterflies," *International Journal of Bifurcation and Chaos* **18**, 841–844.
- Elwakil, A. S., Ozoguz, S. & Kennedy, M. P. [2002a] "Creation of a complex butterfly attractor using a novel Lorenz-type system," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* **49**, 527–530.
- Elwakil, A. S., Salama, K. N. & Kennedy, M. P. [2002b] "An equation for generating chaos and its monolithic implementation," *International Journal of Bifurcation and Chaos* **12**, 2885–2895.
- Ergn, S. & Ozoguz, S. [2010] "Truly random number generators based on non-autonomous continuous-time chaos," *International Journal of Circuit Theory and Applications* **38**, 1–24.
- Galias, Z. & Maggio, G. [2001] "Quadrature chaos-shift keying: theory and performance analysis," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* **48**, 1510–1519.
- Guglielmi, V., Pinel, P., Fournier-Prunaret, D. & Taha, A.-K. [2009] "Chaos-based cryptosystem on DSP," *Chaos, Solitons & Fractals* **42**, 2135–2144.
- Kodba, S., Perc, M. & Marhl, M. [2005] "Detecting chaos from a time series," *European journal of physics* **26**, 205.
- Lorenz, E. [1963] "Deterministic nonperiodic flow," *Atmospheric Sciences* **20**, 130–141.
- Lu, J. & Chen, G. [2006] "Generating multiscroll chaotic attractors: theories, methods and applications," *International Journal of Bifurcation and Chaos* **16**, 775–858.
- Lu, J., Yu, S., Leung, H. & Chen, G. [2006] "Experimental verification of multidirectional multiscroll chaotic attractors," *IEEE Transactions on Circuits and Systems I: Regular Papers* **53**, 149–165.
- Mansingka, A. S., Radwan, A. G. & Salama, K. N. [2011a] "Design, implementation and analysis of fully digital 1-D controllable multiscroll chaos," *IEEE International Conference on Microelectronics (ICM'11)*.
- Mansingka, A. S., Radwan, A. G., Zidan, M. A. & Salama, K. N. [2011b] "Analysis of bus width and delay

- on a fully digital signum nonlinearity chaotic oscillator,” *IEEE International Midwest Symposium on Circuits and Systems (MWSCAS’11)*.
- Mazloom, S. & Eftekhari-Moghadam, A. M. [2009] “Color image encryption based on coupled nonlinear chaotic map,” *Chaos, Solitons & Fractals* **42**, 1745–1754.
- Pareschi, F., Scotti, G., Giancane, L., Rovatti, R., Setti, G. & Trifiletti, A. [2009] “Power analysis of a chaos-based random number generator for cryptographic security,” *IEEE International Symposium on Circuits and Systems (ISCAS’09)*, pp. 2858–2861.
- Pecora, L. M., Carroll, T. L., Johnson, G. A., Mar, D. J. & Heagy, J. F. [1997] “Fundamentals of synchronization in chaotic systems, concepts, and applications,” *Chaos* **7**, 520–543.
- Perc, M. [2010] “User friendly programs for nonlinear time series analysis,” URL <http://www.matjazperc.com/ejp/time.html>, [Retrieved 7 August, 2010].
- Radwan, A. G., Soliman, A. M. & El-Sedeek, A. [2004] “MOS realization of the modified Lorenz chaotic system,” *Chaos, Solitons & Fractals* **21**, 553–561.
- Radwan, A. G., Soliman, A. M. & Elwakil, A. S. [2007] “1-D digitally-controlled multi-scroll chaos generator,” *International Journal of Bifurcation and Chaos* **17**, 277–242.
- Salama, K. N., Ozoguz, S. & Elwakil, A. S. [2003] “Generation of n-scroll chaos using nonlinear transconductors,” *IEEE International Symposium on Circuits and Systems (ISCAS’03)*, pp. 176–179.
- Sidiropoulos, P., Nikolaidis, N. & Pitas, I. [2009] “Invertible chaotic fragile watermarking for robust image authentication,” *Chaos, Solitons & Fractals* **42**, 2667–2674.
- Tavas, V., Demirkol, A., Ozoguz, S., Zeki, A. & Toker, A. [2010] “An adc based random bit generator based on a double scroll chaotic circuit,” *Journal of Circuits, Systems, and Computers* **19**, 621–639.
- Taylor, G. & Cox, G. [2011] “Behind intel’s new random-number generator,” *IEEE Spectrum (September Issue)*, 28–29.
- Xia, Y., Tse, C. & Lau, F. [2004] “Performance of differential chaos-shift-keying digital communication systems over a multipath fading channel with delay spread,” *IEEE Transactions on Circuits and Systems II: Express Briefs* **51**, 680–684.
- Yalcin, M. [2007] “Increasing the entropy of a random number generator using n-scroll chaotic attractors,” *International Journal of Bifurcation and Chaos* **17**, 4471–4479.
- Yalcin, M., Suykens, J. & Vandewalle, J. [2004] “True random bit generation from a double-scroll attractor,” *IEEE Transactions on Circuits and Systems I: Regular Papers* **51**, 1395–1404.
- Yu, S., Tang, W., Lu, J. & Chen, G. [2008] “Multi-wing butterfly attractors from the modified lorenz systems,” *IEEE International Symposium on Circuits and Systems (ISCAS’08)*, pp. 768–771.
- Yu, S., Tang, W., Lu, J. & Chen, G. [2010] “Design and implementation of multi-wing butterfly chaotic attractors via lorenz-type systems,” *International Journal of Bifurcation and Chaos* **20**, 29–41.
- Zhang, C., Yu, S., Lu, J. & Chen, G. [2008] “Generating multi-wing butterfly attractors from the piecewise-linear chen system,” *International Conference for Young Computer Scientists (ICYCS’08)*, pp. 2840–2845.
- Zidan, M. A., Radwan, A. G. & Salama, K. N. [2011a] “The effect of numerical techniques on differential equation based chaotic generators,” *IEEE International Conference on Microelectronics (ICM’11)*.
- Zidan, M. A., Radwan, A. G. & Salama, K. N. [2011b] “Random number generation based on digital differential chaos,” *IEEE International Midwest Symposium on Circuits and Systems (MWSCAS’11)*.