[Egyptian Informatics Journal 22 (2021) 155–166](https://doi.org/10.1016/j.eij.2020.07.002)

Contents lists available at [ScienceDirect](http://www.sciencedirect.com/science/journal/11108665)

Egyptian Informatics Journal

journal homepage: [www.sciencedirect.com](http://www.sciencedirect.com/)

Full length article

[](http://crossmark.crossref.org/dialog/?doi=10.1016/j.eij.2020.07.002&domain=pdf)Trajectory control and image encryption using affine transformation of lorenz system

Wafaa S. Sayed [a](#_bookmark0),[⇑](#_bookmark3), Ahmed G. Radwan [a](#_bookmark0),[b](#_bookmark1), Hossam A.H. Fahmy [c](#_bookmark2), AbdelLatif Elsedeek [a](#_bookmark0)

a *Engineering Mathematics and Physics Department, Faculty of Engineering, Cairo University, Giza 12613, Egypt*

b *Nanoelectronics Integrated Systems Center, Nile University, Cairo 12588, Egypt*

c *Electronics and Communications Engineering Department, Faculty of Engineering, Cairo University, Giza 12613, Egypt*

a r t i c l e i n f o

*Article history:*

Received 30 September 2019

Revised 21 December 2019

Accepted 8 July 2020

Available online 29 July 2020

*Keywords:*

Affine transformations Chaos

Dynamic translation Image encryption Lorenz system Trajectory control

a b s t r a c t

This paper presents a generalization of chaotic systems using two-dimensional affine transformations with six introduced parameters to achieve scaling, reflection, rotation, translation and/or shearing. Hence, the location of the strange attractor in space can be controlled without changing its chaotic dynamics. In addition, the embedded parameters enhance the randomness and sensitivity of the system and control its response. This approach overpasses performing the transformations as post-processing stages by applying them on the resulting time series. Trajectory control through dynamic parameters is demonstrated. Simulation results validate the proposed analysis for both the simplest and Lorenz chao- tic systems. An image encryption scheme is implemented using transformed Lorenz system resulting in a more secure encryption scheme in comparison to Lorenz and other recent related works. The scheme exhibits good performance when assessed using the PRNG properties, encrypted image histogram and its uniformity through chi square test, pixel correlation, Mean Squared Error (MSE), entropy, Peak Signal-to-Noise Ratio (PSNR), the National Institute of Standards & Technology (NIST) test, key space, key sensitivity, resistance to differential, ciphertext-only, known plaintext, and chosen plaintext attacks, robustness against noise and computation time.

© 2021 THE AUTHORS. Published by Elsevier BV on behalf of Faculty of Computers and Artificial Intel-

ligence, Cairo University. This is an open access article under the CC BY-NC-ND license ([http://creative-](http://creativecommons.org/licenses/by-nc-nd/4.0/)

[commons.org/licenses/by-nc-nd/4.0/](http://creativecommons.org/licenses/by-nc-nd/4.0/)).

1. Introduction

Chaotic systems are highly sensitive to initial conditions, sys- tem parameters and implementation. The significant properties of chaotic systems are highly required in many applications such as: modeling [[1]](#_bookmark34), motion control [[2]](#_bookmark35) and cryptography [[3–5]](#_bookmark36). Sev- eral recent Pseudo-Random Number Generation (PRNG) and encryption applications utilized discrete chaotic maps [[3]](#_bookmark36) and con- tinuous chaotic systems [[6]](#_bookmark37). Various digital and analog implemen- tations of discrete and continuous chaotic systems have been presented [[7,8]](#_bookmark38).

To fulfill the needs of all these multidisciplinary fields, there is a continuous need to come up with controllable modified, gener- alized and novel chaotic systems. Several properties of a chaotic

\* Corresponding author.

*E-mail addresses:* [wafaasayed@eng1.cu.edu.eg](mailto:wafaasayed@eng1.cu.edu.eg) (W.S. Sayed), [agradwan@ieee.org](mailto:agradwan@ieee.org) (A.G. Radwan), [hfahmy@alumni.stanford.edu](mailto:hfahmy@alumni.stanford.edu) (H.A.H. Fahmy), [aeah7@yahoo.com](mailto:aeah7@yahoo.com) (A. Elsedeek).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

system, its time series, and hence, strange attractor can be con- trolled, e.g., the attractor’s size, location, shape and number of scrolls.

Several researches developed modified versions of the most famous Lorenz chaotic system [[9]](#_bookmark39) and their implementations [[7,8,10–13]](#_bookmark38). Other researches focused on constructing, analyzing and implementing novel jerk-based chaotic systems that involve

a differential equation of at least third order *x*v *f* €*x*; *x*\_ ; *x* and a

= ( )

nonlinearity [[14–20]](#_bookmark39).

Linear combination ideas were utilized in synchronization schemes [[21]](#_bookmark40) as a post-processing stage for the dynamical equa- tions. Geometric transformations have many applications in mechanical design [[22]](#_bookmark41), control [[23]](#_bookmark42), computer graphics [[24]](#_bookmark49), fractal structures generation [[25]](#_bookmark51) and fractal-based image coding [[26]](#_bookmark53).

Control of locations and number of equilibrium points was fur- ther used in multi-scroll attractors generation [[27–33]](#_bookmark56). Such works provided various combinations of the previously mentioned con- trollable properties of the strange attractors. Although these works barely presented applications for their proposed systems, separate

<https://doi.org/10.1016/j.eij.2020.07.002>

1110-8665/© 2021 THE AUTHORS. Published by Elsevier BV on behalf of Faculty of Computers and Artificial Intelligence, Cairo University. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

image encryption research was ongoing meanwhile [[34–37]](#_bookmark43) based on discrete-time chaotic maps including some transformations as separate encryption stages. This work links chaotic systems and affine transformations and proposes the utilization of extra param- eters and transformations as simple means of generalization and control of chaotic systems.

This paper uses embedded affine transformations to control chaotic systems and enhance their sensitivity. This method enables simultaneous control of the size of the strange attractor through scaling parameters, its location through rotation and/or transla- tion, its shape through shearing and the number of scrolls through dynamic parameters. Section [2](#_bookmark4) briefly reviews the basic mathe- matics of affine transformations. Sections [3 and 4](#_bookmark5) apply the trans- formation to the simplest and Lorenz chaotic systems demonstrating the effects on the time series, attractor diagrams and Maximum Lyapunov Exponent (MLE). Section [5](#_bookmark15) utilizes scaling and translation parameters to dynamically control the trajectory of the strange attractor. Section [6](#_bookmark16) highlights the main advantages of transformed Lorenz system in an image encryption application. Section [7](#_bookmark33) discusses the results in comparison to other recent related works. Section [8](#_bookmark31) summarizes the main contributions of the paper and suggests future work directions.

1. Affine transformations

Two-dimensional affine transformations can be applied to any pair of axes constructing a plane in the coordinate systems. They result in relatively simple equations and allow clear visualization in the different planes of the Cartesian coordinate system. Con- sider a point represented in the three-dimensional space with

the coordinates *x*, *y*, *z* , its two-dimensional affine transformation

( )

from the *x*-*y* to the *u*-*v* plane in the three-dimensional space can be written as:

equilibrium points with eigen values *k*1 = —0.8994 and *k*2,3 = 0.0497 *i* 0.9418. Saddle points of index two result in double-scroll attractors.

Using the inverse transformation [(2)](#_bookmark6), a transformed system in the *u*-*v*-*w* coordinate system is obtained, which is given by:

*u*\_ = *a* (—*du* + *av* + *cd* — *af* ) + *bw* + *c*,

*a*

*v*\_ = *d* (—*du* + *av* + *cd* — *af* ) + *ew* + *f* , (4)

*a*

*w*\_ = —0.8 *w* + 1 ((*e* — *d*)*u* + (*a* — *b*)*v*) — *sgn* 1 (*eu* — *bv*) .

*a*

*a*

The response of the system reduces to that of [(3)](#_bookmark8) at *a* = *e* = 1 and *b c d f* 0 as shown in [Fig. 1](#_bookmark9), where the response of the transformed (original) system is plotted in blue (red) color.

= = = =

The six added parameters provide controllability of the attrac- tor diagram, or its projection in the *u v* plane. In addition, the effect on each coordinate can be inferred from the time series.

—

[Table 1](#_bookmark9) provides the analyses of simplified versions: scaling (in- crease or decrease the values), reflection, translation with fixed distance, and shearing processes.

[Table 2](#_bookmark10) shows the time series and attactor diagrams of the transformed and original coordinates. The transformations given by [(1)](#_bookmark7) on the original time series, i.e., post-processing results are also plotted in black and the new equilibrium points are marked in pink color.

Stability analysis can also be performed for the systems of [Table 1](#_bookmark9). For example, in case of rotation, the Jacobian matrix is given by:

2 3

cos *h* sin *h* cos2 *h* sin *h*

64 75

*J* = — sin2 *h* — cos *h* sin *h* cos *h* .

1.6 cos *hd*(*u* cos *h* — *v* sin *h*) — 0.8(cos *h* + sin *h*) —0.8(cos *h* — sin *h*) —0.8

# (5)

2 *u* 3

2 *a b* 0 32 *x* 3

2 *c* 3

The characteristic polynomial is given by:

64 *v* 75 = 64 *d e* 0 7564 *y* 75 + 64 *f* 75, (1)

*w*

0 0 1

*z*

0

with the inverse transformation

2 *x* 3 1 2 *e* —*b* 0 32 *u* 3 1 2 *bf* — *ce* 3

6 7  6 76 7  6 7

*y* = 4 —*d a* 0 54 *v* 5 + 4 *cd* — *af* 5, (2)

4 5 *a a*

*z*

0 0 *a*

*w*

0

where *a* = *ae* — *bd* and the third coordinate *w* = *z*. The *u*-*v*-*w* coor-

*k*3 — *tr*(*J*)*k*2 + (*M* + *M* + *M* )*k* — |*J*|= 0, (6)

where *tr*(*J*) is the trace of the jacobian matrix, |*J*| is its determinant and *Mij* is the minor determinant of the matrix *J* by removing the *ith*

11

22

33

row and *jth* column. The coefficients of the characteristic polynomial are obtained as follows:

* *tr*(*J*)=— 5 and |*J*|= 5 *d*(*u* cos *h* — *v* sin *h*) — 5.

4

8

4

* *M*11 = 4 cos2 *h* + 4 sin 2*hd*(*u* cos *h* — *v* sin *h*),

5

5

5

5

dinates reduce to the *x*-*y*-*z* coordinates at *a* = *e* = 1 and

*M*22 = 4 sin2 *h* — 4 sin 2*hd*(*u* cos *h* — *v* sin *h*),

*b* = *c* = *d* = *f* = 0.

1. Validation case 1: generalized simplest system

A very simple jerk-based system with piecewise nonlinearity, which is generated by a signum function, was presented in [[14]](#_bookmark39). In its original form, the system is given by:

*x*\_ = *y*, *y*\_ = *z*,

*z*\_ = —0.8(*z* + *y* + *x* — *sgn*(*x*)),

8><

*M*33 = 0 and hence *M*11 + *M*22 + *M*33 = 4.

Consequently, *tr*(*J*) and *M*11 + *M*22 + *M*33 are always indepen- dent of *h*. At the equilibrium points |*J*|=— 4. Hence, the character- istic polynomial evaluated at the equilibrium points and the resulting eigen values are independent of *h* and identical to those of the original system.

5

5

The effect of the transformation on the eigen vectors of the Jaco- bian matrix can also be studied. The Eigen Vectors Inclination (EVI) is plotted against the rotation angle *h*. EVI is the angle between the vector at *h* = 0 and that at a given value of *h*, i.e., D*h* = *h*. In a real

—1, *x* < 0

where *sgn*(*x*)= 0, *x* = 0

(3)

inner product space, the angle */* between two vectors *x* and *y* is

defined by cos  <*x*,*y*> . In a complex vector space, taking the real

*/* =

||*x*|| ||*y*||

ffi{<*x*,*y*>}

# >: 1, *x* > 0

part of this cosine defines the Euclidean angle as cos */E* =

.

||*x*|| ||*y*||

Solving the system results in the chaotic attractor and time series shown in [Fig. 1](#_bookmark9). The equilibrium points of the system are ( 1, 0, 0) and the Jacobian matrix is independent of the

[Fig. 2](#_bookmark12) shows that EVI (*/E* ) follows a pattern similar to that of the rotated system itself where EVI is plotted at the equilibrium points. Further utilization of rotation in the generalization of integer and

fractional-order chaotic systems can be found in [[38,39,50]](#_bookmark57).

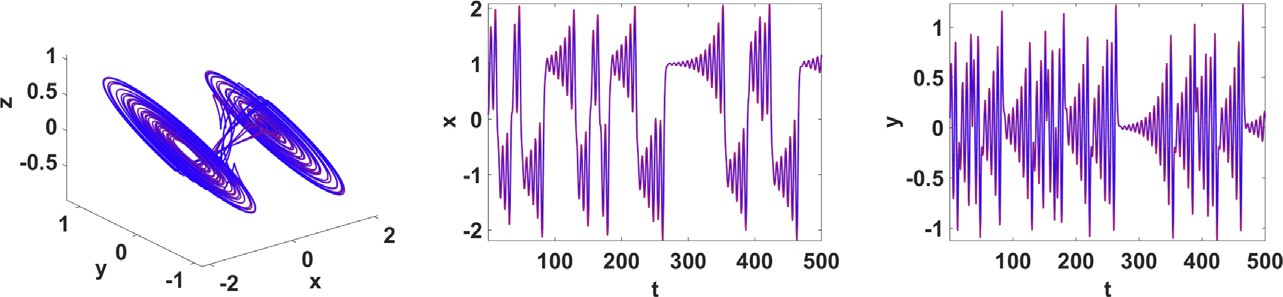


Fig. 1. Attractor diagram and time series of system [(3)](#_bookmark8).

Table 1

Example transformations of the simplest chaotic system.

Scaling (+ve), Reflection (-ve) Rotation

*u*\_ = *a v*,

*e*

*v*\_ = *ew*,

*w*\_ = —0.8 *w* + *u* + *v* — *sgn u*

*u*\_ = cos *h*(sin *h u* + cos *h v*) + sin *h w*,

*v*\_ =— sin *h*(sin *h u* + cos *h v*) + cos *h w*,

*w*\_ = —0.8(*w* + (cos *h* + sin *h*)*u* + (cos *h*— sin *h*)*v* — *sgn*(cos *h u* — sin *h v*))

*a*

*e*

*a*

Equilibria: ( *a*, 0, 0) Equilibria: ( cos *h*, n sin *h*, 0)

Scaling and translation Shearing

*u*\_ = *a* (*v* — *f* ) + *c*,

*e*

*v*\_ = *ew* + *f* ,

*u*\_ 1

—*bd*

= 1

*v*\_ = 1 *d*

(—*du* + *v*) + *bw*,

(—*du* + *v*) + *w*,

*u v*  *u*

—*bd*

*w*\_ = —0.8 *w* + *a* + *e* — *sgn a*

—*bd*

1—*bd*

Equilibria: ( 1, *d*, 0)

Equilibria: *a c* 1 , — *ce* + *f* , — *f*

*a*

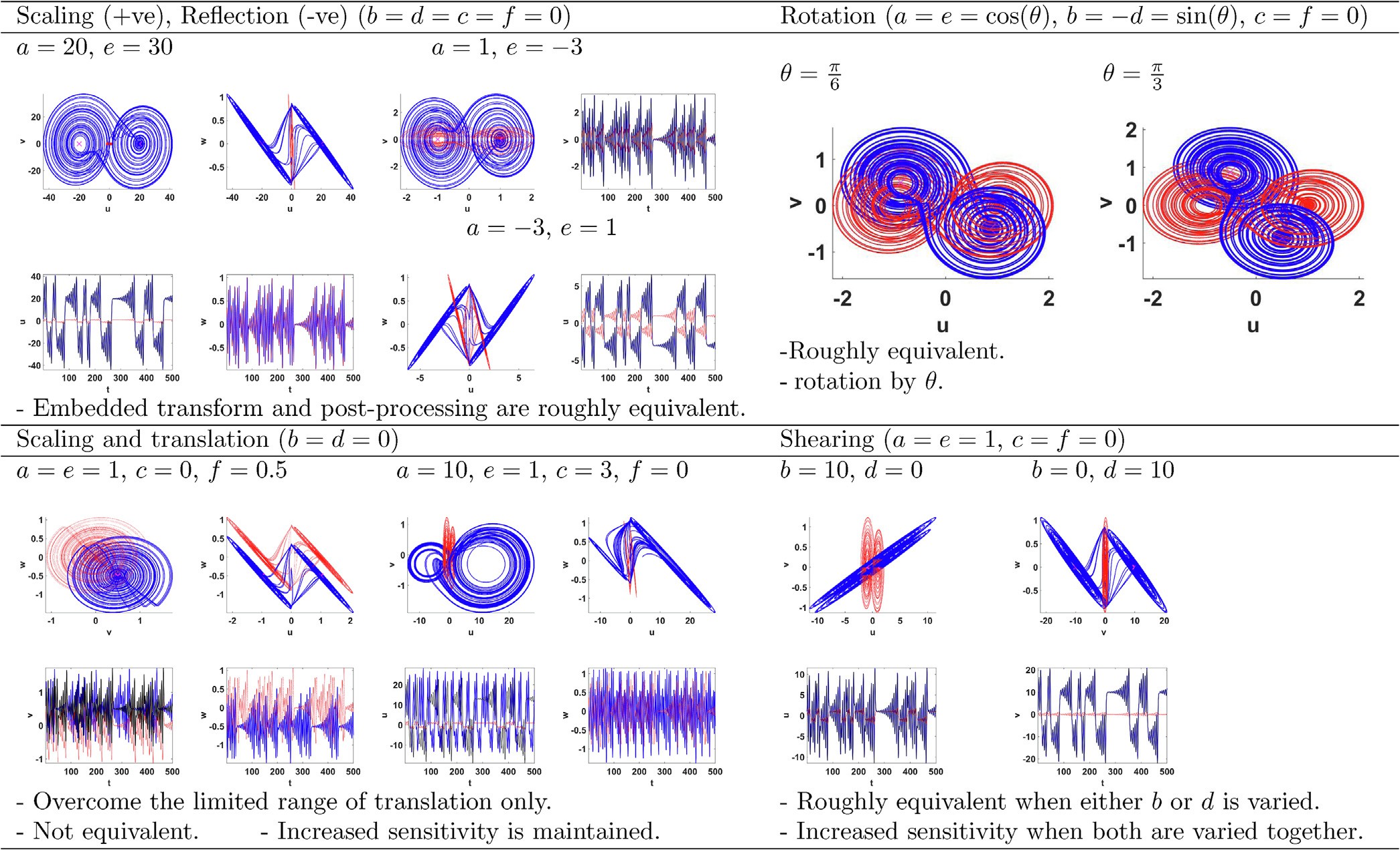
*a*

*e*

*w*\_ = —0.8(*w* + 1 1

((1 — *d*)*u* + (1 — *b*)*v*)—*sgn u*—*bv* )

Table 2

Transformations of the simplest chaotic system: results and discussion.

1. Validation case 2: generalized lorenz system

Lorenz system is given by:

10 *a*

=— *a*

*u*\_

## *b*

((*u* — *c*)(*d* + *e*)— (*v* — *f* )(*a* + *b*))

*x*\_ = 10(*y* — *x*),

*y*\_ = (28 — *z*)*x* — *y*,

*z*\_ = *xy* — 8 *z*. (7)

+ *a* ((*u* — *c*)(*d* + (28 — *w*)*e*)— (*v* — *f* )(*a* + (28 — *w*)*b*)) + *c*, (8)

[Table 3](#_bookmark13) shows the scaling (reflection), translation and shearing transformations of Lorenz system. Chaotic time series is identified

3

Transformed Lorenz system can be obtained similarly, where for example:

using Lyapunov exponents, which quantify the divergence and convergence properties of an attractor [[1]](#_bookmark34). Using Wolf’s algorithm

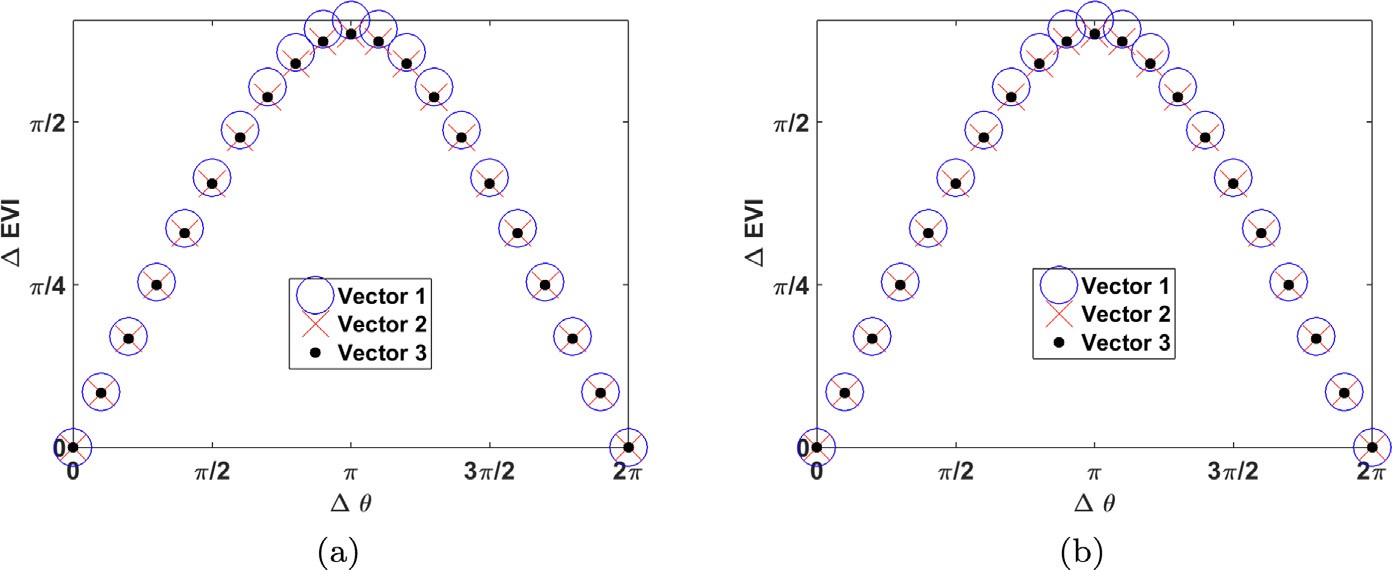


Fig. 2. Eigen Vectors Inclination (EVI) against the rotation angle *h* at the (a) first and (b) second equilibrium point.

Table 3

Attractor diagrams and time series of [(8)](#_bookmark11).

*u*\_ =— 10 (*e*(*u* — *c*)— *a*(*v* — *f* )) + *c*,

*v*\_ = 1 ((*u* — *c*)((28 — *w*)*e*)— *a*(*v* — *f* )) + *f* ,

*e*

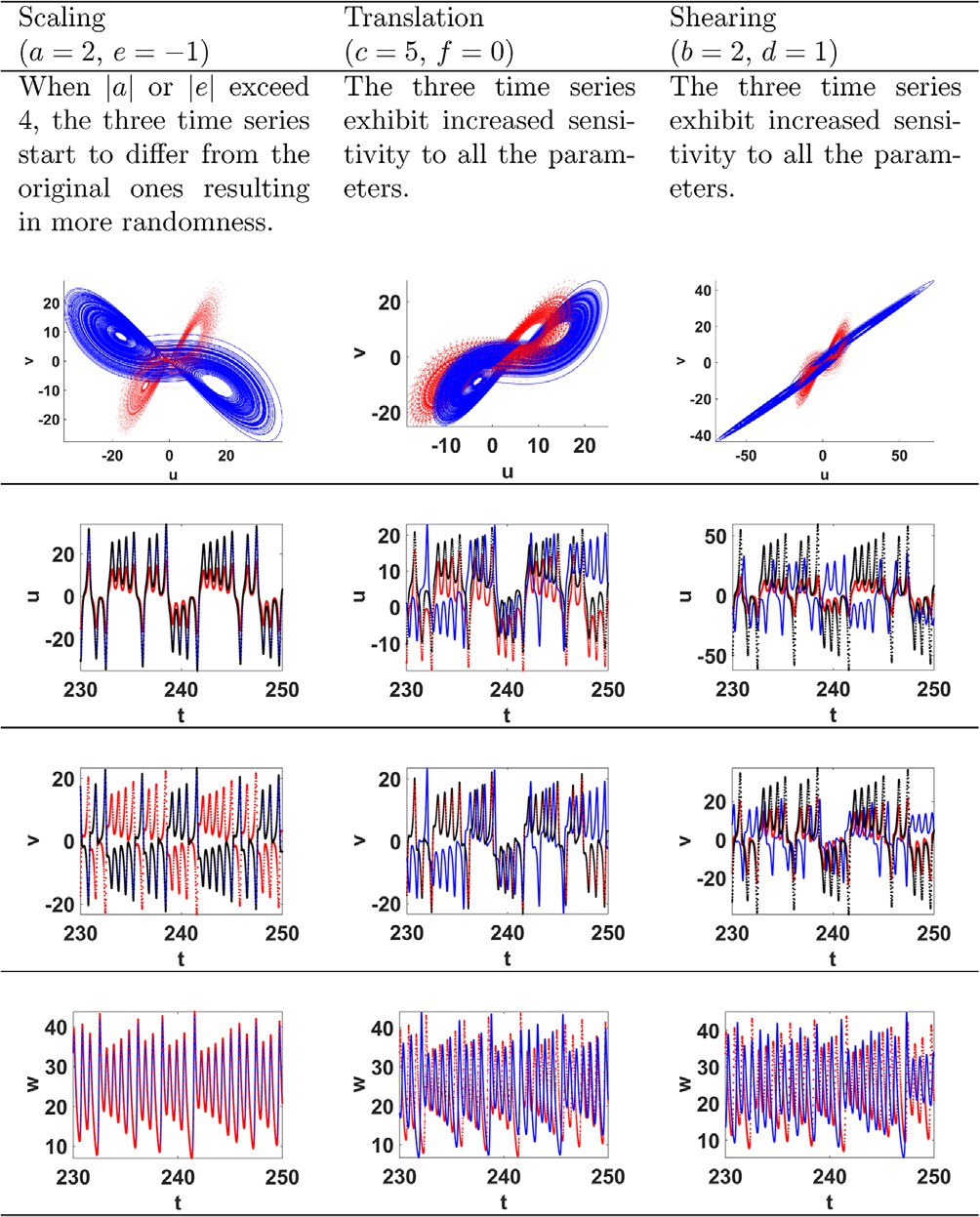
*a*

*w*\_ =— 1 (*u* — *c*)(*v* — *f* )— 8 *w*.

*ae*

3

# (9)

[Fig. 4](#_bookmark18) shows different trajectories that the system follows dynamically in discrete steps. To be capable of visualizing the dynamic translation of the attractor, scaling parameters are used to control the output range. For Lorenz system, the output ranges are wide, hence, the scaling parameters *a* and *e* are set to values less than one. However, the translation parameters *c* and *f* have limited ranges that correspond to chaotic behavior as shown in the bifurcation diagrams of [Fig. 5](#_bookmark19). Hence, it is more suitable to have a closed trajectory rather than open ones.

[Table 4](#_bookmark20) shows a continuous motion of the attractor along differ- ent trajectories, where [[41]](#_bookmark44) provides more examples of plane curves. This is achieved by keeping *c* constant for a period of time, such that it is sufficient to plot a clear part of the diagram. Then, the value of *c* is changed a little bit and so on in gradual steps that take the shape of staircase. The parameter *c* can be generated using the equation:

as implemented in [[40]](#_bookmark43), the system is shown to exhibit chaotic strange attractors since the Maximum Lyapunov Exponent (MLE) is finite positive against the parameters corresponding to the dif- ferent cases as shown in [Fig. 3](#_bookmark17).

1. Trajectory control by dynamic translation

The translation parameters *c* and *f* can be used to move the equilibrium points and, hence, the attractor diagram. The transla- tion along *x*-axis, *c*, can be changed in a piece-wise manner giving sufficient time for each value. In addition, the translation along *y*- axis, *f*, is given as a function of *c*, which is the trajectory. The scaling parameters are kept to control the output range and simplify the visualization of results. Scaled and translated system can be obtained by setting *b d* 0 in the equations of transformed Lor- enz, e.g. [(8)](#_bookmark11) yielding:

= =

*n*

*c*(*t*)= *A*(*i*)(*H*(*t* — *B*(*i*)) — *H*(*t* — *B*(*i* + 1))), (10)

X

*i*=1

where *H* . is the unit step or Heaviside function, *A* and *B* are vectors that correspond to the gradual amplitudes and stop times of the stairs, respectively, of the resulting stair case plot. The first and last elements of the vector *c* equal those of *A*, respectively. The other translation parameter *f* is changed accordingly using the prescribed trajectory equation. In the examples of [Table 4](#_bookmark20), the amplitudes of *c*

( )

are in the interval 2, 2 and the step by which they vary equals 50

[— ]

time units in a total simulation time of 500 time units. The resulting time series of [(9)](#_bookmark14) are compared to the scaled time series of the con- ventional Lorenz system. The resulting attractor diagrams follow the prescribed trajectories, which are red colored. The intensity of the strange attractor color varies with time, where the darker points are plotted first and becomes brighter as time advances.

1. PRNG and image encryption application

This section studies the performance of transformed Lorenz sys- tem, compared to Lorenz system, as a PRNG in an image encryption application. Three standard 1024 1024 color images: Lena, man- dril and peppers [[42]](#_bookmark45) are used for testing the encryption scheme. While Lena image is firstly used in comparing the Lorenz and transformed Lorenz systems performance in the scheme with detailed results, performance metrics are averaged for the three color channels of the two other images.

×

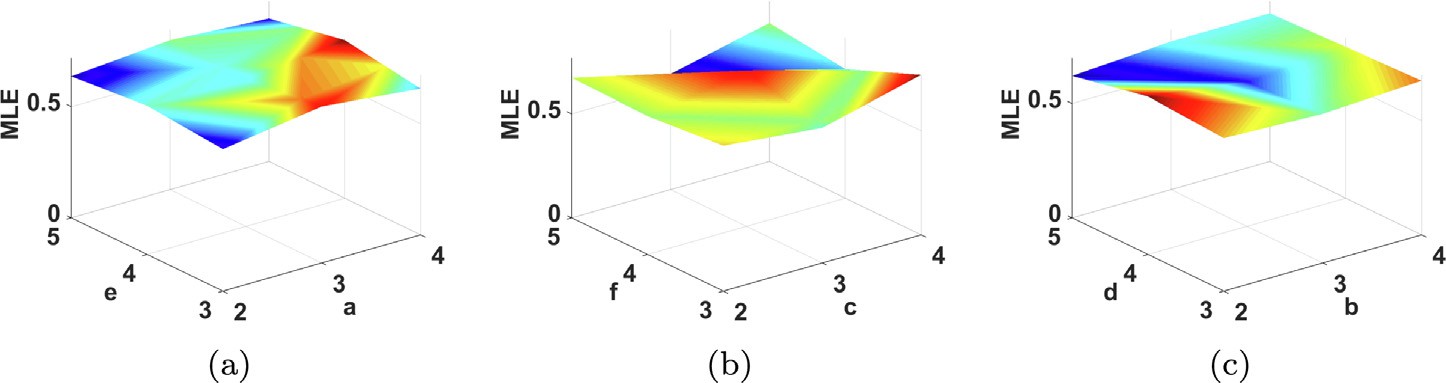


Fig. 3. MLE of transformed Lorenz against the parameters in (a) Scaling, (b) Translation and (c) Shearing cases.

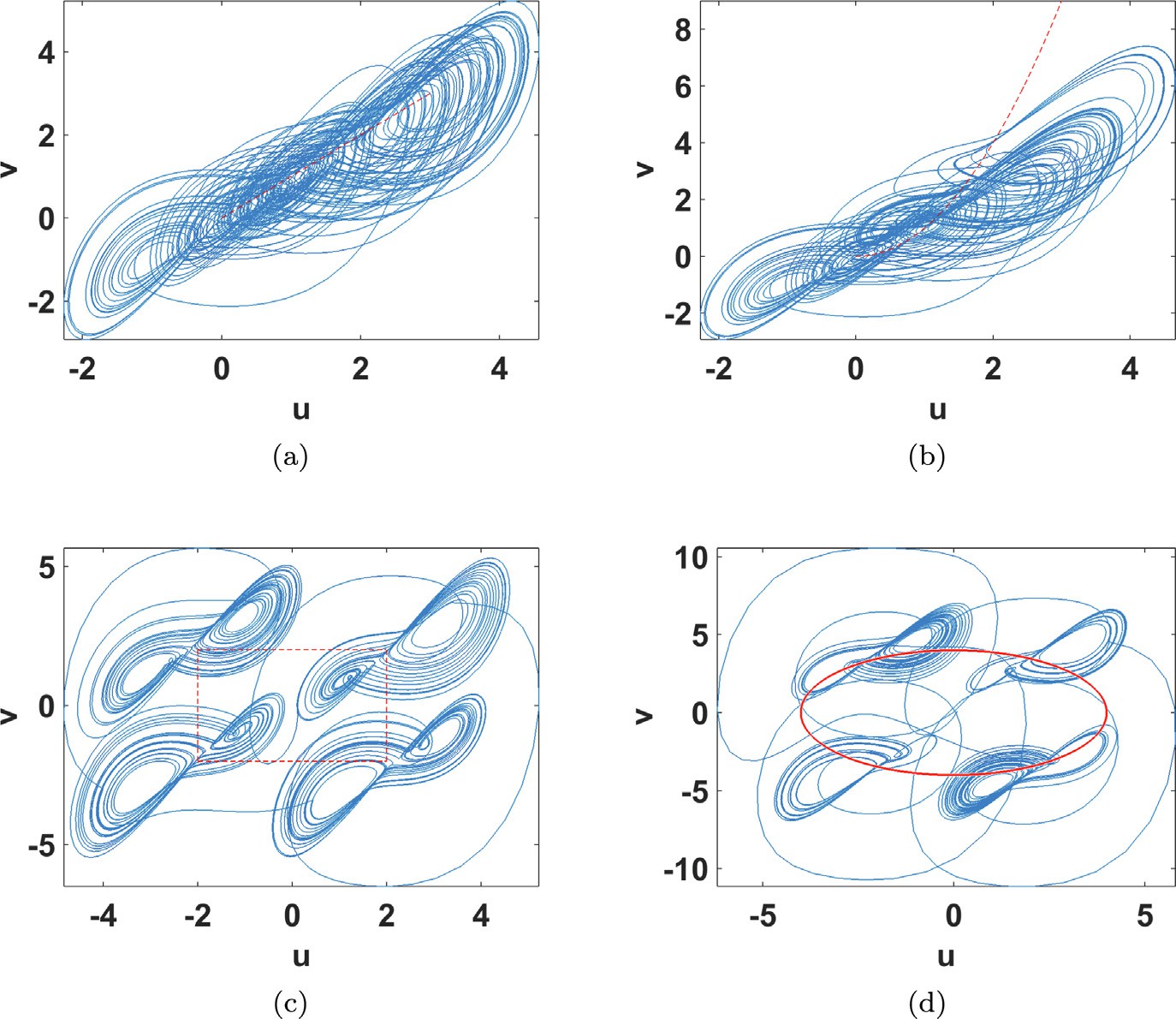


Fig. 4. Trajectory control of transformed Lorenz chaotic system by scaling and translation for (a) line *f* = *c*, (b) parabola *f* = *c*2, (c) a square and (d) a circle of radius 4 (*c*2 + *f* 2 = 16) at *a* = *e* = 1.

8

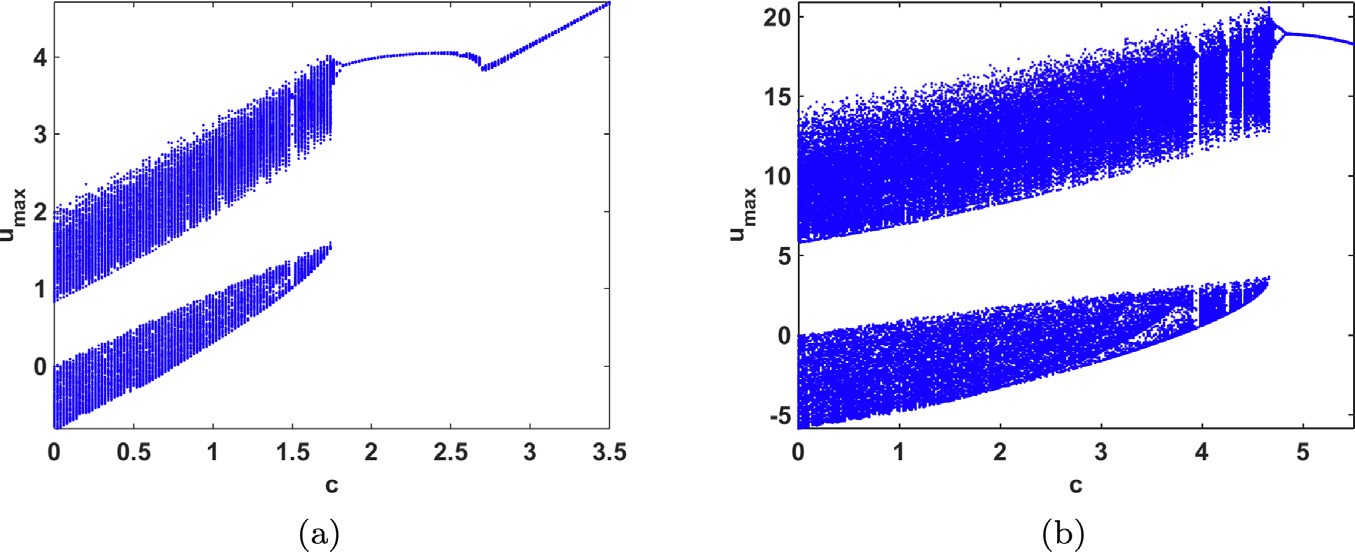
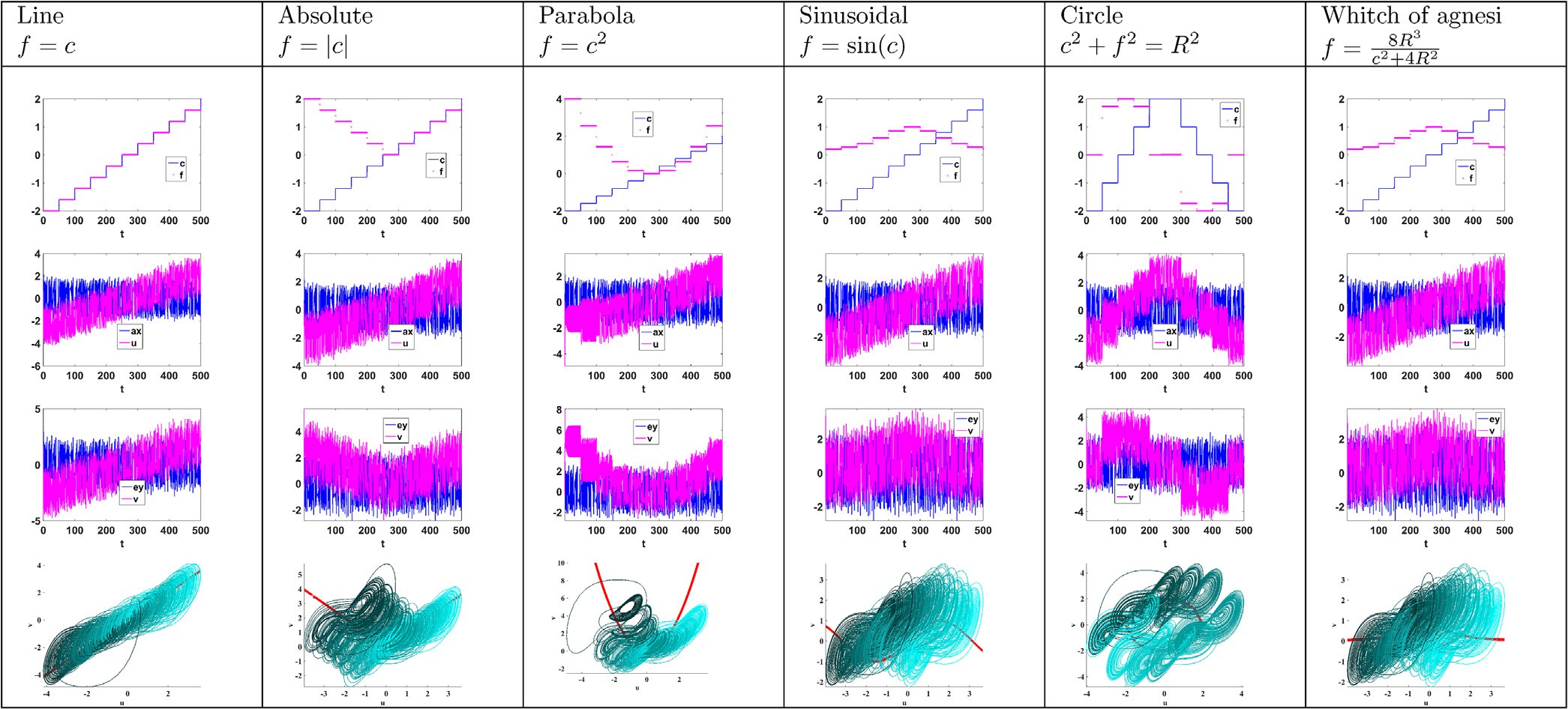


Fig. 5. Bifurcation diagrams of transformed Lorenz chaotic system against the translation parameter *c* for the parabolic trajectory *f* = *c*2 and different values of the scaling parameters (a) *a* = *e* = 0.1 and (b) *a* = *e* = 0.7.

Table 4

Trajectory control of [(9)](#_bookmark14) for *a* = *e* = 0.1 and different dynamic *c* and *f* parameters.

* 1. *Encryption and decryption schemes*

[Fig. 6](#_bookmark21) shows a simple image encryption scheme with both per- mutation and substitution phases, which was presented in [[3]](#_bookmark36). Per- mutation of the original image is performed through generalized Arnold’s map [[43]](#_bookmark46), where the new pixel location is given by:

where *mod* returns the remainder, *ckey* and *bkey* are the key parts of the permutation parameters and chosen as 73 and 35, respectively and the value *Psum Rsum Gsum Bsum*, except where stated other-

wise, represents the input dependent term, which enhances the resistance to different cryptanalysis attacks, where *Rsum*, *Gsum* and *Bsum* are the sums of the red, green and blue channels of the input

= + +

# row

col new =

1 *c*

*b* 1 + *cb*

row

col old

*mod*(*N*)+

1

1

# (11)

image, respectively [[3]](#_bookmark36).

In the substitution phase, the chaotic generator is either Lorenz or transformed Lorenz with the chaotic time series shown in [Fig. 7](#_bookmark22).

for an *N* × *N* image. The generalized Arnold’s map permutation parameters *c* and *b* are computed as:

The correlation coefficients between the *u*, *v* and *w* and the corre- sponding *x*, *y* and *z* time series are —0.0054, —0.0051 and 0.0038.

*c* = *mod* *P*

*sum* +

*ckey* , *N*

# — 1 + 1

# (12)

The systems are solved by Euler numerical technique using a time step of 0.01. The outputs *x* (*u*), *y* (*v*) and *z* (*w*) are then multiplied

*b* = *mod* *P*

*sum*

+ *bkey*

, *N* — 1 + 1

by a scaling factor of 109 to be suitable for conversion to an integer





Fig. 6. (a) Encryption/decryption block diagrams, encryption/decryption key for (b) Lorenz and (c) transformed Lorenz chaotic generators and (d) multiplexing table.



|  |  |  |
| --- | --- | --- |
|  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |

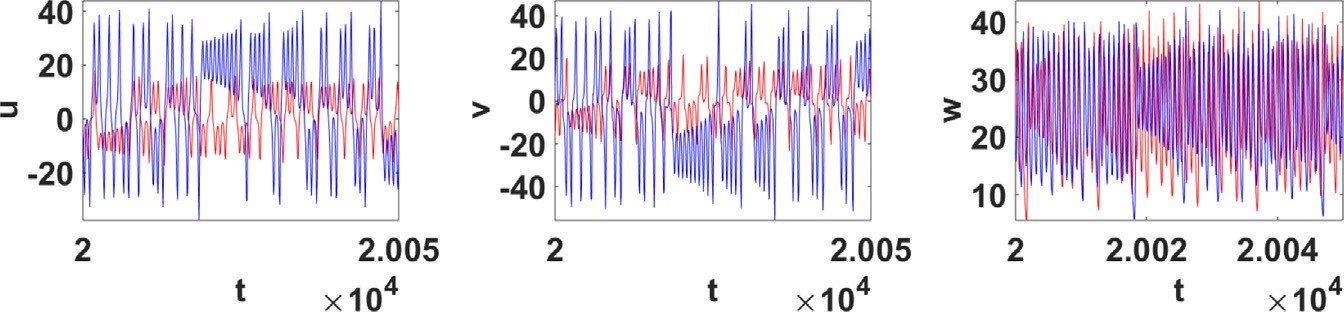


Fig. 7. Time series of Lorenz, in red, and transformed Lorenz, in blue, at *a* = 2, *b* = 0.25, *c* = 3, *d* = —0.5, *e* = —2, *f* = —4, *x*0 = *y*0 = *z*0 = *w*0 = 0.1 *u*0 = 3.225 and *v*0 = —0.425.

value represented in 64 bits. Each component of the permuted image is xored with the 8 Least Significant Bits (LSBs) of the out- puts of the chaotic generator, respectively, xored together with a feedback element from a channel of the previously encrypted image selected by the LSBs of its channels [[3]](#_bookmark36) according to the mul- tiplexing procedure given in [Fig. 6](#_bookmark21)(d). The encryption key determi- nes the parameters of the chaotic generator where it consists of three sub-keys for Lorenz system compared to nine sub-keys using transformed Lorenz system.

Decryption is straightforward as the reverse process shown in [Fig. 6](#_bookmark21)(a). First, an exact duplicate of the same substitution stage is carried out on the encrypted image. Then, the resulting image is permuted by generalized Arnold’s map to return the pixels to their original locations and get the correctly decrypted image.

* 1. *Performance evaluation*

The performance of the scheme is evaluated through the PRNG properties, encrypted image histogram and its uniformity through chi square test, pixel correlation, Mean Squared Error (MSE), entropy, Peak Signal-to-Noise Ratio (PSNR), the National Institute of Standards & Technology (NIST) test, key space, key sensitivity, resistance to differential, ciphertext-only, known plaintext, and chosen plaintext attacks, robustness against noise and computa- tion time comparing Lorenz to transformed Lorenz systems as the chaotic generator. Equations of the performance metrics are given in [Table 5](#_bookmark23).

* + 1. *PRNG properties*

[Fig. 8](#_bookmark24) compares the randomness properties of the chaotic sequence generated from Lorenz and transformed Lorenz systems. For a good chaotic sequence, the histogram should be nearly flat or uniform and the adjacent samples should be completely uncorre- lated. From [Fig. 8](#_bookmark24), it can be inferred that both systems satisfy the requirements, where the nearly aperiodic chaotic sequence has nearly flat frequency distribution. Hence, the transformed Lorenz system provides more control of the Lorenz attractor and is still random and suitable for encryption applications.

More advanced statistical tests are provided by NIST statistical test suite [[44]](#_bookmark47), which is a statistical test suite for random and pseudo-random number generators for cryptographic applications. The tests are designed to examine the randomness characteristics of a sequence of bits by evaluating the P-value distribution (PV) and the proportion of passing sequences (PP). The test is carried out on the 8 LSBs of each chaotic output in the same manner in which they are used in the substitution of the 8-bit pixels. [Table 6](#_bookmark25) shows that the PRNGs based on both Lorenz and transformed Lor- enz successfully pass the tests, which are: frequency, block fre- quency, cumulative sums, runs, longest run, rank, FFT, non- overlapping template, overlapping template, universal, approxi- mate entropy, random excursions, random excursions variant, serial and linear complexity, respectively.

* + 1. *Perceptual and statistical tests*

The encrypted images corresponding to the two chaotic gener- ators are random as shown in [Fig. 6](#_bookmark21) as well as [Fig. 9](#_bookmark26). In addition, the corresponding histograms reveal a uniform intensity distribu- tion compared to the nonuniform histograms of the original image as shown in [Fig. 10](#_bookmark27). To further check the degree of deviation from uniform histogram analysis, chi-square test [[45]](#_bookmark48) is used. The less the chi-square value, the better the uniformity. [Table 7](#_bookmark28) gives the results for the encrypted image using both Lorenz and transformed Lorenz, where both have relatively low values compared to that of

the original image of O 106 .

( )

[Table 7](#_bookmark28) shows the ability of the system to destroy the horizon- tal, vertical and diagonal correlation between the pixels where the correlation coefficients of the encrypted image approach zero. High MSE, entropy approaching 8 and low PSNR further indicate the ran- domness and unpredictability of the encrypted image.

[Table 6](#_bookmark25) also examines the randomness of the encrypted images by evaluating the PV and PP of NIST and they successfully pass the tests.

* + 1. *Key space and key sensitivity*

Key space is defined as the number of encryption keys that are available in the cryptosystem. The maximum key space is deter-

Table 5

Performance metrics of image encryption systems.

*v*2 = P*k* (*oi* —*ei* ) , *k* = 256 is the number of levels in a color, *o* and *e* are the observed and expected occurrence frequencies of each color level (0–255), respectively.

For 1024 × 1024 image, *ei* = 1024 × 1024/256 = 4096.

2

test

*i*=1

*ei*

*i*

*i*

Correlation coefficient (*q*) = ,ﬃﬃﬃﬃ*c*ﬃ*o*ﬃﬃ*v*ﬃﬃﬃ(,*x*,*y*ﬃﬃ)ﬃﬃﬃﬃﬃﬃﬃﬃ, where *cov*(*x*, *y*)= 1 P*S*

(*D*(*x*))

(*D*(*y*))

*S*

*i*=1

*x* — 1 P*S*

*i*

*S*

*j*=1 *j*

*x* *y* — 1 P*S*

*i*

*S*

*j*=1 *j*

*y* , *D*(*x*)= 1 P*S*

*S*

*i*=1

*x* — 1 P*S*

*i*

*S*

*j*=1 *j*

*x* 2 , *S* = *M*(height)× *N*(width).

Mean Squared Error (MSE)= 1 P*N* P*M* (*P*(*i*, *j*)— *D*(*i*, *j*))2 , where *P*(*i*, *j*), *D*(*i*, *j*) are the original & wrong decrypted image pixels

*M*×*N*

*i*=1

*j*=1

Entropy= —P28 *p*(*s* )log *p*(*s* ), where *p*(*s* ) is the probability of symbol *s*

*i*=1

*i*

2

*i*

*i*

*Imax*

*i*

Peak Signal-to-Noise Ratio (PSNR)= 20log10 ,MSE , where *Imax* is the maximum pixel value in the image. NumberofPixelChangeRate(NPCR)= 1 P*N* P*M D*(*i*, *j*) × 100,

ﬃﬃﬃﬃﬃﬃﬃ

*N*×*M*

*i*=1

*j*=1

UnifiedAverageChangingIntensity(UACI)= 1 P*N* P*M* *C*1 (*i*,*j*)—*C*2 (*i*,*j*) × 100,

*M*×*N*

*i*=1

*j*=1

255

where *D*(*i*, *j*)= 1, *C*1 (*i*, *j*) – *C*2 (*i*, *j*) , *C*1 is the ciphered pixel and *C*2 is the ciphered pixel corresponding to a slightly modified original image.

0, *C*1(*i*, *j*)= *C*2(*i*, *j*)

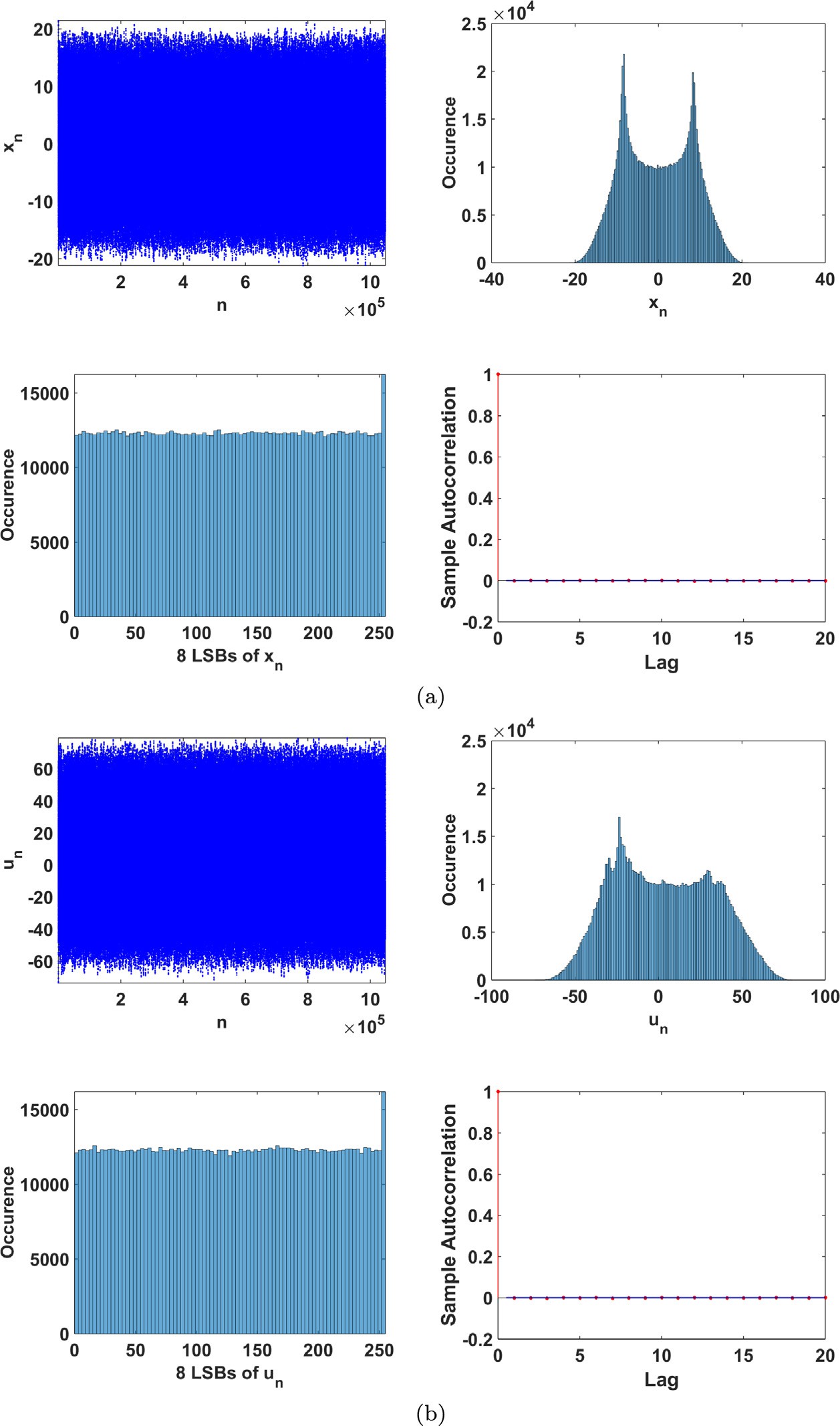


Fig. 8. Time series, frequency distribution of the outputs and histogram of the PRNG using (a) Lorenz and (b) transformed Lorenz chaotic generators.

mined by sensitivity analysis. Sensitivity of Lorenz system for per- turbations in the initial conditions is as follows D*x*0, D*y*0 P 10—17 and D*z*0 P 10—16. Sensitivity of transformed Lorenz system for per- turbations in the initial conditions and parameters is as follows D*x*0, D*y*0 P 10—15, D*z*0 P 10—17, D*a* P 10—15, D*b* P 10—16, D*c* P 10—15, D*d* P 10—16 and D*e*, D*f* P 10—15.

The initial conditions and parameters of the chaotic generator

consist of a fixed part and a key part, which is determined from the sub-keys denoted by *L* for Lorenz system and *T* for transformed Lorenz system as shown in [Figs. 6](#_bookmark21)(b) and (c). For example, *x*0 = *xfix* + D*x*0, where D*x*0 equals *L*1 multiplied by a scaling factor and similarly for the rest of the parameters. The fixed parts are

set to the values of [Fig. 7](#_bookmark22). To ensure high key sensitivity, a mini- mum perturbation of 10—14 is specified. Hence, each sub-key is lim- ited to 44 bits using a scaling factor of 10—13. Consequently, the key space of transformed Lorenz system equals 2396 compared to 2132 of Lorenz system, which is equivalent to 3 times increase in the number of bits.

[Table 7](#_bookmark28) gives the values of high MSE and entropy approaching 8,

which indicate the randomness and unpredictability of the wrong decrypted image when the Least Significant Bit (LSB) of the sub- key D*x*0 (or D*u*0) is changed. Similar results are obtained for the rest of the sub-keys. An advantage of the encryption system is that per- turbation in any parameter affects the three time series and, hence,

Table 6

NIST results for the PRNG and encrypted images.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | PV | PP |  | PV | PP |  | PV | PP |  | PV | PP |  | PV | PP |  | PV | PP |  |
|  | U | 1 |  | U | 1 |  | U | 0.979 |  | U | 1 |  | U | 0.979 |  | U | 1 |  |
|  | U | 0.917 |  | U | 1 |  | U | 1 |  | U | 1 |  | U | 1 |  | U | 0.958 |  |
|  | U | 1 |  | U | 0.979 |  | U | 1 |  | U | 1 |  | U | 0.979 |  | U | 0.979 |  |
|  | U | 1 |  | U | 1 |  | U | 0.958 |  | U | 1 |  | U | 1 |  | U | 1 |  |
|  | U | 0.958 |  | U | 0.958 |  | U | 1 |  | U | 1 |  | U | 1 |  | U | 1 |  |
|  | U | 0.958 |  | U | 0.958 |  | U | 1 |  | U | 1 |  | U | 1 |  | U | 1 |  |
|  | U | 1 |  | U | 1 |  | U | 1 |  | U | 1 |  | U | 1 |  | U | 1 |  |
|  | U | 0.990 |  | U | 0.992 |  | U | 0.989 |  | U | 0.989 |  | U | 0.986 |  | U | 0.989 |  |
|  | U | 1 |  | U | 1 |  | U | 1 |  | U | 1 |  | U | 1 |  | U | 0.917 |  |
|  | U | 1 |  | U | 1 |  | U | 1 |  | U | 0.958 |  | U | 0.917 |  | U | 1 |  |
|  | U | 1 |  | U | 1 |  | U | 1 |  | U | 1 |  | U | 0.958 |  | U | 1 |  |
|  | U | 1 |  | U | 1 |  | U | 1 |  | U | 1 |  | U | 0.993 |  | U | 0.979 |  |
|  | U | 0.996 |  | U | 0.992 |  | U | 1 |  | U | 0.980 |  | U | 0.977 |  | U | 1 |  |
|  | U | 1 |  | U | 1 |  | U | 1 |  | U | 1 |  | U | 1 |  | U | 0.917 |  |
|  | U | 1 |  | U | 0.958 |  | U | 1 |  | U | 1 |  | U | 1 |  | U | 1 |  |
|  |  | Passed |  |  | Passed |  |  | Passed |  |  | Passed |  |  | Passed |  |  | Passed |  |

PRNG Encrypted Lena Enc. mandril Enc. peppers Lorenz Transformed Lorenz Transformed Transform. Transform.



Fig. 9. Original and encrypted (a) mandril and (b) peppers images.

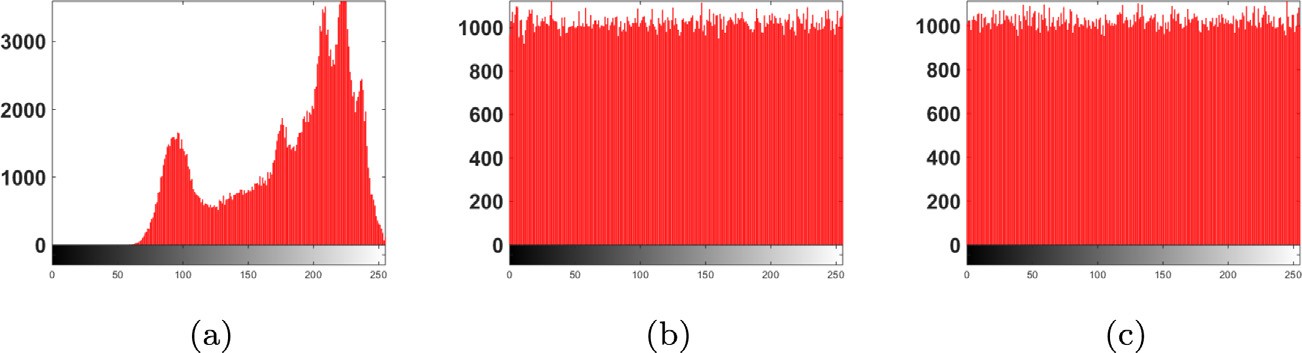


Fig. 10. Histograms of the red channel of (a) Lena image and the corresponding encrypted images using (b) Lorenz and (c) transformed Lorenz systems.

Table 7

Performance metrics of the scheme for three encrypted images.

Test Lena (Lorenz) Lena (Transformed) Mandril Peppers R G B R G B

2

*v*

test

×102 2.4808 2.505 2.6253 3.2239 2.5216 2.8009 2.6778 2.4336

CC Horizontal —0.0626 —0.0634 0.0227 —6.7144 —20.8894 —19.0264 8.0344 —1.0496

×10—4 Vertical 13.7072 —5.8588 0.8549 —8.8684 2.7001 —3.9709 3.2939 —1.1189

Diagonal —15.6653 —1.6203 —8.1332 —4.7629 —9.1812 —3.6888 0.3586 0.0903

MSE

×103 10.6217 9.0629 7.0821 10.6636 9.0617 7.0824 8.7107 8.7984

Entropy 7.9998 7.9998 7.9998 7.9998 7.9998 7.9998 7.9998 7.9998

PSNR 7.8689 8.5581 9.6292 7.8517 8.5587 9.6291 8.7537 5.7898

Key Sens. MSE ×103 10.6606 9.0569 7.1293 10.6599 9.0727 7.1136 8.7019 8.0343

(D*x*0, D*u*0) Entropy 7.9994 7.9993 7.9993 7.9993 7.9993 7.9992 7.9991

7.9992

DA NPCR 99.6061 99.6091 99.6104 99.6094 99.6126 99.6121 99.6101 99.6096

UACI 33.4859 33.4993 33.4859 33.4726 33.4834 33.4571 33.4582 33.4593

the three channels unlike encryption systems based on indepen- dent discrete maps for each channel [[3]](#_bookmark36).

* + 1. *Resistance to differential attacks*

[Table 7](#_bookmark28) shows the values of the NPCR and UACI averaged over 20 trials in which one pixel in the original image is changed, which successfully approach 100% and 33.3%, respectively [[3]](#_bookmark36).

* + 1. *Resistance to other cryptanalysis attacks*

Cryptanalysis is the process of studying encryption systems with the intention of revealing their weaknesses and establishing the appropriate attacking schemes [[46]](#_bookmark50). Other famous cryptanaly- sis techniques, besides brute force and differential attacks, are the ciphertext-only, known plaintext, chosen plaintext and side chan- nel attacks. However, they are less frequently investigated when proposing a new encryption scheme, especially for chaos-based ciphers.

In ciphertext-only attack, the attacker has access only to a ciphertext or a collection of ciphertexts with the objective of find- ing the plaintext image and/or the secret key. This requires the use of brute force [[47]](#_bookmark52), and hence, the large key space and the encryp- tion key design such that it depends on the plaintext image are effective means of enhancing the scheme’s resistance to this attack.

Table 8

Chosen plaintext attack/known plaintext attack analysis.

In known plain text attack, the attacker has a ciphertext or a set of ciphertexts for which the corresponding plaintext is also known with the objective of finding the secret key. Chosen plaintext attack gives more flexibility to an attacker by allowing plaintext to be selected observing the corresponding ciphertext. To depict the capability of the proposed scheme in eliminating all traces of cho- sen patterns in a plainimage, a 4 4 3 image was encrypted sim- ilar to [[37]](#_bookmark43). The resulting pixel values after before and after encryption are shown in [Table 8](#_bookmark29), where any specific patterns, white or black images are fully randomized after encryption with no observable patterns. This is owed to the presence of both per- mutation and substitution stages, key sensitivity and plainimage sensitivity properties of the scheme.

* + 1. *Robustness against noise*

× ×

The encrypted images may suffer from noise effects during transmission from transmitter to receiver such as: Additive White Gaussian Noise (AWGN) and Salt and Pepper (S & P) noise [[48]](#_bookmark54). To enhance the robustness of the scheme against noise, some input dependent terms in the encryption scheme can be modified. For example, [Figs. 11](#_bookmark30)(a) and (b) show the decrypted images corre- sponding to Lena for AWGN of mean 0 and different variances and S & P of different densities, respectively, when *Psum* = 0 and

1 2 3 4 1 1 1 1 255 255 255 255

4 × 4 × 3 1 2 3 4 1 1 1 1 255 255 255 255

plainimage 1 2 3 4 1 1 1 1 255 255 255 255

1 2 3 4 1 1 1 1 255 255 255 255

2 233 184 203 147 137 125 187 73 33 53 97

4 × 4 × 3 141 163 166 245 94 238 193 217 169 119 28 163

cipherimage 34 223 68 190 21 69 189 150 222 106 220 184

239 42 192 231 32 135 236 205 177 36 101 55





Fig. 11. Decrypted images and correlation coefficients corresponding to Lena for (a) AWGN of mean 0 and different variances and (b) S & P of different densities when *Psum* = 0 and MUX is removed.

Table 9

Comparison of the ideas and evaluation of different image encryption schemes.

test

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Ref. | Main Blocks | Corr. | Statistical Key  Hist. *v*2 NIST Space Sens. | DA | Other attacks | Time Analysis |
| This work | Transformed Lorenz and Arnold map | U | U U U U U | U | U | U |
| [[34]](#_bookmark43) | Affine Hill cipher and Arnold transform | U | U — — from | — | — | — |
| [[35]](#_bookmark43) | Tangent Delay Ellipse Reflecting Cavity Map System (TD- | U | parameters  U — — from | U | — | U |
|  | ERCS), skew tent map and affine transform |  | parameters |  |  |  |
| [[36]](#_bookmark43) | Cosine-Transform-Based Chaotic System (CTBCS) | U | U — — U U | U | — | U |
| [[37]](#_bookmark43) | A chaotic map perturbed by another using either logistic, sine or tent maps | U | U — — U U | U | known-plaintext/ chosen-plaintext | U |

the MUX is removed. The correlation coefficients between the noiseless decrypted image and the noisy one are also given. The robustness against noise can be identified by the capability of per- ceptually identifying the image content and the correlation coeffi- cient values approaching one.

* + 1. *Time analysis*

Our main concern is the time consumed in the solution of the system of differential equations in the substitution phase. Simula- tions are performed using Matlab 8.4.0.150421 (R2014b) and Win- dows 8.1 on an Intel(R) Core(TM) i7-4510U CPU @ 2.00 GHz

machine. Averaged over 10 trials, around 46.81 % increase in the

computation time of transformed Lorenz than Lorenz system is reported. This is associated with the gain of about 3 times increase in the maximum number of bits of the substitution part in the encryption key with nine sub-keys each with high sensitivity.

1. Discussion and comparison against other works

Novel chaotic systems were presented in [[27–33]](#_bookmark56) providing var- ious control capabilities over the strange attractors’ size, location, shape and number of scrolls. Yet, these works barely presented applications for their proposed systems. The image encryption scheme utilizing the proposed transformed Lorenz system is com- pared to other recent image encryption schemes [[34–37]](#_bookmark43), which utilized chaotic systems and included separate transformation stages as well. The basic idea and main blocks utilized in each scheme are given in [Table 9](#_bookmark32), where only [[36]](#_bookmark43) embedded chaotic maps in a cosine transformation to generate equation of a new chaotic map. All the utilized chaotic generators were simple low- dimensional chaotic maps. On the other hand, the proposed trans- formed Lorenz system is based on differential equations allowing increased complexity, sensitivity and further enhanced chaotic properties. The capability of generating three chaotic outputs simultaneously makes it more suitable for color image encryption applications. [Table 9](#_bookmark32) also compares the schemes from the view- point of the performance metrics evaluated in each paper. While both [[36,37]](#_bookmark43) gave a clear description of the key design, space and sensitivity analysis, [[34,35]](#_bookmark43) only mentioned the parameters from which the key can be composed and assessed sensitivity by slightly modifying the parameter value. Such preliminary analysis neglects that the effective key space is governed by the basin of attraction and parameter basin of attraction which correspond to chaotic behavior [[49]](#_bookmark55) and the remarkable importance of Least Significant Bit (LSB) sensitivity. While none of the compared works performed chi-square or NIST tests, all of them presented differential attack and time analyses except [[34]](#_bookmark43). None of the other cryptanalysis attacks or robustness against noise were analyzed except in [[37]](#_bookmark43), which discussed known- and chosen-plaintext attacks.

1. Conclusions and future work directions

A generalized scaling, reflection, rotation, translation or shear- ing transformation of chaotic systems was proposed and validated for the simplest and Lorenz systems. The effects on the time series, equilibrium points, attractor diagrams, bifurcations and MLE were demonstrated. This approach overpasses post-processing by apply- ing transformations on the resulting time series. The six parame- ters, which are embedded in the differential equations of the chaotic system, control the system response and enhance its ran- domness and sensitivity. Trajectory control of the dynamic motion of the attractor was also presented exploring different trajectories. In an image encryption system that passes the standard perfor- mance tests, transformed Lorenz system increases the key space and, hence, security in comparison to Lorenz system with an acceptable increase in the computation time as well as overpassing other recent related works.

For future work, transformations in different 2D planes, 3D transformations and nonlinear transformations can be applied to obtain more random and sensitive time series. Using dynamic parameters, a gallery of strange attractors with variable and con- trollable number of equilibrium points and strange attractor shapes can be produced. In addition, they can be utilized in robotic applications for random motion planning along a prescribed trajec- tory. Given the acceptable increase in the computation time, hard- ware realization of the generalized transformed systems or their special cases can be performed.

Declaration of Competing Interest

The authors declare that they have no known competing finan- cial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. [Strogatz SH. Nonlinear dynamics and chaos: with applications to physics,](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0005) [biology, chemistry, and engineering. Westview Press; 2014](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0005).
2. [Gohari PS, Mohammadi H, Taghvaei S. Using chaotic maps for 3D boundary](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0010) [surveillance by quadrotor robot. Appl Soft Comput 2019;76:68–77](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0010).
3. [Radwan AG, AbdElHaleem SH, Abd-El-Hafiz SK. Symmetric encryption](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0015) [algorithms using chaotic and non-chaotic generators: a review. J Adv Res](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0015) [2016;7(2):193–208](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0015).
4. [Abbas NA. Image encryption based on independent component analysis and](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0020) [arnold’s cat map. Egypt Inf J 2016;17(1):139–46](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0020).
5. [Ge M, Ye R. A novel image encryption scheme based on 3d bit matrix and](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0025) [chaotic map with markov properties. Egypt Inf J 2019;20(1):45–54](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0025).
6. [Wang H, Liang H-F, Miao Z-H. A new color image encryption scheme based on](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0030) [chaos synchronization of time-delay Lorenz system. Adv Manuf 2016;4](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0030) [(4):348–54](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0030).
7. [Radwan A, Soliman A, El-Sedeek A. MOS realization of the modified Lorenz](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0035) [chaotic system. Chaos Solitons Fractals 2004;21(3):553–61](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0035).
8. [Zidan MA, Radwan AG, Salama KN. Controllable V-shape multiscroll butterfly](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0040) [attractor: system and circuit implementation. Int J Bifurcation Chaos 2012;22](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0040) [(06):1250143](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0040).
9. [Lorenz EN. Deterministic nonperiodic flow. J Atmos Sci 1963;20(2):130–41](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0045).
10. [Elwakil AS, Ozoguz S, Kennedy MP. Creation of a complex butterfly attractor](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0050) [using a novel Lorenz-type system. IEEE Trans Circuits Syst I: Fundam Theory](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0050) [Appl 2002;49(4):527–30](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0050).
11. [Lü J, Chen G, Cheng D. A new chaotic system and beyond: the generalized](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0055) [Lorenz-like system. Int J Bifurcation Chaos 2004;14(05):1507–37](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0055).
12. [Elwakil AS, Özoguz S. A system and circuit for generating](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0060) [‘‘multi-butterflies”.](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0060) [Int J Bifurcation Chaos 2008;18(03):841–4](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0060).
13. [Yu S, Tang WK, Lü J, Chen G. Design and implementation of multi-wing](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0065) [butterfly chaotic attractors via Lorenz-type systems. Int J Bifurcation Chaos](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0065) [2010;20(01):29–41](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0065).
14. Elwakil A, Salama K, Kennedy M. A system for chaos generation and its implementation in monolithic form. In: Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on, vol. 5, IEEE; 2000. p. 217–20..
15. [Sprott JC. Simple chaotic systems and circuits. Am J Phys 2000;68(8):758–63](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0075).
16. [Sprott JC. A new class of chaotic circuit. Phys Lett A 2000;266(1):19–23](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0080).
17. [Sprott JC. A new chaotic jerk circuit. IEEE Trans Circuits Syst II Express Briefs](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0085) [2011;58(4):240–3](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0085).
18. [Vaidyanathan S. Analysis, control and synchronization of a 3-D novel jerk](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0090) [chaotic system with two quadratic nonlinearities. Kyungpook Math J](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0090) [2015;55:563–86](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0090).
19. Sayed WS, Radwan AG, Fahmy HA. Chaotic systems based on jerk equation and discrete maps with scaling parameters. In: 6th International Conference on Modern Circuits and Systems Technologies (MOCAST), IEEE; 2017. p. 1–4..
20. [Sayed WS, Radwan AG, Fahmy HA. Chaos and bifurcation in controllable jerk-](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0100) [based self-excited attractors. In: Nonlinear Dynamical Systems with Self-](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0100) [Excited and Hidden Attractors. Springer; 2018. p. 45–70](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0100).
21. [Sayed WS, Henein MM, Abd-El-Hafiz SK, Radwan AG. Generalized dynamic](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0105) [switched synchronization between combinations of fractional-order chaotic](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0105) [systems. Complexity 2017;2017](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0105).
22. [Marion JB. Classical dynamics of particles and systems. Academic Press; 2013](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0110).
23. [Brinón-Arranz L, Seuret A, Canudas-de Wit C. Cooperative control design for](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0115) [time-varying formations of multi-agent systems. IEEE Trans Autom Control](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0115) [2014;59(8):2283–8](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0115).
24. [Hearn D, Baker MP, Baker MP. Computer graphics with OpenGL, vol.](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0120)

[3. NJ: Pearson Prentice Hall Upper Saddle River; 2004](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0120).

1. [Salcedo-Sanz S, Aybar-Ruíz A, Camacho-Gómez C, Pereira E. Efficient fractal-](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0125) [based mutation in evolutionary algorithms from iterated function systems.](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0125) [Commun Nonlinear Sci Numer Simul 2018;56:434–46](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0125).
2. [Roy SK, Kumar S, Chanda B, Chaudhuri BB, Banerjee S. Fractal image](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0130) [compression using upper bound on scaling parameter. Chaos Solitons](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0130) [Fractals 2018;106:16–22](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0130).
3. [Ai X, Sun K, He S, Wang H. Design of grid multiscroll chaotic attractors via](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0135) [transformations. Int J Bifurcation Chaos 2015;25(10):1530027](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0135).
4. [Lassoued A, Boubaker O. On new chaotic and hyperchaotic systems: a](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0140) [literature survey. Nonlinear Anal: Modell Control 2016;21(6):770–89](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0140).
5. [Pham V-T, Jafari S, Wang X, Ma J. A chaotic system with different shapes of](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0145) [equilibria. Int J Bifurcation Chaos 2016;26(04):1650069](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0145).
6. [Liu Y, Guo S. Generation and dynamics analysis of n-scrolls existence in new](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0150) [translation-type chaotic systems. Chaos: Interdisc J Nonlinear Sci 2016;26](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0150) [(11):113114](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0150).
7. [Li C, Sprott JC, Mei Y. An infinite 2-D lattice of strange attractors. Nonlinear](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0155) [Dyn 2017;89(4):2629–39](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0155).
8. [Su Q, Wang C, Chen H, Sun J, Zhang X. A new method for generating chaotic](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0160) [system with arbitrary shaped distributed attractors. Chaos: Interdisc J](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0160) [Nonlinear Sci 2018;28(7):073106](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0160).
9. [Wu Q, Hong Q, Liu X, Wang X, Zeng Z. Constructing multi-butterfly attractors](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0165) [based on Sprott C system via non-autonomous approaches. Chaos Interdisc J](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0165) [Nonlinear Sci 2019;29(4):043112](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0165).
10. [Mishra D, Sharma R, Ranjan R, Hanmandlu M. Security of rgb image data by](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0170) [affine hill cipher over SLn (Fq) and Mn (Fq) domains with Arnold transform.](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0170) [Optik 2015;126(23):3812–22](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0170).
11. [Ahmad J, Hwang SO. A secure image encryption scheme based on chaotic maps](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0175) [and affine transformation. Multimedia Tools Appl 2016;75(21):13951–76](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0175).
12. [Hua Z, Zhou Y, Huang H. Cosine-transform-based chaotic system for image](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0180) [encryption. Inf Sci 2019;480:403–19](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0180).
13. [Alawida M, Samsudin A, Teh JS, Alkhawaldeh RS. A new hybrid digital chaotic](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0185) [system with applications in image encryption. Signal Process 2019;160:45–58](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0185).
14. Sayed W, Radwan A, Elnawawy M, Orabi H, Sagahyroon A, Aloul F, Elwakil A, Fahmy H, El-Sedeek A. Two-dimensional rotation of chaotic attractors: Demonstrative examples and fpga realization, Circuits Syst Signal Process.

pp. 1–14..

1. Sayed WS, Radwan AG, Fahmy HA, Elsedeek A. All-dynamic synchronization of rotating fractional-order chaotic systems. In: 2019 Novel Intelligent and Leading Emerging Sciences Conference (NILES), vol. 1, IEEE; 2019. p. 226–29..
2. Govorukhin VN. Calculation lyapunov exponents for ODE, MATLAB Central File Exchange, file ID 4628; 2004..
3. [Lawrence JD. A catalog of special plane curves. Courier Corporation; 2013](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0210).
4. [Weber AG. The USC-SIPI image database version 5. USC-SIPI Report](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0215) [1997;315:1–24](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0215).
5. [Ye G, Wong K-W. An efficient chaotic image encryption algorithm based on a](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0220) [generalized arnold map. Nonlinear Dyn 2012;69(4):2079–87](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0220).
6. Rukhin A, Soto J, Nechvatal J, Smid M, Barker E. A statistical test suite for random and pseudorandom number generators for cryptographic applications, Tech. rep., DTIC Document; 2001..
7. [Kwok H, Tang WK. A fast image encryption system based on chaotic maps with](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0230) [finite precision representation. Chaos Solitons Fractals 2007;32(4):1518–29](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0230).
8. [Schneier B. Applied cryptography: protocols, algorithms, and source code in](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0235)

[C. John Wiley & Sons; 2007](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0235).

1. [Ahmed F, Anees A, Abbas VU, Siyal MY. A noisy channel tolerant image](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0240) [encryption scheme. Wireless Personal Communications 2014;77(4):2771–91](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0240).
2. [Ismail SM, Said LA, Radwan AG, Madian AH, Abu-Elyazeed MF. Generalized](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0245) [double-humped logistic map-based medical image encryption. J Adv Res](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0245) [2018;10:85–98](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0245).
3. [Sayed WS, Tolba MF, Radwan AG, Abd-El-Hafiz SK. FPGA realization of a](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0250) [speech encryption system based on a generalized modified chaotic transition](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0250) [map and bit permutation. Multimedia Tools Appl 2019;78(12):16097–127](http://refhub.elsevier.com/S1110-8665(20)30135-3/h0250).
4. [Sayed WS, Radwan AG. Generalized Switched Synchronization and Dependent](http://refhub.elsevier.com/S1110-8665(20)30135-3/optABSWObMswS) [Image Encryption Using Dynamically Rotating Fractional-Order Chaotic](http://refhub.elsevier.com/S1110-8665(20)30135-3/optABSWObMswS) [Systems. AEU-International Journal of Electronics and Communications](http://refhub.elsevier.com/S1110-8665(20)30135-3/optABSWObMswS) [2020;153268](http://refhub.elsevier.com/S1110-8665(20)30135-3/optABSWObMswS).