



A novel grayscale image encryption approach based on chaotic maps and image blocks

Ashish Girdhar¹ · Himani Kapur² · Vijay Kumar³

Received: 11 October 2020 / Accepted: 4 February 2021 / Published online: 24 February 2021
© The Author(s), under exclusive licence to Springer-Verlag GmbH, DE part of Springer Nature 2021

Abstract

Image encryption converts a meaningful image into some random arrangement of pixel intensities. That means, the intelligible property of an image is destroyed. Taking into consideration excessively large time and space complexity required by the image encryption algorithm using multiple chaotic systems, this paper proposes an image encryption method in which employs three chaotic sequence to achieve fairly high level of encryption. Novelty of the proposed approach lies in the designed algorithm to achieve both permutation and substitution processes of image encryption. In the end, a comparison in the coefficient correlation values is drawn to evaluate the performance of the proposed algorithm with respect to many lately proposed image encryption schemes.

1 Introduction

To convey a message, an image is more helpful than text. Content of an image is easily understood by anybody present in any corner of the world. However, to convey some information using text, two pre-requisites are required. First, the receiver must be a literate person (images are understood by illiterates as well); second, sender and receiver must be well versed with at least one common language. Thus, image is generally preferred over text. However, advances of information technology have brought everyone on the planet on Internet. Which is why, images used in communication are vulnerable to attacks. One of the feasible solutions is cryptography. Cryptography converts a meaningful image into some random collection of pixel intensities (called encrypted image); making it look like some random noise. With only correct and precise keys, the encrypted image can be decrypted to give the original image back. Encrypted image reveals nothing to the intruders. For an additional layer of security, the encrypted image is added to naïve looking 2D or 3D image [25]. Encryption of plain image can be carried

out in optical and digital domain. Optical encryption methods use fractional Fourier transform [26, 27], double random phase encoding [28], wavelength multiplexing [29] and other multiplexing methods [30, 31]. However, as pointed out in [28] some inherent weaknesses of optical methods inhibit their use in image encryption. The proposed image encryption uses digital methods to encrypt image and is based on two chaotic maps—Ikeda map and logistic map.

As reported in a recent survey on image encryption [1], in the 2018 only, about a thousand plus publications have been found related to the field of image encryption. Hence, area of image encryption has piqued the interests of researchers and is continuing to do so. While encrypted image can be sent directly over the communication channel, it can be hidden inside a cover media in an invisible manner [2]. A typical image encryption model consists of two stages—permutation and substitution as pointed out in [3] which is shown in Fig. 1. In the present paper, a novel image encryption algorithm is proposed which utilises two chaotic maps—Ikeda map and logistic chaotic map. Diffusion or substitution is carried out at pixel level while confusion is done at the pixel level while the confusion or permutation is done at the bit level.

The structure of the proposed paper is as follows. Chaotic maps and their advantages are discussed in Sect. 2. A brief review of related image encryption methods is presented in Sect. 3. The proposed algorithm is presented in detail in Sect. 4. Results obtained from simulation of proposed

✉ Ashish Girdhar
ashishgirdhar410@gmail.com

¹ CSED, Delhi Technological University, Delhi, India

² G.G.S.S.S., Kaithal, Haryana, India

³ CSED, National Institute of Technology Hamirpur, Hamirpur, Himachal Pradesh, India

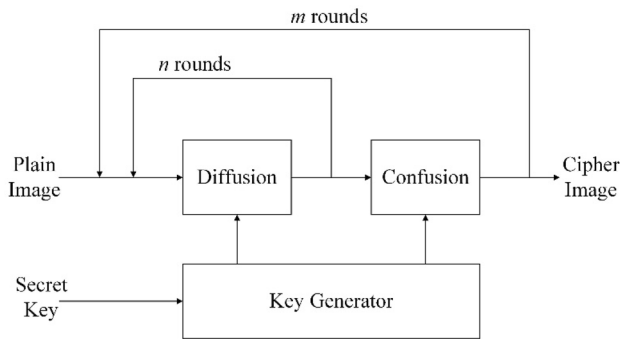


Fig. 1 Skeleton of a typical image encryption procedure

algorithm and comparisons with state of the art approaches is presented in detail in Sect. 5, followed by conclusion in Sect. 6.

2 Chaotic maps

Chaotic maps exhibit various favourable characteristics which make them suitable to be used in image encryption process. These characteristics are—pseudo-randomness, extreme sensitivity towards any change in initial conditions (or control parameters) and ergodicity. In the proposed paper, two chaotic maps are used.

2.1 Ikeda map

The original chaotic map was proposed by Kensuke Ikeda during his experiment [4]. Complex Ikeda map is defined in 2D space as follows:

$$x_{n+1} = 1 + \mu(x_n \cos t_n - y_n \sin t_n), \tag{1}$$

$$y_{n+1} = \mu(x_n \sin t_n - y_n \cos t_n), \tag{2}$$

$$t_n = 0.4 - \frac{6}{1 + x_n^2 + y_n^2}, \tag{3}$$

where μ is control parameter. 2D Ikeda map exhibits chaotic behaviour when $\mu \geq 0.6$. To obtain xy chaotic attractors of Ikeda map, $\mu = 0.9$ is chosen. Twenty starting points were taken and their trajectories were traced as shown in Fig. 2.

In this figure, as can be observed $x \in (-40, 35)$ and $y \in (-30, 30)$. To use Ikeda map for diffusion process of image encryption, these chaotic sequences were taken down to range (0,1).

2.2 Logistic chaotic map

Logistic chaotic map is the most popular chaotic map used in several image encryption algorithms. Mathematically, 1D logistic chaotic map is defined as follows:

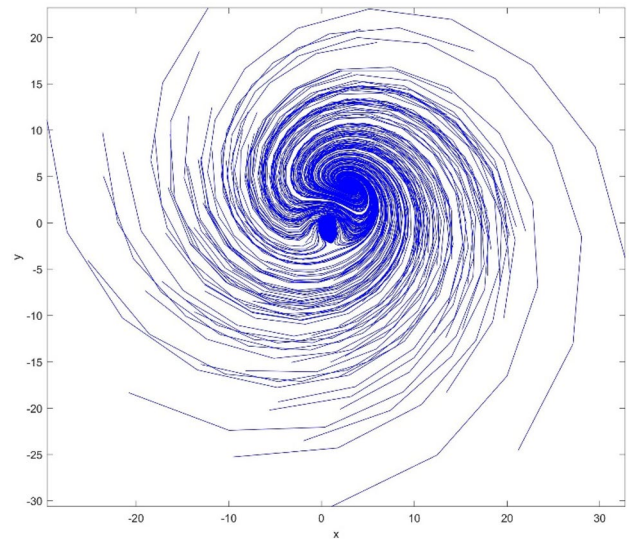


Fig. 2 Chaotic attractors of Ikeda map

$$x_{n+1} = \mu x_n (1 - x_n), \tag{4}$$

where μ is the control parameter. For $\mu > 3.569945$, the system goes into chaotic state [5]. Bifurcation diagram obtained by implementing 1D logistic map in Matlab has been shown in Fig. 3. As can be observed, for the specified range of μ , chaos is exhibited by the map.

Chaotic sequence obtained from 1D logistic map is used in the confusion or permutation process of the proposed image encryption algorithm. A brief review of the above two chaotic maps used in image encryption is presented in next section.

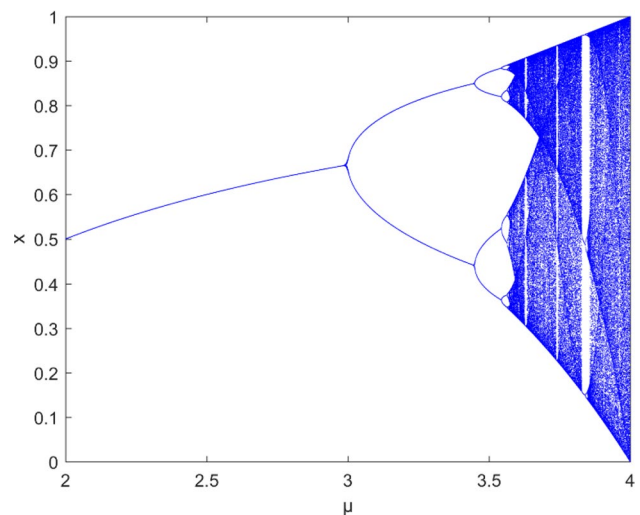


Fig. 3 Bifurcation diagram of logistic map obtained in Matlab

3 Related works

While logistic chaotic map is used in various image encryption techniques proposed so far in the literature; use of Ikeda map for construction of chaotic sequences in image encryption is limited to a very few image encryption algorithms [6]. Since the present work is for the image encryption of grayscale images using Ikeda map, literature review of grayscale image encryption schemes using Ikeda map is presented.

Jia [7] used only Ikeda map for both phases—pixel shuffling (using the sort indices) and pixel substitution. The results obtained from simulation of the algorithm were shown to be robust against the histogram analysis, correlation analysis and key sensitivity analysis. Zhu et al. [8] proposed a bit level permutation than a pixel level permutation. In their approach, Arnold cat map has been used for permutation and for diffusion, logistic map has been used. Mannai et al. [9] proposed discretised version of Ikeda system. Chaotic sequence obtained from discretised Ikeda map is XORed with the plain image pixels to obtain encrypted image. Alshibani et al. [10] used a mix of three Arnold transform, Henon map and Ikeda map for diffusion phase of grayscale images. In this paper, DNA encoding of pixels of plain image and masking key was done. Exclusive OR operation was performed between DNA sequences of plain image and that of masking key. Masking key was obtained using sort operation on the chaotic sequences of Henon map and Ikeda map. Parvees et al. [11] proposed colour image encryption algorithm using Ikeda map and logistic map. For each colour channel, separate chaotic sequences from Ikeda map and logistic map were generated. Şekertekin et al. [12] used Ikeda map for permutation and Henon map for diffusion. Becheikh et al. [13] used 1D Ikeda map and T-function for generation of a S-box which is used for grayscale image encryption. The proposed S-box was proved to have various essential properties such as bijectivity, bit independence criterion (BIC), nonlinearity, strict avalanche criterion (SAC), differential and linear approximation probability. Hikal et al. [14] proposed encryption scheme for palm print images. Since palm print images carry unique information of palm lines, shape, and texture of an individual; these are most reliable biometric authenticators. In addition, decryption process should be able to give back the exactly same plain image because a loss of even a pixel may cause the palm print matching mechanism to fail. The authors used a mix of three chaotic maps—Arnold's cat map (for confusion) and Ikeda map and enhanced Lorenz map for diffusion of pixels in confused (or permuted) image. Li et al. [15] obtained two chaotic sequences from Ikeda map and used one chaotic sequence for confusion phase and other for

diffusion phase. In their approach, the authors proposed a novel approach for encrypting a Preview-Region-Image. The encrypted image and encrypted preview image are placed in Ciphred image. First, the encrypted Preview-Region-Image is decrypted and afterwards encrypted image. This is useful as it saves time in decrypting only the images of interest and not all encrypted images. A recent research by Girdhar et al. [16] applied XOR operations on chaotic sequences obtained from Lorenz and Rossler hyperchaotic system and colour image pixels and very nice results were obtained.

There are a few things that can be observed from this literature review:

- XOR operation on chaotic sequences and image pixel value results in encrypted image.
- Use of Ikeda map increases randomness in plain image.
- As pointed in the review, modification at bit level is preferred over the pixel level.

Keeping the above-mentioned points in mind, an image encryption algorithm is proposed in the next section.

4 Image encryption algorithm

A brief overview of the approach is shown in Fig. 4. A plain image is taken on which diffusion is done using chaotic sequence from Ikeda map and confusion is done using chaotic sequence from logistic map.

As the proposed image encryption process consists of two phases—diffusion and confusion, the encryption algorithm is explained in two parts—first diffusion process followed by confusion.

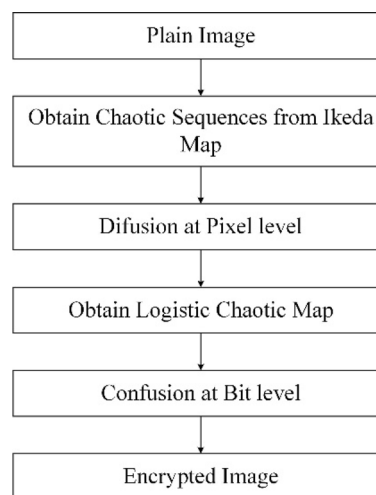


Fig. 4 Brief layout of image encryption algorithm

4.1 Diffusion process

1. Read plain image (I) of dimension ($M \times N = R$).
2. Divide I into two vertical halves— I_1 and I_2 each of size $M \times (N/2)$.
3. Next, obtain chaotic sequences from Ikeda map of size $R/2$.
4. To ensure that the chaotic sequences have unique value, algorithm in [17] is used. This results in two chaotic sequences— x, y which are unique with values lying in $[1, R/2]$.
5. Reshape both x and y arrays to be of same dimension as that of I_1 and I_2 .
6. Apply sort operation on x and y arrays in column wise direction and keep sort_indices in separate arrays as shown in Fig. 5. It is to be kept in mind that the unsorted x and y arrays will be used in the algorithm and sort operation is done to obtain the sort_indices of these two arrays.
7. Next, using sort_indices_y array, perform bitXOR operation on I_1 and x to obtain I'_1 . This step is explained in Fig. 6.
8. Similarly, using sort_indices_x array, perform bitXOR operation on I_2 and y to obtain I'_2 .
9. I'_1 and I'_2 are combined to form I' .
10. Now, I' is divided into two horizontal halves— I_3 and I_4 each of size $(M/2) \times N$.
11. Again, x and y arrays are reshaped to be same dimension as that of I_3 and I_4 .

12. Apply sort operation on x and y arrays in row wise direction and keep sort_indices in separate arrays as shown in Fig. 7. Again, unsorted x and y arrays will be used in the algorithm and sort operation is done to obtain the sort_indices of these two arrays.
13. Now, using sort_indices_x, bitXOR is performed between I_3 and y arrays to obtain I'_3 . This step is explained in Fig. 8.
14. Similarly, using sort_indices_y, I_4 and x arrays are bitXORed to give I'_4 .
15. Afterwards, I'_3 and I'_4 are combined to give encrypted image after diffusion (EI_D). EI_D is then taken to the confusion phase.

4.2 Confusion process

Following steps are performed over the encrypted image after diffusion (EI_D) in this process.

1. All intensity levels of the plain image (I) are added to form S .
2. Next, S is divided by suitable power of 10 so that newly formed $S < 1$.
3. Add S to the initial value of logistic chaotic map so that a unique chaotic sequence is generated for every plain image.

Fig. 5 Sort **a** y array in vertical direction to obtain **b** sort_indices_y array and **c** sorted_y array

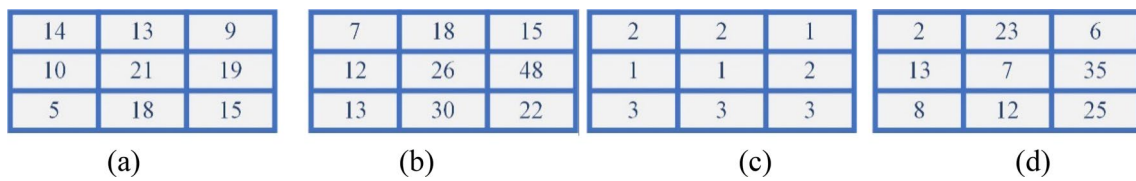
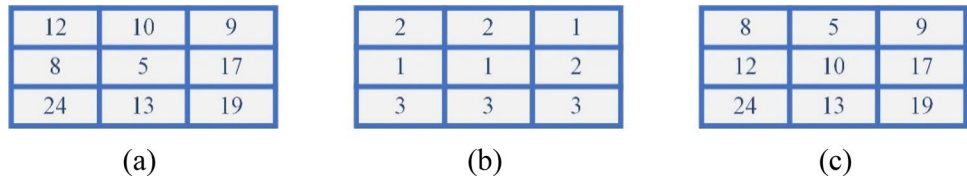
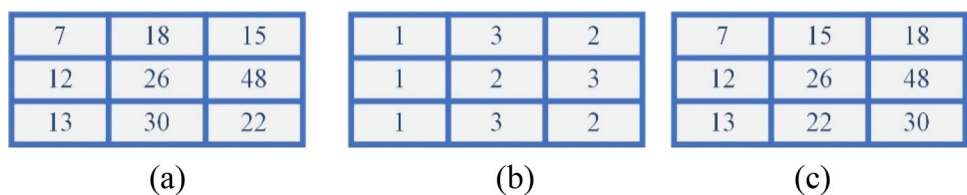


Fig. 6 BitXOR operation on **a** I_1 and **b** x using **c** sort_indices_y to obtain **d** I'_1

Fig. 7 Sort **a** x array in horizontal direction to obtain **b** sort_indices_x array and **c** sorted_x array



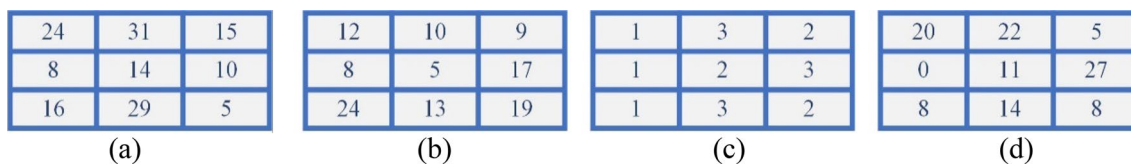


Fig. 8 bitXOR operation on a I_3 and b y using c $sort_indices_x$ to obtain d I_3'

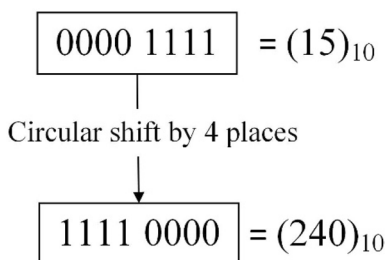


Fig. 9 Right circular shift by four places changes pixel intensity from $(15)_{10}$ to $(240)_{10}$

4. Apply modulo-by-8 operation on the chaotic sequence generated from the above written step, resulting in a chaotic sequence from the range $[0, 7]$.
5. Pixel value from EI_D is read and converted to binary bits in a 8-bit representation.
6. Read a value from chaotic sequence and perform right circular shift on the binary bit representation. This is the permutation step and it not only permutes the binary bits of a pixel but also changes the pixel value. An example of this step is shown in Fig. 9 where a pixel value of $(15)_{10}$ is converted to $(240)_{10}$, considering value = 4.
7. Repeat the entire process of all pixel intensities in the EI_D .
8. Afterwards, convert all binary bit representations to decimal intensities to receive the final encrypted image.

The entire process of the confusion process is summarised in Fig. 10.

To decrypt the encrypted image, exact secret key is to be used and the entire process of encryption is to be repeated, but in reverse order. This implies that, first confusion process is done on the encrypted image. During the confusion phase, first decimal valued intensities are converted to the binary bit representations of 8 bits. Exact same chaotic sequence is generated using the same initial conditions. Perform right circular shift on the binary bit representations to get EI_D . Next, diffusion process is repeated with steps performed in reverse order to get decrypted image which is exactly same to I .

5 Results obtained from simulation

The proposed algorithm was implemented in Matlab and run on a i7 processor with an 8-GB RAM. Table 1 shows plain, encrypted and decrypted images. As can be observed in the table, encrypted image is seemingly a random image and does not reveal anything.

5.1 Key space and key sensitivity

As the proposed image encryption uses two secret keys for Ikeda map generation and one for logistic map generation, each having precision up to 10^{-15} decimal places, 10^{45} ($= 10^{15} \times 10^{15} \times 10^{15}$) brute force attacks would be required to break the system. Large key space ensures safety from brute force attackers. Next, key sensitivity can be ensured by decrypting encrypted image with a slightly modified key. If the decryption process fails to decrypt the encrypted image, then sensitivity of secret key is realised (Fig. 11).

5.2 Statistical analysis

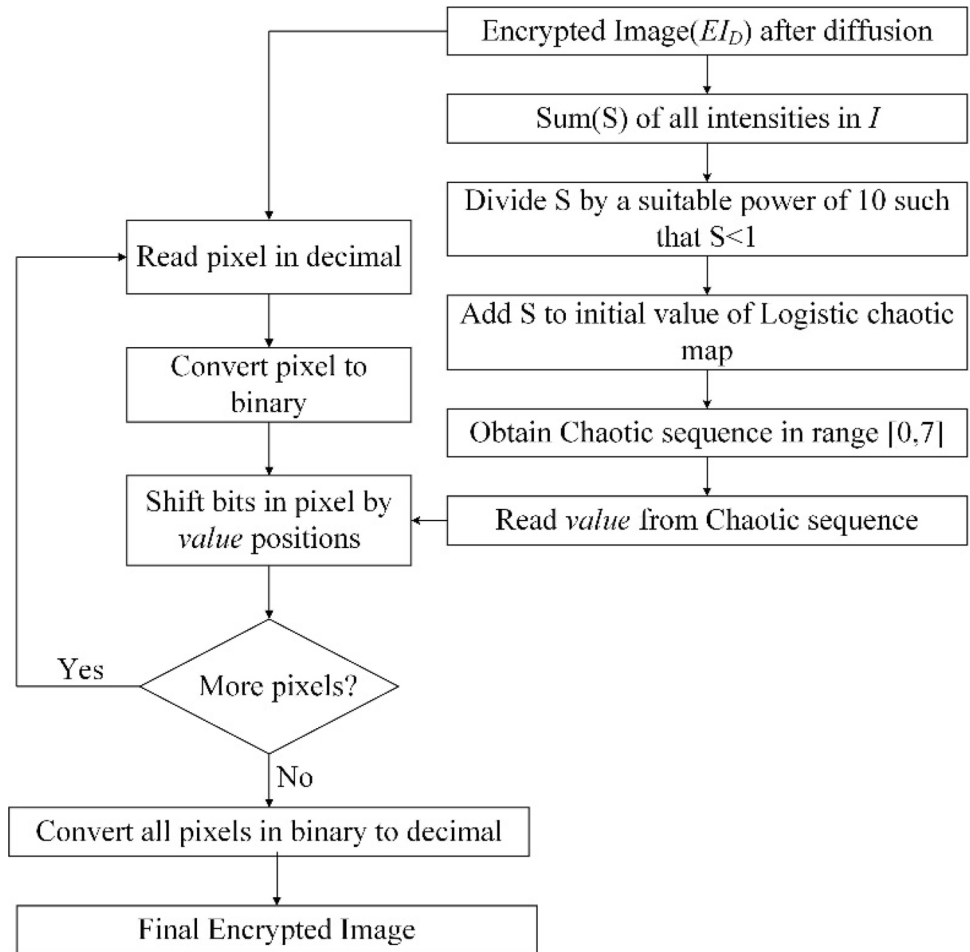
Encrypted images are attacked by statistical analysers to extract information about it. Statistical information about encrypted image is extracted to examine if a seemingly noisy image is carrying any meaningful message or not. This is done by obtaining histogram of the encrypted image and drawing correlations among the pixels.

5.2.1 Histogram analysis

Histogram drawn for a true random image would have absolutely uniform histogram bars [16] because frequency of all pixel intensities is equal. An ideal histogram is shown in Fig. 12 where height of pixel intensities is exactly same.

Histogram for both plain image of baboon and respective encrypted image was obtained as shown in Fig. 13. Uniformity in histogram of encrypted image of baboon can be observed from the figure.

Fig. 10 Confusion process of the proposed approach



5.2.2 Correlation analysis

In a plain image, correlations among adjacent pixels in vertical, horizontal and diagonal directions exist in such a way that the correlation coefficient ≈ 1 . However, the encryption algorithm should be able to destroy the correlations among pixels in all three directions. Calculation of correlation coefficient is done using formula mentioned in [16]. Correlation coefficient between neighbouring pixels in horizontal direction x and y is calculated as follows:

$$E(x) = \frac{1}{T} \sum_{i=1}^T x_i, \tag{5}$$

where $E(x)$ is the mean value of pixel intensities of total number of pixels which are selected randomly from image.

After finding $E(x)$, deviation from mean value and covariance is calculated using the following formula:

$$D_x = \frac{1}{T} \sum_{i=1}^T (x_i - E(x))^2, \tag{6}$$

$$\text{cov}(x, y) = \frac{1}{T} \sum_{i=1}^T (x_i - E(x))(y_i - E(y)), \tag{7}$$

Using deviation and covariance values, correlation coefficient is calculated as follows:

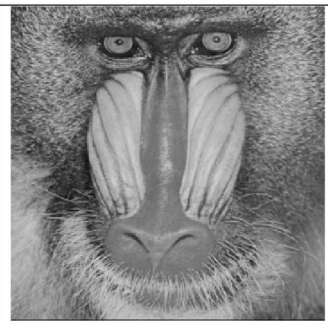
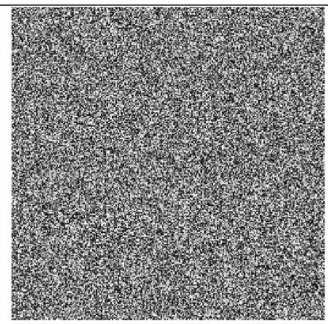
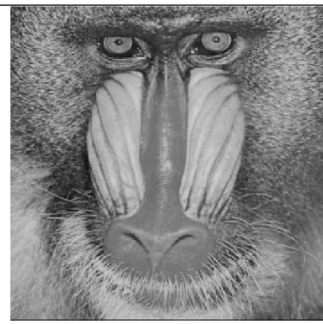
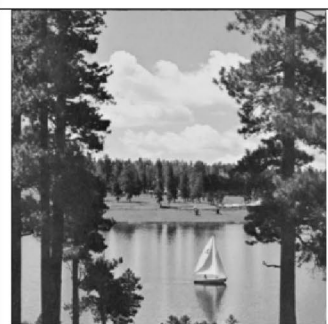
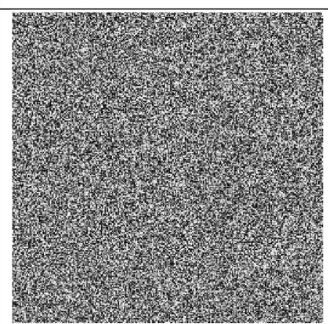

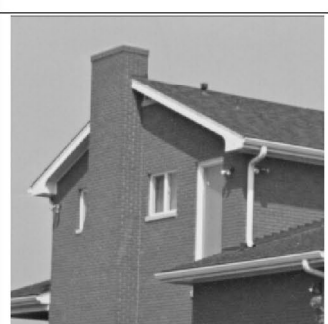
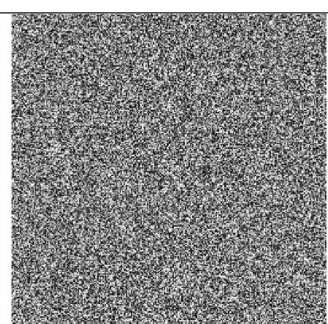
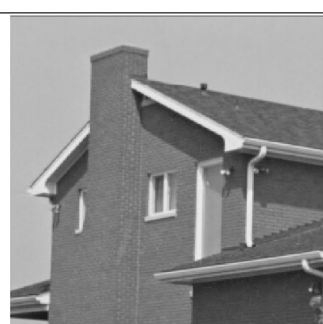
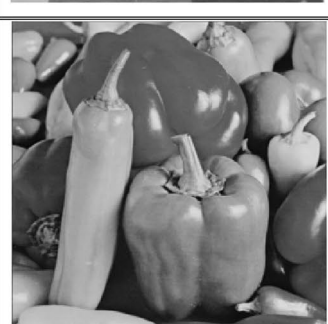
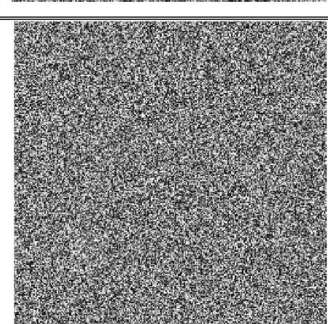


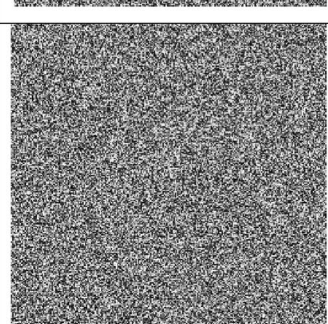

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D_x} \sqrt{D_y}}. \tag{8}$$

Table 2 was obtained for correlation coefficient among pixels of both plain image and encrypted image in horizontal, vertical and diagonal directions for 3000 pixels chosen randomly.

It can be observed from this table that the correlations among neighbouring pixels in horizontal vertical and diagonal directions have been destroyed. Hence, significant descent in correlation coefficient values in encrypted images (Fig. 14).

It is evident from the figure, that pixels are very closely related in plain image of Baboon in horizontal, vertical and diagonal direction. However, pixel intensities are sparsely located from one another in the encrypted image.

Table 1 Plain, encrypted and decrypted images

Plain Image	Encrypted Image	Decrypted Image
		
		
		
		
		

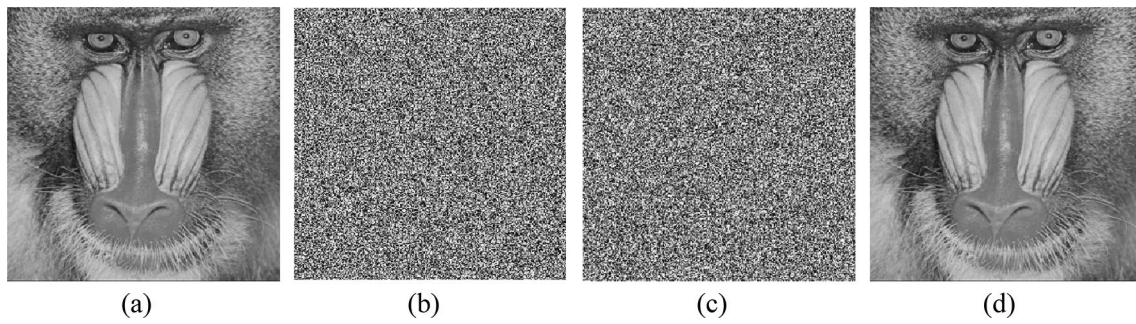
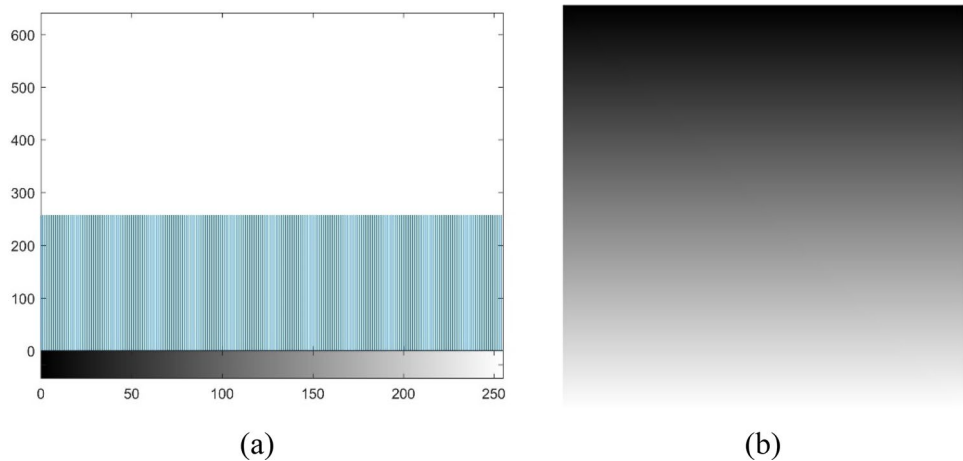


Fig. 11 a Plain image, b encrypted image, decrypted image using c wrong key and d right key

Fig. 12 Uniform histogram bars (a) obtained for a truly random image (b)



Thus, correlations of plain image are destroyed completely by the proposed encryption algorithm.

A comparison with some recent research works in the area of image encryption is shown in Table 3. As can be observed that the encrypted images obtained from proposed image encryption algorithm is able to reduce the correlations among pixels in the best manner. This is because confusion process of the proposed image encryption algorithm works at the bit level. Whereas, all the image encryption algorithms against which comparison is being done, do not perform any operation at bit level. Thus, it can be deduced that operations carried out at bit level encrypt image in a much better way.

5.3 Differential attack analysis

Differential attack analysis is conducted by attackers to establish a relationship between plain image and encrypted image. To determine potency of encryption algorithm to withstand this attack, two parameters—number of pixels change rate (NPCR) and unified average changing intensity (UACI) are determined. Evaluation of NPCR and UACI is done using two encrypted images.

A pixel is chosen at random in plain image and changed to form a new plain image. Then, both plain image and new plain image are encrypted to receive two encrypted images E_1 and E_2 . Using following formulae and E_1 and E_2 , value of NPCR and UACI is determined [18] and mentioned in Table 4:

$$D(i, j) = \begin{cases} 0 & \text{if } E_1(i, j) = E_2(i, j) \\ 1 & \text{otherwise} \end{cases}, \tag{9}$$

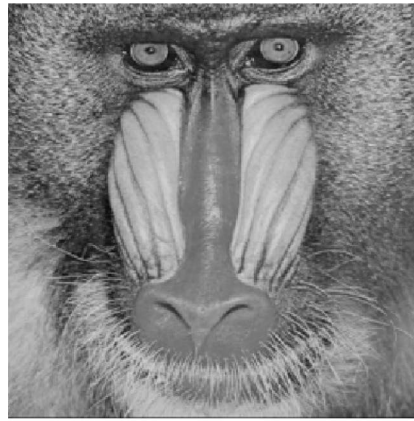
$$\text{NPCR} = \frac{\sum_{i=1}^N \sum_{j=1}^M D(i, j)}{N \times M} \times 100, \tag{10}$$

$$\text{UACI} = \frac{\sum_{i=1}^N \sum_{j=1}^M \frac{E_1(i, j) - E_2(i, j)}{255}}{N \times M}. \tag{11}$$

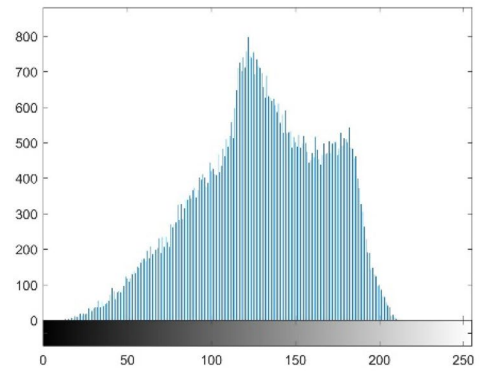
5.4 Information entropy analysis

Information entropy is a measure of randomness in a system. Higher value of information entropy of a system, higher is the randomness or disturbance in the system.

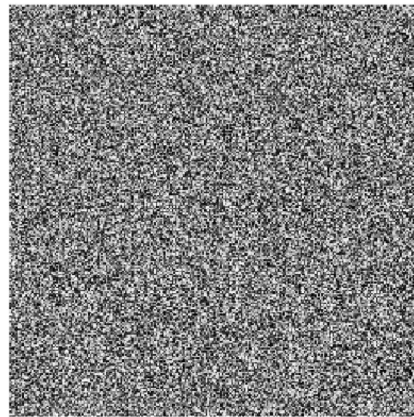
Fig. 13 Histogram of plain image (a) in (b); encrypted image (c) in (d)



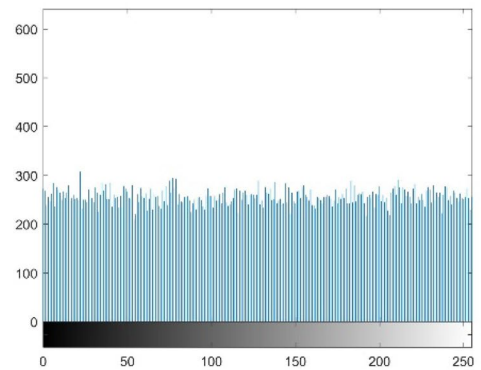
(a)



(b)



(c)



(d)

Table 2 Correlation coefficient of neighbouring pixels in horizontal, vertical and diagonal directions

Image name	Horizontal	Vertical	Diagonal
Plain Baboon	0.874	0.826	0.784
Encrypted Baboon	-0.003	-0.009	0.0005
Plain marbles	0.978	0.982	0.965
Encrypted marbles	0.001	0.008	0.004
Plain hut	0.978	0.953	0.936
Encrypted hut	0.001	-0.007	0.002
Plain peppers	0.963	0.970	0.936
Encrypted peppers	-0.002	0.0001	-0.001
Plain boat	0.958	0.956	0.928
Encrypted boat	-0.0002	0.00007	0.004

Information entropy of an image is calculated using the following formula [19]:

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) \log_2 \frac{1}{p(m_i)} \tag{12}$$

where $p(m_i)$ is probability of appearance of m_i in image and n represents different grey planes. Since a grayscale image contains eight planes, the maximum value of entropy of using formula stated above comes out to be 8. Hence, as close to 8, entropy of an image is, as close to being random the image is. Table 5 lists information entropy values of plain and encrypted images. It can be seen from the table that the information entropy of the images has increased as a result of the encryption algorithm.

5.5 Encryption speed

Speed is another parameter to determine the potency of an image encryption algorithm. Since speed of a procedure is highly dependent on hardware on which it is implemented, a point-to-point comparison cannot be made. Nevertheless, encryption times (in terms of ms) as put up by some research works are taken and compared with the proposed algorithm as jotted down in Table 6. Speed of the proposed algorithm is measured in Matlab using commands tic and toc.

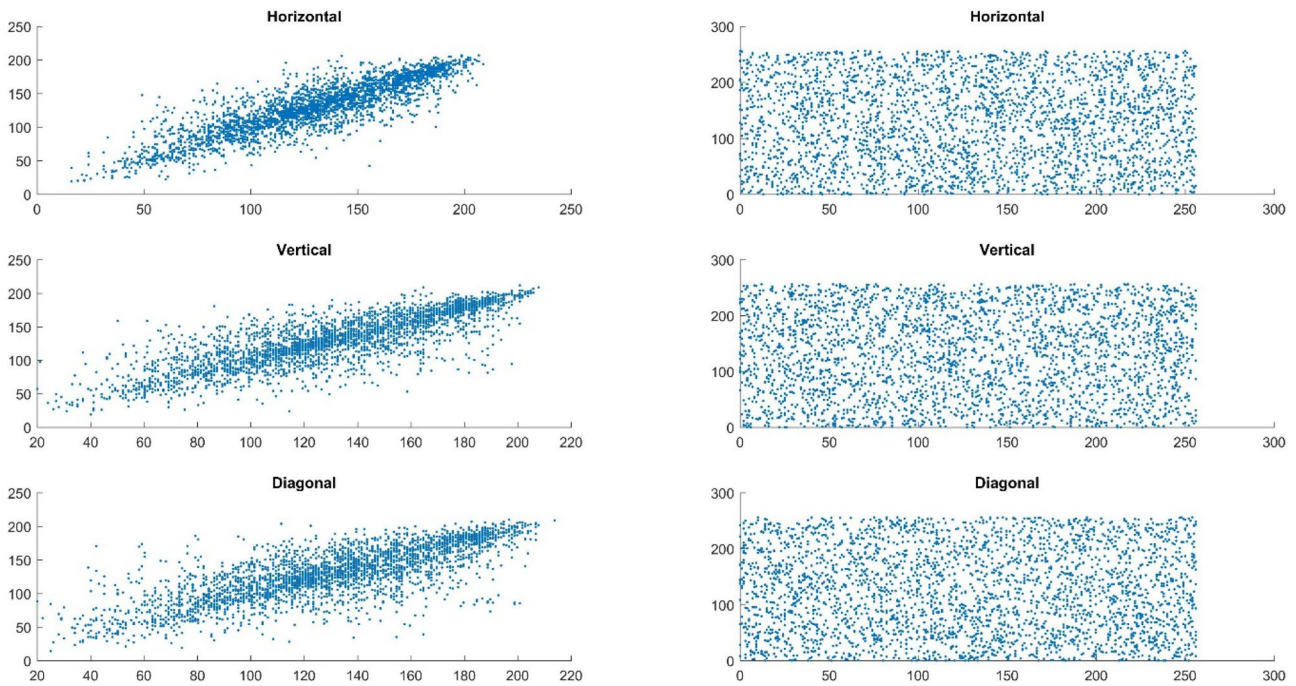


Fig. 14 Correlation coefficient plots for plain (on left) and encrypted image (on right) of Baboon

Table 3 Comparison in terms of correlation coefficient with some recent works

Direction	Proposed work	[20]	[21]	[22]	[23]	[24]
Vertical	0.0000718	-0.0568	-0.0130	0.0305	0.0034	0.000697
Horizontal	-0.00022	0.0456	0.0096	-0.0432	-0.0024	-0.00031
Diagonal	0.000597	-0.0202	-0.0132	0.0275	0.0030	-0.00022

Table 4 NPCR and UACI values for encrypted images of respective plain images

Image name	Parameter	Value
Baboon	NPCR	99.609
	UACI	33.463
Marbles	NPCR	99.737
	UACI	33.434
Hut	NPCR	99.655
	UACI	33.438
Peppers	NPCR	99.587
	UACI	33.762
Boat	NPCR	99.671
	UACI	33.482

Table 5 Information entropy of plain and encrypted images

Image name	Plain	Encrypted
Baboon	7.229	7.998
Marbles	5.728	7.998
Hut	6.496	7.997
Peppers	7.580	7.997
Boat	7.457	7.997

6 Conclusion

The proposed image encryption algorithm encrypts a given plain grayscale image using Ikeda map at pixel level and logistic map at bit level. Encrypted image is obtained by applying bitXOR operations on horizontal and vertical halves of the plain image and the applying circular shift operations bitwise on all pixel intensities of confused image. The proposed image encryption algorithm has been simulated and the results are evaluated under differential, statistical and brute force attacks. Comparison with some

As can be observed, the proposed image encryption takes suitably less time in encrypting a plain image as compared to other research works.

Table 6 Comparison in terms of encryption speed (in ms)

Proposed work	[20]	[21]	[32]	[33]	[34]	[35]
405.85	727.40	392	1184	3284	150	2837

recent works of grayscale image encryption algorithms is also presented. The novelty of the proposed work lies in the manner in which encryption algorithm is applied. Only two chaotic sequences are used for producing such promising results. Blocking and halving is not new, however, unequal halving has not been done prior to the best knowledge of the authors. Introducing more and more chaotic sequences increases both time and space complexity. Hence, this novel grayscale algorithm is the need of the hour and will entice the audience and readers to create efficient and less complex (in terms of time and space) grayscale image encryption algorithm.

References

- C. Li, Y. Zhang, E.Y. Xie, When an attacker meets a cipher-image in 2018: a year in review. *J. Inf. Secur. Appl.* **48**, 102361 (2019)
- A. Girdhar, V. Kumar, Comprehensive survey of 3D image steganography techniques. *IET Image Proc.* **12**(1), 1–10 (2018)
- Y. Wang, K.-W. Wong, X. Liao, G. Chen, A new chaos-based fast image encryption algorithm. *Appl. Soft Comput.* **11**(1), 514–522 (2011)
- K. Ikeda, Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system. *Opt. Commun.* **30**(2), 257–261 (1979)
- L. Liu, Q. Zhang, X. Wei, A RGB image encryption algorithm based on DNA encoding and chaos map. *Comput. Electr. Eng.* **38**(5), 1240–1248 (2012)
- P.R. Sankpal, P.A. Vijaya, Image encryption using chaotic maps: a survey. 2014 Fifth international conference on signal and image processing (2014)
- X. Jia, Image encryption using the Ikeda map. 2010 International conference on intelligent computing and cognitive informatics (2010)
- Z.-L. Zhu, W. Zhang, K.-W. Wong, H. Yu, A chaos-based symmetric image encryption scheme using a bit-level permutation. *Inf. Sci.* **181**(6), 1171–1186 (2011)
- O. Mannai, R. Bechikh, H. Hermassi, R. Rhouma, S. Belghith, A new image encryption scheme based on a simple first-order time-delay system with appropriate nonlinearity. *Nonlinear Dyn.* **82**(1–2), 107–117 (2015)
- D.R. Alshibani, S.A. Qassir, Image enciphering based on DNA exclusive-OR operation union with chaotic maps. 2016 Al-Sadeq international conference on multidisciplinary in IT and communication science and applications (AIC-MITCSA) (2016)
- M.M. Parvees, J.A. Samath, I.K. Raj, B.P. Bose, A colour byte scrambling technique for efficient image encryption based on combined chaotic map: image encryption using combined chaotic map. 2016 International conference on electrical, electronics, and optimization techniques (ICEEOT) (2016)
- Y. Sekertekin, O. Atan, An image encryption algorithm using Ikeda and Henon chaotic maps. 2016 24th Telecommunications forum (TELFOR) (2016)
- R. Becheikh, O. Mannai, R. Rhouma, S. Belghith, A novel family of strong S-Box based on Ikeda map and T-function. 2017 IEEE/ACS 14th international conference on computer systems and applications (AICCSA) (2017)
- N.A. Hikal, M.M. Eid, A new approach for palmprint image encryption based on hybrid chaotic maps. *J. King Saud Univ. Comput. Inf. Sci.* **32**(7), 870–882 (2018)
- C. Li, G. Luo, C. Li, A novel scheme for the preview of the image encryption based on chaotic Ikeda map. *Int. J. Netw. Secur.* **20**(6), 1105–1114 (2018)
- A. Girdhar, V. Kumar, A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences. *Multimed. Tools Appl.* **77**(20), 27017–27039 (2018)
- A.C. Dăscălescu, R.E. Boriga, A novel fast chaos-based algorithm for generating random permutations with high shift factor suitable for image scrambling. *Nonlinear Dyn.* **74**(1–2), 307–318 (2013)
- Y. Wu, J.P. Noonan, S. Agaian, NPCR and UACI randomness tests for image encryption. *Cyber J. Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun.* **1**(2), 31–38 (2011)
- M.B. Farah, R. Guesmi, A. Kachouri, M. Samet, A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. *Opt. Laser Technol.* **121**, 105777 (2020)
- S. Somaraj, M.A. Hussain, Performance and security analysis for image encryption using key image. *Indian J. Sci. Technol.* **8**(35), 1–4 (2015)
- Y. Suryanto, M.T. Suryadi, K. Ramli, A secure and robust image encryption based on chaotic permutation multiple circular shrinking and expanding. *J. Inf. Hiding Multimed. Signal Process.* **7**(4), 697–713 (2016)
- G.A. Sathish kumar, K.B. Bagan, N. Sriraam, Image encryption based on diffusion and multiple chaotic maps. *Int. J. Netw. Secur. Appl.* **3**(2), 181–194 (2011)
- J.D.D. Nkpkop, J.Y. Effa, J.S.A.E. Fouda, M. Alidou, L. Bitjoka, M. Borda, A fast image encryption algorithm based on chaotic maps and the linear diophantine equation. *Comput. Sci. Appl.* **1**(4), 232–243 (2014)
- S.F. Yousif, Grayscale image confusion and diffusion based on multiple chaotic maps. 2018 1st International scientific conference of engineering sciences - 3rd scientific conference of engineering science (ISCES) (2018)
- A. Girdhar, V. Kumar, A reversible and affine invariant 3D data hiding technique based on difference shifting and logistic map. *J. Ambient Intell. Humaniz. Comput.* **10**(12), 4947–4961 (2019)
- P. Refregier, B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **20**(7), 767–769 (1995)
- M.A. Mohamed, A.S. Samarah, M.I. Fath Allah, Optical encryption techniques: an overview. *Int. J. Comput. Sci. Issues IJCSI* **11**(2), 125–129 (2014)
- A. Alfalou, C. Brosseau, Optical image compression and encryption methods. *Adv. Opt. Photon.* **1**(3), 589–636 (2009)
- G. Situ, J. Zhang, Multiple-image encryption by wavelength multiplexing. *Opt. Lett.* **30**(11), 1306–1308 (2005)

30. J.F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, Multiplexing encryption-decryption via lateral shifting of a random phase mask. *Opt. Commun.* **259**(2), 532–536 (2006)
31. J.F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, Multiplexing encrypted data by using polarized light. *Opt. Commun.* **260**(1), 109–112 (2006)
32. P. Ping, F. Xu, Z.J. Wang, Image encryption based on non-affine and balanced cellular automata. *Signal Process.* **105**, 419–429 (2014)
33. R. Enayatifar, A.H. Abdullah, I.F. Isnin, Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. *Opt. Lasers Eng.* **56**, 83–93 (2014)
34. G. Ye, K.-W. Wong, An efficient chaotic image encryption algorithm based on a generalized Arnold map. *Nonlinear Dyn.* **69**, 2079–2087 (2012)
35. X. Wang, C. Jin, Image encryption using Game of Life permutation and PWLCM chaotic system. *Opt. Commun.* **285**, 412–417 (2012)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.