Neural Computing and Applications (2020) 32:11837–11857
https://doi.org/10.1007/s00521-019-04667-y

ORIGINAL ARTICLE

Secure image encryption scheme based on fractals key with Fibonacci series and discrete dynamical system

Majid Khan[1,2] · Fawad Masood[3] · Abdullah Alghafis[4]

Received: 7 February 2019 / Accepted: 5 December 2019 / Published online: 21 December 2019

Abstract
In this article, our aim is to design a new and efficient digital information confidentiality mechanism. We have offered an encryption scheme which is based on fractals and multiple chaotic iterative maps in order to add more confusion and diffusion capability. Due to randomness nature and unique repetitive pattern of fractal increases key space to hundreds of bits and enhance security level of proposed cryptosystem. The projected algorithm is authenticated by utilizing security performance analyses. The security performances elucidate that our suggested technique is quite competent for digital image encryption.

Keywords Fractals · Cryptography · Fibonacci · Chaotic maps · Brute force attack

1 Introduction

The increasing demands of numerous online communication systems and web applications made it possible to access digital information within no time. The existing era is the technologically advanced age of digital information. The transmission of digital information through insecure lines of communication is at its peak. There has always been an increasing demand of information security mechanism for different organizations in order to protect their secret information from being hacked or stolen by an unfair means. Today, digital information can be transmitted via different communication channels which surely adds easiness in our daily lives. This easiness also added number of serious threats due to advancement in cyber threat intelligence. Recently, we have seen several cyber threads in which ransomware is one of the most powerful cyber-attacks which infected several governments and private organization online systems. Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Cryptovirology is a one of the growing fields of further investigations in order to use cryptographic algorithm to construct a powerful malicious viruses and cyber-attacks. This area of research was conceived with the perception that asymmetric key cryptosystems can be utilized to breakdown the balance between what an antivirus examiner perceives in regard to malware and what the assailant sees. The antivirus examiner sees an open key contained in the malware through the invader grasps people in public key enclosed in the software such as viruses or Trojans designed to cause damage or disruption to a computer system and also the relating secret key (outside the Trojans) since the assailant made the key combination for the assault. The public key permits the malware to accomplish trapdoor one-route tasks on the infected computer system that just the invader can fix. There is a need of robust encryption algorithm not only limited to digital information in order to secure the confidentiality of information but also multilayer security systems for online available servers. In recent paradigms, digital information is one of the most important sources in different online web applications

✉ Majid Khan
majid.khan@mail.ist.edu.pk

[1] Department of Applied Mathematics and Statistics, Institute of Space Technology, Islamabad, Pakistan

[2] Cyber and Information Security Lab (CISL), Institute of Space Technology, Islamabad, Pakistan

[3] Department of Electrical Engineering, Institute of Space Technology, Islamabad, Pakistan

[4] King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia

where information travels in different form of digital medium such as email, electronic e-news, online banking and social media. The most relevant digital information mediums are images, audios and videos, etc. The security of digital mediums is one of the vital problems even in the digitally advanced era of science and technology. Now to address this issue of security of digital medium, several encryption techniques were devised in order to provide the secrecy to multimedia contents [1–23].

In modern age, transmission of digital data goes over various sorts of insecure network without treatment with special types of techniques to ensure secure communication. These digital data contain high amount of confidential information which need special types of techniques and algorithms to make it secure over insecure line of communication. Information security is demand of present day which includes three crux principles which are confidentiality integrity and availability commonly known as CIA triad. The expertise of data converting from plain text to intelligible form for security against any type of external illegal acquiring, modification, changing, illegitimate access for the personal benefit or gain while transmitting it over secure or insecure network is known as cryptography [24–27]. It is practice of secure communication against third parties which is known as advertisers [28]. Cryptography demand is increasing constantly in different fields for instance mathematics, engineering, and physics along with different civil as well military sectors. The encryption standards are already developed long ago like advanced encryption standard (AES), data encryption standard (DES), triple data encryption standard (TEDS), Blowfish and RC5 vice versa. Encrypted data will be particular for key which was used with plain text for symmetric key encryption [29]. The strength or robustness of data depends upon two things, i.e., the algorithm designed or proposed, and key used for encryption.

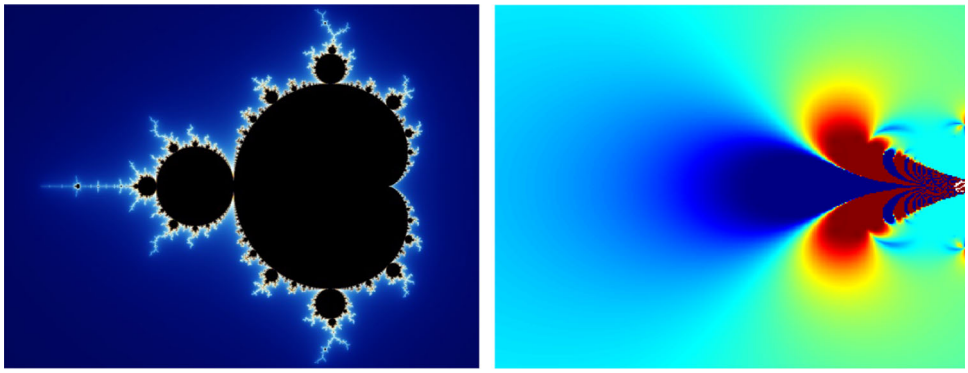
Recently, chaos plays an important role due to its diverse applicability and similar characteristic related to cryptography. In 1989, Robert Mathews for the very first time investigated secure transmission through chaotic behavior and properties of cryptography [30]. The introduction of chaos theory in cryptography attracted many individual's students and researchers. The enduring concerns about their security and utilizing speed continue to limit its implementation [31–35]. Chaotic systems are highly random in nature and exhibit certain type of properties which make it suitable to use it for security intendment. Conceding that the initial conditions are known to bystander, the cryptosystem is known as deterministic with respect to bystander and shows highly unpredictable characteristics including topology mixing, randomness, sensitive to initial condition, ergodicity, vice versa [36]. These unpredictable characteristics are eminently auspicious for constructing and designing secure cryptosystem [37, 38]. Chaotic iterative maps and dynamical systems are in fashion in order to add confusion and diffusion capability which are the most vital possessions while designing any strong cryptosystems [39–57]. The idea of confusion is fundamentally achieved through substitution, and diffusion can be achieved by utilizing permutation. Shannon's [58] highlights his ideas of how to create a secure cipher, including the properties of confusion and diffusion. Confusion refers to how each single bit of a ciphertext should depend on multiple bits of a key. Diffusion refers to how a change in a single bit of plaintext should on average change half the bits of the resulting ciphertext, and vice versa. This effect is also known as the avalanche effect. From last two decades, several image encryption schemes were designed so far which ensure the substitution–permutation (SP) network characteristics. In this article, our principle aim is to design an efficient image encryption scheme based on chaotic fractals, Fibonacci series and discrete map.

The rest of the paper is organized as follows. In Sect. 2, we have discussed brief introduction about fractals which will be quite useful while developing our proposed image encryption scheme. Section 3 is preceded with proposed technique, while Sect. 4 is about security performance test analysis. Finally in Sect. 5, we have added concluding section (Fig. 1).

2 Fractals types and geometry

Fractals are set of collection of sequence of numbers over large number of terms in complex domain [13]. These are reiterative and repetitive geometry shapes in image that have identical degree of irregularity at all proportions and behave similarly under repeated iteration [39]. Images of Mandelbrot fractal [12] and Julia fractals are shown in Fig. 2a, b, respectively. Benoit Mandelbrot (1924–2010) originally scientist of Poland later moved to France introduced Mandelbrot set in 1979 and expended his idea to geometry of nature. Mandelbrot worked on fractals, chaos theory and Mandelbrot set [40]. In 1979, Benoit Mandelbrot after Julia set of fractals studied complex structure of repetitive structures in one another known as Mandelbrot set of fractals [39]. Fractals are based on property of self-similarity and are identical or similar to itself [41]. The Mandelbrot set lies in complex plane 'c' for which orbit 0 under iteration of complex polynomial quadratic equation is $Z_{n+1} = Z_n^2 + c$ which remains bounded. The choice of collection of fractals depends upon minutiae and colors. It can be obtained through IFS systems because of the absence of complication in it. The two main characteristics of fractals are that they have infinite details at single point

Fig. 1 Basic schematic chart of image encryption



(a) **(b)**

Fig. 2 Fractal images **a** Mandelbrot set of fractals for no zoom state, **b** Julia set of fractals

and are self-repetitive structure [42]. Fractals have similar properties related to chaotic nature of sensitiveness which leads to secure cryptosystem; with the combination of these two techniques, it has quite promising output related to secure enciphered system against some external attack to break down cryptosystem [40, 43]. The generation of keys depends upon complex equation and intruder always tries to find out combination of keys to find exact key to decrypt it which is known as Brute force attack; though if any system having large key space, it leads to number of guesses and will lead to more complexity if the number of guesses increases due to larger key space of respective technique. Fractals have large key space as compared to other techniques; so due to these characteristics, intruder will try every combination of keys and will lead to more complex system. Fractals geometry is repeated pattern of images; each image is divided into subsections known as repetition of images inside images or simply copy of images inside one another. Fractal image is identic in nature when zoomed at any point of fractal image [44]. It is iterated for finite number of times in mathematical equation for the generation of fractals. Julia set of fractal starts with nonzero and iterates for fixed '*C*,' while Mandelbrot starts from zero with varying '*C*' factor in equation. The complex plane is always two-dimensional plane having two axes one vertically known as imaginary axis, while the one lies horizontal known as real axis. It is demonstrated as in complex plane with sequence is characterize by the iteration so that infinite sequence $C_0, C_1, \ldots, C_n$ remains bounded. For $C_0 = C_0$ and $n = 0, 1, 2, 3, \ldots$.

$$C_{n+1} = C_n^2 + C_0 \tag{1}$$

The equation for Mandelbrot can be defined in complex plane as:

$$Z_{n+1} = Z_n^2 + c \tag{2}$$

3 Proposed technique for cryptosystem

Main intendment is providing secure and robust algorithm with minimum vulnerability. In this communication, we proceeded with fractals, Fibonacci with chaotic maps and investigated its results with current techniques which showed incomparable security for communication.

3.1 Kaplan–Yorke chaotic map

Chaotic maps have some desirable properties suitable for designing secure and robust cryptosystem. Kaplan–Yorke is a chaotic two-dimensional discrete dynamical map which exhibits chaotic behavior that helps in exceptional security for proposed algorithm [45–47]. The Kaplan–Yorke map takes a point (x_n, y_n) and gives new points in two-dimensional plane; it can be expressed as follows:

$$x_{n+1} = 2x_n (\text{mod} 1), \tag{3}$$

$$y_{n+1} = \alpha y_n + \cos(4\pi x_n). \tag{4}$$

where 'mod' is the modulo operator, and this two-dimensional map depends upon constant α.

3.2 Fibonacci series

Leonardo Fibonacci mathematical genius born in Pisa, Italy, had vast study on computational systems. He wrote several mathematical topics though the mathematical genius is remembering for introducing of mathematical Fibonacci sequence. Fibonacci series have many applications in different fields of mathematics, engineering, vice versa [48, 49]. Fibonacci series in mathematics are sequence of integers in which the assumed integer is the sum of previous two integers, depending on your chosen term from the series (Fig. 3). It can be defined as reoccurrence or repetitiveness relation

$$\mathrm{FN}_n = \mathrm{FN}_{n-1} + \mathrm{FN}_{n-2}, \tag{5}$$

where initial conditions are as follows:

$$F_1 = 1, \quad F_2 = 1$$
$$F_0 = 0, \quad F_1 = 1$$

3.3 Procedure involved in accomplishing proposed algorithm

1. Plain image P entitle Lena of size 512 × 512 with JPG file extension is taken.
2. Plain test image is split into owned three layers (RGB).
3. Generation of Mandelbrot fractal image in no zoom state with dimension of 512 × 512.
4. Extraction of real values from the complex domain of generated fractal in step 3
5. Generation of Fibonacci series having same length of 512 × 512.
6. Multiplication of real values of Mandelbrot fractal with the output values of series generated by Fibonacci series.
7. Generation of chaotic Kaplan–Yorke map having same length of dimension 512 × 512.
8. Bitwise XOR operation of output values of Fibonacci series with preceding values of chaotic Kaplan–Yorke map
9. Finalization is with bitwise XOR operation of previous step 7 with channels generated in step 2 (Fig. 4).

3.4 Software and system specification

In this section, we performed number of tests using registered MATLAB 2017(a) with operating system of windows 10 64-bit architecture. The specifications included for simulation of results are 8 GB ram, 1.9 GHz processor, intel core™ i3 third-generation central processing unit.

4 Performance and security analysis

We investigated multiple tests over proposed algorithm and simulated using MATLAB as a testing environment for certain types of test images, while colored Lena 512 × 512 is taken as standard image for this article.

4.1 Histogram analysis

Histogram is representation of values of pixels graphically. Histogram shows intensity value of each pixel making full of histogram. The number of possible intensity values depends upon image taken with bits. Uniform distribution of values of pixels measure exceptional security against brute force and alternative methods for cracking secure confidential information, while unnecessary jerky or non-uniform pixels values assert insecure information which feel necessity of certain types of secure techniques treatment. We analyzed histogram analysis for different test images with different dimensions. We have investigated different gray channels of test color images at two distinct points, i.e., histogram pixel values after using Mandelbrot and Fibonacci series and pixels values after whole process including chaotic map, addition of chaotic properties of randomness with Mandelbrot or Julia Fractal and Fibonacci series have much exceptional output. The pixels are distributed from 0 to 255 in horizontal direction (Figs. 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26). In Figs. 5b and 7a–c, there are number of slopes of pixels as compared to 512 × 512 of Lena in Fig. 9a–c, and 512 × 512 × 3 of Lena in Fig. 10b, the pixels gone to smooth one level means the security level is much high and information at each pixel is difficult to be taken out. In Figs. 11, 15, 19, 23 part 'b,' there are number of abruptness and ramp of pixels for different test images;

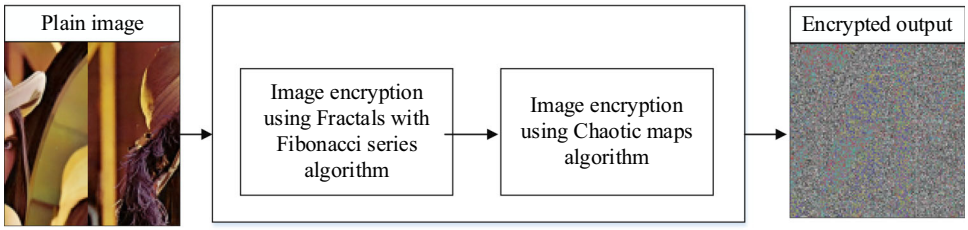


Fig. 3 Detailed schematic chart of image encryption algorithm

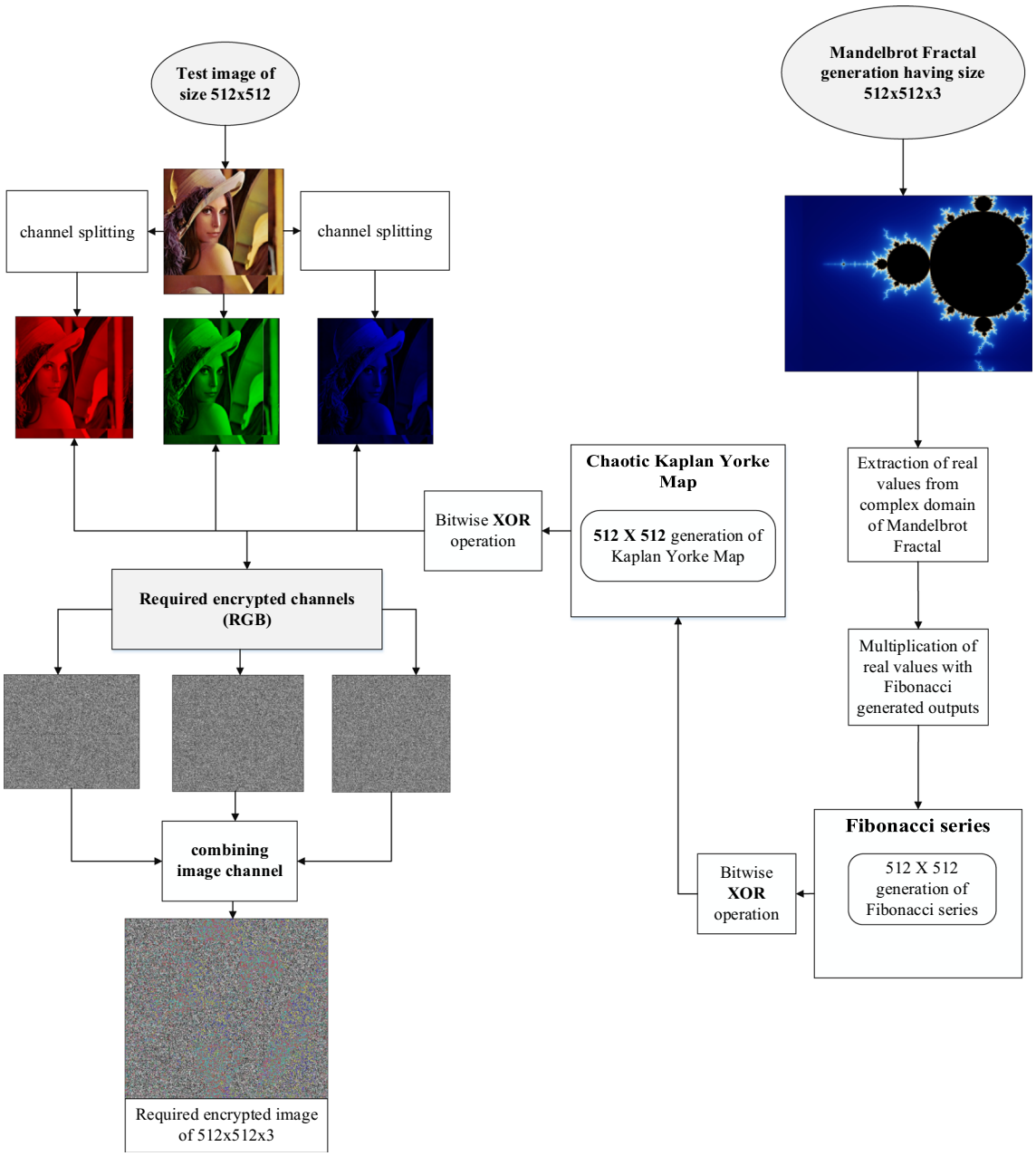


Fig. 4 Flowchart for the proposed algorithm

this means information is vulnerable to be attacked. In our proposed algorithm with other test images for 512 × 512 × 3 and 512 × 512 in Figs. 14, 18, 22, 26 part 'b' and Figs. 13, 17, 21, 25 while examining of pixels values, the information of each pixel shows high resemblance to one another. The intruder will be unable to take out exact information.

4.2 Correlation coefficient analysis

Correlation coefficient is a momentous method for the examination of security of data. In correlation coefficient, we investigate pixel similarities between plain image and encrypted image horizontally, vertically and diagonally. The range of correlation coefficient always spread over extreme values of − 1 and 1. The digit 0 show maximum uncorrelated pixels with respect to nearby pixels, while digit 1 shows maximum correlation of pixels in neighborhood. The mathematical expression for correlation coefficient is given as:

$$r = \frac{\sigma_{xy}}{\sigma_x \sigma_y}, \tag{6}$$

where σ_{XY} is covariance, σ_X and σ_Y are standard deviations of random variables X and Y, respectively. We assumed

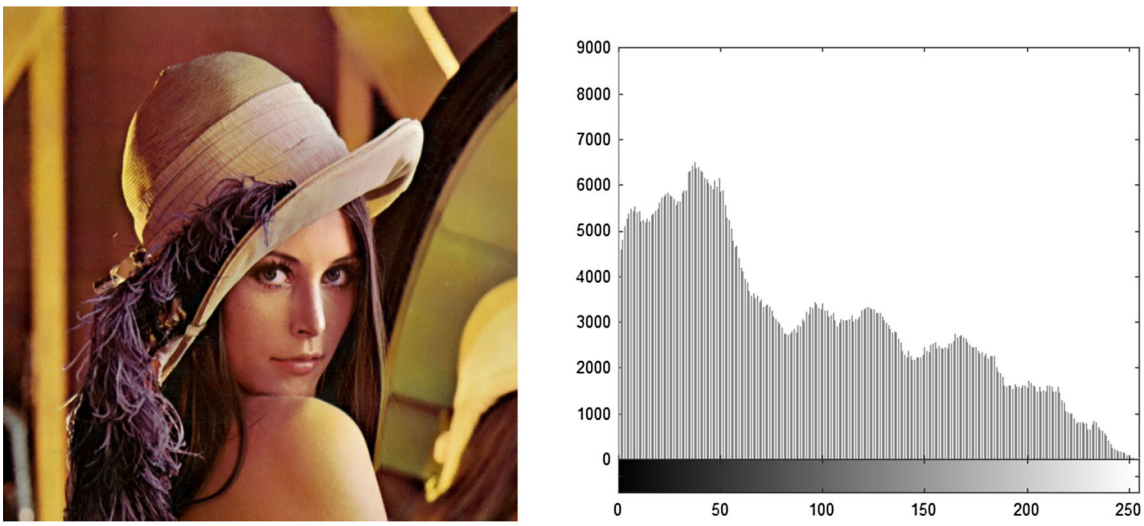


Fig. 5 **a** Plain image of Lena length 512 × 512 × 3; **b** plain image histogram of Lena length 512 × 512 × 3

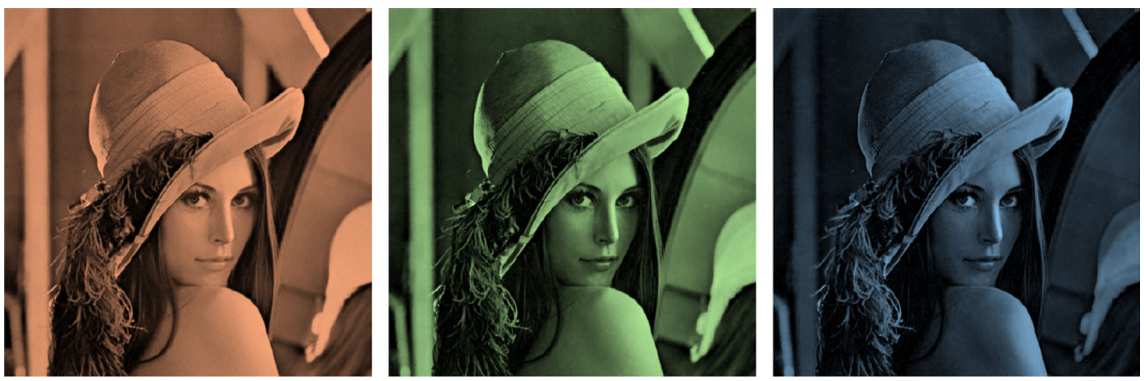


Fig. 6 **a** Plain red layer of Lena size 512 × 512; **b** plain green layer of Lena 256 × 256; **c** plain blue layer of Lena 256 × 256 (color figure online)

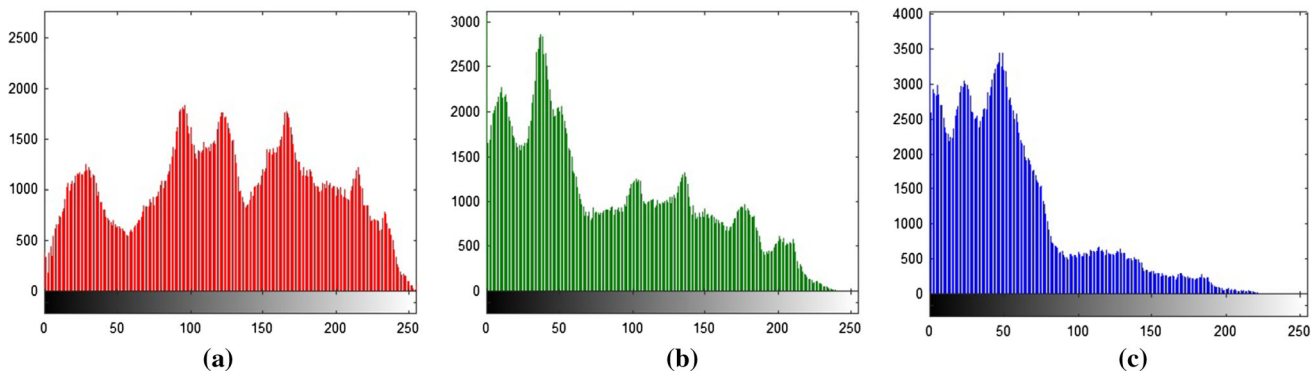


Fig. 7 **a** Plain red layer histogram of Lena size 512 × 512; **b** plain green layer histogram of Lena size 512 × 512; **c** plain blue layer histogram of Lena size 512 × 512 (color figure online)

two cases of correlation. First case is examination for combined channels image, i.e., 512 × 512 × 3 for *R*, *G* and *B* combined in three different directions, while in other cases, individual channels are examined for three directions, respectively.

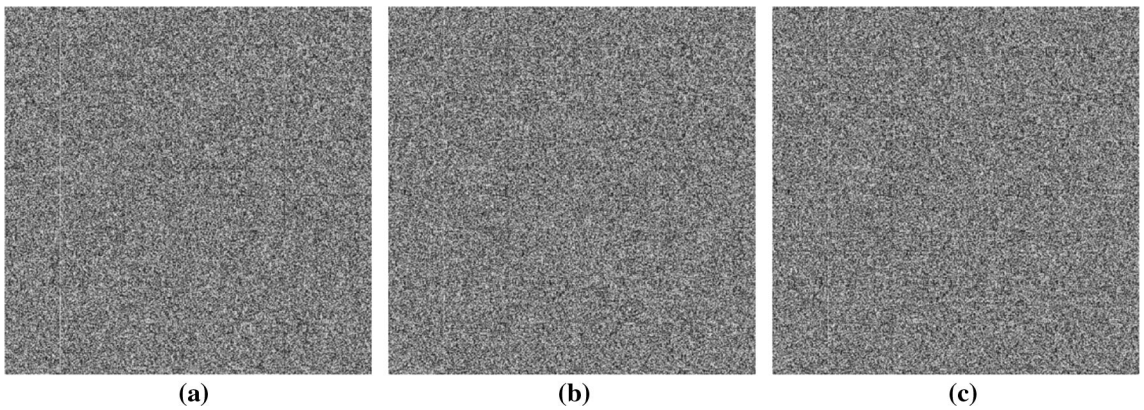


Fig. 8 **a** Enciphered red layer of Lena size 512 × 512; **b** enciphered green layer of Lena size 512 × 512; **c** enciphered blue layer of Lena size 512 × 512

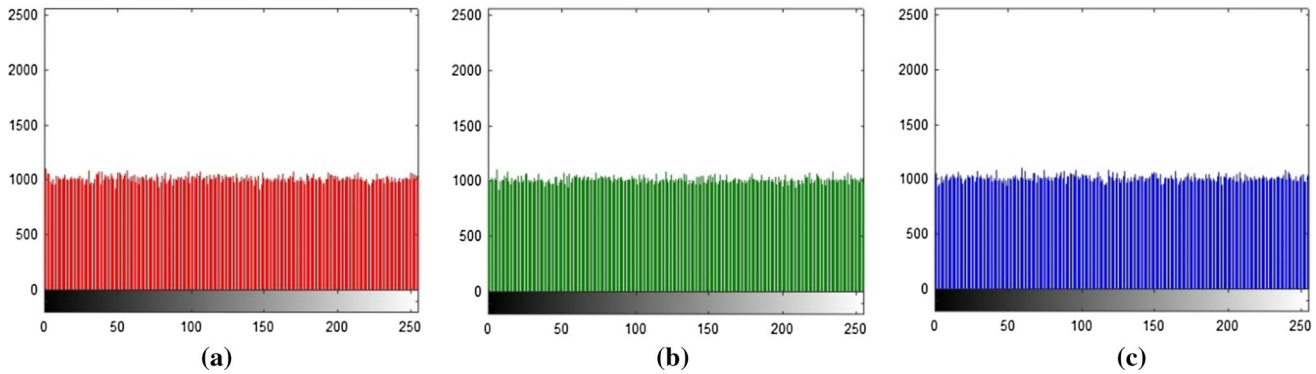


Fig. 9 **a** Enciphered red layer histogram size 512 × 512; **b** enciphered green layer histogram size 512 × 512; **c** enciphered blue layer histogram size 512 × 512 (color figure online)

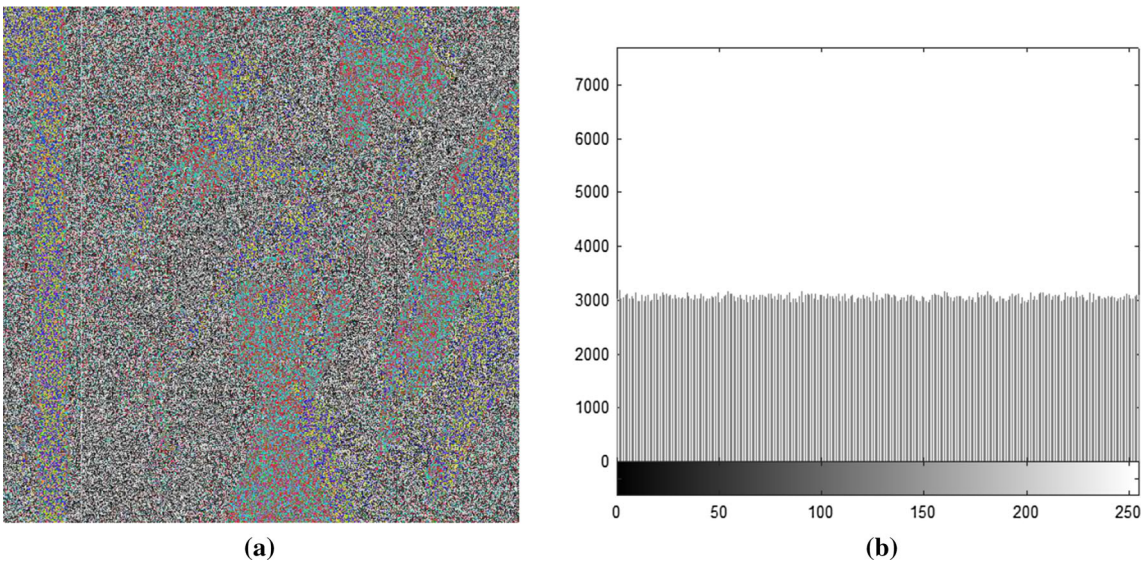


Fig. 10 **a** Combined layers enciphered test image of size 512 × 512 × 3; **b** combined layers encrypted test image of size 512 × 512 × 3 histogram

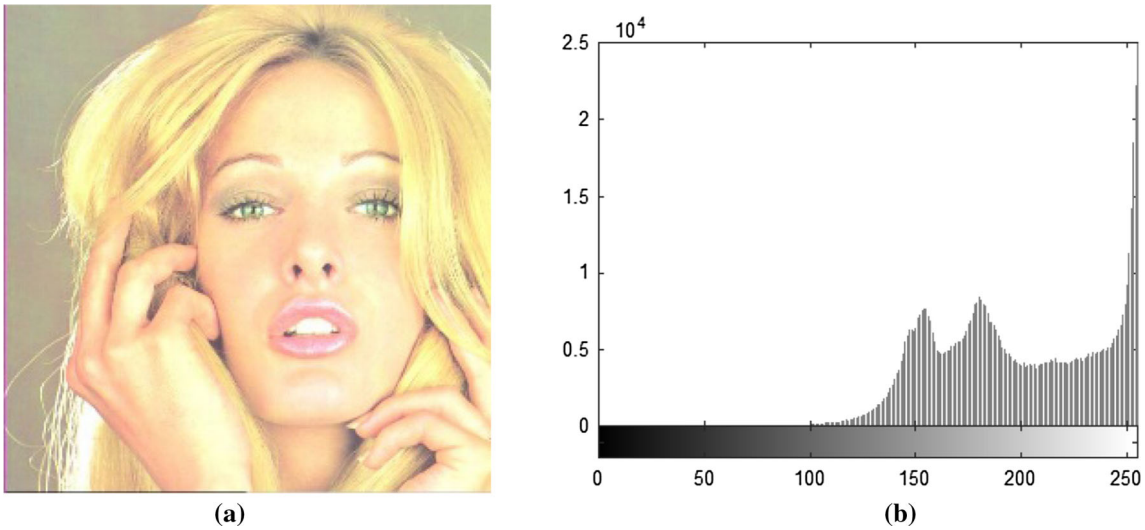


Fig. 11 **a** Plain Tiffany having size 512 × 512 × 3; **b** plain Tiffany histogram having size 512 × 512 × 3

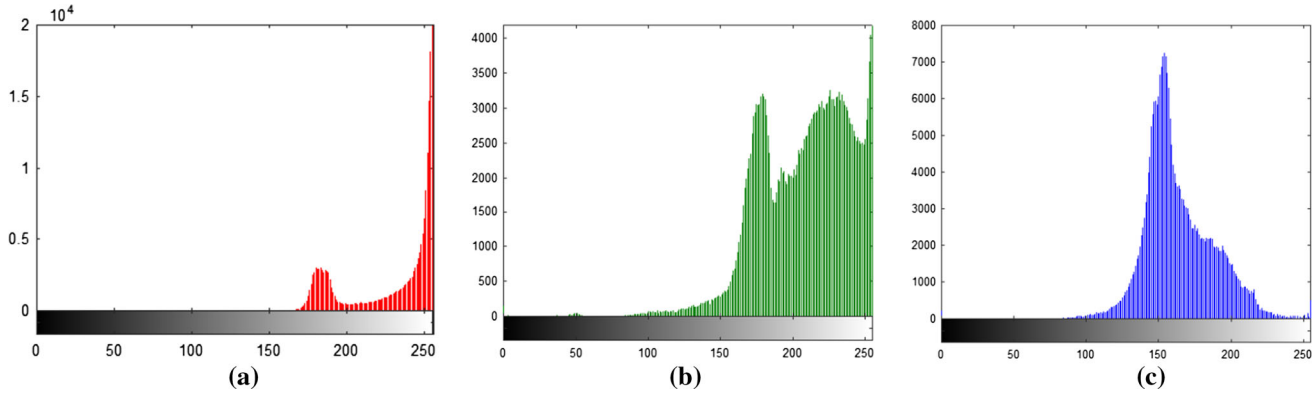


Fig. 12 **a** Plain Tiffany red layer histogram of size 512 × 512; **b** plain Tiffany image green layer histogram of size 512 × 512; **c** plain Tiffany image blue layer histogram of size 512 × 512 (color figure online)

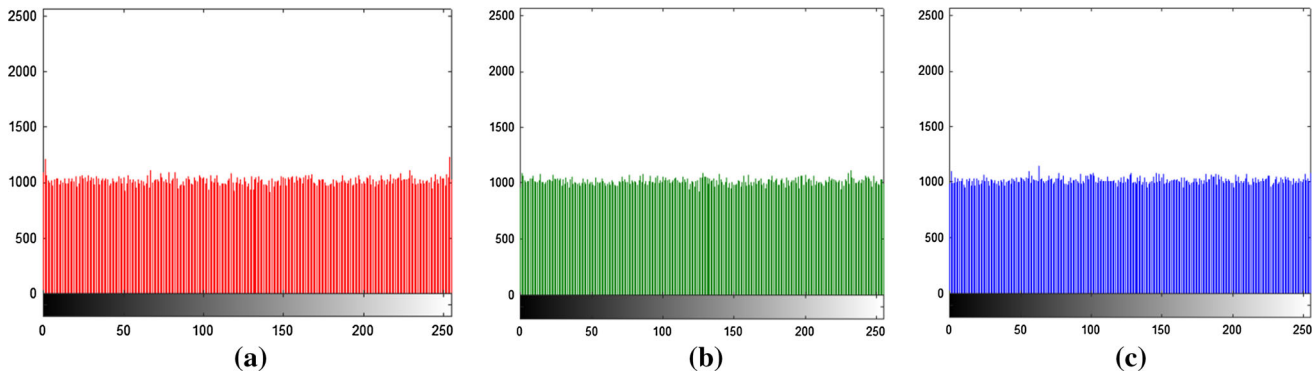


Fig. 13 **a** Enciphered Tiffany red layer histogram of size 512 × 512; **b** enciphered Tiffany green layer histogram of size 512 × 512; **c** enciphered Tiffany blue layer histogram of size 512 × 512 (color figure online)

4.2.1 Image correlation coefficient

We measured correlation of adjacent pixels for 512 × 512 × 3 and 256 × 256 × 3 size images in Table 1. The average value for all ternary direction in Table 1 is 0.9751 for plain image of Lena, and average cipher for all three directions is 0.0005 which shows much better robustness against differential attacks because the

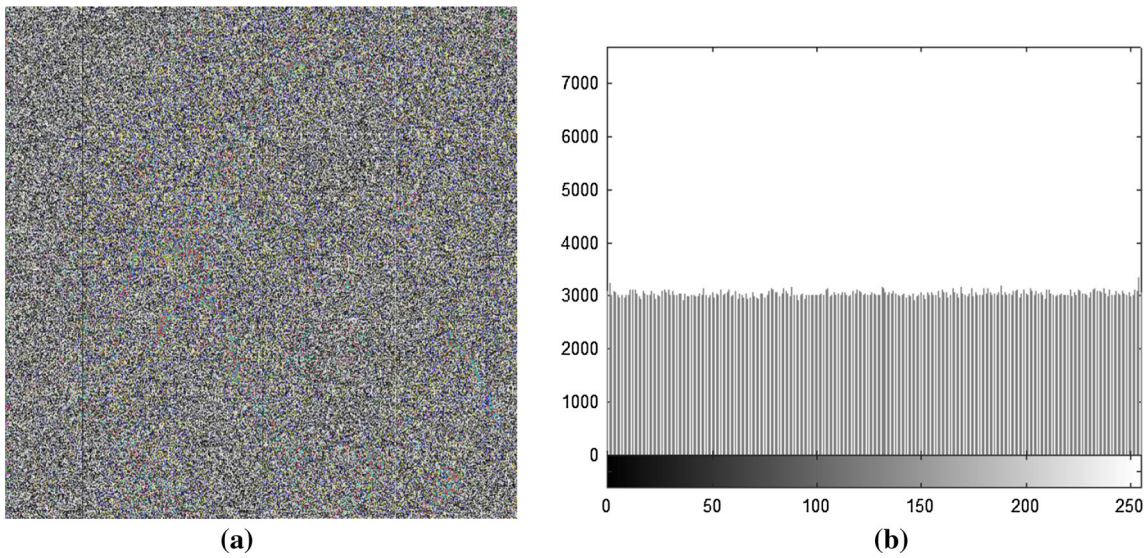


Fig. 14 **a** Combined layers enciphered Tiffany of size 512 × 512 × 3; **b** combined layers enciphered Tiffany histogram of size 512 × 512 × 3

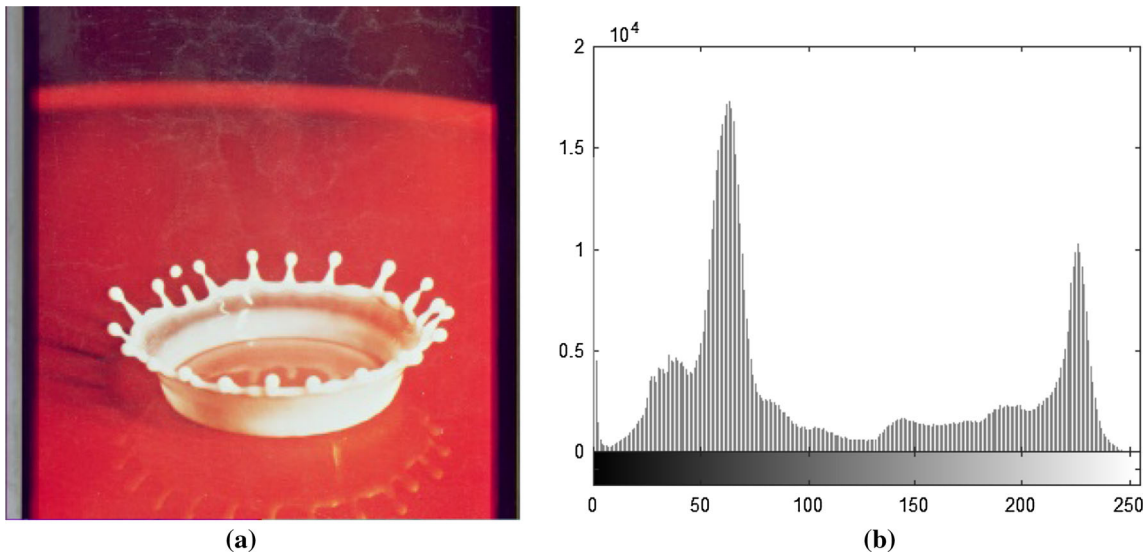


Fig. 15 **a** Plain splash image of size 512 × 512 × 3; **b** plain splash image histogram of size 512 × 512 × 3

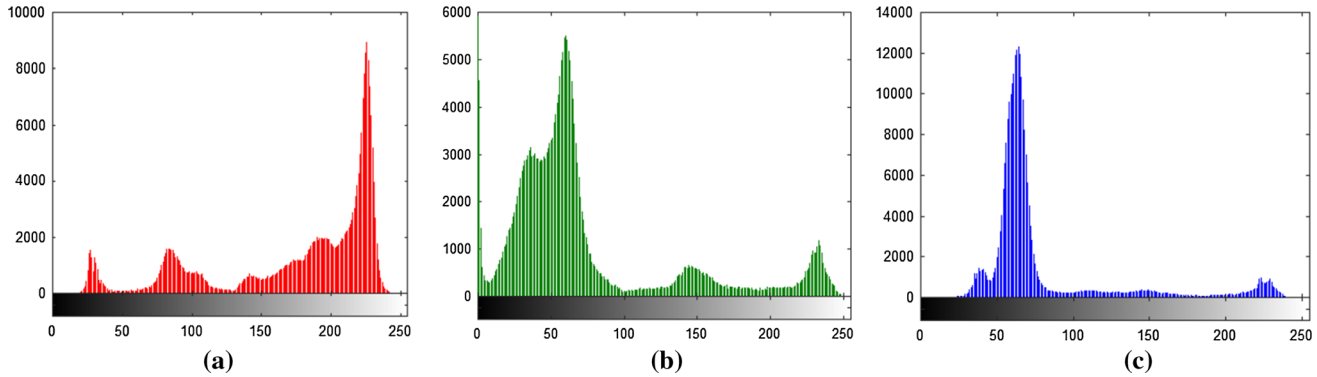


Fig. 16 **a** Plain splash red layer histogram of size 512 × 512; **b** plain splash green layer histogram of size 512 × 512; **c** plain splash blue layer histogram of size 512 × 512 (color figure online)

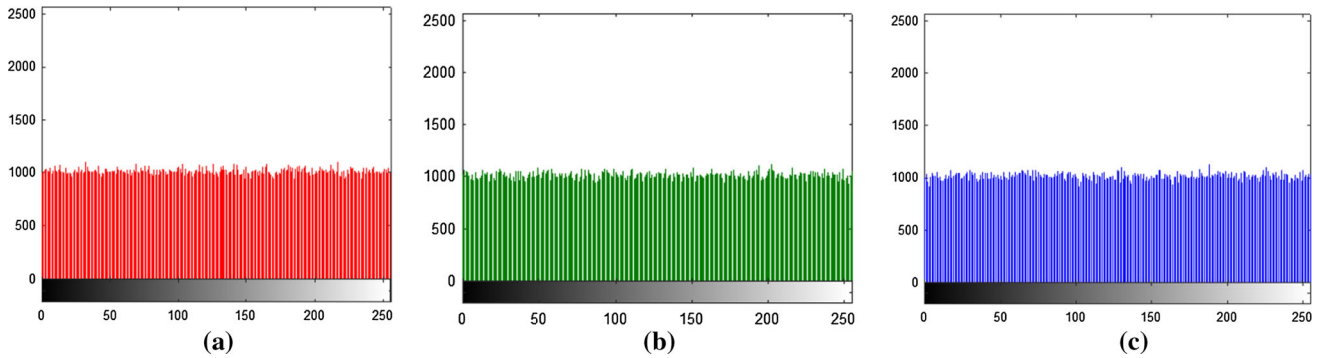


Fig. 17 **a** Enciphered splash red layer histogram of size 512 × 512; **b** enciphered splash green layer histogram of size 512 × 512; **c** enciphered splash blue layer histogram of size 512 × 512 (color figure online)

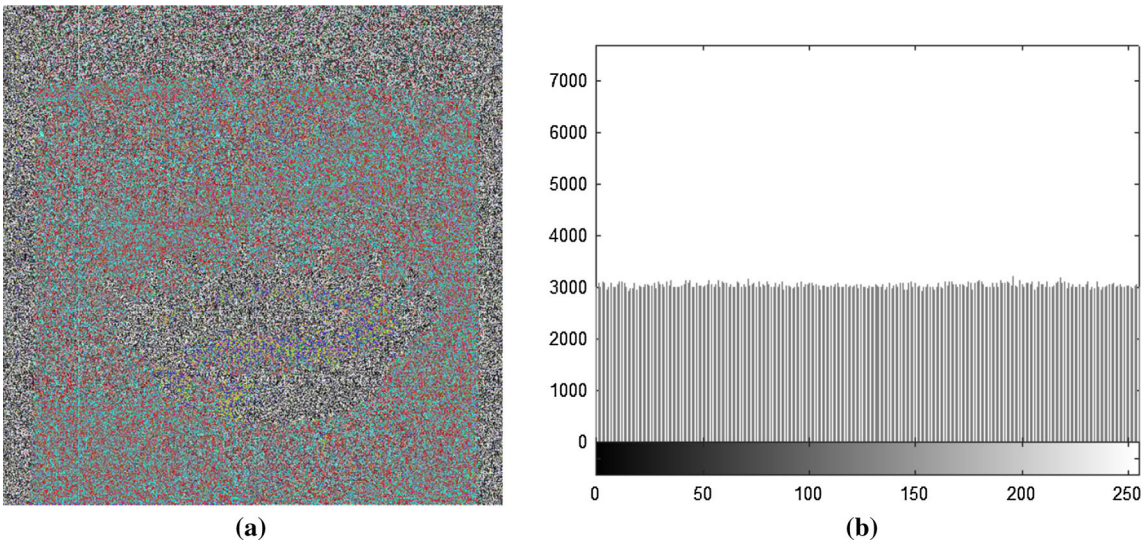


Fig. 18 **a** Combined layers enciphered splash having size 512 × 512 × 3; **b** combined layers enciphered splash histogram having size 512 × 512 × 3

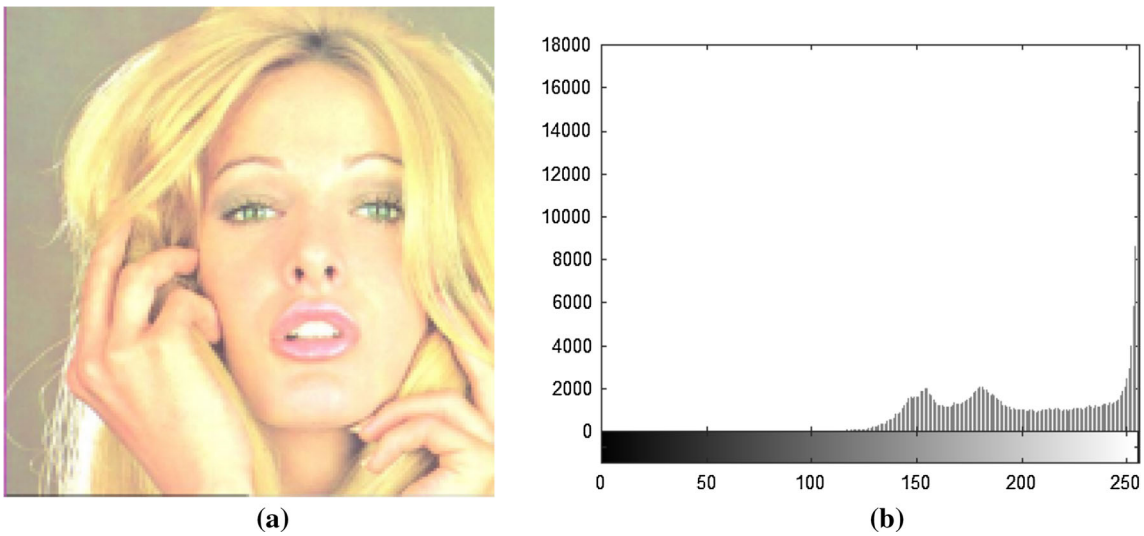


Fig. 19 **a** Plain Tiffany image of size 256 × 256; **b** plain Tiffany histogram 256 × 256

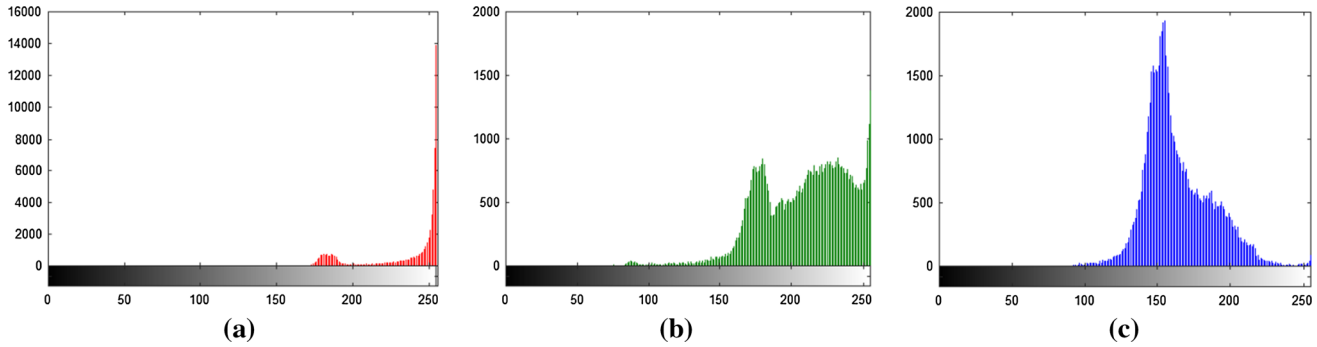


Fig. 20 **a** Plain Tiffany red layer histogram of size 256 × 256; **b** plain Tiffany green layer histogram of size 256 × 256; **c** plain Tiffany blue layer histogram of size 256 × 256 (color figure online)

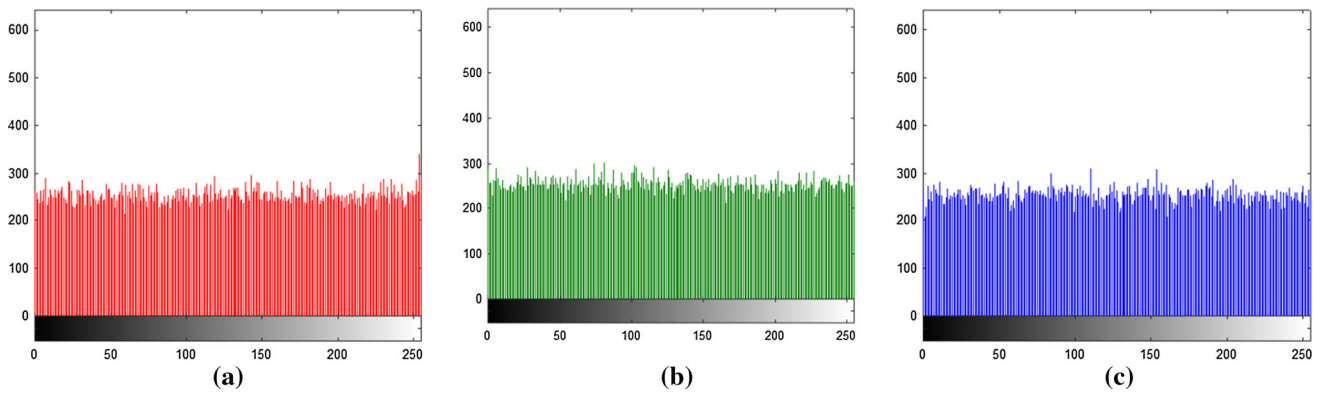


Fig. 21 **a** Encrypted Tiffany red layer histogram of size 256 × 256; **b** encrypted Tiffany green layer histogram of size 256 × 256; **c** encrypted Tiffany blue layer histogram of size 256 × 256 (color figure online)

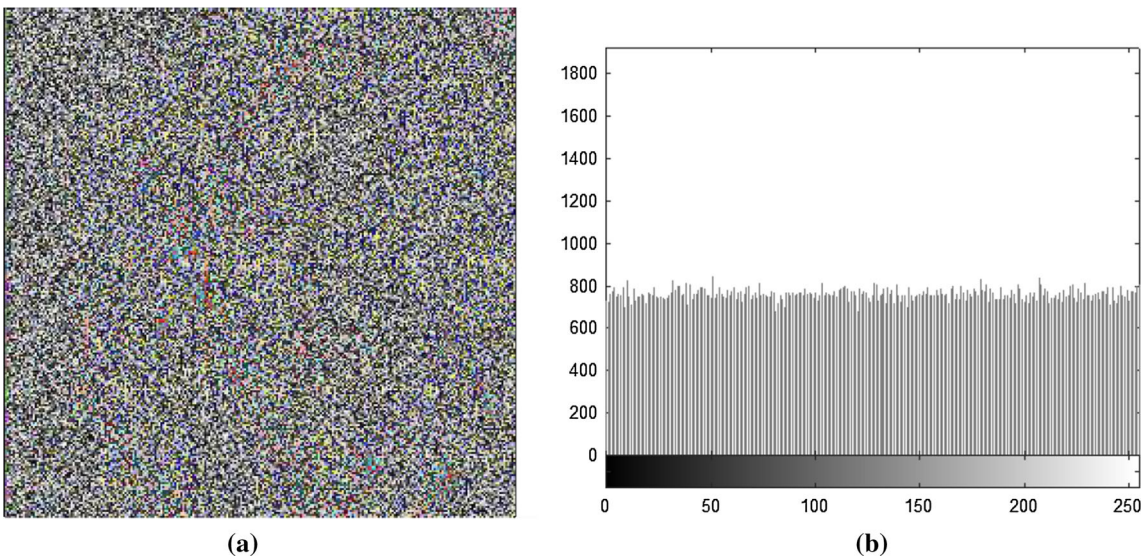


Fig. 22 **a** Combined layers enciphered tiffany having size 256 × 256 × 3; **b** combined layer enciphered tiffany histogram having size 256 × 256 × 3

average value is zero up to three digits after decimal point. In Table 1, plain values of respected test images like Tiffany, Splash, Airplane and additional Tiffany of size 256 × 256 × 3, i.e., with half of size of the previous Tiffany can be seen. The average values for remaining test images are 0.975 which are very close to 1 and show highly vulnerability, while average cipher images at ternary direction are approximately 0.002 which are close to zero

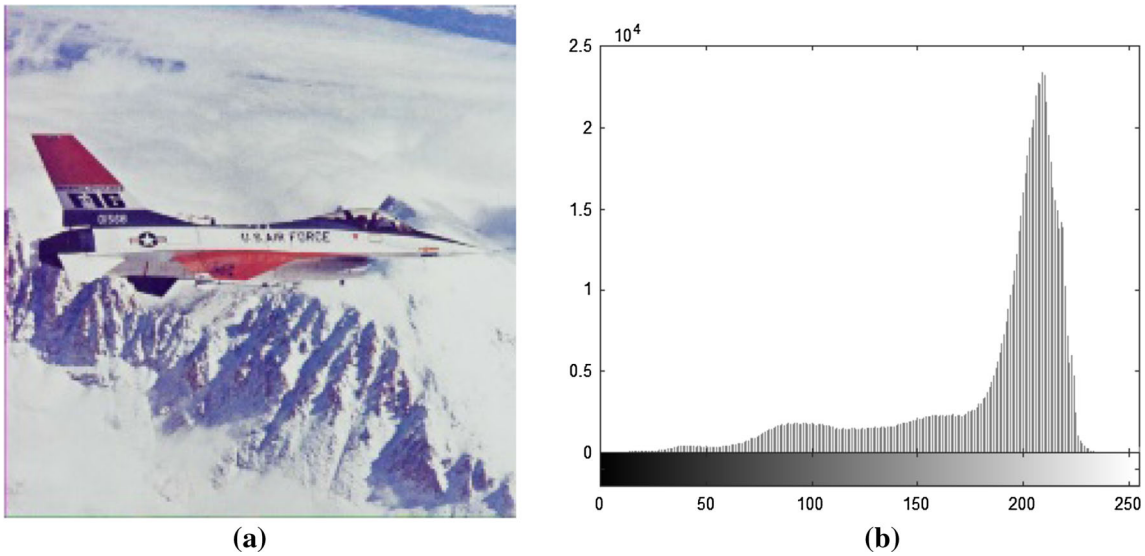


Fig. 23 **a** Plain airplane having size 512 × 512 × 3; **b** plain airplane histogram having size 512 × 512 × 3

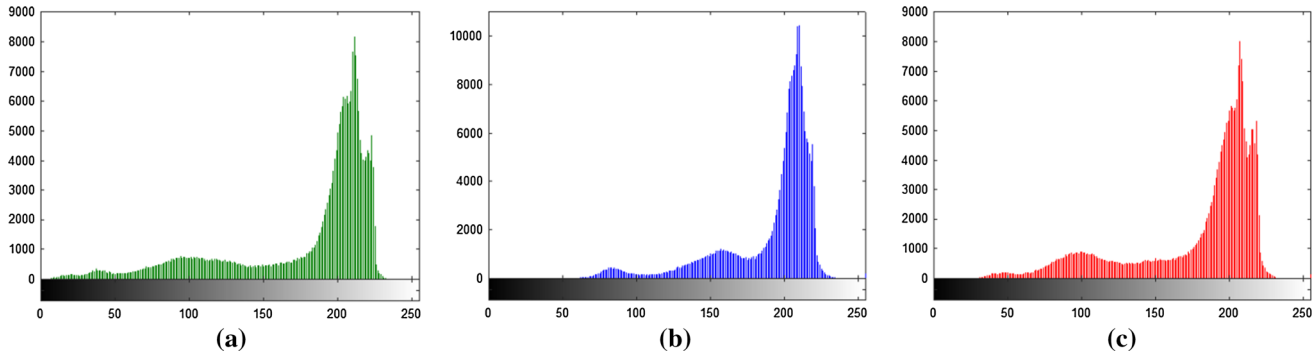


Fig. 24 **a** Plain airplane red layer histogram of size 512 × 512; **b** plain airplane green layer histogram of size 512 × 512; **c** plain airplane blue layer histogram of size 512 × 512 (color figure online)

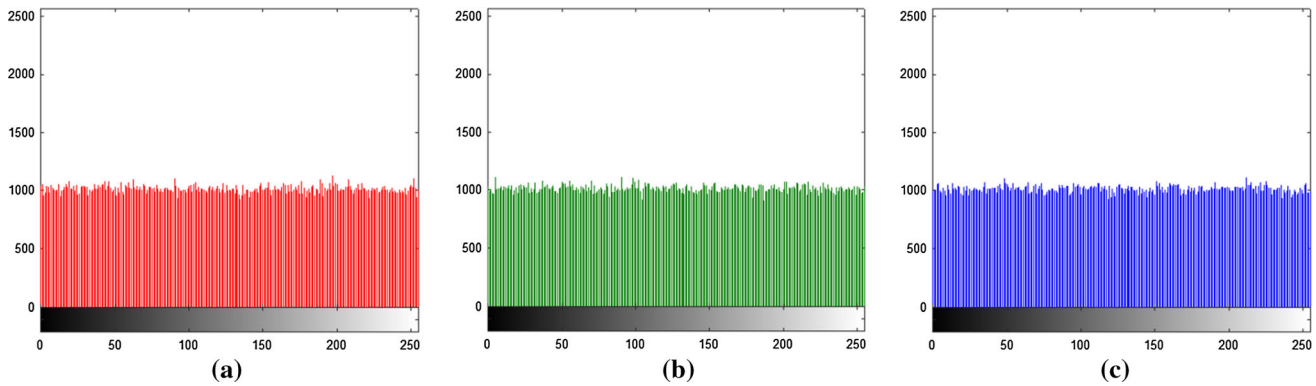


Fig. 25 **a** Enciphered airplane red layer histogram of size 512 × 512; **b** enciphered airplane green layer histogram of size 512 × 512; **c** enciphered airplane blue layer histogram of size 512 × 512 (color figure online)

and show good secure algorithm designed. The comparison of values for plain and enciphered images is shown in Table 2. The proposed average value of encrypted Lena image is calculated approximately to 0.0005 and is compared with the number of preexisting algorithms [50–57] in Table 2. According to [50], the average value for three directions of preexisting algorithm is 0.0045 compared to proposed algorithm value which is 0.0005

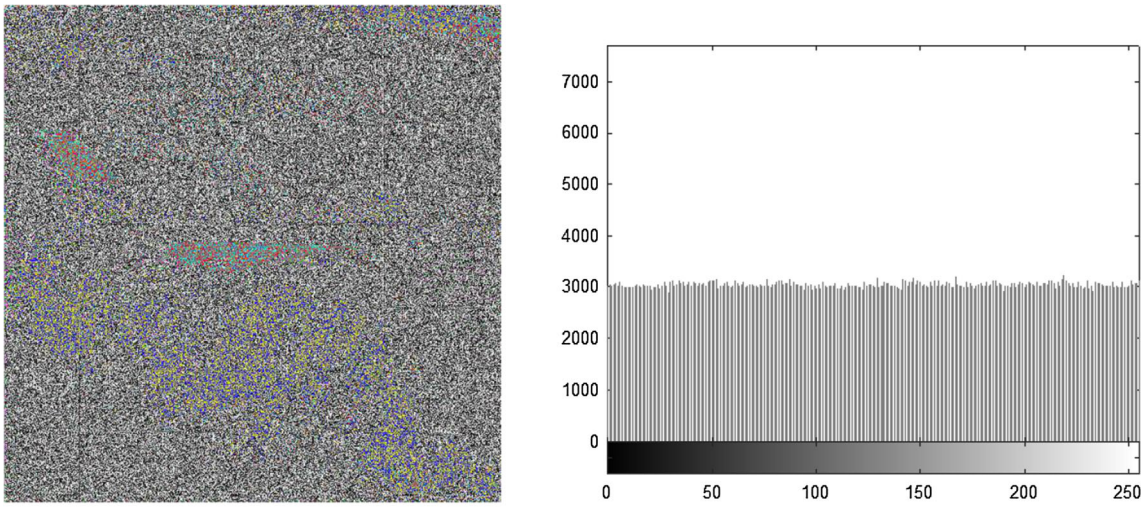


Fig. 26 **a** Enciphered airplane having size 512 × 512 × 3; **b** enciphered airplane histogram having size 512 × 512 × 3

Table 1 Correlation coefficient calculated for different plain and cipher images

	Size	Plain image			Encrypted image		
		Correlation coefficient directions			Correlation coefficient directions		
		HC	DC	VC	HC	DC	VC
Lena	512 × 512	0.9749	0.9639	0.9867	0.0012	0.0007	0.0028
Tiffany	512 × 512	0.9439	0.8992	0.9469	0.0007	− 0.0022	0.0051
Splash	512 × 512	0.9842	0.9775	0.9917	0.0048	− 0.0083	0.0052
Airplane	512 × 512	0.9670	0.9373	0.9646	0.0027	− 0.1001	0.0016
Tiffany	256 × 256	0.9359	0.8887	0.9430	− 0.0033	− 0.0020	0.0031

HC horizontally correlated, *DC* diagonally correlated, *VC* vertically correlated

Table 2 Comparison of correlation coefficient with preexisting algorithms

	Size	Correlation coefficient directions		
		HC	VC	DC
Plain image	512 × 512	0.9749	0.9639	0.9867
Proposed	512 × 512	0.0012	0.0007	0.0028
Ref. [50]	512 × 512	0.0075	0.0012	0.0049
Ref. [51]	512 × 512	0.0005	0.0008	0.0011
Ref. [52]	512 × 512	0.0117	0.0026	0.0010
Ref. [53]	512 × 512	0.0043	0.0054	0.0072
Ref. [54]	512 × 512	0.0108	0.01811	0.0061
Ref. [55]	512 × 512	0.0032	0.0042	0.0018
Ref. [56]	512 × 512	0.0204	-0.0174	0.0231
Ref. [57]	512 × 512	0.0053	-0.0027	0.0016

HC horizontally correlated, *DC* diagonally correlated, *VC* vertically correlated

give evidence of exceedingly robustness of designed system.

4.2.2 Channel-wise image correlation

In this case, we examined correlation of adjacent pixels for three different directions, i.e., horizontal, diagonal and vertical for 512 × 512 and 256 × 256 channel-wise dimension images and compared values with layer-wise plain and encrypted images for different images and are given in Table 3. We examined values for five test images with all three layers of colored images including four 512 × 512 dimension images with one Tiffany for 256 × 256 image. The average value in Table 3 for plain Lena for red layer is approximately 0.9782 with cipher average value of − 0.0014 which is the evidence of good encryption (Figs. 27, 28, 29, 30, 31, 32, 33, 34).

4.3 Information entropy test analysis

Entropy analysis is used to evaluate values of gray-scale layers of various images. It is always important to find out randomness and robustness for proposed secure cryptosystem. The larger the value of entropy, the more

Table 3 Correlation coefficient between plain and cipher images

Image	Channels	Size	Plain image			Encrypted image		
			Correlation coefficient directions			Correlation coefficient directions		
			HC	DC	VC	HC	DC	VC
Lena	*R-C*	512 × 512	0.9781	0.9676	0.9891	− 0.0015	0.0013	− 0.0040
	G-C		0.9779	0.9675	0.9889	− 0.0037	− 0.0013	− 0.0037
	B-C		0.9650	0.9496	0.9809	− 0.0041	− 0.0011	− 0.0032
Splash	*R-C*	512 × 512	0.9926	0.9879	0.9942	0.0017	− 0.0050	0.0029
	G-C		0.9827	0.9729	0.9888	0.0019	− 0.0038	0.0045
	B-C		0.9832	0.9646	0.9795	0.0017	− 0.0017	0.0027
Tiffany	*R-C*	512 × 512	0.9537	0.9140	0.9519	− 0.0009	− 0.0041	0.0063
	G-C		0.9481	0.9098	0.9553	0.0009	− 0.0024	0.0044
	B-C		0.9236	0.8709	0.9328	0.0021	− 0.0009	0.0024
Tiffany	*R-C*	256 × 256	0.9528	0.9128	0.9500	− 0.0027	0.0006	0.0031
	G-C		0.9295	0.8855	0.9489	− 0.0040	− 0.0039	0.0035
	B-C		0.9251	0.8706	0.9297	0.0018	0.0024	0.0024
Airplane	*R-C*	512 × 512	0.9654	0.9329	0.9619	0.0018	− 0.0013	0.0005
	G-C		0.9702	0.9445	0.9695	0.0031	− 0.0021	0.0017
	B-C		0.9476	0.8979	0.9383	0.0031	− 0.0039	0.0030

HC horizontally correlated, *DC* diagonally correlated, *VC* vertically correlated, *R-C* red channel, *G-C* green channel, *B-C* blue channel

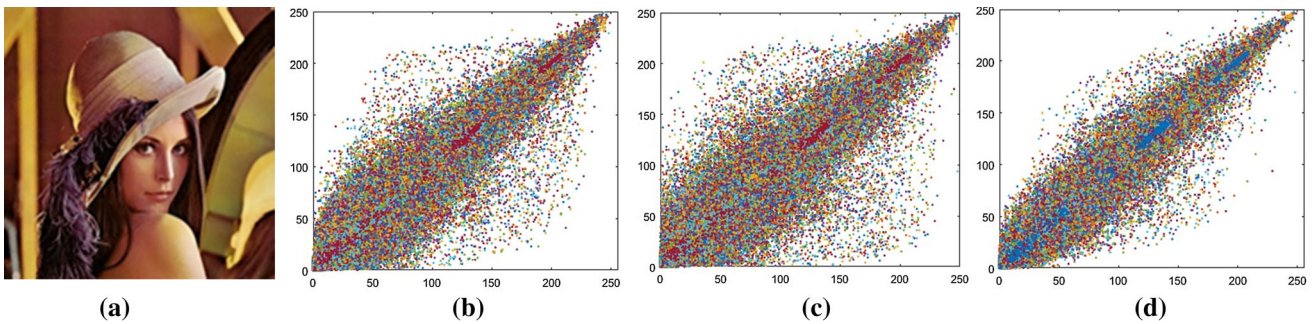


Fig. 27 **a** Plain test image having length 512 × 512 × 3; **b** horizontally correlated plain image; **c** diagonally correlated test image; **d** vertically correlated plain image

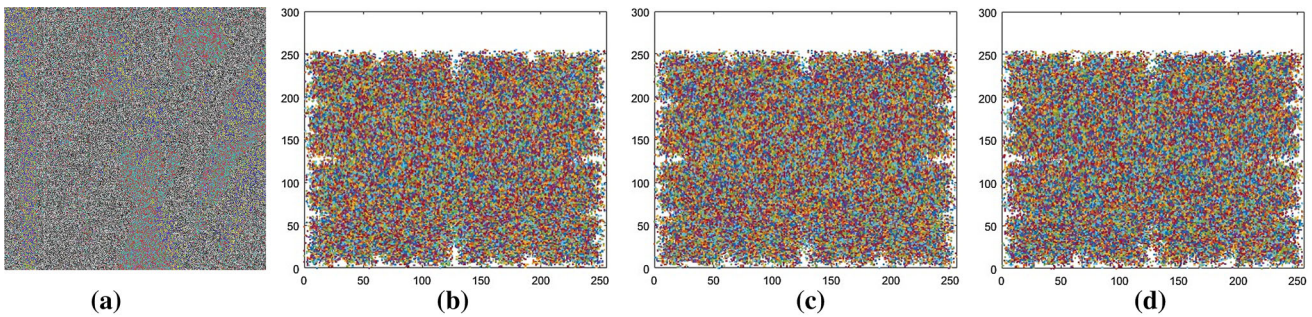


Fig. 28 **a** Enciphered test image having length 512 × 512 × 3; **b** horizontally correlated enciphered test image; **c** diagonally correlated of enciphered test image; **d** vertically correlated enciphered test image

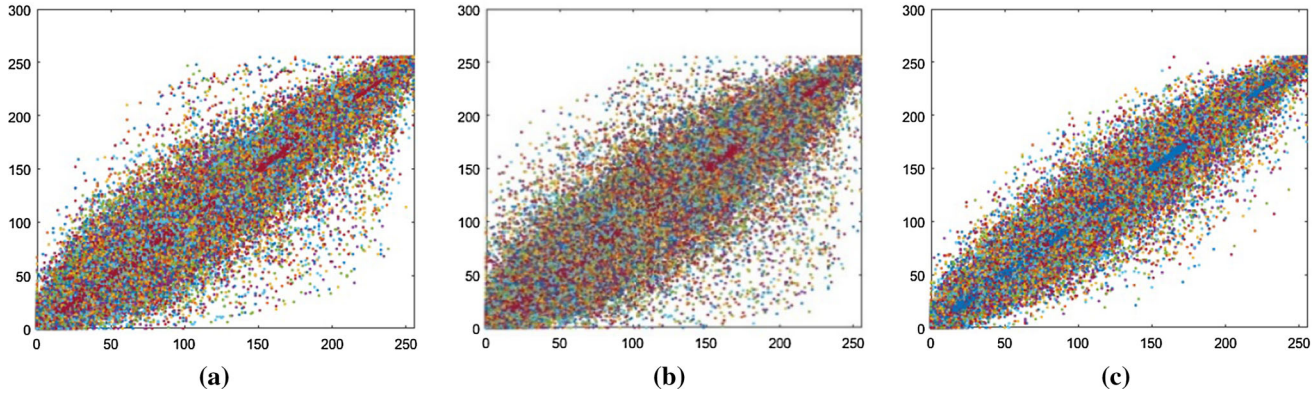


Fig. 29 **a** Plain test image red layer horizontal correlation; **b** plain test image red layer diagonal correlation; **c** plain test image red layer vertical correlation (color figure online)

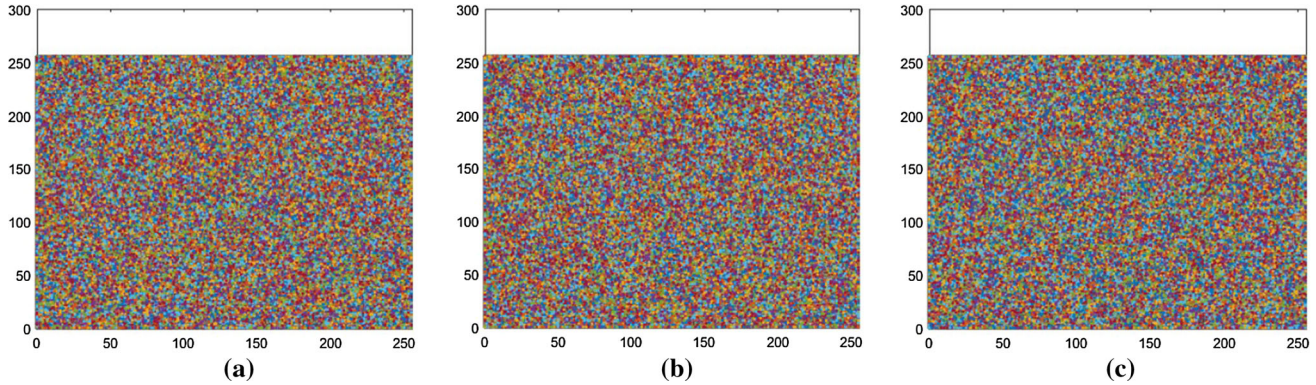


Fig. 30 **a** Enciphered test image red layer horizontal correlation; **b** enciphered test image red layer diagonal correlation; **c** enciphered test image red layer vertical correlation (color figure online)

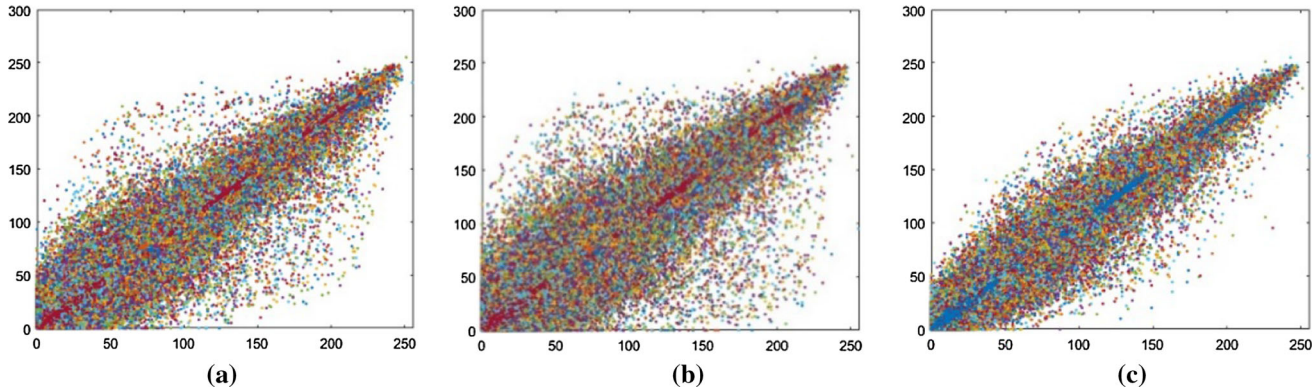


Fig. 31 **a** Plain test image green layer horizontal correlation; **b** plain test image green layer diagonal correlation; **c** plain test image green layer vertical correlation (color figure online)

uniform the distribution of gray-level values in the image. The quality of system can be measured through information entropy analysis [58]. This quantity can be defined as:

$$H = -\sum_{j=0}^{N-1} p(x_j) \log_b p(x_j), \tag{7}$$

where $p(x_j)$ defines probability mass function (PMF) for the event 'x_j,' where 'b' is logarithmic base used in entropy definition and 'X' is the random variable which takes 'n' outcomes. Ideally, entropy value is always equal to 8 for good secure encrypted image. The tabulation of different test images for entropy investigation is given in Tables 4, 5 and 6, respectively. The result shows that entropy values

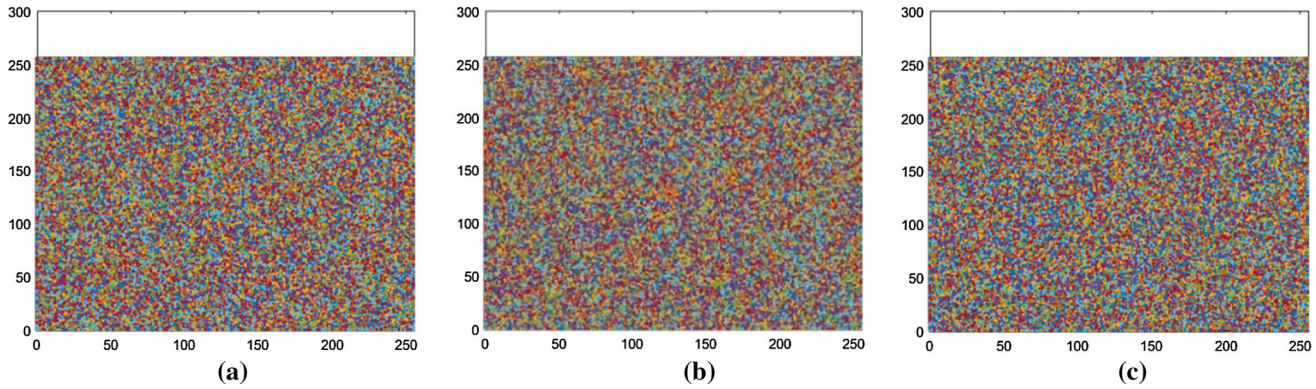


Fig. 32 **a** Enciphered test image green layer horizontal correlation; **b** enciphered test image green layer diagonal correlation; **c** enciphered test image green layer vertical correlation (color figure online)

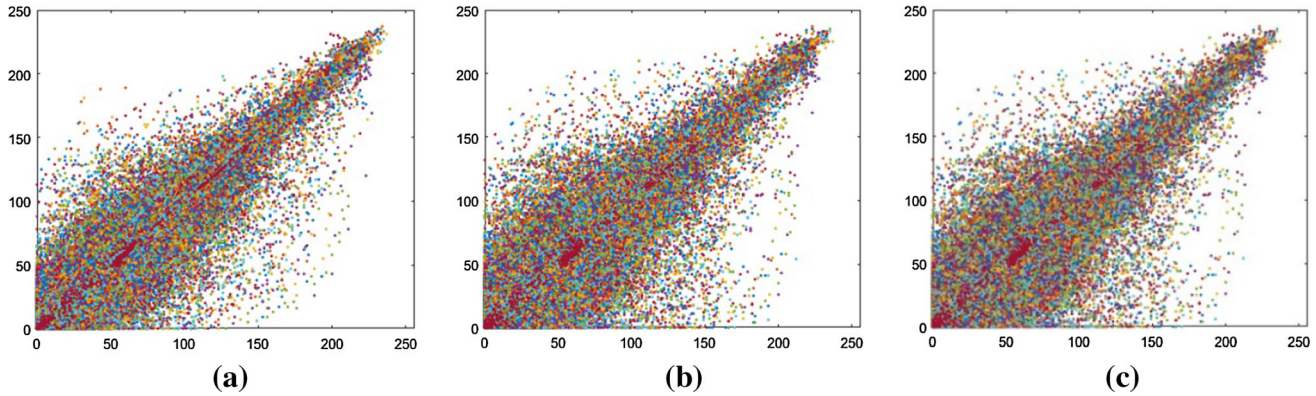


Fig. 33 **a** Plain test image blue layer horizontal correlation; **b** plain test image blue layer diagonal correlation; **c** plain test image blue layer vertical correlation (color figure online)

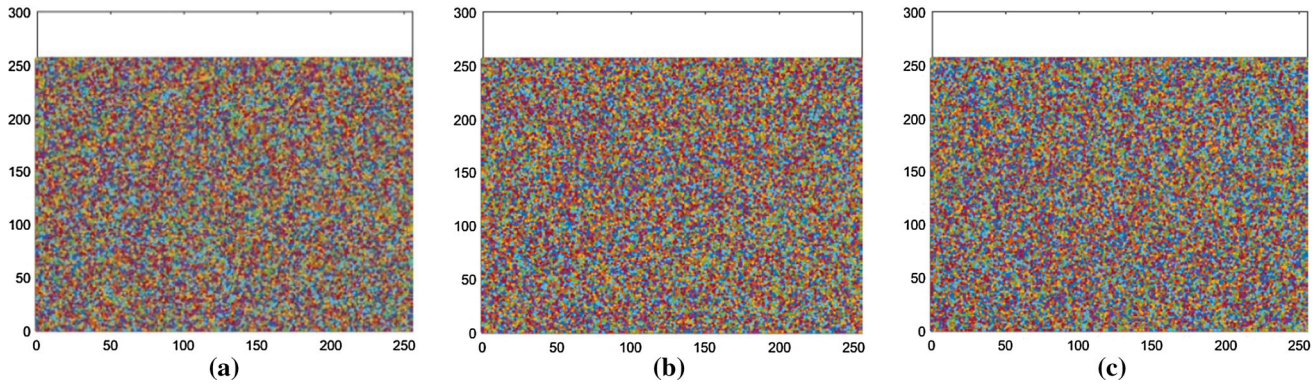


Fig. 34 **a** Enciphered test image blue layer horizontal correlation; **b** enciphered test image blue layer diagonal correlation; **c** enciphered test image blue layer vertical correlation (color figure online)

are approaching to 8, i.e., 7.999 is almost equal to 8 for all test images of 512 × 512 for channel wise. While looking into full image of 512 × 512 × 3, the proposed system value approaches to 7.9998. According to Table 5, the proposed algorithm value has three nine after decimal point for 512 × 512 × 3 while comparing it to the preexisting values of different algorithm designed in [1–8] show improved and superior to available algorithms. Above explanation concludes that the proposed cryptosystem is highly secure against any attack and can be used for today's real communication security.

Table 4 Entropy values of different channels of the proposed algorithm

CI	CC	Dimension	Entropy calculated
Encrypted Lena	R	512 × 512	7.999
	G	512 × 512	7.999
	B	512 × 512	7.999
Encrypted Tiffany	*R*	512 × 512	7.999
	G	512 × 512	7.999
	B	512 × 512	7.999
Encrypted Splash	*R*	512 × 512	7.999
	G	512 × 512	7.999
	B	512 × 512	7.999
Encrypted Tiffany	*R*	256 × 256	7.996
	G	256 × 256	7.997
	B	256 × 256	7.997
Encrypted Airplane	*R*	512 × 512	7.999
	G	512 × 512	7.999
	B	512 × 512	7.999

CI cipher images, *CC* cipher channels

Table 5 Proposed information entropy versus preexisting values

Image	Dimension	Entropy compared
Proposed algorithm	512 × 512	7.999
Ref. [1]-Lena	512 × 512	7.996
Ref. [2]-Lena	512 × 512	7.997
Ref. [3]-Lena	512 × 512	7.989
Ref. [4]-Lena	512 × 512	7.997
Ref. [5]-Lena	512 × 512	7.997
Ref. [6]-Lena	512 × 512	7.993
Ref. [7]-Lena	512 × 512	7.998
Ref. [8]-Lena	512 × 512	7.997

Table 6 Information entropy for various test images

Image	Dimension	Entropy measured
Ideal selection	512 × 512	8.000
Lena	512 × 512	7.999
Tiffany	512 × 512	7.999
Splash	512 × 512	7.999
Tiffany	256 × 256	7.997
Airplane	512 × 512	7.999

4.4 MSE test analysis

Mean square error is an average of pixel-by-pixel squared difference of two images, i.e., original image and encrypted image. MSE can be expressed as

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(P_{(i,j)} - C_{(i,j)}\right)^2, \tag{8}$$

where $M \times N$ shows total size of test image, 'i' and 'j' represent rows and columns, 'P' and 'C' show plain and ciphered image, respectively, at 'i' and 'j' position, respectively. MSE must be greater for better robust cryptosystem. Table 7 shows different values of MSE and PSNR for different taken test images of sizing 512 × 512 and 256 × 256 correspondingly. Maximum channel values are approaching to ten thousand figures and some are much above from ten thousand while examining into Table 7. Tiffany image layer values proved that the algorithm is highly desirable to be implemented for real-time communication.

4.5 PSNR test analysis

Peak signal-to-noise signal (PSNR) is a measure used for quality of image and can be expressed as

Table 7 MSE and PSNR values of different layers for different standard images

CI	CC	Dimension	Projected technique	
			MSE	PSNR
Lena	Red	512 × 512	9466.65	8.40
	Green	512 × 512	11,174.40	7.98
	Blue	512 × 512	12,826.45	7.08
Tiffany	Red	512 × 512	17,614.07	5.71
	Green	512 × 512	13,105.11	6.99
	Blue	512 × 512	7353.79	9.50
Splash	Red	512 × 512	11,427.31	7.59
	Green	512 × 512	12,316.79	7.26
	Blue	512 × 512	9880.11	8.22
Tiffany	Red	256 × 256	17,494.14	5.74
	Green	256 × 256	13,015.62	7.02
	Blue	256 × 256	7324.44	9.52
Airplane	Red	512 × 512	9986.41	8.17
	Green	512 × 512	10,609.41	7.91
	Blue	512 × 512	10,521.51	7.94

CI cipher images, *CC* cipher channels

$$\text{PSNR} = 10\log_2\left(\frac{I_{\max}^2}{\text{MSE}}\right), \tag{9}$$

where $I_{\max}$ is maximum value of pixel for test image. Peak signal-to-noise ratio is a factor which can be calculated in unit of decibels. Mean square output values and peak signal-to-noise ratio output values are contrary to one another. Mean square error must be greater in value for better secure of cryptosystem and peak signal-to-noise ratio must be lesser in value for better secure of data. According to Table 7, PSNR values are different for different test images of different dimensions. The approximate average value is almost 7 which is good enough for ensuring secure cryptosystem.

4.6 Sensitivity Analysis

4.6.1 Mean absolute error analysis

Mean absolute error (MAE) is a type of criterion applied to explore attainment of special attack known as resisting differential attack. Suppose $M \times N$ be the total size of test image, 'C' be the cipher and 'P' be the gray pixels of plain image at ith row and jth column subsequently. Maximum absolute error can be computed from the given formula:

$$\text{MAE} = \frac{1}{M \times N}\sum_{i=0}^{M-1}\sum_{J=0}^{N-1}|C_{(i,j)} - P_{(i,j)}|. \tag{10}$$

The bigger value of mean absolute error investigation represents the strong security of cryptosystem. If mean absolute error value is not enough larger, then fulfillment of resistant differential attack is performed. The average MAE is almost 75 for acceptable secure algorithm. The value of MAE of proposed algorithm is > 75. According to Table 8, the proposed algorithm value is 92 which is above acceptable value of 75, while Tiffany of both dimensions and Airplane show double the value of acceptable range of 75 that satisfies encouraging cryptosystem. According to Table 9, the comparison of values of different test images with proposed and preexisting values takes place. The value of MAE for Lena is 78 in preexisting algorithm in Ref. [9] same as for Tiffany of 512 dimension with 182 almost double of preexisting algorithm value of 94.36 which show better resistivity against cryptographic attacks.

Table 8 MAE test analysis for various test images

Images	Size	Projected technique MAE
Lena	512 × 512	92
Tiffany	512 × 512	182
Splash	512 × 512	76
Tiffany	256 × 256	169
Airplane	512 × 512	154

Table 9 Comparison of MAE test analysis for various test images of 512 and 256 dimensions

Images	Size	Projected technique MAE
Lena	512 × 512	92.00
Ref. [9]	256 × 256	77.82
Tiffany	256 × 256	169.0
Ref. [9]	256 × 256	94.36
Splash	512 × 512	76.00
Ref. [9]	256 × 256	76.78
Tiffany	512 × 512	182.0
Ref. [9]	256 × 256	99.36

4.6.2 NPCR test analysis

Number of pixel change rate is a type of test which refers to change of pixels occurring with alteration of lone pixel of standard plain image. When the value approaches to 99.60 almost for NPCR, then this means that the system will be approached to more sensitive level and will be more efficient for resisting a plain text attack. The ideal value for NPCR is always 100. In Figs. 10, 11 and 12, respectively, the proposed value for NPCR is 99.61 for all three channels and all test images except Tiffany which shows some exceptional value of 99.74 as given in Table 10. According to Table 11, we evaluated and examined for combined channels image with the same value of 99.61 except for Tiffany which is 99.74. In Table 12, comparison of values of the proposed algorithm and some preexisting values in

Table 10 %NPCR and UACI test analysis for various images channel wise

Image	Dimension	Test type	R-C	G-C	B-C
Lena	512 × 512	NPCR	99.61	99.61	99.61
	512 × 512	UACI	33.786	33.786	33.786
Tiffany	512 × 512	NPCR	99.61	99.61	99.61
	512 × 512	UACI	36.13	36.13	36.13
Splash	512 × 512	NPCR	99.61	99.61	99.61
	512 × 512	UACI	33.86	33.86	33.86
Tiffany	256 × 256	NPCR	99.74	99.74	99.74
	256 × 256	UACI	35.9	35.9	35.9

R-C red channel, *G-C* green channel, *B-C* blue channel

Table 11 %NPCR and UACI test for various images

Image	Dimension	Proposed tests	Evaluated value
Proposed image Lena	512 × 512	NPCR	33.78
	512 × 512	UACI	99.61
Tiffany	512 × 512	NPCR	99.61
	512 × 512	UACI	36.13
Splash	512 × 512	NPCR	99.61
	512 × 512	UACI	33.86
Tiffany	256 × 256	NPCR	99.74
	256 × 256	UACI	35.9

Table 12 %NPCR and UACI comparison of proposed values with preexisting values

Images	Size	Tests	Combined
Lena	512 × 512	NPCR	99.61
	512 × 512	UACI	33.78
Ref. [10]	512 × 512	NPCR	99.60
	512 × 512	UACI	33.55
Ref. [2]	512 × 512	NPCR	99.61
	512 × 512	UACI	33.51
Ref. [11]	512 × 512	NPCR	99.24
	512 × 512	UACI	33.13
Ref. [56]	512 × 512	NPCR	99.61
	512 × 512	UACI	33.48
Ref. [8]	512 × 512	NPCR	99.60
	512 × 512	UACI	33.41

[2, 8, 10, 11, 56] is shown. While looking into table, the proposed algorithm value of NPCR of Lena is greater in number than the referred algorithm values shown in Table 12. In this test, we considered two enciphered images whose provenience image is particular. The two cipher images are $C_{1(i,j)}$ and $C_{2(i,j)}$ but the provenience image is different by only pixel difference. NPCR value can be computed from the given formula as follows:

$$\text{NPCR} = \frac{\sum_{i,j} D_{(i,j)}}{W \times H} \times 100, \tag{11}$$

where $D_{(i,j)}$ is illustrated as

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases}.$$

4.6.3 UACI test analysis

UACI also abbreviated as unified average changing intensity testifies intermediate intenseness difference among original and enciphered image. This test when approached to 33 percent shows that cryptosystem is becoming more efficient against any attack. In Table 10, the proposed algorithm value, Tiffany and Slash is 33.786, 36.13 and 33.86, respectively. In Table 12, comparison of values shown with preexisting values in Refs. [10, 2], [11], [56], [11] are 33.373, 33.51, 33.12, 33.48 and 33.41 are lesser in number compared to introduced algorithm confirm robust cryptosystem. UACI can be calculated using the formula:

$$\text{UACI} = \frac{1}{W \times H} \sum_{i,j} \left[\frac{C_{1(i,j)} - C_{2(i,j)}}{255} \right] \times 100\%. \tag{12}$$

4.7 NIST randomness analysis

NIST test analysis which can be abbreviated as national institute of standard and technology is a physical science laboratory and non-regulatory agency which published statistical tests of (SP 800-22) based on numbers and based on complete unpredictability for cryptography. It is one of the most valuable and strongest methods of investigation and inquiry, and it is completely based on zero and one sequence. The main justification of these sequence is that the result out of enciphered image is always predicted as a binary data stream file. The results are shown in Tables 13 and 14, respectively.

Table 13 NIST test random excursion for three channels

R-C		G-C		B-C	
Input	Output	Input	Output	Input	Output
$X_1 = -4$	0.30358	$X_1 = -4$	0.04221	$X_1 = -4$	0.23932
$X_1 = -3$	0.09988	$X_1 = -3$	0.25892	$X_1 = -3$	0.49942
$X_1 = -2$	0.07780	$X_1 = -2$	0.62649	$X_1 = -2$	0.48109
$X_1 = -1$	0.40240	$X_1 = -1$	0.84285	$X_1 = -1$	0.84444
$X_1 = 1$	0.80849	$X_1 = 1$	0.77019	$X_1 = 1$	0.90704
$X_1 = 2$	0.84250	$X_1 = 2$	0.62512	$X_1 = 2$	0.36717
$X_1 = 3$	0.13813	$X_1 = 3$	0.49485	$X_1 = 3$	0.20972
$X_1 = 4$	0.51536	$X_1 = 4$	0.51068	$X_1 = 4$	0.47053

R-C red channel, *G-C* green channel, *B-C* blue channel

Table 14 NIST analysis of random excursion

R-Channel		G-Channel		B-Channel	
Input	Output	Input	Output	Input	Output
$X_1 = -9$	0.62466	$X_1 = -9$	0.27793	$X_1 = -9$	0.27999
$X_1 = -8$	0.63439	$X_1 = -8$	0.25980	$X_1 = -8$	0.27965
$X_1 = -7$	0.84570	$X_1 = -7$	0.27597	$X_1 = -7$	0.56984
$X_1 = -6$	0.93677	$X_1 = -6$	0.29247	$X_1 = -6$	0.72695
$X_1 = -5$	0.97668	$X_1 = -5$	0.24449	$X_1 = -5$	0.65601
$X_1 = -4$	0.89451	$X_1 = -4$	0.26551	$X_1 = -4$	0.52233
$X_1 = -3$	0.93747	$X_1 = -3$	0.40681	$X_1 = -3$	0.20234
$X_1 = -2$	0.47838	$X_1 = -2$	0.70546	$X_1 = -2$	0.16491
$X_1 = -1$	0.25421	$X_1 = -1$	0.91312	$X_1 = -1$	0.59298
$X_1 = 1$	0.86076	$X_1 = 1$	0.58538	$X_1 = 1$	0.12990
$X_1 = 2$	0.47838	$X_1 = 2$	0.75278	$X_1 = 2$	0.07182
$X_1 = 3$	0.36699	$X_1 = 3$	0.96108	$X_1 = 3$	0.17555
$X_1 = 4$	0.28879	$X_1 = 4$	0.96711	$X_1 = 4$	0.25228
$X_1 = 5$	0.26659	$X_1 = 5$	0.82726	$X_1 = 5$	0.35728
$X_1 = 6$	0.42759	$X_1 = 6$	0.51057	$X_1 = 6$	0.70688
$X_1 = 7$	0.62661	$X_1 = 7$	0.62826	$X_1 = 7$	0.98029
$X_1 = 8$	0.71711	$X_1 = 8$	0.86577	$X_1 = 8$	1
$X_1 = 9$	0.71764	$X_1 = 9$	0.75082	$X_1 = 9$	0.89685

R red, *G* green, *B* blue

5 Conclusion

In the above communication, we concluded that chaos with addition to fractals and Fibonacci has exceptional output while examining its results using different tests. Due to fascinating and exceptional results, it can be implemented in real-time communication. The method can be extended by addition of more multiple chaotic maps and fractals with different dimensions with inclusion of different well-generated random behavior series. The method helps us with better encryption, security and robustness with no probability to be attack. The invulnerability of above system can also be extended to video and audio encryption in coming days.

Compliance with ethical standards

Conflict of interest The authors have no conflict of interest.

References

1. Belazi A, El-Latif AAA, Belghith S (2016) A novel image encryption scheme based on substitution-permutation network and chaos. Sig Process 128:155–170
2. Hamza R, Titouna F (2016) A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. Inf Secur J Glob Perspect 25(4–6):162–179
3. Huang X, Ye G (2014) An image encryption algorithm based on hyper-chaos and DNA sequence. Multimed Tools Appl 72(1):57–70
4. Wang X, Liu L, Zhang Y (2015) A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 66:10–18
5. Khan M, Asghar Z (2018) A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S8 permutation. Neural Comput Appl 29(4):993–999
6. Wang XY, Zhang YQ, Bao XM (2015) A colour image encryption scheme using permutation-substitution based on chaos. Entropy 17(6):3877–3897
7. Machkour M, Saaidi A, Benmaati ML (2015) A novel image encryption algorithm based on the two-dimensional logistic map and the latin square image cipher. 3D Res 6(4):36
8. Zhang G, Liu Q (2011) A novel image encryption method based on total shuffling scheme. Opt Commun 284(12):2775–2780
9. Norouzi B, Mirzakuchaki S, Seyedzadeh SM, Mosavi MR (2014) A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. Multimed Tools Appl 71(3):1469–1497
10. Seyedzadeh SM, Norouzi B, Mosavi MR, Mirzakuchaki S (2015) A novel color image encryption algorithm based on spatial permutation and quantum chaotic map. Nonlinear Dyn 81(1–2):511–529
11. Boriga RE, Dăscălescu AC, Diaconu AV (2014) A new fast image encryption scheme based on 2D chaotic maps. IAENG Int J Comput Sci 41(4):249–258
12. Khan M, Hussain I, Jamal SS, Amin M (2019) A privacy scheme for digital images based on quantum particles. Int J Theor Phys. https://doi.org/10.1007/s10773-019-04301-6
13. Khan M, Munir N (2019) A novel image encryption technique based on generalized advanced encryption standard based on field of any characteristic. Wirel Pers Commun. https://doi.org/10.1007/s11277-019-06594-6
14. Khan M, Masood F (2019) A novel chaotic image encryption technique based on multiple discrete dynamical maps. Multimed Tools Appl 78(18):26203–26222
15. Waseem HM, Majid K (2019) A new approach to digital content privacy using quantum spin and finite-state machine. Appl Phys B 125:27. https://doi.org/10.1007/s00340-019-7142-y
16. Khan M, Waseem HM (2019) A novel digital contents privacy scheme based on Kramer's arbitrary spin. Int J Theor Phys 58:2720–2743
17. Rafiq A, Khan M (2019) Construction of new S-boxes based on triangle groups and its applications in copyright protection. Multimed Tools Appl 78:15527–15544
18. Khan M, Waseem HM (2018) A novel image encryption scheme based on quantum dynamical spinning and rotations. PLoS ONE 13(11):e0206460
19. Waseem HM, Khan M (2018) Information confidentiality using quantum spinning, rotation and finite state machine. Int J Theor Phys 57(11):3584–3594
20. Waseem HM, Khan M, Shah T (2018) Image privacy scheme using quantum spinning and rotation. J Electron Imaging 27(6):063022
21. Younas I, Khan M (2018) A new efficient digital image encryption based on inverse left almost semi group and Lorenz chaotic system. Entropy 20(12):913
22. Khan M (2015) A novel image encryption scheme based on multi-parameters chaotic S-boxes. Nonlinear Dyn 82:527–533

23. Khan M (2015) An image encryption by using Fourier series. J Vib Control 21:3450–3455
24. Stallings W (2006) Cryptography and network security, 4/E. Pearson Education India, Bengaluru
25. Chuang CH, Yen ZY, Lin GS, Hong ZW (2011) A virtual optical encryption software system for image security. J Converg Inf Technol 6(2):357–364
26. Al-Najjar HM (2012) Digital image encryption algorithm based on multi-dimensional chaotic system and pixels location. Int J Comput Theory Eng 4(3):357
27. Banthia AK, Tiwari N (2013) Image encryption using pseudo random number generators. Int J Comput Appl 67(20):1–8
28. Rivest RL (1990) Cryptography. In: van Leeuwen J (ed) Algorithms and complexity. MIT Press, Cambridge, pp 717–755
29. Kartit Z, Azougaghe A, Idrissi HK, El Marraki M, Hedabou M, Belkasmi M, Kartit A (2016) Applying encryption algorithm for data security in cloud storage. In: Sabir E, Medromi H, Sadik M (eds) Advances in ubiquitous networking. Springer, Singapore, pp 141–154
30. Wheeler DD, Matthews RA (1991) Supercomputer investigations of a chaotic encryption algorithm. Cryptologia 15(2):140–152
31. Chen Y, Liao X (2005) Cryptanalysis on a modified Baptista-type cryptosystem with chaotic masking algorithm. Phys Lett A 342(5–6):389–396
32. Xie EY, Li C, Yu S, Lü J (2017) On the cryptanalysis of Fridrich's chaotic image encryption scheme. Sig Process 132:150–154
33. Akhavan A, Samsudin A, Akhshani A (2015) Cryptanalysis of "an improvement over an image encryption method based on total shuffling". Opt Commun 350:77–82
34. Akhavan A, Samsudin A, Akhshani A (2017) Cryptanalysis of an image encryption algorithm based on DNA encoding. Opt Laser Technol 95:94–99
35. Baptista MS (1998) Cryptography with chaos. Phys Lett A 240(1–2):50–54
36. Parvaz R, Zarebnia M (2018) A combination chaotic system and application in color image encryption. Opt Laser Technol 101:30–41
37. Solak E, Rhouma R, Belghith S (2010) Cryptanalysis of a multi-chaotic systems based image cryptosystem. Opt Commun 283:232–236
38. Mandelbrot BB (1983) The fractal geometry of nature, vol 173. W. H. Freeman, New York
39. Gomory R (2010) Benoît Mandelbrot (1924–2010). Nature 468:378
40. Addison PS (1997) Fractals and chaos: an illustrated course. CRC Press, Boca Raton
41. Khawaja MA, Khan M (2019) A new construction of confusion component of block ciphers. Multimed Tools Appl. https://doi.org/10.1007/s11042-019-07866-w
42. Kashanian H, Davoudi M, Khorramfar H (2016) Image encryption using chaos functions and fractal key. Int J Comput Sci Netw Secur 16(10):87
43. Abd-El-Hafiz SK, Radwan AG, Haleem SHA, Barakat ML (2014) A fractal-based image encryption system. IET Image Proc 8(12):742–752
44. Peitgen HO, Walther HO (eds) (2006) Functional differential equations and approximation of fixed points. Proceedings, Bonn, July 1978, vol 730. Springer
45. Russell DA, Hanson JD, Ott E (1980) Dimension of strange attractors. Phys Rev Lett 45(14):1175
46. Grassberger P, Procaccia I (1983) Measuring the strangeness of strange attractors. Physica D 9(1–2):189–208
47. Tiner JH (2004) Exploring the world of mathematics: from ancient record keeping to the latest advances in computers. New Leaf Publishing Group, Green Forest
48. Beck M, Geoghegan R (2010) The art of proof: basic training for deeper mathematics. Springer, Berlin
49. Batool SI, Waseem HM (2019) A novel image encryption scheme based on Arnold scrambling and Lucas series. Multimed Tools Appl 78:27611–27637
50. Mazloom S, Eftekhari-Moghadam AM (2009) Color image encryption based on coupled nonlinear chaotic map. Chaos Solitons Fractals 42(3):1745–1754
51. Seyedzadeh SM, Mirzakuchaki S (2012) A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. Sig Process 92(5):1202–1215
52. Liu S, Sun J, Xu Z (2009) An improved image encryption algorithm based on chaotic system. JCP 4(11):1091–1100
53. Akhshani A, Akhavan A, Lim SC, Hassan Z (2012) An image encryption scheme based on quantum logistic map. Commun Nonlinear Sci Numer Simul 17(12):4653–4661
54. Wang X, Teng L, Qin X (2012) A novel color image encryption algorithm based on chaos. Sig Process 92(4):1101–1108
55. El-Latif AAA, Li L, Wang N, Han Q, Niu X (2013) A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. Signal Process 93:2986–3000
56. Wang X, Yang L (2012) A novel chaotic image encryption algorithm based on water wave motion and water drop diffusion models. Opt Commun 285(20):4033–4042
57. Wu Y, Zhou Y, Noonan JP, Agaian S (2014) Design of image cipher using latin squares. Inf Sci 264:317–339
58. Shannon CE (1949) Communication theory of secrecy systems. Bell Labs Tech J 28:656–715