Multimedia Tools and Applications (2019) 78:34901–34925
https://doi.org/10.1007/s11042-019-08086-y

Secure image encryption scheme using high efficiency word-oriented feedback shift register over finite field

Subhrajyoti Deb[1] · Bhaskar Biswas[2] · Bubu Bhuyan[1]

Received: 1 February 2019 / Revised: 27 July 2019 / Accepted: 2 August 2019 /
Published online: 24 August 2019

Abstract
Image encryption is an evolving technique in the arena of data communication. In the last decade, many encryption schemes have been suggested. Unfortunately, most of the current schemes are unable to maintain a balance between security and computational complexity. To overcome this challenge, this paper introduces a novel encryption scheme that effectively maintains the trade-off between security and computational complexity. Initially, the plain image is randomized and scrambled by the Logistic map and Arnold's scrambling technique. The intermediate image found above, is then encrypted by the special word-oriented feedback shift register (wfsr) to get the final cipher image. Wfsr is inherently suitable for high-quality pseudorandom number generation with good statistical properties. It usually posses high throughput. Further, the elliptic curve Diffie-Hellman (ECDH) is used for sharing the keys required for encryption and decryption process. The performance of the proposed cryptosystem is evaluated based on several statistical properties of the cipher image, the resistance of the cipher image to various attacks, and time required for encryption and key sharing process. The statistical properties of the encrypted image are found out through histogram analysis, correlation and entropy finding, key sensitivity analysis, chi-square test, and NIST randomness test. The resistance of the encrypted image to various attacks is either found out experimentally or indirectly by using metrics like Unified Average Changing Intensity (UACI), Number of Pixel Changing Rate (NPCR). The proposed encryption method compares favorably with similar image encryption schemes.

Keywords Image encryption · wfsr · NPCR · UACI · ECDH · NIST randomness test

1 Introduction

Nowadays, image encryption is extensively used for storage and transmission of images in various multimedia applications like telemedicine, military communication, border surveillance, etc. Therefore, security has become a priority concern. Usually, the digital images

✉ Subhrajyoti Deb
subhrajyotideb1@gmail.com

[1] Department of Information Technology, North-Eastern Hill University, Shillong, India

[2] Department of Information Technology, Tripura University, Suryamaninagar, India

have long run of pixels with the same red, green, and blue (RGB) values making the encrypted images using conventional cryptographic primitives, susceptible to cryptographic attacks. The chaotic map is an effective method for randomization of image data to alleviate the mentioned problem. The chaotic map works through a special set of mathematical equations in the one-dimensional (1D), and two-dimensional (2D) platforms [19, 22, 31, 38, 39]. 1D maps allow the high-grade model of chaotic systems like the Logistic map, Henon map, Tent map [4, 18, 28, 41]. For more random performance multi-dimensional chaotic maps have been recommended [2, 3, 5, 9, 19]. Various research articles confirm that the introduction of a scrambling process before the encryption enhances the security level of the encryption scheme [20, 25, 29, 32]. Scrambling is the preprocessing technique that rearranges the pixel positions of the plain image. Arnold's transform, Fibonacci transform, Magic square transform, Tangram algorithm, Hilbert curve method, etc., are some of the popular scrambling techniques that have been used in many encryption systems [11, 20]. Recent encryption schemes generally use Arnold's transform which possesses better scrambling, and security enhancement features [25, 29, 33]. Thus, as mentioned above, the image encryption system is a multi-step process. At first, the plain image is randomized by different types of a chaotic system, and next the image pixel content is encrypted with strong cryptographic primitive. The cryptographic primitives such as symmetric cipher (stream cipher, block cipher, hash function), and asymmetric standards (like elliptic curve cryptography (ECC), RSA, etc.,) are frequently used for image encryption/decryption [1, 3, 6, 7, 10, 14, 16, 23–25, 27, 40, 44, 45]. In order to satisfy the high security in the encrypted image, the chaos-based permutation, diffusion, and substitution processes, as well as high computationally involved cryptographic algorithms are used to encrypt the image [14, 16, 20, 25, 29, 32, 43].

P. Praveenkumar et al. [32] introduced the medical image encryption system, and the scheme exhibited enhanced security performance by using cognitive radio technology. But this scheme suffers from computational delay, and also the scheme does not provide any key sharing techniques. Z. Gan et al. [20] proposed the color image encryption scheme based on three-dimensional (3D) Brownian motion. Their proposed scheme fulfills most of the underlying security requirements because of diffusion, confusion architecture. Moreover, the scheme poses with several complex function operations which lead to high-end delay. H. Liu et al. [29] proposed a chaos-based image encryption scheme with the provision of using different keys periodically. Their proposed system claims to achieve a high-level of security due to the use of multiple keys. However, statistical security of the scheme is not evaluated exhaustively. Later, J. Chen et al. suggested an advanced image encryption scheme using self-adaptive permutation diffusion and DNA random encoding [15]. A self-adaptive permutation diffusion consists of the iterative number of rounds, and therefore, it is unable to maintain a trade-off between security and time complexity. But, their detailed statistical and attack analysis confirmed that the encryption system provides satisfactory performance. A A Abd El-Latif et al. [3] proposed an image encryption scheme based on chaotic system and cyclic elliptic curve. D. S. Laiphrakpam et al. [25] extended a similar idea and performed the scrambled image encryption scheme using elliptic curve. To improve the security of the system, they used the elliptic curve points to generate the random sequence. Their proposed design enhances the security of the image encryption system, but their key sharing time has not been taken into consideration. Inspired by the concept of image encryption, a useful scheme is designed in this paper.

In [8, 14, 15, 18, 23–25, 30, 36, 44–47], a large number of iterations are required for encryption and decryption system. So, the mentioned schemes suffer from a high computation cost. To maintain the computation complexity within the acceptable range, it is desirable to use a word-oriented feedback shift register (wfsr) in the final encryption stage

instead of high processing cryptographic algorithm. Wfsr has a large period and capable of generating the cryptographically secure keystream. Usually, most of the classical Linear-feedback shift register (LFSR)-based stream ciphers are bit-oriented [17, 42]. With the rapid growth of multimedia technology, many emerging applications demand high-speed encryption with desirable randomness properties for dealing with high data volume. In that situation, bit-oriented stream ciphers do not provide adequate performance. So, this issue also may be addressed if one uses a word-oriented feedback shift register [12, 37]. In 2007, Zeng et al. [42] proposed special word-based LFSR. They designed the improved version of wfsr (called as σ-LFSR) that uses word-operations in modern processors with parallelism techniques [42]. Moreover, wfsr provides good quality pseudorandom sequence, high linear complexity, and it is (5-10) times faster than a block cipher in the software implementation [37, 42]. The cryptosystem will be considered as strong if the system generates highly random keystream. Therefore, the scheme is cryptographically secure when the attackers may not be able to obtain valuable information from statistical analyses, adding noise, and different types of attacks. After the image encryption, anonymous key sharing protocol is required that allows sender and receiver to establish the secret key over the insecure channel. ECDH is an efficient key sharing technique because it requires less computational complexity, bandwidth, and memory compared to other public cryptosystems [13]. That motivates to investigate strong cryptographic primitive in the proposed image encryption scheme.

The proposed work focuses on high-level confidentiality in the encryption system. The proposed structure consists of two cryptographic stages, namely, encryption and key sharing phase. The contributions are as follows:

- In the encryption phase Logistic map, Arnold's scrambling, and wfsr are used to produce the cipher image. The use of wfsr contributed to the generation of high-quality pseudorandom number with high speed.
- The key of the encryption system has been efficiently transmitted by ECDH scheme.
- Additionally, the proposed scheme is able to resist known and chosen-plaintext attack, Brute force attack, differential attack, and noise attack.

Before proceeding further, let us describe the organization of this paper. Section 2 presents the basic specifications of the scheme. Section 3 explains the proposed framework. Section 4 shows simulation and statistical result. Section 5 presents performance and security analyses of the proposed scheme. Section 6 provides comparative analysis. Finally, Section 7 concludes the paper.

2 Preliminaries

This section revisits some of the background studies about the Logistic map, Arnold's transformation, and word-oriented feedback shift register.

2.1 Logistic map

The Logistic map represented as:

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

where, φ is the driving parameter. After using the equation, it provides the random sequence for a single pair of φ and x values. Here, the ranges of x is $(0 < x < 1)$ and φ is $(3 < \varphi < 4)$ respectively.

2.2 Arnold's transformation

In the digital image, Arnold's scrambling performed as:

$$\begin{bmatrix} x^{\complement} \\ y^{\complement} \end{bmatrix} = \begin{bmatrix} 1 & \mathcal{A} \\ \mathcal{B} & \mathcal{AB}+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{n} \tag{2}$$

where,

$$\begin{bmatrix} x \\ y \end{bmatrix} \quad : \text{ initial pixel position of the digital image}$$

$$\begin{bmatrix} 1 & \mathcal{A} \\ \mathcal{B} & \mathcal{AB}+1 \end{bmatrix} : 2 \times 2 \text{ matrix with determinant 1}$$

$$\begin{bmatrix} x^{\complement} \\ y^{\complement} \end{bmatrix} \quad : \text{ traversed point after Arnold's scrambling}$$

$$n \quad : \text{the order of digital image matrix like } (256 \times 256)$$

2.3 Word-oriented feedback shift register

This paper reconsiders some definitions and outcomes reported in [12, 37, 42]. In many of the effective applications, one generally uses finite fields with characteristic 2. We shall restrict to fields with characteristic 2 and their extensions. Throughout this paper, σ-LFSR shall be referred to as *wfsr*. The work represents as general by $\mathbb{F}_2$ the finite field with 2 components, by $\mathbb{F}_{2^m}$ the extended field of $\mathbb{F}_2$ of degree m and by $\mathbb{F}_2[Y]$ the ring of polynomials in one variable Y among coefficients in $\mathbb{F}_2$. Let the ring R and assumed $M_d(R)$ is for the set of all $d \times d$ matrices with entries in R where, d is the integer. Subsequently use the positive integers m and n, and a vector space basis $\{\omega_0, \ldots, \omega_{m-1}\}$ of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. For convenience, any $\mathsf{s} \in \mathbb{F}_{2^m}$, there are particular equation $\mathsf{s}_0, \ldots, \mathsf{s}_{m-1} \in \mathbb{F}_2$ to the extent that $\mathsf{s} = \mathsf{s}_0\omega_0 + \cdots + \mathsf{s}_{m-1}\omega_{m-1}$, and next use the corresponding co-ordinate vector $(\mathsf{s}_0, \ldots, \mathsf{s}_{m-1})$ of s by $\mathcal{S}$. In fact, the union $\mathsf{s} \longmapsto \mathcal{S}$ provides a vector space isomorphism of $\mathbb{F}_{2^m}$ onto $\mathbb{F}_2^m$. Elements of $\mathbb{F}_2^m$ might be formation of as row vectors and so $\mathcal{S}B$ is the distinct element of $\mathbb{F}_2^m$ for any $\mathcal{S} \in \mathbb{F}_2^m$ and $B \in M_m(\mathbb{F}_2)$.

Definition 1 Let $B_0, B_1, \ldots, B_{n-1} \in M_m(\mathbb{F}_2)$. For any n-tuple $(\mathcal{S}_0, \ldots, \mathcal{S}_{n-1})$ of elements of $\mathbb{F}_{2^m}$, let $(\mathcal{S}_i)_{i=0}^{\infty}$ represent the infinite sequence of elements of $\mathbb{F}_{2^m}$. It can be measured by the linear recurrence equation:

$$\mathcal{S}_{i+n} = B_0\mathcal{S}_i + B_1\mathcal{S}_{i+1} + \cdots + B_{n-1}\mathcal{S}_{i+n-1} \quad i = 0, 1, \ldots. \tag{3}$$

In general, the equation (3) is called by *wfsr* of order n over $\mathbb{F}_{2^m}$, while the sequence $(\mathcal{S}_i)_{i=0}^{\infty}$ is quoted as the *sequence generated by the wfsr* (3). So, the n-tuple $(\mathcal{S}_0, \mathcal{S}_1, \ldots, \mathcal{S}_{n-1})$ is represented as *initial state* of the *wfsr* (3) and the polynomial $I_m Y^n - B_{n-1}Y^{n-1} - \cdots - B_1 Y - B_0$ with matrix coefficients is the *matrix polynomial* of the *wfsr* (3). The string $(\mathcal{S}_i)_{i=0}^{\infty}$ is *basically periodic* if there are integers r, n_0 with $r \geq 1$ and $n_0 \geq 0$ such that $\mathcal{S}_{j+r} = \mathcal{S}_j$ for all $j \geq n_0$. The least positive integer r with this property is the *period* of $(\mathcal{S}_i)_{i=0}^{\infty}$ and the corresponding least nonnegative integer n_0 is the *preperiod* of $(\mathcal{S}_i)_{i=0}^{\infty}$. The sequence $(\mathcal{S}_i)_{i=0}^{\infty}$ is *periodic* if its preperiod is 0.

The subsequent outcome provides some interesting facts about *wfsr*.

Proposition 1 *In* [37] , *pseudorandom sequence* $(\mathcal{S}_i)_{i=0}^{\infty}$ *produced by the wfsr* (3) *of order* n *over* $\mathbb{F}_{2^m}$*, it consists*

(i) $(\mathcal{S}_i)_{i=0}^{\infty}$ *has periodic behaviour, and the period is* $2^{mn}-1$*;*
(ii) *if* B_0 *is nonsingular, then* $(\mathcal{S}_i)_{i=0}^{\infty}$ *is periodic; in an opposite way, if* $(\mathcal{S}_i)_{i=0}^{\infty}$ *is periodic whenever the initial state is of the form* $(b, 0, \ldots, 0)$*, where,* $b \in \mathbb{F}_{2^m}$ *with* $b \neq 0$*, then* B_0 *is nonsingular.*

The *wfsr* of order n over $\mathbb{F}_{2^m}$ is *primitive* if for any variety of nonzero initial state, the sequence produced by that *wfsr* has periodic behaviour of period $2^{mn}-1$. By Proposition 1 if $I_m Y^n - B_{n-1}Y^{n-1} - \cdots - B_1 Y - B_0 \in M_m(\mathbb{F}_2)[Y]$ is the matrix polynomial of primitive *wfsr*, then the matrix B_0 is assuredly nonsingular. Connected with a matrix polynomial $I_m Y^n - B_{n-1}Y^{n-1} - \cdots - B_1 Y - B_0 \in M_m(\mathbb{F}_2)[Y]$, it can be represented as a (m, n)-block companion matrix $\mathsf{B}_{\mathsf{wfsr}} \in M_{mn}(\mathbb{F}_2)$ as follows

$$\mathsf{B}_{\mathsf{wfsr}} = \begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & \mathbf{0} & B_0 \\ I_m & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & \mathbf{0} & B_1 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & I_m & \mathbf{0} & B_{n-2} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & I_m & B_{n-1} \end{pmatrix}, \tag{4}$$

where, I_m represent the $m \times m$ identity matrix over $\mathbb{F}_2$, while $\mathbf{0}$ signifies the zero matrix in $M_m(\mathbb{F}_2)$. Applying a Laplace expansion or the proper order of elementary column operations, it is clear to identify $\det \mathsf{B}_{\mathsf{wfsr}} = \pm \det(B_0)$. As a result,

$$\mathsf{B}_{\mathsf{wfsr}} \in \mathrm{GL}_{mn}(\mathbb{F}_2) \quad \text{if and only if} \quad B_0 \in \mathrm{GL}_m(\mathbb{F}_2), \tag{5}$$

where, $\mathrm{GL}_m(\mathbb{F}_2)$ is the general linear group of $m \times m$ nonsingular matrices over $\mathbb{F}_2$. With regard to the above mentioned that the block companion matrix (4) is the state transition matrix for the *wfsr* (3). Certainly, the l-th state $\mathcal{S}_{\mathsf{l}} := (\mathcal{S}_{\mathsf{l}}, \mathcal{S}_{\mathsf{l}+1}, \ldots, \mathcal{S}_{\mathsf{l}+n-1}) \in \mathbb{F}_{2^m}^n$ of the *wfsr* (3) is acquired from the initial state $\mathcal{S}_0 := (\mathcal{S}_0, \mathcal{S}_1, \ldots, \mathcal{S}_{n-1}) \in \mathbb{F}_{2^m}^n$ by

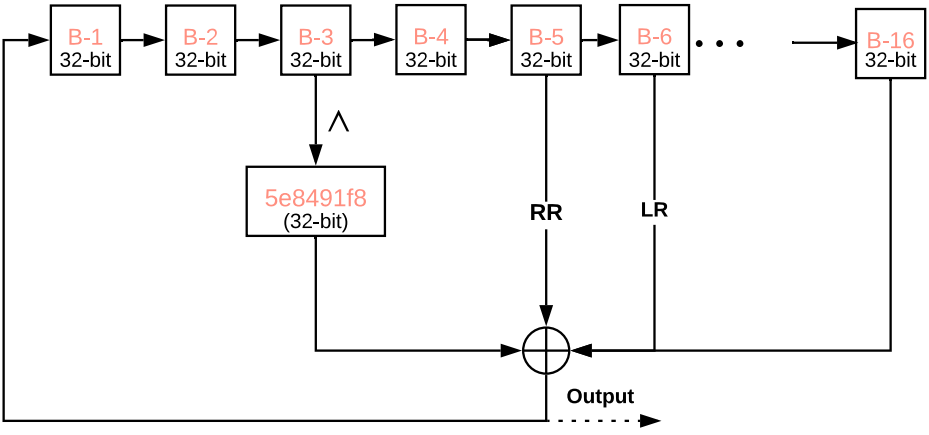

Fig. 1 Schematic diagram of wfsr. **LR**- Left Rotation, **RR**- Right Rotation, ∧- AND operation, and `5e8491f8`- 32-bit vector

$\mathcal{S}_{\mathsf{l}} = \mathcal{S}_0 \mathsf{B}^{\mathsf{l}}_{\mathsf{wfsr}}$, for any $\mathsf{l} \geq 0$. Here, *wfsr* can be recognized by (3) the block companion matrix (4).

This paper studies a special set of wfsr. The value of the word size (m) is identified as (8/16/32/64/128). In the proposed work, 32-bit output based wfsr architecture has been considered and shown in Fig. 1. Before the output sequence generation, the structure must be initialized with nonzero key/seed values. In this case, wfsr loaded by 16 blocks of Hex value and per block contains 32-bit (i.e. $16 \times 32 = 512$-bit).

3 Proposed framework

The proposed cryptosystem is presented in three parts, namely, key sharing, encryption, and decryption. The block diagram of the proposed cryptosystem is shown in Fig. 2.

3.1 Key sharing

After the image encryption system, the user sends the encryption key to the receiver by any public-key sharing algorithm like a digital envelope. Figure 2 illustrates the generic key sharing system.

1. As already discussed, proposed work considered 32-bit wfsr, and it uses 512-bit key value (κ) as shown in Appendix A.
2. In a general way, the sender generates $E_{R_{pub}}(x_0, \varphi, \widehat{r}, \kappa)$ and shared with the receiver by the public key of the receiver. All the notations are mentioned in Fig. 2.
3. Next, the receiver extracts the file $D_{R_{pri}}\left(E_{R_{pub}}(x_0, \varphi, \widehat{r}, \kappa)\right)$ by own private key.

In the asymmetric key sharing cryptosystem, particularly ECDH have a great prospect to satisfy the requirements of high security as well as less computation time. The proposed scheme has used ECDH key sharing algorithm and summarized in Section 5.8.

3.2 Encryption scheme

In this work, the cipher image is generated by a strong cryptosystem. The steps for generating a cipher image is as follows:

1. Select the plain image of size ($n \times n$).
2. In the plain image, Logistic map has been used to provide random behavior in the digital image. As discussed, the ranges of φ and x in the Section 2.1.
3. Let (x, y) coordinate belongs to the plain image. The Arnold's cat map performed on the pair (x, y), and it becomes $(x^{\complement}, y^{\complement})$. Next, the value of $\mathcal{A}$ and $\mathcal{B}$ are set to 1 (see (2)). Here, the number of scramble rounds termed as $\widehat{r}$.
4. A special kind of 32-bit wfsr is used for further encryption system. Now it is important to explain, how many times wfsr run to obtain pseudorandom sequence. Wfsr output sequence depends on the number of pixel values of the scrambled image (as the value of RGB is $\frac{n \times n \times 3 \times 8}{m}$). A pixel value typically consists of ($3 \times 8 = 24$) bits for the color image that is one byte each for R, G, and B, and $m = 32$ is the output size/clock of the wfsr. For example, if (256×256) RGB image is used, and run the wfsr upto $\left\lceil \frac{256 \times 256 \times 3 \times 8}{32} = 49152 \right\rceil$ times for random number sequence generation.

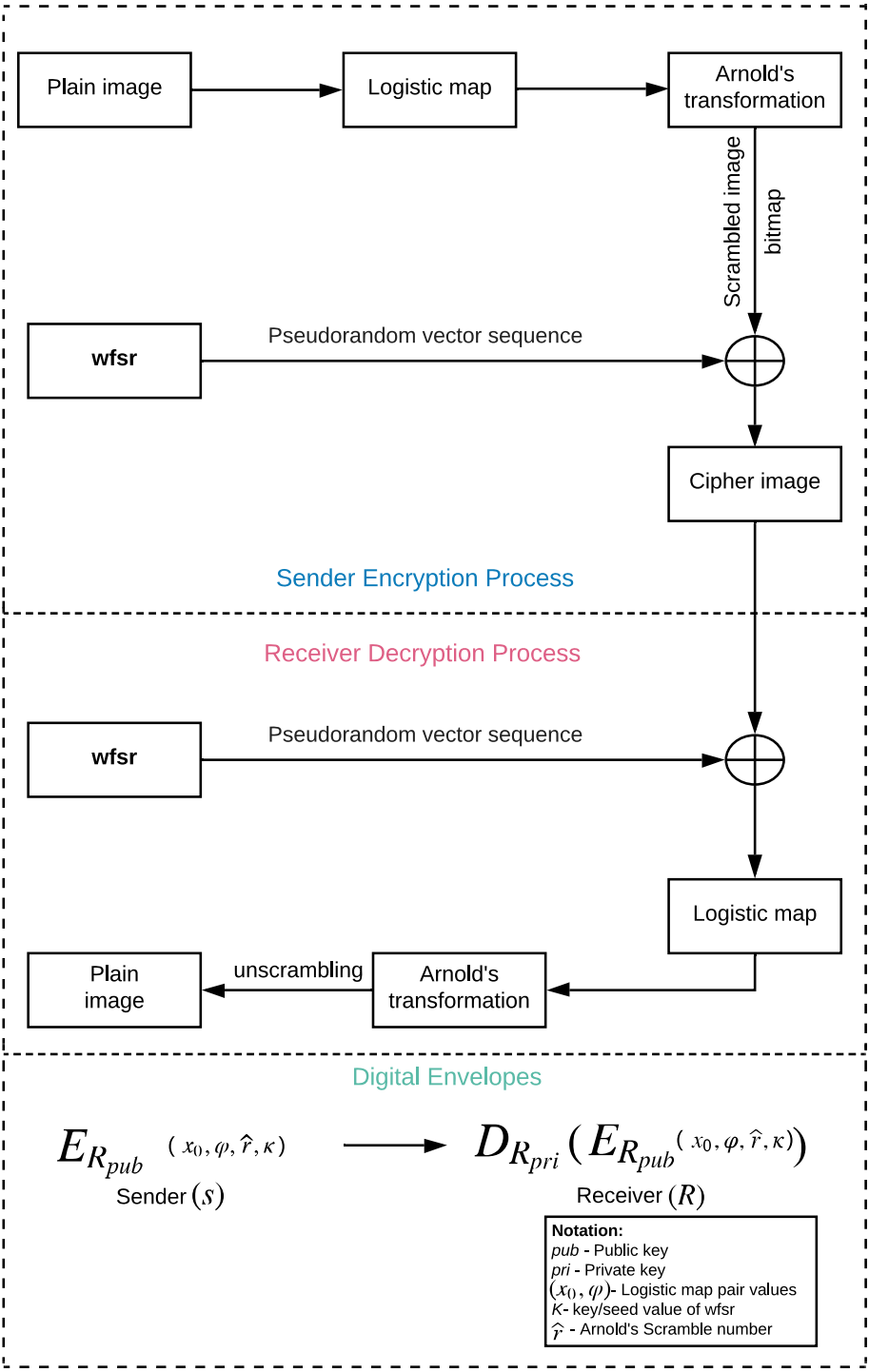

Fig. 2 Schematic view of the proposed structure

5. Next, perform Exclusive OR (XOR) operation of the keystream of wfsr, and the binary pixel values of the scrambled image. From this result, the cipher image has been obtained.

3.3 Decryption scheme

Decryption is the inverse process of encryption system.

1. Select the cipher image. Also collect the values of (x_0, φ, $\widehat{r}$, and κ). Specifically, (x_0, φ) values for Logistic map, $\widehat{r}$ for Arnold's cat-map round number, and κ for wfsr key.
2. Now receiver run the wfsr based on the cipher image pixel size as mentioned in step number 4 of the encryption system 3.2.
3. XOR (cipher image pixel value, wfsr keystream).
4. Perform Logistic map using the parameters of (x_0, φ).
5. Unscramble the scrambled image by using Arnold's cat map round ($\widehat{r}$) and get the original image.

4 Simulation and statistical analysis

In this section, simulation result has been performed to show the resistance of the proposed scheme against several statistical properties. A sample of plain images **(a-d)**, scrambled images **(e-h)**, and cipher images **(i-l)** are presented in Fig. 3 respectively. This encryption

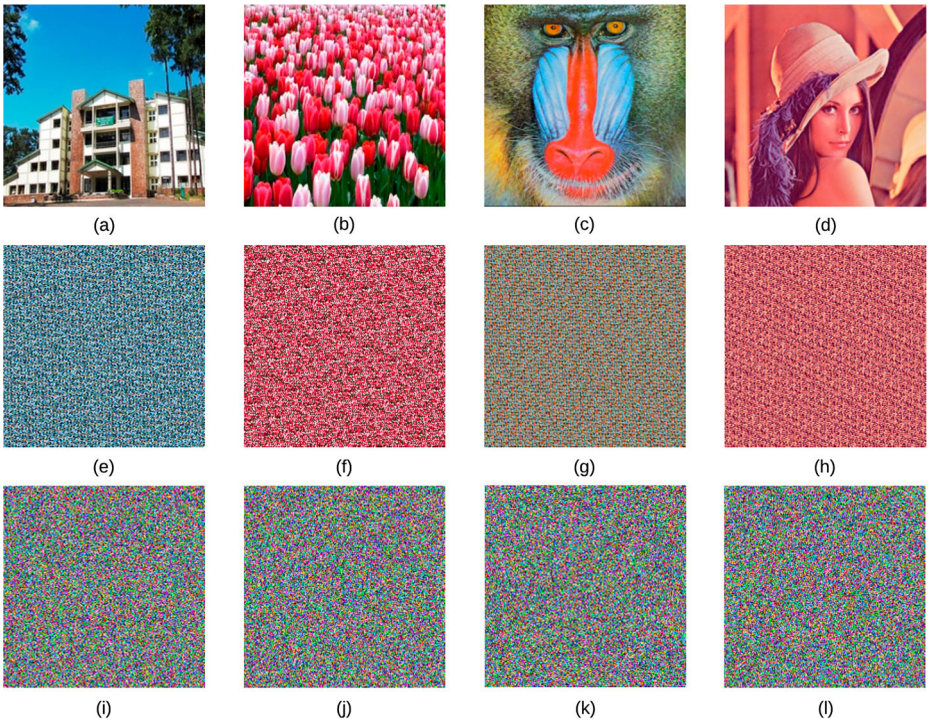

Fig. 3 (**a-d**) Plain images of Nehu, Tulip, Baboon, and Lena; (**e-h**) Scrambled images; (**i-l**) Cipher images

Table 1 Results of PSNR and SSIM

Test images	Encrypted image		Decrypted image	
	PSNR	SSIM	PSNR	SSIM
Nehu	8.129861	0.0148609	Infinity (∞)	1
Tulip	7.597365	0.0019662	Infinity (∞)	1
Baboon	9.139676	0.0042376	Infinity (∞)	1
Lena	8.746787	0.0097224	Infinity (∞)	1

system is operated on Matlab 2016, Mathematica 10, SageMath Version 7.0, and GCC-4.8. It may be noted that (512 $\times$ 512) cipher images are considered in the paper. But the sake of simplicity, (201 $\times$ 201) dimension images have been shown in the article. In order to assess the plain image and cipher image quality, two important metrics, namely structural similarity (SSIM) index, and Peak signal-to-noise ratio (PSNR) have been measured and shown in Table 1.

In this section, we have presented histogram, correlation coefficient, entropy, and Chi-square test for the proposed cryptosystem.

4.1 Histogram analysis

In digital image processing, the histogram of an image usually indicates the frequency distribution of the pixel intensity values. Cryptographic primitive is intended to make good cipher image which comprises the uniform distribution of pixel intensity values. Thus the attacker is unable to obtain valuable data from the cipher image. Figure 4 illustrates the histogram plot of plain images, and its corresponding cipher images.

4.2 Correlation coefficient

The Correlation coefficient signifies the correlation or similarity among two adjacent pixels in the digital image. Usually, image pixels are extremely repetitive, so they have a large correlation among adjacent pixels. In that regard, the cipher image should be produced in such a way that the image has a low correlation among the adjacent pixels and it would be hard to recognize the similarity between the pixel contents by the attacker. It is measured as follows:

$$Corr_{(X,Y)} = \frac{Cov\,(X,Y)}{St.\,Dev\,(X) \times St.\,Dev\,(Y)} \tag{6}$$

where,

$$Cov(X,Y) : \text{covariance of } X, Y$$

The correlation coefficients results of the plain images and cipher images are tabulated in Table 2. The tabulated results are close to zero that indicates there is no correlation among the adjacent pixels of the cipher images in horizontal, vertical, and diagonal areas. Correlation plot for plain and cipher Baboon image along horizontal, vertical, and diagonal element are illustrated in Fig. 5a-f.

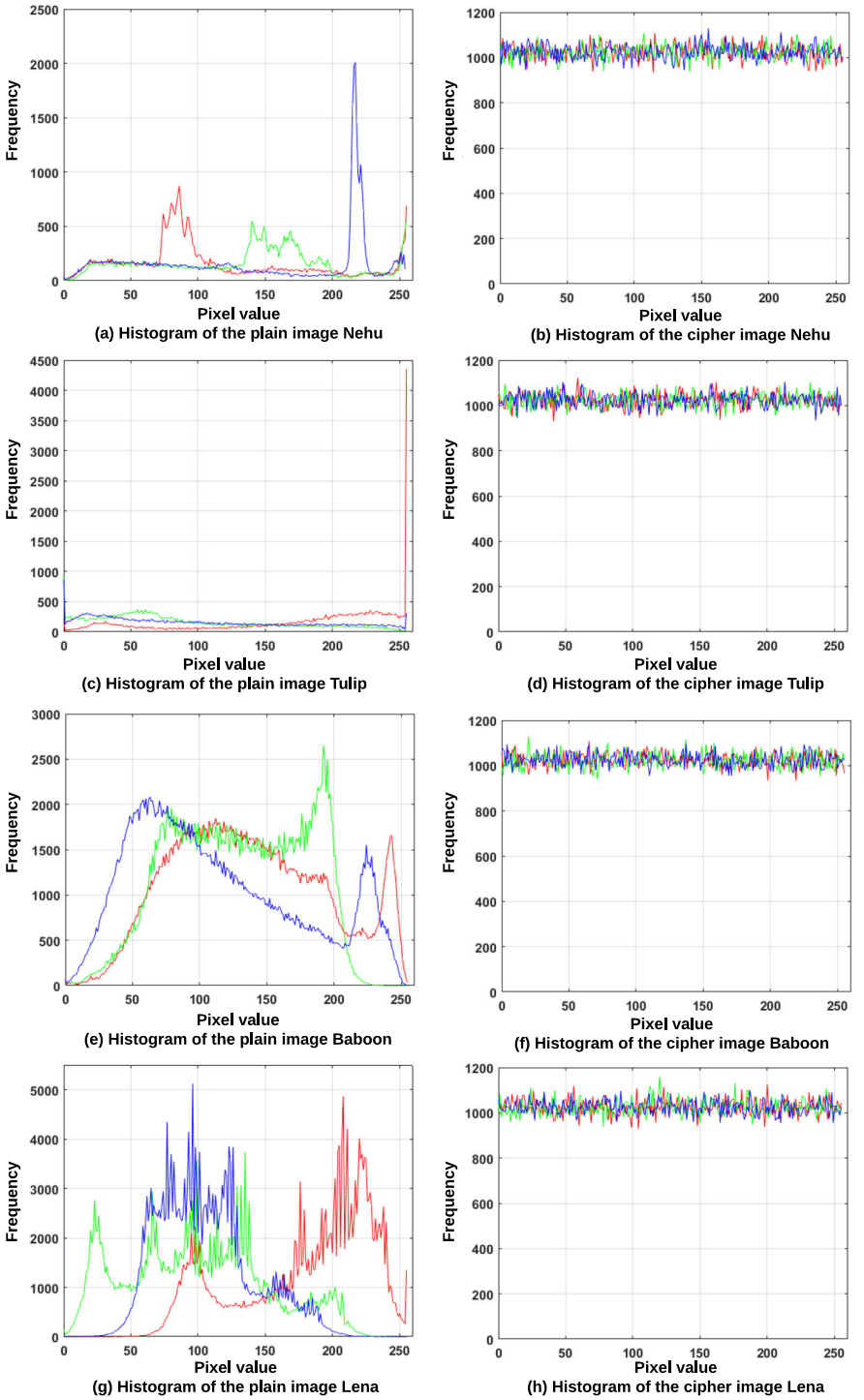

Fig. 4 Histogram plot for plain and cipher images

Table 2 Results of correlation coefficients (CC) of the plain images and cipher images

	CC	Plain images				Encrypted images			
		Nehu	Tulip	Baboon	Lena	Nehu	Tulip	Baboon	Lena
R	HC	0.8992	0.8889	0.9284	0.9373	0.0046	0.0014	0.0019	0.0031
	VC	0.9296	0.9564	0.9125	0.9688	−0.0049	−0.0069	−0.0013	−0.0039
	DC	0.8458	0.8622	0.8868	0.9066	0.0039	−0.0011	0.0054	0.0073
G	HC	0.8884	0.8236	0.8835	0.9195	−0.0071	0.0071	0.0013	0.006
	VC	0.9207	0.9297	0.8617	0.9589	−0.0094	0.0043	0.0038	−0.0031
	DC	0.8286	0.7776	0.8171	0.8903	−0.0043	−0.0028	−0.0044	−0.0102
B	HC	0.9243	0.8616	0.9310	0.9049	−0.0031	0.0041	0.0026	−0.0065
	VC	0.9451	0.9453	0.9234	0.9405	0.0071	−0.003	0.0031	0.001
	DC	0.8829	0.8269	0.8931	0.8715	0.0037	−0.0097	0.004	−0.0001

R = Red; G = Green; B = Blue; HC = Horizontal correlation; VC = Vertical correlation; DC = Diagonal correlation

4.3 Information entropy

Shannon proposed the fundamental notion of information entropy, and it is reported in [35]. It can be defined as follows:

$$H(X) = -N \sum_{i=1}^{N} p(x_i)\, log_2\ p(x_i) \tag{7}$$

where, $p(x_i)$ is the probability mass function. In data communications, the word 'entropy' associates to the relative degree of randomness. Thus, a high value of the entropy indicates

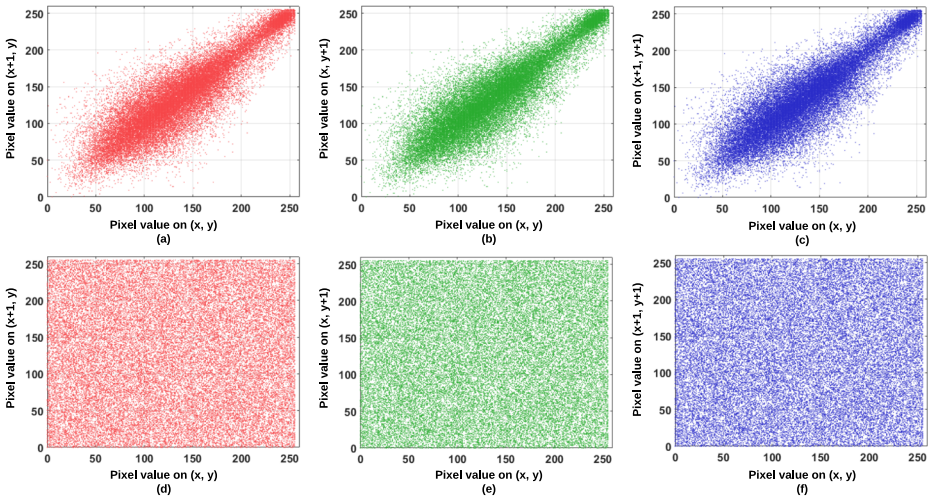

Fig. 5 Distributions of adjacent pixel pairs of the Baboon plain image and cipher image. (**a-c**) depicts the horizontal, vertical, and diagonal pixel distribution of the Baboon plain image; (**d-f**) corresponding cipher image regions

Table 3 Entropy evaluation

Test images	Channel	Plain images	Cipher images
Nehu	R	7.5616	7.9994
	G	7.6679	7.9991
	B	7.5257	7.9993
Tulip	R	7.4676	7.9994
	G	7.7342	7.9992
	B	7.8800	7.9991
Baboon	R	7.5077	7.9992
	G	7.2142	7.9993
	B	7.5264	7.9991
Lena	R	7.2018	7.9994
	G	7.4867	7.9994
	B	6.9168	7.9991

the high-level of randomness. Table 3 summarizes the entropy results of plain images and the corresponding cipher images.

4.4 Chi-square test

Chi-square test measuring the difference between the observed and the expected result to evaluate the statistical value of the uniform distribution of pixels in the cipher image. There is a well-known equation for measuring this Chi-square test (χ^2):

$$\chi^2 = \sum_{i=0}^{255} \frac{(O_i - E_i)^2}{E_i} \tag{8}$$

where,

O_i : observed intensity distribution of each gray level (0-255)
E_i : expected intensity distribution of each gray level (0-255)

In this test, $\alpha = 0.05$ value has been preferred for the significance level, which is the default value for the Chi-square test. Next, the Chi-square values of the different size cipher images are tabulated in Table 4. Chi-square test reveals that the cipher image produces a uniform distribution of pixel values.

Table 4 Chi-square test result

Size of the image	Chi sq. (χ^2) value	Decision
Lena (201 × 201)	279.63384836667	✓
Nehu (256 × 256)	271.37352906667	✓
Baboon (256 × 256)	269.52426903333	✓
Lena (512 × 512)	249.8807171	✓

✓ = Accepted

5 Security and performance analysis

This section provides known and chosen-plaintext attack, key sensitivity test, differential attack, noise attacks, occlusion attack, NIST randomness test, encryption time, and ECDH performance analysis.

5.1 Known and chosen-plaintext attack

In the chosen plaintext attack, an attacker can choose random plaintext data to encrypt and get the ciphertext. After achieving good cryptographic results also, a few image encryption systems have been vulnerable to known and chosen-plaintext attacks [20]. In the suggested scheme, firstly the plain image pixel has been randomized by the Logistic map and further, it has been scrambled by Arnold's scrambling technique. Next, the highly random keystream is used for cipher image generation. Therefore, it is extremely difficult for an attacker to obtain any information from plain and cipher image. Hence, it can be claimed that the proposed encryption system efficiently resists known-plaintext and chosen-plaintext attacks.

5.2 Key analysis

Key analysis is used to show the sensitivity of the image encryption scheme for the input key. A small level of difference in the key may produce a severe difference in the output image. Kerckhoffs stated [21]: `'A cryptosystem should be secure even if everything about the system, except the key, is public knowledge'`. In general, the bigger keyspace helps to resist the ciphers Brute force attack. In this scheme, 512-bit key has been used. That signifies 2^{512} keyspace of the proposed scheme has enough capability to resist the Brute force attack.

Typically, the key sensitivity analysis of the cryptosystem can be judged by two phases: (a) solely modified plain image should be obtained while slightly altered keys are used to decrypt the same cipher image; (b) the cipher image should not be extracted in the correct manner if there is a small change between the encryption and decryption keys.

In order to evaluate the key sensitivity test, two types of faulty key has been used which is simply (i) a bit and (ii) a word changed from the original key of the recipient. As seen from Fig. 6, that the proposed scheme performs no similarity between the original cipher image and wrong decipher image.

5.3 Differential attack

In general, NPCR and UACI are used to compute the differential attack resistance of the cryptographic system. Specifically, NPCR means the rate of variation of pixel position

Fig. 6 Key sensitivity test. (**a**) Plain image; (**b**) corresponding cipher image; (**c**) decryption with original key; (**d**) decryption with one bit changes in the original key; and (**e**) decryption with one word changes in the original key

between the original and the cipher image, and UACI represented as the variations in average intensity rates among the plain and cipher image. The NPCR and UACI formulas are specified as follows:

$$NPCR = \frac{\sum_{(\iota,\jmath)} D(\iota,\jmath)}{width\ (w) \times height\ (h)} \times 100\% \tag{9}$$

$$UACI = \frac{1}{(w) \times (h)} \left[\sum_{(\iota,\jmath)} \frac{P_1(\iota,\jmath) - P_2(\iota,\jmath)}{255} \right] \times 100\% \tag{10}$$

where,

$$D(\iota,\jmath) = \begin{cases} 0\ when\ P_1(i,j) = P_2(i,j) \\ 1\ when\ P_1(i,j) \neq P_2(i,j) \end{cases} \tag{11}$$

The NPCR and UACI results are tabulated in Table 5, and it is observed that the proposed scheme has the ability to avoid the differential attack.

5.4 Noise attack analysis

Noise attack is one of the powerful attacks for the cipher image. If anyone imposes high noise on the cipher image, it would be very difficult to obtain the original image. In order to evaluate the robustness test of the proposed scheme against noise attacks, two types of noises, namely the Gaussian, salt and pepper are applied in the encrypted images. The data obtained from the experiments are presented in the following parts.

5.4.1 Gaussian noise

This part measures the robustness test, i.e., how the proposed scheme is resisting against the four variances of Gaussian noise. Figure 7a-d shows the Baboon cipher images, **(e-h)** Baboon decrypted images, and **(i-l)** Nehu decrypted images. As seen from Fig. 7, that if the attacker attaches different parameters of noises (like 0.01, 0.02, 0.03, and 0.05), the proposed scheme has the capability to recover the maximum information of the image.

5.4.2 Salt and pepper attack

This noise is popular as impulse noise. Here, the noise can be affected by sharp and unexpected interruptions inside the image signal. The performance of the cipher image has been evaluated using various levels of salt and pepper noise. After imposing 10%, 20%, 30%, and 50% salt and pepper noise, it is capable of recovering the original images, as shown in Fig. 8.

Table 5 NPCR and UACI values

Channel	Metrics	Nehu	Tulip	Baboon	Lena
R	NPCR	99.55941	99.54209	99.64109	99.61139
	UACI	33.02935	33.95504	33.46354	33.99944
G	NPCR	99.62624	99.56932	99.58169	99.59901
	UACI	33.22466	33.88935	33.46354	33.63769
B	NPCR	99.59407	99.62130	99.66089	99.58664
	UACI	33.69788	33.37182	33.46354	33.62594

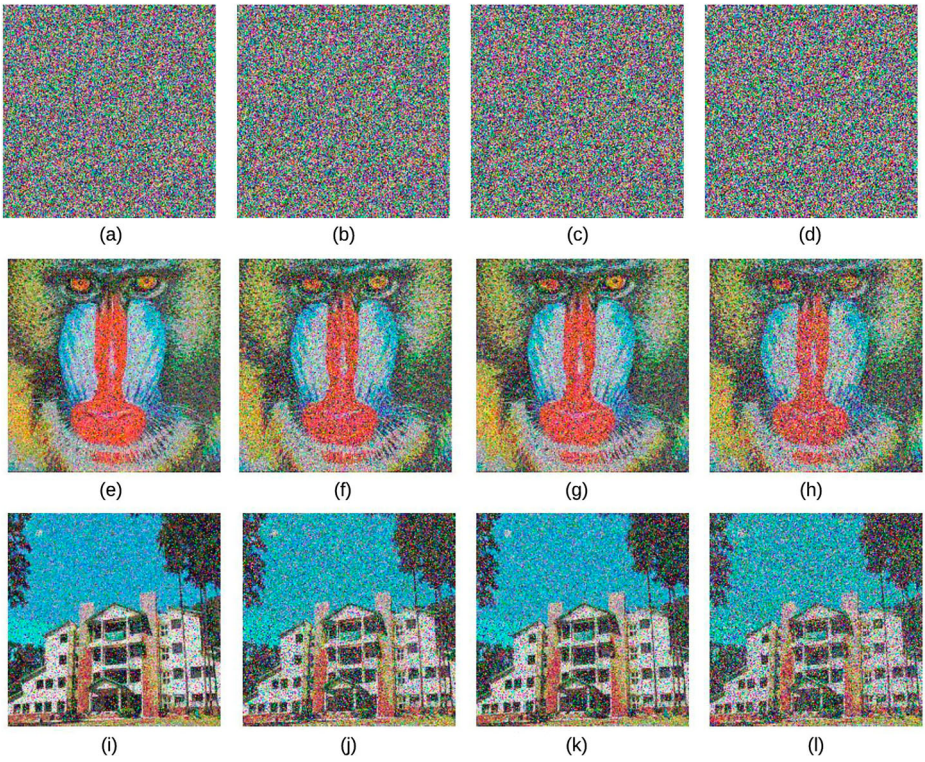

Fig. 7 Different forms of encrypted and decrypted images under Gaussian noise attack. **(a)** Baboon Cipher image added noise with mean = 0, variance = 0.01; **(b)** cipher image added noise with mean = 0, variance = 0.02; **(c)** cipher image added noise with mean = 0, variance = 0.03; and **(d)** cipher image added noise with mean = 0, variance = 0.05. **(e-h)** decrypted images of Baboon; and **(i-l)** decrypted images of Nehu

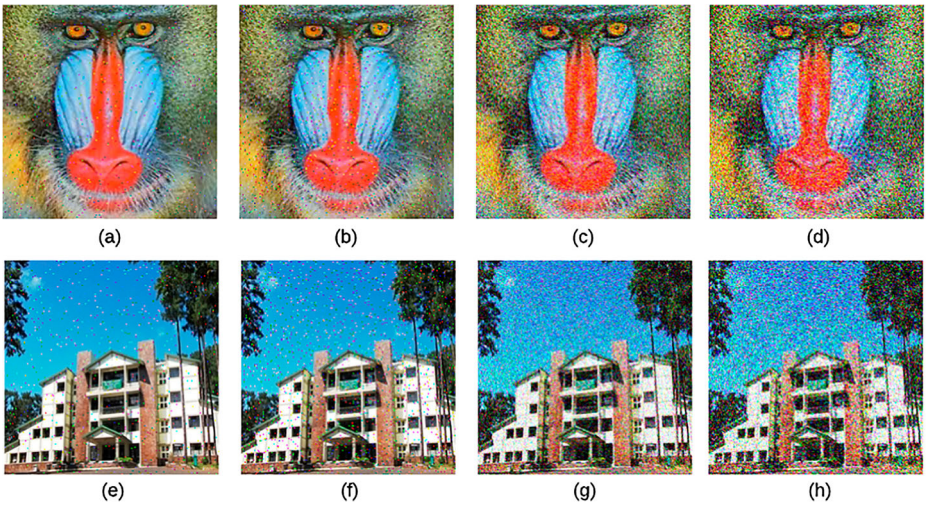

Fig. 8 Different forms of decrypted images under salt and pepper noise attack. The cipher image added with 10%, 20%, 30%, and 50% noise. (**a, e**) decrypted images with 10% noise; (**b, f**) decrypted images with 20% noise; (**c, g**) decrypted images with 30% noise; and (**d, h**) decrypted images with 50% noise

5.5 Occlusion attack

When the sender send some images and if knowingly or unknowingly, some portion of the image pixel values are dissipated is known as occlusion attack. To evaluate the proposed scheme, different levels of occlusions (like 6.25%, 12.5%, 25%, and 50%) are tempered with the encrypted images. Figure 9i-l illustrates the decrypted images of Fig. 9a-d, respectively. As seen from Fig. 9, that even after contaminated by different levels of occlusions, the plain image can be recovered to some extent.

Different noise variances against PSNR (dB) results are plotted graphically, and shown in Fig. 10. Further, Mean square error (MSE) and SSIM results for the different types of noise attacks are tabulated in Table 6. From the result, it is clear that the mentioned attacks unable to affect the proposed scheme.

5.6 Randomness analysis

The randomness test plays a vital role in the design of cryptosystem because it easily detects the weaknesses of the crypto structure. Randomness test of the selected cipher images has been carried out by NIST test suite [34]. For randomness test, at least 10^6 (1 Million) keystream is required from cipher image pixel value. The result of the randomness test is analyzed by *P*-value. Throughout the test, the *P*-value is evaluated, if the *P*-value is less than

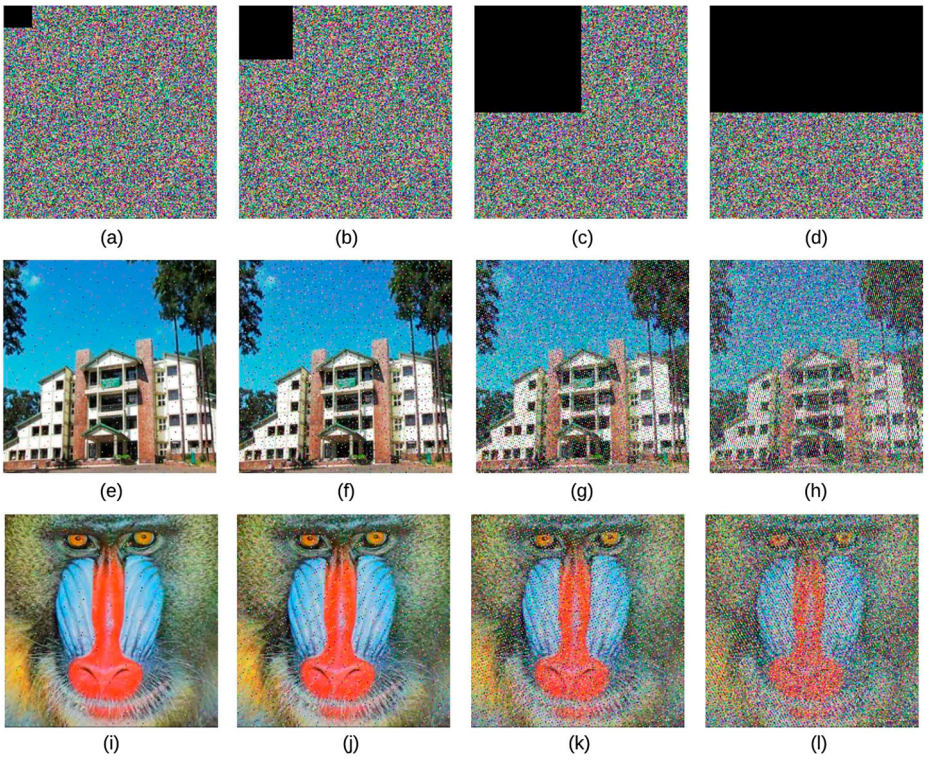

Fig. 9 Cipher and decrypted images under occlusion attack. **(a-d)** cipher images with occlusion levels 6.25%, 12.5%, 25%, and 50%; **(e-h)** decrypted images of Nehu; **(i-l)** decrypted images of Baboon

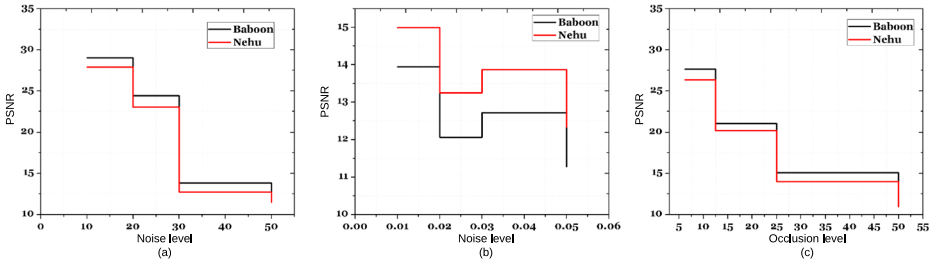

Fig. 10 PSNR results. (**a**) salt and pepper noise; (**b**) Gaussian noise; and (**c**) occlusion attack

0.01, then the selected keystream is supposed to be non-random else it is judged to be random. NIST test suite consists of 15 different statistical tests. NIST randomness test results of cipher images are elaborated in Table 7.

5.7 Encryption time

Computational speed is very much important for real-time encryption system. The configuration of the system is as follows: Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz, 3408 MHz, 4 Core(s), 8 Logical processor(s). The encryption time requirement is measured by the sum of time spent during wfsr random number generation, XOR operation of wfsr keystream sequence with scrambled image bitstream, and parameter initialization. The average encryption time (in seconds) taken by the algorithm for (512 × 512) sized image is presented in Table 8.

Table 6 SSIM and MSE values for different levels of noises

Types	SSIM		MSE	
	Baboon	Nehu	Baboon	Nehu
Occlusion level				
6.25%	0.01005	0.01181	8130.80	10438.48
12.5%	0.00951	0.01060	8532.07	10992.91
25%	0.00880	0.00778	10161.94	13974.43
50%	0.00607	0.00345	13060.83	15625.39
Salt and pepper				
10%	0.00849	0.01090	9107.49	11479.26
20%	0.00821	0.00976	10197.60	12583.47
30%	0.00800	0.00438	11272.02	13702.83
50%	0.00746	0.00627	13389.25	15849.94
Gaussian noise				
0.01	0.008970	0.011269	8323.22	10677.69
0.02	0.010229	0.012780	8823.86	11176.07
0.03	0.009559	0.011568	9247.06	11627.31
0.05	0.008715	0.010808	8594.51	10935.11

Table 7 Cipher images randomness test result using NIST test suite

Name of the test	*P*-value				Result
	Nehu	Tulip	Baboon	Lena	
Frequency	0.275709	0.015598	0.834308	0.401199	Pass
Block frequency	0.181557	0.023545	0.042808	0.289667	Pass
Cumulative sums	0.494392	0.249284	0.401199	0.474986	Pass
Runs	0.025193	0.534146	0.003996	0.595549	Pass
Longest run	0.181557	0.001030	0.181557	0.494392	Pass
Rank	0.003274	0.074903	0.012650	0.008266	Pass
FFT	0.350485	0.010988	0.108791	0.005358	Pass
Non overlapping template	0.366918	0.574903	0.262249	0.108791	Pass
Overlapping template	0.108791	0.739918	0.437274	0.678686	Pass
Universal	0.851383	0.289667	0.249284	0.051942	Pass
Approximate entropy	0.181557	0.366918	0.474986	0.275709	Pass
Serial1	0.699313	0.514124	0.129620	0.719747	Pass
Serial2	0.437274	0.964295	0.289667	0.657933	Pass
Linear complexity	0.554420	0.275709	0.574903	0.816537	Pass
Random excursions					
$x = -4$	0.851383	0.719747	0.334538	0.383827	Pass
$x = -3$	0.574903	0.366918	0.080519	0.883171	Pass
$x = -2$	0.867692	0.262249	0.678686	0.102526	Pass
$x = -1$	0.637119	0.759756	0.122325	0.779188	Pass
$x = 1$	0.025193	0.162606	0.574903	0.834308	Pass
$x = 2$	0.090936	0.115387	0.213309	0.401199	Pass
$x = 3$	0.055361	0.455937	0.026948	0.224821	Pass
$x = 4$	0.162606	0.657933	0.071177	0.350485	Pass
Random excursions variant					
$x = -9$	0.574903	0.048716	0.574903	0.851383	Pass
$x = -8$	0.554420	0.011791	0.816537	0.534146	Pass
$x = -7$	0.574903	0.115387	0.574903	0.514124	Pass
$x = -6$	0.534146	0.137282	0.304126	0.911413	Pass
$x = -5$	0.115387	0.249284	0.997823	0.911413	Pass
$x = -4$	0.657933	0.798139	0.262249	0.350485	Pass
$x = -3$	0.048716	0.181557	0.719747	0.595549	Pass
$x = -2$	0.514124	0.574903	0.419021	0.739918	Pass
$x = -1$	0.275709	0.678686	0.224821	0.137282	Pass
$x = 1$	0.994250	0.816537	0.162606	0.616305	Pass
$x = 2$	0.955835	0.289667	0.719747	0.897763	Pass
$x = 3$	0.236810	0.494392	0.834308	0.678686	Pass
$x = 4$	0.851383	0.699313	0.494392	0.122325	Pass
$x = 5$	0.719747	0.350485	0.595549	0.798139	Pass
$x = 6$	0.678686	0.851383	0.657933	0.514124	Pass
$x = 7$	0.779188	0.455937	0.534146	0.262249	Pass
$x = 8$	0.964295	0.798139	0.574903	0.534146	Pass
$x = 9$	0.595549	0.366918	0.213309	0.657933	Pass

Table 8 Encryption time requirement

Image size	Ours	Ref. [25]	Ref. [2]	Ref. [5]	Ref. [9]
(512 × 512) color image	0.0745	0.3436	0.395	0.739	0.155

5.8 Performance analysis of ECDH

In a generic way, the proposed scheme has shown that digital envelope has used for key exchange among sender and receiver. Usually, RSA, Diffie-Hellman, ECDH, Curve25519, etc., are some common public key protocols generally considered for key exchange. But, in the proposed scheme, the key exchange protocol needs to be lightweight. The ECDH key sharing protocol [13] is normally much faster than other conventional public key systems. Additionally, ECDH has some benefits in terms of key length and secure performance. The elliptic curve discrete logarithm problem (ECDLP) [26] is assumed to be a hard problem by the state of till date best practices technology. But still, there are a few uncertainties linked with it because of the lack of mathematical proof.

In this experimental work, ECDH has been implemented in C language. Moreover, key exchange time performances have been analyzed by two important attainable parameters, namely encryption time and decryption time. Experimental results are tabulated in Table 9. Specifically, the proposed method uses 512-bit lengths key in ECDH, which requires in total 0.150202 seconds for encryption and decryption.

6 Comparison

This section highlights the performance of the proposed system compared with state-of-the-art schemes [2, 3, 5, 9, 10, 20, 25, 29, 32]. Table 10 shows the comparison result of some important performance metrics such as entropy, NPCR, UACI, and correlation coefficient (in terms of HC, VC, DC). As seen from Table 10, proposed scheme performance metrics results are better and close to the recent schemes. Projected system security is enhanced by wfsr, which is designed as a high-quality pseudo-random number generator. Despite this pseudo-random behavior, the system can maintain a proper balance between robustness and computational performance. Regarding the computation cost as one of the tools to resolve the complexity of the system; Table 8 reveals that the proposed system is faster than the schemes of [2, 5, 9, 25] for encryption speed. Compared to Ref. [2, 5, 9, 25] key sharing time has not considered while it has been addressed in the proposed method and shown in

Table 9 Time requirement for Key sharing using ECDH

Key size	Total time (sec.)	Encryption time (sec.)	Decryption time (sec.)
64-bit	0.036943	0.030422	0.006521
128-bit	0.047524	0.035330	0.012194
256-bit	0.091032	0.071235	0.019797
512-bit	0.150202	0.110397	0.039805
1024-bit	0.253473	0.193957	0.059516
2048-bit	0.485423	0.376057	0.109366

Table 10 Entropy, NPCR, UACI, and correlation results of different image encryption schemes

Scheme		Entropy	NPCR	UACI	HC	VC	DC
Ref. [32]	R	7.9953	99.88	33.49	0.0682	−0.0840	0.0092
	G	7.9953	99.88	33.49	0.0682	−0.0840	0.0092
	B	7.9953	99.88	33.49	0.0682	−0.0840	0.0092
Ref. [25]	R	7.9992	99.5	33.3	−0.0031	0.0055	−0.0060
	G	7.9992	99.5	33.3	−0.0067	−0.0048	0.0127
	B	7.9992	99.5	33.3	−0.0005	−0.0016	−0.0041
Ref. [20]	R	7.9993	99.59	33.45	0.0363	−0.0002	−0.0002
	G	7.9993	99.59	33.38	−0.0008	0.0139	−0.0006
	B	7.9994	99.60	33.46	−0.0092	0.0011	−0.0101
Ref. [29]	R	7.9896	99.62	33.47	0.0007	0.0018	0.0037
	G	7.9893	99.63	33.56	0.0007	0.0018	0.0037
	B	7.9896	99.61	33.33	0.0007	0.0018	0.0037
Ref. [2]	R	7.9896	99.5	33.3	0.0010	0.0017	0.0125
	G	7.9896	99.5	33.3	0.0010	0.0017	0.0125
	B	7.9896	99.5	33.3	0.0010	0.0017	0.0125
Ref. [3]	R	7.9997	99.5	33.3	0.0002	0.0061	0.0004
	G	7.9997	99.5	33.3	0.0002	0.0061	0.0004
	B	7.9997	99.5	33.3	0.0002	0.0061	0.0004
Ref. [10]	R	7.9993	99.63	33.67	−0.0283	−0.0317	−0.0344
	G	7.9990	99.62	33.79	−0.0026	−0.0173	−0.0015
	B	7.9989	99.62	33.62	−0.0217	−0.0036	−0.0191
Ref. [5]	R	7.9997	99.61	33.69	–	–	–
	G	7.9997	99.65	34.32	–	–	–
	B	7.9997	99.64	32.23	–	–	–
Ref. [9]	R	7.9030	99.58	33.46	−0.0294	−0.0014	−0.0180
	G	7.9030	99.58	33.46	−0.0294	−0.0014	−0.0180
	B	7.9030	99.58	33.46	−0.0294	−0.0014	−0.0180
Ours	R	7.9994	99.61	33.99	0.0031	−0.0039	0.0073
	G	7.9994	99.59	33.63	0.0060	−0.0031	−0.0102
	B	7.9991	99.58	33.62	−0.0065	0.0010	−0.0001

Table 9. Therefore, the comparative evaluation assures that the performance of the proposed system has the ability to maintain the trade-off between high security with computational complexity.

7 Conclusions

The proposed method is an efficient and secure image encryption scheme. A three-level image encryption method is implemented where first two levels namely Logistic map and Arnold's scrambling are used for the randomization of pixel values, and third-level encrypt the pixel values by the keystream generated by a special wfsr. The wfsr offers not only fast software encryption but also provides high-quality pseudorandom sequences with desired

level statistical properties. Next, the ECDH scheme has been suggested for the image encryption key sharing. Simulations and performance evaluations showed that the scheme requires lower time complexity in encryption and key sharing. Detailed statistical analyses like entropy, correlation coefficient, keyspace, key sensitivity, NIST randomness test were carried out to show the effectiveness of the proposed system. The various security analyses show that the proposed scheme can resist many attacks like known and chosen-plaintext attack, differential attack, different types of noise attacks. Further, some important metrics are compared with state-of-the-art schemes, and the proposed method exhibits superior performance. Therefore, the proposed system has good prospects in real-time multimedia-based applications.

Acknowledgements The authors would like to thank Dr. P. Praveenkumar and Dr. Sartaj Ul Hasan for suggesting the problem and for discussions. We are also thankful to the editor and the anonymous reviewers for the useful comments and it has immensely helped us to significantly improve both technical and editorial quality of the manuscript.

Appendix A: wfsr details

Note for Test Vectors: In [42, B, Page No. -13], all the polynomial equations are listed. As mentioned earlier, 32-bit wfsr has been considered. Initially, 16 blocks of Hex value (i.e., $16 \times 32 = 512$ bit key/seed value) are loaded in the wfsr and as shown in below.

```
0x810204ce, 0x5632fb81, 0x8396f478, 0x1720c1f2, 0x84789fc4, 0x10a1c396,
0x85fa1028, 0x5720c081, 0x83041c33, 0x70404eb1, 0xa494bc18, 0xef408561,
0x81020808, 0x102fca96, 0xbce85637, 0x04568521.
```

Appendix B: PSNR, MSE, and SSIM

$$\text{PSNR} = 1 - \log_{10}[m \times n]\frac{1}{\text{MSE}} \tag{12}$$

where,

$m \times n$: image size

$$\text{MSE} = \frac{1}{m \times n}\sum_{i=0}^{m-1}\sum_{i=0}^{n-1}\left[I_{i,j} - K_{i,j}\right]^2 \tag{13}$$

where,

$I_{i,j}$: plain image pixel
$K_{i,j}$: cipher image pixel

$$\text{SSIM}_{x,y} = \frac{(2\eta_x\eta_y + l_1)(2\tau_{xy} + l_2)}{(\eta_x^2 + \eta_y^2 + l_1)(\tau_x^2 + \tau_y^2 + l_2)} \tag{14}$$

where,

η_x : Average of x
η_y : Average of y
τ_{xy} : Covariance of x, y

τ_x : St. Dev of x
τ_y : St. Dev of y
ε_1 : 0.01
ε_2 : 0.03
l_1 : $(\varepsilon_1 b)^2$
l_2 : $(\varepsilon_2 b)^2$
b : $2^{\text{Number of bits per pixel}} - 1$

References

1. Abd EL-Latif AA, Abd-El-Atty B, Venegas-Andraca SE (2019) A novel image steganography technique based on quantum substitution boxes. Opt Laser Technol 116:92–102
2. Abd El-Latif AA, Niu X (2013) A hybrid chaotic system and cyclic elliptic curve for image encryption. AEU-Int J Electron C 67(2):136–143
3. Abd El-Latif AA, Li L, Niu X (2014) A new image encryption scheme based on cyclic elliptic curve and chaotic system. Multimed Tools Appl 70(3):1559–1584
4. Abd El-Latif AA, Li L, Wang N, Peng J-L, Shi Z-F, Niu X (2012) A new image encryption scheme for secure digital images based on combination of polynomial chaotic maps Research Journal of Applied Sciences. Eng Technol 4(4):322–328
5. Abd El-Latif AA, Li L, Wang N, Qi H, Niu X (2013) A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. Signal Process 93(11):2986–3000
6. Aïssa B, Nadir D, Mohamed R (2013) Image encryption using stream cipher based on nonlinear combination generator with enhanced security. New Trends in Mathematical Sciences 1(1):10–19
7. 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
8. Abd El-Latif AA, Wang N, Peng J-L, Li Q, Niu X (2013) A new encryption scheme for color images based on quantum chaotic system in transform domain. In: Fifth International Conference on Digital Image Processing (ICDIP 2013), vol 8878. International society for optics and photonics, pp 88781s
9. Belazi A, Abd El-Latif AA, Diaconu A-V, Rhouma R, Belghith S (2017) Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Opt Lasers Eng 88:37–50
10. Belazi A, Khan M, Abd El-Latif AA, Belghith S (2017) Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption. Nonlinear Dyn 87(1):337–361
11. Benrhouma O, Hermassi H, Abd El-Latif AA, Belghith S (2015) Cryptanalysis of a video encryption method based on mixing and permutation operations in the dct domains. SIViP 9(6):1281–1286
12. Bishoi SK, Haran HK, Ul Hasan S (2017) A note on the multiple-recursive matrix method for generating pseudorandom vectors. Discret Appl Math 222:67–75
13. Bos JW, Alex Halderman J, Heninger N Jonathan Moore, Michael Naehrig, and Eric Wustrow. Elliptic curve cryptography in practice. Cryptology ePrint Archive, Report 2013/734, 2013. Available: https://eprint.iacr.org/2013/734
14. Chai X, Yang K, Gan Z (2017) A new chaos-based image encryption algorithm with dynamic key selection mechanisms. Multimed Tools Appl 76(7):9907–9927
15. Chen J, Zhu Z-l, Zhang L-b, Zhang Y, Yang B-q (2018) Exploiting self-adaptive permutation–diffusion and dna random encoding for secure and efficient image encryption. Signal Process 142:340–353
16. Das P, Deb S, Kar N, Bhattacharya B (2015) An improved dna based dual cover steganography. Procedia Computer Science 46:604–611
17. Deb S, Bhuyan B, Ch. Gupta N (2018) Design and analysis of lfsr-based stream cipher. In: Mandal JK, Saha G, Kandar D, Maji AK (eds) Proceedings of the International Conference on Computing and Communication Systems. Springer, Singapore, pp 631–639
18. Dzwonkowski M, Papaj M, Rykaczewski R (2015) A new quaternion-based encryption method for dicom images. IEEE Trans Image Process 24(11):4614–4622
19. Fridrich J (1998) Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurcation Chaos 8(06):1259–1284
20. Gan Z, Chai X, Zhang M, Yang L (2018) A double color image encryption scheme based on three-dimensional brownian motion. Multimed Tools Appl 77(21):27919–27953
21. Kerckhoffs A (1883) La cryptographic militaire. Journal des Sciences Militaires IX:5–38
22. Kocarev L (2001) Chaos-based cryptography: a brief overview. IEEE Circuits Syst Mag 1(3):6–21

23. Kumar P, Rana SB (2016) Development of modified aes algorithm for data security. Optik-International Journal for Light and Electron Optics 127(4):2341–2345
24. Kumar M, Iqbal A, Kumar P (2016) A new rgb image encryption algorithm based on dna encoding and elliptic curve diffie–hellman cryptography. Signal Process 125:187–202
25. Laiphrakpam DS, Khumanthem MS (2018) A robust image encryption scheme based on chaotic system and elliptic curve over finite field. Multimed Tools Appl 77(7):8629–8652
26. Lauter KE, Stange KE The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences. Cryptology ePrint Archive, Report 2008/099, 2008. Available: https://eprint.iacr.org/2008/099
27. Li L, Abd ElLatif AA, Qi H, Niu X (2012) An improved additively homomorphic image encryption scheme based on elliptic curve elgamal. International Journal of Advancements in Computing Technology 4:223–230
28. Liu W, Sun K, Zhu C (2016) A fast image encryption algorithm based on chaotic map. Opt Lasers Eng 84:26–36
29. Liu H, Kadir A (2015) Asymmetric color image encryption scheme using 2d discrete-time map. Signal Process 113:104–112
30. Meenpal T, Banik S, Maitra S (2017) A scheme for conditional access-based systems using index locations of dct coefficients. J Real-Time Image Proc 13(2):363–373
31. Praveenkumar P, Amirtharajan R, Thenmozhi K, Rayappan JBB (2015) Medical data sheet in safe havens–a tri-layer cryptic solution. Comput Biol Med 62:264–276
32. Praveenkumar P, Kerthana Devi N, Ravichandran D, Avila J, Thenmozhi K, Rayappan JBB, Amirtharajan R (2018) Transreceiving of encrypted medical image–a cognitive approach. Multimed Tools Appl 77(7):8393–8418
33. Roy S, Pal AK (2018) An svd based location specific robust color image watermarking scheme using rdwt and arnold scrambling. Wirel Pers Commun 98(2):2223–2250
34. Rukhin A, Soto J, Nechvatal J, Smid M, Barker E (2001) A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, National Institute of Standards and Technology
35. Shannon CE (1948) A mathematical theory of communication. Bell Syst Tech J 27(3):379–423
36. Teng L, Wang X (2012) A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive. Opt Commun 285(20):4048–4054
37. Ul Hasan S, Panario D, Wang Q (2018) Nonlinear vectorial primitive recursive sequences. Cryptogr Commun 10(6):1075–1090
38. Wang L, Dong T, Ge M-F (2019) Finite-time synchronization of memristor chaotic systems and its application in image encryption. Appl Math Comput 347:293–305
39. Wang X, Teng L, Qin X (2012) A novel colour image encryption algorithm based on chaos. Signal Process 92(4):1101–1108
40. Zaghloul A, Zhang T, Hou H, Amin M, Abd El-Latif AA, Abd El-Wahab MS (2014) A block encryption scheme for secure still visual data based on one-way coupled map lattice. International Journal of Security and Its Applications 8(4):89–100
41. Zaghloul A, Zhang T, Amin M, Abd El-Latif AA (2014) Color encryption scheme based on adapted quantum logistic map. In: Sixth International Conference on Digital Image Processing (ICDIP 2014), vol 9159. International Society for Optics and Photonics, pp 915922
42. Zeng G, Han W, He K High efficiency feedback shift register: $\sigma-$lfsr. Cryptology ePrint Archive, Report 2007/114, 2007. Available: https://eprint.iacr.org/2007/114
43. Zhang TJ, Abd El-Latif AA, Amin M, Zaghloul A (2014) Diffusion-substitution mechanism for color image encryption based on multiple chaotic systems. In: Electronic Engineering and Information Science, vol. 981 of Advanced Materials Research, pp 327–330. Trans Tech Publications Ltd 8
44. Zhang Y, Di X (2013) Double optical image encryption using discrete chirikov standard map and chaos-based fractional random transform. Opt Lasers Eng 51(4):472–480
45. Zhang T, El-Fatyany A, Li L, Amin M, Abd El-Latif AA (2015) Secret sharing-based chaotic image encryption. International Journal of Security and Its Applications 9(7):217–224
46. Zhang TJ, Manhrawy IM, Abdo AA, Abd El-Latif AA, Rhouma R (2014) Cryptanalysis of elementary cellular automata based image encryption. In: Electronic Engineering and Information Science, vol 981 of advanced materials research, pp 372–375. Trans tech publications ltd, 8
47. Zhao T, Ran Q, Chi Y (2015) Image encryption based on nonlinear encryption system and public-key cryptography. Opt Commun 338:64–72

Subhrajyoti Deb has received his M. Tech degree in Computer Science and Engineering from National Institute of Technology Agartala, India in 2015. He is currently PhD scholar under Visvesvaraya PhD Scheme in the Department of Information Technology, School of Technology, NEHU, Shillong. His research interests includes Cryptology, Security issues in Internet of Things, and Steganography.

Bhaskar Biswas has received his M. Tech degree in Computer Science and Engineering from National Institute of Technology Agartala, India in 2015. Currently he is working as a faculty member in the Department of Information Technology, Tripura University. His areas of interests includes Cryptography, Internet of Things, and Steganography.

Dr. Bubu Bhuyan has received his M.Tech and Ph.D degree from Tezpur University and Jadavpur University respectively. He is currently serving as an Associate Professor in the Department of Information Technology, NEHU, Shillong. His current area of research includes Cryptographic Algorithms, Information Theoretic Security, Steganography, and Cloud Security.