RESEARCH ARTICLE

A lightweight noise-tolerant encryption scheme for secure communication: An unmanned aerial vehicle application

Arslan Shafique[1☯]*, **Abid Mehmood**[2☯], **Mourad Elhadef**[2‡], **Kashif Hesham khan**[3‡]

1 Department of Electrical Engineering, Riphah International University, Islamabad, Pakistan, **2** Department of Computer Sciences, Abu Dhabi University, Abu Dhabi, UAE, **3** Department of Computer Sciences, RMIT University, Melbourne, Australia

☯ These authors contributed equally to this work.
‡ ME and KHK also contributed equally to this work.
* arslan.shafique@riphah.edu.pk

Citation: Shafique A, Mehmood A, Elhadef M, khan KH (2022) A lightweight noise-tolerant encryption scheme for secure communication: An unmanned aerial vehicle application. PLoS ONE 17(9): e0273661. https://doi.org/10.1371/journal.pone.0273661

Editor: Lei Zhang, Beijing Institute of Technology, CHINA

Received: December 4, 2021

Accepted: August 14, 2022

Published: September 19, 2022

Data Availability Statement: All relevant data are within the paper.

Funding: The author(s) received no specific funding for this work.

Competing interests: The authors have declared that no competing interests exist.

Abstract

In the modern era, researchers have focused a great deal of effort on multimedia security and fast processing to address computational processing time difficulties. Due to limited battery capacity and storage, Unmanned Aerial Vehicles (UAVs) must use energy-efficient processing. In order to overcome the vulnerability of time inefficiency and provide an appropriate degree of security for digital images, this paper proposes a new encryption system based on the bit-plane extraction method, chaos theory, and Discrete Wavelet Transform (DWT). Using confusion and diffusion processes, chaos theory is used to modify image pixels. In contrast, bit-plane extraction and DWT are employed to reduce the processing time required for encryption. Multiple cyberattack analysis, including noise and cropping attacks, are performed by adding random noise to the ciphertext image in order to determine the proposed encryption scheme's resistance to such attacks. In addition, a variety of statistical security analyses, including entropy, contrast, energy, correlation, peak signal-to-noise ratio (PSNR), and mean square error (MSE), are performed to evaluate the security of the proposed encryption system. Moreover, a comparison is made between the statistical security analysis of the proposed encryption scheme and the existing work to demonstrate that the suggested encryption scheme is better to the existing ones.

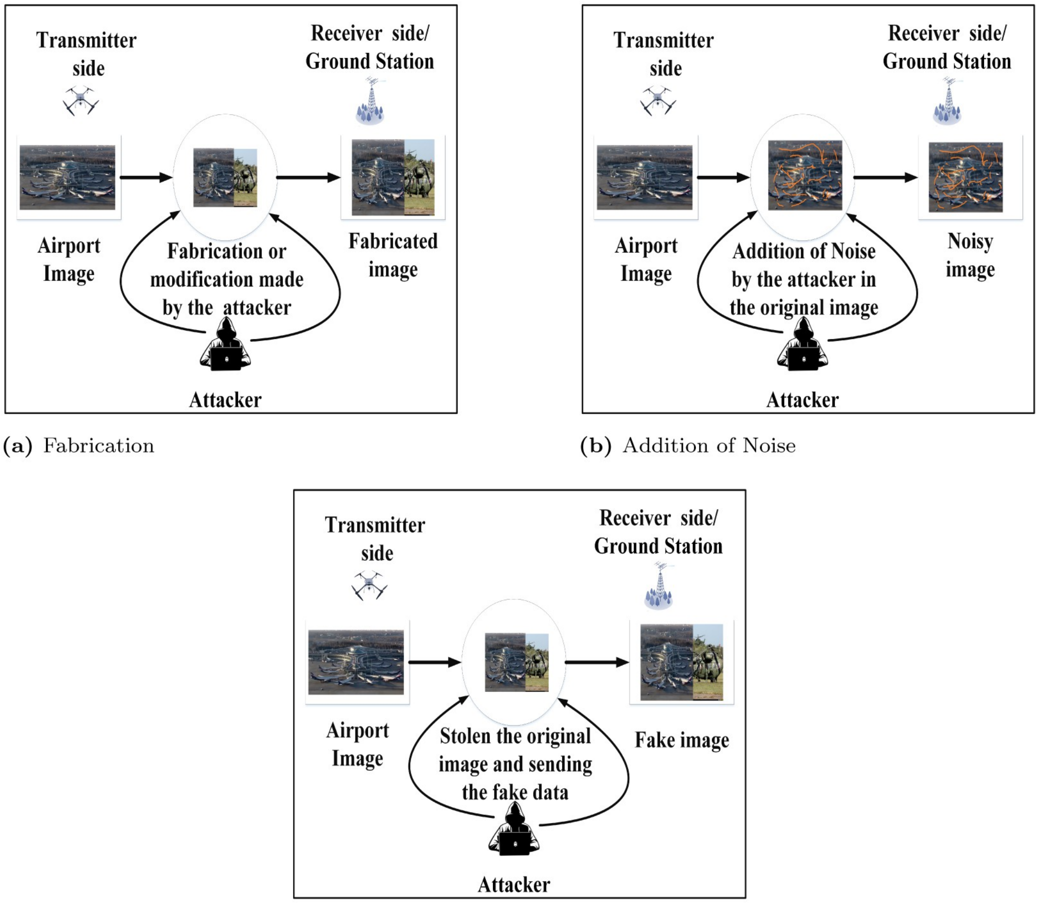
1 Introduction

UAVs are popularly known as drones can be used in real-time applications such as security, communication, transfer of payload, and rescue operations. Drones help us to communicate with other parties where it is difficult to access for humans. Initially, UAVs were used independently, but nowadays, they are integrated with other UAVs to communicate with each other [1–3]. During transmission of data among the UAVs, the attacker can also launch their drone to steal the information which is transmitted between the authentic UAVs or from the UAVs to the ground station.

UAVs mostly capture the data in the form of images [4]. As in the UAVs, the storage is limited, therefore it is not possible to store multiple images in its memory at a time. To avoid such issues, the UAV must have to send the taken photographs and delete them instantly so that the UAV will have enough storage to save the upcoming data [5–7]. While sending the data without any security protocols, the data can be attacked by the eavesdropper in the following ways:

- Data fabrication
- Addition of noise
- The attacker can send fake data after stealing the original version. Fig (1a)–(1c) shows the pictorial representation of aforementioned attacks.

The data can easily be interrupted or modified if it is transmitted over an insecure channel (Internet) which posses a great security threat [8–12]. Therefore, it is meaning full to encrypt the digital data (images) before sending it to the destination. To secure such data, well-known encryption algorithms such as Advanced Encryption Standard (AES), Data Encryption Standard (DES) and blow fish are proposed in recent years [13–15]. Although such algorithms offers suitable security to the digital images, but due to the number of encryption rounds,


Transmitter side
Receiver side/ Ground Station
Airport Image
Fabrication or modification made by the attacker
Fabricated image
Attacker
Transmitter side
Receiver side/ Ground Station
Airport Image
Addition of Noise by the attacker in the original image
Noisy image
Attacker
Transmitter side
Receiver side/ Ground Station
Airport Image
Stolen the original image and sending the fake data
Fake image
Attacker

(a) Fabrication

(b) Addition of Noise

(c) Fake data transmission

Fig 1. Different categories of attacks. (a) Fabrication, (b) Addition of Noise and (c) Fake data transmission.

https://doi.org/10.1371/journal.pone.0273661.g001

the encryption computational time of such techniques is high which is not suitable for real-time applications. However,the encryption proposed in [16–18] can be considered for mobile applications as their performance in terms of computational speed is suitable for such applications.

To reduce time complexity, images can be encrypted using chaos and transformation techniques such as Discrete Cosine transform (DCT) and DWT [19–28]. In the past few years, chaos has played a vital role in image encryption due to its some unique features such as sensitivity in initial conditions, unpredictability, pseudo randomness, ergodicity, and non-deterministic behavior [29–34]. Chaotic systems can be divided into low-dimensional and high-dimensional maps. In low-dimensional chaotic maps such as chaotic sine map and chaotic logistic map consists of less number of initial conditions and control parameters [35, 36]. This makes them easy to implement with fewer resources. On the other side, high-dimensional chaotic maps such as hyper chaotic map and Lorenz system chaos consist of a significant number of initial and control parameters [37, 38]. Although the structure of the high-dimensional chaotic maps is complex, but it occupies more storage and also difficult to implement, requiring more resources and high computational time. Therefore, such high-dimensional chaotic maps are not suitable for real-time applications. The issues of high computational time cannot be ignored in UAVs application as it utilizes limited resources such as finite battery capacity and limited storage that does not allow to store the large data. Storing large data may reduce the computational power of the system [39, 40].

To overcome computational time complexity issues and to provide a suitable security to the digital images, a new technique is proposed based on DWt and chaos theory. The major contributions of the proposed work are as follows:

- A new image encryption scheme is proposed which is especially designed for such real time applications where less processing time is required.
- A DWT is used to decompose the plaintext image at the 5th level in order to minimize the computing time required for encryption. When DWT is used to convert a plaintext image into frequency sub-bands, the sub-bands are reduced by a factor of two. The size of the frequency sub-band at the *nth* level of decomposition will be $\frac{\text{size of image}}{2^n}$. Where *n* represents the level of decomposition, Therefore, the sub-band size at the 5th level decomposition will be $\frac{\text{size of image}}{2^5}$.
- To enhance the security of the proposed encryption scheme, a new algorithm for the generation of noisy images is presented in order to create the diffusion in the plaintext image.
- The cropping and noise attack are carried out by utilising XOR peration to inject random noise into the ciphertext image.
- Several statistical security measures, including entropy, contrast, energy, mean square error, and peak signal-to-noise ratio are conducted to demonstrate the resilience of the proposed encryption scheme

The rest of the paper is structured as follows: The section 1 is devoted to related work and flaws in existing work. In section 3, bit-plane extraction methodology is explained with an example in which an image portion of size 3 × 3 is taken from the original image. The overview and the detailed steps of the proposed methodology are explained in sections 4 and 5 respectively. In section 6, the experimental results and analysis of the proposed and existing encryption schemes are presented to show the effectiveness of the proposed encryption scheme over the existing work. In the last, section 7 concluded the proposed work.

2 Related work

To sort out the issues of computation complexity and providing a high level of security to the digital data, significant research has been carried out in which some of them are based on frequency transformation, and chaotic systems based integrated with substitution boxes (S-boxes) [41–49].

2.1 Encryption using transform techniques

Pixels do not undergo any direct manipulation in encryption systems that are based on frequency transforms. It does this by converting the pixels into their frequency components, which may then be utilised in conjunction with the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT).

Joshi et al. [50] introduced an image encryption technique in their research work. This scheme is intended to protect digital images from any kind of cyberattack. The authors made use of DWT, which involves first converting the plaintext image pixels into its frequency components, such as LL, LH, HL, and HH frequency sub-bands. The LL frequency sub-band stores the majority of the plaintext information, while the other three sub-bands store the finer details. The authors believed that any of these frequency sub-bands may be used effectively to encrypt the plaintext image. As a direct consequence of this, the amount of time required for the calculation is greatly increased. Therefore, when a low processing time is required, it is not ideal to manipulate all of the frequency sub-bands; rather, just the low frequency sub-band should be manipulated (LL).

In [51], Ding et al. suggested an encryption scheme based on DWT and a high-dimensional chaotic map. The high-dimensional map has the potential to provide better safety, but it is challenging to deploy. As a result, the cryptosystem that is suggested in [51] is not appropriate for use in real-time applications. On the other hand, in [52], a method of partial encryption is suggested, which makes use of both DWT and low-dimensional chaotic maps. Despite the fact that the authors' strategy to cut down on the amount of computational time was effective since it made use of a low-dimensional chaotic map, On the other hand, there are two important flaws: (a) compression is employed after encryption, which can cause an increase in the amount of time required for encryption; and (b) the suggested encryption technique is applied to both high-frequency and low-frequency components. Both of these flaws result in an increase in the amount of time required for encryption of the plaintext image.

In [53], Li et al. presented a DWT and chaos-based image encryption scheme. In this technique, the authors encrypted a portion of the low-frequency components of the plaintext image after the image was decomposed into four different frequency sub-bands. Due to the fact that certain sections of the low frequency subbands are encrypted, this technique is lossy in nature. Even if the encrypted version of the plaintext image makes the contents of the plaintext image visible, the original image's pixels are not an exact replica of the original image. As a consequence of this, the approach might be costly in situations in which everybody needs the exact original information. In [54] Li et al. coupled Lifting Wavelet Transform (LWT) with XOR operation to alter the image pixels in order to provide a high degree of security. The resultant XORed images are subjected to further processing in his suggested methodology's compression operation, which ultimately results in a reduction in the size of the ciphertext image. The method has the benefit of requiring a minimal amount of bandwidth for the transmission of the ciphertext image due to the relatively tiny size of the encrypted image. The time required to encrypt a digital image with dimensions of 256 × 256 pixels takes around three seconds, which is a duration that is considered quite excessive for use in real-time applications.

2.2 Chaos theory and substitution based encryption techniques

Apart from the transform approaches to encrypt digital images, substitution boxes and chaos theory have played a key role in the field of cryptography. Naseer et al. [55] suggested an encryption method based on chaos-based and substitution permutation networks. The permutation and substitution are applied using the permutation box (P-box) and substitution-permutation box respectively. The authors applied the permutation and substitution one by one on the plaintext image having the size of 256 × 256. As a consequence, encryption computational time may increase. All of the mathematical steps in their proposed encryption scheme can be performed simultaneously to reduce the cost of computing.

Encryption methods that are based on chaos also include S-boxes as a key component. It is vital to utilise a robust S-box that is able to withstand any security attacks in order to improve the efficacy of chaos and substitution-based encryption schemes that also make use of S-boxes. This is done in order to make the schemes more secure. Shafique et al. [42] presented a novel approach to construct an S-box, which was based on a 1-dimensional cubic logistic map (CLM). In his work, 256 elements of the S-box have been created with the help of the CLM. This method ensures that the right initial conditions are applied. In order to demonstrate the effectiveness of the suggested S-box, a number of different security evaluations were carried out. These evaluations included the Bit independent criterion (BIC), the Linear Approximation Probability (LP), and the Differential Approximation Probability (DAP).

Using a single S-box in any encryption technique may reduce the strength of the entire encryption process. The vulnerabilities of utilising a single S-box are addressed in [56]. In [56], Anees et al. presented the solution of employing multiple S-boxes in an encryption scheme to increase the security of the encrypted images. The authors employed numerous S-boxes instead of a single S-box. The selection of a particular S-box is dependent on the random sequence created using a chaotic logistic map. The multiple S-boxes based image encryption exhibited much better results when compared with the single S-box results. However, the pattern of the plaintext image may be seen in the encrypted image. To tackle this problem, Ahmad et al. [57] continue with the technique described in [56], and build another multiple S-box based image encryption approach which yields considerably better results.

Hua et al. introduced a novel encryption method based on a 2D Sine logistic modular map (SLMM), which is comprised of chaotic sine and logistic maps. [58]. Although both of these chaotic maps exhibit highly non-linear behaviour, it is possible to breach the security of the proposed method by using chaotic signal estimating technologies [59]. Sahteesh et al. [60] employed S-P networks and chaotic maps in their research, which included the use of pixel permutation and diffusion. However, the only XOR operation was used for diffusion purposes, which degrades the security of their proposed algorithm. Liu et al. [61] proposed a new encryption scheme that improved the S-box-based schemes by adding noise and converting the data into blocks. This scheme worked well for images that contained a greater number of grey levels, but it was unable to successfully encrypt images that contained a lower number of grey levels.

The overview of the existing encryption schemes is presented in Table 1 in which several features such as category, advantages, drawbacks and their related possible countermeasures are displayed.

Keeping in mind the issues discussed in this section, in this paper, an encryption scheme is proposed which is time efficient and is capable of providing a significant level of security to the digital images. The proposed encryption scheme is presented specifically for such real time applications in which less processing time is required to encrypt the information. For reducing the computational complexity of the encryption scheme, a DWT is used to decompose the

Table 1. Summary of transform based existing encryption schemes.

Category	Technique	Advantages	Vulnerabilities	Countermeasures
Frequency transform based encryption	DWT based encryption [50]	Can resist brute force attack due to large key space	Time inefficient	Encrypt only low frequency component instead of all frequency components including low and high frequencies
	DWT and chaos-based encryption [51]	Strong security	Difficult to implement	Use low dimensional chaotic map
	Partial image encryption [52]	Suitable level of security	Compression followed by encryption makes the encryption scheme time inefficient	Encryption without compression
	DWT and chaos-based image encryption scheme [53]	Low processing time	Data loss during decryption process	Used full image encryption instead of partial or selective image encryption
	Lifting Wavelet Transform (LWT) based encryption [54]	Low bandwidth required	Non-resistive against chosen plaintext and ciphertext attack	Multiple rounds of encryption may use to withstand cyberattcks
Chaos and substitution based encryption techniques	substitution permutation networks-based encryption [55]	Resistive against cyber attacks such as entropy attack, chosen plaintext and ciphertext attacks	Time inefficient	Use robust substitution permutation processes
	Chaos-based S-box is proposed [42]	Easy to implement	-	-
	Multiple S-boxes [56]	Can replace single S-box with multiple boxes	Patterns of plaintext image cannot be encrypted properly	Permutation may apply before using multiple Boxes
	Multiple S-boxes [57]	Properly encrypted plaintext image patterns	Time inefficient	Perform multiple operations simultaneously
	S-P networks and chaos based image encryption [60]	Weak security	A bit fast algorithm	Replace XOR operation with some powerful transformation operation
	Chaos based [61]	Improved S-box based schemes	Cannot properly encrypt those images which contain less number of gray levels	Use S-boxes and integrate with chaotic maps

https://doi.org/10.1371/journal.pone.0273661.t001

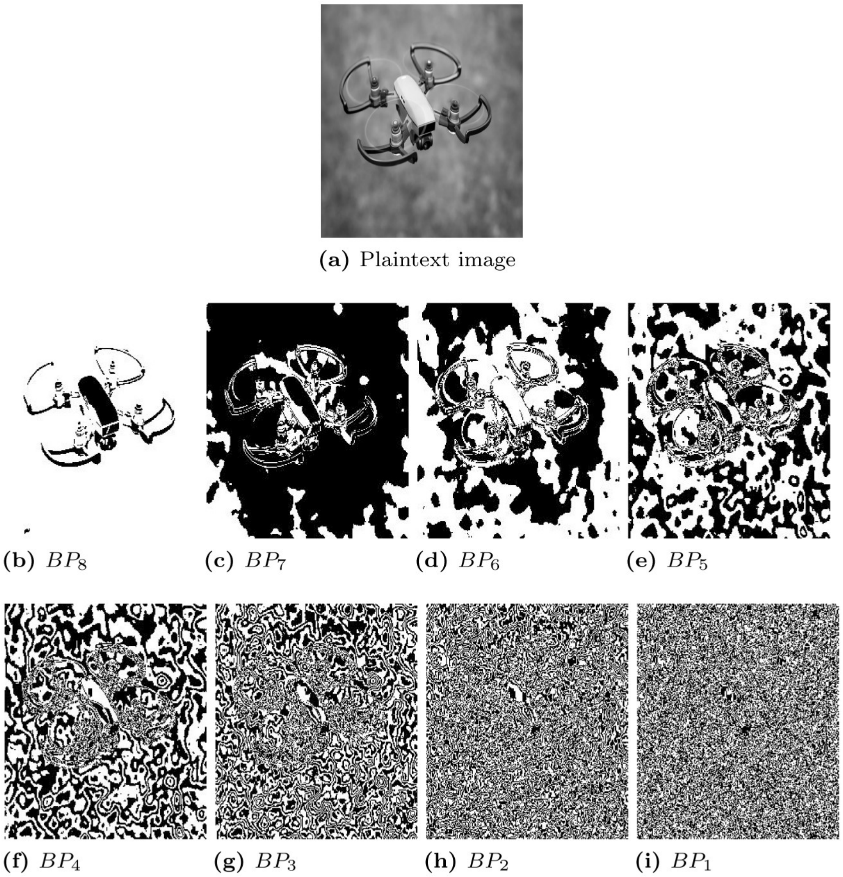
plaintext image at 5th level decomposition. At the 5th level decomposition, the size of the plaintext image becomes $\frac{M}{2^5} \times \frac{N}{2^5}$. Therefore, at that level, fast encryption may be performed. Moreover, to further reduce the computational complexity of the encryption algorithm, only low-frequency sub-bands are considered.

3 Bit plane extraction

For the eight-bit plaintext image, eight bits can be extracted using the Eq (3). Each bit-plane consists of a different amount of plaintext image information. The four least significant bit planes (BP_1, BP_2, BP_3, and BP_4) have the least amount of information, as shown in Fig 2. The percentage of information in each bit-plane can be calculated using Eq (2) and the statistical values of information percentage in each bit-plane are displayed in Table 2.

$$\left.\begin{array}{r} BP_1 = \left(\frac{I}{1}\right) mod2, \;\; BP_2 = \left(\frac{I}{2}\right) mod2 \;\; BP_3 = \left(\frac{I}{4}\right) mod2, \;\; BP_4 = \left(\frac{I}{8}\right) mod2 \\ BP_5 = \left(\frac{I}{16}\right) mod2, \;\; BP_6 = \left(\frac{I}{32}\right) mod2 \;\; BP_7 = \left(\frac{I}{64}\right) mod2, \;\; BP_8 = \left(\frac{I}{128}\right) mod2 \end{array}\right\} \tag{1}$$

$$I_i = \frac{2^{i-1}}{\sum_{i=1}^{8} 2^{i-1}} \tag{2}$$



(a) Plaintext image

(b) BP_8 **(c)** BP_7 **(d)** BP_6 **(e)** BP_5

(f) BP_4 **(g)** BP_3 **(h)** BP_2 **(i)** BP_1

Fig 2. Pliantext image and its corresponding extracted bit-planes. (a) Plaintext image, (b) BP_8, (c) BP_7, (d) BP_6, (e) BP_5, (f) BP_4, (g) BP_3, (h) BP_2, and (i) BP_1.

https://doi.org/10.1371/journal.pone.0273661.g002

From Table 2, it can be seen that most of the plaintext information lies in the most significant bit planes ($BP_8 - BP_5$) and therefore, only such bit-planes are under consideration for the encryption of plaintext image to reduce the encryption computational time.

Apart from the consideration of only most significant bit planes, the simultaneous process of confusion (which refers to scrambling) and diffusion (which refers to the change in the pixel values) also play a vital role to reduces the overall encryption computational time. The process of achieving confusion and diffusion simultaneously is explained in Example 1.

Table 2. Information percentage.

BP_i (i = 1, 2, . . .8)	Information percentage
1	0.30
2	0.79
3	1.42
4	3.12
5	6.25
6	12.23
7	25.7
8	50.20

https://doi.org/10.1371/journal.pone.0273661.t002

Example 1: Let we have an image I is:

$$I = \begin{bmatrix} 120 & 110 & 96 \\ 200 & 186 & 116 \\ 174 & 55 & 169 \end{bmatrix}$$

Convert the pixel values of image I into binary values:

$$\begin{bmatrix} 01111000 & 01101110 & 01100000 \\ 11001000 & 10111010 & 01110100 \\ 10101110 & 00110111 & 10101001 \end{bmatrix}$$

For the extraction of first binary bit-plane (BP_1 bit-plane), LSB_1 of all the pixel values will be considered, and for the extraction of second binary bit-plane (BP_2 bit-plane), LSB_2 of all the pixel values will be considered and so on. The eight extracted binary bit-planes from image I will be:

$$BP_8 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, BP_7 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, BP_6 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, BP_5 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

$$BP_4 = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, BP_3 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, BP_2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, BP_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

After the scrambling process, combine the binary values which are placed at (1,1) in each scrambled bit-plane. It will return the eight bits of the first pixel value. similarly, for the second pixel value, combine the binary bits which are placed at (1,2) and so on. The resultant image (I') will be:

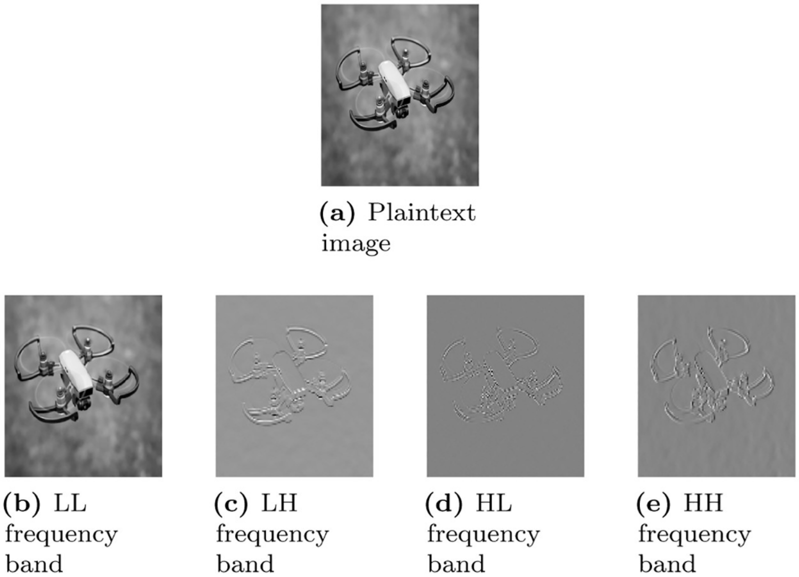
$$I' = \begin{bmatrix} 01101111 & 00010000 & 11101110 \\ 10110110 & 01100101 & 10101010 \\ 10111000 & 01101010 & 11111000 \end{bmatrix} \rightarrow \begin{bmatrix} 111 & 16 & 238 \\ 182 & 101 & 170 \\ 184 & 106 & 248 \end{bmatrix}$$

It can be seen from the image I', the pixel values are completely different from the original image I pixels.

4 Overview of the proposed encryption scheme

In this scheme, a plaintext image is decomposed into different frequency bands using DWT. To make the proposed scheme time-efficient, a fifth-level DWT decomposition is performed, and only low-frequency components are taken to be dealt with. Apart from the DWT, multiple chaotic maps and the bit-plane extraction method are also used. In the bit-plane extraction method, confusion and diffusion are achieved simultaneously by performing only scrambling operation on extracted bit-planes, which helps to reduce the computational complexity.

The Haar wavelet transform can be represented as $Q' = HPH^T$ in which P is a plaintext image having equal number of pixel rows and columns i.e the size of image P is R(rows) × R (columns), H represents the Haar transform matrix having the size equal to the plaintext image and Q is the transform matrix which contain the Haar basis function $h_a(w)$. Where $w \in [0\ 1]$ and a is defined as $a|\ a \in N \wedge 0 \leq a \leq R - 1\}$. It can be decompose uniquely as:



(a) Plaintext image

(b) LL frequency band

(c) LH frequency band

(d) HL frequency band

(e) HH frequency band

Fig 3. Frequency bands extracted from the drone image using DWT. (a) Plaintext image, (b) LL frequency band, (c) LH frequency band, (d) HL frequency band, and (e) HH frequency band.

https://doi.org/10.1371/journal.pone.0273661.g003

4.1 DWT and its role in the proposed scheme

DWT is used to decompose the plaintext image into different frequency components. In every iteration of DWT, the plaintext image divides not four frequency sub-bands such as *LL* sub-band, *LH* sub-band, *HL* sub-band, and *HH* sub-band. *LL* sub-bands correspond to the low-frequency components in which more than 90% of the plaintext information is present as shown in Fig 3. Therefore, to reduce the encryption time, only *LL* sub-band should consider for the encryption of plaintext image.

In the proposed research, Haar wavelet is used which can be represented as $W = HOH^p$ in whcih O is an original image, H shows the haar transform array in which the number of rows (R) and columns (C) are equal to the R and C of the original image and T represents the function of Haar basis $Y_x(w)$. Where $w \in [0\ 1]$ and x is defined as $x|\ x \in N \wedge 0 \leq x \leq R - 1\}$. It can be split uniquely using Eq (3) [62].

$$Q = 2^f + L, \tag{3}$$

Where f shows the maximum exponential number of 2 and L represents the reminder ($\mathrm{L} = 2^{\mathrm{f}} - Q$). Mathematically, Haar basis function can be defined as:

$$Y_x(w) = \frac{1}{\sqrt{R}} \begin{cases} 1 & if x = 0\ \&\ 0 \leq w < 1 \\ 2^{f/2} & if x > 0\ \&\ L/2^f \leq w < \dfrac{L + 0.5}{2^f} \\ -2^{f/2} & if x > 0\ \&\ (L + 0.5)/2^f \leq w < \dfrac{L + 1}{2^f} \\ 0 & \text{Otherwise} \end{cases} \tag{4}$$

After taking the Haar wavelet transform, the size of each frequency sub-band becomes half of the plaintext image. For instance, if the size of the plaintext image is $M \times N$, the size of each sub-band will be one-half of the plaintext image i.e. $\frac{M}{2} \times \frac{N}{2}$. During the second level

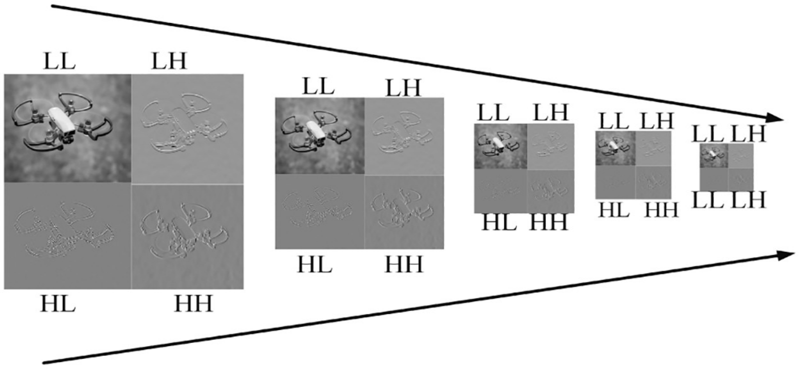


Fig 4. Fifth level DWT decomposition.

https://doi.org/10.1371/journal.pone.0273661.g004

decomposition, the dimensions of the sub-bands will be $\frac{M}{4} \times \frac{N}{4}$ and so on. The decomposition level can be changed according to the application. In the proposed encryption algorithm, fifth-level DWT decomposition is performed to reduce the encryption computational time. Fig 4 shows the fifth level DWT decomposition.

4.2 Chaotic maps used in the proposed scheme

The proposed scheme is also based on chaotic maps. In the proposed work, the chaotic logistic and chaotic sine maps are used for generating the random sequqences and random image to create the diffusion in the plaintext image. The details of such chaotic aps can be seen in [63, 64].

Over the last few years. Chaotic maps are widely used in image encryption due to their tremendous properties such as sensitivity to initial conditions, ability to generate randomness and non-periodicity. Following are the chaotic maps used in the proposed work:

4.2.1 Chaotic logistic map (CLM). CLM is a one-dimensional chaotic map that is used to generate a random sequence for the permutation of rows of pixels in the plaintext image. The reason for choosing the one-dimensional chaotic map over the high-dimensional maps is easy to implement and comparatively faster. Mathematically, the chaotic map can be written as:

$$\Omega_{n+1} = \lambda \times \Omega(1 - \Omega_n) \tag{5}$$

Where Ω_0 and λ are the initial condition and the control parameters respectively. The ranges of these parameters are:

$$\Omega \in (0, 1)$$

$$\lambda \in (0, 4)$$

To generate the random sequence using CLM, Ω must lie in the chaotic range. Fig 5(a) shows the bifurcation diagram of the logistic map in which it can be seen that the CLM shows chaotic behavior when the value of Ω lies in the range [0, 4]. Moreover, the sequence generated using CLM when the value of λ is selected from the chaotic range is shown in Fig 5(b) in which a lot of random values can be seen graphically.

4.2.2 Chaotic sine map (CSM). Like CLM, CSM is a one-dimensional chaotic map. CSM is used in the proposed work to generate the random vector for the permutations of pixels

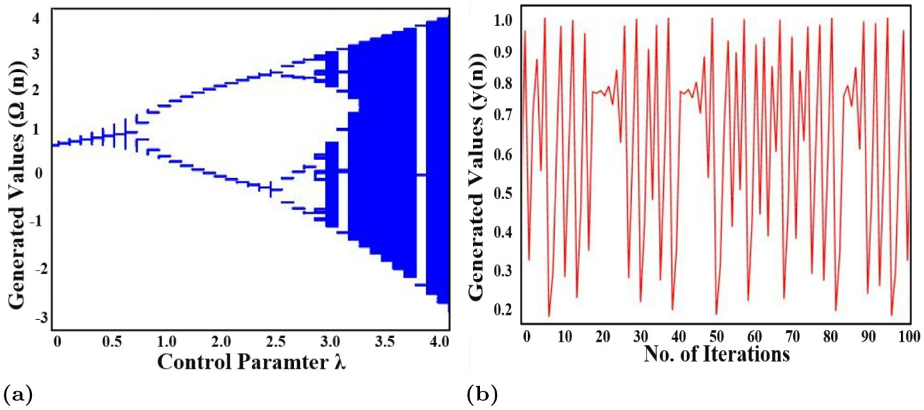


Fig 5. (a) Bifurcation diagram of CLM and (b) random sequence generated using CLM.

https://doi.org/10.1371/journal.pone.0273661.g005

columns in the plaintext image. CTM is given in Eq (6).

$$y_{n+1} = \beta * sin(\pi\alpha_i) \tag{6}$$

Where $y(0)$ and β are the initial or seed values which lie in the range [0, 1] and [0.87, 1] respectively. The chaotic range for CSM is [0.87, 1]. As it can be seen in Fig 6(a), most of the different values are generated in their chaotic range. Therefore, to generate the maximum random values, the value of α is selected as 0.91. This effect is shown in Fig 6(b).

5 DWT based proposed encryption scheme

The three major components of the proposed encryption are bit-plane extraction, chaotic maps (logistic and sine map) and DWT. The secret keys which are used in the proposed work are generated using chaotic maps. The process of key generation is given in section 5.1.

5.1 Key generation process

1. Iterate Eqs 5 and 6 $M \times N$ times using the initial conditions ω, λ, β and y to generate different random values. Such random values are stored in an array known as $key - stream(KS)$.

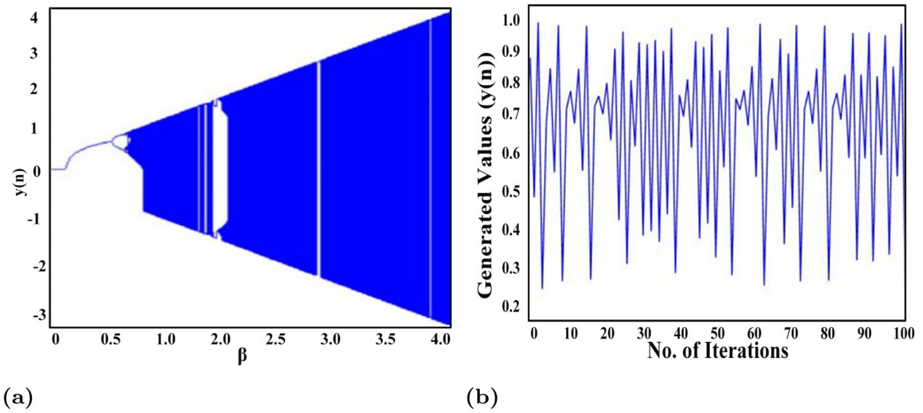


Fig 6. (a) Bifurcation diagram of CSM and (b) Random sequence generated using CTM.

https://doi.org/10.1371/journal.pone.0273661.g006

2. The values generated in *KS* are in the range (0 1). Therefore, to amplify the *KS* values, any large multiplication factor (*N*) is used.
3. The amplified values are converted into an integers values by truncating all the numbers which are placed after the decimal point.
4. The values generated in step 3 are now restricted in the range [0 255] using the modulo operation as follows:

$$X = uint8(mod(floor((RN_1) * N_1); \quad \text{Keys are}: \Omega, \lambda \tag{7}$$

$$Y = uint8(mod(floor((RN_1) * N_2); \quad \text{Keys are}: \beta, y_0 \tag{8}$$

5. The sequences *X*, and *Y* are used as scrambling keys for the permutation of rows and columns of the bit-planes (BP_8 and BP_7).

5.2 Encryption procedure

The image encryption scheme proposed in this paper is for-real time applications. Step wise block diagram of the proposed encryption model is show in Fig 7. While the detail of each step the proposed scheme is given below:

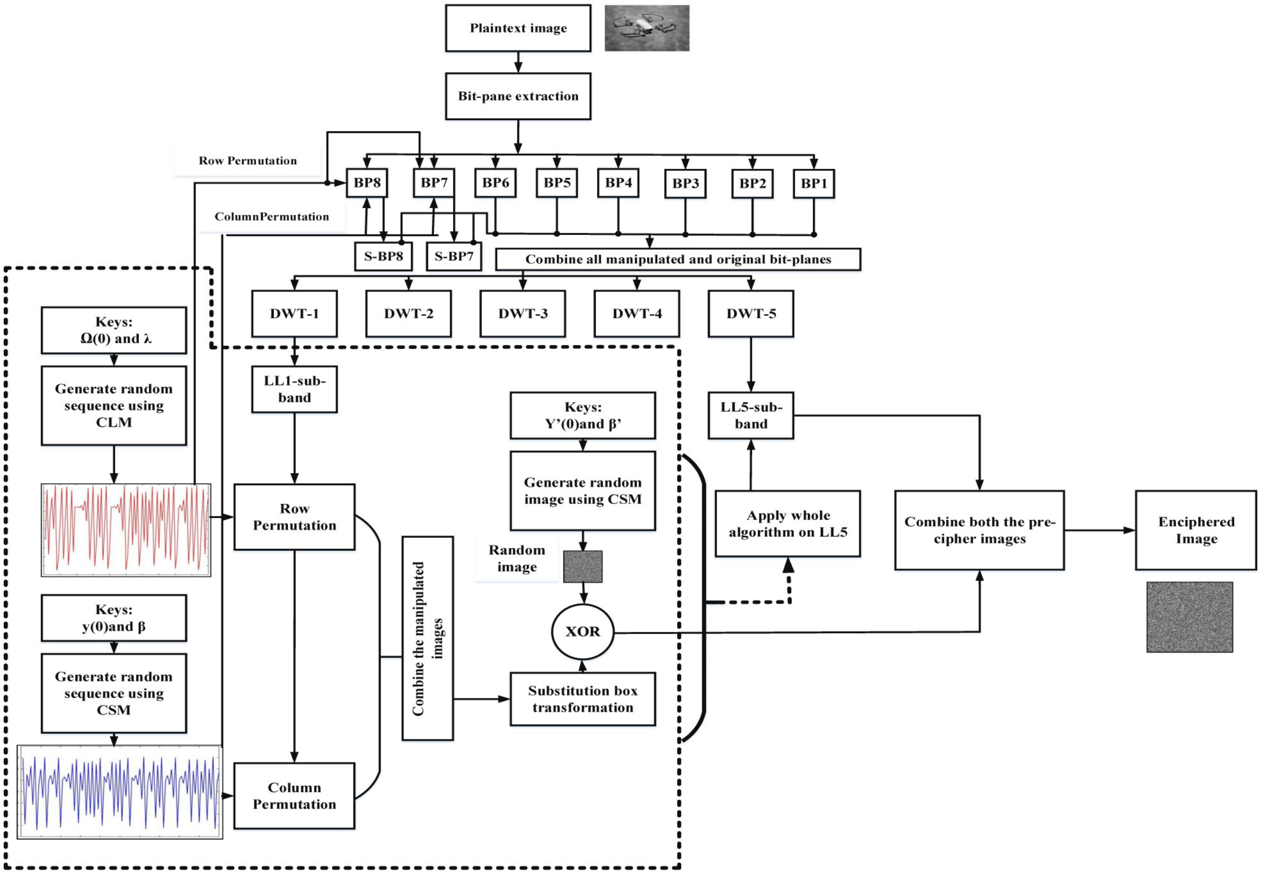

Plaintext image
Bit-pane extraction
Row Permutation
ColumnPermutation
BP8
BP7
BP6
BP5
BP4
BP3
BP2
BP1
S-BP8
S-BP7
Combine all manipulated and original bit-planes
DWT-1
DWT-2
DWT-3
DWT-4
DWT-5
Keys: Ω(0) and λ
Generate random sequence using CLM
LL1-sub-band
Keys: Y'(0)and β'
LL5-sub-band
Generate random image using CSM
Row Permutation
Apply whole algorithm on LL5
Combine both the pre-cipher images
Enciphered Image
Random image
Keys: y(0)and β
XOR
Combine the manipulated images
Generate random sequence using CSM
Substitution box transformation
Column Permutation

Fig 7. Proposed algorithm for fast image encryption.

https://doi.org/10.1371/journal.pone.0273661.g007

- Take a plaintext image of sized $M \times N$ and decompose into eight bit-planes. For the encryption procedure, only BP_8 and BP_7 are considered because more than 90% of plaintext information is present in such bit-planes. Therefore, it is not necessary to encrypt all the bit-planes.
- For row and column scrambling, the sequences generated X, Y and Z in the key generation process are used.
- Combine the permuted bit-planes ($S - BP_8$ and $S - BP_7$) and the unchanged bit-planes using Eq (9).

$$I' = 2 \times (2 \times (2 \times (2 \times (2 \times (2 \times (2 \times S - BP_8 + S - BP_7) + BP_6) + BP_5) + BP_4) + BP_3) + BP_2) + BP_1 \tag{9}$$

- Apply DWt to I' up to 5th level. The size of the LL_5 will be $\frac{M}{2^5} \times \frac{N}{2^5}$. For the encryption time reduction, only LL sub-bands will be considered because most of the information of the plaintext image present in the low-frequency sub-bands. The extracted frequency sub-bands are shown in Eqs 10–13.

$$DWT_1 \rightarrow [LL_1, LH_1, HL_1, HH_1], \tag{10}$$

$$DWT_2 \rightarrow [LL_2, LH_2, HL_2, HH_2], \tag{11}$$

$$DWT_3 \rightarrow [LL_3, LH_3, HL_3, HH_3], \tag{12}$$

$$DWT_4 \rightarrow [LL_4, LH_4, HL_4, HH_4] \tag{13}$$

$$DWT_5 \rightarrow [LL_5, LH_5, HL_5, HH_5] \tag{14}$$

- For the rows and column permutation of LL_5 frequency band, the sequences X and Y are used.
- Combine both the manipulated images generated in the above two steps and apply the S-box transformation on them to get substituted image (S_{image}). The detailed process of S-box transformation is given in [56].
- To create diffusion in the ciphertext image, XOR is applied on the S_{image} and the random image. The random image is generated according to algorithm 1.

Algorithm 1 Substitution of LL_4 sub-band values with S-box

```
Start Input: Initial conditions as secrete keys ($\lambda$ and $\Omega_0$), CLM.
→ Implementation of CLM to generate $M \times N$ values.
→ Stored the generated values in an array $\phi$.
→ Update $\phi$ using the below Equation:
                    $\theta = \phi_i * K_{num}$        (15)
  → $K_{num}$ is a key num which is used to amplify the values stored in $\phi$.
→ Apply floor function to truncate the fractional digits and stored
the result in $\alpha$.
```

```
→ To restrict the generated value in the range [0 255], apply modulo
function as given below:
```

$$M = modulo(\alpha, 256) \tag{16}$$

```
→ Convert $M$ into 2-D array ($R_{image}$).
End
```

- Eq (17) is used to apply *XOR* operation on the S_{image} and R_{image} to get final encrypted image.

$$\text{Encrpted image} : C' = \sum_{i=1}^{M}\sum_{j=1}^{N} R_{image}(i,j) \oplus \sum_{i=1}^{M}\sum_{j=1}^{N} S_{image}(i,j) \tag{17}$$

The plaintext images and their corresponding enciphered images which are encrypted using the proposed encryption scheme are shown in Fig 8. While the histograms of the plaintext and enciphered images are shown in Fig 9.

The two advantages of this scheme are: the computational complexity of the proposed encryption algorithm is low, and the image recovered in its decryption holds the original pixel values. Therefore, it is a lossless encryption scheme.

6 Security analysis

To gauge the proposed encryption scheme, several statistical security analyses such as entropy, correlation contrast, peak signal to noise ratio, and mean square error. Moreover, apart from the statistical analyses, several attacks such as cropping attacks, noise addition attack and brute force attack are also performed to evaluate the robustness of the proposed encryption.

6.1 Histogram analysis

A histogram of an image shows the pixel distribution. The histogram analysis is used to evaluate the performance of the encryption scheme. For the strong encryption scheme, the histogram of the ciphertext image should be flat, uniform, and completely different from the histogram of the plaintext image. The histogram of the plaintext and its corresponding images is shown in Fig 8 where it can be seen that the pixel distribution in the histogram of the plaintext images is fairly uniform, which makes them different from the histogram of the plaintext images. Moreover, the uniformity in the pixel distribution reveals that the proposed encryption scheme can resist the histogram attack.

6.2 Histogram variance analysis

Variance is another parameter to evaluate the uniformity of the histogram of the ciphertext images. This metric may be considered more reliable because it gives the statistical values rather than the histogram visualization. Variance can be calculated as [65]:

$$Var(P) = \frac{1}{256}\sum_{L=1}^{256}[p_i - E(P)]^2 \tag{18}$$

Where P is the pixels stream, $P = \{p_1, p_2, p_3 \ldots .., p_{256}, p_i$ is the pixel value at L^{th} position and $E(P) = \frac{1}{256}\sum_{L=1}^{256} p_i$. For strong encryption, variance values should be low. Table 3 shows the different variance values for the enciphered images generated from the proposed and existing encryption schemes. From the variance values, it can be seen that the proposed scheme performs better than the existing ones.

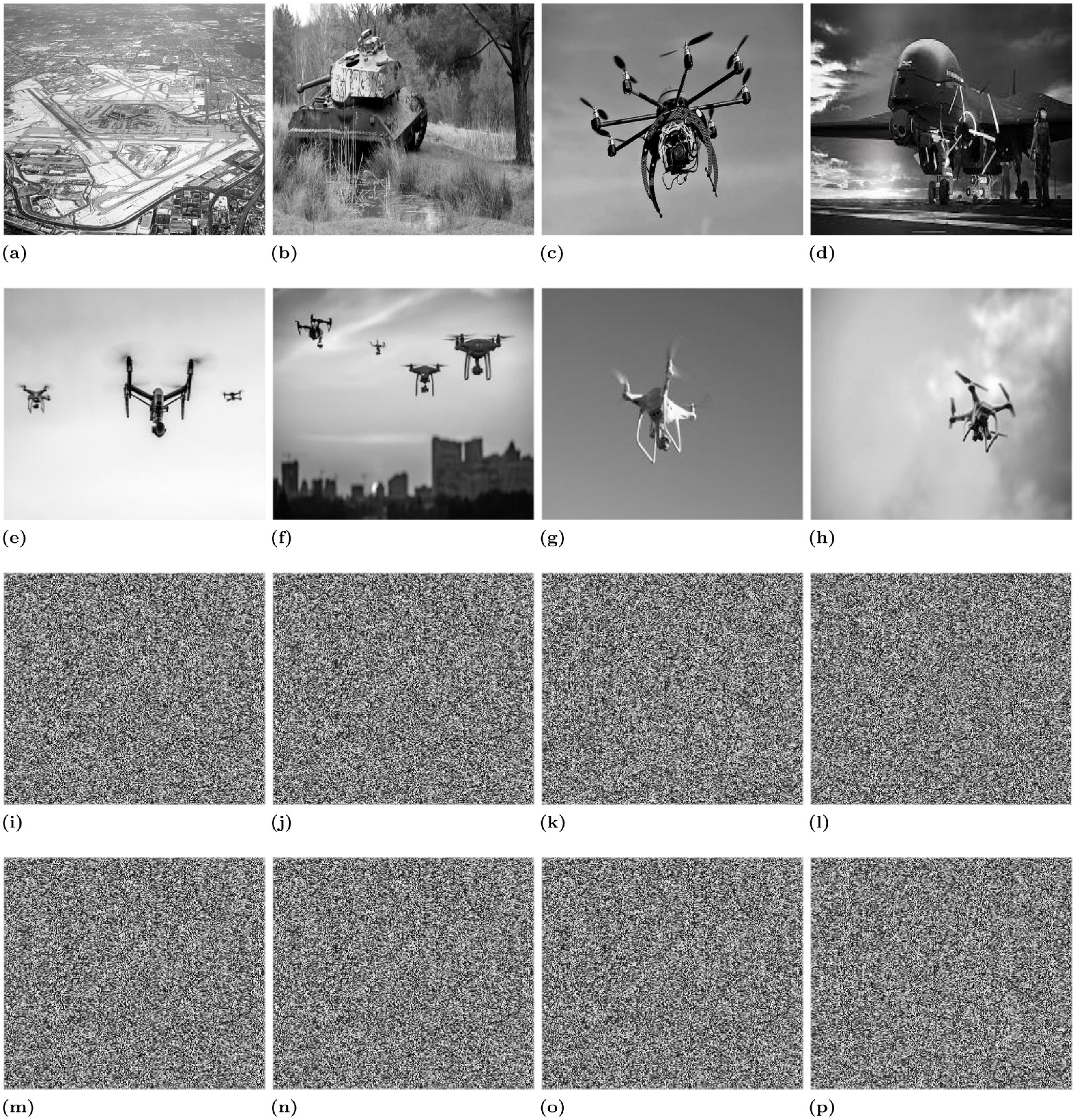


Fig 8. Plaintext and their corresponding enciphered images.

https://doi.org/10.1371/journal.pone.0273661.g008

6.3 Maximum deviation

A cryptographic algorithm's quality may be determined by the deviation in pixel values between the plaintext and ciphertext images [45]. If the deviation (changes) in pixels between the plaintext and ciphertext images is the maximum, the encryption technique is the more

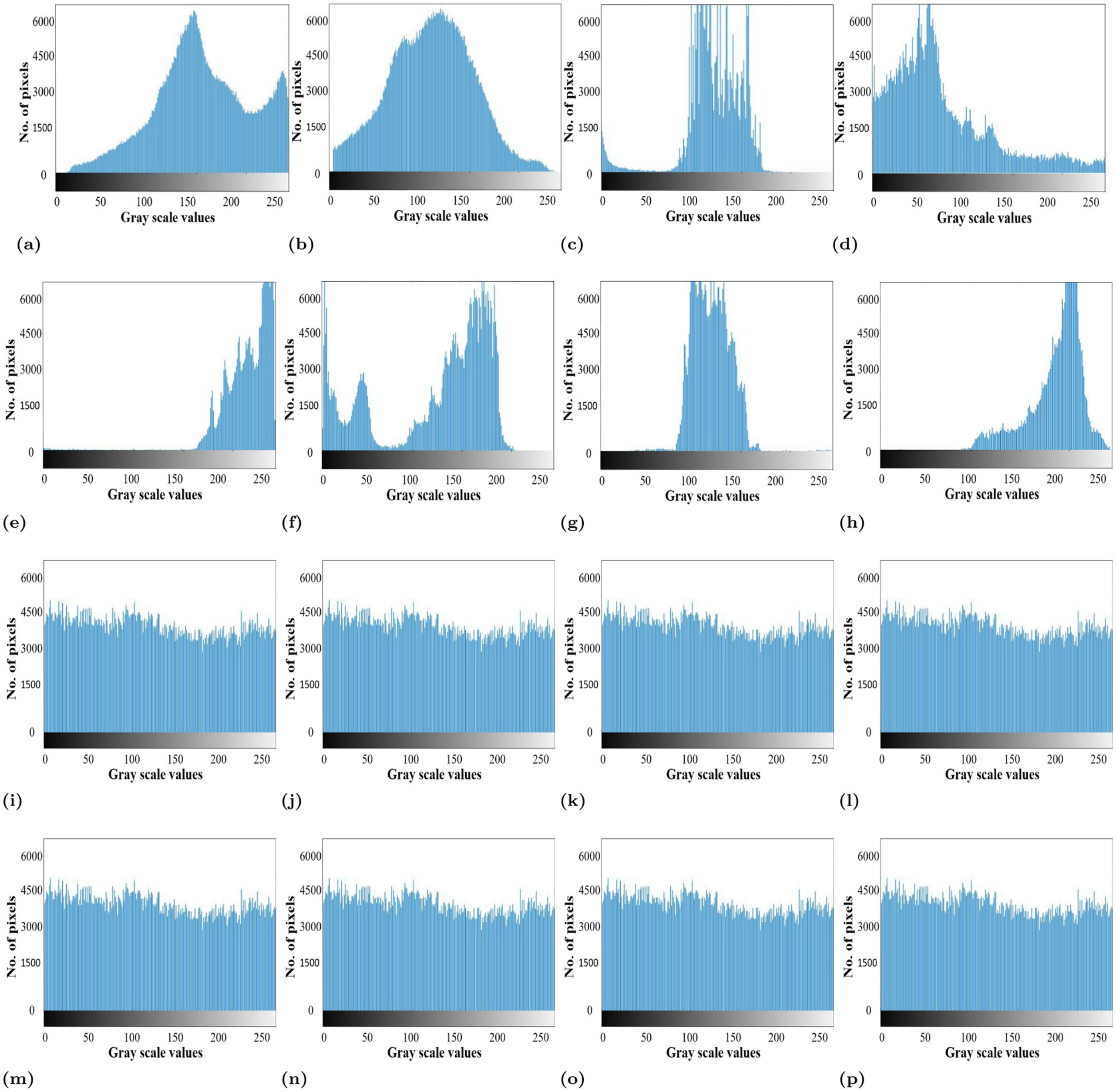


Fig 9. Histograms of plaintext images and the histogram of the corresponding enciphered images.

https://doi.org/10.1371/journal.pone.0273661.g009

robust in terms of security. Mathematically, maximum deviation can be written as:

$$M_A = \frac{A_0 + A_{N-1}}{2} + \sum_{L=1}^{N-2} A_L \tag{19}$$

Where N, and A_L represent the total number of gray levels and the amplitude of the difference histogram at index L respectively. A higher value of "M" implies that the ciphertext is significantly different from the plaintext image. The results of the maximum deviation for the proposed method and the existing algorithms are shown in Table 4. According to a comparison of

Table 3. Histogram variance analysis.

Plaintext images	Ref [66]	Ref [67]	Ref [68]	Ref [69]	Ref [70]	Ref [71]	Ref [72]	Ref [73]	Proposed
Airport	270.671	271.379	269.630	278.136	274.3694	269.679	270.669	268.368	256.637
Tank	260.697	261.378	270.672	276.994	260.978	266.330	259.679	270.641	260.300
Drone	271.370	271.336	272.039	277.698	276.451	271.036	270.678	273.971	258.633
Military base	270.637	271.336	277.987	276.831	270.379	275.689	275.986	275.300	261.596
Ground station	270.687	271.678	274.689	271.678	279.678	270.354	271.669	273.067	263.116

https://doi.org/10.1371/journal.pone.0273661.t003

Table 4. Maximum deviation.

Plaintext images	Ref [66]	Ref [67]	Ref [68]	Ref [69]	Ref [70]	Ref [71]	Ref [72]	Ref [73]	Proposed
Airport	25110	25897	24998	24631	25300	25001	25317	24630	25978
Tank	25993	25796	24689	24336	25700	25314	25371	24998	26789
Drone	26196	26036	24687	24303	25003	24998	25003	24698	26231
Military base	25978	26639	24367	25031	24889	24697	24889	24631	26791
Ground station	25830	25136	25003	25013	25112	24983	24320	24316	25590

https://doi.org/10.1371/journal.pone.0273661.t004

average values of maximum deviations, the suggested encryption algorithm, as well as methods in [66, 67], have superior performance than the other comparable schemes. In light of such findings, we may infer that the maximum deviations of the proposed method do not expose any meaningful information regarding the encryption's quality.

6.4 Irregular deviation

To check the encryption quality, only M_D is not enough. Another metric I_D is used to assess the encryption quality of the enciphered image by determining how close the statistical distribution of deviation between the original and enciphered image is to a uniform statistical distribution. I_D can be calculated as:

$$I_D = \sum_{L=0}^{N-1} |A_L - B_H| \tag{20}$$

Where A_L is the peak of the histogram at position L and B_H is the average sum of the histogram values. The lower the value of I_D, the better the enciphered image quality. The values of I_D for the proposed exciting encryption schemes are displayed in Table 5 where it can be seen that the I_D values for the proposed encryption method are lower than the existing ones, which reflects the better strength of the proposed encryption scheme when it compares with other.

Table 5. Irregular deviation.

Plaintext images	Ref [66]	Ref [67]	Ref [68]	Ref [69]	Ref [70]	Ref [71]	Ref [72]	Ref [73]	Proposed
Airport	46978	47635	48569	47301	46631	47780	47889	46663	45031
Tank	45569	46996	47894	46687	49978	47886	48886	46670	45064
Drone	46691	47630	47133	49963	48955	47790	49371	46698	45666
Military base	46791	46698	47656	46687	47699	46660	46901	47760	45339
Ground station	46975	46639	47339	48664	46881	47720	46698	45966	45798

https://doi.org/10.1371/journal.pone.0273661.t005

Table 6. Information entropy analysis.

Plaintext images	Ref [66]	Ref [67]	Ref [68]	Ref [69]	Ref [70]	Ref [71]	Ref [72]	Ref [73]	Proposed
Airport	7.9871	7.9953	7.9920	7.9935	7.9971	7.9970	7.9963	7.8963	7.9990
Tank	7.9765	7.9963	7.9915	7.9991	7.9986	7.9941	7.9453	7.8983	7.9991
Drone	7.9796	7.9970	7.9903	7.9943	7.9965	7.9936	7.9516	7.8716	7.9990
Military base	7.9899	7.9932	7.9934	7.9968	7.9980	7.9926	7.9695	7.8896	7.9989
Ground station	7.9886	7.9975	7.9971	7.9982	7.9971	7.9912	7.9593	7.8640	7.9986

https://doi.org/10.1371/journal.pone.0273661.t006

6.5 Entropy

Entropy is used to find the robustness in the plaintext or ciphertext image. More randomness in an image results in a higher value of entropy. This relation is shown in Eq (21):

$$Ent \propto randomness \tag{21}$$

Entropy can be calculated as:

$$Entropy = -\sum p(k_i)log_2p(k_i) \tag{22}$$

Where: k_i is the probability of occurrence in the variable i.

The maximum entropy value depends on the nature of the image. For instance, if the image is eight-bit, the entropy cannot be exceeded to eight [11]. Similarly, for the binary images, the maximum entropy value can be two. In the proposed scheme, eight-bit images are tested. This means, if the entropy value is close to eight, the proposed scheme can be considered a secure scheme. In Table 6, the entropy values for the different ciphertext images are displayed. Moreover, a comparison with the existing is also shown in Table 6. Where it can be seen that the entropy values for the proposed scheme are much closer to the ideal value which is eight. Also, the entropy values for the existing scheme are less than the entropy values of the proposed encryption scheme.

6.6 Correlation

Correlation between the image pixel shows the relationship between the intensity of the pixel values. i.e. how close the pixel values are. Greater the difference between the pixel values shows the minimum correlation [74]. Mathematically, it can be written as:

$$Correlation \propto \frac{1}{\text{pixel difference}} \tag{23}$$

Correlation between the image pixel can be calculated as:

$$\mathrm{CorrCoff} = \frac{Cov(w,t)}{\sigma_w\sigma_t}, \quad \sigma_w = \sqrt{VAR_w}, \quad \sigma_t = \sqrt{VAR_t}$$

$$\mathrm{VAR(n)} = \frac{1}{R}\sum\nolimits_{u=1}^{R}(\mathrm{n}_s - \mathrm{E(n)})^2, \quad \mathrm{Cov(n,m)} = \frac{1}{R}\sum\nolimits_{u=1}^{R}(\mathrm{n}_s - \mathrm{E(n)}(\mathrm{h}_s - \mathrm{E(m)}))$$

Where: E and σ represent the expected value operator and the standard deviation respectively.

In the plaintext image, the correlation between the pixel values is always high because the content in the plaintext image can easily be visualized. In contrast, a ciphertext image in which the pixel is properly concealed shows less correlation between the pixels. Therefore, it is always required that the correlation value of pixels in the ciphertext image should be less, so that, no content can be visualized in an encrypted image [75]. Table 7 shows the correlation analysis of

Table 7. Correlation analysis.

Plaintext images	Ref [66]	Ref [67]	Ref [68]	Ref [69]	Ref [70]	Ref [71]	Ref [72]	Ref [73]	Proposed
Airport	0.0027	0.0015	0.0018	0.0021	0.0015	0.0012	0.006	0.0019	0.0001
Tank	0.0019	0.0011	-0.0021	-0.0016	0.0011	0.0022	0.0027	0.0013	-0.0017
Drone	0.0023	-0.0021	-0.0015	0.0021	-0.0015	-0.0020	0.0041	-0.0034	-0.0001
Military base	0.0027	-0.0035	-0.0023	-0.0023	0.0042	0.0031	0.0015	0.0023	-0.0028
Ground station	0.0031	-0.0088	-0.0043	0.0011	0.0035	-0.0043	0.0060	0.0019	-0.0039

https://doi.org/10.1371/journal.pone.0273661.t007

the plaintext images, existing schemes, and the proposed scheme. It can be analyzed from Table 7, that the correlation values of the ciphertext images which are generated through the proposed scheme are significantly less than the plaintext images and exiting schemes.

6.7 Homogeneity

The ability of combinations of pixel brightness results is represented in tabular form by the GLCM. By performing a homogeneity analysis on the distribution in the (GLCM), one can evaluate how close it is to the diagonal of the distribution. The lower the homogeneity measure, the more effective encryption is considered to be. As illustrated in Table 8, the proposed encryption scheme is more effective as compared to the existing schemes. The homogeneity values can be calculated using Eq (24).

$$H_{om} = \sum_{x}\sum_{y}\frac{p(x,y)}{1+|x-y|} \tag{24}$$

Where x and y represents the pixel rows and columns of the plaintext image (p(x,y)) respectively.

6.8 Contrast

Contrast analysis is used to identify the objects in an image. In an enciphered image, the randomness raises the contrast value. Higher contrast values imply better encryption. Mathematically, it can be calculated as [76]:

$$Contrast = \sum_{q,r=0}|q-r|^{2}\gamma(q-r) \tag{25}$$

Where q and r are the 8-bit gray level images and $\gamma(q-r)$ is the gray level occurrence matrix. Contrast values for the proposed and the existing encryption algorithm are reported in Table 9. By analyzing such values, it can be seen that the proposed encryption algorithm works better than comparable schemes.

Table 8. Homogeneity analysis.

Plaintext images	Ref [66]	Ref [67]	Ref [68]	Ref [69]	Ref [70]	Ref [71]	Ref [72]	Ref [73]	Proposed
Airport	0.4936	0.4978	0.4606	0.5998	0.4679	0.4778	0.4978	0.4690	0.4532
Tank	0.4933	0.4977	0.4116	0.4999	0.4699	0.4898	0.4887	0.4766	0.4533
Drone	0.4899	0.4996	0.4663	0.4996	0.4697	0.4788	0.4763	0.4996	0.4500
Military base	0.4866	0.4896	0.4668	0.4986	0.4796	0.4861	0.4730	0.4986	0.4550
Ground station	0.4866	0.4866	0.4796	0.4701	0.4866	0.4700	0.4901	0.4896	0.4510

https://doi.org/10.1371/journal.pone.0273661.t008

Table 9. Contrast analysis.

Plaintext images	Ref [66]	Ref [67]	Ref [68]	Ref [69]	Ref [70]	Ref [71]	Ref [72]	Ref [73]	Proposed
Airport	9.3986	9.6789	9.4689	9.9980	9.6487	9.7832	9.9613	9.9992	10.6989
Tank	9.8826	9.7910	9.8960	9.8741	9.9982	9.7966	9.9710	9.8761	10.2311
Drone	9.9784	9.7812	9.8850	9.8713	9.8775	9.8873	9.9970	9.9460	10.6790
Military base	9.9741	9.6780	9.7710	9.8820	9.8711	9.9462	9.9910	9.9784	10.3460
Ground station	9.8746	9.6692	9.9740	9.7601	9.7880	9.9970	9.9631	9.9631	10.3102

https://doi.org/10.1371/journal.pone.0273661.t009

6.9 Energy

The term energy is used to find the amount of information present in the image [9]. More information present in an image shows that the image has more energy. Therefore, for strong encryption, it necessary that the encryption algorithm should be able to generate such type of ciphertext images in which minimum information can be visualized. As the plaintext images contain more information than the ciphertext images, the energy value for the plaintext image is always higher than that of the energy value of the ciphertext images [77]. Mathematically, energy can be represented as:

$$Energy = \sum (g, m)^2 \tag{26}$$

Table 10 shows the comparison of different energy values corresponds to the plaintext images, existing scheme and the proposed encryption scheme. It can be analyzed from Table 10 that the proposed encryption algorithm can generate such ciphertext images which have fewer energy values than that of plaintext images and other existing schemes.

6.10 Lossless analysis

To retrieve the exact pixel values of the plaintext image from the ciphertext image, the encryption algorithm must be lossless. To show the encryption algorithm is lossless or not, two different terms Peak signal to noise ratio (PSNR) and mean square error (MSE) are frequently used. Mathematically these terms can be represented as:

$$MSE = \frac{1}{LM}\sum_{w=0}^{L-1}\sum_{t=0}^{M-1}(O(w,t) - X(w,t))^2 \tag{27}$$

$$PSNR = 10 \times log_2 \frac{P_{max}^2}{MSE} \tag{28}$$

PSNR and MSE are two opposite terms. PSNR is used to check the similarity index between the plaintext and ciphertext images. More the similarity between the plaintext and ciphertext image will result in the higher values of PSNR which is not required in image encryption.

Table 10. Energy analysis.

Plaintext images	Ref [66]	Ref [67]	Ref [68]	Ref [69]	Ref [70]	Ref [71]	Ref [72]	Ref [73]	Proposed
Airport	0.0159	0.0158	0.0168	0.0169	0.0163	0.0162	0.0160	0.0160	0.0153
Tank	0.0162	0.0161	0.0159	0.0164	0.0161	0.0160	0.0163	0.0154	0.0151
Drone	0.0159	0.0159	0.0159	0.0160	0.0162	0.0161	0.0163	0.0164	0.0154
Military base	0.0159	0.0158	0.0158	0.0161	0.0163	0.0161	0.0167	0.0163	0.0153
Ground station	0.0161	0.0160	0.0164	0.0160	0.0162	0.0163	0.0165	0.0162	0.0154

https://doi.org/10.1371/journal.pone.0273661.t010

Table 11. MSE for loseless analysis.

Plaintext images	Ref [66]	Ref [67]	Ref [68]	Ref [69]	Ref [70]	Ref [71]	Ref [72]	Ref [73]	Proposed
Airport	5.68	8.91	6.86	5.13	3.18	9.98	3.67	6.64	0
Tank	6.97	9.93	5.68	3.90	4.54	9.78	4.31	3.67	0
Drone	3.67	8.54	4.16	3.48	3.66	3.61	2.61	4.10	0
Military base	7.97	6.87	9.18	8.99	3.97	3.99	3.37	4.36	0
Ground station	7.97	9.38	3.94	4.033	4.08	4.16	3.34	3.32	0

https://doi.org/10.1371/journal.pone.0273661.t011

Therefore, an encryption algorithm having strong security always produced minimum PSNR values. In contrast, MSE is used to evaluate the difference between the two desired images. For strong encryption, the MSE value should be high. Maximum MSE value shows that the plaintext and ciphertext images are completely different from each other [78]. To evaluate the proposed encryption algorithm is lossless, PSNR values and MSE values are calculated which are shown in Tables 11 and 12 where it can be analyzed that the PSNR and MSE values for the proposed work are zero and infinity respectively. Whereas the existing schemes show the PSNR and MSE values other than zero and infinity which means that the comparable scheme cannot be used where exact pixel values are required to retrieve.

6.11 Cropping attack analysis

While sending the encrypted images to the ground station, it is possible that the attacker may crop the image to destroy the original information (which is encrypted in the ciphertext image). To gauge the performance of the proposed work in terms of cropping attack analysis, a portion of the ciphertext image is cropped and then send to the ground station. It is decrypted at the receiver end, and it is analyzed that if the attacker cropped the encrypted image, the proposed algorithm is still able to decrypt the original image with little loss of information. Fig 10 shows the cropping attack analysis in which Fig 10(a) shows the cropped version of the ciphertext image and Fig 10(b) shows the decrypted image which is retrieved from the cropped version of the encrypted image. It is clear from Fig 10 that the proposed encryption algorithm can resist the cropping attack analysis.

6.12 Noise attack analysis

There is another category of attack that attackers can launch to shatter the original information. To perform the noise attack analysis for the proposed encryption algorithm, salt (S) and pepper (P) noise is added in the ciphertext image using Eq (29):

$$\text{Noisy ciphertext image} = S + P + C(i, j) \tag{29}$$

Where i, j is the pixel position of the ciphertext image C in which the noise in the form of S and P is added. After the addition of noise in the ciphertext image, decryption is performed

Table 12. PSNR for loseless analysis.

Plaintext images	Ref [66]	Ref [67]	Ref [68]	Ref [69]	Ref [70]	Ref [71]	Ref [72]	Ref [73]	Proposed
Airport	202.3581	209.9781	189.9831	198.3641	192.6798	216.9987	253.6713	196.378	∞
Tank	216.0146	218.3987	196.0166	207.1982	209.4930	207.1887	266.3014	186.3751	∞
Drone	207.8913	239.4680	207.6798	219.6782	207.1889	213.3368	228.3871	205.3781	∞
Military base	228.8712	216.0387	215.9780	205.7965	215.3687	207.7341	286.3746	206.3781	∞
Ground station	217.6715	216.3363	207.6985	229.9981	215.7319	227.1472	199.3741	199.6712	∞

https://doi.org/10.1371/journal.pone.0273661.t012

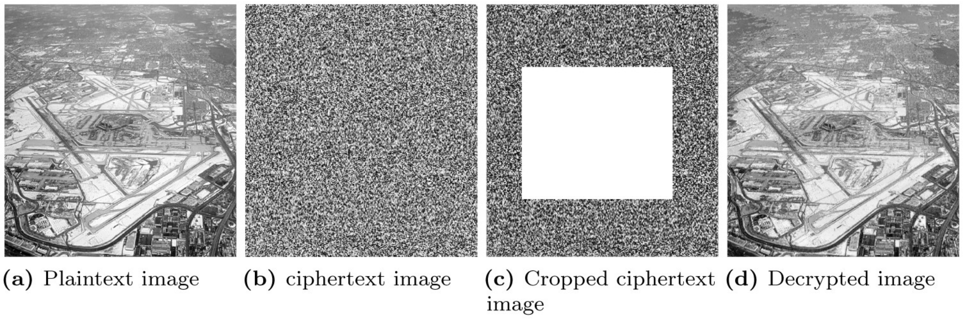


Fig 10. Cropping attack analysis. (a) Plaintext image, (b) ciphertext image, (c) Cropped ciphertext image, and (d) Decrypted image.

https://doi.org/10.1371/journal.pone.0273661.g010

through the proposed decryption algorithm, and it is found that the information in the decrypted image can be clearly visualized as can be seen in Fig 11. Although there is a little noise in the decrypted image, but perceptually there is no difference between the original and ciphertext image.

6.13 Keyspace analysis

Keyspace analysis can be used to evaluate that the weather the encryption scheme can resists the brute force attack or not. Brute force attacks refer to the number of possible combinations of the security keys. For the strong and secure encryption algorithm, the key size should be large enough to resist the brute force attack [79]. According to Alvazari [80], the key size should be at least 10^{100}. In the proposed work, there are four security keys (x_0, x_1, r_0, r_1) are used. As the sensitivity of the each key is 10^{-15}, the key space of each key will be 10^{+15}. This means the total key space for keys used in the proposed work will be 10^{15^*4} which is approximately equal to 2^{200}. Therefore, according to Alvazari's criteria, our algorithm can resist the brute force attack.

6.14 Key sensitivity analysis

The security strength also depends on the keys which are used in the encryption algorithm. It refers to a small change in the security keys generate significant different ciphertext image. To prove the proposed encryption algorithm is a key sensitive, a tiny change ($\Delta = 10^{-15}$) made in

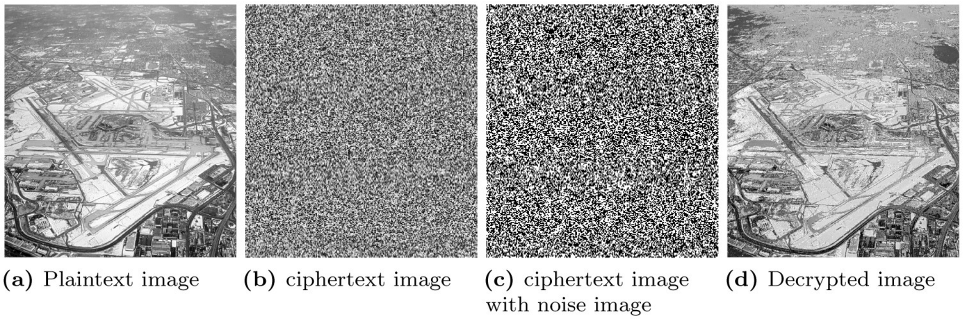


Fig 11. Noise attack analysis. (a) Plaintext image, (b) ciphertext image, (c) ciphertext image with noise image, and (d) Decrypted image.

https://doi.org/10.1371/journal.pone.0273661.g011

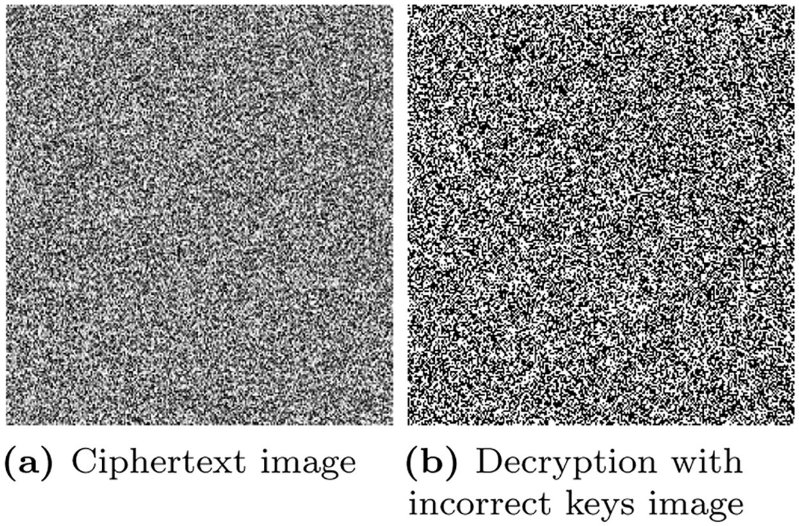


Fig 12. Key sensitivity analysis.

https://doi.org/10.1371/journal.pone.0273661.g012

the security keys (r and x$_0$) I,e r'' = r + delta, and $x_0'\prime = x_0 +$ delta. The modified keys (X_0', r') are then used to decrypt the plaintext image. The resultant decrypted image is shown in Fig 12(b). It can be seen that a tiny change in the security can led to decryption failure.

6.15 MSE and PSNR analysis

MSE is used to calculate the error between the plaintext and ciphertext image. For strong encryption, MSE values should be as high as possible. While PSNR is the reciprocal of MSE. Therefore, if the encryption algorithm offers strong security, the PSNR between the plaintext and ciphertext image will be low. These two metrics can be calculated using Eqs 27 and 28 respectively. In Table 13, MSE and PSNR values are displayed for the proposed and existing encryption schemes. The displayed values reveal that the proposed scheme works better than the existing encryption schemes in terms of PSNR and MSE.

6.16 Sensitivity analysis

Attackers often make a small change in plaintext image and encrypt it before and after this change. By comparing both the encrypted images, they find the relationship between such encrypted images. This attack is known as differential attack. To resists this attack, two well-known metrics number of pixels' change rate (NPCR) and unified average changing intensity

Table 13. MSE and PSNR analysis.

Plain images	Proposed algorithm		Ref [68]		Ref [69]		Ref [70]	
	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
Airport	10.9871	6579	15.3710	2679	17.9790	3511	21.9786	2973
Tank	10.9731	5988	17.5899	3033	20.6681	36536	20.3681	3066
Drone	10.6687	5866	14.6582	3136	21.6797	3496	19.6681	3079
Military base	11.6792	6431	13.6497	3386	20.9987	3596	20.3676	3367
Ground station	10.3798	6226	12.6797	3267	19.9990	3193	19.9965	3567

https://doi.org/10.1371/journal.pone.0273661.t013

Table 14. UACI analysis.

Plaintext images	Ref [66]	Ref [67]	Ref [68]	Ref [69]	Ref [70]	Ref [71]	Ref [72]	Ref [73]	Proposed
Airport	33.4050	33.5972	33.4125	33.2831	33.1831	33.5831	33.5831	33.3831	33.6554
Tank	33.5050	33.4972	33.4125	33.5831	33.5831	33.5831	33.5831	33.3831	33.6654
Drone	33.4050	33.4972	33.5125	33.3831	33.3831	33.5831	33.3831	33.3831	33.6754
Airport	33.4050	33.4972	33.5125	33.5831	33.3831	33.3831	33.5831	33.3831	33.6532
Military base	33.4050	33.2972	33.2125	33.5831	33.5831	33.5831	33.3831	33.2831	33.6111
Airport	33.4050	33.4972	33.3125	33.5831	33.3831	33.3831	33.3831	33.1831	33.6330
Ground station	33.4050	33.4972	33.5125	33.5831	33.3831	33.3831	33.3831	33.2831	33.6390

https://doi.org/10.1371/journal.pone.0273661.t014

can be used. NPCR and UACI can be calculated using Eqs 30 and 31 respectively [81].

$$NPCR = \frac{\sum_{q,r} D(q,r)}{A \times B} \times 100\% \tag{30}$$

$$UACI = \frac{1}{A \times B} \sum_{q,r} \frac{|C_1(q,r) - C_2(q,r)|}{255} \times 100\% \tag{31}$$

Where, A and B represents the pixel rows and columns of the image. C_1 and C_2 are the two ciphertext images whose corresponding plaintext images have only pixel change. The difference matrix $D(q, r)$ can be determined by C_1 and C_2. If $C_1 = C_2$, then $D(q, r) = 0$; otherwise. The larger the value of UACI and NPCR, the better encryption. Apart from UACI and NPCR, another metric known as Mean Absolute Error (MAE) is used to evaluate the performance of the encryption against differential attacks. Mathematically, it can be represented as;

$$MAE = \frac{1}{A \times B} \sum_{q=1}^{A} \sum_{r=1}^{B} |C_1(q,r) - P(q,r)| \tag{32}$$

Where, $C(q, r)$ and $P(q, r)$ are the ciphertext and plaintext image, respectively. For better encryption, the value of MAE must be larger. The UACI, NPCR and MAE for the proposed and existing encryption schemes values are displayed in Tables 14–16 respectively. It can be analyzed from these values that the proposed encryption scheme works better and can resist the differential attack.

6.17 NIST-800-22

To assess the performance of random sequences, NIST-800-22 was designed. Based on the findings of the NIST test, one can identify whether the chaotic sequence is appropriate for use

Table 15. NPCR analysis.

Plaintext images	Ref [66]	Ref [67]	Ref [68]	Ref [69]	Ref [70]	Ref [71]	Ref [72]	Ref [73]	Proposed
Airport	33.4050	33.4972	33.2125	33.3831	33.3831	33.3831	33.3831	33.3831	33.6532
Tank	33.4050	33.2972	33.4125	33.5831	33.5831	33.5831	33.5831	33.5831	33.6615
Drone	33.5050	33.2972	33.4125	33.3831	33.3831	33.5831	33.3831	33.5831	33.6723
Airport	33.5050	33.4972	33.5125	33.5831	33.5831	33.3831	33.3831	33.2831	33.6899
Military base	33.4050	33.4972	33.4125	33.3831	33.3831	33.3831	33.5831	33.5831	33.6783
Airport	33.5050	33.4972	33.4125	33.3831	33.3831	33.3831	33.3831	33.3831	33.6063
Ground station	33.4050	33.4972	33.4125	33.3831	33.3831	33.3831	33.3831	33.2831	33.6166

https://doi.org/10.1371/journal.pone.0273661.t015

Table 16. MAE analysis.

Plaintext images	Ref [66]	Ref [67]	Ref [68]	Ref [69]	Ref [70]	Ref [71]	Ref [72]	Ref [73]	Proposed
Airport	2687	2366	2454	2963	2999	2876	2331	2677	3668
Tank	2879	2364	2100	2336	2794	2650	2116	2998	3570
Drone	2973	2347	2017	2367	2496	2887	2778	2736	3321
Airport	2964	2376	2886	2640	2641	2007	2666	2987	3336
Military base	2679	2446	2665	2314	2007	2667	2476	2766	3166
Airport	2793	2467	2366	25559	2367	2674	2554	2778	3369
Ground station	2674	2116	2779	2466	2311	2555	2491	2676	3560

https://doi.org/10.1371/journal.pone.0273661.t016

in a cryptographic method or not. In addition to the frequency and run tests, the NIST-800-22 contains thirteen more test methods, which include random excursions, approximate entropy tests, etc. The p value may be used to determine the randomness of a test sequence. The sequence is random if $p \geq 0.01$, otherwise $p < 0.01$ shows that the sequence is not random. Moreover, the randomness of the sequence improves when the p value is larger. According to Table 17, the generated sequences in the proposed encryption algorithm pass all random tests.

6.18 Encryption computational time analysis

Apart from security analysis, time analysis is a critical metric for evaluating the performance of an encryption algorithm. The proposed encryption scheme is specifically designed for UAV applications where the encryption scheme must be time-efficient. For the encryption computational analysis, platform having a specification and 8GB of RAM is considered. Moreover, a built-in command in MATLAB called tic toc is used to calculate the processing time of the encryption and decryption. The platform to calculate the computational complexity for the proposed and existing work is kept the same. The processing time of the proposed and existing schemes is given in Table 18, and it can be seen that the proposed scheme is more suitable than the existing schemes for real-time applications.

Table 17. NIST analysis.

Test methods	P-value	Result
Longest Run	0.5988	Cleared
Random Excursions	0.5130	Cleared
Nonoverlapping Template	0.5316	Cleared
Overlapping Template	0.4961	Cleared
Linear Complexity	0.4689	Cleared
Random Excursions Varient	0.5013	Cleared
FFt	0.5316	Cleared
Ranks	0.4770	Cleared
Frequency	0.5697	Cleared
Runs	0.5336	Cleared
Cumulative Sum	0.4986	Cleared
Serial Test	0.5110	Cleared
Block Frequency	0.5987	Cleared
Maurer’s Universal	0.6761	Cleared
Approximate Entropy	0.4798	Cleared

https://doi.org/10.1371/journal.pone.0273661.t017

Table 18. Computational time analysis (sec).

Plaintext images	Ref [66]	Ref [67]	Ref [68]	Ref [69]	Ref [70]	Ref [71]	Ref [72]	Ref [73]	Proposed
Airport	2.5813	0.569	0.3381	0.6649	0.8644	0.3973	0.6690	2.9793	0.0058
Tank	2.6610	0.5812	0.2871	0.8671	0.6112	0.6971	0.8668	2.6352	0.0018
Drone	3.7710	0.6187	0.8371	0.7741	0.6478	0.4972	0.6541	3.8733	0.0041
Military base	2.6792	0.9912	0.2987	0.6178	0.9349	0.8963	0.4896	2.6970	0.0043
Ground station	2.6913	0.7613	0.6175	0.8360	0.6336	0.7339	0.9799	3.6934	0.0041

https://doi.org/10.1371/journal.pone.0273661.t018

6.19 Ciphertext only attack

In this case, the attacker has access to only the ciphertext image and if he does not know which encryption algorithm is used to generate that ciphertext image, this attack is the most difficult to successfully execute to decrypt the plaintext image, as it is also stated in [82]. In our case, the ciphertext image is generated using the confusion-diffusion mechanism, which is achieved by employing DWT, bit-plane extraction, XOR operation, and a few random sequences. According to the statistical analysis such as entropy, contrast, energy, and correlation, it might be very difficult to recover the plaintext image from the only ciphertext image. Therefore, the proposed encryption scheme can resist this attack.

6.20 Known plaintext attack

In this case, the attackers have few plaintext images and their ciphertext images. Based on the knowledge of plaintext-ciphertext pairs, the attackers try to find the secret keys used in the encryption algorithm so that a correct version of the original message can be recovered. To show the robustness of the proposed encryption algorithm against this attack, key-space analysis plays a vital role. From the key-space analysis, it can be seen that it is nearly impossible to find the correct encryption keys in a meaningful time slot. Therefore, the proposed encryption algorithm is resistive to known plaintext attack.

6.21 Chosen plaintext attack

To execute this attack successfully by the attack or cryptanalyst, several plaintext images are encrypted with the encryption algorithm to find the secret keys. From the key-sensitivity analysis, one can see that the secret keys used in the proposed encryption algorithm are sensitive. Even a minor change can make a huge difference in the decrypted image. Therefore, according to the key sensitive analysis, the proposed scheme can resist this attack.

6.22 Chosen ciphertext attack

In this case, the cryptanalyst has different ciphertext images and tries to decrypt them with the decryption algorithm. Again, the purpose of this attack is to find the original keys that are used to encrypt the meaningful message. The random sequences used in the proposed work are based on the initial conditions of the chaotic maps, which are highly sensitive, as shown in the key-sensitivity analysis. Therefore, according to such analysis, the proposed work can withstand a chosen ciphertext attack.

7 Conclusion

The proposed encryption scheme is especially designed for usage in real-time applications. When it comes to real-time applications, they always need less time for encryption and computing. The bit-plane extraction technique and DWT are included in the proposed scheme in order to make it appropriate for use in real-time applications. Only the most significant bit bit planes and low-frequency sub-bands are taken into consideration throughout the encryption process. This is because the majority of the plaintext information is located in these bit planes and sub-bands. In addition to this, several chaotic maps are incorporated in order to increase its level of security. These chaotic maps produce unpredictable sequences and random images for the purposes of confusion and diffusion. In order to evaluate how well the proposed scheme works, a number of security analysis, including entropy, energy, correlation, PSRN, and MSE are carried out. The results of such analysis are compared with those of the existing scheme, which demonstrates that the proposed scheme works more effectively than the existing schemes. In addition to the statistical analysis, several security attacks, including cropping, noise, and brute force attacks, are carried out on encrypted images that are encrypted using the proposed encryption scheme. It is demonstrated that the proposed encryption algorithm is capable of withstanding such attacks.

Author Contributions

Conceptualization: Abid Mehmood.

Formal analysis: Abid Mehmood.

Investigation: Mourad Elhadef.

Methodology: Arslan Shafique.

Resources: Kashif Hesham khan.

Software: Arslan Shafique.

References

1. Faraji-Biregani M, Fotohi R. Secure communication between UAVs using a method based on smart agents in unmanned aerial vehicles. The Journal of Supercomputing. 2021; 77(5):5076–5103. https://doi.org/10.1007/s11227-020-03462-0
2. Vinogradov E, Minucci F, Pollin S. Wireless communication for safe UAVs: From long-range deconfliction to short-range collision avoidance. IEEE Vehicular Technology Magazine. 2020; 15(2):88–95. https://doi.org/10.1109/MVT.2020.2980014
3. Shafique A, Mehmood A, Elhadef M. Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles. IEEE Access. 2021; 9:46927–46948. https://doi.org/10.1109/ACCESS.2021.3066778
4. Surmann H, Worst R, Buschmann T, Leinweber A, Schmitz A, Senkowski G, et al. Integration of uavs in urban search and rescue missions. In: 2019 IEEE International Symposium on Safety, Security, and Rescue Roright (SSRR). IEEE; 2019. p. 203–209.
5. Dinh P, Nguyen TM, Sharafeddine S, Assi C. Joint location and beamforming design for cooperative uavs with limited storage capacity. IEEE Transactions on Communications. 2019; 67(11):8112–8123. https://doi.org/10.1109/TCOMM.2019.2936354
6. Sachs G, Lenz J, Holzapfel F. Unlimited endurance performance of solar UAVs with minimal or zero electrical energy storage. In: AIAA guidance, navigation, and control conference; 2009. p. 6013.
7. Shafique A, Mehmood A, Elhadef M. Detecting Signal Spoofing Attack in UAVs Using Machine Learning Models. IEEE Access. 2021; 9:93803–93815. https://doi.org/10.1109/ACCESS.2021.3089847
8. Ahmed F, Anees A, Abbas VU, Siyal MY. A noisy channel tolerant image encryption scheme. Wireless personal communications. 2014; 77(4):2771–2791. https://doi.org/10.1007/s11277-014-1667-5
9. Anees A, Hussain I. A novel method to identify initial values of chaotic maps in cybersecurity. Symmetry. 2019; 11(2):140. https://doi.org/10.3390/sym11020140
10. Hussain I, Anees A, Alkhaldi AH, Aslam M, Siddiqui N, Ahmed R. Image encryption based on Chebyshev chaotic map and s8 s-boxes. Optica Applicata. 2019; 49(2).
11. Rehman MU, Shafique A, Khalid S, Hussain I. Dynamic Substitution and Confusion-Diffusion-Based Noise-Resistive Image Encryption Using Multiple Chaotic Maps. IEEE Access. 2021; 9:52277–52291. https://doi.org/10.1109/ACCESS.2021.3069591

12. Shafique A, Ahmed J, Rehman MU, Hazzazi MM. Noise-Resistant Image Encryption Scheme for Medical Images in the Chaos and Wavelet Domain. IEEE Access. 2021; 9:59108–59130. https://doi.org/10.1109/ACCESS.2021.3071535
13. Daemen J, Rijmen V. Reijndael: The Advanced Encryption Standard. Dr Dobb's Journal: Software Tools for the Professional Programmer. 2001; 26(3):137–139.
14. Hussain I, Anees A, Aslam M, Ahmed R, Siddiqui N. A noise resistant symmetric key cryptosystem based on S 8 S-boxes and chaotic maps. The European Physical Journal Plus. 2018; 133(4):167. https://doi.org/10.1140/epjp/i2018-11987-x
15. Anees A. An image encryption scheme based on Lorenz system for low profile applications. 3D Research. 2015; 6(3):1–10. https://doi.org/10.1007/s13319-015-0059-2
16. Wang X, Yang J. A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient. Information Sciences. 2021; 569:217–240. https://doi.org/10.1016/j.ins.2021.04.013
17. Wang X, Feng L, Zhao H. Fast image encryption algorithm based on parallel computing system. Information Sciences. 2019; 486:340–358. https://doi.org/10.1016/j.ins.2019.02.049
18. Shafique A, Ahmed J. A Color Image Encryption Algorithm Based on Chaotic Map and Discrete Wavelet Transform. In: 2022 Global Conference on Wireless and Optical Technologies (GCWOT). IEEE; 2022. p. 1–5.
19. Abuturab MR. Securing multiple information using wavelet transform and Yang-Gu mixture amplitude-phase retrieval algorithm. Optics and Lasers in Engineering. 2019; 118:42–51. https://doi.org/10.1016/j.optlaseng.2019.01.015
20. Shafique A, Ahmed F. Image Encryption Using Dynamic S-Box Substitution in the Wavelet Domain. Wireless Personal Communications. 2020; 115(3):2243–2268. https://doi.org/10.1007/s11277-020-07680-w
21. Hussain I, Ahmed F, Khokhar UM, Anees A. Applied Cryptography and Noise Resistant Data Security; 2018.
22. Panna B, Kumar S, Jha RK. Image encryption based on block-wise fractional fourier transform with wavelet transform. IETE Technical Review. 2019; 36(6):600–613. https://doi.org/10.1080/02564602.2018.1533892
23. Anees A, Hussain I, Algarni A, Aslam M. A robust watermarking scheme for online multimedia copyright protection using new chaotic map. Security and Communication Networks. 2018; 2018. https://doi.org/10.1155/2018/1840207
24. Al-Maadeed TA, Hussain I, Anees A, Mustafa MT. A image encryption algorithm based on chaotic Lorenz system and novel primitive polynomial S-boxes. Multimedia Tools and Applications. 2021; p. 1–22.
25. Wang XY, Yang L, Liu R, Kadir A. A chaotic image encryption algorithm based on perceptron model. Nonlinear Dynamics. 2010; 62(3):615–621. https://doi.org/10.1007/s11071-010-9749-8
26. Liu H, Wang X, et al. Image encryption using DNA complementary rule and chaotic maps. Applied Soft Computing. 2012; 12(5):1457–1466. https://doi.org/10.1016/j.asoc.2012.01.016
27. Liu H, Wang X. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Optics Communications. 2011; 284(16-17):3895–3903. https://doi.org/10.1016/j.optcom.2011.04.001
28. Wang X, Zhang M. An image encryption algorithm based on new chaos and diffusion values of a truth table. Information Sciences. 2021; 579:128–149. https://doi.org/10.1016/j.ins.2021.07.096
29. Fadhel S, Shafry M, Farook O. Chaos image encryption methods: A survey study. Bulletin of Electrical Engineering and Informatics. 2017; 6(1):99–104. https://doi.org/10.11591/eei.v6i1.599
30. Liu J, Ma Y, Li S, Lian J, Zhang X. A new simple chaotic system and its application in medical image encryption. Multimedia Tools and Applications. 2018; 77(17):22787–22808. https://doi.org/10.1007/s11042-017-5534-8
31. Alawida M, Teh JS, Samsudin A, et al. An image encryption scheme based on hybridizing digital chaos and finite state machine. Signal Processing. 2019; 164:249–266. https://doi.org/10.1016/j.sigpro.2019.06.013
32. Bai B, Nazir S, Bai Y, Anees A. Security and provenance for Internet of Health Things: A systematic literature review. Journal of Software: Evolution and Process. 2021; 33(5):e2335.
33. Anees A, Khan WA, Gondal MA, Hussain I. Application of mean of absolute deviation method for the selection of best nonlinear component based on video encryption. Zeitschrift fur Naturforschung A. 2013; 68(6-7):479–482. https://doi.org/10.5560/zna.2013-0022
34. Ahmed F, Anees A. Hash-based authentication of digital images in noisy channels. In: Robust image authentication in the presence of noise. Springer; 2015. p. 1–42.

35. Kadhim FA, Emad MH. Mouse movement with 3D chaotic logistic maps to generate random numbers. Diyala Journal For Pure Science. 2017; 13(3 -part 2):24–39. https://doi.org/10.24237/djps.1303.268B

36. Usama M, Rehman O, Memon I, Rizvi S. An efficient construction of key-dependent substitution box based on chaotic sine map. International Journal of Distributed Sensor Networks. 2019; 15 (12):1550147719895957. https://doi.org/10.1177/1550147719895957

37. Patro KAK, Acharya B, Nath V. Secure multilevel permutation-diffusion based image encryption using chaotic and hyper-chaotic maps. Microsystem Technologies. 2019; 25(12):4593–4607. https://doi.org/10.1007/s00542-019-04395-2

38. Munmuangsaen B, Srisuchinwong B. A hidden chaotic attractor in the classical Lorenz system. Chaos, Solitons and Fractals. 2018; 107:61–66. https://doi.org/10.1016/j.chaos.2017.12.017

39. Hashemi SR, Esmaeeli R, Aliniagerdroudbari H, Alhadri M, Alshammari H, Mahajan A, et al. New Intelligent Battery Management System for Drones. In: ASME International Mechanical Engineering Congress and Exposition. vol. 59438. American Society of Mechanical Engineers; 2019. p. V006T06A028.

40. Shafique A. A noise-tolerant cryptosystem based on the decomposition of bit-planes and the analysis of chaotic gauss iterated map. Neural Computing and Applications. 2022; p. 1–24.

41. Jamal SS, Anees A, Ahmad M, Khan MF, Hussain I. Construction of cryptographic S-boxes based on mobius transformation and chaotic tent-sine system. IEEE Access. 2019; 7:173273–173285. https://doi.org/10.1109/ACCESS.2019.2956385

42. Shafique A. A new algorithm for the construction of substitution box by using chaotic map. The European Physical Journal Plus. 2020; 135(2):1–13. https://doi.org/10.1140/epjp/s13360-020-00187-0

43. Hussain I, Anees A, Al-Maadeed TA, Mustafa MT. Construction of s-box based on chaotic map and algebraic structures. Symmetry. 2019; 11(3):351. https://doi.org/10.3390/sym11030351

44. Shafique A, Shahid J. Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps. The European Physical Journal Plus. 2018; 133(8):1–16. https://doi.org/10.1140/epjp/i2018-12138-3

45. Wang S, Wang C, Xu C. An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm. Optics and Lasers in Engineering. 2020; 128:105995. https://doi.org/10.1016/j.optlaseng.2019.105995

46. Xian Y, Wang X. Fractal sorting matrix and its application on chaotic image encryption. Information Sciences. 2021; 547:1154–1169. https://doi.org/10.1016/j.ins.2020.09.055

47. Xian Y, Wang X, Teng L. Double parameters fractal sorting matrix and its application in image encryption. IEEE Transactions on Circuits and Systems for Video Technology. 2021;.

48. Wang X, Liu C, Jiang D. A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT. Information Sciences. 2021;. https://doi.org/10.1016/j.ins.2021.06.032

49. Shafique A, Hazzazi MM, Alharbi AR, Hussain I. Integration of Spatial and Frequency Domain Encryption for Digital Images. IEEE Access. 2021; 9:149943–149954. https://doi.org/10.1109/ACCESS.2021.3125961

50. Joshi AB, Kumar D, Mishra D, Guleria V. Colour-image encryption based on 2D discrete wavelet transform and 3D logistic chaotic map. Journal of Modern Optics. 2020; 67(10):933–949. https://doi.org/10.1080/09500340.2020.1789233

51. Ding L, Ding Q. A Novel Image Encryption Scheme Based on 2D Fractional Chaotic Map, DWT and 4D Hyper-chaos. Electronics. 2020; 9(8):1280. https://doi.org/10.3390/electronics9081280

52. Khan MA, Ahmad J, Javaid Q, Saqib NA. An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps and substitution box. Journal of Modern Optics. 2017; 64(5):531–540. https://doi.org/10.1080/09500340.2016.1246680

53. Wang W, Tan H, Pang Y, Li Z, Ran P, Wu J. A novel encryption algorithm based on DWT and multichaos mapping. Journal of sensors. 2016; 2016. https://doi.org/10.1155/2016/2646205

54. Li CL, Li HM, Li FD, Wei DQ, Yang XB, Zhang J. Multiple-image encryption by using robust chaotic map in wavelet transform domain. Optik. 2018; 171:277–286. https://doi.org/10.1016/j.ijleo.2018.06.029

55. Naseer Y, Shah T, Shah D. A novel hybrid permutation substitution base colored image encryption scheme for multimedia data. Journal of Information Security and Applications. 2021; 59:102829. https://doi.org/10.1016/j.jisa.2021.102829

56. Anees A, Siddiqui AM, Ahmed F. Chaotic substitution for highly autocorrelated data in encryption algorithm. Communications in Nonlinear Science and Numerical Simulation. 2014; 19(9):3106–3118. https://doi.org/10.1016/j.cnsns.2014.02.011

57. Ahmad J, Hwang SO. Chaos-based diffusion for highly autocorrelated data in encryption algorithms. Nonlinear Dynamics. 2015; 82(4):1839–1850. https://doi.org/10.1007/s11071-015-2281-0

58. Hua Z, Zhou Y, Pun CM, Chen CP. 2D Sine Logistic modulation map for image encryption. Information Sciences. 2015; 297:80–94. https://doi.org/10.1016/j.ins.2014.11.018

59. Hussain I, Anees A, Al-Maadeed TA, Mustafa M. A novel encryption algorithm using multiple semifield S-boxes based on permutation of symmetric group. arXiv preprint arXiv:200412264. 2020;.

60. Sam IS, Devaraj P, Bhuvaneswaran RS. Chaos based image encryption scheme based on enhanced logistic map. In: International Conference on Distributed Computing and Internet Technology. Springer; 2011. p. 290–300.

61. Liu H, Wang X. Color image encryption based on one-time keys and robust chaotic maps. Computers Mathematics with Applications. 2010; 59(10):3320–3327. https://doi.org/10.1016/j.camwa.2010.03.017

62. Mondal B, Mandal T, Khan DA, Choudhury T. A secure image encryption scheme using chaos and wavelet transformations. Recent Patents on Engineering. 2018; 12(1):5–14. https://doi.org/10.2174/1872212111666170223165916

63. Belazi A, Abd El-Latif AA. A simple yet efficient S-box method based on chaotic sine map. Optik. 2017; 130:1438–1444. https://doi.org/10.1016/j.ijleo.2016.11.152

64. Pareek NK, Patidar V, Sud KK. Image encryption using chaotic logistic map. Image and vision computing. 2006; 24(9):926–934. https://doi.org/10.1016/j.imavis.2006.02.021

65. Zhang YQ, Wang XY. A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. Information Sciences. 2014; 273:329–351. https://doi.org/10.1016/j.ins.2014.02.156

66. Ahmad J, Tahir A, Khan JS, Khan MA, Khan FA, Habib Z, et al. A partial ligt-weight image encryption scheme. In: 2019 UK/China Emerging Technologies (UCET). IEEE; 2019. p. 1–3.

67. Hasanzadeh E, Yaghoobi M. A novel color image encryption algorithm based on substitution box and hyper-chaotic system with fractal keys. Multimedia Tools and Applications. 2019; p. 1–19.

68. Hayat U, Azam NA. A novel image encryption scheme based on an elliptic curve. Signal Processing. 2019; 155:391–402. https://doi.org/10.1016/j.sigpro.2018.10.011

69. Toughi S, Fathi MH, Sekhavat YA. An image encryption scheme based on elliptic curve pseudo random and advanced encryption system. Signal processing. 2017; 141:217–227. https://doi.org/10.1016/j.sigpro.2017.06.010

70. Balajee MK, Gnanasekar J. Evaluation of key dependent S-box based data security algorithm using Hamming distance and balanced output. Tem Journal. 2016; 5(1):67.

71. Katiyar S, Jeyanthi N. Pure dynamic S-box construction. International Journal of Computers. 2016; 1.

72. Ao T, Rao J, Dai K, Zou X. Construction of high quality key-dependent S-boxes. Nonlinearity (Ns). 2017; 13(14):15.

73. Khan J, Ahmad J, Hwang SO. An efficient image encryption scheme based on: Henon map, skew tent map and S-Box. In: 2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO). IEEE; 2015. p. 1–6.

74. Anees A, Ahmed Z. A technique for designing substitution box based on van der pol oscillator. Wireless Personal Communications. 2015; 82(3):1497–1503. https://doi.org/10.1007/s11277-015-2295-4

75. Shafique A, Ahmed J. Dynamic substitution based encryption algorithm for highly correlated data. Multidimensional Systems and Signal Processing. 2021; 32:91–114. https://doi.org/10.1007/s11045-020-00730-3

76. Wang XY, Zhang YQ, Bao XM. A novel chaotic image encryption scheme using DNA sequence operations. Optics and Lasers in Engineering. 2015; 73:53–61. https://doi.org/10.1016/j.optlaseng.2015.03.022

77. Anees A, Hussain I, AlKhaldi AH, Aslam M. Linear triangular optimization technique and pricing scheme in residential energy management systems. Results in Physics. 2018; 9:858–865. https://doi.org/10.1016/j.rinp.2018.03.015

78. Anees A, Chen YPP. Designing secure substitution boxes based on permutation of symmetric group. Neural Computing and Applications. 2020; 32(11):7045–7056. https://doi.org/10.1007/s00521-019-04207-8

79. Anees A, Chen YPP. Discriminative binary feature learning and quantization in biometric key generation. Pattern Recognition. 2018; 77:289–305. https://doi.org/10.1016/j.patcog.2017.11.018

80. Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. International journal of bifurcation and chaos. 2006; 16(08):2129–2151. https://doi.org/10.1142/S0218127406015970

81. Zhang YQ, Wang XY. A new image encryption algorithm based on non-adjacent coupled map lattices. Applied Soft Computing. 2015; 26:10–20. https://doi.org/10.1016/j.asoc.2014.09.039

82. Wang X, Teng L, Qin X. A novel colour image encryption algorithm based on chaos. Signal Processing. 2012; 92(4):1101–1108. https://doi.org/10.1016/j.sigpro.2011.10.023