remote sensing

MDPI

Article

A Novel Privacy Approach of Digital Aerial Images Based on Mersenne Twister Method with DNA Genetic Encoding and Chaos

Fawad Masood [1], Wadii Boulila [2,3], Jawad Ahmad [4,*], Arshad [5], Syam Sankar [6], Saeed Rubaiee [7] and William J. Buchanan [4]

1 Department of Electrical Engineering, Institute of Space Technology, Islamabad 44000, Pakistan; Fawadkttk@gmail.com
2 College of Computer Science and Engineering, Taibah University, Medina 42353, Saudi Arabia; wadii.boulila@riadi.rnu.tn
3 RIADI Laboratory, University of Manouba, Manouba 2010, Tunisia
4 School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, UK; B.Buchanan@napier.ac.uk
5 Institute for Energy and Environment, University of Strathclyde, Glasgow G11 1XQ, UK; arshad.100@strath.ac.uk
6 Department of Computer Science and Engineering, NSS College of Engineering, Palakkad 678008, India; syam.sankar8@gmail.com
7 Department of Industrial and Systems Engineering, University of Jeddah, Jeddah 21589, Saudi Arabia; salrubaiee@uj.edu.sa
* Correspondence: Jawadkhattak@ieee.org

Received: 13 May 2020; Accepted: 5 June 2020; Published: 11 June 2020

Abstract: Aerial photography involves capturing images from aircraft and other flying objects, including Unmanned Aerial Vehicles (UAV). Aerial images are used in many fields and can contain sensitive information that requires secure processing. We proposed an innovative new cryptosystem for the processing of aerial images utilizing a chaos-based private key block cipher method so that the images are secure even on untrusted cloud servers. The proposed cryptosystem is based on a hybrid technique combining the Mersenne Twister (MT), Deoxyribonucleic Acid (DNA), and Chaotic Dynamical Rossler System (MT-DNA-Chaos) methods. The combination of MT with the four nucleotides and chaos sequencing creates an enhanced level of security for the proposed algorithm. The system is tested at three separate phases. The combined effects of the three levels improve the overall efficiency of the randomness of data. The proposed method is computationally agile, and offered more security than existing cryptosystems. To assess, this new system is examined against different statistical tests such as adjacent pixels correlation analysis, histogram consistency analyses and its variance, visual strength analysis, information randomness and uncertainty analysis, pixel inconsistency analysis, pixels similitude analyses, average difference, and maximum difference. These tests confirmed its validity for real-time communication purposes.

Keywords: aerial images; remote sensing; hybrid techniques; mersenne twister; MT-DNA-Chaos; cryptosystem; nucleotide; Chaos sequencing; DNA

1. Introduction

Aerial photography, or the process of capturing images from aircraft or other flying objects is one of the most widely used methods of remote sensing. The images captured using this method are used in a wide variety of applications ranging from urban planning, real-estate management, disaster evaluation, traffic congestion management, to road network detection, vehicle detection,

military detection and more [1–3]. In many cases, aerial images may contain important information related to sensitive sites that requires secure processing. It is of utmost importance to ensure the security of transmission and processing of images captured by aerial photography technologies as these images may contain crucial data concerning national security.

Securing the content of aerial images is one of the critical problems that necessitate proper investigation. The three fundamental security laws are confidentiality, integrity, and authentication, which is generally known as the CIA triad [4]. The security predicament can be mitigated by utilizing mapped shielded algorithms. These shielded algorithms assist in minimizing the security scarcity over an unreliable transmission channel. Encryption systems use fundamental techniques of confusion and diffusion that were introduced by one of the notable scientists Claude Shannon in the year 1949. These blended properties are very important for a secure cipher that can be effectively utilised in text, image, video, and audio security. Researchers and cryptographers are using a mix of confusion and diffusion for robust security of text and multimedia data. Both researchers and scientists alike are actively involved in designing high-security encryption mechanisms that can process multimedia data in order to avoid theft, attacks, or interception. Many such processes and mechanisms are being developed every year.

Encryption algorithms attempt to conceal the actual image data by devising proper and efficient confusion-diffusion procedures [5,6]. The confusion procedure aims at pixel rearrangement (or pixel permutation), and the diffusion process changes the actual pixel values. Both these operations must be reversible so that the actual image can be deciphered at the receiver end. However, traditional methods such as Data Encryption Standard (DES) or Advanced Encryption Standard (AES) will not suffice at encrypting images due to their high correlation among pixels. A more promising recent area of study in designing encryption mechanisms for images is chaos-based cryptography [7–19]. In chaos-based cryptographic technique, images are transformed at both confusion and diffusion stages with a set of random numbers generated by a mathematical function called a chaotic map. The chaotic maps are an effective tool in cryptography due to its property of sensitivity towards initial conditions [20]. The values of parameters or constants of the chaotic maps act as keys to the encryption algorithm. Chaotic maps like Arnold cat map [21], Logistic map [22], Lorenz map [23] and so forth are being used extensively in various research works to generate random numbers so that it can be used to shift or modify pixel values. Researchers use DNA sequence operation [5], Transforms [6], Cellular automata [24], S-Box [25] and so forth in combination with chaotic cryptography to enhance security further. Chai et al. [26] have suggested a cryptosystem, which consists of a hyper-chaotic system, along with cellular automata, and DNA sequence-based operation, that effectively resisted both known-plaintext and chosen-plaintext attacks cryptanalysis attacks. Some cryptosystems are developed using multiple chaotic systems [27]. Chaotic cryptography techniques are applied effectively in encrypting various forms of images ranging from medical to remote sensing and many more. This work focuses on the secure transmission of images produced by remote sensing. Lijie et al. [28] proposed a remote sensing encryption scheme combining Zerotree Embedded Wavelet encoding (EZW) and a chaotic based on the Tangent-Delay Elliptic Reflecting Cavity map System (TD-ERCS). This method offered rich key-space, accomplishing image encryption across the domain of both spatiality and transformation. The work proposed by Zhang et al. [29] attempted to encrypt remote sensing images in hybrid domains. Discrete Wavelet Transforms (DWT) decomposition was applied in transformation domain and operations with two-dimensional logistic map are applied in the spatial domain. The authors claimed that their work was resistant against various forms of attacks like statistical, brute-force, and so forth. Some researchers have also made use of techniques such as compressed sensing [30,31] combined with a chaotic cryptographic environment in order to achieve both compressions as well as encryption on remote sensing images. Unlike other methods, Ye et al. [32] proposed using the chaotic Lorenz system as the basis for block-based remote sensing image encryption. A fast block circular permutation is added to their work. This method proposed by Ye et al. [32] was shown to resist both known-plaintext and chosen-plaintext cryptanalysis attacks. Though AES is not

common in encrypting images, Zhang et al. [33] have successfully combined both AES and Piece-Wise Linear Chaotic Map (PWLCM) to create an effective new means for the secure transmission of remote sensing images and achieved fast encryption. Recently, Liu et al. [34] proposed an encryption system that combines both DNA bases probability with two-dimensional logistic map in order to process remote sensing images. Here, the pixel rearrangement (or confusion) was accomplished by having the logistic map generate sequences, while the DNA sequence operation helped the process achieve diffusion. The proposed cryptosystem demonstrated an acceptable running speed. As the data represented by a remote sensing image is of having inevitable relevance and of national importance, specific encryption mechanisms for their secure transmission are necessary. The basic schematic chart of our proposed image encryption system is demonstrated by Figure 1. This cryptosystem works in three distinct phases, that is, Mersenne Twister (MT) method phase, DNA phase, and Rossler Dynamical chaotic map phase. Figure 2 shows the encrypted output of the two aerial images.

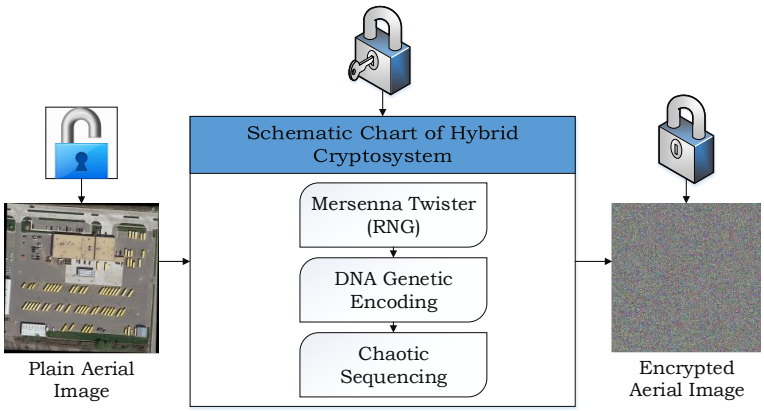

Figure 1. Basic procedure of proposed cryptosystem.

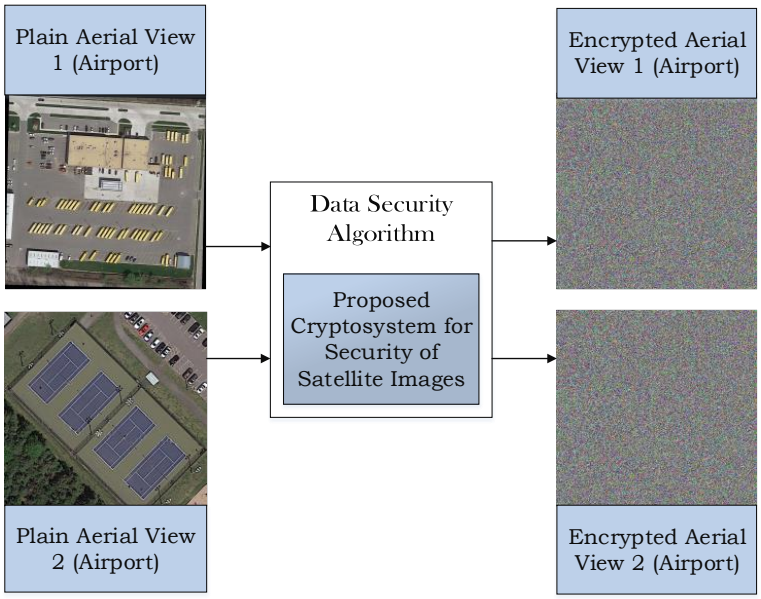

Figure 2. Schematic chart of image encryption.

2. Contribution

The main contributions of this research article are summarized as follows:

- Developing an efficient cryptosystem based on multiple phases using a substitution permutation process. This will generate high randomness sequencing and exhibit low correlation among the pixels of aerial images, ensuring secure transmission.

- Investigating numerous existing algorithms and conducting randomness test for existing cryptosystems that used coloured images.
- Comparing results of the proposed cryptosystem with Younas et al. [35] results according to MSE, PSNR, NCC, SC, and NAE.
- Developing a modernized version of the chaos-based diffusion algorithm, which provides a higher value of MSE and entropy-based randomness than existing algorithms. The higher value demonstrate that the cryptosystem proposed here is capable of generating highly protected encrypted images.

The remainder of our work is organized in the following order. The three methods (e.g., Mersenne Twister, DNA encoding/decoding process, and CDRS) that constitute the phases of the proposed cryptosystem are detailed in Section 3. Section 4 discusses the dataset and detailed steps of the proposed image encryption scheme. In Section 5, many statistical tests are applied to the proposed scheme to authenticate it. Finally, concluding remarks and thoughts on directions for future works are presented in Section 6.

3. Background

This section discusses the MT method, DNA encoding/decoding and CDRS.

3.1. Mersenne Twister

The Mersenne Twister (MT) method was initially proposed by Makoto Matsumoto in 1997 as a means of building high-quality pseudo-random numbers for image encryption schemes [36–38]. The system based on the MT method generates random sub-sequences (periods), known as Mersenne primes, in an efficient process that exhibits high computational speed and reliability as well. Diverse variants of MT provides high computational speed and strong levels of security. The two most highly utilized MT are SIMD-oriented Fast MT (SFMT) and CryptMT. Makoto Matsumoto introduced SFMT, system is based on a Linear Feedback Shift Register (LFSR) that generates 128 bits long integers, in 2006. CryptMT is a streaming cipher that generates prime numbers (random sub-sub-sequences) in a modified form of Twisted Generalized Feedback Shift Register (TGFSR) that takes an incomplete array to realize the periods. This system is based on the inversive decimation method often used for primitivity testing regarding the characteristic polynomial of a linear recurrence with its computational complexity of operation OP^2, where 'P' denotes the degree of the polynomial. It should be noted that MT generates a very long period, that is $2^{(19937-1)}$ that includes 263 dimensions of equidistribution and has a limit of 32 bit of accuracy, as it generates random numbers that are free from correlation. This system offers high-speed computations.

MT Theories

The system is based on a uniform pseudo-random sequence that generates word of vectors [39]. The uniform integers have a limit between 0 and $2^w - 1$. The w is a row vector over the binary finite field F_2. The equation is based on a recurring process, and is defined in Equation (1):

$$x_{k+n} := x_{k+m} \oplus \left(x_k^u | x_{k+1}^l \right) A, \tag{1}$$

whereas in Equation (1), A is constant while $w \times w$ is the chosen matrix that is shown in Equation (3):

$$1 \leq m \leq n, \tag{2}$$

whereas, n denotes the degree of recurrence and m denotes the integer with a range as shown in Equation (2):

$$\begin{bmatrix} & 1 & & & & \\ 0 & 0 & 1 & & & \\ 0 & \cdots & \cdots & \cdots & & \\ & & & & & \\ a_{w-1} & a_{w-2} & \cdots & \cdots & \cdots & a_0. \end{bmatrix} \tag{3}$$

The value of K = 0,1,2,3, $\cdots$. X_n is the row vector for the word size w that is generated when $K = 0$. The initial seeds for the aforementioned system is X_0, X_1, X_2, $\cdots$, X_{n-1}.

- x_{k+1}^l shows the lower rightmost r bits from x_{k+1}.
- x_k^u shows the upper leftmost w-r bits from x_k.
- $\oplus$ is used to bit-wise XOR operation between the original pixels and random numbers generated through a proposed step using an MT generator.
- $|$ is the concatenating operation.
- $\left(x_k^u | x_{k+1}^l\right)$ is known as concatenation vector, generated when concatenating the upper leftmost w-r bits from x_k^u and the lower rightmost r bits from x_{k+1}^l orderly.
- Finally vector A, as shown above is multiplied with right-side of this vector.
- Lastly, bit-wise $\oplus$ is employed for the purpose of addition of x_{k+m} to give rise to another vector that is, x_{k+n}. The simple bit shift operation is further utilized for the process of multiplication of $\left(x_k^u | x_{k+1}^l\right) \times A$.

The system is further elaborated in Equation (4):

$$xA = \begin{array}{ll} x >> 1 & \text{if } x_0 = 0 \\ (x >> 1) \oplus a & \text{if } x_0 = 1, \end{array} \tag{4}$$

whereas, the value of x = $(x_{w-1}, x_{w-2}, \ldots, x_0)$ and a indicates a vector that has been formed at the bottom (row) of A. "$\gg$" signifies bit-wise right shift. Thus the recurrence (1) calculation takes bit-shift, bit-wise XOR, or bit-wise AND operation. It is to be noted that MT has a total (n$-$1) dimensional distribution; that is the reason it exhibits excellent characteristics of PRNG k distribution tests, and it is assumed to be the best way to gauge the randomness of PRNG. Improving the k-distribution to v-bit accuracy within the raw sequence generated from recurrence (1) is known as tempering and this process produces final pseudo-random numbers. Each generated word is multiplied to $w \times w$ invertable matrix T from right, which yields the result of tempering matrix x into $z := x \times T$. The matrix T is to chosen in such a way that the binary operation is possible, which is shown in Equation (5):

$$\begin{aligned} y &:= x \oplus (x >> u) \\ y &:= y \oplus ((y << s) \& b) \\ y &:= y \oplus ((y << t) \& c) \\ z &:= y \oplus (y >> l), \end{aligned} \tag{5}$$

whereas, the preceding equation asserts that u, s, t, and l are known as tempering bit shifts while b and c are tempering bit-masks. Here, the bit-wise left shift is signified by "$\ll$". MT works on two parts, that is, recurring, and tempering. The process of recurring is similar to LFSR in that both entail that each bit is state deriving from the recursion, while each individual bit occurring at the output end satisfies the recurring of the bits forming the states.

3.2. DNA Encoding/Decoding

Deoxyribonucleic Acid (DNA) is comprised of four distinct varieties of nucleotides whose sequences forms the whole DNA molecule. The four nucleotides are adenine (A), cytosine (C),

guanine (G), and thymine (T) and combination of these four types can be used to encode binary numbers: 00, 01, 10, and 11. Out of the 24 possible encoding rules in DNA only eight types meet Watson-Crick (W-C) complementary rule [40] as demonstrated in Table 1. Because an image pixel is represented with 8 bits, four DNA bases are needed in order to encode it. Different encoding rules produce different DNA sequences for a single pixel. If the pixel value of an image is 81, then the value in its corresponding binary form can be represented as [01000111]. Depending on the rule being used, we get different DNA base combinations. If we draw on Rule 1 for DNA encoding, then the encoded binary results in [CACT].

By contrast, the sequence will be [GTGA] after adopting rule 8. The reverse method of encoding is the decoding rule. Thus, the same DNA sequence will be decoded differently depending upon the rule referenced in encoding it. As an example, the DNA sequence [ATCG] could be decoded to show a binary sequence [01100011] when using Rule 3 or to the binary sequence [10011100] if using Rule 6. Table 1 demonstrates all possible encoding rules.

Table 1. Rules of DNA encoding.

Rule	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01

3.3. Chaotic Dynamical Rossler System

CDRS was initially investigated in 1976 by Otto Rossler in his work on chemical kinetics study [41]. This system is based on three traditional differential equations, all non-linear dynamical systems. The system operates as a continuous-time differential equation. It has better chaotic characteristics and exhibits fractals behavior as well. The map attractor resembles the Lorenz chaotic system. The chaotic map has many applications in various fields. It is defined in Equation (6):

$$\begin{aligned} x &= -y - z \\ y &= x + ay \\ z &= b + z(x - c), \end{aligned} \tag{6}$$

whereas, in the above equation, a, b, and c are control parameters. The values are adjusted as: $a = 0.2$, $b = 0.2$, and $c = 5.7$. The value of c is in the range of $1 \leq c \leq 6$. It is important to note that we can find finite iteration from CDRS that exhibits infinite iterations. The attractor is generated using a Rossler system is shown in Figure 3. The plotting of random sequences generated at three phases (MT, DNA, and CDRS) is shown in Figure 4.

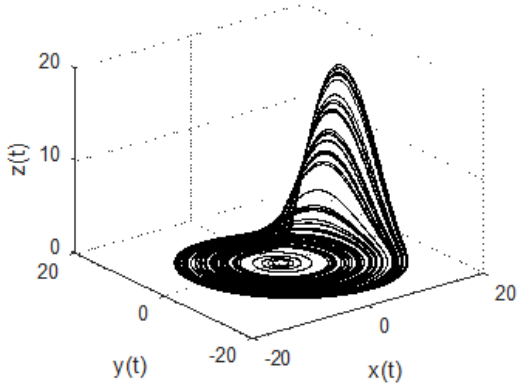

Figure 3. CDRS generated attractor.

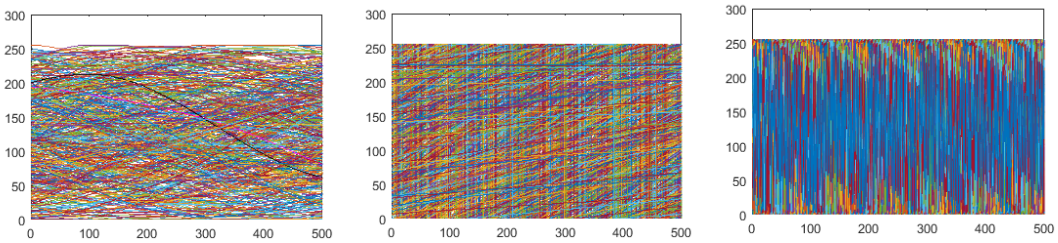

Figure 4. Plotting of MT, DNA, and CDRS random numbers.

4. Dataset Description and the Proposed Scheme

In our work, we used Dataset for Object Detection in Aerial images (DOTA) which is a large-scale public database of aerial images taken from various sensors and plate-forms such as Google Earth, satellite JL-1, and satellite GF-2 [42]. Before their inclusion in DOTA, The collected images are scanned and annotated by experts to verify their nature. The contents of DOTA includes images of Airplanes, ships, sports venues and vehicles of various sizes, colours, and natures. In this paper, we have used different images with different colors schemes so that the proposed scheme could be verified on a number of images. The sensitive images such as buses and airplanes are encrypted in this paper. However, one can also encrypt natural scene images via the proposed scheme. The encryption steps can verify that the proposed scheme has the ability to encrypt any image. The encryption steps are outlined as:

step 1: Let us consider an image I with the dimension $M \times N \times 3$. I is resized to $512 \times 512 \times 3$.
step 2: The resized image I is then divided into three respective layers, that is, R = red, G = green, and B = blue, where R, G, and B measure 512×512.
step 3: Twister Seed Function (TSF) is initiated and used to generate uniformly distributed random numbers from MT.
step 4: MT is iterated for N = 270,000 times, and the first 7858 values thus generated are discarded in order to overwhelm the transient effect, Random values are stored in α.
step 5: The value of α is multiplied with a higher number of 10^{14} to get β.
step 6: Absolute and round function are applied on β, and the value is stored in γ.
step 7: Modulus 256 operation is applied on γ to get a row matrix ζ.
step 8: ζ is XOR with R, G and B to get encrypted channels, R_1, G_1 and B_1.
step 9: In this step the output of the DNA code random sequencing is XOR with R_1, G_1 and B_1 (previous step) to get new encrypted layers R_2, G_2 and B_2 .
step 10: CDRS is added as an additional layer of security and R_2, G_2 and B_2 pixels are permuted using CDRS random sequence which is stored in R_3, G_3 and B_3.
step 11: All layers, that is, red, green, and blue, are encrypted,

5. Statistical Analysis

This section is based on several statistical tests that have been performed on various aerial images with different views procured through DOTA. We have taken five aerial images to analyse with the proposed scheme. Various tests were carried out to check the resistance level of the hybrid-based cryptosystem. The security analysis includes Histogram Analysis (HA), Adjacent Correlation Analysis (ACA), Peak to Signal Noise Ratio (PSNR), Mean Square Error (MSE), Homogeneity Level (HL), Contrast Level (CL), Energy Level (EL), Average Difference (AD), Maximum Difference (MD), Information Entropy (IE), Normalized Absolute Error (NAE), Structural Content (SC), and Normalized Cross-Correlation (NCC). Stepwise flow chart for the securing of digital aerial images are shown in Figure 5. The aerial view images are considered as test images for the proposed technique of image encryption as shown in Figures 6–8. Cumulative five colored images are considered and we have calculated their results in this section.

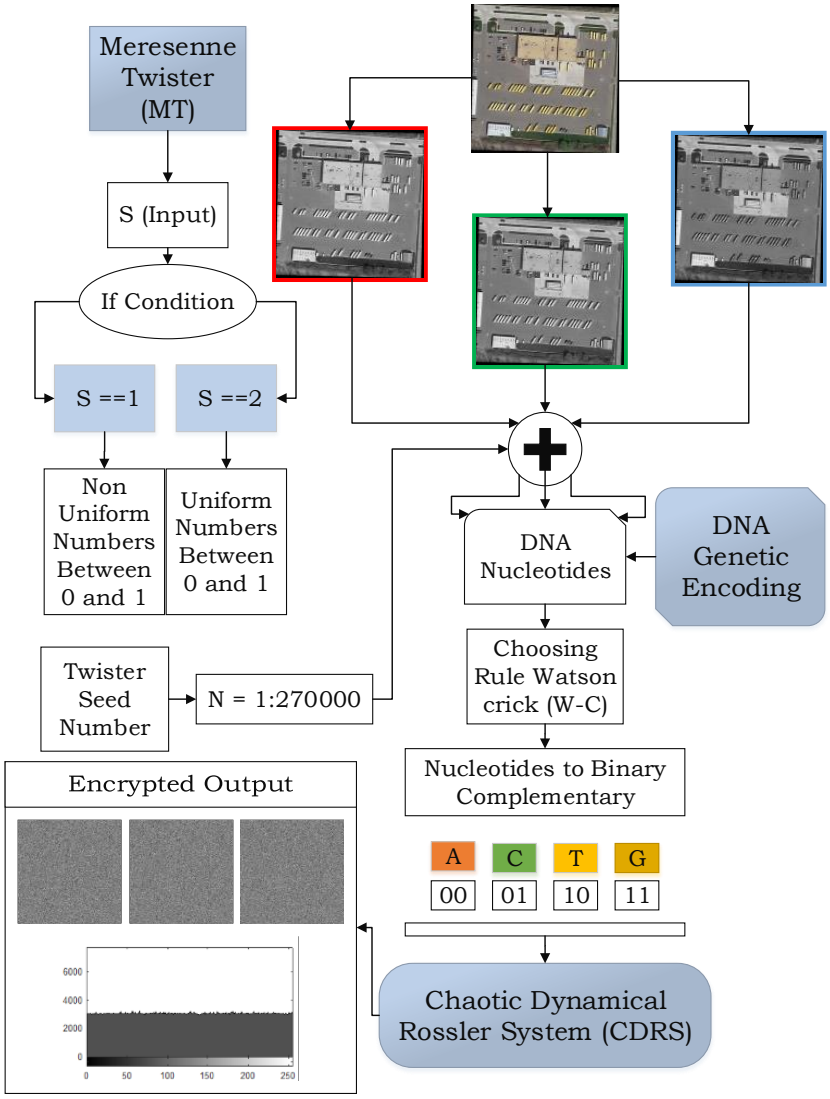

Figure 5. Flow chart of aerial view images encryption.

Figure 6. Aerial view photography 1: Yellow and white buses.

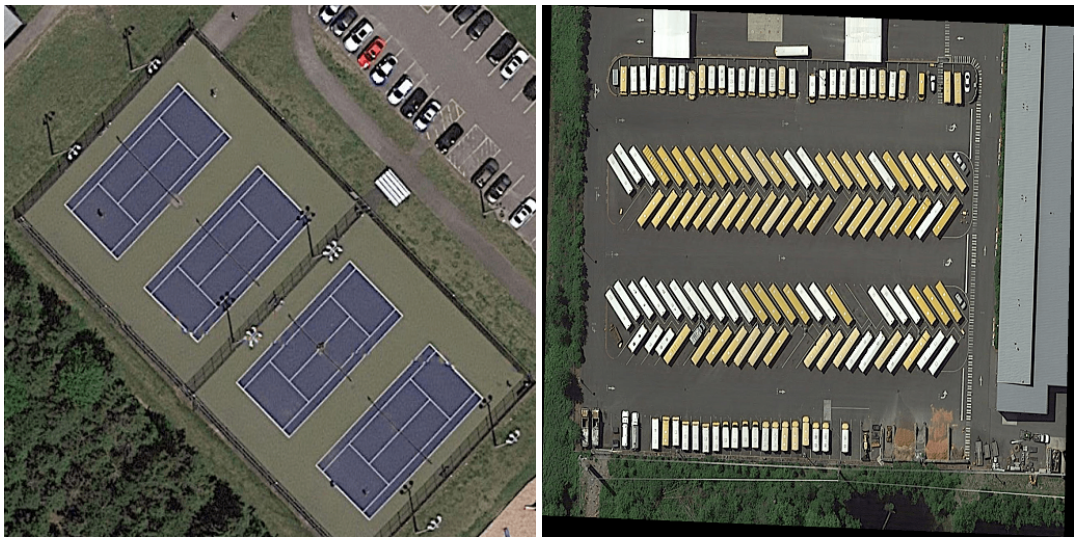

Figure 7. Aerial view photography 2: Cars and mixed buses.

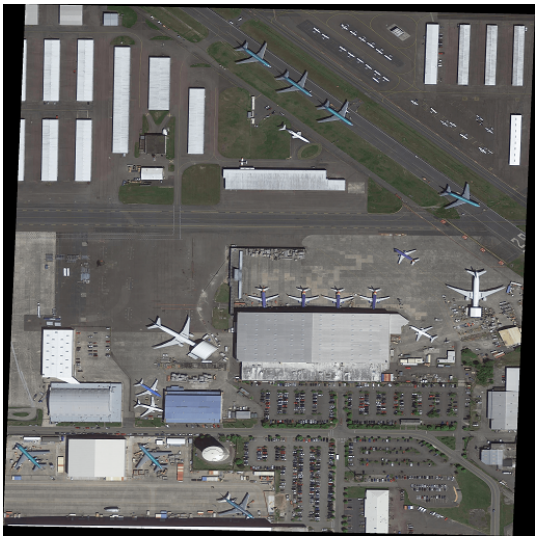

Figure 8. Aerial view photography 3: airplanes.

5.1. Histogram Consistency Analyses and Its Variance

The test is applied in order to examine the distribution of pixels within each channels of the colour image. The regularity of the pixels depends on the randomness (random numbers) that have been produced through the presented scheme. In contrast, the non-uniformity of the pixels indicate that the system is not performing well with the generated random numbers. Maximum randomness is achieved when the pixels are distorted at MT level, and are further inserted to DNA genetic encoding and CDRS. The uniformity has been assessed by the distribution of the pixel's value with χ^2 and the variance of the histogram analysis. The variance with its 256 grey level is defined in Equation (7)

$$\mathrm{var}(Z) = \frac{1}{256^2} \sum_{i=0}^{255} \sum_{j=0}^{255} \frac{1}{2} \left(z_i - z_j\right)^2 \tag{7}$$

whereas in Equation (7), as mentioned earlier the value of $Z = \{z_0, z_1, \cdots, z_{255}\}$ is the vector representing histogram values. Both Z_i as well as Z_j indicate the total number of pixels whose grey level value is equivalent to i and j. Visually histograms for channels wise and full-coloured images with a 3D surface is investigated. In Figure 9, the colored image based on yellow buses is divided into three respective grey layers. The grey layers are initially treated by the MT process in phase 1.

The encrypted layers are shown in Figure 10. The highly encrypted grey layers are obtained after XOR and the permutation process in phases 2, and 3 (DNA, CDRS) respectively as shown in Figure 11. In Figures 12–14 are the plain and encrypted histogram layers (R, G, and B) where R = red, G = green, and B = blue using MT method. The randomness of the pixels is increased by executing additional layers of DNA and CDRS, as shown in Figures 15 and 16. The final encrypted image with its respective histogram is shown in Figure 17. The layers are further examined using a three-dimensional surface process. The pixels of the final three encrypted images are depicted in Figures 18–20. The uniformity of the pixels in encrypted layers implies that the proposed scheme generates maximum random values.

Figure 9. Aerial view photography 1, plain image with three layers (red, green, blue) of yellow buses. Images measures 512 × 512 × 3 and each of three layers measures 512 × 512.

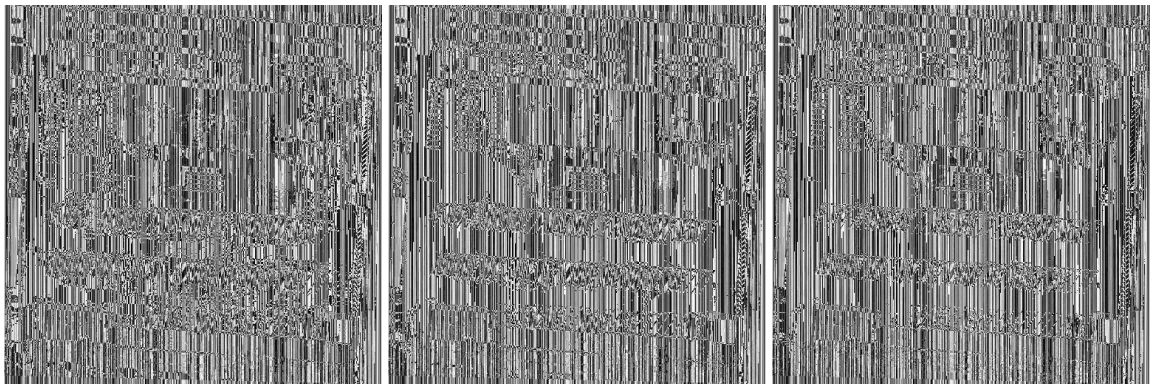

Figure 10. Aerial view photography 1, encrypted image three layers (R, G, B) of yellow buses using MT method : Each layer size 512 × 512.

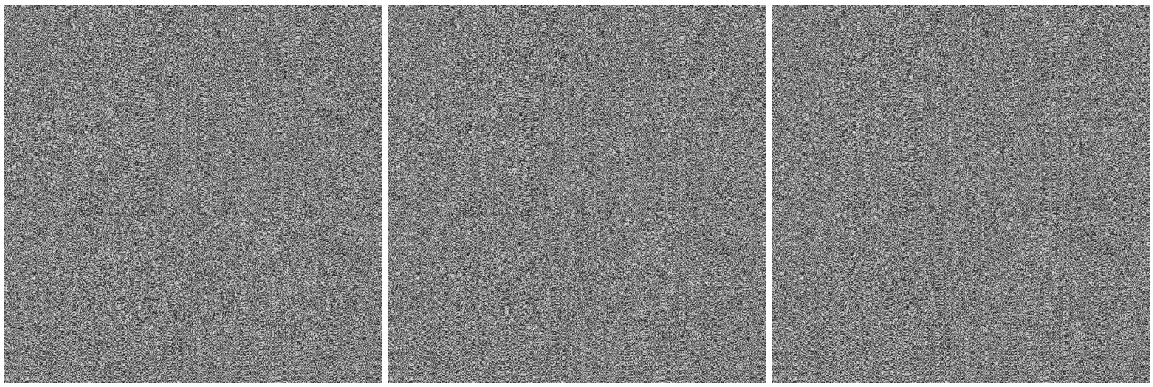

Figure 11. Aerial view photography 1, encrypted image with three layers (R, G, B) of yellow buses using DNA and Rossler system. Each layer measure 512 × 512.

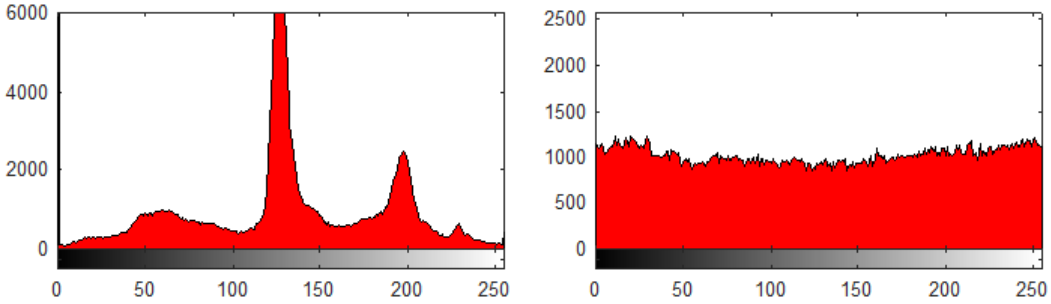

Figure 12. Red layer using the MT method: plain image (**left**) and encrypted image (**right**) histogram.

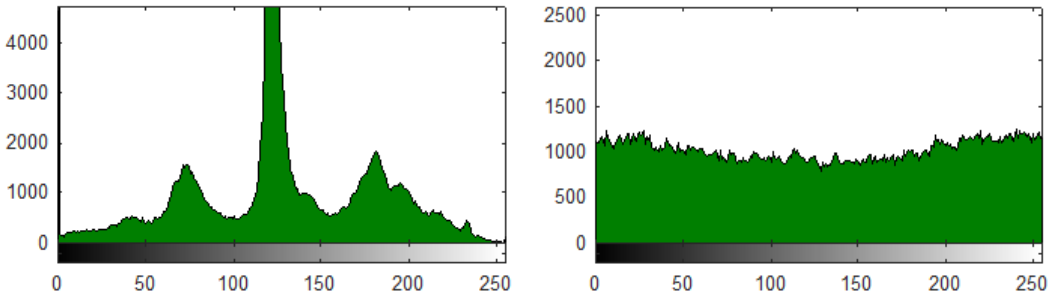

Figure 13. Green layer using the MT method: plain image (**left**) and encrypted image (**right**) histogram.

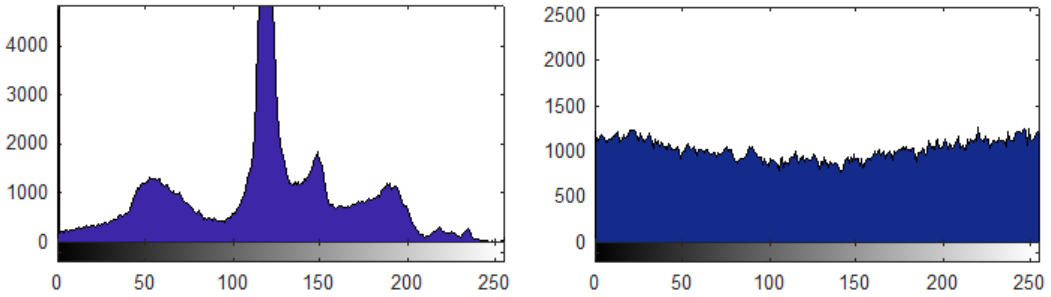

Figure 14. Blue layer using the MT method: plain image (**left**) and encrypted image (**right**) histogram.

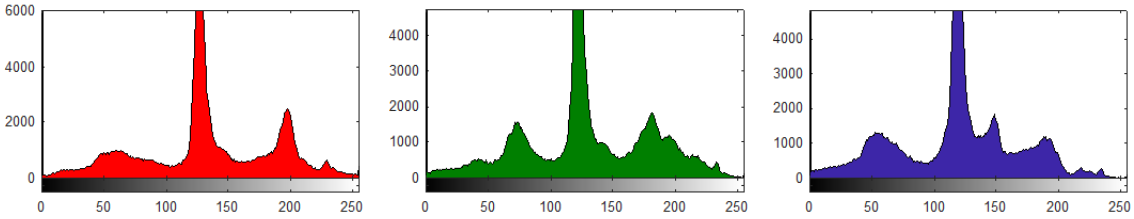

Figure 15. Aerial view photography 1, plain image three layers (R, G, B) of yellow buses measuring 512 × 512 × 3. Each histogram alone measures 512 × 512.

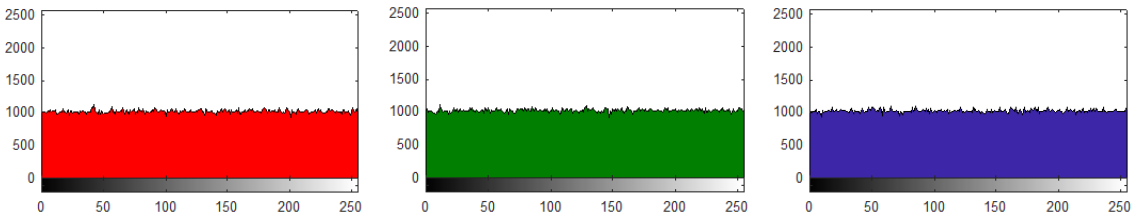

Figure 16. Aerial view photography 1, encrypted image with three layers (R, G, B) of yellow buses measuring 512 × 512 × 3. Each histogram alone measures 512 × 512.

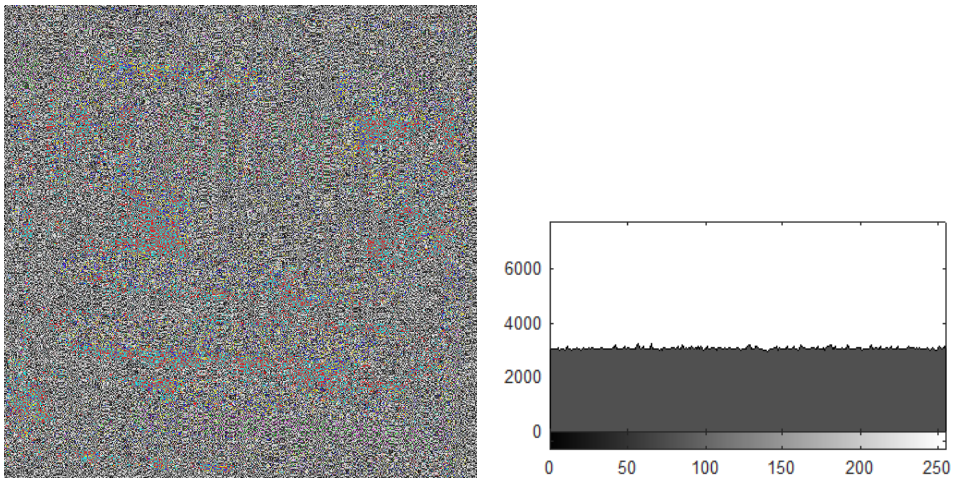

Figure 17. Aerial view photography 1, colored encrypted image of yellow buses measuring 512 × 512 × 3 and its respective histogram.

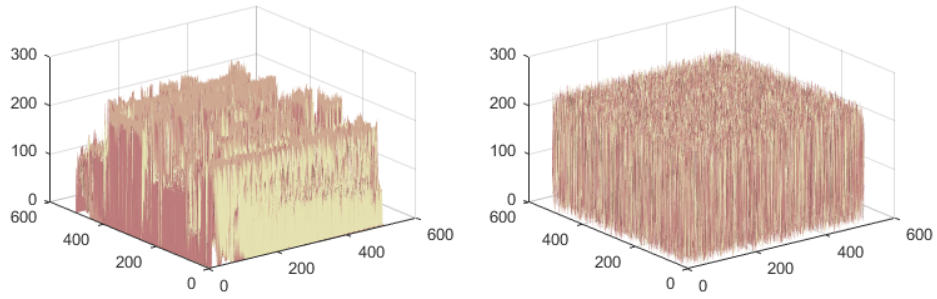

Figure 18. Aerial view photography 1, red layer 3D surface histogram with plain image (**left**) and encrypted counterpart (**right**).

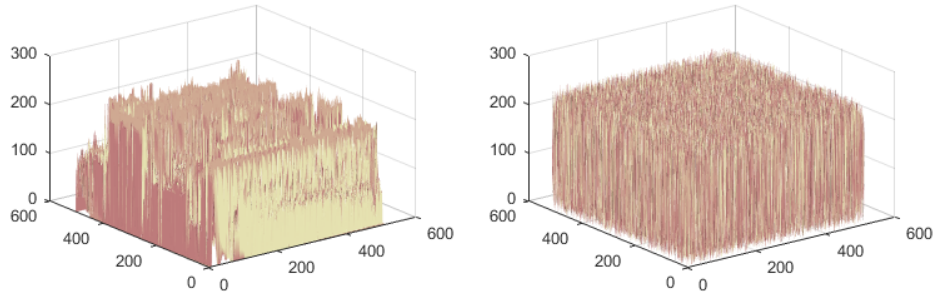

Figure 19. Aerial view photography 1, green layer 3D surface histogram with plain image (**left**) and encrypted counterpart (**right**).

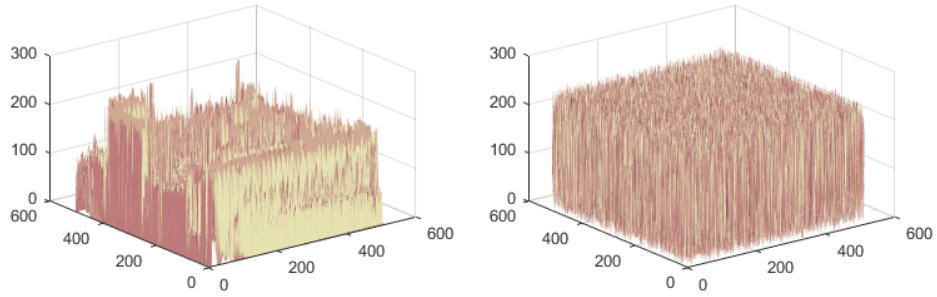

Figure 20. Aerial view photography 1, blue layer 3D surface histogram with plain image (**left**) and encrypted counterpart (**right**).

5.2. Visual Strength Analysis

Visual Strength Analysis (VSA) intends to investigate the visual quality of an image using a Gray Level Co-occurrence Matrix (GLCM). The necessary tests that are included in VSA are the homogeneity level, energy level and contrast level test. Homogeneity level examines the pixels diagonally. The energy level can be examined by an aggregate squared method. The texture of an object is recognized by contrast analysis. The tests are elaborated as follows:

5.2.1. Homogeneity Level

The closeness of distribution in GLCM is used to find the homogeneity level. Mathematically the statistical parameter is defined in Equation (8):

$$H = \sum_{x,y=1}^{M} \frac{g(x,y)}{1+|x-y|}. \tag{8}$$

In each case, the value under evaluation must be properly sized in order to validate our proposed method. The average homogeneity test result values for colored images of $512 \times 512 \times 3$ dimensions are tabulated in Table 2 while layer-wise homogeneity result for 5 types of aerial images are shown in Tables 3–7. The calculated values are less than 0.4, which indicates the higher levels of security achieved by the proposed scheme.

Table 2. The calculated values of average homogeneity, energy, and contrast analysis.

S. No.	Algorithms	Avg. Homogeneity	Avg. Energy	Avg. Contrast
1	Proposed	0.3894	0.0156	10.5240
2	Yellow buses	0.3901	0.0156	10.5209
3	Airplanes	0.3899	0.0156	10.5046
4	White buses	0.3894	0.0156	10.4931
5	Cars	0.3897	0.0156	10.5124
6	Fadia et al. [43]	0.5428	0.0262	6.6862
7	Fadia et al. [43]	0.4653	0.0204	7.7000
7	Fadia et al. [43]	0.4941	0.0251	6.7512
8	Fadia et al. [43]	0.4312	0.0211	7.8101
9	Fadia et al. [43]	0.5389	0.0204	7.6801
10	Fadia et al. [43]	0.5401	0.0258	6.6911
11	Fadia et al. [43]	0.4644	0.0210	7.7123
12	Ahmad et al. [30]	0.9307	0.2093	0.2307
13	Ahmad et al. [30]	0.9216	0.2181	0.2388
14	Ahmad et al. [30]	0.9411	0.2088	0.2403
15	Ahmad et al. [30]	0.9455	0.2133	0.2219

Table 3. Layer wise homogeneity, energy, and contrast test for yellow white buses image.

S. No.	Images	Tests	Layers	Values
1	Yellow white buses	Homogeneity	R-layer	0.3896
2	Yellow white buses	Homogeneity	G-layer	0.3893
3	Yellow white buses	Homogeneity	B-layer	0.3893
4	Yellow white buses	Energy	R-layer	0.0156
5	Yellow white buses	Energy	G-layer	0.0156
6	Yellow white buses	Energy	B-layer	0.0156
7	Yellow white buses	Contrast	R-layer	10.5433
8	Yellow white buses	Contrast	G-layer	10.5240
9	Yellow white buses	Contrast	B-layer	10.5048

Table 4. Layer wise homogeneity, energy, and contrast test for yellow buses image.

S. No.	Images	Tests	Layers	Values
1	Yellow buses	Homogeneity	R-layer	0.3903
2	Yellow buses	Homogeneity	G-layer	0.3901
3	Yellow buses	Homogeneity	B-layer	0.3899
4	Yellow buses	Energy	R-layer	0.0156
5	Yellow buses	Energy	G-layer	0.0156
6	Yellow buses	Energy	B-layer	0.0156
7	Yellow buses	Contrast	R-layer	10.5331
8	Yellow buses	Contrast	G-layer	10.5095
9	Yellow buses	Contrast	B-layer	10.5201

Table 5. Layer wise homogeneity, energy, and contrast test for airplanes image.

S. No.	Images	Tests	Layers	Values
1	Airplanes	Homogeneity	R-layer	0.3902
2	Airplanes	Homogeneity	G-layer	0.3898
3	Airplanes	Homogeneity	B-layer	0.3899
4	Airplanes	Energy	R-layer	0.0156
5	Airplanes	Energy	G-layer	0.0156
6	Airplanes	Energy	B-layer	0.0156
7	Airplanes	Contrast	R-layer	10.4993
8	Airplanes	Contrast	G-layer	10.5172
9	Airplanes	Contrast	B-layer	10.4975

Table 6. Layer wise homogeneity, energy, and contrast test for white buses image.

S. No.	Images	Tests	Layers	Values
1	White buses	Homogeneity	R-layer	0.3895
2	White buses	Homogeneity	G-layer	0.3895
3	White buses	Homogeneity	B-layer	0.3893
4	White buses	Energy	R-layer	0.0156
5	White buses	Energy	G-layer	0.0156
6	White buses	Energy	B-layer	0.0156
7	White buses	Contrast	R-layer	10.4965
8	White buses	Contrast	G-layer	10.4914
9	White buses	Contrast	B-layer	10.4916

Table 7. Layer wise homogeneity, energy, and contrast test for cars image.

S. No.	Images	Tests	Layers	Values
1	Cars	Homogeneity	R-layer	0.3896
2	Cars	Homogeneity	G-layer	0.3900
3	Cars	Homogeneity	B-layer	0.3897
4	Cars	Energy	R-layer	0.0156
5	Cars	Energy	G-layer	0.0156
6	Cars	Energy	B-layer	0.0156
7	Cars	Contrast	R-layer	10.5244
8	Cars	Contrast	G-layer	10.4944
9	Cars	Contrast	B-layer	10.5185

5.2.2. Energy Level

Energy test monitors the actual information content. The test is based upon mean squared values as demonstrated in Equation (9):

$$\text{Energy } = p(\boldsymbol{x}, \boldsymbol{y})^2. \tag{9}$$

The test has been conducted using GLCM. The valid range of energy lies in [0, 1]. It is essential to have a smaller value for an encrypted image in order to validate the presented scheme. The value of 0.156 is obtained for all the colored and channel-wise aerial images, which is shown in Tables 2–7. The results validated the proposed scheme.

5.2.3. Contrast Level

Contrast experiment is used to explore the texture of an image. The analysis is suitable to find the intensity level of the pixels. The test is defined in Equation (10):

$$\text{Contrast} = \sum_{i,j=1}^{M} |x - y|^2 p(x, y). \tag{10}$$

It is essential to attain a large value to validate the proposed scheme, that is to show its robustness and statistically better resistance against external attacks. The results are shown for five distinct coloured aerial images, and the test is implemented on three grey layers as well. The values of contrast analysis are shown in Tables 2–7. The assessed values are greater than '10' which depicts that the calculated results are valid and ensures the potential robustness of the presented scheme. The cryptosystem proposed can be executed in order to secure real-time communication.

5.3. Adjacent Pixels Correlation Analysis

The plain images are transformed in such a way that they become visually meaningless as every pixel is distorted through our encryption procedures. The presented scheme must avoid any statistical attack by reducing the correlation among the pixels. The correlation among pixels is reduced to conceal the actual image data. We have selected certain large aerial images. The test is defined in Equations (11)–(13):

$$r_{xy} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{D(x)D(y)}} \tag{11}$$

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i \tag{12}$$

$$D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2. \tag{13}$$

The expectation of the variable x can be calculated by $E(x)$ and the variance by $D(x)$. The total number of pixels are denoted by N which is equal to 512×512. The calculated values are shown in Table 8. The extreme values of the correlation analysis are 0 and 1. The value that converges to 1 indicates that the adjacent pixels are decidedly correlated, while 0 demonstrates that these pixels are highly dissimilar and dispersed in actual range from 0 to 255. All the values in the table for an encrypted image are less than 0, as shown in Table 8. The resulting images are depicted in Figures 21–23.

Table 8. Correlation coefficient values for each dimension wherein: H-D = Horizontal dimension, D-D = Diagonal dimension, V-D = Vertical dimension, A-V = Cumulative average value.

	Plain Image Dimensions					**Encrypted Image Dimensions**			
	Images	**H-D**	**D-D**	**V-D**	**A-V**	**H-D**	**D-D**	**V-D**	**A-V**
1	Proposed	0.9066	0.7743	0.8117	NA	−0.0014	0.0039	−0.0027	NA
2	Yellow buses	0.9111	0.8046	0.8896	NA	−0.0015	-0.0008	−0.0385	NA
3	Airplanes	0.9408	0.8775	0.9210	NA	−0.0002	0.0023	−0.0017	NA
4	White buses	0.8652	0.8507	0.9669	NA	−0.0002	0.0011	−0.0033	NA
5	Cars	0.8468	0.7570	0.8597	NA	−0.0025	0.0018	−0.0009	NA

Table 8. *Cont.*

	Plain Image Dimensions					Encrypted Image Dimensions			
	Images	**H-D**	**D-D**	**V-D**	**A-V**	**H-D**	**D-D**	**V-D**	**A-V**
6	Ref. [44]	0.9727	0.9204	0.9573	-	−0.0394	-0.0194	-0.0223	-
7	Ref. [45]	-	-	-	-	0.0681	0.0128	0.0049	-
8	Ref. [46]	-	-	-	-	0.0965	0.0362	−0.0581	-
9	Ref. [47]	-	-	-	-	0.1257	0.0226	0.0581	-

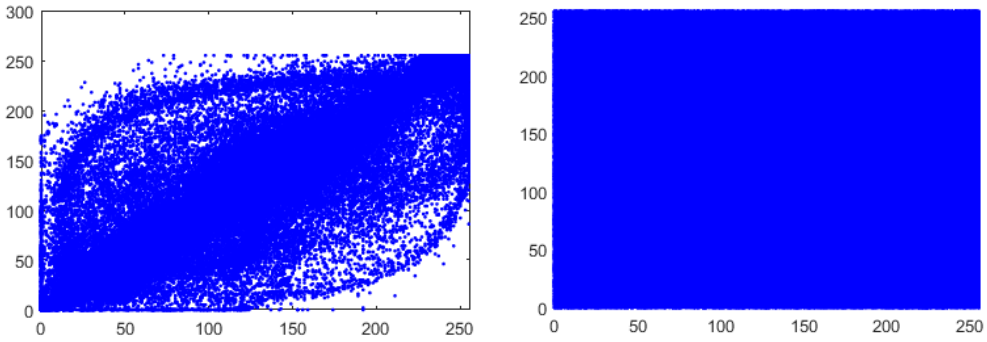

Figure 21. Correlation coefficient: Aerial view photography 1, plain (**left**) and encrypted (**right**) image pixels in horizontal view.

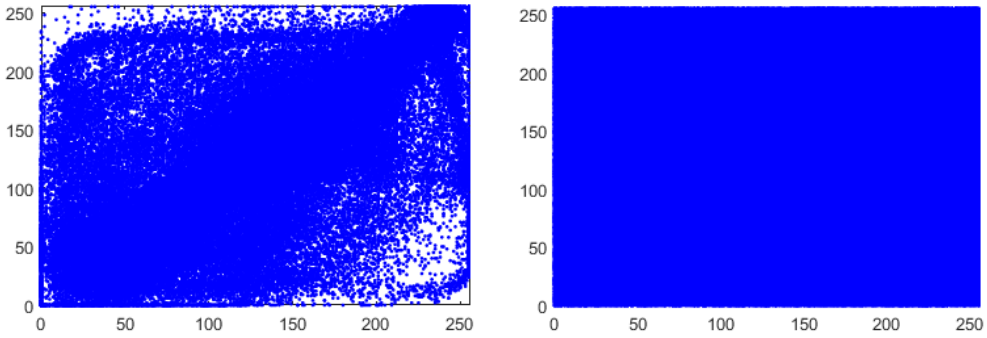

Figure 22. Correlation coefficient: Aerial view photography 1, plain (**left**) and encrypted (**right**) image pixels in diagonal view.

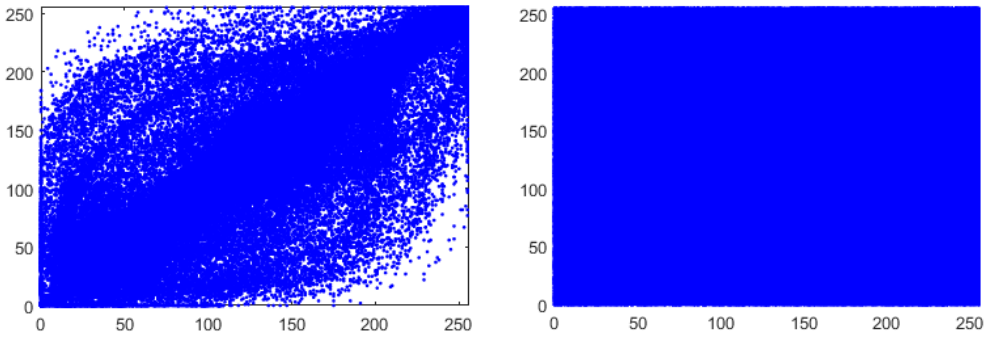

Figure 23. Correlation coefficient: Aerial view photography 1, plain (**left**) and encrypted (**right**) image pixels in vertical view.

5.4. Information Randomness and Uncertainty Analysis

The most appropriate test to find the security level of the proposed system is the entropy test, which measures the degree of randomness present in the source of information. Here entropy, $H(mm_i)$,is defined in Equation (14):

$$H(m) = \sum_{i=0}^{2^*-1} p\,(m_i) \log \frac{1}{p\,(m_i.)} \tag{14}$$

In the equation above, the $P(m_i)$ is the probability occurrence of message signal m_i. The test is applied to certain aerial images captured through UAV. Entropy has a theoretical value of 8 and by converging here, the value indicates that the pixel values from 0 and 255 are randomly distributed in the cipher images, thereby making the actual image data concealed in a better way. The attacker must not be able to crack any image data from the encrypted form. The results of this test are recorded in Table 9 for each of the five aerial view images. The channel-wise results are shown in Table 10 and then compared with several other current processes, as outlined in both Tables 10 and 11.

Table 9. Information entropy test for various aerial images.

S. No	Name	Yellow White Buses	Yellow Buses	Airplanes	White Buses	Cars
1	Actual Entropy	7.0899	7.2618	7.0868	6.9841	6.9906
2	Ideal Entropy	8.0000	8.0000	8.0000	8.0000	8.0000
3	Ciphered Entropy	7.9999	7.9997	7.9997	7.9998	7.9998

Table 10. Layer wise entropy test for various standard images.

S. No.	Images	Layers	Values
1	Yellow white buses	Red	7.9994
		Green	7.9993
		Blue	7.9993
2	Yellow buses	Red	7.9994
		Green	7.9993
		Blue	7.9993
3	Airplanes	Red	7.9993
		Green	7.9992
		Blue	7.9994
4	White buses	Red	7.9993
		Green	7.9994
		Blue	7.9994
5	Cars	Red	7.9992
		Green	7.9993
		Blue	7.9993
6	Liu et al. [48]	Red	7.9791
		Green	7.9802
		Blue	7.9827
7	Wu et al. [49]	Red	7.9893
		Green	7.9898
		Blue	7.9894

Table 11. The comparison of entropy values.

S. No.	Algorithms	Entropy Values
1	Ideal	8.0000
2	Proposed	7.9998
3	Sun et el. [50]	7.9965
4	Baptisa et al. [50]	7.9260
4	Wong et al. [50]	7.9690
5	Xiang et al. [50]	7.9950

5.5. Pixel's Inconsistency Analysis

5.5.1. Mean Square Analysis

This security test is utilized in order to assess the reliability of our suggested scheme. MSE can be calculated between the original plain image $P(i,j)$ and the ciphered image $C(i,j)$. Mathematically, MSE is defined as outlined in Equation (15):

$$\text{MSE} = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{n} (\text{X}(i,j) - \text{Y}(i,j))^2, \tag{15}$$

where $M \times N$ denotes the total image size. It is desirable to have high value for MSE, and it signifies high-level of security. The MSE values for several UAV-based aerial images are shown in Table 12. The value we proposed is now compared with the work conducted by Younas et al. Table 13. The estimated values indicate that robust security is achieved using three-phase encryption process. Three plain images are considered for its counterpart encrypted images to show the MSE level, which is shown in Figures 24 and 25. The encrypted part of each colored image is shown in Figure 26.

Table 12. Calculated MSE and PSNR values.

S. No.	Algorithms	MSE Values	PSNR Values
1	Proposed	9.8755^{03}	29.0110 (db)
2	Yellow buses	7.5083^{03}	27.8456 (db)
3	Airplanes	8.1728^{03}	28.6258 (db)
4	White buses	8.1946^{03}	28.7089 (db)
5	Cars	7.5252^{03}	29.2284 (db)

Table 13. Comparison of MSE and PSNR values.

S. No.	Algorithms	MSE Values	PSNR Values
1	Proposed	9.8755^{03}	29.0110 (db)
2	Younas et al. [35]-Lena	4859.03	11.30
3	Younas et al. [35]-Baboon	6399.05	10.10
4	Younas et al. [35]-Pepper	7274.44	9.55

Figure 24. Colored aerial images: Yellow buses, Cars, and Airplanes.

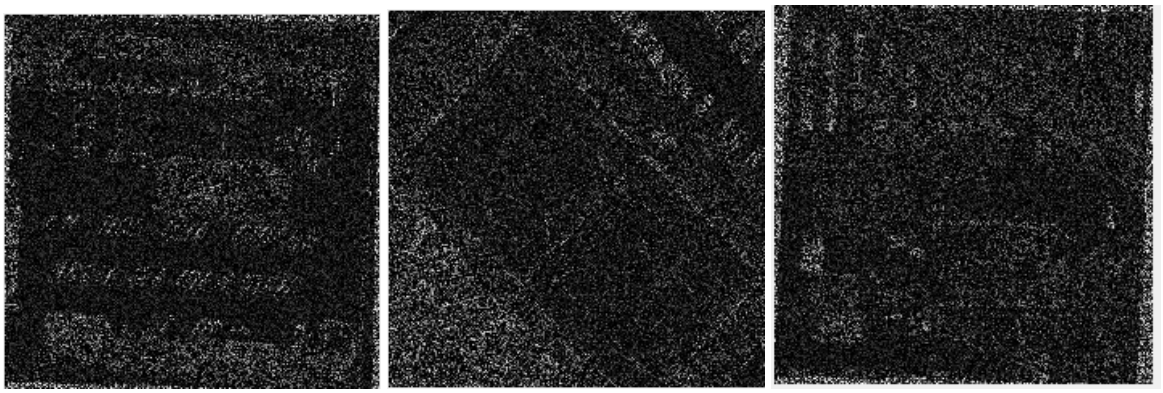

Figure 25. MSE of aerial images: Yellow buses, cars, and Airplanes.

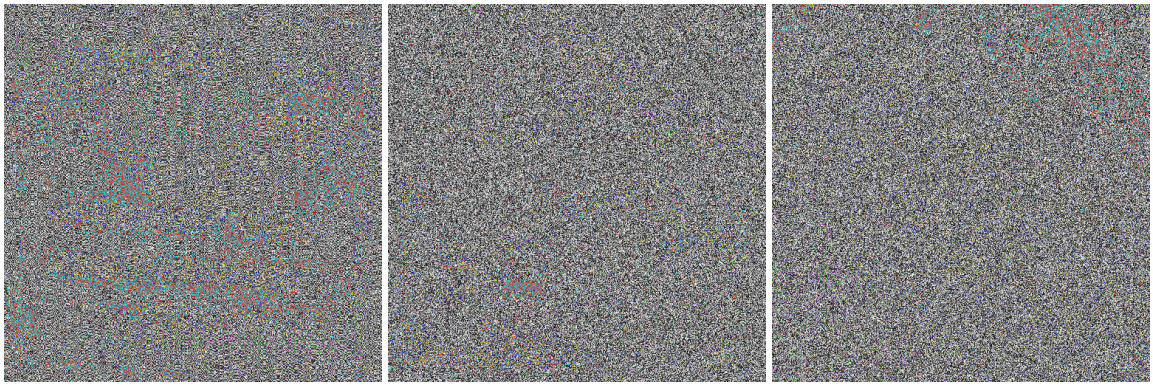

Figure 26. Encryption results of Figure 24.

5.5.2. Peak to Signal Noise Ratio

This metric is utilized in order to evaluate the quality of an encryption. The statistical test is described in Equation (16):

$$\text{PSNR} = 10 \times \log_{10}\left(\frac{255 \times 255}{\text{MSE}}\right) \tag{16}$$

In Equation (16) above, it is shown that the increase in MSE value also results in a decrease in PSNR. The two crucial security parameters are contrary to each other, that is, increasing one quantity decreases another. For better image encryption process, the value of PSNR should be high. We have calculated PSNR value in decibels as shown in Table 12, and the result is compared with one of the existing schemes, as demonstrated in Table 13. The results have validated the proposed scheme.

5.6. Average Difference

This criterion is utilized in order to identify the average difference of pixels between the original plain image and its encrypted counterpart. This test has applications in various fields such as image processing techniques, image quality, object detection and recognition systems. The value for AD must be high which implies that there must be large difference between plain image and encrypted counterparts. The equation for AD is shown in Equation (17):

$$AD = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j) - y(i,j)). \tag{17}$$

In the above equation, $x(i,j)$ are plain images and $y(i,j)$ are cipher images. M indicates image width and N indicates image height and overall measure is $512 \times 512 \times 3$. The test results of AD are shown in Table 14 and these results validated the cryptosystem we have proposed.

Table 14. Calculated AD and MD values.

S. No.	Algorithms	AD Values	MD Values
1	Proposed	23.9291	255
2	Yellow buses	32.3314	255
3	Airplanes	24.0846	255
4	White buses	23.1922	253
5	Cars	17.6097	255

5.7. Maximum Difference

Maximum Difference (MD) is extensively used to differentiate two images. With this process, we find out the actual difference between the pixels of both the original and the encrypted images. Here, the higher value of MD implies the existence of a large difference between the source image and its encrypted counterpart. By contrast, the low value of MD implies that the intimated scheme is weak; thus, the robustness of the scheme towards statistical attack is small making it more susceptible to other attacks as well. Mathematically the test is defined in Equation (18):

$$MD = MAX|x(i,j) - y(i,j)| \tag{18}$$

whereas in the aforementioned Equation (18), $x(i,j)$ and $y(i,j)$ are two images for which we are calculating MD. The $x(i,j)$ denotes the plain image while $y(i,j)$ denotes encrypted image. The test is applied to numerous channels of different aerial images. The estimated values are shown in Table 14. As indicated in Table 14, differences between pixels of these two images are high. The results in Table 14 has validated the requirement of a secure cryptosystem.

5.8. Pixels Similitude Analyses

The subsection is divided into three types of tests, that is, NCC, SC, and NAE. The criteria are explained in subsequent subsections.

5.8.1. Normalized Cross Correlation

The test is conducted to determine the levels of similarity, if any between two images through cross correlation analysis. This is expressed in Equation (19):

$$NCC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j) - y(i,j))}{\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j))^2}. \tag{19}$$

Here we compare the plain image and cipher counterpart.

In Equation (19) above, $x(i,j)$ indicates the plain image while $y(i,j)$ indicate the cipher counterpart. M denotes the width of the image and N denotes the height. The range of NCC lies in $[-1, 1]$ where values approaching 1 indicates that the correlation among pixels is weak and value of -1 indicate high correlation. We applied NCC on various aerial photography to see the normalized correlation of plain and encrypted image to authenticate the proposed scheme. The results as depicted by Table 15 make clear that relation of pixels in the encryption case is not strong.

Table 15. Calculated values of NCC, SC, and NAE .

S. No.	Images	Test	Calculated Values
1	Proposed	NCC	1
	-	SC	0.5934
	-	NAE	0.8404

Table 15. *Cont.*

S. No.	Images	Test	Calculated Values
2	Yellow buses	NCC	1
	-	SC	0.8759
	-	NAE	0.5519
3	Airplanes	NCC	1
	-	SC	0.5950
	-	NAE	0.7207
4	White buses	NCC	1
	-	SC	0.5643
	-	NAE	0.7390
5	Proposed	NCC	1
	-	SC	0.4511
	-	NAE	0.7667

5.8.2. Structural Content

This measure intends to identify any structural relationship between aggregate weight of two images. The plain and encrypted images must have no close relationship with each other. SC is defined in Equation (20):

$$SC = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (y(i,j))^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} (x(i,j))^2}. \tag{20}$$

As above $M \times N$ denotes the image size through its height and width. Similarly $x(i,j)$ and $y(i,j)$ denote the two test images (plain and cipher).

The value nearest unity demonstrate that there is strong relationship between the structural content of both plain and encrypted image. The calculated list of values is not close to unity, as shown in Table 15, which implies the relationship is weak for the suggested scheme. The average value of 0.5, intimates that high confusion, diffusion, and noise is added to the source images to obtain highly secure cryptosystem.

5.8.3. Normalized Absolute Error

The NAE is one of the popular security metrics to determine the encryption quality of an image. The metric determines the absolute error to differentiate the plain and encrypted image. The test is defined in Equation (21):

$$NAE = \frac{\sum_{m=1}^{M} \sum_{n=1}^{N} |x(m,n) - x^{\wedge}(m,n)|}{\sum_{m=1}^{M} \sum_{n=1}^{N} |x(m,n)|}. \tag{21}$$

In the above Equation (21), $x(m,n)$ is the plain image that has m rows and n columns. $x^{\wedge}(m,n)$ is the cipher image. The Equation (21) calculate the absolute error between plain and encrypted image. The larger estimated value of NAE, for example, approaching unity, indicates the good nature of the scrambled image. The values of NAE are calculated for various aerial images that are depicted in Table 15. The average value here is greater than 0.7, which indicates that a higher level of security has been achieved. A comparison between our results and the NCC, SC,and NAE values obtained by Younas et al. [35] is made in Table 16. Here the improved result of our works are demonstrated.

Table 16. Comparative values of NCC, SC, and NAE.

S. No.	Images	Avg Results (R, G, B)	Calculated Values
1	Younas et al. [35]-Lena	NCC	0.9145
	-	SC	0.9163
	-	NAE	0.6456
2	Younas et al. [35]-Baboon	NCC	0.8813
	-	SC	0.7944
	-	NAE	0.6527
3	Younas et al. [35]-Airplane	NCC	0.6614
	-	SC	1.6114
	-	NAE	0.4600
4	Younas et al. [35]-Pepper	NCC	0.9639
	-	SC	0.7615
	-	NAE	0.8420

5.8.4. Time Complexity

The level of efficiency of any cryptographic algorithm can be judged by its computational/time complexity which is also known as execution time for an encryption scheme. The execution time is calculated for each channel at three different phases and results are shown in Table 17. From Table 18, we can note that the proposed system is computationally agile comparing to existing cryptosystems. The execution time is calculated using Windows 10 pro, Matlab 2017 (a) version, with a CPU core^{TM} i3 3227U, 1.9 GHZ, and 4 GB RAM.

Table 17. Layer wise time complexity of the proposed scheme.

S. No.	Images	Layers	Calculated Time (sec)
1	Proposed-Phase 1	Red	0.000917
		Green	0.000355
		Blue	0.000319
2	Proposed-Phase 2	Red	0.000323
		Green	0.000655
		Blue	0.000212
3	Proposed-Phase 3	Red	0.000216
		Green	0.000325
		Blue	0.000307
4	Total Execution Time	All	0.003629

Table 18. Time complexity of the proposed scheme and its comparison.

S. No.	Images	Calculated Time (sec)
1	Proposed Scheme	0.003
2	Ahmad et al. [12]-Pepper	3.68
3	Ahmed et al. [51]-pepper	2.76
4	Khan et al. [16]-pepper	2.17
5	Ahmad et al. [12]-Lena	3.23
6	Ahmed et al. [51]-Lena	2.25
7	Khan et al. [16]-Lena	2.14

6. Concludings Remarks and Future Projections

In this study, we presented a novel encryption algorithm designed to guarantee secure transmission of aerial images. The system has appropriated numerous phases of aerial photography

encryption process using random sequencing of DNA and MT. XORed operation is applied on all channels of an aerial image. Furthermore, the permutation process is employed using CDRS to strengthen the security of the proposed solution. The proposed algorithm is further subjected to multiple experiments conducted to confirm the robustness and security analyses. Finally, the algorithm and its results are compared to several other existing methods in the literature. It is evident from all security measures that the proposed scheme is secure against many attacks including entropy and correlation, and so forth. In future, we will investigate the proposed encryption method for securing remote sensing big data [52–55]. Moreover, our future goal is to compare the security level of the proposed scheme with other traditional cryptosystems such as AES and DES. Another challenging topic to be explored is the feasibility of the proposed scheme for real-time videos and audios. In fact, the proposed scheme provides high computational efficiency and chaos-based sensitivity, which can be beneficial in the case of real-time audio and video encryption.

Author Contributions: Conceptualization, F.M. and J.A.; methodology, J.A., F.M., W.B. and W.J.B.; software, F.M.; validation, J.A., W.B., A.A. and W.J.B.; formal analysis, F.M., J.A., and S.S.; investigation, F.M., J.A. and W.B.; resources, J.A. and F.M.; data curation, F.M., J.A., W.B. and S.S.; writing–original draft preparation, F.M., J.A. and S.S.; writing–review and editing, J.A., W.B., W.J.B., F.M., A.A. and S.R.; visualization, F.M.; supervision, J.A., W.B. and W.J.B.; project administration, J.A., W.B., and W.J.B.; funding acquisition, J.A., W.B. and S.R.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Noronha, S.; Nevatia, R. Detection and modeling of buildings from multiple aerial images. *IEEE Trans. Pattern Anal. Mach. Intell.* **2001**, *23*, 501–518. [CrossRef]
2. Hu, J.; Razdan, A.; Femiani, J.C.; Cui, M.; Wonka, P. Road network extraction and intersection detection from aerial images by tracking road footprints. *IEEE Trans. Geosci. Remote Sens.* **2007**, *45*, 4144–4157. [CrossRef]
3. Tang, T.; Zhou, S.; Deng, Z.; Zou, H.; Lei, L. Vehicle detection in aerial images based on region convolutional neural networks and hard negative example mining. *Sensors* **2017**, *17*, 336. [CrossRef] [PubMed]
4. Bashir, I.; Ahmed, F.; Ahmad, J.; Boulila, W.; Alharbi, N. A Secure and Robust Image Hashing Scheme Using Gaussian Pyramids. *Entropy* **2019**, *21*, 1132. [CrossRef]
5. Jithin, K.; Sankar, S. Colour image encryption algorithm combining, Arnold map, DNA sequence operation, and a Mandelbrot set. *J. Inf. Secur Appl.* **2020**, *50*, 102428. [CrossRef]
6. Sneha, P.; Sankar, S.; Kumar, A.S. A chaotic colour image encryption scheme combining Walsh–Hadamard transform and Arnold–Tent maps. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 1289–1308. [CrossRef]
7. Li, S.; Zheng, X. Cryptanalysis of a chaotic image encryption method. In Proceedings of the 2002 IEEE International Symposium on Circuits and Systems, Phoenix-Scottsdale, AZ, USA, 26–29 May 2002; Volume 2, p. II.
8. Guo, J.I. A new chaotic key-based design for image encryption and decryption. In Proceedings of the 2000 IEEE International Symposium on Circuits and Systems, Geneva, Switzerland, 28–31 May 2000; Volume 4, pp. 49–52.
9. Wang, X.Y.; Zhang, Y.Q.; Bao, X.M. A novel chaotic image encryption scheme using DNA sequence operations. *Opt. Lasers Eng.* **2015**, *73*, 53–61. [CrossRef]
10. Alroobaea, R.; Rubaiee, S.; Bourouis, S.; Bouguila, N.; Alsufyani, A. Bayesian inference framework for bounded generalized Gaussian-based mixture model and its application to biomedical images classification. *Inter. J. Imaging Syst. Technol.* **2019**. [CrossRef]
11. Xie, E.Y.; Li, C.; Yu, S.; Lü, J. On the cryptanalysis of Fridrich's chaotic image encryption scheme. *Signal Process.* **2017**, *132*, 150–154. [CrossRef]
12. Ahmad, J.; Hwang, S.O. A secure image encryption scheme based on chaotic maps and affine transformation. *Multimed. Tools Appl.* **2016**, *75*, 13951–13976. [CrossRef]
13. Ahmad, J.; Hwang, S.O. Chaos-based diffusion for highly autocorrelated data in encryption algorithms. *Nonlinear Dyn.* **2015**, *82*, 1839–1850. [CrossRef]

14. Khan, J.S.; ur Rehman, A.; Ahmad, J.; Habib, Z. A new chaos-based secure image encryption scheme using multiple substitution boxes. In Proceedings of the 2015 Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, Pakistan, 18 December 2015; pp. 16–21.
15. Khan, M.; Masood, F. A novel chaotic image encryption technique based on multiple discrete dynamical maps. *Multimed. Tools Appl.* **2019**, *78*, 26203–26222. [CrossRef]
16. Khan, M.; Masood, F.; Alghafis, A.; Amin, M.; Naqvi, S.I.B. A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and Brownian motion. *PLoS ONE* **2019**. [CrossRef]
17. Khan, M.; Masood, F.; Alghafis, A. Secure image encryption scheme based on fractals key with Fibonacci series and discrete dynamical system. *Neural Comput. Appl.* **2019**, 1–21. [CrossRef]
18. Masood, F.; Ahmad, J.; Shah, S.A.; Jamal, S.S.; Hussain, I. A Novel Hybrid Secure Image Encryption Based on Julia Set of Fractals and 3D Lorenz Chaotic Map. *Entropy* **2020**, *22*, 274. [CrossRef]
19. Ahmad, J.; Masood, F.; Shah, S.A.; Jamal, S.S.; Hussain, I. A Novel Secure Occupancy Monitoring Scheme Based on Multi-Chaos Mapping. *Symmetry* **2020**, *12*, 350. [CrossRef]
20. He, D.; He, C.; Jiang, L.G.; Zhu, H.w.; Hu, G.R. Chaotic characteristics of a one-dimensional iterative map with infinite collapses. *IEEE Trans. Circuits Syst. I Fundam. Theory Appl.* **2001**, *48*, 900–906.
21. Soleymani, A.; Nordin, M.J.; Sundararajan, E. A chaotic cryptosystem for images based on Henon and Arnold cat map. *Sci. World J.* **2014**, *2014*, 536930. [CrossRef]
22. Pareek, N.K.; Patidar, V.; Sud, K.K. Image encryption using chaotic logistic map. *Image Vision Comput.* **2006**, *24*, 926–934. [CrossRef]
23. Peng, J.; El-Atty, B.A.; Khalifa, H.S.; El-Latif, A.A.A. Image watermarking algorithm based on quaternion and chaotic Lorenz system. *Proc. SPIE* **2019**, *11179*, 111790W.
24. Zhang, T.J.; Manhrawy, I.; Abdo, A.; El-Latif, A.; Rhouma, R. Cryptanalysis of elementary cellular automata based image encryption. *Adv. Mater. Res.* **2014**, *981*, 372–375. [CrossRef]
25. Khan, J.; Ahmad, J.; Hwang, S.O. An efficient image encryption scheme based on: Henon map, skew tent map and S-Box. In Proceedings of the 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), Istanbul, Turkey, 27–29 May 2015; pp. 1–6.
26. Chai, X.; Gan, Z.; Yang, K.; Chen, Y.; Liu, X. An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations. *Signal Process. Image Commun.* **2017**, *52*, 6–19. [CrossRef]
27. Li, L.; Abd-El-Atty, B.; El-Latif, A.A.A.; Ghoneim, A. Quantum color image encryption based on multiple discrete chaotic systems. In Proceedings of the 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), Prague, Czech Republic, 3–6 September 2017; pp. 555–559.
28. Yin, L.; Zhao, J.; Duan, Y. Encryption scheme for remote sensing images based on EZW and chaos. In Proceedings of the 9th International Conference for Young Computer Scientists, Hunan, China, 18–21 November 2008; pp. 1601–1605.
29. Zhang, X.; Zhu, G.; Ma, S. Remote-sensing image encryption in hybrid domains. *Opt. Commun.* **2012**, *285*, 1736–1743. [CrossRef]
30. Ahmad, J.; Khan, M.A.; Hwang, S.O.; Khan, J.S. A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices. *Neural Comput. Appl.* **2017**, *28*, 953–967. [CrossRef]
31. Huang, X.; Ye, G.; Chai, H.; Xie, O. Compression and encryption for remote sensing image using chaotic system. *Secur. Commun. Netw.* **2015**, *8*, 3659–3666. [CrossRef]
32. Ye, G.; Huang, X. A novel block chaotic encryption scheme for remote sensing image. *Multimed. Tools Appl.* **2016**, *75*, 11433–11446. [CrossRef]
33. Zhang, X.; Wang, X. Remote-sensing image encryption algorithm using the advanced encryption standard. *Appl. Sci.* **2018**, *8*, 1540. [CrossRef]
34. Liu, H.; Zhao, B.; Huang, L. A Remote-Sensing Image Encryption Scheme Using DNA Bases Probability and Two-Dimensional Logistic Map. *IEEE Access* **2019**, *7*, 65450–65459. [CrossRef]
35. Younas, I.; Khan, M. A new efficient digital image encryption based on inverse left almost semi group and Lorenz chaotic system. *Entropy* **2018**, *20*, 913. [CrossRef]
36. Matsumoto, M.; Nishimura, T. Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Trans. Model. Comput. Simul.* **1998**, *8*, 3–30. [CrossRef]
37. Matsumoto, M.; Nishimura, T. Mersenne Twister: A Random Number Generator (Since 1997/10). Available online: www.math.sci.hiroshima-u.ac.jp/m-mat/MT/emt (accessed on 17 August 2007).

38. Cokus, S.; Matsumoto, M.; Nishimura, T.; Eddelbuettel, D. RANDMT: Octave Function to Produce Random Numbers via Mersenne Twister. Octave Codes. 2000. Available online: https://EconPapers.repec.org/RePEc:cod:octave:c021101 (accessed on 10 March 2020)
39. Jagannatam, A. Mersenne Twister—A Pseudo Random Number Generator and Its Variants. Available: http://cryptography.gmu.edu/~jkaps/download.php?docid=1083 (accessed on 12 March 2020)
40. Watson, J.D.; Crick, F. Molecular Structure of Nucleic Acids—A Structure for Deoxyribose Nucleic Acid. *Nature* **1953**, *421*, 397–3988. [CrossRef] [PubMed]
41. Rössler, O.E. An equation for continuous chaos. *Phys. Lett. A* **1976**, *57*, 397–398. [CrossRef]
42. Xia, G.S.; Bai, X.; Ding, J.; Zhu, Z.; Belongie, S.; Luo, J.; Datcu, M.; Pelillo, M.; Zhang, L. DOTA: A Large-Scale Dataset for Object Detection in Aerial Images. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Salt Lake City, UT, USA, 18–23 June 2018; pp. 3974–3983.
43. Khan, F.A.; Ahmed, J.; Khan, J.S.; Ahmad, J.; Khan, M.A. A novel substitution box for encryption based on Lorenz equations. In Proceedings of the 2017 International Conference on Circuits, System and Simulation (ICCSS), London, UK, 14–17 July 2017; pp. 32–36.
44. Ahmad, J.; Larijani, H.; Emmanuel, R.; Mannion, M. Secure occupancy monitoring system for iot using lightweight intertwining logistic map. In Proceedings of the 2018 10th Computer Science and Electronic Engineering (CEEC), Colchester, UK, 19–21 September 2018; pp. 208–213.
45. Rhouma, R.; Meherzi, S.; Belghith, S. OCML-based colour image encryption. *Chaos Solitons Fractals* **2009**, *40*, 309–318. [CrossRef]
46. Liu, H.; Wang, X. Color image encryption based on one-time keys and robust chaotic maps. *Comput. Math. Appl.* **2010**, *59*, 3320–3327. [CrossRef]
47. Huang, V.L.; Zhao, S.Z.; Mallipeddi, R.; Suganthan, P.N. Multi-objective optimization using self-adaptive differential evolution algorithm. In Proceedings of the 2009 IEEE Congress on Evolutionary Computation, Trondheim, Norway, 18–21 May 2009; pp. 190–194.
48. Liu, Z.; Xu, L.; Liu, T.; Chen, H.; Li, P.; Lin, C.; Liu, S. Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. *Opt. Commun.* **2011**, *284*, 123–128. [CrossRef]
49. Wu, X.; Li, Y.; Kurths, J. A new color image encryption scheme using CML and a fractional-order chaotic system. *PLoS ONE* **2015**, *10*, e0119660. [CrossRef]
50. Zhang, G.; Liu, Q. A novel image encryption method based on total shuffling scheme. *Opt. Commun.* **2011**, *284*, 2775–2780. [CrossRef]
51. Ahmed, F.; Anees, A.; Abbas, V.U.; Siyal, M.Y. A noisy channel tolerant image encryption scheme. *Wirel. Pers. Commun.* **2014**, *77*, 2771–2791. [CrossRef]
52. Chebbi, I.; Boulila, W.; Farah, I.R. Big data: Concepts, challenges and applications. In *Computational Collective Intelligence*; Springer International Publishing: Cham, Switzerland 2015; pp. 638–647.
53. Chebbi, I.; Boulila, W.; Farah, I.R. Improvement of satellite image classification: Approach based on Hadoop/MapReduce. In Proceedings of the 2016 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), Monastir, Tunisia, 16–19 March 2016; pp. 31–34.
54. Boulila, W.; Farah, I.R.; Hussain, A. A novel decision support system for the interpretation of remote sensing big data. *Earth Sci. Inf.* **2018**, *11*, 31–45. [CrossRef]
55. Boulila, W. A top-down approach for semantic segmentation of big remote sensing images. *Earth Sci. Inf.* **2019**, *12*, 295–306. [CrossRef]