applied sciences

MDPI

Article

Configurational Entropy for Optimizing the Encryption of Digital Elevation Model Based on Chaos System and Linear Prediction

Xinghua Cheng [1] and Zhilin Li [1,2,*]

[1] Department of Land Surveying and Geo-Informatics, The Hong Kong Polytechnic University, Hong Kong, China; xingh.cheng@connect.polyu.hk
[2] Faculty of Geosciences and Environmental Engineering, Southwest Jiaotong University, Chengdu 611756, China
* Correspondence: lszlli@polyu.edu.hk

Abstract: A digital elevation model (DEM) digitally records information about terrain variations and has found many applications in different fields of geosciences. To protect such digital information, encryption is one technique. Numerous encryption algorithms have been developed and can be used for DEM. A good encryption algorithm should change both the compositional and configurational information of a DEM in the encryption process. However, current methods do not fully take into full consideration pixel structures when measuring the complexity of an encrypted DEM (e.g., using Shannon entropy and correlation). Therefore, this study first proposes that configurational entropy capturing both compositional and configurational information can be used to optimize encryption from the perspective of the Second Law of Thermodynamics. Subsequently, an encryption algorithm based on the integration of the chaos system and linear prediction is designed, where the one with the maximum absolute configurational entropy difference compared to the original DEM is selected. Two experimental DEMs are encrypted for 10 times. The experimental results and security analysis show that the proposed algorithm is effective and that configurational entropy can help optimize the encryption and can provide guidelines for evaluating the encrypted DEM.

Keywords: digital elevation model; information security; chaos system; configurational information; configurational entropy

check for updates

Citation: Cheng, X.; Li, Z. Configurational Entropy for Optimizing the Encryption of Digital Elevation Model Based on Chaos System and Linear Prediction. *Appl. Sci.* **2021**, *11*, 2402. https://doi.org/10.3390/app11052402

Academic Editor: Yosoon Choi

Received: 2 February 2021
Accepted: 5 March 2021
Published: 8 March 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

A digital elevation model (DEM) is a digital representation of terrain variations and can explicitly reveal information about the topographic complexity with computer graphics. With the development of advanced equipment for data acquisition (e.g., high-resolution satellite sensors, unmanned aerial vehicle (UAV), and LiDAR (Light Detection and Ranging)), it is becoming more and more easy to acquire DEMs. In addition, DEM transmission becomes more and more frequent due to the development of advanced computer and network communication technologies. However, due to the openness and sharing of networks, there exists a serious threat in information security and confidentiality [1,2]. Therefore, information protection is desired and hence has attracted much attention. The literature on information protection can be traced back to Shannon's paper entitled "Communication Theory of Secrecy System" [3]. By now, numerous information protection methods have been proposed, and encryption is one such solution.

An increasing number of encryption algorithms have been developed to protect information from images as much as possible, and such algorithms can be employed to protect DEMs as well. Since chaotic systems are sensitive to the initial parameters, determinacy, ergodicity, and so forth [4–7], chaotic-systems-based encryption algorithms [8–15] are popular among these methods. In general, a chaotic-system-based algorithm encrypts an

image via two stages (i.e., confusion and diffusion). At the confusion stage, the positions of pixels are changed. To enhance security, the pixel values are changed at the diffusion stage. Sometimes, these two stages can be achieved simultaneously. Nevertheless, one may notice that the precision of initial parameters for generating chaotic sequences can influence the encryption performance of a chaotic system. At this point, for a given image, one may ask two questions: (i) Can we employ a metric to help optimize an encryption algorithm based on the chaos system? and (ii) What abilities should such a metric have? To answer these two questions, let us first recall the viewpoint proposed by Shannon that it is possible to break many kinds of ciphers using a statistical analysis on the histogram and the correlation of adjacent pixels in the cipher image [3]. From this viewpoint, we know that both the composition (proportions of pixels) and configurational information (spatial structures) of an image should be considered when designing an encryption algorithm and when evaluating its performance. This further suggests that we may need to find metrics for capturing both compositional and configurational information of an image.

Some metrics have been developed to evaluate the performance of encryption systems upon an image, e.g., correlation [9], NPCR (Number of Pixels Change Rate) [9,16], UACI (Unified Average Changing Intensity) [9], histogram [17], and Shannon entropy [18–20]. Theoretically speaking, these metrics are not good enough for capturing both compositional and configurational information. For example, Shannon entropy is a type of statistical entropy [21] and thus is unable to completely capture the configurational information of an image since its calculation relies on the occurrence probabilities of pixels, not the two-dimensional spatial structures. Three DEMs are shown in Figure 1, where the ones in the middle and right frames are the scrambled results of the one in the left frame. They have different spatial structures, whereas their Shannon entropy values are the same. Additionally, the information content of the multiscale representation of a DEM cannot be well-quantified by these metrics.

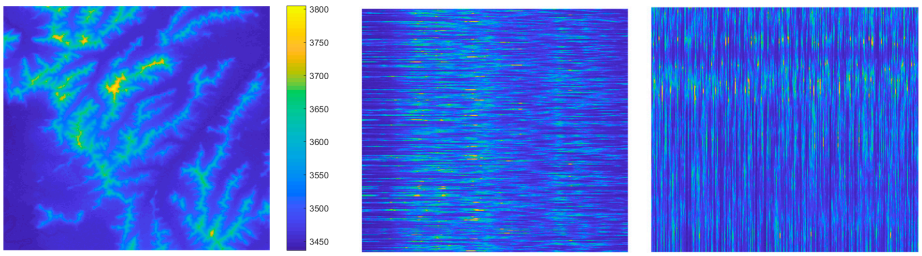


Figure 1. Three digital elevation models (DEMs) with the same histogram and, thus, same Shannon entropy values.

To bridge the gaps induced by these metrics mentioned above, this study utilizes the configurational entropy (thermodynamic entropy) to encrypt DEM. An encryption algorithm is proposed with the integration of a chaos system and linear prediction and is optimized by leveraging the configurational entropy. Apart from the Introduction section, the remainder of this study is organized as follows. The Second Law of Thermodynamics and configurational entropy are introduced first as the perspective for optimizing the DEM encryption in Section 2. Then, a novel encryption algorithm based on the leverage of configurational entropy is proposed and described in Section 3. Two DEMs are used in experiments followed by the results analysis in Section 4. Finally, a conclusion is made in Section 5.

2. The Second Law of Thermodynamics as a New Perspective for Optimizing Encryption of Numerical Raster Data

The Second Law of Thermodynamics is concerned with the direction of natural processes. This law states that an isolated and closed thermodynamic system can spontaneously evolve towards thermodynamic equilibrium, where its disorder degree (which can be measured by entropy) is at maximum [22–24]. Inspired by this law, we can assume

that a DEM could be considered an isolated and closed thermodynamic system where pixels are taken as gas molecules. Different temperatures (i.e., different encryption techniques or same techniques with different initial parameters) are imposed on the same thermodynamic system (an image), and then, the gas molecules (pixels) move in different directions and finally reach one type of status. Figure 2 shows different statuses of a closed thermodynamic system under different temperatures. The disorder of the thermodynamic system represents the complexity (randomness) of an image. The gas molecules move in different directions and then form different distributions. The disorder degree of gas molecules increases from (a) to (d).

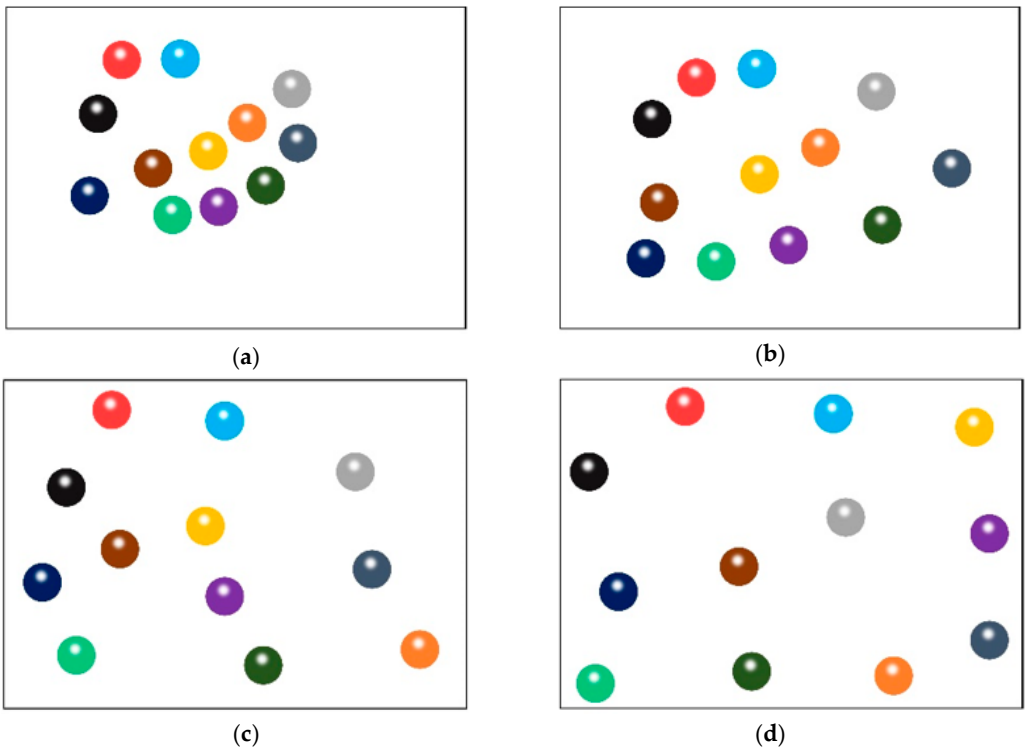


Figure 2. Four closed and isolated thermodynamic systems with the same gas molecules but different distributions.

The disorder of an isolated and closed thermodynamic system can be quantified by the thermodynamic entropy proposed by Ludwig Boltzmann [25,26]. The calculation formula for the thermodynamic entropy (configurational entropy and Boltzmann entropy) is as follows:

$$S = K \log W \tag{1}$$

where K is the Boltzmann constant (1 in the case of digital images, as suggested by [27]) and W is the number of microstates for a given macrostate. The configurational entropy of numerical raster data has been defined and computed in [28] with the assistance of the concept of multiscale representation, leading to two types of terms: relative and absolute. Concretely, the macrostate is defined as the upscaling results by an operation with a 2×2 sliding window; the microstates are all possible downscaling results, which can be seen in Figure 3. For an image, its relative configurational entropy (S_R) is the sum of configurational entropies of pixels in a sliding window of size 2×2 through the whole image. The absolute configurational entropy (S_A) is the sum of relative configurational entropies across all scales, capturing the multiscale information, which can help us enhance the analysis of the complexity of an encrypted DEM.

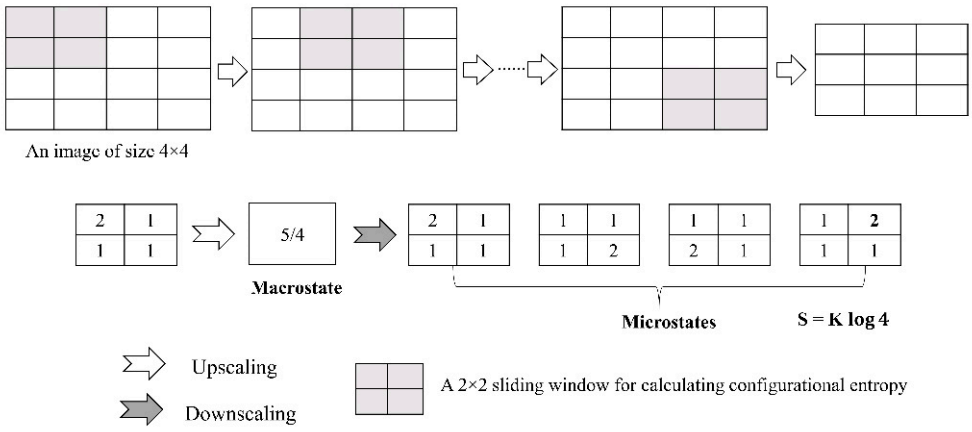


Figure 3. An example of computing the configurational entropy.

The experiments conducted in [29] demonstrates that S_R can measure the scrambling degree of grayscale images at the confusion stage. Regarding the diffusion phase included by an encryption function, the range of pixel values is modified. A good encrypted image should have various value ranges and pixel structures different from the original one. At this point, we can take the absolute configurational entropy as a metric to help choose the best one among all encrypted images. Theoretically speaking, the higher the absolute configurational entropy, the higher the complexity (and the lower the compressibility concerning lossless compression). To improve the encryption security, we should select the one with the maximum S_A value among all cases. In this study, the base of the logarithmic function in Equation (1) is set to 2 to measure the configurational information in units of bits. The configurational entropy of an image is proportional to its complexity.

3. Encryption Based on the Integration of Chaos System and Linear Prediction

Inspired by the Second Law of Thermodynamics, this section proposes an encryption algorithm consisting of two parts: (i) the encryption function and (ii) determination of the best-encrypted image with configurational entropy, which are shown in Figures 4 and 5.

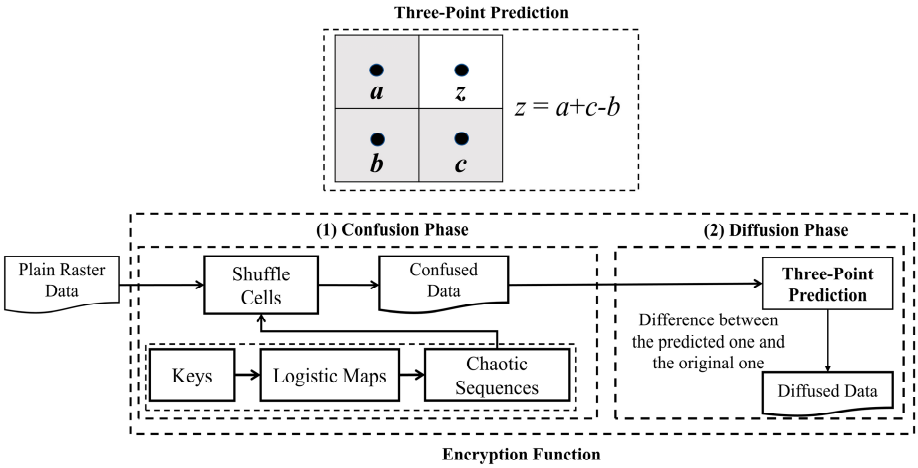


Figure 4. The proposed encryption algorithm.

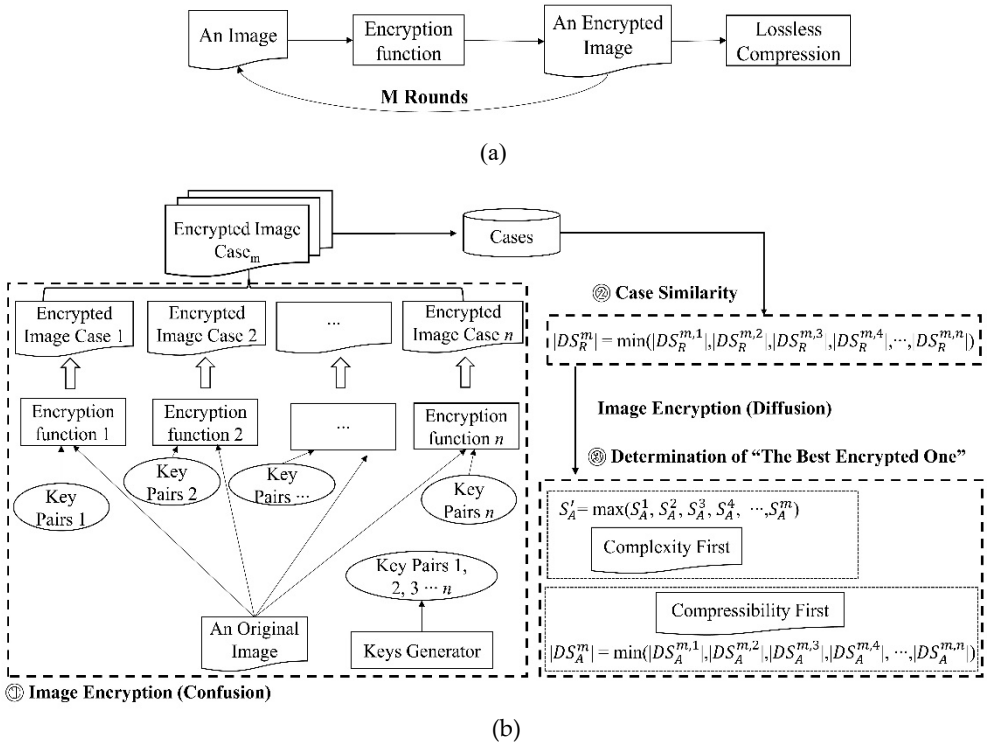


Figure 5. The schematic process of the proposed encryption function. (**a**) Encryption of a DEM (an image) for m rounds. (**b**) Determination of the best encrypted one with configurational entropy; m ($\geq$1) represents the m total encryption rounds; n ($\geq$1) represents the number of scrambled images with respect to 2n key pairs for generating logistic maps.

The confusion phase included under the proposed encryption function is implemented by the chaos system generated by two logistic maps with different initial parameter values. Mathematically, the logistic map [30] is written as follows

$$x_{n+1} = rx_n(1 - x_n) \tag{2}$$

where x_n is located in the interval [0,1] and $0 \leq r \leq 4$. When $r \in (3.5699456, 4)$, the sequence generated by the logistic map can show chaotic status, though there are many periodic windows in this interval. We can assume that a DEM is read as a numerical matrix of size M $\times$ N. The confusion phase scrambles the whole image, indicating that both row and column scrambling are needed. To begin this process, first, we set the initial parameter r_0 and x_0 values to iterate the chaotic system (i.e., Equation (2)) for M times and then a chaotic sequence of length M, { x_1, x_2, x_3, x_4, x_5, ,x_m}, is generated and referred to as S_M. Then, sorting this chaotic sequence in ascending or descending order, we get {$\overline{x}_1$, $\overline{x}_2$, $\overline{x}_3$, $\overline{x}_4$, $\overline{x}_5$, ,$\overline{x}_m$} named $\overline{S}_m$. Next, we need to find the position values of S_M in $\overline{S}_m$ and to record the transformation positions TP = { tp_1, tp_2, tp_3, tp_4, tp_5, tp_m}. When we use TP for row scrambling, we only need to move the tp_1 row to the first row and the tp_2 row to the second row until all rows are scrambled. Similarly, regarding column scrambling, new parameter r_0 and y_0 values are needed to iterate the logistic map for N times and then to conduct the same operation as the row scrambling.

Concerning the diffusion phase, the three-point prediction is employed. A 2 $\times$ 2 sliding window is moved pixel by pixel, which generates the predicted pixels. Regarding the edge pixels, the missing ones among pixels a, b, and c are automatically set to 0. Thereafter, the difference between the confused image and the predicted one is computed and then taken as the final encrypted DEM in one round. The advantages of three-point prediction are (i) reducing the correlation between pixels (increasing the complexity of an image) and (ii) changing the range of pixel values.

After introducing the encryption function, we describe how the whole encryption algorithm is optimized with the assistance of configurational entropy. As shown in Figure 5a, users can determine the total encryption rounds, m, and the number of different confusion phases, n, as illustrated in Figure 5b. The encrypted image (DEM) in the last round is taken as the input of the encryption function for the next round in the whole encryption process. Figure 5b shows how to select the best-encrypted image. An image can be scrambled by $2n$ logistic maps with $2n$ different key pairs (r_0, x_0) at the confusion phase; thus, n confused DEMs with the same histogram but different structures. Among these n confused DEMs, the one with the maximum absolute S_R difference ($|DS_R|$) compared to the original is selected as the input for the diffusion phase in which the range of pixel values is changed. The absolute configurational entropy (S_A) is finally employed to determine which one is the most suitable for transmission. From a theoretical perspective of information, the higher S_A value, the higher the complexity (lower compressibility) of a DEM, indicating higher encryption performance. Two modes are provided for users: (i) complexity first and (ii) compressibility first. For the former, the one with the maximum S_A is finally selected. Regarding the latter, the one with the minimum absolute S_A difference ($|DS_A|$) compared to the original DEM is chosen.

The encrypted image can be further processed by lossless compression techniques, such as Huffman encoding [31], free lossless image format (FLIF) [32], and multiscale compression [33], to reduce the burden on transmission and storage. To improve the encryption performance as much as possible, it is recommended that users encrypt a DEM for at least 4 times (i.e., $m \geq 4$) using the proposed algorithm.

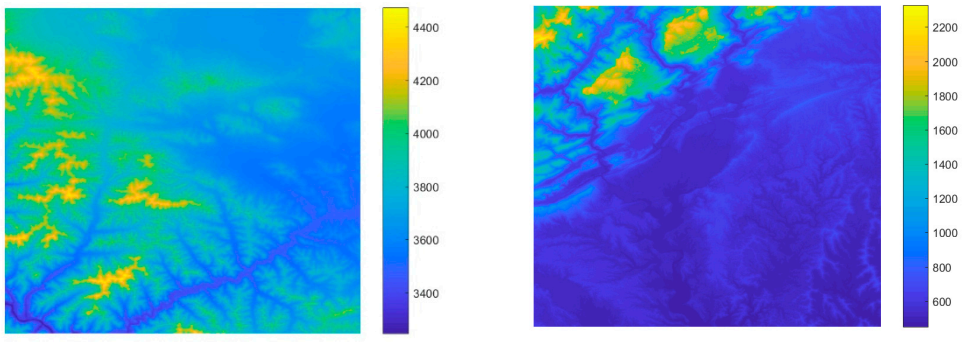
4. Experimental Results and Analysis

4.1. Encryption Results

Two 600 × 600 DEMs with different complexities tabulated in Table 1 were considered experimental images. Their data formats were plain text, and their elevation values were integer. Figure 6 shows these two DEMs, showing different complexities and various ranges of pixel values.

Table 1. Two DEMs for the experiments [28]; S_R and S_A denote relative and absolute configurational entropy, respectively.

DEM	Latitude Extent	Longitude Extent	S_R	S_A	Size (KB)
A	34°27′04″ N–35°02′53″ N	100°36′21″ E–101°49′23″ E	2,502,048.3	401,204,550.0	1758
B	31°23′17″ N–32°06′40″ N	104°07′31″ E–105°06′55″ E	2,416,595.3	308,809,911.3	1459



(**a**) (**b**)

Figure 6. Two experimental DEMs with different complexities.

For convenience conducting the experiments, both m and n were set to 10 to encrypt two DEMs. The development environment was Microsoft Visual studio 2013 with .Net Framework 4.5, and the language used for programming was C#. The keys for generating chaotic sequences and corresponding $|DS_R|$ of the confused DEM A in the confusion phase

of the first round are tabulated in Table 2. Figure 7 shows the scrambled images, while they have the same histogram. The fourth one was selected for the diffusion phase because its $|DS_R|$ was the maximum compared with the remaining confused images. By using the proposed encryption algorithm, we obtained 10 encrypted DEM A, which are shown in Figure 8, and the key pairs are shown in Table 3, where C_R represents the lossless compression ratio (i.e., the ratio between the bytes used for storing the original data and that for storing the compressed data) by using LZMA [34,35], which is a dictionary-based compression algorithm and takes into consideration the spatial structure of data. From Figure 8, we find that the pixel value range has been modified and the tenth one has the maximum $|DS_A|$ and S_A as shown in Table 3. Therefore, it is selected as the best one when mode (i) is activated. Regarding mode (ii), Figure 8e is considered the best one. From Figure 9, we find that the S_A values of the encrypted images increased, whereas the C_R values decreased with the increase in the total encryption rounds (i.e., m). This can be explained by the viewpoint derived from [19] that, from a theoretical perspective, the lower the redundancy (which is measured by configurational entropy here) of an image, the lower the compression ratio of the image achieved.

Table 2. Comparisons of relative configurational entropy of confused DEM A under different keys in the first round. (r_0, x_0) and (r_0, y_0) denote the keys to scramble the row and column of DEM A, respectively. $|DS_R|$ means the absolute S_R difference compared to the original one.

No.	(r_0, x_0)	(r_0, y_0)	$\|DS_R\|$
1	(3.6949202, 0.94)	(3.6477592, 0.16)	1,425,882.9
2	(3.7278720, 0.12)	(3.7657562, 0.64)	1,455,723.6
3	(3.6158898, 0.54)	(3.7451577, 0.34)	1,440,030.0
4	(3.6694297, 0.82)	(3.6036054, 0.56)	1,490,201.9
5	(3.7033331, 0.43)	(3.8601213, 0.80)	1,478,572.8
6	(3.5919501, 0.58)	(3.7767205, 0.53)	1,472,217.3
7	(3.7562061, 0.76)	(3.9686558, 0.74)	1,449,584.6
8	(3.7254665, 0.13)	(3.942484, 0.03)	1,455,760.0
9	(3.7873567, 0.05)	(3.6882554, 0.48)	1,443,565.6
10	(3.8638823, 0.83)	(3.6808917, 0.04)	1,453,363.9

Table 3. The best key pairs among 10 encryption times for DEM A. $|DS_A|$ means the absolute S_A difference compared to the original one. S_A is the absolute configurational entropy.

mth Round	(r_0, x_0)	(r_0, y_0)	S_A	$\|DS_A\|$	Size (KB)	C_R
1	(3.6694297, 0.82)	(3.6036054, 0.56)	267,144,464.1	134,060,085.9	1759	3.239
2	(3.9720618, 0.63)	(3.8118391, 0.31)	300,969,521.6	100,235,028.4	1529	2.682
3	(3.9982823, 0.61)	(3.6946723, 0.56)	329,305,875.0	71,898,675.0	1641	2.634
4	(3.6911029, 0.24)	(3.7563811, 0.84)	359,120,512.9	42,084,037.1	1764	2.602
5	(3.6761227, 0.71)	(3.9535386, 0.56)	393,026,254.4	8,178,295.6	1850	2.531
6	(3.6468789, 0.54)	(3.7460818, 0.2)	427,592,398.5	26,387,848.5	1946	2.485
7	(3.9889696, 0.77)	(3.7643806, 0.9)	464,150,752.2	62,946,202.2	2074	2.474
8	(3.7666660, 0.74)	(3.7904553, 0.39)	511,483,888.6	110,279,338.6	2172	2.435
9	(3.9793047, 0.27)	(3.7826054, 0.06)	550,795,418.0	149,590,868.0	2253	2.392
10	(3.8921841, 0.88)	(3.8734612, 0.19)	604,312,707.5	203,108,157.5	2373	2.380

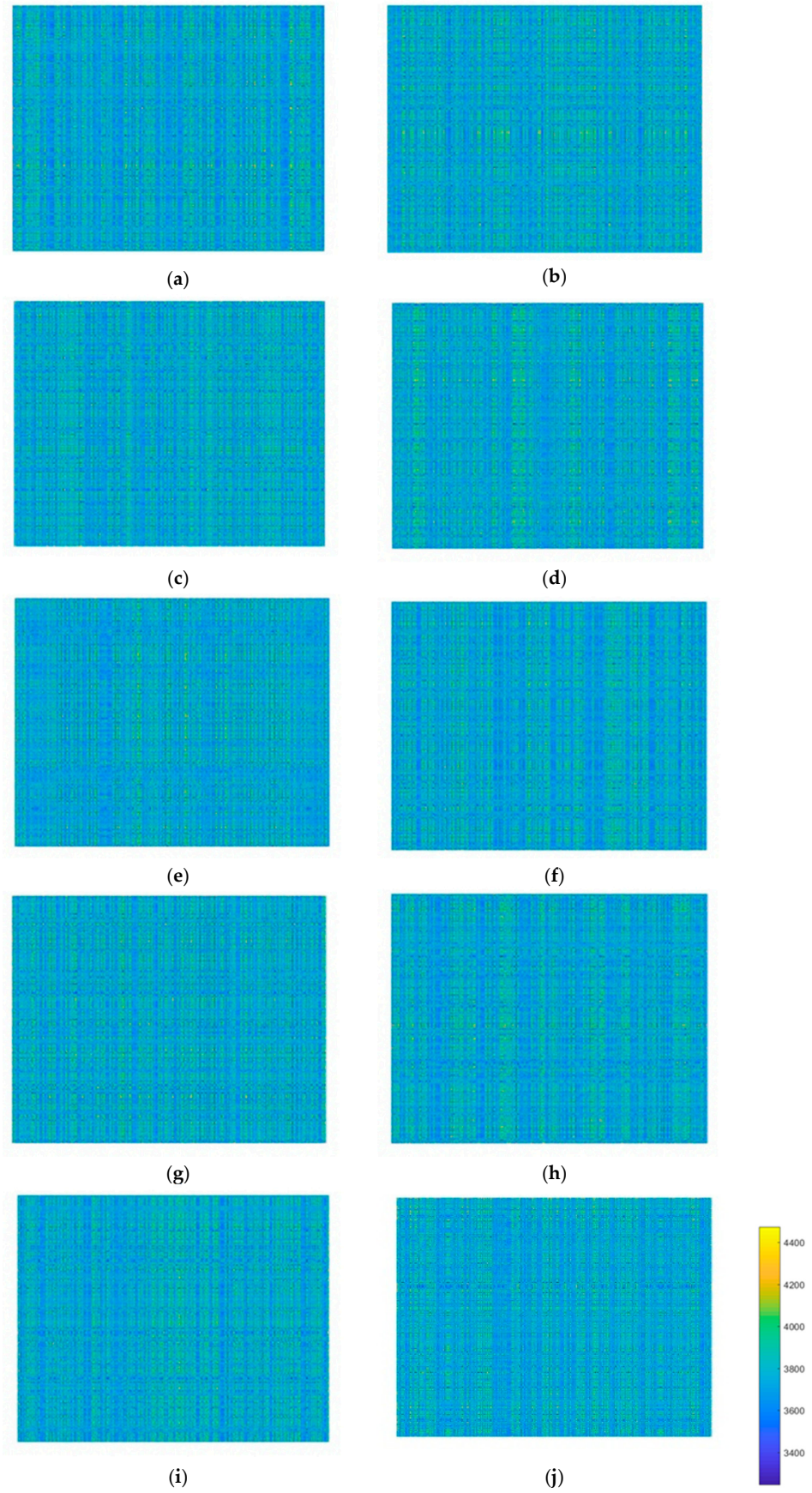


Figure 7. Ten confused DEM A.

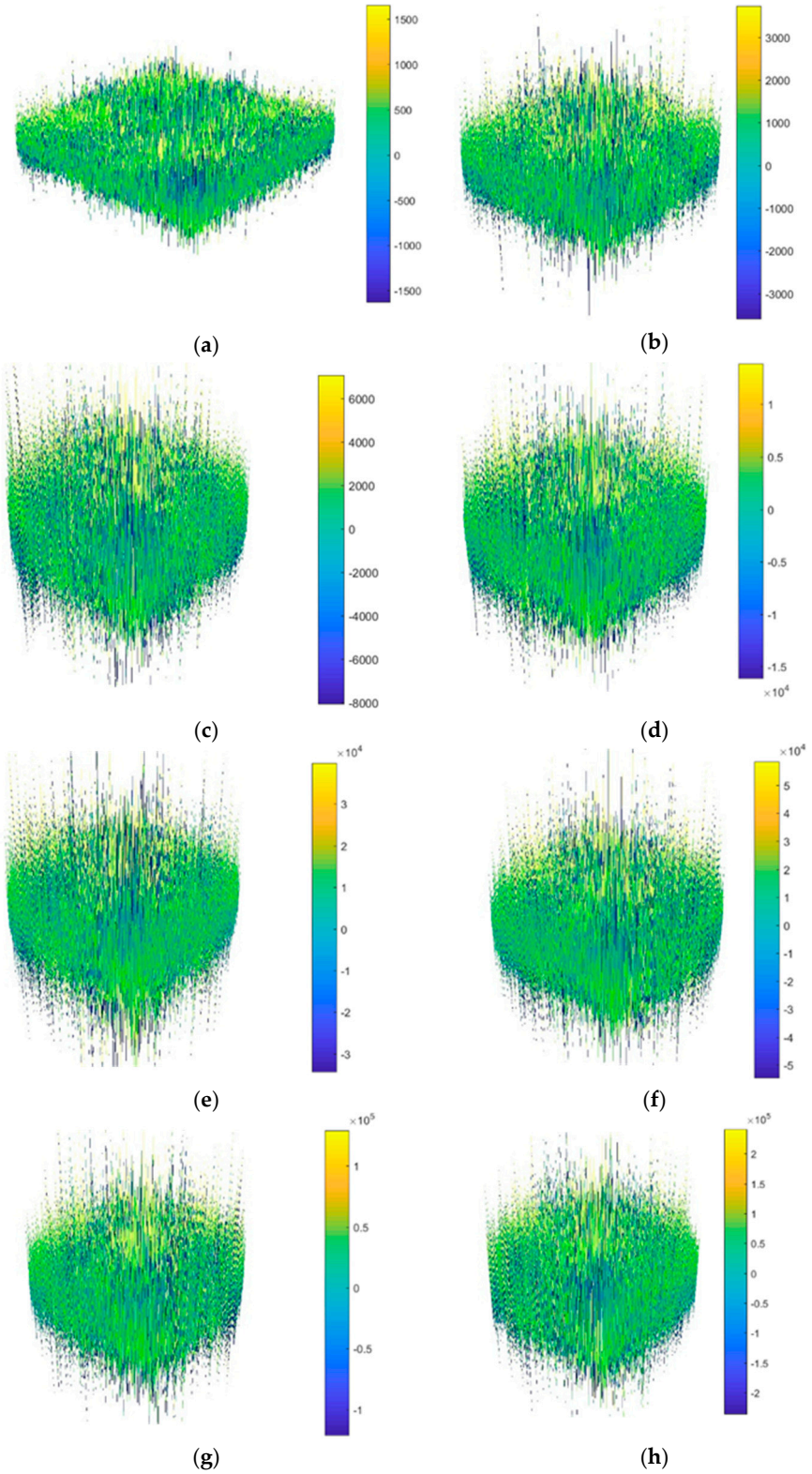
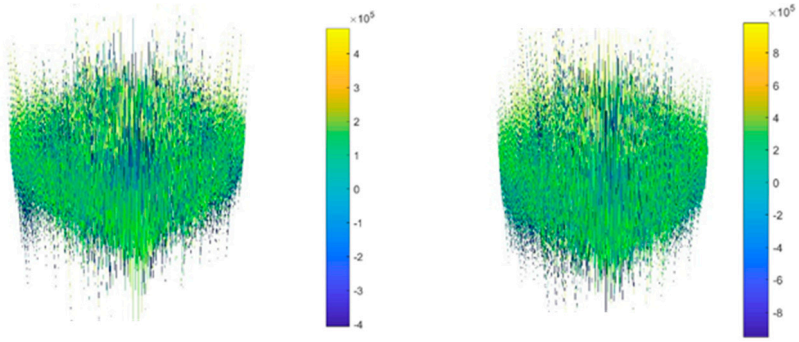
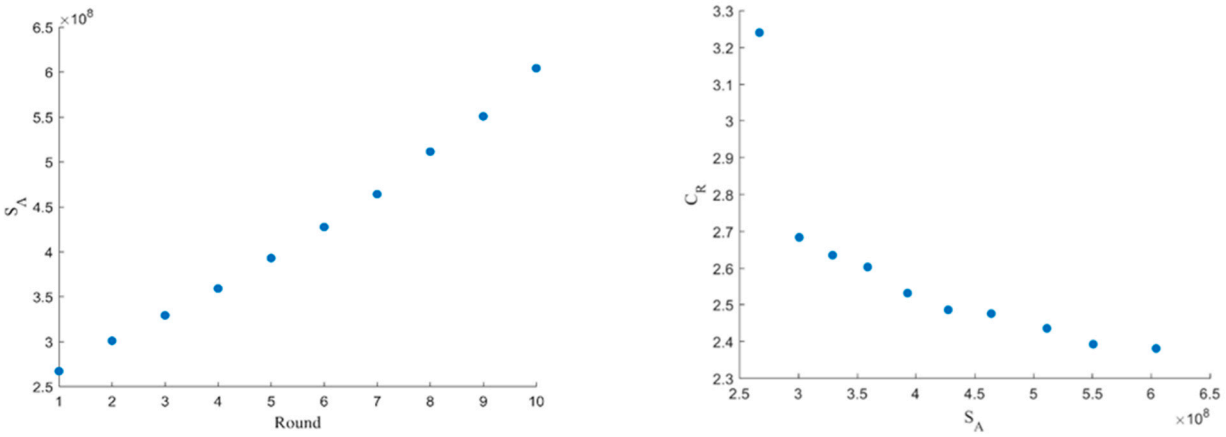


Figure 8. *Cont*.



(**i**) (**j**)

Figure 8. Three-dimensional images of confused and diffused DEM A. The numbering sequence is consistent with the encryption round.



(**a**) (**b**)

Figure 9. Scatters plot of m rounds compared to the S_A value of the encrypted DEM A and that of C_R compared to the S_A values.

Regarding DEM B, Table 4 shows the $|DS_R|$ values of 10 confused ones illustrated in Figure 10. We find the 10th one is the best in the confusion phase. Table 5 shows similar results to DEM A. Obviously, when mode (i) is employed, the 10th one is the best since it has the maximum S_A value in comparison with the others shown in Figure 11. However, the second one is selected when mode (ii) is activated. Figure 12a illustrates that the S_A values increase with the increase in encryption rounds. However, we find that the C_R values decrease in Figure 12b. These experimental results indicate that the configurational entropy is useful to optimize the proposed encrypted algorithm.

Table 4. Comparisons of the relative configurational entropy of confused DEM B under different keys in the first round.

No.	(r_0, x_0)	(r_0, y_0)	$\|DS_R\|$
1	(3.9127452, 0.56)	(3.9430024, 0.44)	1,366,081.4
2	(3.7803406, 0.42)	(3.7118742, 0.28)	1,371,377.5
3	(3.9446201, 0.10)	(3.6720488, 0.25)	1,401,148.1
4	(3.8410564, 0.11)	(3.7863010, 0.4)	1,201,102.3
5	(3.6867861, 0.75)	(3.5896140, 0.09)	1,373,653.2
6	(3.5921033, 0.19)	(3.9948832, 0.07)	1,381,518.3
7	(3.6462285, 0.68)	(3.5859005, 0.23)	1,375,019.6
8	(3.7970835, 0.63)	(3.8113753, 0.49)	1,377,774.8
9	(3.9591995, 0.05)	(3.9107138, 0.70)	1,382,701.9
10	(3.9429938, 0.25)	(3.7159570, 0.45)	1,388,199.0

Table 5. The best key pairs among 10 encryption rounds for DEM B.

*m*th Round	(r_0, x_0)	(r_0, y_0)	S_A	$\lvert DS_A \rvert$	Size (KB)	C_R
1	(3.9446201, 0.1)	(3.6720488, 0.25)	285,857,730.3	22,952,181.0	1491	2.696
2	(3.6978437, 0.44)	(3.9206044, 0.49)	320,402,657.6	11,592,746.3	1592	2.636
3	(3.6557073, 0.03)	(3.8864578, 0.33)	350,085,107.0	41,275,195.7	1728	2.606
4	(3.9037505, 0.02)	(3.7374396, 0.21)	383,939,349.7	75,129,438.4	1826	2.550
5	(3.7128502, 0.56)	(3.7213353, 0.35)	413,822,209.8	105,012,298.5	1911	2.492
6	(3.8007097, 0.09)	(3.9265191, 0.78)	452,157,235.0	143,347,323.7	2031	2.477
7	(3.5822104, 0.46)	(3.7138054, 0.15)	494,673,201.5	185,863,290.2	2139	2.453
8	(3.6359581, 0.57)	(3.9861503, 0.54)	532,925,355.6	224,115,444.3	2220	2.403
9	(3.9345383, 0.58)	(3.7636595, 0.61)	590,387,815.5	281,577,904.2	2325	2.382
10	(3.8741445, 0.34)	(3.900868, 0.25)	635,882,520.3	327,072,609.0	2446	2.377

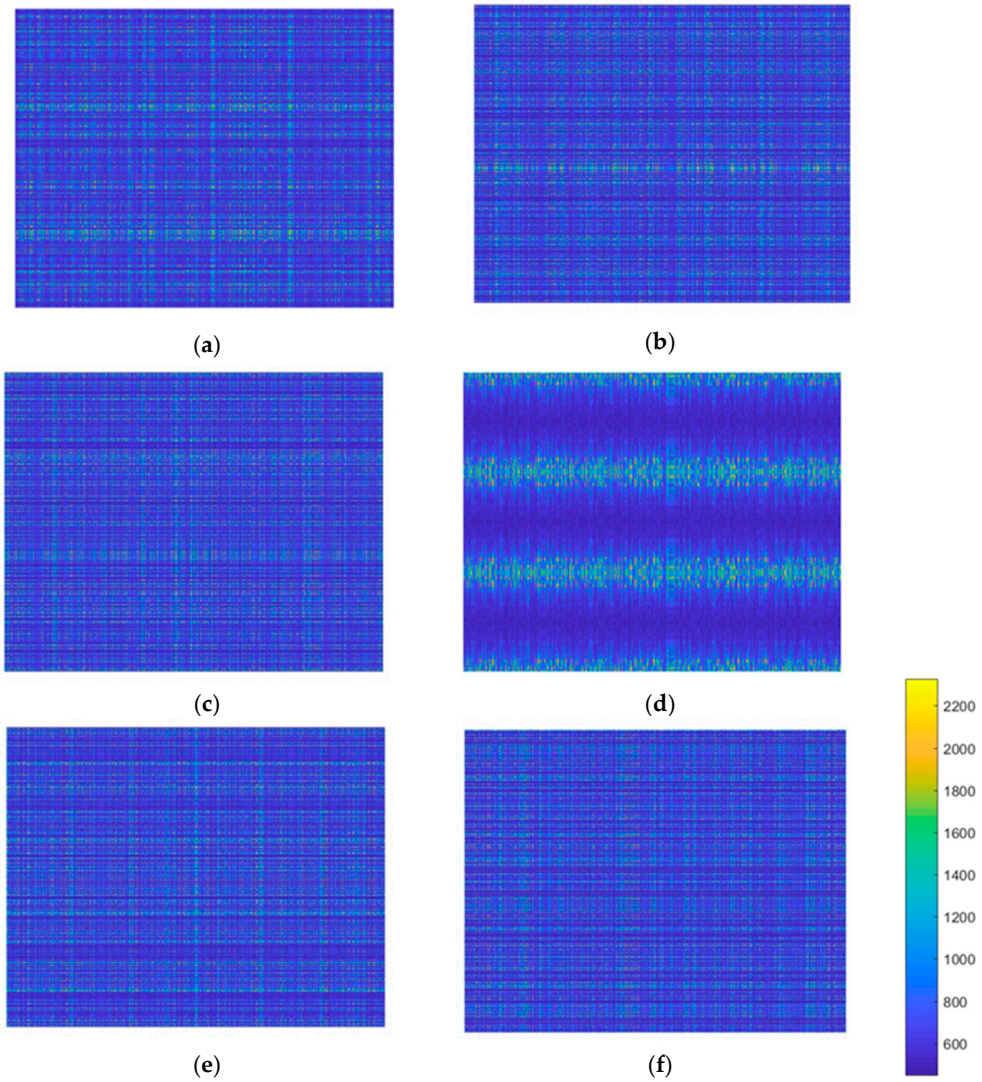


Figure 10. *Cont.*

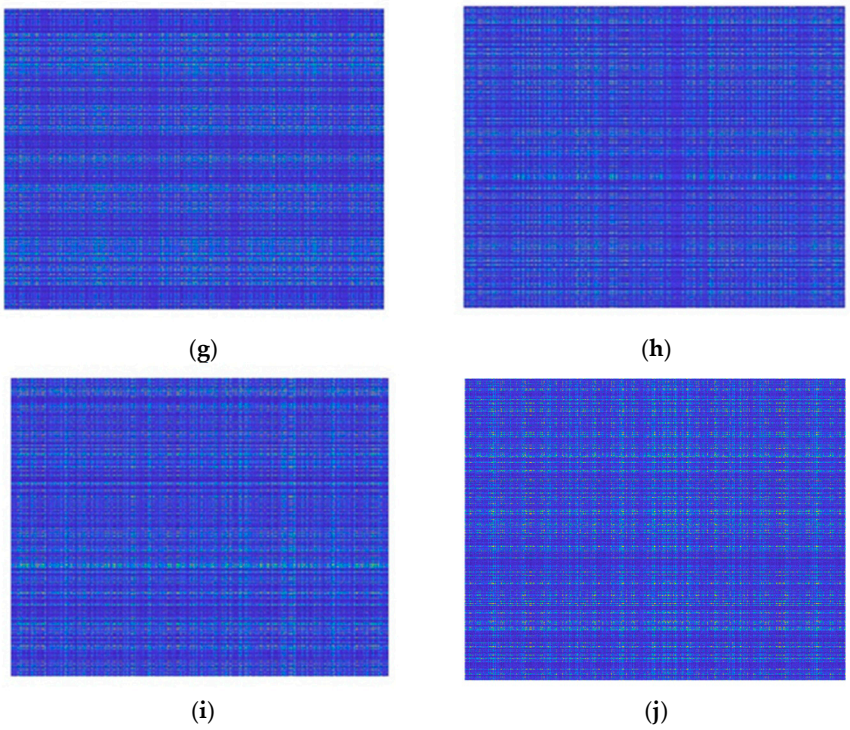


Figure 10. Ten confused DEM B. Their histograms are the same.

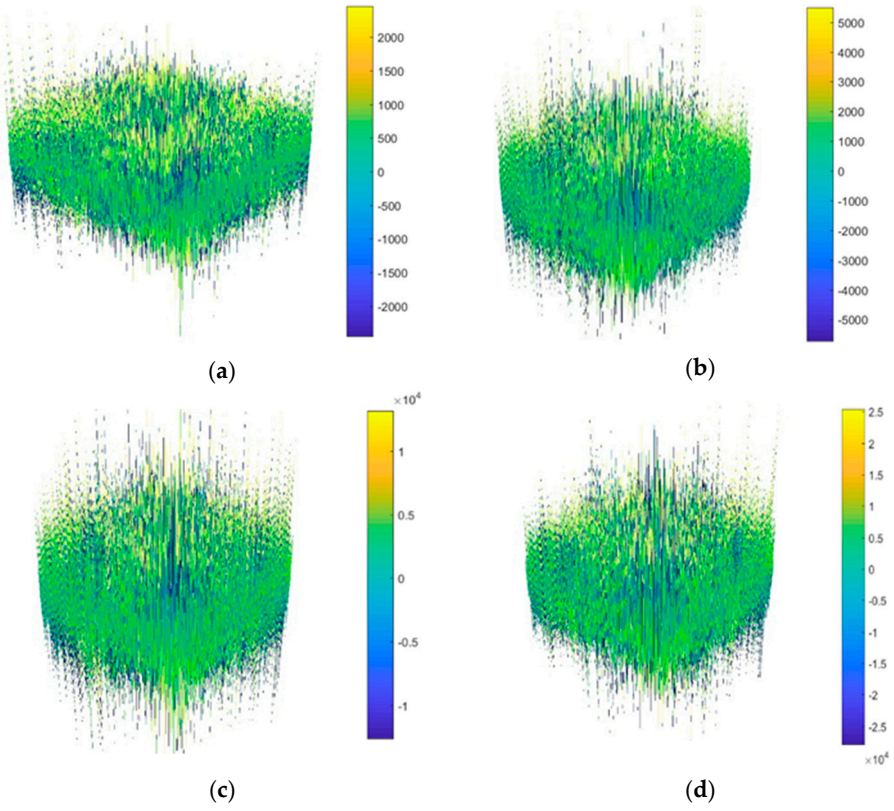


Figure 11. *Cont*.

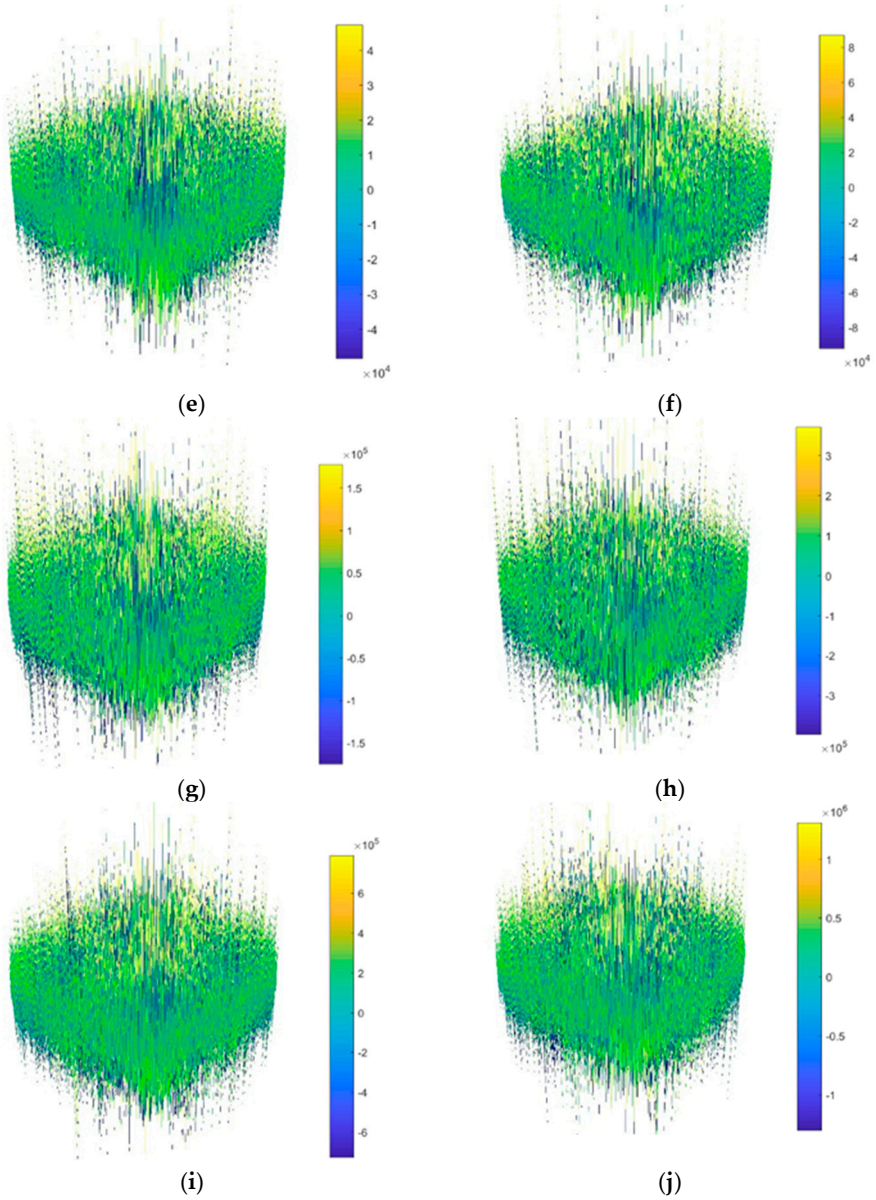


Figure 11. Three-dimensional images of encrypted DEM B. The numbering sequence is consistent with the encryption round.

From the two aforementioned encryption examples, we find that configurational entropy can help users choose the best-encrypted one according to specific requirements, e.g., the size of encrypted data should be as small as possible, and the encrypted image should be as complicated as possible. For instance, in consideration of transmission bandwidth, users can choose the encryption with the minimum S_A value. To enhance the complexity of the encrypted image, users can set larger and larger m and n values if possible.

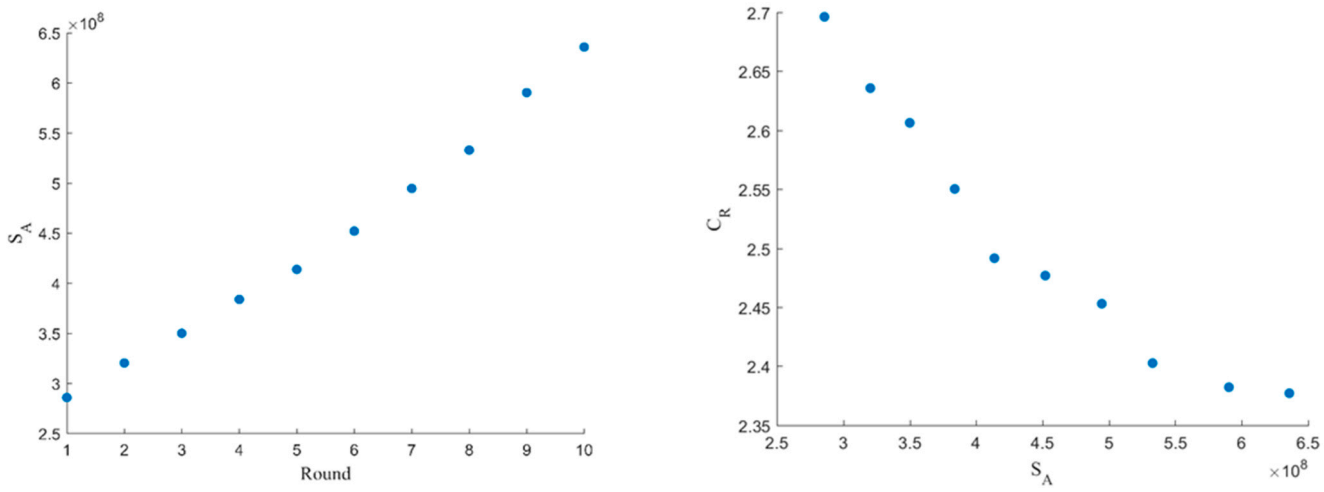


Figure 12. Scatter plots of m rounds compared to the S_A value of the encrypted DEM B and that of C_R compared to the S_A values.

4.2. Security Analysis

A good encryption algorithm should be capable of resisting all attacks. In this section, we perform a security analysis on the proposed encryption algorithm.

1. Key space and sensitivity analysis

A good encryption approach should be sensitive to the secret keys. In this study, the iteration times, (i.e., m and n) can be used as keys as well as the parameters r_0 and x_0 of a logistic map. Moreover, the precision of parameters of the logistic map can be used as keys as it can influence the performance of chaotic sequences. The key space is proportional to the parameter precision: m ($\geq$1) and n ($\geq$1). If the precision is 10^{-20}, the key space size can be at least $m \times 10^{40}$. Hence, the key space is big enough to resist brute-force attacks. Moreover, using keys (r_0, x_0) only to recover the original image is very difficult as the range of pixel values is changed after using the proposed encryption algorithm. Figure 13 shows two decrypted DEM A with wrong keys.

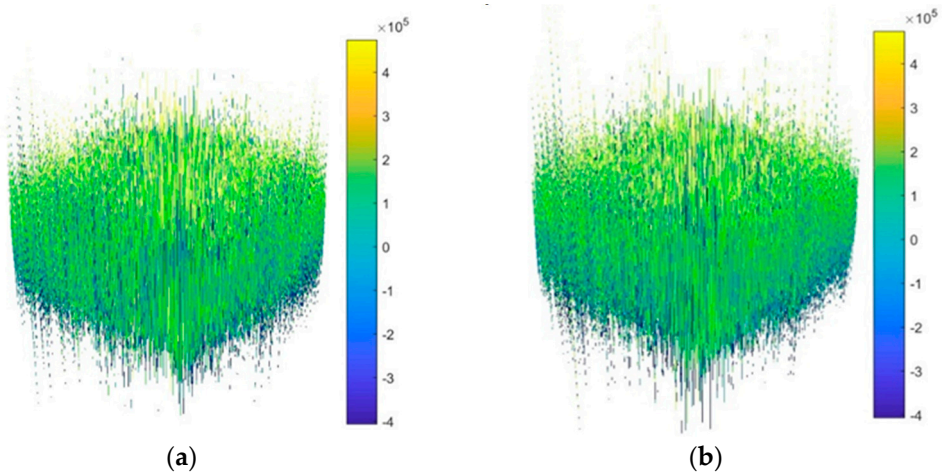


Figure 13. Three-dimensional images of decrypted DEM A: (**a**) with keys r_0 = 3.7004182, x_0 = 0.28, r_0 = 3.8994119, and y_0 = 0.86; (**b**) with keys r_0 = 3.8777651, x_0 = 0.21, r_0 = 3.7276262, and y_0 = 0.27.

2. Classical attacks

Attackers have many methods of attack. Four classical types of attacks [7] are listed as follows:

- Selected plaintext: The opponent chooses a plaintext string and constructs the ciphertext string when temporary access to the encryption machine is granted.
- Selected cipher text: The opponent obtains a ciphertext string and constructs the corresponding plaintext string when temporary access to the encryption machine is granted.
- Known plaintext: The opponent owes a plaintext string and its corresponding ciphertext.
- Ciphertext only: The opponent owes a ciphertext string

The selected plaintext attack is considered the most powerful one. The proposed encryption approach is highly sensitive to the initial parameters for a logistic map. Moreover, at the fusion phase, the encryption data are related to not only the one in the confusion phase but also the one predicted by the three-point prediction technique used at the diffusion stage. Moreover, different encrypted numerical raster data are derived from various former ones because m and n are variable. This means that the encrypted data are able to resist the chosen plaintext attack, indicating that it can resist the remaining attacks.

4.3. Decryption Results with True Keys

To decrypt the encrypted DEMs A and B, the true keys tabulated in Tables 3 and 5 are used. The decryption of an image is the inverse process of its encryption. With true keys, the reconstructed DEMs A and B are illustrated in Figure 14.

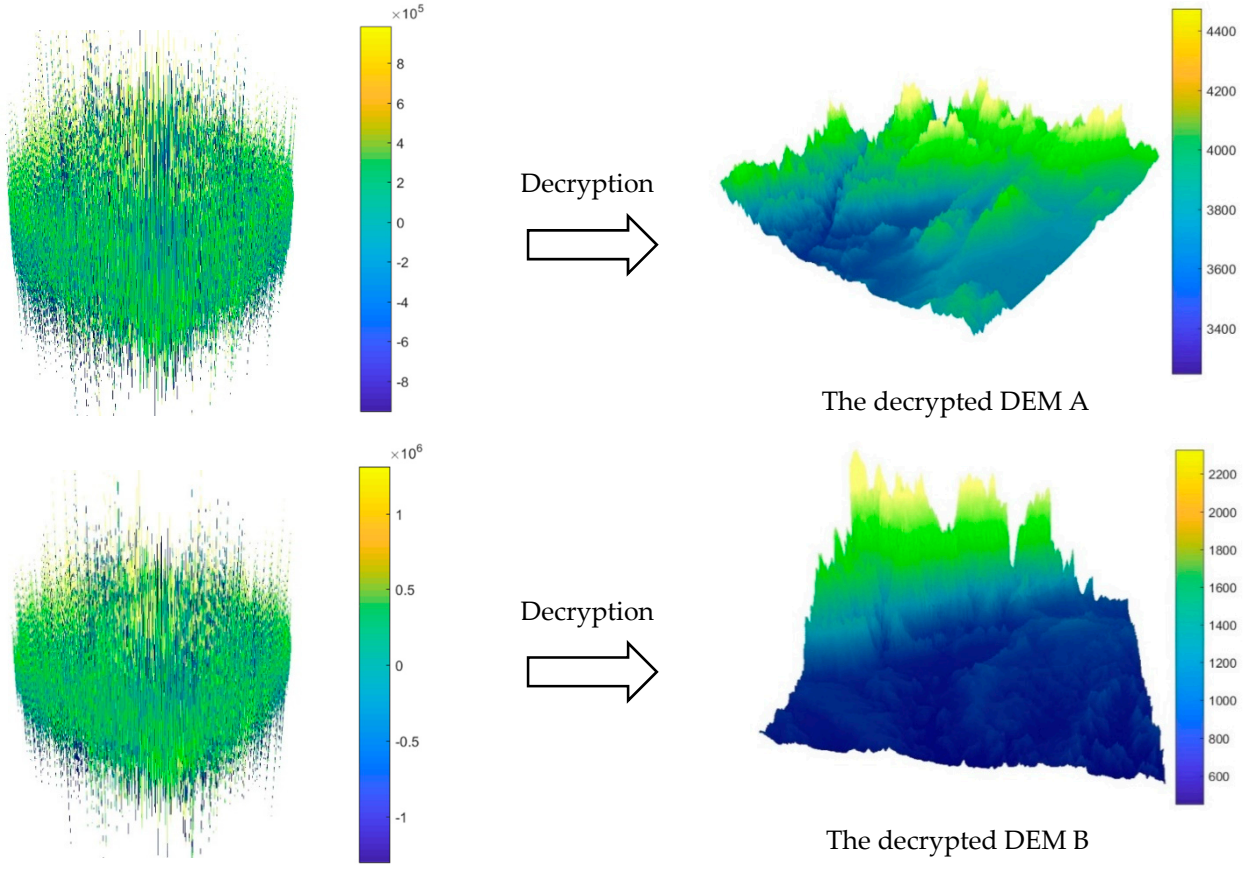


Figure 14. The decryption results of DEMs A and B with the use of true keys.

5. Conclusions

DEM is a digital representation of terrain information. Information security for DEMs is an important topic due to the openness of computer and network communication. By using encryption, the information from DEMs can be well protected. In this study, an

algorithm based on chaos system and linear prediction is proposed. To optimize the proposed encryption algorithm, configurational entropy is employed. At the confusion stage, the one with the maximum relative configurational entropy different from the original is selected for the diffusion stage, where the one with the maximum absolute configurational entropy is chosen for the sake of obtain the best encryption performance and the one with the minimum absolute configurational entropy is chosen to reduce the burden on transmission and storage. Two DEMs are taken as experimental data and encrypted 10 times. From the experimental results and analysis, we draw the following major conclusions

- The proposed encryption algorithm is valid, and its security is high.
- Configurational entropy is helpful for optimizing the encryption process.

On the other hand, three areas are recommended for future research. The first is to investigate the effects of different predictors in the diffusion phase of an encryption performance. The second is to explore multiscale DEM encryption with the help of absolute configurational entropy. Finally, more advanced chaos systems and watermark signature techniques [36–39] are expected to be employed as one part of this study to provide excellent performance in only one encryption round.

Author Contributions: Conceptualization, X.C.; methodology, X.C.; software, X.C.; validation, X. Cheng and Z.L.; formal analysis, X.C.; investigation, X.C.; resources, X.C.; data curation, X.C.; writing—original draft preparation, X.C.; writing—review and editing, Z.L.; visualization, X.C.; supervision, Z.L.; project administration, Z.L.; funding acquisition, Z.L. All authors have read and agreed to the published version of the manuscript.

Funding: This study was funded by the Research Grant Council of Hong Kong SAR, China (grant number 15221918) and the Natural Science Funding Council of China (grant number 41930104).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Two experimental DEMs can be downloaded from the website of NASA's Shuttle Radar Topography Mission (http://srtm.csi.cgiar.org/) according to the geographical extent tabulated in Table 1. All encrypted DEMs are available upon request.

Acknowledgments: Special thanks are given to Na Ren of Nanjing Normal University, China, for her constructive comments.

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

References

1. Lian, S. *Multimedia Content Encryption: Techniques and Applications*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2008; pp. 7–10.
2. Uhl, A.; Pommer, A. *Image and Video encryption: From Digital RIGHTS management to Secured Personal Communication*, 1st ed.; Springer: New York, NY, USA, 2004; pp. 11–22.
3. Shannon, C.E. Communication theory of secrecy system. *Bell Labs Tech. J.* **1949**, *28*, 656–715. [CrossRef]
4. Lian, S. A block cipher based on chaotic neural networks. *Neurocomputing* **2009**, *72*, 1296–1301. [CrossRef]
5. Huang, C.K.; Nien, H.H. Multi chaotic systems based pixel shuffle for image encryption. *Opt. Commun.* **2008**, *282*, 347–350. [CrossRef]
6. 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]
7. Zhang, L.; Liao, X.; Wang, X. An image encryption approach based on chaotic maps. *Chaos Soliton Fract.* **2005**, *24*, 759–765. [CrossRef]
8. Xiang, T.; Wong, K.; Liao, X. Selective image encryption using a spatiotemporal chaotic system. *Chaos* **2007**, *17*, 023115. [CrossRef]
9. Zhu, Z.; Zhang, W.; Wong, K.W.; Yu, H. A chaos-based symmetric image encryption scheme using a bit-level permutation. *Inf. Sci.* **2011**, *181*, 1171–1186. [CrossRef]
10. Lian, S.; Sun, J.; Wang, Z. Security analysis of a chaos-based image encryption algorithm. *Physica. A.* **2005**, *351*, 645–661. [CrossRef]
11. Wong, K.W.; Kwok, B.; Law, W.S. A fast image encryption scheme based on chaotic standard map. *Phys. Lett. A.* **2008**, *372*, 2645–2652. [CrossRef]

12. Li, H.; Wang, Y.; Zuo, Z. Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms. *Opt. Lasers Eng.* **2019**, *115*, 197–207. [CrossRef]
13. Farah, M.B.; Guesmi, R.; Kachouri, A.; Samet, M. A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. *Opt. Laser Technol.* **2020**, *121*, 105777. [CrossRef]
14. Chai, X.; Fu, X.; Gan, Z.; Zhang, Y.; Lu, Y.; Chen, Y. An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata. *Neural. Comput. Appl.* **2020**, *32*, 4961–4988. [CrossRef]
15. Wang, Y.; Wong, K.W.; Liao, X.; Xiang, T.; Chen, G. A chaos-based image encryption algorithm with variable control parameters. *Chaos Soliton Fract.* **2009**, *41*, 1773–1783. [CrossRef]
16. Praveenkumar, P.; Amirtharajan, R.; Thenmozhi, K.; Rayappan, J. Triple chaotic image scrambling on RGB–a random image encryption approach. *Secur. Commun. Netw.* **2015**, *8*, 3335–3345. [CrossRef]
17. Wei, X.; Guo, L.; Zhang, Q.; Zhang, J.; Lian, S. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. *J. Syst. Softw.* **2012**, *85*, 290–299. [CrossRef]
18. Guan, Z.; Huang, F.; Guan, W. Chaos-based image encryption algorithm. *Phys. Lett. A.* **2005**, *346*, 153–157. [CrossRef]
19. Shannon, C.E. A mathematical theory of communication. *Bell Labs Tech. J.* **1948**, *27*, 379–423. [CrossRef]
20. Wu, Y.; Zhou, Y.; Saveriades, G.; Again, S.; Noonan, J.P.; Natarajan, P. Local Shannon entropy measure with statistical tests for image randomness. *Inf. Sci.* **2013**, *222*, 323–342. [CrossRef]
21. Gao, P.; Li, Z.; Zhang, H. Thermodynamics-based evaluation of various improved Shannon entropies for configurational information of gray-level images. *Entropy* **2018**, *20*, 19. [CrossRef]
22. Kaufman, M. *Principles of Thermodynamics*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2019; pp. 71–92.
23. Huettner, D.A. Net energy analysis: An economic assessment. *Science* **1976**, *192*, 101–104. [CrossRef] [PubMed]
24. Lebowitz, J. Macroscopic laws, microscopic dynamics, time's arrow and Boltzmann's entropy. *Physica A* **1993**, *194*, 1–27. [CrossRef]
25. Benson, H. *Entropy and the Second Law of Thermodynamics*, 1st ed.; University Physics, Wiley: New York, NY, USA, 1996; pp. 417–439.
26. Boltzmann, L. Weitere studien über das wärmegleichgewicht unter gasmolekülen [Further studies on the thermal equilibrium of gas molecules]. *Sitzungsber. Akad. Wiss.* **1872**, *66*, 275–370.
27. Cushman, S. Calculating the configurational entropy of a landscape mosaic. *Landsc. Ecol.* **2016**, *31*, 481–489. [CrossRef]
28. Gao, P.; Zhang, H.; Li, Z. A hierarchy-based solution to calculate the configurational entropy of landscape gradients. *Landsc. Ecol.* **2017**, *32*, 1133–1146. [CrossRef]
29. Cheng, X.; Li, Z. Using Boltzmann entropy to Measure Scrambling Degree of Grayscale Images. In Proceedings of the IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), IEEE, Zhuhai, China, 8–10 January 2021.
30. May, R.M. Simple mathematical models with very complicated dynamics. *Nature* **1976**, *261*, 459–467. [CrossRef]
31. Huffman, D.A. Method for the construction of minimum-redundancy codes. *Proc. IEEE* **1952**, *40*, 1098–1101. [CrossRef]
32. Sneyers, J.; Wuille, P. FLIF: Free lossless image format based on MANIAC compression. In Proceedings of the IEEE International Conference on Image Processing (ICIP), Phoenix, AZ, USA, 25–28 September 2016.
33. Ratakonda, K.; Ahuja, N. Lossless image compression with multiscale segmentation. *IEEE Trans. Image Process* **2002**, *11*, 1228–1237. [CrossRef] [PubMed]
34. Ziv, J.; Lempel, A. A universal algorithm for sequential data compression. *IEEE Trans. Inf. Theory* **1977**, *23*, 337–343. [CrossRef]
35. Martín, G. Range encoding: An algorithm for removing redundancy from a digitised message. In Proceedings of the Video and Data Recording Conference, Southampton, UK, 24–27 July 1979; Institution of Electronic and Radio Engineers: London, UK.
36. Lan, R.; He, J.; Wang, S.; Gu, T.; Luo, X. Integrated chaotic systems for image encryption. *Signal Process.* **2018**, *147*, 133–145. [CrossRef]
37. Chai, X.; Gan, Z.; Yuan, K.; Chen, Y.; Liu, X. A novel image encryption scheme based on DNA sequence operations and chaotic systems. *Neural. Comput. Appl.* **2019**, *31*, 219–237. [CrossRef]
38. Qi, G. Modelings and mechanism analysis underlying both the 4D Euler equations and Hamiltonian conservative chaotic systems. *Nonlinear Dyn.* **2019**, *95*, 2063–2077. [CrossRef]
39. Liu, X.; Wang, J.; Luo, Y. Lossless DEM watermark signature based on directional wavelet. In Proceedings of the 2nd International Congress on Image and Signal Processing, Tianjin, China, 17–19 October 2009.