ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.10, 8957–8967
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.10.118

AN IMAGE ENCRYPTION USING DYNAMIC DNA CODING, CHAOTIC MAP, AND THE PROVISION FOR IMPROVED ROBUSTNESS

R. RATHEESH KUMAR [1] AND JABIN MATHEW

ABSTRACT. This paper suggests a system for encrypting color images using Hui Liu-Bo Zhao-Linquan Huang algorithm and having improved robustness. The system is an extension for encrypting color and grayscale images using DNA Bases Probability and 2D Logistic Map. The system has four subsystems – the subsystem for grayscale images, the subsystem for color images, the subsystem with scrambling and descrambling for grayscale images for more robustness, and the subsystem with scrambling and descrambling for color images for more robustness. The proposed system has the advantages of high security, great performance, parallelism, and improved robustness.

1. INTRODUCTION

A good image encryption for grayscale remote-sensing images was proposed by Hui Liu, Bo Zhao, and Linquan Huang in their paper titled "A Remote-Sensing Image Encryption Scheme Using DNA Bases Probability and Two-Dimensional Logistic Map" published in IEEE Access of May 2019 [1]. Their system has great advantages – parallelism, high security, and greater performance, and is well suited for grayscale remote-sensing images. It explains histogram, variance, correlation, information entropy, differential, key sensitivity, keyspace, complexity and speed analyses. We extended the idea and developed a system with four subsystems – the subsystem for grayscale images, the subsystem for

[1]*corresponding author*

2020 *Mathematics Subject Classification.* 68U10.

Key words and phrases. DNA, Chaos, DNA bases probability, 2D logistic map, Robustness.

color images, and the subsystems with an additional scrambling and descrambling for grayscale images and color images to provide improved robustness, and explain chi-square, robustness, perceptual, and PSNR and information loss analyses in addition to the abovesaid analyses. The basic idea is the Hui Liu-Bo Zhao-Linquan Huang algorithm, i.e., image encryption using DNA bases probability and 2D Logistic Map. The system is an outcome of the combination of two alternative methods of image encryption, DNA cryptography and chaotic theory.

2. Hui Liu-Bo Zhao-Linquan Huang Algorithm

(Algorithm courtesy [1]). Hui Liu, Bo Zhao, and Linquan Huang developed an image encryption algorithm that is well suited for grayscale remote-sensing images. This algorithm is based on DNA computing and chaotic theory. For DNA computing, it uses DNA encoding and decoding, DNA addition and subtraction, and DNA bases probability calculation. For chaos, it uses 2D Logistic Map [1].

2.1. **DNA Encoding and Decoding Rules.** The algorithm uses dynamic coding.

Table 1. DNA encoding/decoding rules

Rules	Rule1	Rule2	Rule3	Rule4	Rule5	Rule6	Rule7	Rule8
00	A	A	T	T	C	C	G	G
01	C	G	C	G	A	T	A	T
10	G	C	G	C	T	A	T	A
11	T	T	A	A	G	G	C	C

2.2. **DNA Addition and Subtraction Rules.**

Table 2. DNA addition rules

+	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

Table 3. DNA subtraction rules

-	A	G	C	T
A	A	T	C	G
G	G	A	T	C
C	C	G	A	T
T	T	C	G	A

2.3. **2D Logistic Map.** This two-dimensional chaotic map produces good pseudo-random numbers.

$$x_{n+1} = \mu_1 x_n(1 - x_n) + \gamma_1 y_n^2,$$
$$y_{n+1} = \mu_2 y_n(1 - y_n) + \gamma_1(x_n^2 + x_n y_n),$$

where μ_1, μ_2, γ_1 and γ_2 are chaotic map control parameters. When these control parameters meet $2.75 < \mu_1 \leq 3.4$, $2.75 < \mu_2 \leq 3.45$, $0.15 < \gamma_1 \leq 0.21$ and $0.13 < \gamma_2 \leq 0.15$, the chaotic map generate good pseudo-random numbers in the region (0,1]. The control parameters are set as $\mu_1 = 2.99$, $\mu_2 = 3.25$, $\gamma_1 = 0.18$, $\gamma_2 = 0.14$.

3. The Proposed System

3.1. **Basic Architecture of the System.**

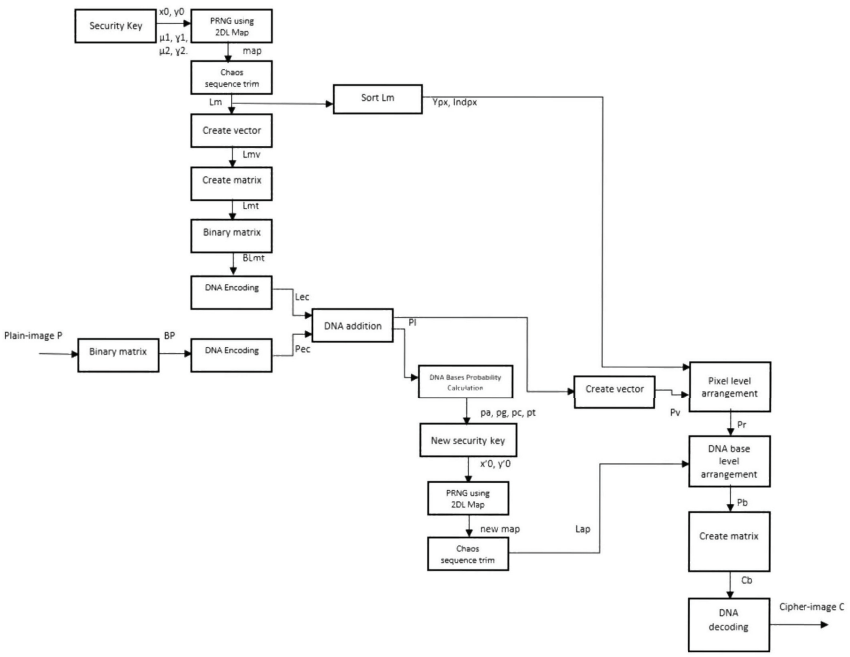

FIGURE 1. Basic architecture of the system

3.2. **Architecture of Encryption for Color Subsystem.** Since a color-image has three matrices, namely R, G, and B, the color subsystem has to prepare and process the image accordingly for the encryption and decryption.

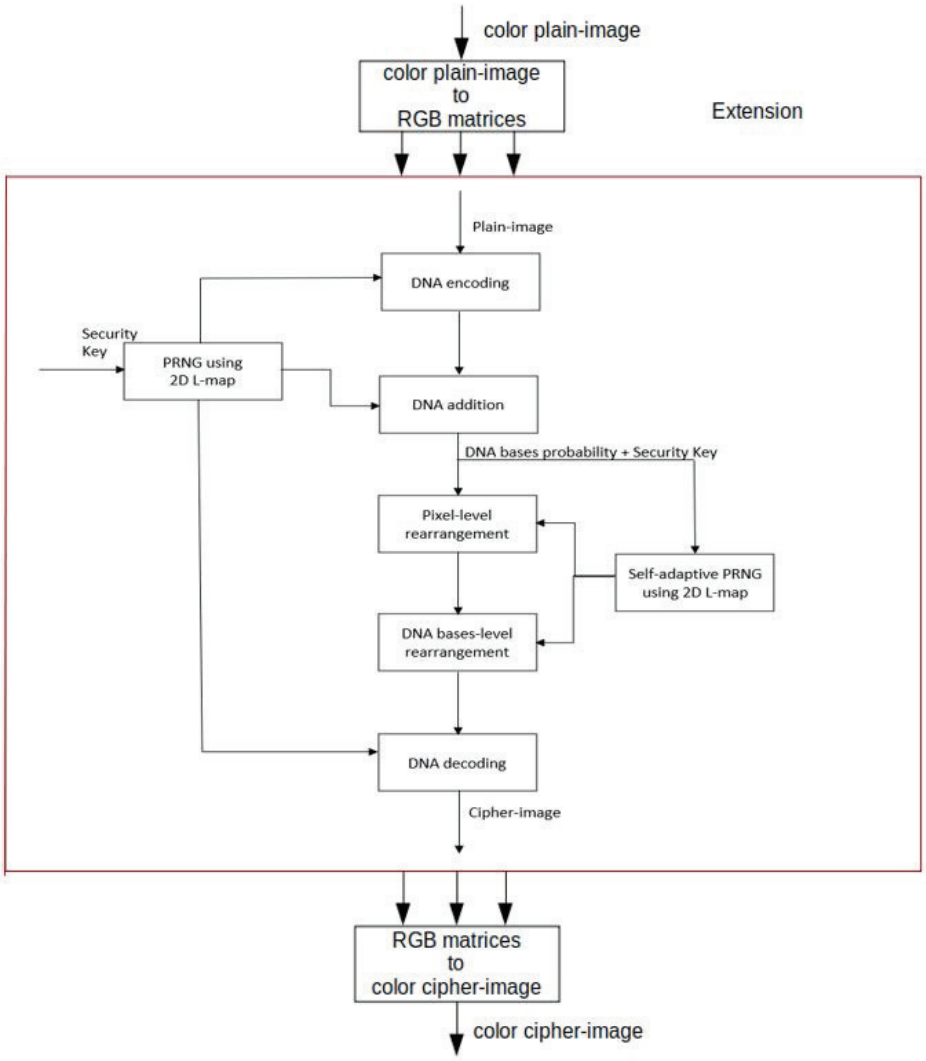

FIGURE 2. Architecture of encryption for color subsystem

The decryption is just the reverse of the encryption. Therefore, its architecture is easier to visualize and simpler to understand.

3.3. **Architecture of Subsystems with additional Scrambling-Descrambling.** First, the cipher is converted to an image having a combination of four numbers of the same cipher, two each horizontally and vertically. Second, a random scrambling is performed on the new image. Then, the scrambled image is transmitted to the receiver. During transmission, the scrambled image gets clipped

due to noise. On the receiver side, first, descrambling of the clipped scrambled image is performed. Then, from the resultant descrambled image, we have to derive the 'actual' cipher for the decryption by using the idea – check all the groups of four respective pixels of the image, if at least two corresponding pixels are same, then take that pixel as the pixel of the resultant cipher, otherwise, take the corresponding first pixel as the particular pixel. Statistically, the probability of information loss is zero or negligible. Therefore, we can maximize the robustness.

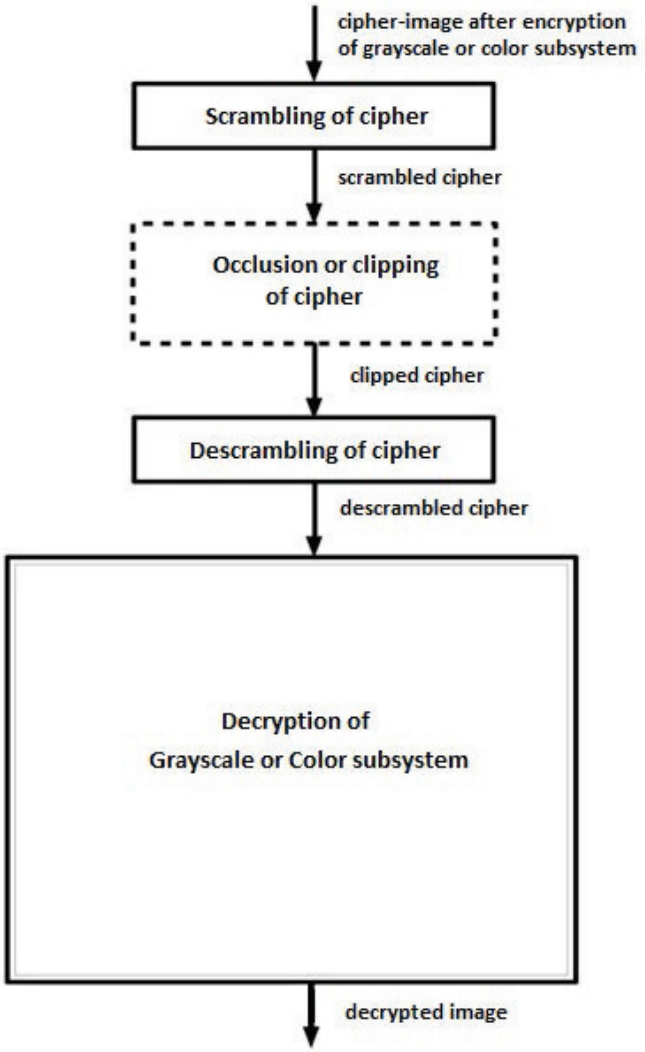

FIGURE 3. Architecture of subsystem with additional scrambling-descrambling

4. Analyses

4.1. **Histogram Analysis.**

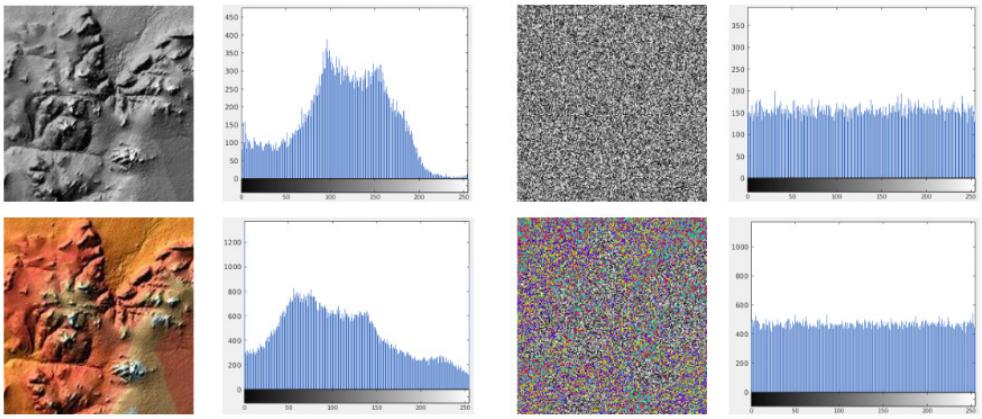

FIGURE 4. Plain-images, cipher-images and their histograms

Figure 4 shows plain-images (GrayImage and ColorImage) have the concentration on some pixel values while their cipher-images have a fairly uniform distribution. The system can resist statistical attacks.

4.2. **Variance Analysis.**

TABLE 4. Variance of images (I)

	Variance Values for GrayImage	
	Plain-image	Cipher-image
	11843	144

TABLE 5. Variance of images (II)

	Variance Values for ColorImage	
	Plain-image	Cipher-image
R	8482	155
G	16844	136
B	47988	130

Variances of ciphers are much smaller than that of plain-images. Therefore, we conclude that the cryptosystem can resist statistical attacks.

4.3. χ^2 **Analysis.**

TABLE 6. χ^2 of images (I)

	χ^2 Values of Grayimage	
	Plain-image	Cipher-image
	19404	252

TABLE 7. χ^2 of images (II)

	χ^2 Values of ColorImage	
	Plain-image	Cipher-image
R	13897	255
G	27597	223
B	78624	212

The χ^2 values of the plain-images are very large and that of the encrypted images are very small [5]. We can conclude that the histogram distribution is uniform.

4.4. **Correlation Analysis.**

TABLE 8. Correlation coefficients of images

	Correlation Coefficients					
	Plain-image			Cipher-image		
Image	CC-D	CC-H	CC-V	CC-D	CC-H	CC-V
GrayImage	0.7323	0.8766	0.8666	-0.0021	-0.0134	0.0025
ColorImage	0.8334	0.9219	0.9170	-0.0008	-0.0012	0.0010

The correlation coefficients of plain-images are closer to 1, on the other hand, that of ciphers are closer to 0. Therefore, the attacker cannot get any useful correlation information to break up the encryption system.

4.5. **Information Entropy Analysis.**

TABLE 9. Information entropy of images

	Information Entropy	
Image	Plain-image	Cipher-image
GrayImage	7.5853	7.9954
ColorImage	7.8076	7.9985

The information entropy values of the plain-images and their ciphers show that the encryption system barely reveals any image information.

4.6. **Differential Analysis.**

TABLE 10. NPCR and UACI of images

Differential Attack Analysis		
Image	NPCR	UACI
GrayImage	0.9963	0.3365
ColorImage	0.9961	0.3341

Results show that the algorithm can resist differential attacks since the reference values of NPCR and UACI are 99.6093% and 33.4635% respectively.

4.7. **Key Sensitivity Analysis.**

TABLE 11. NPCR and UACI for key sensitivity analysis

Key Sensitivity Analysis		
Image	NPCR	UACI
GrayImage	0.9962	0.3319

These values of NPCR and UACI for key sensitivity analysis indicate the significant difference between any two ciphers of the same plain-image.

4.8. **Noise and Information Loss Analyses.**

TABLE 12. Noise and information loss analyses

	Hue	Saturation	Luminosity	R	G	B	Resolution	Aspect ratio	PSNR of image	Contrast	Energy	PSNR (img/ img)
Plain-image	0.0667	0.7143	0.8235	210	120	60	200x200x3	1	11.9341	255	$1.2737x10^7$	P/C : 8.1040
Cipher-image	0.5488	0.9216	0.8	16	149	204	200x200x3	1	10.761	255	$1.5322x10^7$	P/D : ∞
Decrypted image	0.0667	0.7143	0.8235	210	120	60	200x200x3	1	11.9341	255	$1.2737x10^7$	D/C : 8.1040

From the values of Color Image, we can say that the encryption and decryption have no information loss during the execution of algorithms [2,3].

4.9. **Robustness Analysis.**

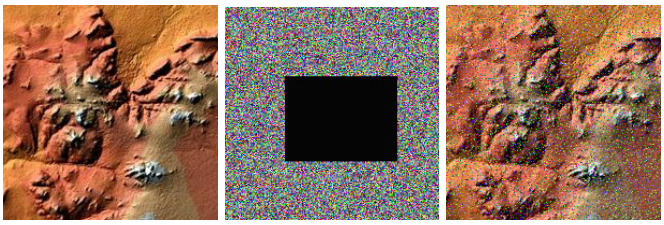

FIGURE 5. Plain-image, Cipher-image, Decrypted image.

The subsystems I and II support only some robustness (some pixels of the decrypted image are lost). The subsystems (III and IV) with additional scrambling and descrambling help maximizing the robustness. The improved robustness can be achieved and viewed as follows:

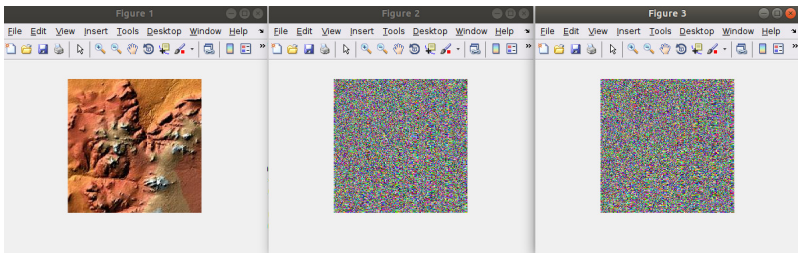

FIGURE 6. Plain-image, cipher-image, and scrambled cipher-image

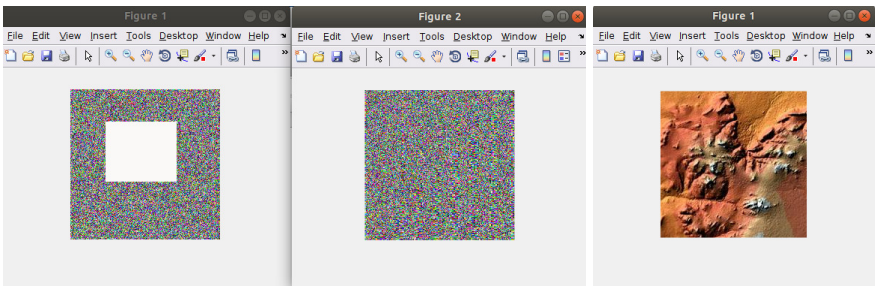

FIGURE 7. Clipped cipher, descrambled cipher, and decrypted image

4.10. **Perceptual Analysis.**

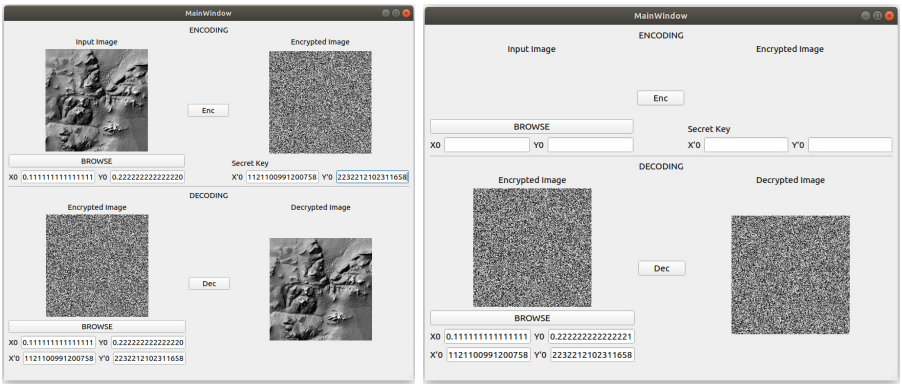

FIGURE 8. Perceptual analysis

The right key produces the plain-image back. The slightly different key does not produce the plain-image back.

4.11. **Keyspace, Complexity, and Speed Analyses.**

TABLE 13. Keyspace, Complexity and Speed Analyses

Keyspace	Complexity		Speed (200x200 images)			
	Grayscale SS	Color SS	Grayscale SS		Color SS	
			Enc	Dec	Enc	Dec
$> 2^{300}$	$6 \times M \times N$	$18 \times M \times N$	79s	56s	185s	168s

The system can resist the brute force attacks. The system is O(N^2). [4] It has acceptable encryption and decryption speeds.

5. Conclusion

The system provides fairly uniform distribution, high information entropy, reduction in high correlation, and improved robustness. It supports high security, high encryption and decryption speeds, and parallel operation. This may be extended to medical-image, audio and video encryption.

References

[1] H. Liu, B. Zhao, L. Huang: *A Remote-Sensing Image Encryption Scheme Using DNA Bases Probability and Two-Dimensional Logistic Map*, IEEE Access, **7** (2019), 65450–65459.

[2] R. Ratheesh Kumar, J. Mathew: *Image Encryption: Traditional Methods vs Alternative Methods*, IEEE, Proceedings of the Fourth International Conference on Computing Methodologies and Communication (ICCMC) 2020), 619-625, 2020.

[3] R. Ratheesh Kumar, J. Mathew: *How to Evaluate the Security and Performance of an Image Encryption System*, International Journal of Scientific Research in Science, Engineering and Technol-ogy (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, **7**(3) (2020), 302-311.

[4] R. Ratheesh Kumar, J. Mathew: *A Mathematical Interpretation of Images and Image Encryption*, International Journal of Mathematics Trends and Technology (IJMTT), **66**(6) (2020), 190-194.

[5] X. Wang, S. Gao, L. Yu, Y. Sun, H. Sun: *Chaotic Image Encryption Algorithm Based on Bit-Combination Scrambling in Decimal System and Dynamic Diffusion*, IEEE Access, **7** (2019), 103662-103677.

Department of Computer Engineering
Government Polytechnic College
Nedumangad, Kerala, India
Email address: ani76r@gmail.com

Department of Computer Science and Engineering
Government Engineering College
Idukki, Kerala, India
Email address: jabin1984@gmail.com