ISSN 2229-5518

A Comparison of Two Image Encryption Algorithms with Chaotic Maps

Ratheesh Kumar R

Abstract — Two image encryption algorithms based on chaotic theory are compared with respect to security. The first algorithm works on the principles of DNA cryptography and pseudo-random number generation; its chaotic map is 2D Logistic Map. The second algorithm uses the principles of Bit-scrambling and Dynamic Diffusion; it has three chaotic maps - Arnold, Logistic, and 2D Logistic-adjusted-Sine maps. Both algorithms have their own merits and limitations. Several evaluation factors are compared here.

Index Terms — chaos, security analyses, correlation, entropy, NPCR, UACI, keyspace, diffusion, uniform distribution.

1 Introduction

Valuable images need to be encrypted because there are susceptible to various security attacks. Security attacks may change the content of images or steal the images or make copies of images or change the identities of the sender. There are also noise and occlusion attacks that may affect the quality of images. So, the security attacks and noise and occlusion attacks are to be taken care of. There are numerous image encryptions and they have their merits and limitations. Here, we are trying to compare two different image encryptions that use chaotic maps along with other techniques. The first [1] uses DNA cryptography and a chaotic map. The second [2] uses three chaotic maps.

Medical, police, military, and remote sensing images have a great value of money and information. User data in these images have both confidential and private information. So, securing images is very essential. Cryptographic schemes help the user to protect the information. Encryption can be done using traditional methods such as DES, AES, RSA and XOR or alternative methods like DNA and Chaos or combinations of them. Security is a major element in image handling, because it is necessary to ensure the secured and authorized access to images. The security issues can be handled by chaotic maps. The Chaotic cryptographic techniques help the users of images to protect their information from unknown access. Image handling has huge security risks as it deals with valuable information. The concept of using Chaotic Maps in the field of cryptography has been identified as a possible technology that brings forward a new ray of hope for unbreakable algorithms as traditional cryptographic techniques built upon mathematical and theoretical models are vulnerable to security attacks.

• *Ratheesh Kumar R is working at Govt. Polytechnic College, Nedumangad, India as a Lecturer in Computer Technology. E-mail: ratheesh1976kumar@gmail.com*

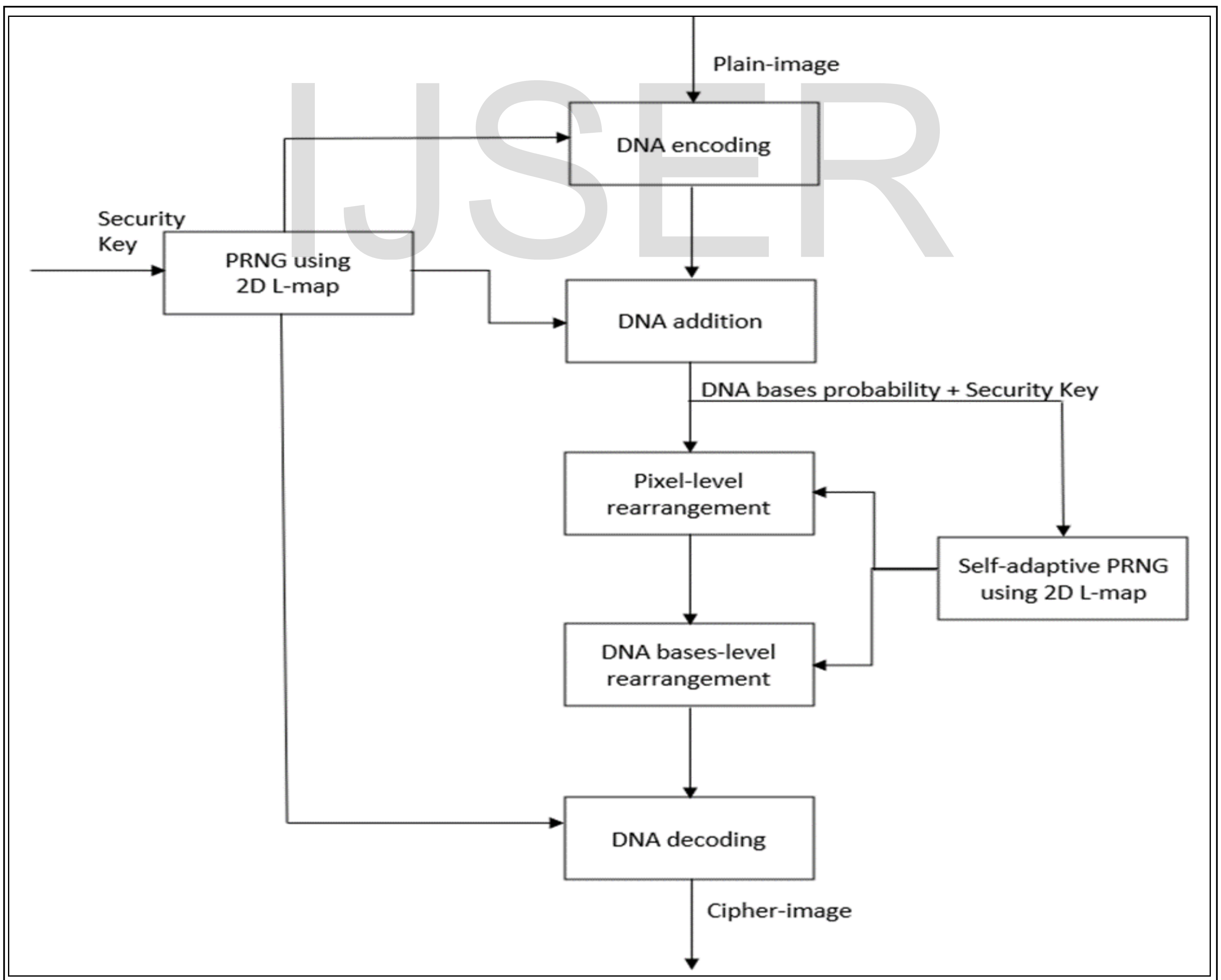
2 Security and Other Analyses

To evaluate image encryption, there are many analyses to be performed – statistical, differential, correlation, entropy, key, robustness, perceptual, speed and performance analyses, etc. For analyzing statistical attacks, we have to compute histogram, variance, and chi-square analyses. Image encryption is said to resist statistical attacks if its cipher-image has uniform frequency distribution. Differential attacks can be analyzed by computing NPCR (number of pixels change rate) and UACI (unified average changing intensity) - to measure the difference between ciphers - NPCR calculates the percentage of different pixel numbers between two images and UACI calculates the average intensity of the difference between the two images. The reference values of NPCR and UACI are 99.6093% and 33.4635% respectively. Correlation coefficients of plain-images must be closed to 1 while that of cipher-images are closed to 0. Then only, the attacker cannot get useful correlation information to break up the cryptosystem by correlation analysis of plain- and cipher- images. Information entropy represents the degree of information confusion, and the more confused the pixel value, the closer of information entropy is to 8 and the less likely the information is leaked. To resist brute force attacks, any image encryption algorithm must have a keyspace greater than $2^{(100)}$. To evaluate the performance, the algorithmic complexity and speed of image encryption algorithm are to be computed and analyzed. Robustness and PSNR (peak signal-to-noise ratio) can be analyzed for noise and occlusion attacks. Verifying whether the cipher-image has information loss or not is another important analysis. For this, resolution, aspect ratio, RGB, hue, saturation, SNR, contrast, luminosity, energy, etc are to be calculated. Key-sensitivity and perceptual analyses are also be used for verifying the quality, effectiveness, and purpose of the key of the image encryption algorithm. NIST-SP800-22 tests can be performed for verifying the pseudo-randomness of keys of the image encryption method.

3 "A Remote-Sensing Image Encryption Scheme Using DNA Bases Probability and Two-Dimensional Logistic Map" of Hui Liu, Bo Zhao, and Linquan Huang [1]

This algorithm works on the principles of DNA and pseudo-random number security. A permutation-and-diffusion structure (PDS) is used for chaotic cryptography. DNA structures and pseudo-random numbers generated out of a secret key mix and shuffle to produce a greater level of chaos. Pseudo-random numbers will be generated by 2D Logistic Map which has good cryptographic features. 2D L-Map uses a security key for pseudo-random number generation (PNRG). For more chaos, DNA addition, and DNA bases- and pixel-level rearrangements are used. The algorithm for encryption involves DNA encoding, two rounds of pseudo-random number generation, DNA addition, DNA Bases probability calculation, pixel-level and DNA bases level rearrangements, and DNA decoding.

Analyses are performed for evaluating keyspace, key sensitivity, security, speed, etc. High NPCR, good UACI, good information entropy, uniform distribution, uniform variance values, low correlation coefficient, good key sensitivity, and good efficiency indicates high security provided by the encryption scheme. Even though the keyspace is greater than the reference value, it is low. It is a demerit. The system can encrypt images with good encryption speed. It supports high security for high-resolution remote-sensing grayscale images. With these features, purpose, complexities, and analyses, this encryption scheme can be considered as a good image cryptographic system.

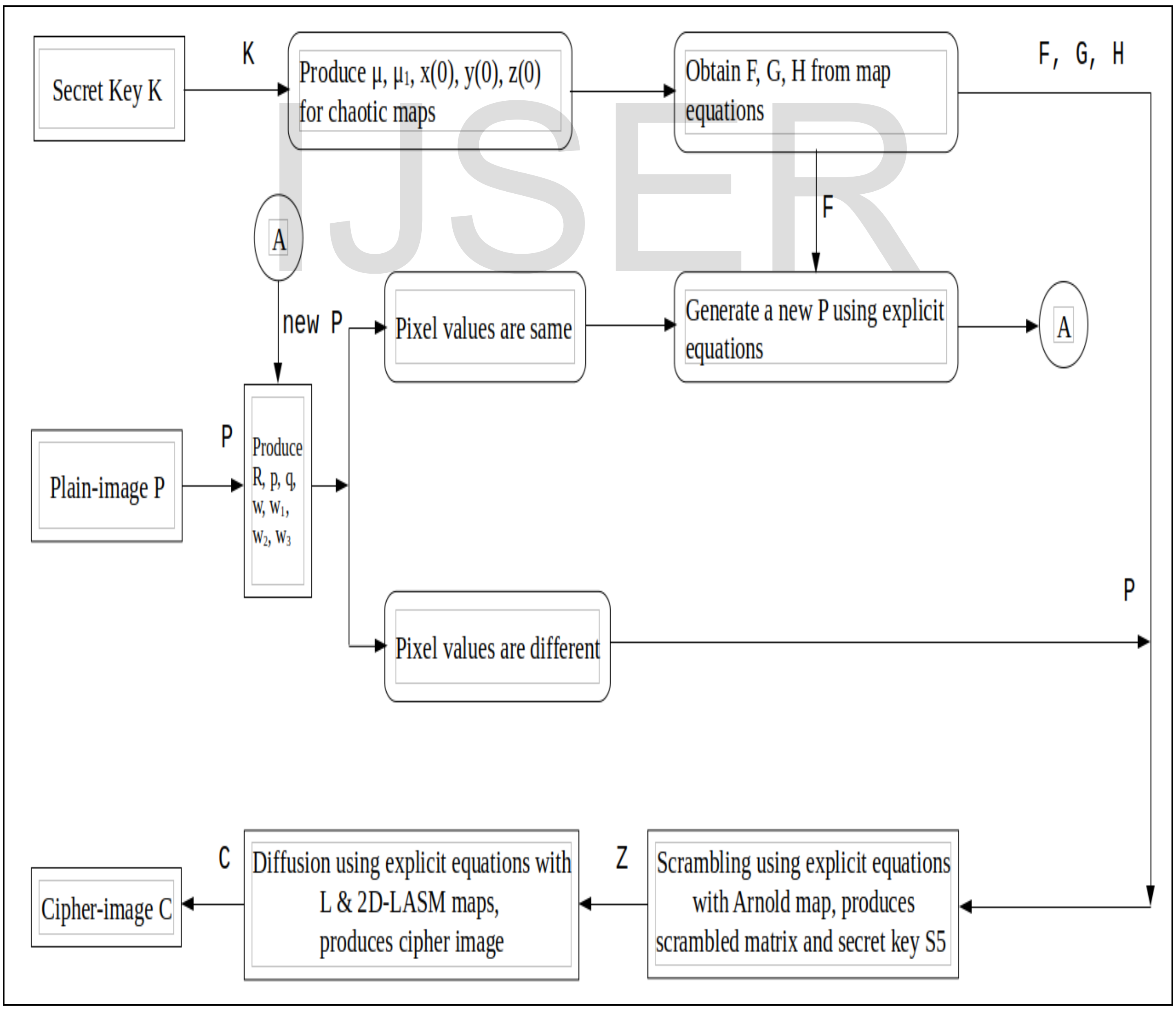


ISSN 2229-5518

4 "Chaotic Image Encryption Algorithm Based on Bit-Combination Scrambling in Decimal System and Dynamic Diffusion" of Xingyuan Wang, Suo Gao, Longjiao Yu, Yuming Sun, and Huaihuai Sun

This algorithm presents an image encryption system using chaos, bit-combination scrambling, and dynamic diffusion. The overall encryption algorithm has two sub-algorithms - one for scrambling and the other for diffusion. Scrambling works based on decimal systems and Arnold mapping and diffusion is based on binary system and XOR theory. Logistic and 2D Logistic-adjusted-Sine maps are utilized for performing diffusion. The ingredients of the overall chaotic system - Arnold, Logistic and 2D-LASM maps - provide more chaos, thereby more security. But the overall chaotic system makes the algorithm complex.

Analyses are performed for evaluating keyspace, key sensitivity, security, robustness, etc. High NPCR, good UACI, good information entropy, uniform distribution, uniform chi-square values, low correlation coefficient, low PSNR, good perceptual property, and good robustness indicates high security provided by the encryption scheme. Even though the keyspace is greater than the reference value, it is low. It is a demerit. The system can encrypt images with good encryption speed. It supports high security for both grayscale and color images. The algorithmic and mathematical complexity of the system is a minus. With these features, purpose, complexities, and analyses, this encryption scheme also can be considered as a good image cryptographic system.



5 COMPARISON OF THE TWO ALGORITHMS

Comparison Factors	A Remote-Sensing Image Encryption Scheme Using DNA Bases Probability and 2-Dimensional Logistic Map [1]	Chaotic Image Encryption Algorithm Based on Bit-Combination Scrambling in Decimal System and Dynamic Diffusion [2]
Authors	Hui Liu, Bo Zhao, and Linquan Huang	Xingyuan Wang, Suo Gao, Longjiao Yu, Yuming Sun, and Huaihuai Sun
Journal	IEEE Access	IEEE Access
Published Date	May 17, 2019	July 25, 2019
Purpose	Image Encryption	Image Encryption
Method	DNA Bases Probability and 2-Dimensional Logistic Map	Bit-Combination Scrambling and Dynamic Diffusion
Chaotic Maps	2D Logistic Map	Arnold Map, Logistic Map, and 2D Logistic-adjusted-sine Map
DNA computing	Yes	No
Input Image Type	Grayscale	Grayscale and Color
Output Image Type	Grayscale	Grayscale and Color
Key Analyses		
1. Keyspace (>2^{100})	Not computed	2^{165}
2. Key Sensitivity	Yes	Not analyzed
3. Perceptual	Not analysed	Yes
Differential Analyses		
1. NPCR	99.5987% to 99.6235%	99.5968% to 99.6219% for Grayscale and 99.5949% to 99.6273% for Color
2. UACI	33.3371% to 33.5084%	33.3308% to 33.5607% for Grayscale and 33.3948% to 33.4829% for Color
Statistical Analyses		
1. Variance	Uniform distribution	Not computed
2. Histogram	Uniform distribution	Uniform distribution
3. Chi-square (χ^2)	Not computed	Uniform distribution
Correlation Coefficient	0.0017 to 0.0250	-0.0002 to 0.0045
Information Entropy	7.9972 to 7.9993	7.9992 to 7.9994
Noise Analyses		
1. Robustness	Not analyzed	Supported
2. PSNR	Not analyzed	8.0908 to 9.5452
Speed and Performance Analyses		
1. Speed	High	High
2. Complexity	Medium	High
NIST Test	Not tested	Not tested
Information Loss Analyses for Resolution, Aspect Ratio, RGB, Hue, Saturation, SNR, Contrast, Luminosity, Energy, etc	Not analyzed	Not analyzed
Applications	Remote-Sensing Grayscale Images	Grayscale and Color Images No specific applications
Merits	Good for remote-sensing image, Not so complex	Superior analyses and values, Good encryption method
Limitations	Not for color images	Complex algorithm

6 Some Inferences

Both algorithms have good values for NPCR, UACI, correlation coefficient, information entropy, speed, etc. Keyspace, perceptual, chi-square, NIST, robustness, noise, and information loss analyses are not done in the first algorithm [1], whereas variance, key-sensitivity, NIST, and information loss analyses are not done in the second algorithm [2].

7 Conclusion

This comparison is not for finding which image encryption algorithm is better. This is only to state their working ideas, their characteristics, and the security and other analyses. Both algorithms support good image encryption and they have many merits and limitations. The first [1] system can be extended to support image encryption of high resolution remote-sensing color images. The second [2] can be extended to provide video and medical image encryption.

Acknowledgment

The author wishes to thank Ms. Jabin Mathew, Assistant Professor in Computer Science and Engineering, Govt. Engineering College, Idukki for her guidance and support.

References

[1] Hui Liu, Bo Zhao, and Linquan Huang, *"A Remote-Sensing Image Encryption Scheme Using DNA Bases Probability and Two-Dimensional Logistic Map"*, IEEE Access, vol. 7, pp. 65450–65459, May 17, 2019.

[2] Xingyuan Wang, Suo Gao, Longjiao Yu, Yuming Sun, and Huaihuai Sun, *"Chaotic Image Encryption Algorithm Based on Bit-combination Scrambling in Decimal System and Dynamic Diffusion"*, IEEE Access, vol. 7, pp. 103662-103677, July 25, 2019.

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

[4] Ratheesh Kumar R and Jabin Mathew, *"How to Evaluate the Security and Performance of an Image Encryption System"*, International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Vol. 7 Issue 3, pp. 302-311, May-June 2020.

[5] Ratheesh Kumar R and Jabin Mathew, *"A Mathematical Interpretation of Images and Image Encryption"*, International Journal of Mathematics Trends and Technology (IJMTT), Vol. 66.6 (2020):190-194.

[6] Ratheesh Kumar R and Jabin Mathew, *"A System with 5-Level Security for Cloud Data and a Comparison of AES and 3DES"*, International Journal of Advanced Research in Engineering and Technology (IJARET), Volume 11, Issue 6, pp. 1046-1055, 2020.

[7] Ratheesh Kumar R and Jabin Mathew, *"An Image Encryption Using Dynamic Dna Coding, Chaotic Map, And The Provision For Improved Robustness"*, Advances in Mathematics: Scientific Journal 9 (2020), no.10, pp. 8957–8967.

[8] Ahmed A. Abd El-Latif, Bassem Abd-El-Atty, and Muhammad Talha, *"Robust Encryption of Quantum Medical Images"*, IEEE Access, vol. 6, pp. 1073–1081, 2017.

[9] Tian Tian Zhang, Shan Jun Yan, Cheng Yan Gu, Ran Ren and Kai Xin Liao, *"Research on Image Encryption Based on DNA Sequence and Chaos Theory"*, Physics: Conf. Series, vol. 1004, pp. 1–6, 2018.

[10] Xing-Quan Fu, Bo-Cheng Liu, Yi-Yuan Xie, Wei Li, and Yong Liu, *"Image Encryption-Then-Transmission Using DNA Encryption Algorithm and The Double Chaos"*, IEEE Photonics, vol. 10, no. 3, 2018.

[11] Xingbin Liu, Di Xiao, and Yanping Xiang, *"Quantum Image Encryption Using Intra and Inter Bit Permutation Based on Logistic Map"*, IEEE Access, vol. 7, pp. 6937-6946, 2019.

[12] Zhenjun Tang, Ye Yang, Shijie Xu, Chunqiang Yu, and Xianquan Zhang, *"Image Encryption with Double Spiral Scans and Chaotic Maps"*, Hindawi Sec.and Comm. Networks, vol. 2019, pp. 1-15, 2019.

[13] Yuling Luo, Xue Ouyang, Junxiu Liu, and Lvchen Cao, *"An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems"*, IEEE Access, vol. 7, pp. 38507–38522, 2019.

[14] Akram Belazi, Muhammad Talha, Sofiane Kharbech, and Wei Xiang, *"Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding"*, IEEE Access, vol. 7, pp. 36667–36681, 2019.

[15] Chunhu Li, Guangchun Luo, and Chunbao Li, *"An Image Encryption Scheme Based on The Three-dimensional Chaotic LogisticMap"*, Network Security, vol. 21, No.1, PP.22-29, 2019.

[16] Zhijuan Deng and Shaojun Zhong, *"A Digital Image Encryption Algorithm Based on Chaotic Mapping"*, Algorithms Computational Technology, vol. 13, pp. 1–11, 2019.

[17] Shikha Jaryal and Chetan Marwaha, *"Comparative Analysis of Various ˙Image Encryption Techniques"*, Computational Intelligence Research, vol. 13, No. 2, pp. 273-284, 2017.

[18] Taiyong Li, Jiayi Shi, Xinsheng Li, Jiang Wu and Fan Pan, *"Image Encryption Based on Pixel-Level Diffusion with Dynamic Filtering and DNA Level Permutation with 3D Latin Cubes"*, Entropy, vol. 21, no. 319, pp. 1-21, 2019.

[19] Priyanka and Deepika Arora, *"Survey and Analysis of Current Methods of Image Encryption Algorithm based on DNA Sequencing"*, IJCST, vol. 9, pp. 34-41, 2018.

[20] Omar Farook Mohammad, Mohd Shafry Mohd Rahim, Subhi Rafeeq Mohammed Zeebaree and Falah Y.H. Ahmed, *"A Survey and Analysis of the Image Encryption Methods"*, Applied Engineering Research, vol. 12, no. 23, pp. 13265-13280, 2017.