Improving the RSA Encryption for Images by Introducing DNA Sequence Encoding

Ali Hennache
Electrical Engineering Department, College of Engineering, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia
ashennache@imamu.edu.sa (corresponding author)

Mamoun Lyes Hennache
Electrical Engineering Department, College of Engineering, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia
G202115910@kfupm.edu.sa

Sidi Mohamed Ahmed Ghaly
Electrical Engineering Department, College of Engineering, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia | Ecole Normale Superieure, Nouakchott, Mauritania
smghaly@imamu.edu.sa

Received: 30 July 2024 | Revised: 18 August 2024 | Accepted: 4 September 2024

 DOI: https://doi.org/10.48084/etasr.8557

ABSTRACT

Recent research is focused on the exploitation of DNA-based molecules for data encryption due to their high capacity to store larger volumes of data and lower computation requirements [1, 2]. This study proposes a Hybrid Image Encryption method (HIE) that convolves DNA sequence encoding with the Rivest–Shamir–Adleman (RSA) algorithm to enhance the security of image encryption. The proposed scheme uses small prime numbers to encrypt the image, which is then encoded as a DNA sequence. Subsequently, the encrypted DNA sequence is stored in a physical medium. The encrypted DNA sequence can then be decrypted using the RSA algorithm and the corresponding private key to recover the original image. The results show that using small prime numbers for RSA encryption of an image and encoding it as a DNA sequence can enhance security and reduce computational time.

Keywords-image encryption; RSA algorithm; DNA sequence; cryptography

I. INTRODUCTION

As the volume of digital media increases on the Internet, so does the need to protect digital identities. Digital data privacy becomes crucial to protect sensitive data across various domains, such as medical, government, and military operations. Key applications of digital data protection include private medical records, classified information of personnel in any organization, digital media, and financial documentation held by banking companies [3]. In this scope of ensuring the confidentiality, integrity, and authenticity of digital data, image encryption becomes essential. Image encryption can be defined as the process of converting an image file into a secure format that is not readable/understood by anyone who does not have authentication rights. In broader terms, image encryption can be categorized into Symmetric Image Encryption (SIE) and Asymmetric Image Encryption (AIE). These techniques can be combined to produce more advanced Hybrid Image Encryption (HIE) techniques.

Symmetric encryption, being the most basic method, uses only a single key for the overall encryption/decryption process. SIE can further be divided into more unique techniques, such as AES/DES, S-Box/Chaos-based algorithms, Cellular automata/Neural Network-based algorithms, or DNA and RNA-based encryption algorithms. On the contrary, AIE uses private-public key configurations for the overall protection process. It is considered more secure but it is computationally more complex due to the use of prime number factorization. RSA, ElGamal, and elliptic curve cryptography are some of the popular algorithms in asymmetric encryption [4]. Combining the performance of symmetric encryption methods with the complexity of asymmetric methods can achieve more powerful hybrid encryption methods [5]. RSA encryption has been widely used in the context of hybrid methods, as traditional encryption methods, such as DES and AES, are not used often in image encryption due to the complex nature of images compared to text or other types of data. Although they have been proven secure, in the case of images, they cannot protect

against transmission noise, which can occur during the transmission of digital images [6, 7].

When the pixels of an image are directly manipulated, the approach is considered a spatial domain approach. DNA encoding is categorized under spatial domain approaches [8]. Inspired by the principle of molecular biology, the DNA-based image encryption process is widely used nowadays. It divides the image into three primary color channels, i.e., Red (R), Blue (B), and Green (G), and then DNA encoding operations are used to encode the channels. This process converts the pixel values to DNA base pairs (A, T, G, and C). Then a chaotic map is utilized to generate complex, pseudorandom sequences to scramble or permutate pixel values to increase security. Other algorithms, such as permutation or substitution, can be introduced at this stage to complement the security mechanism. Finally, the three channels (RGB) are combined to obtain the cipher image.

A. RSA Algorithm

RSA is a widely used asymmetric encryption algorithm based on public key cryptography [9]. RSA employs a public key for encryption and a distinct private key for decryption. This study leverages DNA encoding techniques with RSA due to its advantages in efficient storage and minimal resource consumption. The aim is to enhance image security by applying one of the most robust cryptographic algorithms, i.e., DNA coding, to scramble the image pixels. The public and private keys are generated as follows:

- Two different large prime numbers are chosen, let's say f and g, which must be kept secret.
- The interval $N = f \times g$ is calculated, which is used with the public and the private keys.
- $En = (f-1) \times (g-1)$ is calculated and kept.
- An integer number e is chosen, which must be greater than 1 and less than En, such that the greater common divisor of e and En be equal to 1.
- The modulus multiplicative inverse is calculated using $(d \times e)\%\ En = 1$.
- Finally, the public key is obtained, which contains (e and N), while the private key contains (d and N) [9].

Encryption is given by

$$C = P^e \ \%\ N \quad (1)$$

where C is the cipher image and P is the plain image. On the other hand, decryption is given by

$$P = C^d \ \%\ N \quad (2)$$

B. DNA Sequence Coding

DNA sequence-based image encryption is a relatively new approach that uses the unique characteristics of DNA sequences to encrypt and decrypt images. In this technique, the pixels in an image are first converted into DNA nucleotide bases, i.e., Adenine (A), Thymine (T), Cytosine (C), and Guanine (G), where A&T, and C&G bases form complementary pairs, arranged in a specific order within the DNA molecule to encode genetic information [10]. This is then used to generate a DNA sequence. The DNA sequence is then encrypted using a secret key, and finally, the encrypted DNA sequence is used to represent the encrypted image. To decrypt the image, the DNA sequence must be decrypted using the secret key, and then the pixels can be reconstructed from the decrypted DNA sequence. It is imperative to note that a DNA code can represent a binary number. Based on the base complementation concept, Table I shows eight encoding methods for binary numbers [11]. DNA coding is used to map the digital data to A, C, G, and T. After encoding the data, all the information is obtained as combinations of A, C, G, and T.

TABLE I. DNA SEQUENCE ENCODING RULES

DNA	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

For example, let's assume having a pixel with an intensity of 170 in an image. The binary representation of 170 is 10101010. Using rule number 4 gives the DNA sequence T T T T. Now, this sequence should be encrypted using DNA coding. A key is chosen, assume 75, which is represented as 1001011 in binary. Mapping with rule number 4 gives A G T C.

TABLE II. XOR OPERATION FOR DNA SEQUENCES

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

Now, the sequence T T T T is encoded with the key AGTC using the XOR table above. This gives T C A G, and by using the same rule number 4 chosen earlier for mapping, gives the binary number 10110100, which is 180 in decimal. Hence, the pixel value 170 was encoded to 180.

II. LITERATURE REVIEW

Image encryption techniques are classified primarily into optical, spatial, transformative, and compressive sensing domains [8]. In the spatial domain, DNA coding has been extensively exploited and various approaches have been adopted to date. For secure image transmissions, chaos-based cryptography was proposed in [12], using a diffusive layer in a binary matrix to perform bit permutation instead of byte permutation. The results showed high performance with an average time of 2.24 to 31.72 ms for various algorithms compared to standard 2-D cat maps [12]. In [13], random encoding rules and DNA encoding were proposed, in which three DNA matrices were created from an image depending on the DNA encoding rules. The generated DNA was joined to a modern matrix and then permutated by the chaotic matrix to generate the ciphered image. In [14], a Hyper Image Encryption Algorithm (HIEA) was proposed, using dynamic S-boxes calm of DNA and chaotic system. Dynamic S-box calm

of the DNA encoding operation is used to confuse the pixel values of the image to encrypt it. In [15], chaotic-based encryption systems were reviewed and two challenges were discussed: resistance to attack and processing of encrypted images [15]. Similarly, in [3, 16], various other hyperchaotic systems that used DNA coding methods were reviewed, illustrating a proven vulnerability of chaotic systems to being insecure to chosen plaintext.

This study suggests using the RSA algorithm instead of the chaotic map approach. The RSA algorithm is one of the most widely used algorithms in cryptography and one of the strongest yet [17]. The employment of RSA as an image encryption technique is limited due to its inherent approach of choosing large prime numbers for stronger encryption. The format and size of an image pose a computational burden over its efficient working due to its time and memory constraints. To solve this conundrum, in [18], it was described that in practical use cases, symmetric and asymmetric encryption systems are used in tandem. Data were encrypted using AES/DES, harvesting the higher performance benefits of symmetric systems, while using RSA for key management. Thus, better performance was obtained in terms of the speed of symmetric systems while utilizing the enhanced security of RSA systems. As this study aims at reducing complexity and improving performance in conjunction with an enhanced security mechanism, the proposed scheme is based on a novel approach to DNA operation that is expected to provide a strong cipher.

III. PROPOSED APPROACH

RSA depends on selecting high prime numbers to achieve high security against brute-force attacks. However, larger prime numbers cause the encryption and decryption operation to consume time and memory, especially when dealing with image data due to the larger size of the format. Therefore, RSA is not suitable for image encryption [19]. Subsequently, to achieve better security while using the RSA algorithm with relatively small prime numbers, another layer of security must be considered, as small prime numbers can reveal some insight into the nature of the encrypted image.

Figure 1 shows the approach followed. Python code was developed to implement the proposed scheme. The proposed approach describes a DNA-based image encryption method that combines DNA sequence encoding with the RSA algorithm. The method involves encoding the image as a DNA sequence, encrypting it using the RSA algorithm, and storing the encrypted DNA sequence in a physical medium. The encrypted DNA sequence can then be decrypted using the RSA algorithm and the corresponding private key to recover the original image. An RGB image is encrypted using the RSA algorithm with small prime numbers (less than 300). These numbers are generated randomly. The image is encoded with the DNA sequence coding rules. The rule used to obtain the results is Rule no. 1, where A = 00, T=11, C=01, G=10. Subsequently, the reverse process was used to decrypt the data and obtain the original image.

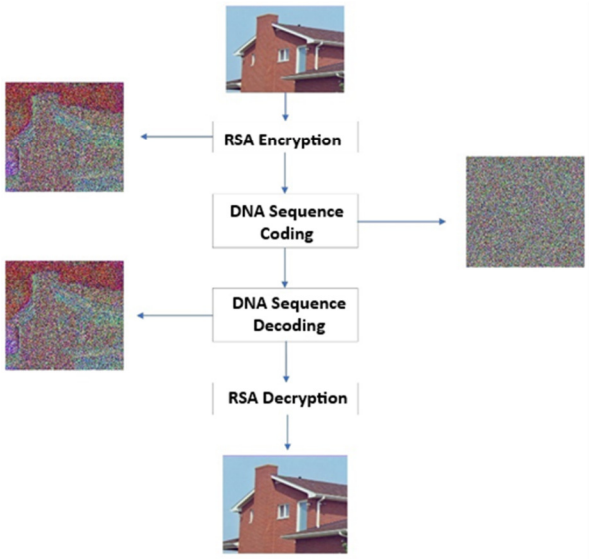

Fig. 1. Flowchart of the proposed scheme with the obtained image after each block.

IV. EXPERIMENTAL RESULTS AND VALIDATION

Six images sized 256×256 and 512×512 were selected to examine the effectiveness of the proposed method. The simulation was carried out on a computer equipped with an Intel Core i5-6300U CPU operating at 2.40 GHz and 8.00 GB of RAM. Figure 1 shows that the encrypted image using the RSA algorithm with small prime numbers is noticeable and can be detected even with the naked eye. However, after the addition of one more layer of encryption that exploits DNA coding, an enhanced cipher image was obtained. Thus, it can be concluded that the proposed approach can correctly encrypt an image for transmission and decrypt it at the reception site.

A. Histogram Analysis

The histogram analysis shows the distribution of the pixel values in the image. To prevent the attacker from obtaining useful statistical information, an encrypted image should have a histogram that is distributed uniformly as much as possible [18, 19]. Figure 2(a) shows three plain images, and Figure 2(b) shows their RGB histograms. Figures 2(c,d) show the cipher images and their corresponding RGB histograms. The change in the distribution of the pixel values in the histograms of the cipher images can be observed compared to that of the plain images. Pixels are uniformly distributed in a triangular manner, forming a neat Gaussian distribution curve that does not reveal much information about the original image. Hence, it can be concluded that this cipher cannot be easily reverse-engineered to obtain the original image.

B. Cross-Correlation Coefficient

There is a high correlation coefficient between adjacent pixels in every normal image. A secure encryption algorithm should be able to produce cipher images with a low correlation of adjacent pixels. The values of the correlation coefficient range from -1 to +1 [20]. The closer the coefficient value is to zero, the more secure is the image [19, 21]. The correlation is calculated in vertical, horizontal, and diagonal directions. x and

y are the gray values of adjacent pixels in the image and r is the correlation coefficient. Table III shows the correlation of pixels along the vertical, horizontal, and diagonal directions. The following equations show how to calculate the correlation coefficient.

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - mean(x) \times (y_i - mean(y)) \quad (3)$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{(\sigma_x \sigma_y)}} \quad (4)$$

where σ is the standard deviation. From Table III, it can be inferred that the six images performed well in terms of obtaining a coefficient value that is close to zero. The highest cipher correlation was in the baboon image due to the abrupt change of color in adjacent pixel levels.

TABLE III. CORRELATION VALUES OF DIFFERENT IMAGES

		Vertical	Horizontal	Diagonal
House	Plain image	0.958757	0.980803	0.943865
	Cipher image	0.001955	0.005921	0.015613
Candy	Plain image	0.982800	0.97979	0.966208
	Cipher image	0.007594	0.013358	0.009641
Baboon	Plain image	0.788992	0.875385	0.753312
	Cipher image	0.006599	0.010452	0.016890
Lena	Plain image	0.967821	0.938141	0.915685
	Cipher image	0.010045	0.007638	0.020075
Airplane	Plain image	0.964191	0.9625744	0.9345
	Cipher image	0.006223	0.013216	0.011969
Peppers	Plain image	0.982701	0.98008	0.968719
	Cipher image	0.009017	0.013113	0.017594

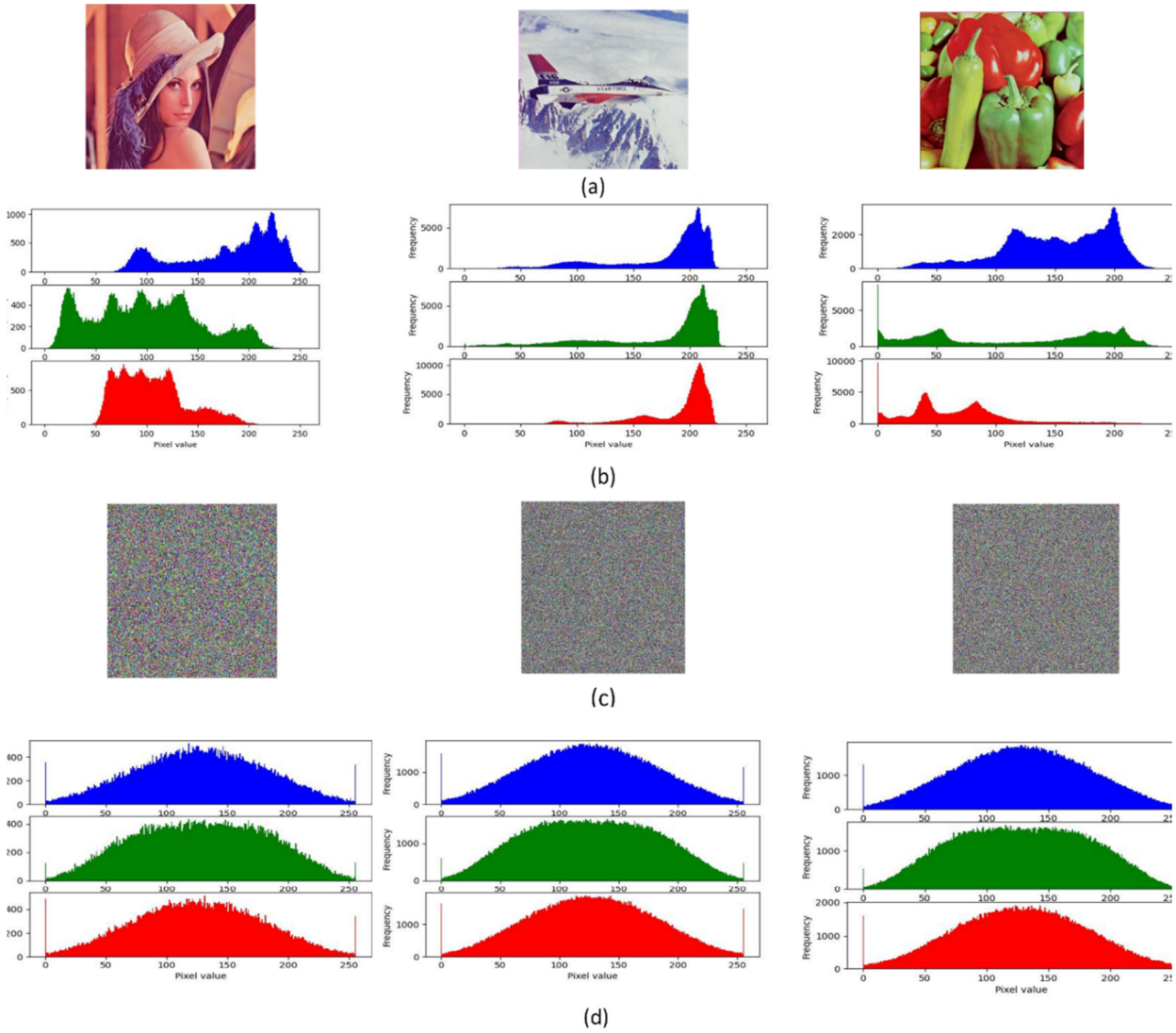

Fig. 2. (a) Plain images, (b) RGB histogram of the plain images, (c) cipher images after encryption, (d) RGB histogram of the cipher images

C. Comparison of Performance Metrics

Encryption/decryption times and memory usage were calculated for the proposed method. Table IV provides an overview of the encryption/decryption and encoding/decoding times. The results show that time is directly proportional to the image size. Hence, the larger the image size, meaning a higher

pixel density, the longer the algorithm will take to create the cipher. Figure 3 shows a graphical view. This points out that the proposed model can be used in applications where smaller image sizes are primarily used, e.g., social media profile photos, web thumbnails, chat and messaging apps, etc.

TABLE IV. MEMORY COMPARISON

	Image size	Memory Usage (in MB)
1	89.7 KB	11.98
2	54.1 KB	11.98
3	498 KB	48.11
4	96.9 KB	11.98
5	280 KB	48.15
6	374 KB	48.09

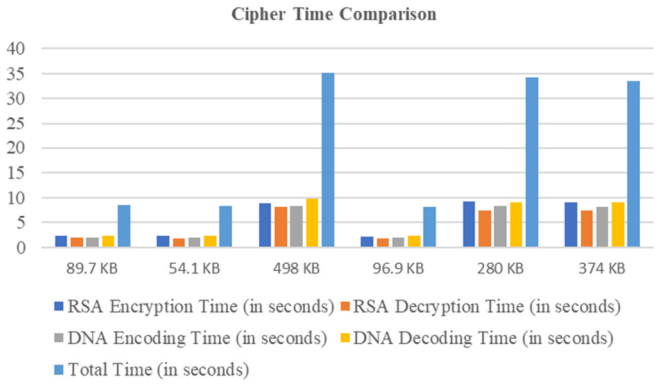

Fig. 3. Cipher time comparison chart.

V. CONCLUSION

The proposed HIE scheme is based on the convolution of the RSA and DNA sequence coding. Low-valued prime numbers were used for encryption and then coded with DNA sequencing techniques. The analysis of RGB histograms of the cipher images showed that image features can be effectively encrypted, providing uncertainty. In addition, a cross-correlation coefficient comparison of adjacent pixels in tested images showed values close to zero, signifying the condition that the closer the correlation coefficient value of adjacent pixels is to zero, the more secure the image. Lastly, the performance of the proposed algorithm was examined in terms of encryption/decryption times and memory usage. The average encryption times (8.1 to 35.1 ms) and memory usage make the proposed model ideal for smaller images [13, 18]. The proposed model can be practically exploited in applications with small-sized images. Furthermore, the proposed approach can be used in military domains to share UAV and satellite imagery data from remote sites to higher headquarters. Similarly, remote sensors deployed for motion detection, fencing arrangement, etc., use smaller image sizes due to their lower power requirements and low processing power. These applications can effectively utilize the proposed image encryption approach before sending sensitive and highly confidential data. Therefore, it can be concluded that this approach has potential use-case scenarios where lower power/performance requirements have to complement a stronger security mechanism. In this case, the proposed scheme of using small prime numbers with RSA and subsequently coding in DNA sequencing can provide an efficient security mechanism. Future research should investigate improvements for the proposed scheme by studying the optimization of hybrid DNA coding schemes. Moreover, with the advent of quantum computing, quantum resistance techniques should be employed in RSA to further complement its mechanism. Moreover, effective case studies on military applications should be conducted to explore potential use.

REFERENCES

[1] X. Xue, D. Zhou, and C. Zhou, "New insights into the existing image encryption algorithms based on DNA coding," *PLOS ONE*, vol. 15, no. 10, 2020, Art. no. e0241184, https://doi.org/10.1371/journal.pone.0241184.

[2] V. A. Gasimov and J. I. Mammadov, "DNA-based image encryption algorithm," *IOP Conference Series: Materials Science and Engineering*, vol. 734, no. 1, Jan. 2020, Art. no. 012162, https://doi.org/10.1088/1757-899X/734/1/012162.

[3] S. Nisha and M. Farik, "RSA Public Key Cryptography Algorithm – A Review," *International Journal of Scientific & Technology Research*, vol. 6, no. 7, pp. 187–191, 2017.

[4] M. SaberiKamarposhti, A. Ghorbani, and M. Yadollahi, "A comprehensive survey on image encryption: Taxonomy, challenges, and future directions," *Chaos, Solitons & Fractals*, vol. 178, Jan. 2024, Art. no. 114361, https://doi.org/10.1016/j.chaos.2023.114361.

[5] C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, K. Perumal, and M. F. Ijaz, "Analytical Study of Hybrid Techniques for Image Encryption and Decryption," *Sensors*, vol. 20, no. 18, Jan. 2020, Art. no. 5162, https://doi.org/10.3390/s20185162.

[6] H. R. Shakir, "A Color-Image Encryption Scheme Using a 2D Chaotic System and DNA Coding," *Advances in Multimedia*, vol. 2019, no. 1, 2019, Art. no. 7074264, https://doi.org/10.1155/2019/7074264.

[7] Z. A. Mohammed, H. Q. Gheni, Z. J. Hussein, and A. K. M. Al-Qurabat, "Advancing Cloud Image Security via AES Algorithm Enhancement Techniques," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 12694–12701, Feb. 2024, https://doi.org/10.48084/etasr.6601.

[8] M. Kaur, S. Singh, and M. Kaur, "Computational Image Encryption Techniques: A Comprehensive Review," *Mathematical Problems in Engineering*, vol. 2021, no. 1, 2021, Art. no. 5012496, https://doi.org/10.1155/2021/5012496.

[9] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Oct. 1978, https://doi.org/10.1145/359340.359342.

[10] C. Qiuqiong, D. Yao, and N. Zhiyong, "An Image Encryption Algorithm Based on Combination of Chaos and DNA Encoding," in *2020 International Conference on Computer Vision, Image and Deep Learning (CVIDL)*, Chongqing, China, Jul. 2020, pp. 182–185, https://doi.org/10.1109/CVIDL51233.2020.00043.

[11] Y. Liu, J. Wang, J. Fan, and L. Gong, "Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences," *Multimedia Tools and Applications*, vol. 75, no. 8, pp. 4363–4382, Apr. 2016, https://doi.org/10.1007/s11042-015-2479-7.

[12] S. El Assad and M. Farajallah, "A new chaos-based image encryption system," *Signal Processing: Image Communication*, vol. 41, pp. 144–157, Feb. 2016, https://doi.org/10.1016/j.image.2015.10.004.

[13] K. Xuejing and G. Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system," *Signal Processing: Image Communication*, vol. 80, Feb. 2020, Art. no. 115670, https://doi.org/10.1016/j.image.2019.115670.

[14] H. Rathod, M. S. Sisodia, and S. K. Sharma, "Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)," *International Journal of Computer Technology and Electronics Engineering*, vol. 1, no. 3, pp. 7–13, 2011.

[15] B. Zhang and L. Liu, "Chaos-Based Image Encryption: Review, Application, and Challenges," *Mathematics*, vol. 11, no. 11, Jan. 2023, Art. no. 2585, https://doi.org/10.3390/math11112585.

[16] Z. Dong, Z. Zhang, H. Zhou, and X.-B. Chen, "Color Image Encryption Based on 4D Hyperchaotic System and RSA Algorithm Combined Scrambling and Diffusion," in *2023 5th International Conference on Industrial Artificial Intelligence (IAI)*, Shenyang, China, Aug. 2023, pp. 1–5, https://doi.org/10.1109/IAI59504.2023.10327529.

[17] B. Mahalakshmi, G. Deshmukh, and V. N. L. N. Murthy, "Image Encryption Method Using Differential Expansion Technique, AES and RSA Algorithm," in *2019 Fifth International Conference on Image Information Processing (ICIIP)*, Shimla, India, Nov. 2019, pp. 363–366, https://doi.org/10.1109/ICIIP47207.2019.8985665.

[18] X. Zhou and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption," in *Proceedings of 2011 6th International Forum on Strategic Technology*, Harbin, China, Aug. 2011, vol. 2, pp. 1118–1121, https://doi.org/10.1109/IFOST.2011.6021216.

[19] E. A. Albahrani and T. K. Alshekly, "New Chaotic Substation and Permutation Method for Image Encryption," *International Journal of Applied Information Systems*, vol. 12, no. 4, pp. 33–39, Jul. 2017.

[20] M. Babu, G. S. Devi, M. Y. Khrisna, M. V. Prasanna, and N. Iswarya, "Image Encryption Using Chaotic Maps and DNA Encoding," *Journal of Xidian University*, vol. 14, no. 4, Apr. 2020, https://doi.org/10.37896/jxu14.4/206.

[21] G. Hanchinamani and L. Kulakarni, "A New Approach for Image Encryption Based on Cyclic Rotations and Multiple Blockwise Diffusions Using Pomeau-Manneville and Sin Maps," *Journal of Computing Science and Engineering*, vol. 8, no. 4, pp. 187–198, 2014, https://doi.org/10.5626/JCSE.2014.8.4.187.