BAREKENG: Jurnal Ilmu Matematika dan Terapan
March 2022 Volume 16 Issue 1 Page 235-242
P-ISSN: 1978-7227 E-ISSN: 2615-3017
https://doi.org/10.30598/barekengvol16iss1pp235-242

MEDICAL IMAGE ENCRYPTION USING DNA ENCODING AND MODIFIED CIRCULAR SHIFT

Kiswara Agung Santoso[1*], Ahmad Kamsyakawuni[2], Muhammad Seggaf[3]

[1,2,3]Departement of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Jember
Jl. Kalimatan No. 37 Kampus Tegalboto Jember, 68121, Indonesia

Corresponding author e-mail: [1] kiswara.fmipa@unej.ac.id*

Abstract. *This paper proposes a new encryption method for the encryption of medical images. The method is used to divide the image into several blocks and then scramble the image blocks using DNA chains and then shift the pixels in a circle with certain rules. To provide a more secure result, the input key contains a DNA chain and is equipped with complementary rules, and is converted into a hexadecimal number using a DNA coding table. Experimental results and values of NPCR and UACI show that the scheme achieves good encryption and decryption results.*

Keywords: *DNA encoding, medical image, cryptography*

Article info:

Submitted: 11th January 2022 *Accepted: 3rd March 2022*

How to cite this article:
K. A. Santoso, A. Kamsyakawuni and M. Seggaf, "MEDICAL IMAGE ENCRYPTION USING DNA ENCODING AND MODIFIED CIRCULAR SHIFT", *BAREKENG: J. Il. Mat. & Ter.*, vol. 16, no. 1, pp. 235-242, Mar. 2022.

1. INTRODUCTION

Technology is developing very rapidly in the era of globalization. Huge amounts of data and information from all industries have been digitized and stored in various cloud storage. The data is not only stored as text data but also in the form of audio and visual data. All of this data and information can be reached and accessed by the public so that it has positive and negative impacts [1]. Some data with personal information may not be consumed by the public because the data has its own level of confidentiality. The authorized party must provide data security guarantees, and only the owner can access the data [2] . Data security has become the focus of research by scientists in the field of technology and information in this modern era. Therefore, a technique called encryption and decryption to secure data and information has emerged to communicate privately and maintain data confidentiality in the field of cryptography [3] [4].

In the medical scope, digitization makes it easier to store and transmit medical data. The transition from film-based imaging to digital imaging simplifies the data acquisition system [5]. With the development of digital imaging, paper-based medical record systems have changed to computer-based medical record systems. The computer-based medical record system stores data in a database to facilitate access to medical data from various parties. However, computer-based medical images also have a high risk because of the possibility that people abroad will access digital images more widely [6]. Sensitive medical images allow them to be accessed instantly by anyone over an unsafe network. Dissemination of digital medical images and bad management of patient medical records can also leak patient data. Therefore, medical images require encryption techniques to protect the confidentiality and integrity of patient medical records through communication networks [7].

According to algorithms that have been proposed for X-Ray images encryption [8], such as Elliptical Curve Cryptography (EEC), the decrypted images are not the same as the original image. Medical images are also encrypted using circular bit shift operations with the modulo principle [9]. This small shift key combination has an effect on the cipher image which still looks the same as the plain image and the level of image randomness is also very low. Dealing with this medical image, pixel arrangement, and random permutation methods were used to encrypt medical images at a high-security level [10]. Modern cryptography such as DNA encoding was used to produce like-randomly medical images with high-security levels [11] [12]. The goal of many previous methods was to ensure image information protection.

In this study, we will utilize DNA encoding and modification circular shift to encrypt medical images. The encryption process is done at the image block level. The image will be shuffled using a random DNA chain key and the modification circular shift. The DNA chain key is also secured by DNA complement rules and converted to a hexadecimal number so that it is not easy to use. The combination of DNA encoding techniques and circular shift is expected to create a new cryptographic algorithm and has a good level of security, because there has been no previous research that discusses medical image security, but discusses medical image compression.

2. RESEARCH METHODS

2.1 DNA Cryptography

Deoxyribonucleic acid (DNA) is formed using four basic nucleic acids, namely, adenine (A), cytosine (C), guanine (G), and thymine (T). The pairs (A, T) and (C, G) complement each other. These alphabets can easily be substituted for binary values (A-00, C-01, G-10, T-11). The number of possible encodings with this rule is 4! = 24. However, only eight combinations are suitable for the DNA complement principle. Just as the binary numbers "0" and "1" complement each other, "00" and "11" and "01" and "10" also complement each other[13].

Table 1. DNA Encoding Rules

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

2.2 Modified Circular Shift

The circular shift is one kind of special shifting based on cyclic permutation. The circular shift is the process of changing values sequentially by shifting the last element or entry to the earliest entry and the rest shifting in order. This circular shift can be done in the reverse direction by shifting the earliest entry to the last entry and so on. If the number of entries (n) in the list and the entries in it are not patterned, then there will be n circular arrays. For example, if there are four entries such as abcd, then the circular shift will have four possibilities like bcda, cdab, dabc, and abcd itself. The basic circular shift is usually used in row vector entries. This method will be modified and used in the matrix form of image pixels. While the basic circular shifts the entries left and right, the modified circular shifts the entries both clockwise and counterclockwise consecutively.

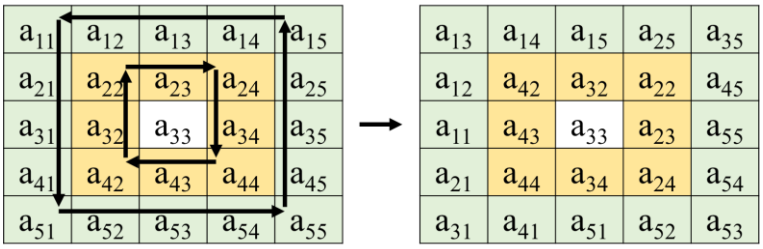

Figure 1. Modified Circular Shift

Generally, for the $\boldsymbol{N \times M}$ matrix, it will be done with iterations as follows. If $\boldsymbol{N \leq M}$, then the number of iterations is $\frac{\boldsymbol{N}}{\boldsymbol{2}}$, otherwise, the number of iterations is $\frac{\boldsymbol{M}}{\boldsymbol{2}}$. Each iteration will arrange the matrix entries as follows.

Table 2. Matrix Arrangement into Row Vector

Iteration	Row vector
1	$a_{1,1}, a_{1,2}, \cdots, a_{1,M}, a_{2,M}, \cdots, a_{N-1,M}, a_{N,M}, a_{N,M-1}, \cdots, a_{N,2}, a_{N,1} \cdots, a_{2,1}$
2	$a_{2,2}, a_{2,3}, \cdots, a_{2,M-1}, a_{3,M-1}, \cdots, a_{N-1,M-2}, a_{N-1,M-1}, a_{N-2,M-1}, \cdots, a_{N-1,3}, a_{N-1,2} \cdots, a_{3,2}$
⋮	⋮
last	(case $\frac{N}{2}$) $a_{\frac{N}{2},\frac{N}{2}}, \cdots, a_{\frac{N}{2},M-\frac{N}{2}}, \cdots, a_{\frac{N}{2}+1,M-\frac{N}{2}}, \cdots, a_{\frac{N}{2}+1,\frac{N}{2}}$ (case $\frac{M}{2}$) $a_{\frac{M}{2},\frac{M}{2}}, \cdots, a_{N-\frac{M}{2},\frac{M}{2}+1}, \cdots, a_{N-\frac{M}{2},\frac{M}{2}+1}, \cdots, a_{\frac{M}{2},\frac{M}{2}}$

The shift key is an integer. If the key is positive, then the shift will be made to the right, or in the modified method, it will be shifted clockwise. Conversely, if the key is negative, the shift will be made to the left, or counterclockwise. For even iterations, the shift is done clockwise, while for odd iterations, the shift is done counterclockwise.

2.3 DNA Encoding with Modified Circular Shift

The proposed encryption and decryption algorithms will use three keys. For the encryption process, the first key (temporal) is given by the user, consisting of 4 digits containing one of the permutations of the four basic nucleic acids to name the variable for image block parts. Then, this key will be inserted into the DNA chain that is generated randomly with the number of iterations $\frac{\boldsymbol{1}}{\boldsymbol{4}}$ times the sum of image blocks. This key is named the "final first key" and is used in the decryption process later. The second key is the DNA encoding key, and the third is the shifting key for modification circular shift.

The image blocks are divided into four parts. If the size of image blocks $\boldsymbol{r \times c}$, the first part contains image blocks from row blocks 1 to $\frac{\boldsymbol{r}}{\boldsymbol{2}}$ and columns 1 to $\frac{\boldsymbol{c}}{\boldsymbol{2}}$. The second part contains image blocks from row

blocks 1 to $\frac{r}{2}$ and columns $\frac{c}{2}+1$ to c. The third part contains image blocks from row blocks $\frac{r}{2}+1$ to r and columns 1 to $\frac{c}{2}$. The fourth part contains image blocks from row blocks $\frac{r}{2}+1$to r and columns $\frac{c}{2}+1$ to c. Each part is assigned to a variable with a variable name according to the key digits of 1(temporal).

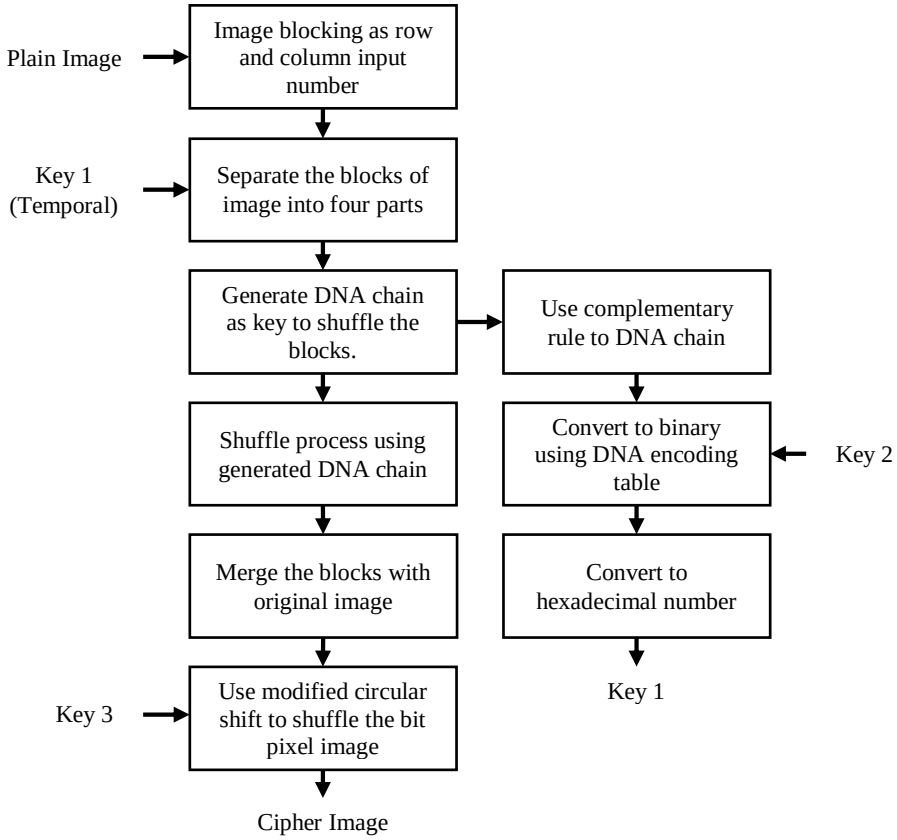

Figure 2. Block Diagram of Encryption Process

The decryption process is done as follows.

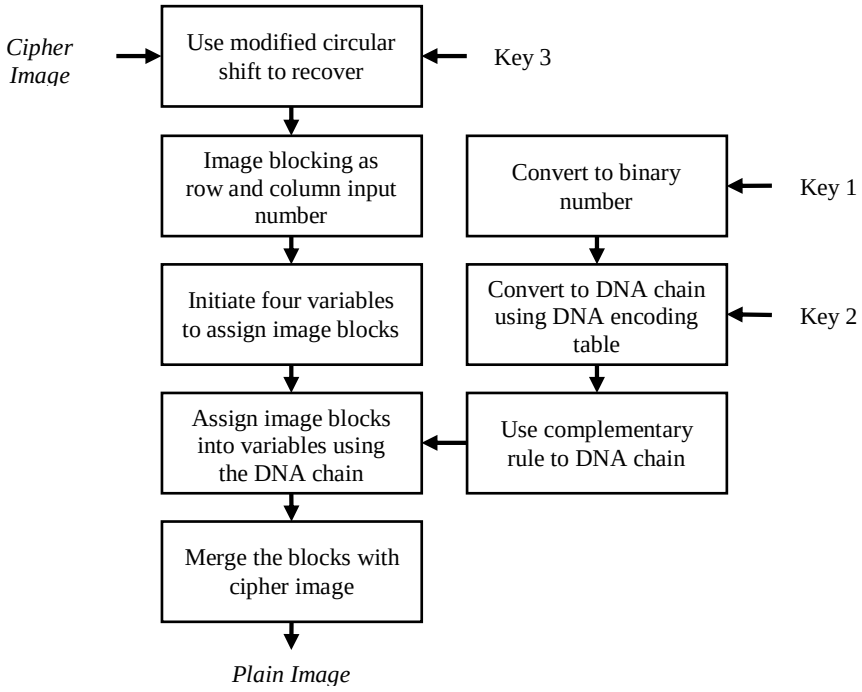

Figure 3. Block Diagram of Decryption Process

The algorithm can be demonstrated using given $\mathbf{4} \times \mathbf{4}$ pixels matrix representation of image. This pixels will be blocked into $\mathbf{2} \times \mathbf{4}$ blocks.

11	201	10	2
7	13	21	255
129	97	65	93
76	51	44	38

The first key (temporal) is generated randomly, such as 'AGTC'. Then, these blocks are divided into four variables as the first key. It is simply illustrated by giving colored blocks. The red blocks are part A, the blue ones are part G, the green ones are part T, and the last ones are part C.

11	201	10	2
7	13	21	255
129	97	65	93
76	51	44	38

The DNA chain is needed to shuffle or encrypt the image blocks, so it is generated randomly once from one of the four basic nucleic acids permutations, such as 'TACG'. The first key is inserted into this DNA chain and it becomes 'AGTCTACG'. The shuffled blocks are given below.

11	10	129	65
7	21	76	44
97	201	93	2
51	13	38	255

After the shuffling block process is done, the image pixels are shuffled again using modification circular shift. Let the shifting key be 5 (key 3). The image will be shown as follows.

2	255	38	13
44	93	201	51
65	76	21	97
129	10	11	7

While the encryption process for the image has been completed, the key is secured using the DNA complement method and DNA encoding. Recall the DNA chain 'AGTCTACG', it is complemented and becomes 'TCAGATGC'. Then the complemented DNA chain is converted to a binary number using DNA encoding table key (key 2) with value 7, it becomes 0001111011001001. The last one, this binary number, is converted to a hexadecimal number as 1EC9.

The decryption is processed by returning the pixel position by using the modification circular shift. The key shift is the negative number of key 3, so it will process the modification circular shift in the opposite way. The result is shown as follows.

11	10	129	65
7	21	76	44
97	201	93	2
51	13	38	255

Then, the next process is image blocking for the image pixels. The number of row and column blocks is inputted as the encryption process rows and column blocks. The first key in the encryption process must be converted to a DNA chain before continuing to the next process. Recall that the first key is 1EC9. Then, this key is converted to a binary number as 0001111011001001. Then, this binary number is converted to a DNA chain using a DNA encoding table whose key 2 value is 7. It becomes 'TCAGATGC', then using complementary rule the DNA chain becomes 'AGTCTACG'.

11	10	129	65
7	21	76	44
97	201	93	2
51	13	38	255

These blocks are assigned to variables as parts A, C, G, and T using the DNA chain, and we get the decrypted image after combining every part in order as the first four digits of the DNA chain. The image result is as below.

11	201	10	2
7	13	21	255
129	97	65	93
76	51	44	38

2.4 NPCR and UACI Analysis

The encrypted image must be checked to ensure that it is different from the plain image. One of the commonly calculated values for such difference is the Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) value [14]. UACI and NPCR value analysis were used to examine the effect of a pixel change on the entire encrypted image. If an encrypted image is given and the plain image has the one-pixel difference, it is denoted by C_1 and C_2. The pixel value at (i,j) pixel in C_1 and C_2 are denoted C_1 (i,j) and C_2 (i,j), respectively. The value of D(i,j) is determined by Equation 2.1

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases} \tag{2.1}$$

Here is the formulas of NPCR and UACI.

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{T} \times 100\% \tag{2.2}$$

$$\text{UACI} = \frac{\sum_{i,j} |C_1(i,j) - C_2(i,j)|}{255 \times T} \times 100\% \tag{2.3}$$

with $\boldsymbol{T}$ is the sum of image pixels.

3. RESULTS AND DISCUSSION

The data used in this study are medical images sourced from the literature [15]. The book contains many medical images with descriptions of the diagnosed patient's diseases. The following are some medical images that are used as material in this study.

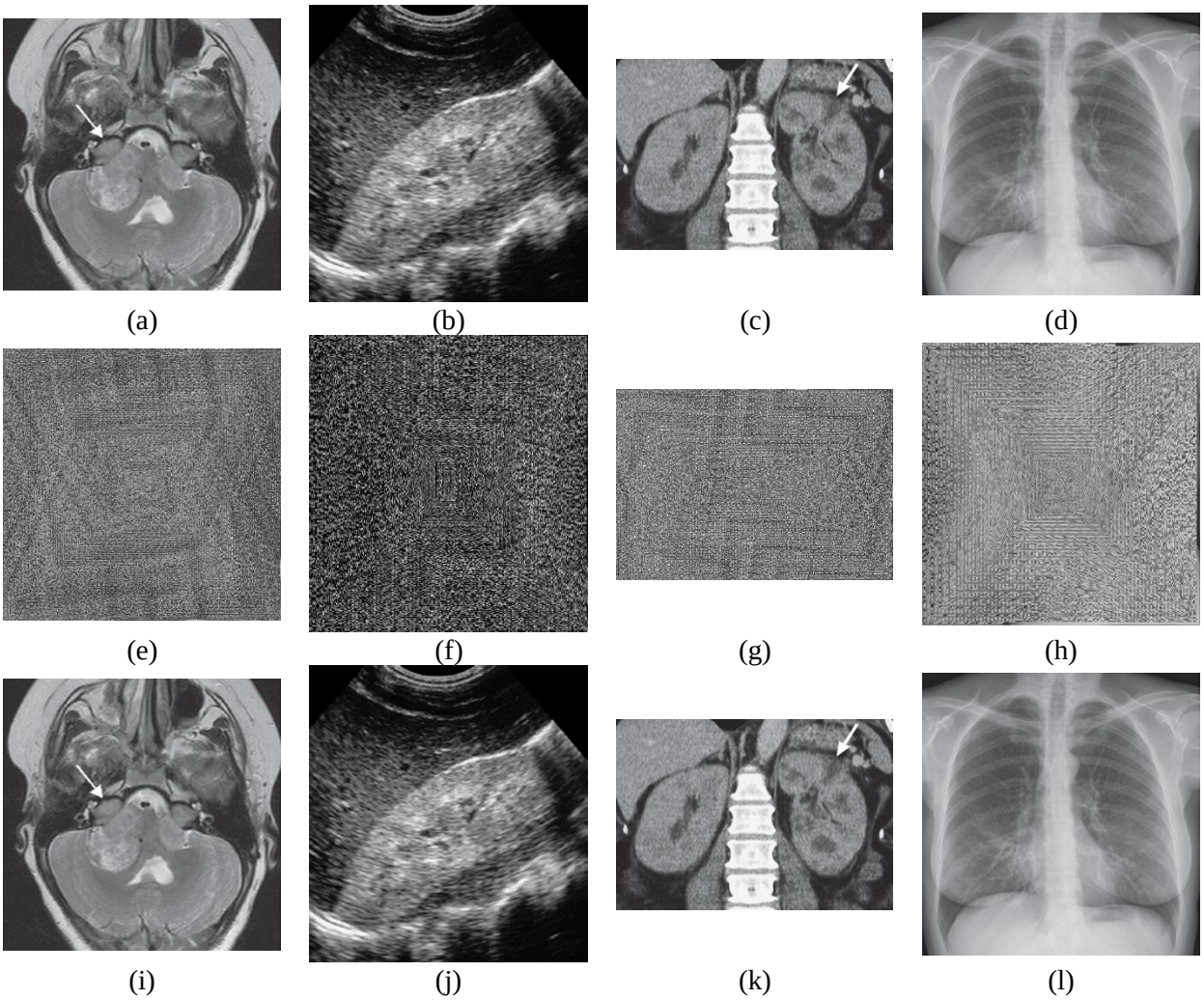

Figure 3. Plain Images (a-d), Encrypted Images (e-h), Decrypted Images (i-l)

Based on the encryption algorithm, the image blocks will be divided into four equal parts. This means that the number of image blocks and column blocks must be 2n so that the encryption algorithm can run properly. Whether the sum of row blocks or column blocks is 2n+1, the algorithm will not execute, because the column blocks or row blocks cannot be divided by two. Figure 3 shows plain images and encrypted images consecutively. The plain images cannot be seen in the encrypted images by visual inspection. It does not have a similarity between the plain images and the encrypted images. While the plain images and the encrypted images look different, the decrypted images are identical to the plain images. Then, using NPCR and UACI, these images will be analyzed further. Table 3 shows the values of NPCR and UACI between plain images and encrypted images and between plain images and decrypted images.

Table 3. NPCR and UACI values

Image 1	Image 2	NPCR	UACI
Brain MRI (plain image)	Brain MRI (encrypted image)	99.1738%	10.1909%
Renal US (plain image)	Renal US (encrypted image)	98.9084%	13.0961%
Kidney CT (plain image)	Kidney CT (encrypted image)	99.2111%	11.4732%
Chest X-Ray (plain image)	Chest X-Ray (encrypted image)	99.2824%	8.4956%
Brain MRI (plain image)	Brain MRI (decrypted image)	0 %	0 %
Renal US (plain image)	Renal US (decrypted image)	0 %	0 %
Kidney CT (plain image)	Kidney CT (decrypted image)	0 %	0 %
Chest X-Ray (plain image)	Chest X-Ray (decrypted image)	0 %	0 %

According to Table 3, the NPCR values between the plain images and the encrypted images are close to 100%. For example, the brain MRI image has an NPCR value of 99.1738%. This number means 99.1738% of image pixels that changed and do not have the same value because the algorithm scrambled the pixel position of the plain images. The brain MRI image also has a UACI value of 10.1909%. This number means

10.1909% of pixels have changed intensity values at each intensity level. This low number of UACI values happens because the encryption process only changes the position of the pixel, not its value. The UACI value represents how much the pixel intensity differences. The next reason is that the images that were used in this case are grayscale images. There is only a small variation in the intensity of the sample images, so it does affect the low UACI value.

The value of NPCR and UACI between the plain images and the encrypted images is 0%. It represents that both of those pixels are identically similar. There is not even a one-pixel difference in the decrypted images. It implies that this algorithm is still worthy and acceptable. One-pixel change may be sensitive to the medical image interpretation and it can be assumed as another diagnoses.

4. CONCLUSION

The proposed encryption and decryption method using DNA encoding rules and modification circular shift can be implemented well. This is indicated by the information from each encrypted image that cannot be seen visually. The encrypted image can also be decrypted or returned to the original image without losing any information. Based on the results of NPCR and UACI calculations, when comparing the plain image and the encrypted image, the image security algorithm using DNA encoding rules and modification circular shift shows a high NPCR value, although the UACI value is still quite low because the pixel intensity variations of the medical images do not vary. When comparing the original image and the decrypted image, the NPCR and UACI values are zero, which indicates that the cryptographic algorithm used is good because it is able to obtain a decrypted image that is identical to the original image.

REFERENCES

[1] S. Paul, P. Dasgupta, P. K. Naskar, and A. Chaudhuri, "Secured image encryption scheme based on DNA encoding and chaotic map," p. 6.
[2] D. Puspa, A. Soegiharto, A. Nizar Hidayanto, and Q. Munajat, "Data Privacy, What Still Need Consideration in Online Application System?," *J. Sist. Inf.*, vol. 16, no. 1, pp. 49–63, Apr. 2020, doi: 10.21609/jsi.v16i1.941.
[3] S. Y. Wulandari, "Cryptography: A Combination of Caesar and Affine Cipher to Conceal the Message," *Proceeding Int. Conf. Sci. Eng.*, vol. 3, pp. 741–744, Apr. 2020, doi: 10.14421/icse.v3.595.
[4] D. E. Agrawal and D. J. Jain, "A Review on Various Methods of Cryptography for Cyber Security," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 6, no. 7, p. 5.
[5] D. C. McWay, *Legal aspects of health information management*. Albany: Delmar Publishers, 1997.
[6] D. E. Detmer and E. B. Steen, "The computer-based record: patient moving from concept toward reality," *Int. J. Biomed. Comput.*, vol. 42, no. 1–2, pp. 9–19, Jul. 1996, doi: 10.1016/0020-7101(96)01176-2.
[7] B. A. N. Nadiyya, K. Usman, S. Aulia, and B. C. Erizka, "X-Ray Images Encryption Analysis Using Arnold's Cat Map and Bose Chaudhuri Hocquenghem Codes," *J. Southwest Jiaotong Univ.*, vol. 55, no. 6, p. 41, 2020, doi: 10.35741/issn.0258-2724.55.6.41.
[8] V. Pardesi and A. Khamparia, "Encryption/Decryption of X-Ray Images Using Elliptical Curve Cryptography with Issues and Applications," in *Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2*, vol. 338, S. C. Satapathy, A. Govardhan, K. S. Raju, and J. K. Mandal, Eds. Cham: Springer International Publishing, 2015, pp. 357–365. doi: 10.1007/978-3-319-13731-5_39.
[9] V. K. Singh, P. K. Singh, and K. N. Rai, "Image Encryption Algorithm based on Circular Shift in Pixel Bit Value by Group Modulo Operation for Medical Images," in *2018 4th International Conference on Computing Communication and Automation (ICCCA)*, Greater Noida, India, Dec. 2018, pp. 1–7. doi: 10.1109/CCAA.2018.8777588.
[10] K. Usman *et al.*, "Medical Image Encryption Based on Pixel Arrangement and Random Permutation for Transmission Security," in *2007 9th International Conference on e-Health Networking, Application and Services*, Taipei, Taiwan, Jun. 2007, pp. 244–247. doi: 10.1109/HEALTH.2007.381640.
[11] H. Liu, X. Wang, and A. kadir, "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft Comput.*, vol. 12, no. 5, pp. 1457–1466, May 2012, doi: 10.1016/j.asoc.2012.01.016.
[12] M. Najaftorkaman, "A Method to Encrypt Information with DNA-Based Cryptography," *Int. J. Cyber-Secur. Digit. Forensics*, vol. 4, no. 3, pp. 417–426, 2015, doi: 10.17781/P001648.
[13] K. S. Mohamed, *New Frontiers in Cryptography: Quantum, Blockchain, Lightweight, Chaotic and DNA*. Cham: Springer International Publishing, 2020. doi: 10.1007/978-3-030-58996-7.
[14] Y. Wu and S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption," p. 9, 2011.
[15] L. A. Grant and N. Griffin, *Grainger & Allison's diagnostic radiology essentials*, Second edition. Edinburgh: Elsevier, 2019.