

Bit-based cube rotation for text encryption

Rihartanto¹, Didi Susilo Budi Utomo¹, Heryn Februariyanti², Arief Susanto³, Wardatul Khafidhah¹

¹Department of Information Technology, State Polytechnic of Samarinda, Samarinda, Indonesia

²Department of Information System, Stikubank University, Semarang, Indonesia

³Faculty of Engineering, Muria Kudus University, Kudus, Indonesia

Article Info

Article history:

Received Nov 27, 2021

Revised Jul 14, 2022

Accepted Aug 22, 2022

Keywords:

Bit-based cube rotation

Encryption

Diffusion

Confusion

Avalanche Effect

ABSTRACT

Today's rapid technological developments make information increasingly important. Not just its content, but the channels or media used for information distribution also need to be secured. Information security is an important aspect that requires serious attention. One of the most important parts of information security is implementation of encryption using certain methods or techniques. This study proposes bit-based cube rotation to secure a plaintext. The aim is to produce a ciphertext that satisfies the two properties of cryptography through diffusion to produce confusion. The result shows that in a normal sentence, there is a significant change in the ciphertext which has the highest avalanche effect value of 55.47% and a correlation coefficient of 0.115. This result proves that the bit-based cube rotation can produce a good ciphertext, where the encryption result is not influenced by its original text.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Rihartanto

Department of Information Technology, State Polytechnic of Samarinda

Jl. Cipto Mangunkusumo, Gunung Panjang Campus, Samarinda 75131, Indonesia

Email: rihart.c@gmail.com

1. INTRODUCTION

Information is an important commodity for governments, private organizations, universities, non-governmental organizations (NGOs), or even individuals. Today's rapid development in technologies makes information increasingly important. Not just its content, but the channels or media used for information distribution also need to be secured. The extensive use of the internet makes it easier for a person or certain parties to get whatever information he wants. This ease of access opens opportunities for abuse by irresponsible parties in carrying out illegal actions such as hacking sensitive or confidential data.

Information security is an important aspect that requires serious attention. Encryption using certain methods or techniques is included to the efforts in securing information. Meanwhile, the type of information that can be secured is not only in the form of text but also images or other digital forms. Cryptography is an art or science that is used to secure or protect data and information [1], [2]. The purpose of securing information is to secure it from unauthorized users, in the context that only those who have appropriate permission can access the contents of the information. The cryptography process is divided into two parts, namely encryption and decryption process. Both processes usually require a keyword, where the keyword can be symmetrical or asymmetrical [3] depending on the cryptographic technique that is being used.

According to information theorist Claude Shannon in his 1945 classified report "A Mathematical Theory of Cryptography", there are two important properties in strong encryption algorithms [4]–[6], they are confusion and diffusion. Confusion is an encryption operation where the relationship between key and ciphertext is obscured. It hides the relationship between the ciphertext and the key. Thus increases the ambiguity of ciphertext and it is used by both block and stream ciphers. Diffusion is an encryption operation

where the influence of one plaintext symbol is spread over many ciphertext symbols with the goal of hiding statistical properties of the plaintext. A simple diffusion element is the bit permutation, which is used frequently within data encryption standard (DES).

Transposition is a technique that satisfies diffusion properties in cryptography. In the transposition, an element experiences a displacement from its original location to another. There is no change in the data, but the displacement can produce a different sequence of data than its original. There are several transposition techniques that are widely used in data encryption, including columnar transposition [7]–[9], double transposition [10] and zigzag transposition [11]. This technique can be used either for text [7], [8], [12], image [13] or audio encryption [14]. In a number of studies, transposition and permutation is also used to optimize other encryption algorithms such as rail-fence cipher [15], Vigenere cipher [10], [12], [16] and advanced encryption standard (AES) [17]. Another study uses transposition for image processing [18].

In three-dimensional space, transposition is carried out using a cube shape [19], [20] imitating the Rubik's cube principle [21]–[23]. In its implementation, there are two ways of placing data into the cube, the first on the side of the cube as in the Rubik game [19], [20], [24] and the second by considering the cube as a 3D array [25]. All of these studies that implement the cube rotation approach are used to encrypt the image. Mostly by combining cube rotation with other methods such as Fourier transform [20], scrambling algorithm [20], [21], chaotic sequence [21] and logistic sequence [21], [23]. The encrypted data is the intensity value of the pixels that are in the value space of 0 to 255. Changes in the intensity value and displacement of the pixel positions will produce an image that is visually different from the original one.

In contrast to those studies, in this study the encrypted data are text characters that have American standard code for information interchange (ASCII) values in the range 32 to 126. The transposition is carried out in the form of bit-based cube rotation to produce characters that are in the ASCII value space of 0 up to 255. Each cube element contains a single bit of a character. The cube is an array of $8 \times 8 \times 8$, so each cube will need 512 bits or 64 bytes of data. Meanwhile, the rotation of the cube follows the X, Y, and Z axes. The aim of this study is to produce a ciphertext that satisfies the two properties of cryptography through diffusion to produce confusion.

2. METHOD

2.1. Cube rotation

The operation of the cube rotation imitates the operation of square rotation, whereas the square rotation was originally intended to optimize the Vigenere cipher [26]. Square rotation is a process to get a change in the position of an element in a square matrix by rotating it through a certain center and/or angle. This operation is implemented in a two-dimensional array where the number of rows in the array is equal to the number of columns. While the center of rotation is the center of the square. The direction of rotation is clockwise (CW) or counterclockwise (CCW). Whereas the rotating distance in one rotation is a displacement of 90 degrees. The illustration of square rotation is shown in Figure 1(a) for CW and Figure 1(b) for CCW. They both show positional shifting and examples of array element displacement in each direction.

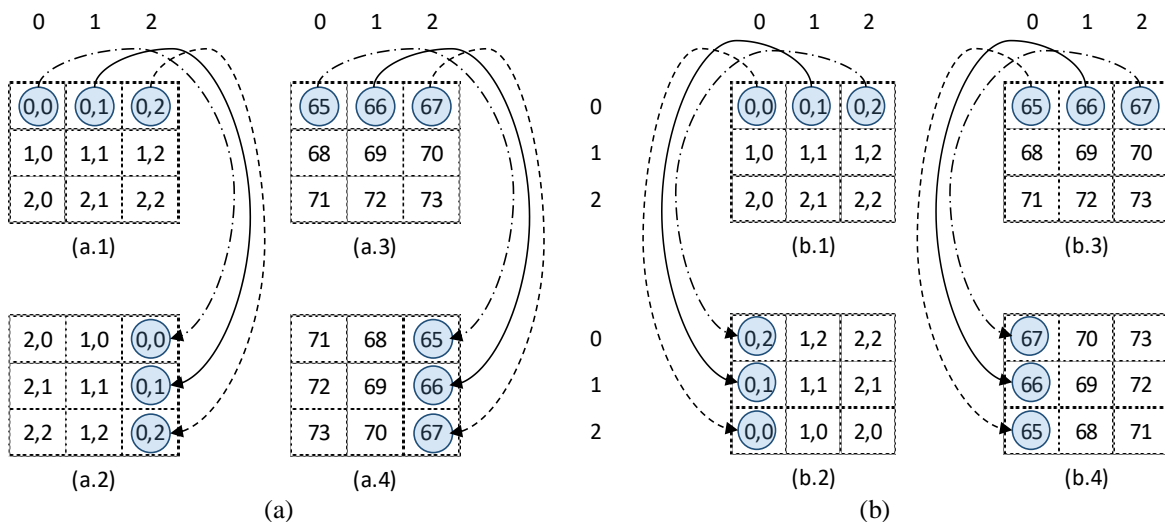


Figure 1. Square rotation: (a) 90° clockwise direction and (b) 90° counterclockwise direction

In Figure 1, (a.1) and (b.1) show the initial array position while (a.3) and (b.3) are the array element before rotation. Furthermore, (a.2) and (b.2) show the displacement results after the rotation was performed. It can be seen in a CW rotation, the element 65 which was originally in the position [0,0] has moved to [0,2]. Element 66 which was originally in the position [0,1] moves to [1,2] and element 67 which was originally in the position [0,2] moves to [2,2], and so on for all other elements in the array.

The mathematical notation for CW rotation can be written as (1) and (2) for CCW rotation [26]. S is the array before rotation while S' is the array after rotation, i is the row index, and j is the column index. The number of rows and the number of columns is represented by n , where in Figure 1 the value of n is 3. An example of using (1), the element of $S'[1,2]$ is taken from $S[0,1]$ which is obtained from $[3-2-1, 1]$. Similarly, using (2), the element $S'[1,0]$ is taken from $S[0,1]$ which is obtained from $[0, 3-1-1]$.

$$S'[i, j] = S[n - j - 1, i] \quad (1)$$

$$S'[i, j] = S[j, n - i - 1] \quad (2)$$

The rotation operation of the cube is similar to the square rotation, except that it works on the 3D space. In the square, each element of the array is represented by $[x, y]$ where x is the row and y is the column. In the cube, each element of the array is represented by $[x, y, z]$ where z is the layer. The facing direction of the cube is on the x -axis, as shown in Figure 2. The rotation on the x -axis is called roll, the rotation on the y -axis is called pitch, and the rotation on the z -axis is called yaw.

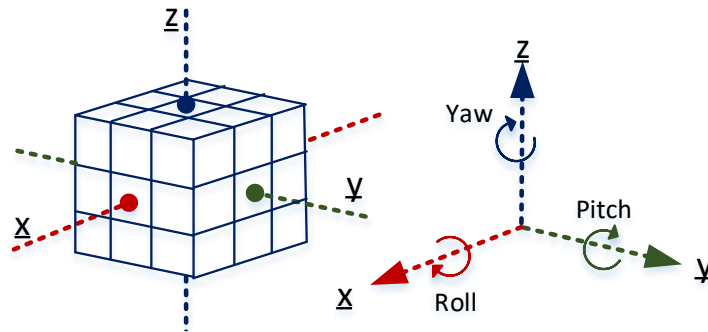


Figure 2. Cube and its rotation

The mathematical notation for cube rotation was written as (3) to (8). xCW and $xCCW$ representing roll, yCW and $yCCW$ representing pitch, while zCW and $zCCW$ representing yaw. $i, j,$ and k are indices for the $X, Y,$ and Z axes, respectively.

$$xCW[i, j, k] = X[n - j - 1, i, k] \quad (3)$$

$$xCCW[i, j, k] = X[j, n - i - 1, k] \quad (4)$$

$$yCW[i, j, k] = X[n - k - 1, j, i] \quad (5)$$

$$yCCW[i, j, k] = X[k, j, n - 1 - i] \quad (6)$$

$$zCW[i, j, k] = X[i, n - k - 1, j] \quad (7)$$

$$zCCW[i, j, k] = X[i, k, n - j - 1] \quad (8)$$

Rotation of the cube can be performed on a specific axis, and it can also be performed on two or three axes in the CW or CCW direction. If more than one axis is involved, then the rotation is carried out sequentially according to the desired axis. On the same axis, twice CW rotation gives the same result as twice CCW rotations. Likewise, three CW rotations are equal to one CCW rotation and vice versa. Whether the CW or CCW, while rotations are performed four times, the result is the same as no rotation.

2.2. Implementation of bit-base cube rotation

Bit-based cube rotation is implemented using an 8×8×8 array. The size of this cube is different from similar studies which mostly apply the use of 3×3×3 cubes [19], [20], [24]. Each element of the array will be filled with bit 0 or bit 1. In order for the cube to be completely filled, 512 bits or 64 bytes of data are needed. These 64 bytes will represent 64 ASCII characters, where each character will be represented by 8 bits of data. Each character bit is stored in sequential columns on the same row. They will start from the first row of the first layer, the second row of the first layer, and so on until the eighth row of the eighth layer.

In cases where the number of characters is less than 64, padding characters are required to cover the deficiency. This shows that bit-based cube rotation belongs to the block cipher group. The number of characters resulting from encryption will always be a multiple of 64.

Each rotation process requires two arrays of the same size. The first array is filled with plaintext and the second array is used to store the rotation results. A cube rotation is the displacement of a cube element that moves 90 degrees in the given direction. While the rotation is done more than once, then on the second rotation, the first array will contain the result of the first rotation while the second array will accommodate the result of the second rotation, and so on. Likewise, when the plaintext length is more than 64 characters, the encryption is carried out sequentially per 64 characters in each process.

The application of (3) and (4) for the rotation on the x -axis is shown in Algorithm 1, and rotation on the y -axis is shown in Algorithm 2. A nested looping is performed according to rows, columns, and layers. The displacement is performed for each array element according to its respective index.

Algorithm 1. Roll, rotation on x -axis

```

Input: cube
Output: cube
1  Function xCW(cube_in)
2  n ← side of the cube
3  for k ← 0 to n-1
4  for i ← 0 to n-1
5  for j ← 0 to n-1
6  cube_out[i,j,k] ← cube_in[n-j-1,i,k]
7  end for
8  end for
9  end for
10 return cube_out

1  Function xCCW(cube_in)
2  n ← side of the cube
3  for k ← 0 to n-1
4  for i ← 0 to n-1
5  for j ← 0 to n-1
6  cube_out[i,j,k] ← cube_in[j,n-i-1,k]
7  end for
8  end for
9  end for
10 return cube_out

```

Algorithm 2. Pitch, rotation on y -axis

```

Input: cube
Output: cube
1  Function yCW(cube_in)
2  n ← side of the cube
3  for j ← 0 to n-1
4  for i ← 0 to n-1
5  for k ← 0 to n-1
6  cube_out[i,j,k] ← cube_in[n-k-1,j,i]
7  end for
8  end for
9  end for
10 return cube_out

1. Function yCCW(cube_in)
2. n ← side of the cube
3. for j ← 0 to n-1
4. for i ← 0 to n-1
5. for k ← 0 to n-1
6. cube_out[i,j,k] ← cube_in[k,j,n-i-1]
7. end for
8. end for
9. end for
10. return cube_out

```

2.3. Differential metric

Avalanche effect (AE) is used to assess how significant the changes that occur in ciphertext are due to small changes in both the message and the key. AE is calculated using (9). AE is said to be good if the bit change that occurs is greater than 45% [27] and very good if it is greater than 50% [28], [29]. The more bits that changed, indicating that the encryption algorithm is increasingly difficult to crack.

$$AE = \frac{\text{number of changed bits in ciphertext}}{\text{number of bits in ciphertext}} \times 100\% \quad (9)$$

2.4. Correlation metric

The correlation coefficient assesses the randomness of the encryption results, in this case, by assessing the relationship between plaintext and ciphertext. The correlation coefficient close to zero or less than 0.2 indicates a very weak relationship between plaintext and ciphertext. Conversely, if the value is close to 1 or -1 means that the encryption result is strongly influenced by the given plaintext. Correlation between plaintext and ciphertext is measured using (10).

$$r = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^n (y_i - \bar{y})^2}} \quad (10)$$

3. RESULTS AND DISCUSSION

Performance measurement of the encryption results using bit-based cube rotation is performed using avalanche effect (AE) and correlation coefficient. Both to measure the amounts of bit changes and the randomness of the encryption results. The four different texts used for these tests are shown in Table 1. Each text contains 64 characters to fill in the cube which each of it has different characteristics. The first text is a normal sentence, the second text consists of repeated phrases, the third text consists of consecutive characters in the ASCII table, and the fourth text consists of the same letter; it is the U letter which has a binary value of 01010101.

Table 1. The plaintexts

Table with 2 columns: Textfile and Content. It lists four textfiles (text1.txt to text4.txt) and their corresponding contents, including a normal sentence, a repeated phrase, an ASCII character sequence, and a binary sequence of U's.

The test is carried out by performing one rotation on each axis, a combination of two axes, and a combination of three axes. The direction of rotation on each axis can be a CW, a CCW, twice CW, or twice CCW. For example, encryption with one rotation of CCW on the XY axis means the displacement of the array elements as far as 90° counterclockwise on the x-axis (roll) and followed by a displacement of 90° counterclockwise on the y-axis (pitch). The decryption process is conducted in the reverse order, namely the rotation on the y-axis followed by the x-axis for one rotation of CW each.

The use of the same direction of rotation on all axes aims to determine the characteristics of the direction of rotation. Likewise, the use of different plaintext aims to determine whether there are text characteristics that are not affected by bit-based cube rotation. When these characteristics are known, optimization can be carried out efficiently.

The first experiment used one CW rotation on all axes, the second used one CCW rotation on all axes, and the third used two CW rotations on all axes. Twice a CW rotation gives the same result as twice a CCW rotation. An example of encrypted text using bit-based cube rotation is shown in Table 2. These ciphertexts are shown in UTF-8 encoding.

Table 2. The ciphertexts of a CW rotation of text1

Table with 2 columns: Axes and Ciphertext. It lists 26 axes (X, Y, Z, xy, xz, yx, yz, zx, zy, xyz, xzy, yxz, yzx, zyx) and their corresponding ciphertexts in UTF-8 encoding.

The test results for each test data are shown in Tables 3 and 4, respectively, to show the AE value and the correlation coefficient on the determined axis according to the direction of CW, CCW, or twice CW. These values show that twice CW in all axes is a worse choice. Meanwhile the ciphertexts in Table 2 obtained from one CW rotation on one or more axes gives completely different results from the original plaintext. This is because bit-based cube rotation changes the plaintext that was in the standard ASCII space in the range value of 0-127 into characters that are in the 0-255 ASCII space. The change in ASCII space value applies to all test data.

Table 3 shows that the AE values in the CW and CCW rotations are mostly above 45% satisfied with scale stated in [27] and many of those values above 50% are relevant to previous studies [17], [28], [29]. It means that the bit-based cube rotation is able to change the data significantly. Of the 15 combinations of rotational axes, in general, only two axis combinations produce AE below 45%, namely on the Y and ZYX axes in CW rotation and Y and XYZ axes in CCW rotation. If it is related to the characteristics of plaintext there is an additional one axis which results in an AE below 45%. The low AE value is due to the encrypted characters are mostly still in the ASCII standard space, different from those generated in the rotation on the other axes where the encryption result is in the ASCII extended space. This is supported by the ciphertext shown in Table 2 where none of the ciphertext shows the characteristics of the original text.

Table 3. The avalanche effects

axes	CW				CCW				2CW			
	text1	text2	text3	text4	text1	text2	text3	text4	text1	text2	text3	text4
x	48.44	48.83	49.22	50.00	48.44	48.83	49.22	50.00	54.69	54.30	50.00	100.00
y	33.20	37.89	42.19	0.00	33.20	37.89	42.19	0.00	31.25	23.83	68.75	0.00
z	53.52	50.39	50.00	50.00	53.52	50.39	50.00	50.00	55.47	54.30	50.00	100.00
xy	48.83	50.78	54.30	50.00	50.78	50.39	48.05	50.00	55.47	54.30	50.00	100.00
xz	51.17	51.56	47.27	50.00	48.83	50.78	54.30	50.00	31.25	23.83	68.75	0.00
yx	50.78	50.39	48.05	50.00	48.83	50.78	54.30	50.00	55.47	54.30	50.00	100.00
yz	48.83	50.78	54.30	50.00	53.13	50.39	50.39	50.00	54.69	54.30	50.00	100.00
zx	48.83	50.78	54.30	50.00	51.17	51.56	47.27	50.00	31.25	23.83	68.75	0.00
zy	53.13	50.39	50.39	50.00	48.83	50.78	54.30	50.00	54.69	54.30	50.00	100.00
xyz	55.47	57.42	43.75	100.00	33.20	37.89	42.19	0.00	0.00	0.00	0.00	0.00
xzy	53.52	50.39	50.00	50.00	55.47	49.61	54.69	50.00	0.00	0.00	0.00	0.00
yxz	48.44	48.83	49.22	50.00	48.44	43.36	53.91	50.00	0.00	0.00	0.00	0.00
yzx	55.47	49.61	54.69	50.00	53.52	50.39	50.00	50.00	0.00	0.00	0.00	0.00
zxy	48.44	43.36	53.91	50.00	48.44	48.83	49.22	50.00	0.00	0.00	0.00	0.00
zyx	33.20	37.89	42.19	0.00	55.47	57.42	43.75	100.00	0.00	0.00	0.00	0.00

Table 4. The correlation coefficient

axes	CW				CCW				2CW			
	text1	text2	text3	text4	text1	text2	text3	text4	text1	text2	text3	text4
x	0.158	(0.048)	0.111	-	0.168	(0.062)	0.079	-	(0.098)	0.279	(0.062)	-
y	(0.178)	(0.046)	0.000	-	(0.178)	(0.046)	0.000	-	(0.003)	0.529	(1.000)	-
z	0.172	0.113	(0.211)	-	(0.154)	0.222	0.075	-	(0.057)	0.004	0.062	-
xy	0.186	(0.023)	(0.381)	-	0.207	0.013	0.105	-	(0.057)	0.004	0.062	-
xz	(0.018)	(0.209)	0.271	-	0.051	(0.005)	0.219	-	(0.003)	0.529	(1.000)	-
yx	(0.077)	(0.243)	(0.219)	-	0.051	(0.005)	0.219	-	(0.057)	0.004	0.062	-
yz	0.186	(0.023)	(0.381)	-	(0.210)	(0.016)	0.381	-	(0.098)	0.279	(0.062)	-
zx	0.186	(0.023)	(0.381)	-	(0.297)	0.026	(0.105)	-	(0.003)	0.529	(1.000)	-
zy	0.038	0.114	(0.271)	-	0.051	(0.005)	0.219	-	(0.098)	0.279	(0.062)	-
xyz	0.315	(0.007)	0.564	-	(0.178)	(0.046)	0.000	-	1.000	1.000	1.000	-
xzy	0.172	0.113	(0.211)	-	0.155	0.180	(0.075)	-	1.000	1.000	1.000	-
yxz	0.158	(0.048)	0.111	-	0.019	0.159	(0.111)	-	1.000	1.000	1.000	-
yzx	0.155	0.180	(0.075)	-	(0.154)	0.222	0.075	-	1.000	1.000	1.000	-
zxy	0.019	0.159	(0.111)	-	0.168	(0.062)	0.079	-	1.000	1.000	1.000	-
zyx	(0.178)	(0.046)	0.000	-	0.315	(0.007)	0.564	-	1.000	1.000	1.000	-

The test results also show that the bit-based cube rotation, which is a diffusion process, is able to produce different characters from the original text as it is generated from the confusion process. This result is supported by a correlation coefficient that is close to zero which indicates no relationship between plaintext and ciphertext. What is considered as the encryption key in this study is the direction and axis of rotation. In contrast to other studies where other algorithms [19]–[21], [23] are involved in producing confusion, in this study, the confusion and diffusion are obtained only from the bit-based cube rotation process.

However, rotation on certain axes gives the same result. In CW rotation, the result of rotation on the Y-axis is the same as the result of rotation on the ZYX axis, as well as the ciphertext that results from rotation on the YZ and ZX axes. In CCW rotation, the same result is produced from the rotation on the Y and XYZ axes as well as the rotations on the XZ and YX axes. This applies to plaintext text1, text2 and text3, while text4 gives different results and really depends on the letters or characters used.

Rotation with twice CW gives the same result as twice CCW rotation. The results of twice CW or twice CCW are not as good as those of a CW or a CCW. At 2CW, twice rotation on the three axes will produce the same text as the original, while a combined rotation on the two axes will produce the same ciphertext with rotation on one axis only. So, twice rotations on all axes are not a recommended option. To overcome this issue, it is recommended to use a different combination of rotation directions on each axis to get a better result while implemented to two or three axes.

The correlation coefficient value is not directly related to the AE value. This is because a high AE value does not always give a correlation coefficient value close to zero. Likewise, a low AE value does not mean it has a correlation coefficient that is further away from zero. Especially for text4, the correlation value cannot be calculated because its standard deviation is zero since all the characters in text4 are the same letter.

In the CW and CCW rotations, most of the correlation values were in the range -0.2 to 0.2, indicating no relationship or very weak relationship between plaintext and ciphertext. It can also be stated that plaintext does not affect the encryption result. There is only one rotation combination whose value is greater than 0.4, which is 0.564 for text3. However, this does not mean that the ciphertext is still influenced by the original text, but rather that most of the encrypted characters still have the same value range, which is still in the ASCII standard space. It should be taken into consideration since this encryption works at the bit level where each character has a different bit sequence, it is possible that even though using the same rotation operation, different plaintext will produce different values of avalanche effect and correlation coefficients from the results of this study.

Although the results of this study cannot be directly compared with previous studies, due to the different nature of the data (image vs. text), the size of the cube, the involvement of other algorithms, the different number of rotations, and the presence of separate rotations in rows, columns, and layers. This study shows a very low correlation between ciphertext and plaintext. These results are relevant to those studies, although the results are not as good as those shown in image encryption. However, when compared with [25] which is used to encrypt text, this study gives better results because it successfully fulfills both characteristics of good encryption, it is confusion and diffusion.

4. CONCLUSION

This study shows that bit-based cube rotation successfully fulfills two cryptographic properties: confusion and diffusion. Bit-based cube rotation which is a diffusion process is able to produce confusion in the form of a significant change in the ciphertext compared to its original. In normal sentences using a CW or a CCW rotation is able to produce ciphertext with avalanche effects above 50%, which indicates a significant change. However, bit-based cube rotation has a disadvantage when the rotation in the same direction on each axis is applied twice, where the rotation on the three axes gives the same result as the original text while rotation on the two axes produces the same ciphertext on one axis. Therefore, further study is aimed at improving the performance of this bit-based cube rotation. One of them is by adding rotation to a number of rows, columns, or layers between the rotations of the cube.

ACKNOWLEDGEMENTS

The authors would like to thank the DPRM Ministry of Research, Technology, and Higher Education for their financial support through Contract No. 151/SP2H/LT/DPRM/2019.





REFERENCES

- [1] S. A. Hannan and A. M. A. M. Asif, "Analysis of polyalphabetic transposition cipher techniques used for encryption and decryption," *International Journal of Computer Science and Software Engineering (IJCSSE)*, vol. 6, no. 2, pp. 41–46, 2017.
- [2] H. Delfs and H. Knebl, *Introduction to Cryptography: Principles and Applications*, Third Edit. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015.
- [3] R. Dixit and K. Ravindranath, "Encryption techniques & access control models for data security: A survey," *International Journal of Engineering & Technology*, vol. 7, no. 1.5, pp. 107–110, Dec. 2017, doi: 10.14419/ijet.v7i1.5.9130.
- [4] B. Schneier, *Applied cryptography*, 20th Anniv. Indianapolis: John Wiley & Sons, Inc, 2015.
- [5] W. Stallings, *Cryptography and network security: Principles and practice*, Seventh Ed. Harlow: Pearson Education Limited, 2017.
- [6] C. Paar and J. Pelzl, *Understanding cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.





- [7] M. B. Pramanik, "Implementation of cryptography technique using columnar transposition," *International Journal of Computer Applications*, pp. 19–23, 2014.
- [8] B. Bjorkman and R. Talbert, "Fixed points of columnar transpositions," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 18, no. 5, pp. 541–557, Sep. 2015, doi: 10.1080/09720529.2014.986910.
- [9] S. Majumdar, A. Maiti, B. Bhattacharyya, and A. Nath, "A new bit-level columnar transposition encryption algorithm," *International Journal of Advance Research in Computer Science and Management Studies*, vol. 3, no. 7, pp. 176–184, 2015.
- [10] N. Sinha and K. Bhamidipati, "Improving security of Vigenère cipher by double columnar transposition," *International Journal of Computer Applications*, vol. 100, no. 14, pp. 6–10, Aug. 2014, doi: 10.5120/17591-8290.
- [11] M. Annalakshmi and A. Padmapriya, "Zigzag ciphers : A novel transposition method," in *International Conference on Computing and Information Technology (IC2IT-2013)*, 2013, pp. 8–12.
- [12] O. P. Baghel, "Combination of transposition and alpha-numeric vigenere table for secure communication," *Journal of Network Communications and Emerging Technologies*, vol. 7, no. 4, pp. 15–17, 2017.
- [13] A. Rizal, D. Susilo Budi Utomo, R. Rihartanto, and A. Susanto, "Encryption of RGB image using hybrid transposition," in *Proceedings of the 1st International Conference on Life, Innovation, Change and Knowledge (ICLICK 2018)*, 2019, vol. 203, pp. 57–61, doi: 10.2991/iclick-18.2019.13.
- [14] A. Jawahir and H. Haviluddin, "An audio encryption using transposition method," *International Journal of Advances in Intelligent Informatics*, vol. 1, no. 2, pp. 98–106, Jul. 2015, doi: 10.26555/ijain.v1i2.24.
- [15] J. A. Dar, "Humanizing the security of rail fence cipher using double transposition and substitution techniques," *International Journal of Science and Research (IJSR)*, vol. 3, no. 9, pp. 1787–1791, 2014.
- [16] A. Priyam, "Extended Vigenère using double transposition cipher with one time pad cipher," *International Journal of Engineering, Sciences and Advanced Research*, vol. 1, no. 2, pp. 62–65, 2015.
- [17] H. V. Gamido, "Implementation of a bit permutation-based advanced encryption standard for securing text and image files," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 3, pp. 1596–1601, Sep. 2020, doi: 10.11591/ijeecs.v19.i3.pp1596-1601.
- [18] R. Rihartanto, S. Supriadi, and D. S. Budi Utomo, "Image tiling using columnar transposition," in *2018 International Conference on Applied Information Technology and Innovation (ICAITI)*, Sep. 2018, pp. 118–123, doi: 10.1109/ICAITI.2018.8686758.
- [19] X. Feng, X. Tian, and S. Xia, "A novel image encryption algorithm based on fractional Fourier transform and magic cube rotation," in *2011 4th International Congress on Image and Signal Processing*, Oct. 2011, vol. 2, no. 5, pp. 1008–1011, doi: 10.1109/CISP.2011.6100319.
- [20] X. Feng, X. Tian, and S. Xia, "An improved image scrambling algorithm based on magic cube rotation and chaotic sequences," in *2011 4th International Congress on Image and Signal Processing*, Oct. 2011, vol. 2, pp. 1021–1024, doi: 10.1109/CISP.2011.6100274.
- [21] L. Zhang, X. Tian, and S. Xia, "A scrambling algorithm of image encryption based on rubik's cube rotation and logistic sequence," in *2011 International Conference on Multimedia and Signal Processing*, May 2011, vol. 1, pp. 312–315, doi: 10.1109/CMSP.2011.69.
- [22] K. Loukhaoukha, J. Chouinard, and A. Berdai, "A secure image encryption algorithm based on rubik's cube principle," *Journal of Electrical and Computer Engineering*, vol. 2012, pp. 1–13, 2012, doi: 10.1155/2012/173931.
- [23] P. Praveenkum *et al.*, "Rubik's cube blend with logistic map on RGB: A way for image encryption," *Research Journal of Information Technology*, vol. 6, no. 3, pp. 207–215, Mar. 2014, doi: 10.3923/rjit.2014.207.215.
- [24] F. Twum, J. B., and M.-D. William, "A proposed enhanced transposition cipher algorithm based on rubik's cube transformations," *International Journal of Computer Applications*, vol. 182, no. 35, pp. 18–26, Jan. 2019, doi: 10.5120/ijca2019918323.
- [25] D. Rajavel and S. P. Shantharajah, "Cubical key generation and encryption algorithm based on hybrid cube's rotation," in *International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME-2012)*, Mar. 2012, pp. 183–187, doi: 10.1109/ICPRIME.2012.6208340.
- [26] R. Rihartanto, R. K. Ningsih, A. F. O. Gaffar, and D. S. B. Utomo, "Implementation of vigenere cipher 128 and square rotation in securing text messages," *Jurnal Teknologi dan Sistem Komputer*, vol. 8, no. 3, pp. 201–209, Jul. 2020, doi: 10.14710/jtsiskom.2020.13476.
- [27] H. Noura, L. Sleem, M. Noura, M. M. Mansour, A. Chehab, and R. Couturier, "A new efficient lightweight and secure image cipher scheme," *Multimedia Tools and Applications*, vol. 77, no. 12, pp. 15457–15484, 2018, doi: 10.1007/s11042-017-5124-9.
- [28] S. D. Mohammed and T. M. Hasan, "Cryptosystems using an improving hiding technique based on Latin square and magic square," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 20, no. 1, pp. 510–520, Oct. 2020, doi: 10.11591/ijeecs.v20.i1.pp510-520.
- [29] J. N. B. Salameh, "A new symmetric-key block ciphering algorithm," *Middle East Journal of Scientific Research*, vol. 12, no. 5, pp. 662–673, 2012, doi: 10.5829/idosi.mejsr.2012.12.5.1685.

BIOGRAPHIES OF AUTHORS







Rihartanto     received the B.Sc. degree in computer engineering from Institute of Science and Technology "Akprind" Yogyakarta in 1996 and the M.Sc. degree in environmental science from Mulawarman University, Samarinda, Indonesia, in 2017. Currently, he is a lecturer at Department of Information Technology, State Polytechnic of Samarinda, Samarinda, Indonesia. His research interests are in the areas of information security, data compression and image processing. He can be contacted at rihart.c@gmail.com.







Didi Susilo Budi Utomo     get his diploma degree in power electronics from LuccasNule. GmbH in 1996, B.Sc. degree in electrical engineering from the Islamic University of Malang, in 1999 and M.Sc. degree in electrical engineering System design and technology from Fachhochschule Darmstadt Germany, in 2003. Currently, he is a lecturer at the Department of Information Technology, State Polytechnic of Samarinda, Samarinda, Indonesia. His research interests are in computer control and green energy. He can be contacted at dsbudiutomo10@gmail.com.







Herny Februariyanti     received the B.Sc. degree in Management of Informatics and Computer Engineering from Institute of Science and Technology “Akprind” Yogyakarta in 1998 and the M.Sc. degree in Computer Science from Gadjah Mada University, Yogyakarta, Indonesia, in 2010. Currently, she is a lecturer at Faculty of Information Technology, Stikubank University, Semarang, Indonesia. Her research interests are in the areas of information retrieval and information security. She can be contacted at email: hernyfeb@edu.unisbank.ac.id.



Arief Susanto     received the B.Sc. degree in Management of Informatics and Computer Engineering from Institute of Science and Technology “Akprind” Yogyakarta in 1997 and the M.Sc. degree in Computer Science from STTI Benarif, Jakarta, Indonesia, in 2001. Currently, he is a lecturer at Faculty of Engineering, Muria Kudus University, Kudus, Indonesia. His research interests are in the areas of information systems and SCADA. He can be contacted at ariefpjl@gmail.com.



Wardatul Khafidhah     is a B.Sc. student at State Polytechnic of Samarinda. Her bachelor thesis is in the area of data security using certain transposition algorithm. She graduated in 2020 and can be contacted at wardatul.khafidhah@gmail.com.