Bit-based cube rotation for text encryption

by Rihartanto Rihartanto

Bit-based cube rotation for text encryption

Rihartanto[1], Didi Susilo Budi Utomo[2], Wardah Khafidhah[3], Herny Februariyanti[4], Arief Susanto[5]
[1, 2, 3]Department of Information Technology, State Polytechnic of Samarinda, Samarinda, Indonesia
[4]Faculty of Information Technology, Stikubank University, Semarang, Indonesia
[5]Faculty of Engineering, Muria Kudus University, Kudus, Indonesia

Article Info

Article history:

Received month dd, yyyy
Revised month dd, yyyy
Accepted month dd, yyyy

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. Among them is using 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.

Corresponding Author:

Rihartanto
Department of Information Technology, State Polytechnic of Samarinda
Jl. Cipto Mangunkusumo, Kampus Gunung Lipan, Samarinda 75131, Indonesia
Email: rihart.c@gmail.com

1. INTRODUCTION (10 PT)

Information is an important commodity for government, private organizations, universities, NGOs, and even individuals. 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. The widespread 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 in the efforts in securing information. Meanwhile, the type of information that can be secured is not only in the form of text but also in 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, the encryption and the decryption process. Both processes usually require a keyword, where the keyword can be symmetrical or asymmetrical [3] depending on the cryptographic technique that is 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. This 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 the statistical properties of the plaintext. A simple diffusion element is the bit permutation, which is used frequently within 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], [11], Myszkowski transposition[12] and zigzag transposition[13]. This technique can be used either for text[7], [8], [14], image[15] or audio encryption[16]. In a number of studies, transposition and permutation is also used to optimize other encryption algorithms such as Rail-fence cipher[17], Vigenere cipher[10], [11], [14], Playfair cipher[12] and AES[18]. Another study uses transposition for image processing[19].

In three-dimensional space, transposition is carried out using a cube shape [20], [21] imitating the Rubik's cube principle[22]–[24]. 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[20], [21], [25] and the second by considering the cube as a 3D array[26].

In this study, the transposition is carried out in the form of bit-based cube rotation. Each cube element contains a single bit. The cube is an array of 8×8×8, 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 [27]. 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. As 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.

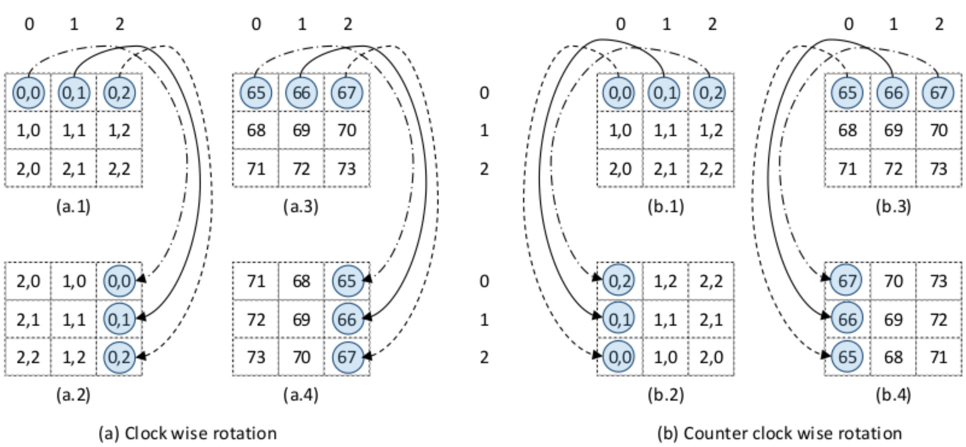

Figure 1. Square rotation

In Figure 1, (a.1) and (b.1) shows 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, that 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 Equation (1) and Equation (2) for CCW rotation [27]. S is the array before rotation while S' is 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 Equation (1), the element of S'[1,2] is taken from S[0,1] which is obtained from [3-2-1, 1]. Similarly, using Equation (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 in 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 3. The rotation on the x-axis is called the roll, the rotation on the y-axis is called pitch, and the rotation on the z-axis is called yaw.

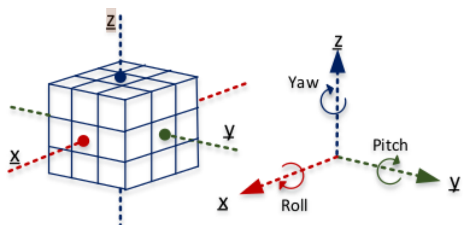

Figure 2. Cube and its rotation

The mathematical notation for cube rotation was written as Equations (3), (4), (5), (6), (7), and (8). xCW and xCCW represent roll, yCW and yCCW represent pitch, while zCW and zCCW represent yaw.

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

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

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

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

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

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

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 3x3x3 cubes[20], [21], [25]. Each element of the array will be filled with bit 0 or bit 1. 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 were starting 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 equations (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 where displacement is performed for each array element according to its respective index.

Algorithm 1: Roll, rotation on x-axis

Input: cube
Output: cube

```
Function xCW(cube_in)
 n ← side of the cube
  for k ← 0 to n-1
   for i ← 0 to n-1
    for j ← 0 to n-1
     cube_out[i,j,k] ← cube_in[n-j-1,i, k]
    end for
   end for
  end for
 return cube_out

Function xCCW(cube_in)
 n ← side of the cube
  for k ← 0 to n-1
   for i ← 0 to n-1
    for j ← 0 to n-1
     cube_out[i,j,k] ← cube_in[j,n-i-1, k]
    end for
   end for
  end for
 return cube_out
```

Algorithm 2: Pitch, rotation on y-axis

Input: cube
Output: cube

```
Function yCW(cube_in)
 n ← side of the cube
  for j ← 0 to n-1
   for i ← 0 to n-1
    for k ← 0 to n-1
     cube_out[i,j,k] ← cube_in[n-k-1,j,i]
    end for
   end for
  end for
 return cube_out

Function yCCW(cube_in)
 n ← side of the cube
  for j ← 0 to n-1
   for i ← 0 to n-1
    for k ← 0 to n-1
     cube_out[i,j,k] ← cube_in[k,j,n-i-1]
    end for
   end for
  end for
 return cube_out
```

3. RESULTS AND DISCUSSION

Performance measurement of the encryption results using bit-based cube rotation is performed using Avalance Effect (AE) and correlation coefficient. Avalanche Effect 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 Equation (9). AE is said to be good if the bit change that occurs is greater than 45% [28] and very good if it is greater than 50%[29], [30]. The more bits that change, indicating that the encryption algorithm is increasingly difficult to crack.

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

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.

The four different texts used for the bit-based cube rotation test are shown in Table 1. Each text contains 64 characters to fill in the cube. Each text 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.

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 90º counterclockwise on the x-axis (roll) and followed by a displacement of 90º 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.

Table 1. The plaintexts

Textfile	Content
text1.txt	Coronavirus disease is an infectious disease caused by COVID-19.
text2.txt	river side city river side city river side city river side city.
text3.txt	0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmno
text4.txt	UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU

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.

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

Axes	Ciphertext
X	Ã¿Ã¾DÂšZ_Â«Ã·Ã¿G Â'EÃ¦Â·Ã¿""Â·Ã½Ã¿Â€ Â¹YdÃ¯Ã¿ÂŒC&ÂŠÃ□Ã¯Ã¿Â„Â‰$Ã¯Â·□! Â'Â£Ã°bÃ•Ã›Âƒu
Y	ieatsuC.vs cia 9aisedcy1ndif b-o nse DrseiusdIous oaeVCraniesO
Z	Â¯Ã®}ÂŒ!Ã·]Ã®Ã"Â©Ã„Â˜Â'$Ã• Ã‹*Â•Ã'Â€UÂˆÂ□Â¡B Â□BaÃŒ#Ã□~Ã¾Ã¾Ã¾Ã¿Ã¿Ã¿Ã½Ã¿Ã¯Ã¿Â□Ã²Ã¾ÃœÃ¾
xy	Â«Ã¦Â·dÃ• Ã¯Â£u_E"YÂŠ$Â'ÂƒZÂ'Â¹&Â‰Â›Âš C Ã•DG"Â€ÂŒÂ„!bÃ¾Ã¿Ã¿Ã¿Ã¿Ã¿• Ã°Ã¿Ã·Â·Ã½Ã¯ Ã¯ Â·
xz	Ã¿~BÃ"Â¯Ã¯Ã¾aÂˆÃ‹Â©Ã®Ã¿Ã¾ÃŒ*Ã„}Â□Ã¾Â□Â•Â˜ÂŒÃ²Ã¿Â¡Ã'Â'!Ã¾Ã¿#B$Ã·ÃœÃ¿Ã□ Â€Ã•]Ã¾Ã½Â• U Ã®
yx	□Â¿8Â□ÂªÃ□w;Ã¿ÂƒÂ□ Âº□Ã¿Ã„B$Ã¯OÃ¿Â…Â‹IÂ„Â¹□Â©1Ã¿□3ÂˆT#Â¾Ã·□Â†Ã"Â•wÃ¿~BÂ˜Â¨Ã‹Âµ
yz	Â«Ã¦Â·dÃ□Ã¯Â£u_E"YÂŠ$Â'ÂƒZÂ'Â¹&Â‰Â›Âš C Ã•DG"Â€ÂŒÂ„!bÃ¾Ã¿Ã¿Ã¿Ã¿Ã¿• Ã°Ã¿Ã·Â·Ã½Ã¯ Ã¯ Â·
zx	Â«Ã¦Â·dÃ□Ã¯Â£u_E"YÂŠ$Â'ÂƒZÂ'Â¹&Â‰Â›Âš C Ã•DG"Â€ÂŒÂ„!bÃ¾Ã¿Ã¿Ã¿Ã¿Ã¿• Ã°Ã¿Ã·Â·Ã½Ã¯ Ã¯ Â·
zy	Ã® UÂ□Ã½Ã¾]Ã□Â€ Ã□Ã¿ÃœÃ·$B#Ã¿Ã¾!Â'Ã'Â¡Ã¿Ã²ÂŒÂ˜Â•Â□Ã¾Â□}Ã„*ÃŒÃ¾Ã¿Ã®Â©Ã‹ÂˆaÃ¾Ã¯Â¯Ã"B~Ã¿
xyz	Ã‚NÂ†vÂ–Â¦ÃŽÃ²Ã¶Â®ÃŽÃ¶Â†Â¦jNÃŽÂ¦Â–Â®ÃŽ&Â'Ã¶vÃŽÂ¦"v&Â–fFÂ´Â†Â– ÃŽÂ¦&Ã†ÂžÂŒnÃŽÃ†Â–Â†ÂœÂ–Â¦Â†.ÃŽÂ®Ã‚t
xzy	Â¯Ã®}ÂŒ!Ã·]Ã®Ã"Â©Ã„Â˜Â'$Ã• Ã‹*Â•Ã'Â€UÂˆÂ□Â¡B Â□BaÃŒ#Ã□~Ã¾Ã¾Ã¾Ã¿Ã¿Ã¿Ã½Ã¿Ã¯Ã¿Â□Ã²Ã¾ÃœÃ¾
yxz	Ã¿Ã¾DÂšZ_Â«Ã·Ã¿G Â'EÃ¦Â·Ã¿""Â·Ã½Ã¿Â€ Â¹YdÃ¯Ã¿ÂŒC&ÂŠÃ• Ã¯ Ã¿Â„Â‰$Ã¯Â·□! Â'Â£Ã°bÃ•Â›Âƒu
yzx	wÂºÃ¯Â„1Â¾wÃµÃ• $I#Â•Ã‹ÂªÂ‹Â©TÃ"Â¨Â□Â□BÂ… ÂˆÂ˜8ÂƒÃ„3Â†BÂ¿Ã¿Ã¿Ã¿□□□~□;□OÂ¹Ã¿Ã·Ã¿
zxy	uÂƒÂ›Ã•bÃ°Â£Â' !□Â·Ã¯$Â‰Â„Ã¿Ã¯Ã□ÂŠ&CÂŒÃ¿Ã¯dYÂ¹ Â€Ã¿Ã½Â·""Ã¿Â·Ã¦EÂ' GÃ¿Ã·Â«_ZÂšDÃ¾Ã¿
zyx	ieatsuC.vs cia 9aisedcy1ndif b-o nse DrseiusdIous oaeVCraniesO

The test results for each test data are shown in Table 3 and Table 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. While the graph in Fig. 4 shows the difference in AE value and their correlation coefficient for each data when using different rotations.

Ciphertexts in Table 2 obtained from one CW rotation on one or more axes give 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 the scale stated in [28] and many of those values above 50% are relevant to previous studies [18],[29], [30]. 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 axis that results in an AE below 45%. The low AE value is because 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 ciphertexts shows the characteristics of the original text.

Table 3. The avalanche effect

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 3. 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 confusing process. This result is supported by a correlation coefficient that is close to zero which indicates no relationship between plaintext and ciphertext. What has considered the encryption key in this study is the direction and axis of rotation. In contrast to other studies where other algorithms[20]–[22], [24] 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 implementing 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.

4. CONCLUSION

This study shows that bit-based cube rotation successfully fulfills two cryptographic properties, it is confusion and diffusion. Bit-based cube rotation which is a diffusion process can 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 can 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 rotating a number of rows, columns, or layers before rotating the cube.

ACKNOWLEDGEMENTS

The authors would like to thank DPRM Ministry of Research, Technology, and Higher Education 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," *Int. J. Comput. Sci. Softw. Eng.*, vol. 6, no. 2, pp. 41–46, 2017.
[2] H. Delfs and H. Knenbl, *Introduction to Cryptography: Principles and Application*, Third Edit. Berlin: Springer-Verlag GmbH, 2015.
[3] R. Dixit and K. Ravindranath, "Encryption techniques & access control models for data security : A survey," *Int. J. Eng. Technol.*, vol. 7, no. 1.5, pp. 107–110, 2018.
[4] B. Schneier, *Applied Crypthography*, 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: Springer-Verlag, 2010.
[7] M. B. Pramanik, "Implementation of Cryptography Technique using Columnar Transposition," *Int. J. Comput. Appl.*, pp. 19–23, 2014.
[8] B. Bjorkman and R. Talbert, "Fixed Points of Columnar Transpositions," *J. Discret. Math. Sci. Cryptogr.*, vol. 18, no. 5, pp. 541–557, 2015.
[9] S. Majumdar, A. Maiti, B. Bhattacharyya, and A. Nath, "A New Bit-level Columnar Transposition Encryption Algorithm," *Int. J. Adv. Res. Comput. Sci. Manag. Stud.*, vol. 3, no. 7, pp. 176–184, 2015.
[10] N. Sinha and K. Bhamidipati, "Improving Security of Vigenère Cipher by Double Columnar Transposition," *Int. J. Comput. Appl.*, vol. 100, no. 14, pp. 6–10, 2014.
[11] A. Priyam, "Extended Vigenère using double Transposition Cipher with One Time Pad Cipher," *Int. J. Eng. Sci. Adv. Reaserch*, vol. 1, no. 2, pp. 62–65, 2015.
[12] A. Bhowmick, A. V. Lal, and N. Ranjan, "Enhanced 6x6 Playfair Cipher using Double Myszkowski Transposition," *Int. J. Eng. Res. Technol.*, vol. 4, no. 07, pp. 1100–1104, 2015.
[13] 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.
[14] O. P. Baghel, "Combination of Transposition and Alpha-Numeric Vigenere Table for Secure Communication," *J. Netw. Commun. Emerg. Technol.*, vol. 7, no. 4, pp. 15–17, 2017.
[15] A. Rizal, D. Susilo Budi Utomo, R. Rihartanto, and A. Susanto, "Encryption of RGB Image Using Hybrid Transposition," in *Advances in Social Science, Education and Humanities Research*, 2019, vol. 203, no. ICLICK 2018, pp. 57–61.
[16] A. Jawahir and H. Haviluddin, "An Audio Encryption Using Transposition Method," *Int. J. Adv. Intell. Informatics*, vol. 1, no. 2, July 2015, pp. 98–106, 2015.

[17] J. A. Dar, "Humanizing the Security of Rail Fence Cipher Using Double Transposition and Substitution Techniques," *Int. J. Sci. Res.*, vol. 3, no. 9, pp. 1787–1791, 2014.

[18] H. V. Gamido, "Implementation of a bit permutation-based advanced encryption standard for securing text and image files," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 19, no. 3, pp. 1596–1601, 2020.

[19] R. Rihartanto, S. Supriadi, and D. S. B. Utomo, "Image Tiling Using Columnar Transposition," in *2018 International Conference on Applied Information Technology and Innovation (ICAITI)*, 2018, pp. 118–123.

[20] X. Feng, X. Tian, and S. Xia, "A novel image encryption algorithm based on fractional Fourier transform and magic cube rotation," *Proc. - 4th Int. Congr. Image Signal Process. CISP 2011*, vol. 2, no. 5, pp. 1008–1011, 2011.

[21] X. Feng, X. Tian, and S. Xia, "An improved image scrambling algorithm based on magic cube rotation and chaotic sequences," *Proc. - 4th Int. Congr. Image Signal Process. CISP 2011*, vol. 2, pp. 1021–1024, 2011.

[22] L. Zhang, X. TiaN, and S. Xia, "Scrambling algorithm of image encryption based on Rubik's cube rotation and logistic sequence," *Proc. - 2011 Int. Conf. Multimed. Signal Process. C. 2011*, vol. 1, pp. 312–315, 2011.

[23] K. Loukhaoukha, J. Chouinard, and A. Berdai, "A Secure Image Encryption Algorithm Based on Rubik ' s Cube Principle," *J. Electr. Comput. Eng.*, vol. 2012, 2012.

[24] P. Praveenkumar *et al.*, "Rubik's Cube Blend with Logistic Map on RGB: A Way for Image Encryption," *Reasearch J. Inf. Technol.*, vol. 6, no. 3, pp. 207–215, 2557.

[25] F. Twum, J. B., and M.-D. William, "A Proposed Enhanced Transposition Cipher Algorithm based on Rubik's Cube Transformations," *Int. J. Comput. Appl.*, vol. 182, no. 35, pp. 18–26, 2019.

[26] D. Rajavel and S. P. Shantharajah, "Cubical key generation and encryption algorithm based on hybrid cube's rotation," *Int. Conf. Pattern Recognition, Informatics Med. Eng. PRIME 2012*, pp. 183–187, 2012.

[27] 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," *J. Teknol. dan Sist. Komput.*, vol. 8, no. 3, pp. 201–209, 2020.

[28] H. Noura, L. Sleem, M. Noura, M. M. Mansour, A. Chehab, and R. Couturier, "A new efficient lightweight and secure image cipher scheme," *Multimed. Tools Appl.*, vol. 77, no. 12, pp. 15457–15484, 2018.

[29] S. D. Mohammed and T. M. Hasan, "Cryptosystems using an improving hiding technique based on latin square and magic square," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 20, no. 1, pp. 510–520, 2020.

[30] J. N. B. Salameh, "A new symmetric-key block ciphering algorithm," *Middle East J. Sci. Res.*, vol. 12, no. 5, pp. 662–673, 2012.

BIOGRAPHIES OF AUTHORS

Rihartanto received the B.Sc degree in computer engineering from Institute of Science and Technolgy "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 email rihart.c@gmail.com.

Didi Susilo Budiutomo 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 Fachhochscule 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 email dsbudiutomo10@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 email: wardatul.khafidhah@gmail.com.

Herny Februariyanti received the B.Sc degree in Management of Informatics and Computer Engineering from Institute of Science and Technolgy "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 Technolgy "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 Fakulty of Engineering, Muria Kudus University, Kudus, Indonesia. His research interests are in the areas of information system and SCADA. He can be contacted at email ariefpjl@gmail.com.

Bit-based cube rotation for text encryption

ORIGINALITY REPORT

12%	9%	9%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Wollongong Student Paper	2%
2	cs.uok.edu.in Internet Source	1%
3	ijece.iaescore.com Internet Source	1%
4	www.cs.rochester.edu Internet Source	1%
5	Reza N. Jazar. "Vehicle Dynamics", Springer Science and Business Media LLC, 2017 Publication	1%
6	Soundous Zougari, Mariam Tanana, Abdelouahid Lyhyaoui. "Validity of a graph-based automatic assessment system for programming assignments: human versus automatic grading", International Journal of Electrical and Computer Engineering (IJECE), 2022 Publication	1%

7	CH Karthik, Pramod Sreedharan. "Design and Development of Pipe-inspection robot with vision 360°", Journal of Physics: Conference Series, 2021 Publication	1 %
8	cloud.tencent.com Internet Source	<1 %
9	kupdf.net Internet Source	<1 %
10	www.di.unito.it Internet Source	<1 %
11	M.B. Tahoori, J. Huang, M. Momenzadeh, F. Lombardi. "Testing of Quantum Cellular Automata", IEEE Transactions On Nanotechnology, 2004 Publication	<1 %
12	Submitted to American Public University System Student Paper	<1 %
13	Submitted to Entregado a Universiti Teknologi Petronas el 2012-08-15 Student Paper	<1 %
14	Madhava Prabhu S., Seema Verma. "Automatic segmentation of plantar thermograms using adaptive C means	<1 %

	technique", International Journal of Electrical and Computer Engineering (IJECE), 2021 Publication	
15	Submitted to Jawaharlal Nehru Technological University Student Paper	<1 %
16	Submitted to Universiti Teknologi Malaysia Student Paper	<1 %
17	beei.org Internet Source	<1 %
18	en.wikipedia.org Internet Source	<1 %
19	mdpi-res.com Internet Source	<1 %
20	www.mdpi.com Internet Source	<1 %
21	www.ijrte.org Internet Source	<1 %
22	www.pdf-archive.com Internet Source	<1 %
23	Rihartanto Rihartanto, Supriadi Supriadi, Didi Susilo Budi Utomo. "Image Tiling Using Columnar Transposition", 2018 International Conference on Applied Information Technology and Innovation (ICAITI), 2018 Publication	<1 %

24	journal.ugm.ac.id Internet Source	<1 %
25	"Contributors", IEEE Transactions on Information Theory, 3/2002 Publication	<1 %
26	Yasser H. Khalil, Hussein T. Mouftah. "LiCaNet: Further Enhancement of Joint Perception and Motion Prediction Based on Multi-Modal Fusion", IEEE Open Journal of Intelligent Transportation Systems, 2022 Publication	<1 %
27	projects.iq.harvard.edu Internet Source	<1 %
28	Muhammad Fadlan, Haryansyah, Rosmini. "Three Layer Encryption Protocol: an Approach of Super Encryption Algorithm", 2021 3rd International Conference on Cybernetics and Intelligent System (ICORIS), 2021 Publication	<1 %
29	Arief Susanto, Tutik Khotimah, Muhammad Taufik Sumadi, Joko Warsito, Rihartanto .. "Image encryption using vigenere cipher with bit circular shift", International Journal of Engineering & Technology, 2018 Publication	<1 %

30	Bjorkman, Beth, and Robert Talbert. "Fixed Points of Columnar Transpositions", Journal of Discrete Mathematical Sciences and Cryptography, 2015. Publication	<1 %
31	"International Conference on Intelligent Computing and Smart Communication 2019", Springer Science and Business Media LLC, 2020 Publication	<1 %
32	Achmad Fanany Onnilita Gaffar, Rheo Malani, Arief Bramanto Wicaksono Putra. "Magic cube puzzle approach for image encryption", International Journal of Advances in Intelligent Informatics, 2020 Publication	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		