Advances in Social Science, Education and Humanities Research, volume 203
International Conference on Life, Innovation, Change, and Knowledge (ICLICK 2018)

Encryption of RGB Image Using Hybrid Transposition

Ansar Rizal[1]
Politeknik Negeri Samarinda
Department of Information Technology
Samarinda, Indonesia
anrisal@yahoo.com

Rihartanto[3]
Politeknik Negeri Samarinda
Department of Information Technology
Samarinda, Indonesia
rihart.c@gmail.com

Didi Susilo Budi Utomo[2]
Politeknik Negeri Samarinda
Department of Information Technology
Samarinda, Indonesia
dsbudiutomo10@gmail.com

Arief Susanto[4]
Universitas Muria Kudus
Faculty of Engineering
Kudus, Indonesia
ariefpjl@gmail.com

***Abstract*—Nowadays digital imagery is used for many purposes. Starting just as a hobby of photography up to the purpose of security or identification. For more sensitive purposes, an image needs to be encrypted so that the image is not recognized by an unauthorized person. In this study, hybrid transposition is used to encrypt and decrypt RGB images. The hybrid transposition here involves the process of randomization and repositioning of pixels before transposition is made. The performance of the encryption is measured by the correlation coefficient where the good result is indicated by the correlation coefficient value close to 0 (zero). The smallest coefficient values obtained are -0.0227 for test images in the form of chessboard pieces that have almost the same black and white areas. The decryption process produces the exact same image as the original image, this is indicated by the MAE value equal to 0 (zero) and the correlation coefficient equal to 1.0.**

Keywords*—*Hybrid transposition, pixel reposition, random number, RGB image.

I. INTRODUCTION

RGB Image is a digital image where each pixel has three color components[1]. These three components are red (R), green (G) and blue (B). Unlike the grayscale image that which is an array of dimensions n * m, the RGB image is an array of dimension $n * m * 3$ where n is the number of rows and m is the number of columns, and *3* indicates the number of the layer or the color components. Each layer of a pixel has its own intensity value. The color intensity is an integer value from 0 to 255, where 0 represents black (the darkest) and 255 represents white (the lightest). Fig. 1 shows the intensities of each color component which form a colored image.

Images that are visually recognized by humans in the form of pictures or photographs or other, are recognized by computers as a collection of values represented in the form of arrays or matrices. Fig. 2 shows some of the intensity values for each RGB color component of an image. This intensity value can be further processed or manipulated for a more specific purpose.

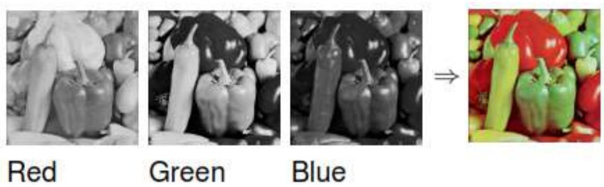


Fig. 1. The color components of an RGB image

In today's digital world, imagery is used for many purposes. Start from just showing photos up for security or identification purposes. QR code is one example of an image used for identification purposes. Sometimes the image also needs to be kept secret for security purposes. The method used for data security is encryption. Encryption techniques or also known as a cipher, can be grouped according to various approaches. For example, according to the key type the encryption is differentiated into encryption with symmetric keys and asymmetric keys. According to the way data handling is grouped into stream cipher and block cipher. It is also grouped into classic cryptography and modern cryptography, and many others.

Transposition is one of the classic cryptography typically used to encrypt text. In contrast to the substitution technique, the transposition simply changes the position of each letter in the text to produce a new arrangement that is different from the original[2]. So it can be said that the ciphertext of the transposition is a permutation[3] of the plaintext. The widely used transposition techniques for text encryption include rail fence [3], route transposition[4], columnar transposition[4], double transposition [5], [6] and Myszkowsky transposition[7].

Copyright © 2019, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

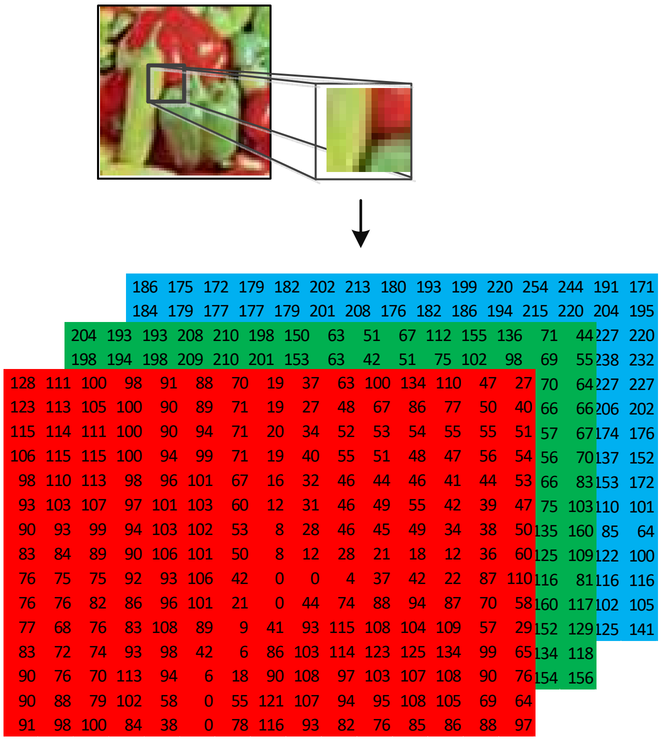


Fig. 2. The intensity values of each component of an RGB image

In this research, transposition technique is implemented to encrypt RGB image. The transposition used is the transposition operation of the matrix in general. To improve the performance of this simple transposition, also applied the use of random numbers to improve the randomness of encryption.

II. METHOD AND MATERIAL

In this section we will describe the method of generating random numbers, repositioning pixels and transpositions used as stages in RGB image encryption. Random numbers are generated based on the seeds obtained from the key values given for encryption. Seed is calculated by summing the power of each ASCII value of each character multiplied by its position. Suppose the given key is "ab12". The ASCII values for each character in the keys are 97, 98, 49 and 50 respectively. Then the seed value derived from the key is ((97 ^ 2) * 1) + ... + ((50 ^ 2) * 4) which is 45820. The determination of a seed like this aims to obtain a different seed value if the given key has the same character but has a different sequence. So "12ab" will generate value 74044 and "a1b2" generate value 53023.

Then random numbers are generated as many as the number of columns and the number of image rows. If an image has 100 columns, then the generated value is from 0 to 99 without repetition. The purpose of using random numbers is to randomize the positions of columns and rows. Suppose the array of components R in Fig. 2 which consists of 15 columns and 15 rows, using 45820 as seeds obtained random sequences from 0 to 14 in order of [1, 9, 11, 3, 5, 6, 8, 10, 0, 7, 14, 13, 4, 12, 2] for the columns and [8, 6, 1, 13, 3, 11, 0, 2, 12, 10, 7, 5, 4, 9, 14] for rows.

After obtaining random sequences for columns and rows, then columns and rows reposition are conducted. Repositioning is the process of re-ordering each column and row of the initial matrix in the order of the generated random number generations. The column repositioning is conducted on each column of the three components while the line repositioning is conducted on components G and B only. The repositioning of columns using random sequences obtained in the previous stage is illustrated in Fig. 3.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
128	111	100	98	91	88	70	19	37	63	100	134	110	47	27
123	113	105	100	90	89	71	19	27	48	67	86	77	50	40
115	114	111	100	90	94	71	20	34	52	53	54	55	55	51
106	115	115	100	94	99	71	19	40	55	51	48	47	56	54
98	110	113	98	96	101	67	16	32	46	44	46	41	44	53
93	103	107	97	101	103	60	12	31	46	49	55	42	39	47
90	93	99	94	103	102	53	8	28	46	45	49	34	38	50
83	84	89	90	106	101	50	8	12	28	21	18	12	36	60
76	75	75	92	93	106	42	0	0	4	37	42	22	87	110
76	76	82	86	96	101	21	0	44	74	88	94	87	70	58
77	68	76	83	108	89	9	41	93	115	108	104	109	57	29
83	72	74	93	98	42	6	86	103	114	123	125	134	99	65
90	76	70	113	94	6	18	90	108	97	103	107	108	90	76
90	88	79	102	58	0	55	121	107	94	95	108	105	69	64
91	98	100	84	38	0	78	116	93	82	76	85	86	88	97

1	9	11	3	5	6	8	10	0	7	14	13	4	12	2
111	63	134	98	88	70	37	100	128	19	27	47	91	110	100
113	48	86	100	89	71	27	67	123	19	40	50	90	77	105
114	52	54	100	94	71	34	53	115	20	51	55	90	55	111
115	55	48	100	99	71	40	51	106	19	54	56	94	47	115
110	46	46	98	101	67	32	44	98	16	53	44	96	41	113
103	46	55	97	103	60	31	49	93	12	47	39	101	42	107
93	46	49	94	102	53	28	45	90	8	50	38	103	34	99
84	28	18	90	101	50	12	21	83	8	60	36	106	12	89
75	4	42	92	106	42	0	37	76	0	110	87	93	22	75
76	74	94	86	101	21	44	88	76	0	58	70	96	87	82
68	115	104	83	89	9	93	108	77	41	29	57	108	109	76
72	114	125	93	42	6	103	123	83	86	65	99	98	134	74
76	97	107	113	6	18	108	103	90	90	76	90	94	108	70
88	94	108	102	0	55	107	95	90	121	64	69	58	105	79
98	82	85	84	0	78	93	76	91	116	97	88	38	86	100

Fig. 3. Column reposition of R component

In matrix operations, transposition is the displacement of the element's position from row to column and vice versa. Each element *a(i, j)* will switch its position to *a(j, i)*. All elements of the matrix will swap its position except for the elements in the diagonal position. This operation will also change the size of the matrix if the number of rows is not equal to the number of columns, That is, the matrix of size *n x m* will be an *m x n* sized matrix after transposition. Fig. 4 illustrates the transposition of a 4 x 3 matrix. It can be said that this transposition operation is a reflection operation on the diagonal axis.

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \\ j & k & l \end{bmatrix} \rightarrow \begin{bmatrix} a & d & g & j \\ b & e & h & k \\ c & f & i & l \end{bmatrix}$$

Fig. 4. Transposition of a 4 x 3 matrix

The result of the transposition of the repositioned matrix in Fig. 3 is shown in Fig. 5.

111	63	134	98	88	70	37	100	128	19	27	47	91	110	100
113	48	86	100	89	71	27	67	123	19	40	50	90	77	105
114	52	54	100	94	71	34	53	115	20	51	55	90	55	111
115	55	48	100	99	71	40	51	106	19	54	56	94	47	115
110	46	46	98	101	67	32	44	98	16	53	44	96	41	113
103	46	55	97	103	60	31	49	93	12	47	39	101	42	107
93	46	49	94	102	53	28	45	90	8	50	38	103	34	99
84	28	18	90	101	50	12	21	83	8	60	36	106	12	89
75	4	42	92	106	42	0	37	76	0	110	87	93	22	75
76	74	94	86	101	21	44	88	76	0	58	70	96	87	82
68	115	104	83	89	9	93	108	77	41	29	57	108	109	76
72	114	125	93	42	6	103	123	83	86	65	99	98	134	74
76	97	107	113	6	18	108	103	90	90	76	90	94	108	70
88	94	108	102	0	55	107	95	90	121	64	69	58	105	79
98	82	85	84	0	78	93	76	91	116	97	88	38	86	100

$$\downarrow$$

111	113	114	115	110	103	93	84	75	76	68	72	76	88	98
63	48	52	55	46	46	46	28	4	74	115	114	97	94	82
134	86	54	48	46	55	49	18	42	94	104	125	107	108	85
98	100	100	100	98	97	94	90	92	86	83	93	113	102	84
88	89	94	99	101	103	102	101	106	101	89	42	6	0	0
70	71	71	71	67	60	53	50	42	21	9	6	18	55	78
37	27	34	40	32	31	28	12	0	44	93	103	108	107	93
100	67	53	51	44	49	45	21	37	88	108	123	103	95	76
128	123	115	106	98	93	90	83	76	76	77	83	90	90	91
19	19	20	19	16	12	8	8	0	0	41	86	90	121	116
27	40	51	54	53	47	50	60	110	58	29	65	76	64	97
47	50	55	56	44	39	38	36	87	70	57	99	90	69	88
91	90	90	94	96	101	103	106	93	96	108	98	94	58	38
110	77	55	47	41	42	34	12	22	87	109	134	108	105	86
100	105	111	115	113	107	99	89	75	82	76	74	70	79	100

Fig. 5. Transposition of the repositioned matrix

The complete stages of RGB image encryption using hybrid transpositions are shown in the flowchart in Fig. 6, while the decryption is a reverse process of the encryption.

The test data used in the implementation of the hybrid transposition for RGB image encryption is shown in Fig. 7. The three test data have different characteristics, both from image size and color characteristics.

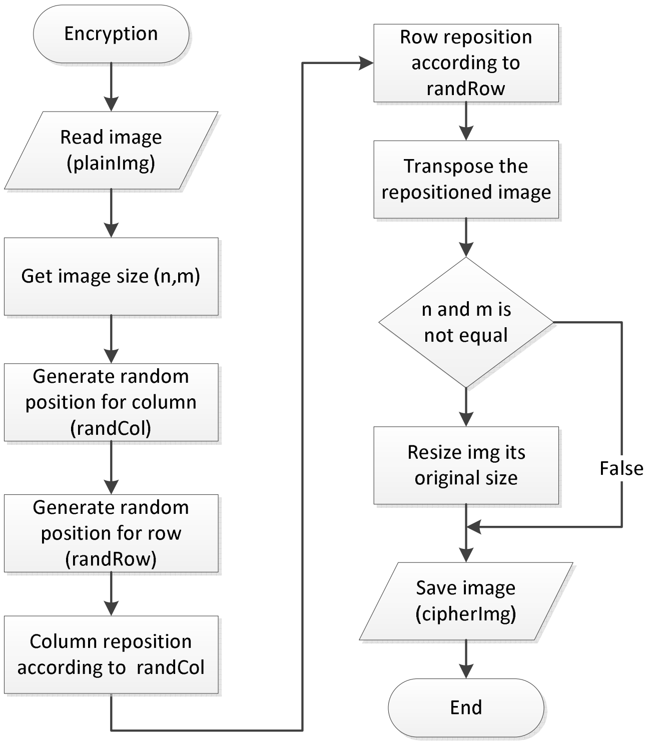
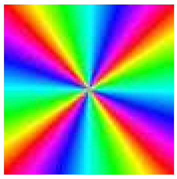
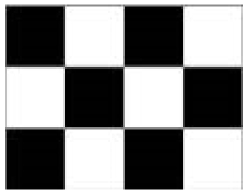


Fig. 6. Image encryption process using hybrid transposition



(a) Rainbow: 85 x 85



(b) Chessboard: 86 x 111

(c) Lena: 225 x 225

Fig. 7. The test data

Mean Absolute Error (MAE) and correlation coefficients are used to measure the performance of encryption using hybrid transposition on RGB imagery. MAE is used to assess the accuracy of the decrypted image compared to the initial image, while the correlation coefficient is used to assess the randomness of the encrypted image compared to its original. MAE is calculated using Eq. (1) and the correlation coefficient is calculated using Eq. (2).

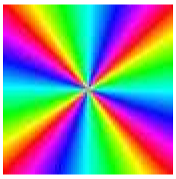
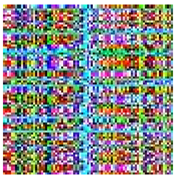
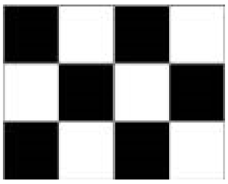
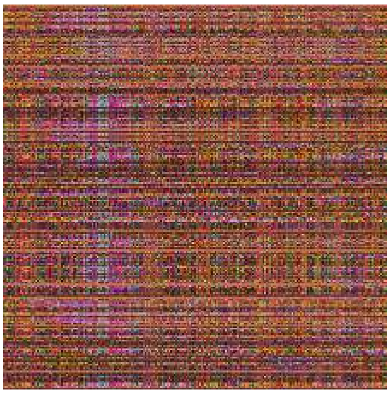
$$MAE = \frac{1}{n}\sum_{i=0}^{n}|x_i - y_i| \tag{1}$$

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

III. RESULT AND DISCUSSION

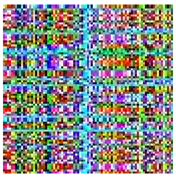
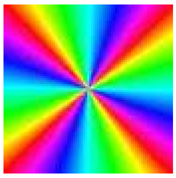
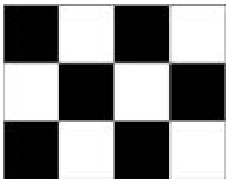
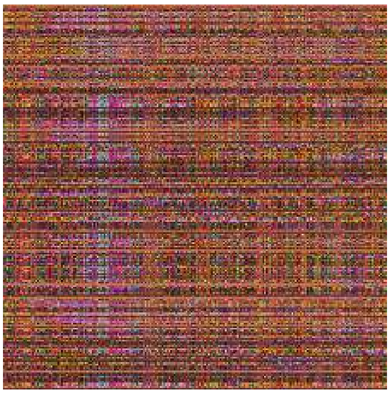
In this study, programs for encryption and decryption are made using Python programming by implementing openCV and numPy modules. Encryption is done on the intensity value of each color component in RGB image. The encryption results using the hybrid transposition is shown in Table I. As the key used to perform the encryption and decryption process is "abc123". To get a different seed, the minimum key length is 3 characters consisting of at least three different characters. To avoid any data changes in the storage process, the encrypted image is stored in a PNG format which is a lossless compression.

TABLE I. THE ENCRYPTION RESULT

Plain image	Cipher image	MAE	Corr. Coef.
		111.6986	0.0537
		129.3938	-0.0227
		49.1265	0.2958

From the Table I it appears that the results of the encryption are visually completely different from the original image. In the second test data, the encryption even has a different color composition than the original image. The MAE value shows a significant change in the intensity value of each corresponding pixel. The lowest MAE score is in the third test data which has the dominant base color of brown. The highest MAE value of 129.3938 is obtained on an image representing a chessboard image consisting of only two colors, black and white in nearly equal numbers. The encryption results of all test data have very high randomness indicated by correlation coefficient value close to 0 (zero).

TABLE II. THE DECRYPTION RESULT

Cipher image	Decrypted image	MAE	Corr. Coef.
		0.0	1.0
		0.0	1.0
		0.0	1.0

The results of the decryption are shown in Table II. It is seen from all test results that the MAE value is 0 and the correlation coefficient is 1.0 indicating that the decrypted image is exactly the same as the original image.

IV. CONCLUSION

This study shows that although without changing the intensity value of RGB images, matrix transposition operations combined with random repositioning were successfully implemented to encrypt RGB imagery. Random repositioning of columns and rows are conducted for the purpose of improving transposition performance in encrypting images. The randomness of the row and column positions is obtained using a random generator with the seed calculated from the encryption key provided.

REFERENCES

[1] T. Kumar and K. Verma, "A Theory Based on Conversion of RGB image to Gray image," *Int. J. Comput. Appl.*, vol. 7, no. 2, pp. 5–12, 2010.

[2] B. Banker and C. Singh, "Study of Effectiveness and Analysis of Mathematical Equation Used In Cryptographic Technique For Data Security," *J. Glob. Res. Math. Arch.*, vol. 4, no. 8, pp. 22–33, 2017.

[3] R. Talbert, "The Cycle Structure and Order of The Rail Fence Cipher," *Cryptologia*, vol. 30, no. 2, pp. 159–172, 2006.

[4] 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.

[5] M. B. Pramanik, "Implementation of Cryptography Technique using Columnar Transposition," *Int. J. Comput. Appl.*, pp. 19–23, 2014.

[6] 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.

[7] A. Bhowmick, A. V. Lal, and N. Ranjan, "Enhanced 6x6 Playfair Cipher using Double Myszkowski Transposition," *Int. J. Eng. Res. Technol.*, vol. 4, no. 7, pp. 1100–1104, 2015.