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.

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].
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 randomizations 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.
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.

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 three test data have different characteristics, both from image size and color characteristics.

Fig. 5. Transposition of the repositioned matrix

The test data used in the implementation of the hybrid transposition for RGB image encryption is shown in Fig. 7.

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).

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

(1)

\[
R = \frac{\sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n} (x_i - \bar{x})^2 \sqrt{\sum_{i=1}^{n} (y_i - \bar{y})^2}} 
\]

(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>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Plain image" /></td>
<td><img src="image2.png" alt="Cipher image" /></td>
<td>111.6986</td>
<td>0.0537</td>
</tr>
<tr>
<td><img src="image3.png" alt="Plain image" /></td>
<td><img src="image4.png" alt="Cipher image" /></td>
<td>129.3938</td>
<td>-0.0227</td>
</tr>
<tr>
<td><img src="image5.png" alt="Plain image" /></td>
<td><img src="image6.png" alt="Cipher image" /></td>
<td>49.1265</td>
<td>0.2958</td>
</tr>
</tbody>
</table>

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).
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