Encryption of Color Images using Pixel Shift Algorithm and Developed Hill Algorithm

Mohsen Norouzi[1*], Ali Arshaghi[2], Mohsen Ashourian[3]
1- Researcher, Faculty of Computer, Imam Hossein University, Tehran, Iran.
Email: m.norouzi@ihu.ac.ir (Corresponding author)
2- Researcher, Faculty of Computer, Imam Hossein University, Tehran, Iran.
Email: a.arshaghi@ihu.ac.ir
3- Department of Electrical Engineering, Majlesi Branch, Islamic Azad University, Isfahan, Iran.
Email: ashourian@iaumajlesi.ac.ir

Received: 6 August 2022 Revised: 10 September 2022 Accepted: 21 October 2022

ABSTRACT:
With the advent of communication networks, the speed of data transmission has increased dramatically. One of the important factors in each transfer is to maintain data security and prevent unauthorized access to data transmitted. Using cryptography is one of the methods used to keep data secure throughout the transmission path. Today, with the growth of computer networks, the use of video conferencing, the transfer of military information, image data, the need for encryption of data in a variety of image data plays an important role. Encryption in images due to its specific features, such as the high volume of transmitted images, the amount of additional data for encryption, the correlation coefficient and the high repetition among the pixels, are very different from the text data; this has led to all traditional encryption methods It is not suitable for image data and there are changes in their structure to use traditional methods in image cryptography. In this paper, using pixel shift algorithms and Hill's encryption algorithm, ciphering of color images has been addressed; the pixel shift algorithm has been used to maintain greater dependency and security, and Hill's encryption algorithm has been used to change the amount of pixels. For analysis of the work, the algorithm is presented and for comparison with other methods, images and standard analysis methods have been used. The obtained results improve the efficiency of the proposed algorithm in comparison with the standard hail algorithm (especially in images with similar pixels) And compared with other comparable algorithms.

KEYWORDS: Hill algorithm, Pixel shift algorithm, Encryption.

1. INTRODUCTION

With the advent of computer networks, the speed and availability of information has increased significantly. Important and private data is easily transmitted in various environments and networks, such as the internal network of an organization, mobile networks and also on the Internet. Different methods are available for confidential transmission of data; one of the most important methods for secure communication is the use of data encryption [1]. Cryptography is the knowledge of changing text, message, or information using a key encryption using a cryptographic algorithm, so that only the person who knows the key and the decryption algorithm is able to extract the main information from the encrypted information and the person who is from one or They both do not know, they cannot access the information [2]. One of the types of data that has been gradually being transmitted in various networks is image data that has many uses in various fields, including Internet communications, multimedia systems, medical images, etc. [5-3] In image data, depending on the nature of the data, such as high data volumes, the dependence of the pixels on the formation of an image and the time required for encryption, the use of text encryption methods for the differences between the image and the text and the large amount of data It is not directly applicable to cryptography of images and should make changes to their structure [1]. Hill's encryption algorithm is a text encryption algorithm. Which is slightly changed in the ciphering of image data. In many years, this algorithm has been used in many researches. In cases where only encrypted data is available to an attacker, the attack on the Hill encryption algorithm is difficult. However, in attacks that in addition to encrypted text, there is the possibility of choosing the input to the encryption system, it is possible to break the

Paper type: Research paper
DOI: 10.30486/mjtd.2022.1974418.1000
How to cite this paper: M. Norouzi, A. Arshaghi and M. Ashourian, "**Encryption of Color Images using Pixel Shift Algorithm and Developed Hill Algorithm**", Majlesi Journal of Telecommunication Devices, Vol. 11, No. 4, pp. 177-184, 2022.

password with respect to the same encryption key for the entire image. To improve the Hill algorithm in the project, Hill's algorithm has been used with different keys for encryption. Using this method also improves cryptography in cases where images with similar and adjacent pixels are present. In this project, a matrix is used as many times as encryption has been done. In each house, a random number has been set from this matrix. The amount of any key used in the Hill algorithm is multiplied at the home corresponding to this presentation. Due to this method, at each step of the encryption, the key used in the encryption changes. For comparison of the encryption algorithm provided with standard Hill, Algorithm of error coefficient, correlation coefficient and irregularity factor are used. In the project [7], encryption is based on Hill's algorithm, which states the security and interpolation of more pixels using a number of reversible capability keys. For further synchronization in the proposed algorithm, three algorithms with their sequential combinations are used. Hill's cryptographic algorithm is the first algorithm outlined in this research. In this algorithm, the original image is initially divided into blocks of 8*8 and each block is encrypted using a return key. In the next algorithm, it refers to one of the major problems in the Hill algorithm and has provided a solution to this problem. In the project [8], to improve Hill encryption in images with similar pixels, XOR is a randomized matrix with a main image. In this algorithm, a chaotic single-dimensional function is used to construct a random matrix. The integration of encrypted image with the chaotic function results in better encryption of the final image and improvement in cryptographic security factors. In this project, XOR is used to improve the cryptographic resolution of images with similar pixels, using a randomized matrix with a main image. In this algorithm, a chaotic single-dimensional function is used to construct a random matrix. The integration of encrypted image with the chaotic function results in better encryption of the final image and improvement in cryptographic security factors. The following algorithm has been used to analyze the work of the algorithm, using PSNR, SSID and MSE analyzes. In the research [9], the pixel intersection method is based on the clustering algorithm and logistic inertia algorithm. In the algorithm, the original image is divided initially into 6 unmatched equal parts. The six parts are mapped in the upper, lower, front, back, left and right sides of the cube, respectively. To fill the cube at each stage, 54 elements are needed. According to the divisions, 9 pixels are selected from each area. To calculate the number of rotations in each stage, a logistic randomization algorithm has been used. At this stage, the required numbers for the desired fiber rotation, in the interval (18-18), are constructed by the logistic function, and the cubes are considered according to the random numbers obtained.

2. THE PRPPOSED METHOD

In image data, because of the high volume of information being transmitted, cryptography is very important for maintaining security. Different methods have been proposed for image cryptography. In some of these methods, new encryption algorithms and some other traditional encryption methods such as AES encryption, DES, and other encryption methods have been used. In the proposed algorithm in this thesis, an effective method based on disturbance, diffusion and change of pixels has been used. In the turbulence phase and the release of pixels, the proposed pixel shift algorithm has been used and for the pixel transformation and modification, the proposed developed hail encryption algorithm has been used, which is considered as one of the traditional encryption algorithms. The pixel shift algorithm used in this project has been used to increase the sensitivity of input image pixels and encryption key. The proposed shifting algorithm shifts pixels to vertical, horizontal, and interlayer methods using the remainder of the division of pixel values. In this algorithm, by changing only one bit of the input image or the main key of the variations in the entire image, it creates a different image than the original image. To change the values of pixels in the proposed method, the proposed helium algorithm is used to change the amount of pixels using the encryption key matrix. Figure 1 shows the proposed encryption algorithm. As stated, pixel and helix shift encryption algorithms have been used in encryption.

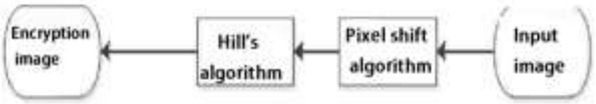

Fig. 1. proposed algorithm.

a. Hill proposed algorithm

Depending on the dependence of the pixels of the three layers of the image (red, green and blue), to fill the matrix used in each step, the composition of the pixels of each of the three layers instead of encryption of each layer is used separately. This combination helps to better capture the image due to the dependence of different pixels on each other. The range chosen for encryption in the standard Hill algorithm is based on numbers assigned to English letters (0-25). For proper operation of the algorithm and appropriate encryption and decryption operations, split operations should be performed in the image pixel range (0-255). Changing the range of the Hill algorithm results in the proper mapping of the pixels of the image. In Figure 2, the result of the encryption is visible

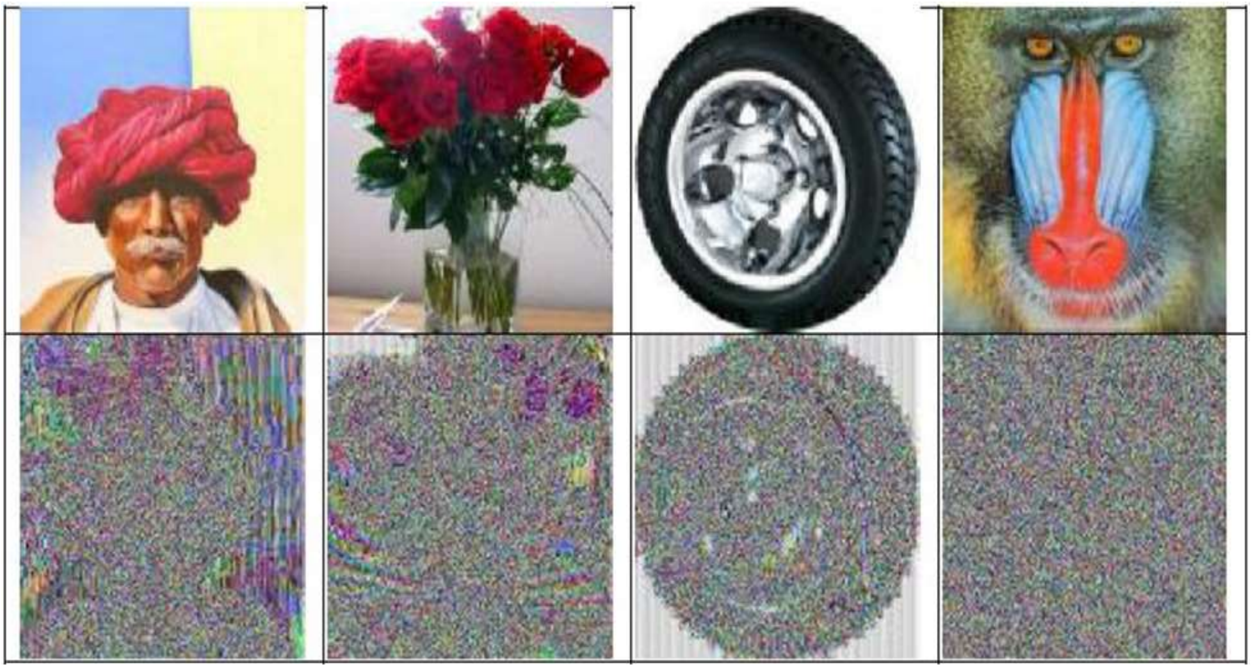

Fig. 2. Encrypted images are developed using Hill's algorithm.

As seen in Fig. 2, despite the change in the standard hail algorithm, in images with similar and adjacent pixels, the mapping of pixels will be the same due to the use of a similar password matrix for the entire image. In these images, the Hill algorithm alone is not sufficient for cryptography, and the encrypted image is largely recognizable. To improve the Hill algorithm, the image is combined with the pixel shift algorithm

b. Proposed Pixel Shift Algorithm

One of the most important cryptographic criteria is the sensitivity to minor changes in the input image and the key to encryption. To measure the sensitivity, one bit of input image or cryptographic key is changed and the results of the changes published in the whole image are examined. Encryption should be sensitive to the change in pixels, even when changing a bit of the original image. A pixel shift has been used to create a greater dependency on the original encryption system and the encryption key. At this point, pixel shifts have been used to further interact with the main image elements and cryptographic key. The pixel shifts are used horizontally, vertically and in depth in a combination; the steps are described below.

1. Using a random number algorithm, an array is generated in the number of rows and columns using the random number generation algorithm presented in the range of 0 to 256.
2. At the pixel shift stage in row mode, for each row, the sum of the pixels of each row is calculated. The sum of the remaining aggregate pixels is calculated on 2 (the number 2 is obtained from the minimum number and since the number 1 does not affect the operation, the next number of which 2 is used). If this remainder is equal to zero, the existing pixels in the row as large as the number in the house of the random array, it turns to the right in a rotational manner. In the absence of zero, the rotation of pixels in the direction of the image will take place.
3. In column mode, for each column, the sum of the pixels of each column is calculated. The remainder of the sum of the pixels is calculated on 2. If this remainder is equal to zero, the pixels in the row are rotated in the same row as the number in the random array header. In the absence of zero, the rotation of pixels in the direction of the image will take place.
4. In the interlayer stage, for all elements in a row or a column, the sum of all three pixels in a spatial position is computed. Considering that 3 pixels in 6 modes can be put together. The sum of the remainder is summed to 6. The resulting number indicates the position of the pixels together. Fig. 3. The result of pixel shifts after 2 stages and only using the pixel shift algorithm are presented on different images.

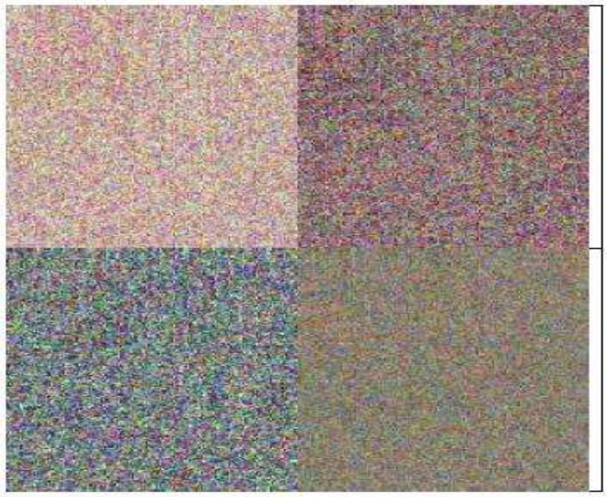

Fig. 3. Results obtained only from the pixel shift algorithm.

c. The final combination of proposed algorithms

In the proposed algorithm, we use two general steps of pixel shifts and Hill's algorithm.

1. Pixel Shift: In the first step of encryption, pixel shifts are used to interfere with the sensitivity of pixels to minor variations. Pixel Shift Action is a three-step algorithm that runs in a combination. In this algorithm, due to the specific structure of the implementation, the image should be square. In non-square images, the pixel shift algorithm adds pixels to rows and columns with a value of zero. The number of pixel shift steps depends on the number of rows (the image is square and the number of rows and columns is the same). If the original image is 256 * 256, the number of executable algorithms is 256 repetitions. Shift operation is initially performed on the vertical axis. At this stage, for each repetition, the sum of the same lines is divided by the number 2 (if the first is repeated, the sum of the numbers in the first row). If the remainder is divisible by 2, the sum of the same row is zero, depending on the amount of the array at the repetition location, the rotation of the row is rotated to the right and rotated. In the case of non-zero, the shift of the elements of the row is done to the left. After each row in the column corresponding to that operation, the sum of the pixels is done on it. If the remainder of the column is 2 times as large as zero, the pivot rotation of the pillar is upward and is placed in the corresponding place according to the random array repetition. In the case of non-zero remaining split, the shift is done down. In each repetition of the corresponding row and column, the pixel shift algorithm is applied to it. In the third step, proportional to each repetition, each of the pixels of the row and column in each of the three layers are tangled with respect to the random array values. At this stage, for each pixel, the sum of the pixels in each of the three layers is computed. Given the fact that the movement of the three elements has 6 different modes (green pixel, red pixel, pixel of the blue layer, red pixel, green layer pixel, blue layer pixel). The remainder of the division of 6 indicates the selection of each of the migration modes per pixel in the row or column corresponding to the repetition. The mentioned steps are performed until the end of the repetitions. In the pixel shift algorithm, a change of only one bit in the sum of the pixel's changes, resulting in these changes throughout the image.

2. Hill's algorithm: In the cryptographic algorithm, pixels have performed two different hemispheric steps. Pixels are distributed throughout the image, and any changes to the original image will cause a change in the entire image. In the next step of encryption, the modified Hill algorithm is used to change the values of the pixels. In this algorithm, from each of the three layers of the image in each step to change the pixels, which is due to the dependence of the pixels of each of the three layers of the image to form the final image, a better encryption is done. In the Hill algorithm used, division 256 is used instead of the common number 26, which will cause proper mapping of the pixels. In the proposed algorithm, a modified Hill algorithm with a 3 * 3 matrix is used. The final encrypted image is shown in Fig. 4.

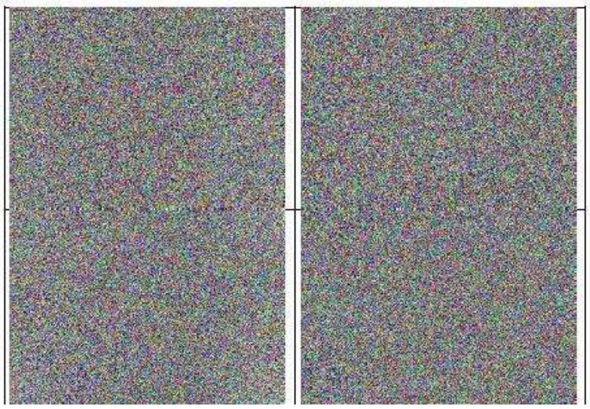

Fig. 4. Ultimate encoded image.

3. The RESULTS OF THE PROPOSED ALGORITHM

For analysis of the proposed algorithm, standard tests have been used. Matlab software is used to implement the proposed algorithm. Selected images are standard images of images or images in other researches. In the analysis stage, at first, various tests have been performed on the proposed method. In the next step, in comparison with other methods, several projects have been selected and the numbers and results obtained in the same images are compared with these papers. In Fig. 5, 6 images are selected for testing and comparison with other methods. These images have been selected in most articles as references for cryptography and provide a good benchmark for comparison.

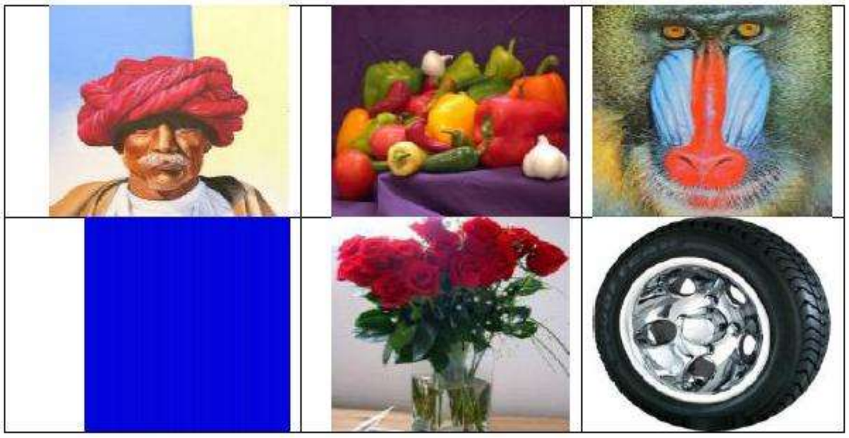

Fig. 5. The images used to compare the encryption provided.

a. Histogram analysis

In Fig. 6, the results of the histogram analysis are shown on the shapes in Fig. 5 as shown in the figure. A remarkable point in this algorithm is the inhaling, which makes the three layers of the image have almost identical histograms. In the proposed algorithm, the pixels are combined in each of the three layers of the image, and according to this, the histogram of the three layers of the image has a shape and is not similar to the histogram of the original image.

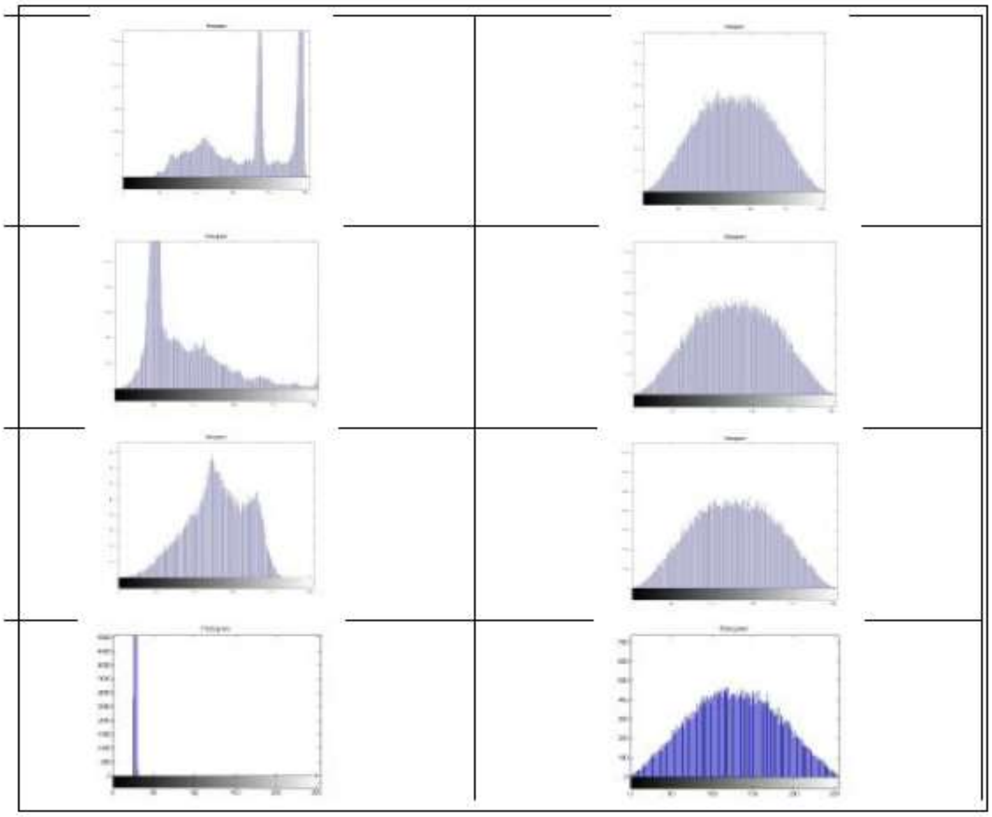

Fig. 6. Histogram analysis of the image encoded with the original image. The first histogram, the person's image, the second histogram, the pepper image, the third histogram of the image of the baboon, the fourth histogram of the blue image.

b. Signal to error ratio

In the encryption of images as noted, the ratio of the signal strength to the error in the encrypted image is lower. Better encryption and the original image with a ciphered image are less similar to each other. The signal-to-error ratio is also used to measure the quality of the decoded image. The more this figure is in the decoded image, the higher the quality of the decoded image and the better the decoding image is. In Table (1), the signal-to-error ratio has been compared in the encryption and decryption stage.

Table 1. Comparing the PSNR of the image decoded with the original image

PSNR rate of encrypted image	Desired image
9.137	person
9,8249	peppers
9,9827	baboon
8.7171	Flower
6.9657	wheel

c. Structural Similarity

Structural similarity is one of the factors measuring the similarity between the encrypted image and the main image and is more recent than the PSNR parameter and is a more appropriate criterion for the expression of cryptographic properties. In Table 2, the structural similarity between the encoded image and the original image is shown.

Table 2. Comparing the SSID of the image decoded with the original image

SSIM	Desired image
0,020396	Person
0,019609	peppers
0,018566	baboon
0,017635	Flower
0,01098	wheel

d. Correlation Coefficient

Correlation coefficient is one of the criteria for comparing cryptographic algorithms with each other. The maximum correlation coefficient is equal to one, indicating that two images are identical. If the two images have a similar resemblance to each other, the relation between the adjacent pixels is very low and equal to zero, indicating a good encryption. To compare the correlation coefficient, select 2500 pixels of the image and the pixels are displayed in the dimensions of the longitudinal row and in the diameter. Also, the comparison of the numbers obtained from the comparison of these images is shown in Table (3).

Table 3. Comparison of correlation coefficient in different images

Pearson Correlation Coefficient	Total Correlation Coefficient	Diameter correlation coefficient	Column correlation coefficient	Row correlation coefficient	Desired image
-0,0071075	-0,010966	-0,0032038	-0,010324	-0,010068	person
0,0011731	0,0021515	-0,010091	-0,020854	0,0057918	peppers
0,002973	-0,0050275	-0,016657	-0,018103	-0,0060865	baboon
0,00039174	0,00061568	-0,010576	-0,023061	0,0010566	Flower
-0,0013872	0,00056016	-0,014883	-0,016179	0,005181	wheel

4. COMPARISON BETWEEN DIFFERENT ALGORITHMS

To analyze the sensitivity between encrypted images, the image is again encrypted using a key that differ in only one bit. In Table 4, the results of the comparison of the two images using the criteria (NPCR, UACI) and its comparison with other studies have been presented. As you can see, the more NPCRs are closer to the number one, the proposed algorithm has a higher sensitivity to the change of the main key, and the higher the UACI value, the greater the sensitivity to the key. To compare the results of the proposed algorithm with other algorithms, several projects that use this parameter to analyze their security results have been used; the results of this comparison can be seen in Table 4.

Table 4. Comparison of NPCR and UACI factors in main key analysis for Lena image

UACI	NPCR	algorithm
0,334635	0,996094	proposed algorithm
----	0,996024	Ref. [11]
0,334629	0,996098	Ref. [12]
0,335561	0,996689	Ref. [13]
0,333245	0,995765	Ref. [14]

5. CONCLUSION

In this study, an efficient solution for image encryption was introduced using Hill's encryption algorithm. In the structure of this algorithm, two combinatorial algorithms are used to encrypt the image. Pixel shift algorithm and Hill encryption algorithm. In the pixel shift algorithm, the dependency on the input image and the main key increases. Hill's algorithm is used to change the amount of pixels. The pixel shift algorithm is the first encryption step in the proposed algorithm. The algorithm consists of three pixel shift rotation, pixel shift and pixel shifts in interlayers. At the row stage, the sum of a row is computed and if it is 2, then the line is shifted to the right as the random number calculated by the random function. Otherwise, the pixel shift will be to the left. In the column stage, the sum of the pixels of the row is computed and in the case of the remaining zero, dividing by 2, the rotation of the rotation will be upward. The nonzero result causes a rotation to go down. In an interlayer shaft, each pixel has 3 pixels selected to form the color of a pixel, and depending on the remainder, dividing the sum of three pixels by 6, one of the three-pixel scroll modes is selected and placed. In the cryptographic algorithm of Hill, pixel values change. Given the block of this encryption, each block of pixels in the image is selected and the encryption process is performed on them. In the Hill algorithm, the remainder of the split 256 is used for proper mapping and selection of different pixels in each block. To evaluate the proposed method, visual analysis, qualitative analysis, histogram analysis was used. In the visual analysis, the algorithm was improved with the standard Hill method of encryption and the efficiency of the proposed algorithm. In the histogram analysis, the statistical similarity between the encrypted image, the original image and the decoded image was examined. In qualitative analysis, the quality of the image was encrypted and the image decoded with the original image was examined. In the correlation analysis, the correlation between the pixels in the image encoded with the original image was examined. In the next step, in order to better compare the efficiency of the tested algorithms on the Lena image, the results were compared with other algorithms, which in all the tests the proposed algorithm has a good performance. There is a significant improvement over Hill's encryption algorithm in the provided factors. It has a disturbance and a good distribution of pixels. Sensitivity to the main key and the input image is high and according to the results obtaind, it has high security.

REFERENCES

[1] Roger A. Prichard, "**History of Encryption**" January 26, 2002.

[2] Andreas Uhl, Andreas Pommer, "**image and video encryption**",SpringerScience, p.1, 2005.

[3] O. S. Faragallah, Utilization of Security Techniques for Multimedia Applications, Ph. D. Thesis, Department of Computer and Engineering, FacultyofElectronic Engineering, Menofia University, 2007.

[4] A. J. Menezes, P. C. V. Oorschot and S. Vanstone, "**Handbook of Applied Cryptography**",CRC Press Boca Raton ,USA, 1996.

[5] L. Qiao, "**Multimedia Security and CopyrightP Urbana-Champaign, Urbana, Illinois**", USA, 1998.

[6] ISMAIL I.A, AMIN Mohammed, DIAB Hossam, "**How to repair the Hill cipher**", Journal of Zhejiang University SCIENCE A, Volume 7(12),pp. 2022-2030,2006.

[7] S.K.Muttoo, Deepika Aggarwal, Bhavya Ahuja, "**A Secure Image Encryption Algorithm Based on Hill Cipher System, Bulletin of Electrical Engineering and Informatics**;, Vol.1, No.1, PP. 51

[8] Dipanwita Debnath, Suman Deb, Nirmalya Kar "**Using Hill Cipher & RGB Image Steganography**" ,178-183 ,2015

[9] Li ZHANG, Xiaolin TIAN, ShaoweiXIA, "**A Scrambling Algorithm of Image Encryption Based on Rubik's CubeRotation Logistic Sequence**", IEEE Computer Society, Volume 1, pp. 312

[10] Zhi-liang ZHU , Chong WANG , Hua CHAI , Hai YU, "**A Chaotic Image Encryption Scheme Based on Mag Transformation**", Fourth International Workshop on Chaos

[11] Kwok, H.S. Tang, W.K.S. "**A fast image encryption system based on chaotic maps with finite precision representation** ", Chaos solitons Fractals ELSEVIER, Volume 32,pp.1518

[12] S. M. Seyedzadeh, S. Mirzakuchaki, "**A fast color image encryption algorithm based on coupled two chaotic map**", Signal ProcessingELSEVIER,

[13] Benyamin Norouzi, Seyed Mohammad Seyedzadeh, Sattar Mirzakuchaki, Mohammad Reza Mosavi, "**A novel image encryption basedhash function withonly two-round diffusion process**", springer,2013.

[14] Yang Liu, Xiaojun Tong, Shicheng Hu, "**A family of new complex number chaotic maps based image encryption algorithm**" Signal Processing: Image Communication,Volume 28, pp.1 548-1559-2013.