AN EFFICIENT COLOR IMAGE ENCRYPTION SCHEME BASED ON COMBINATION OF HILL CIPHER AND CELLULAR NEURAL NETWORK

Azza A. Abdo
Imam Abdulrahman Bin Faisal University, Saudi Arabia,
department of Computer Science, Faculty of Science and Humanities.
(aaaali@iau.edu.sa)

Hanaa F. Morse
Imam Abdulrahman Bin Faisal University, Saudi Arabia,
department of Computer Science, Faculty of Science and Humanities.
(hfmorse@iau.edu.sa)

Maissa A. El-Mageed
Imam Abdulrahman Bin Faisal University, Saudi Arabia,
department of Mathematics, Faculty of Science and Humanitis.
(melmageed@iau.edu.sa)

Abstract. This paper presents an enhancement of Hill cipher-based image encryption scheme by deployment of cellular neural network. Initial secret values are generated using cellular neural network to be used in image diffusion with hill matrix. Our proposed scheme is compared with using Hill cipher algorithm without depending on random grid cellular neural network as an image encryption scheme. Using Hill cipher and cellular neural network to encrypt image increases the security of secret images with lossless image encryption. Experimental results demonstrate the efficiency of the scheme.

***Keywords*:** Image Encryption; Hill Cipher; CNN

1. Introduction

Security is playing an important role for protecting information when it flows over in a network. The scheme claimed to provide secure communication with easy decryption. Some of Image encryption algorithms uses the traditional encryption such as Hill cipher[1], other papers used the slandered algorithms in image encryption such as advanced encryption slandered AES[2]. Recently numerous papers used chaotic system in image encryption where it has a good effectiveness in the quality of encryption up on the sensitivity of initial values[3-11]. On the other hand, most of chaotic systems used for image encryption have a weakness in security analysis [12, 13, 14]. Other encryption algorithms used DNA in encryption process[15,16,17,18].

Hill cipher is one of the tradition algorithms used in encryption. It depends on multiplication of matrices. One of these matrices is said to be secret key matrix and the other is given from the plaintext which will be encrypted. The secret key is a singular matrix.

Cellular neural network (CNN) is one the chaotic systems. CNN has a nonlinear identical cell arranged in a rectangular grid connected with the neighbor's cells. The generated numbers from CNN are very sensitive to initial values changing.

In this paper Hill cipher algorithm is used for color image encryption, but for enhancement the Hill cipher-based image encryption, a deployment of CNN with Hill cipher, is used. Initial secret values are generated using CNN to be used in image confusion phase with Hill matrix. Our proposed scheme is compared with using Hill cipher algorithm without depending on random grid cellular neural network as an image encryption scheme. Using Hill cipher and CNN in image encryption increases the security of secret images with lossless image encryption. Experimental results demonstrate the efficiency of the scheme.

The rest of the paper is organized as follows. In Section 2 a brief overview of Hill Cipher, Cellular Neural network (CNN) are presented. The proposed image encryption scheme is discussed in section 3. Experimental results of the proposed scheme are shown in section 4. Section 5 gives the conclusion.

2. Overview

2.1 Hill cipher based image encryption[1]

The core of Hill cipher is matrix multiplication. Given a secret image I and key matrix $k = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$, under the condition of K which must be invertible. The encryption is carried out as follows. Image encryption based on Hill cipher depends on dividing the image I into equal size blocks, and then Hill cipher is applied on each of these blocks. Consider a block P of two consecutive pixels p_1 , p_2 of the plain image I. The encryption of the block P is equivalent to cipher block $C = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$ based on the following equation:

$$\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} \quad mod\ 256 \qquad (1)$$

Then based on above equation, the cipher image is generated as $\mathrm{C} = \mathrm{KP} \bmod 256$, Where $C = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$, $k = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$ and $P = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$

The secret plain can be retrieved as $= K^{-1}P\ mod\ 256$, where K^{-1} is the inverse of the matrix k .

2.2 Cellular Neural Network [18]

Cellular neural network is a rectangular grid of identical cells. Each cell has a nonlinear equation and connected to its 8 closets surrounding neighbors. 1'st- order circuit components are a linear resistance, a linear capacitance, and some voltage-controlled current sources. In [11] the chaotic phenomena in the 3rd-order CNN system is described as follows:

$$\dot{x}_j = -x_j + a_j y_j + \sum_{k=1,k\neq 1}^{3} a_{jk} y_j + \sum_{k=1}^{3} S_{jk} x_k + i_j, \qquad j = 1,2,3. \qquad (2)$$

Where x_j is a state variable, a_j a constant, i_j the edge value, and y_j a cell output? The output is connected to the state by the nonlinear equation:

$$y_j = 0.5 \times \left|(x_j + 1)\right| - \left|(x_j - 1)\right|.$$

By substituting in the values $a_{12} = a_{13} = a_2 = a_{23} = a_{32} = a_3 = a_{21} = a_{31} = 0$; $S_{13} = S_{31} = S_{22} = 0$; $i_1 = i_2 = i_3 = 0$; $S_{33} = S_{21} = S_{23} = 1$. In Eq. 1, the three cells parameters x_1, x_2, x_3 will be given as follow [19]:

$$\begin{aligned} \dot{x}_1 &= -x_{j1} + a_1 * y_1 + S_{11} * x_1 + S_{12} * x_2, \\ \dot{x}_2 &= -x_2 + x_1 + x_3, \\ \dot{x}_3 &= -x_3 + S_{32} * x_2 + x_3 \end{aligned} \qquad (3)$$

From these equations, we can get different chaotic output parameters by using different input parameters x_1, x_2, x_3, a_1, S_{11} , S_{12} , S_{32} .

3. The proposed scheme

In the proposed scheme, the secret key contains secret matrix $\begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$, initial input parameters for CNN conditions $x_1, x_2, x_3, a_1, a_0, a_{11}, S_{11}, S_{32}, a$ where $0 < x_1, x_2, x_3 < 1$, and K, λ are a large integer numbers used as a map for transforming the CNN output to integer number between 0 and 256. The integer value $1 < a < 255$.

The encryption process consists of two phases, the first phase is the permutation phase, and the second is the diffusion phase. Figure.1 represents the two phases of the proposed scheme

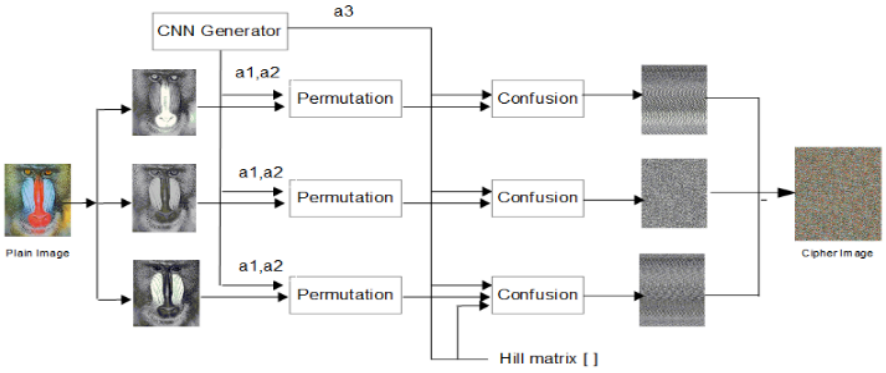


Figure.1: Diagram of the proposed scheme

For image $G$of size $M \times N$, where M is the height and width of G . The permutation is applied on each row and each column of the plain image, and then a pixels values are changed in the diffusion phase. Permutation. Steps of the proposed encryption applied as in the following steps in Algorithm.1.

Algorithm1. The proposed encryption algorithm.

Step1: CNN is utilized with the initial parameters $x_1, x_2, x_3, a_1, a_0, a_{11}, S_{11}, S_{32},$ to generate the valuesx_1, x_2, x_3 .

Step2: ***Row permutation:***

For $\boldsymbol{i = 1}$: M *(i.e. for each row)*

- $\boldsymbol{S1}$: Utilize CNN to generate the next new values x_1, x_2, x_3 .
- $\boldsymbol{S2}$: Compute X, where: $X = mod(\lfloor x_1 * 10\text{^}6 \rfloor, 256)$
- $\boldsymbol{S3}$: Compute the parameter C, where:
$$c = mod(a * (i - 1) + x_1, n);$$
- ***S4:*** *G'(i1:N)= G(c+1).* Where G′ is the new permuted image.

End For

Step3: ***Column permutation:***

For $\boldsymbol{j = 1}$: N *(i.e. for each column)*

- $\boldsymbol{S1}$: Utilize CNN to generate the next new values x_1, x_2, x_3 .
- $\boldsymbol{S2}$: Compute$X$, where: $X = mod(\lfloor x_2 * 10\text{^}6 \rfloor, 256)$
- $\boldsymbol{S3}$: Compute the parameter C, where:
$$c = mod(a * (j - 1) + x_1, n);$$
- ***S4:*** $G''(1{:}\,M, j) = G'(c + 1)$. Where G″ is the new permuted image.

End For

Step4: ***Diffusion phase:***

For $\boldsymbol{j = 1}$: N

For $\boldsymbol{j = 1}$: 2: N

$\boldsymbol{S1}$: Construct p_1 and p_2 pixels block $P = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$, where p_1 and p_2 are chosen as $G''^{(\mathrm{i},j)} and\ G''$ $(\mathrm{i}, j + 1)$ respectively.

$\boldsymbol{S2}$: Construct the encrypted values c_1 and c_2 pixels block $C = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$as follows:

$$\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \begin{bmatrix} k_{11}\ k_{12} \\ k_{21}\ k_{22} \end{bmatrix}$$

$\boldsymbol{S3}$: Replace values of pixels $G''(\mathrm{i}, j)\ and\ G''(\mathrm{i}, j + 1)$ with c_1 and c_2 respectively.

End For

End For

Step5: Return G'' as encrypted image.

The decrypted image is computed through the following in decryption algorithm.2:

Algorithm.2. The proposed decryption algorithm.

Step1: ***Diffusion inverse phase:***

For $\boldsymbol{j = 1}: N$

For $\boldsymbol{j = 1}: 2: N$

$\boldsymbol{S1}$: Construct c_1 and c_2 pixels block $c = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$, where p_1 and p_2 are chosen as $G''(\mathrm{i}, j)\ and\ G''(\mathrm{i}, j+1)$ respectively.

$\boldsymbol{S2}$: Construct the decrypted values p_1 and p_2 pixels block $P = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$as follows:

$$\begin{bmatrix} p_1 \\ p_2 \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} \begin{bmatrix} k_{11}\ k_{12} \\ k_{21}\ k_{22} \end{bmatrix}^{-1}$$

$\boldsymbol{S3}$: Replace values of pixels $G''(\mathrm{i}, j)\ and\ G''(\mathrm{i}, j+1)$ with p_1 and p_2 respectively.

End For

End For

Step2: CNN is utilized with the initial parameters $x_1, x_2, x_3, a_1, a_0, a_{11}, S_{11}, S_{32},$ to generate the valuesx_1, x_2, x_3 .

Step3: ***Column inverse permutation:***

For $\boldsymbol{j = 1}: N$ *(i.e. for each column)*

- $\boldsymbol{S1}$: Utilize CNN to generate the next new values x_1, x_2, x_3 .
- $\boldsymbol{S2}$: Compute$X$, where: $X = mod(\lfloor x_2 * 10\text{^}6 \rfloor, 256)$
- $\boldsymbol{S3}$: Compute the parameter C, where:
$$c = mod(a * (j-1) - x_1, n);$$
- ***S4:*** $G'(1: M, j) = G''(c+1)$.

End For

Step4: ***Row permutation inverse:***

For $\boldsymbol{i = 1}: M$ *(i.e. for each row)*

- $\boldsymbol{S1}$: Utilize CNN to generate the next new values x_1, x_2, x_3 .
- $\boldsymbol{S2}$: Compute X, where: $X = mod(\lfloor x_1 * 10\text{^}6 \rfloor, 256)$
- $\boldsymbol{S3}$: Compute the parameter C, where:
$$c = mod(a * (i-1) - x_1, n);$$
- ***S4:*** *G(i1:N)= G'(c+1).*

End For

Step5: Return G as decrypted image.

4. Results and Analysis

Results of the proposed scheme is discussed in this section. Algorithm is implemented for encrypting the color images for different sizes. The secret color images Paper, Sky, and Papon are shown in Figure 2(a-c) and are used to be enciphered using the secret encryption key matrix $\begin{bmatrix} 3 & 2 \\ 4 & 3 \end{bmatrix}$ and the initial values $x_1 = 0.30, x_2 = 0.30, x_3 = 0.33;, a_1 = 127, a_0 = 1.99, a_{11} = 3.86, S_{11} = -1.55; S_{12} = 8.98, S_{32} = -14.25, K = 3500, \lambda = 127$. Figure.2 (d-f) shows the first output permutation path for the proposed scheme using the secret values generated using initial CNN values as in equation1. Also Figures.2 (g-i) show the final ciphered Paper, Sky, and Papon images. For color plain image, the plain image is spilt into three color levels red, green, and blue color images, and then each panel is encrypted, then the three encrypted panels are merged to generate the final encrypted image. Figure.3 (a-d) shows the plain image Papon, and its red, green, blue channels. Also, the corresponding cipher images for the three channels are shown in Figure.3 (e-g). As it is seen from figures 2 and 3, the results of the ciphered image quality have a good confusion and diffusion properties. Security, Quality of encryption, sensitive analysis and other measures for the proposed scheme are discussed at the remaining at this this section.

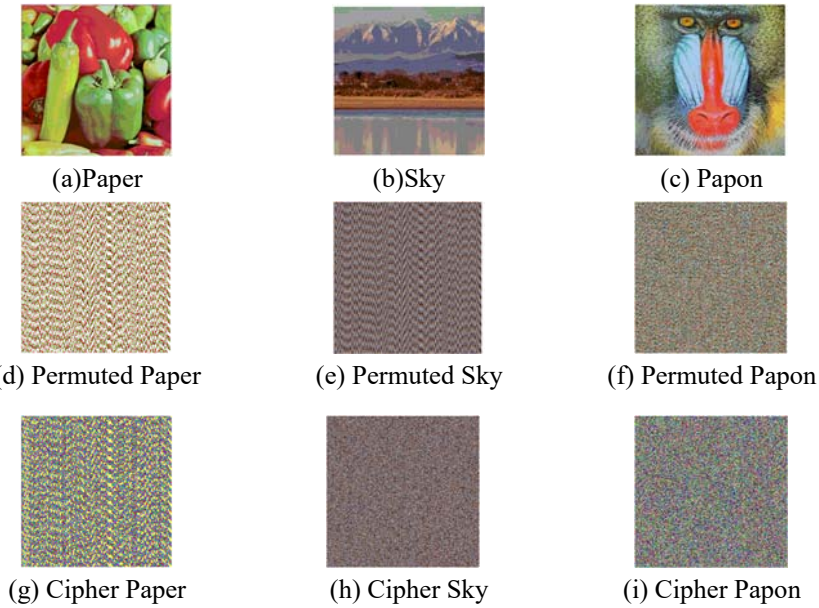


Figure2. Encrypted color images for two phases permutation and diffusion for color images of the propped scheme.

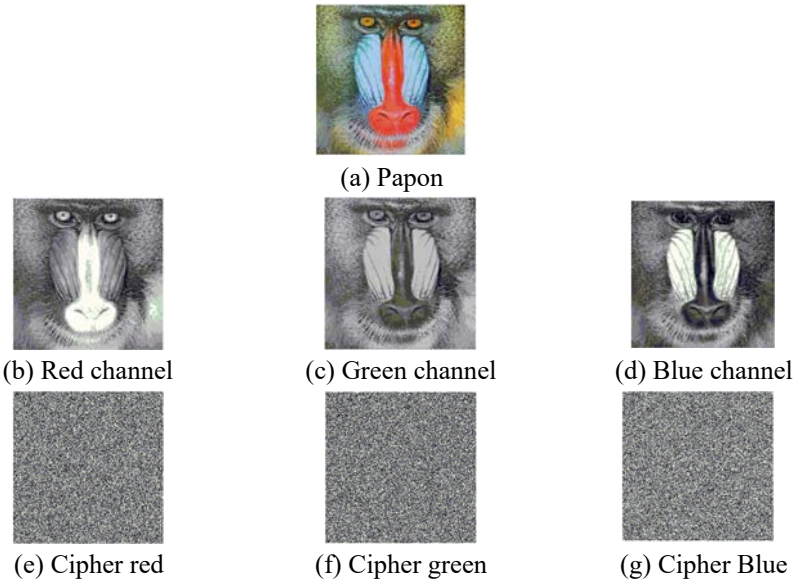
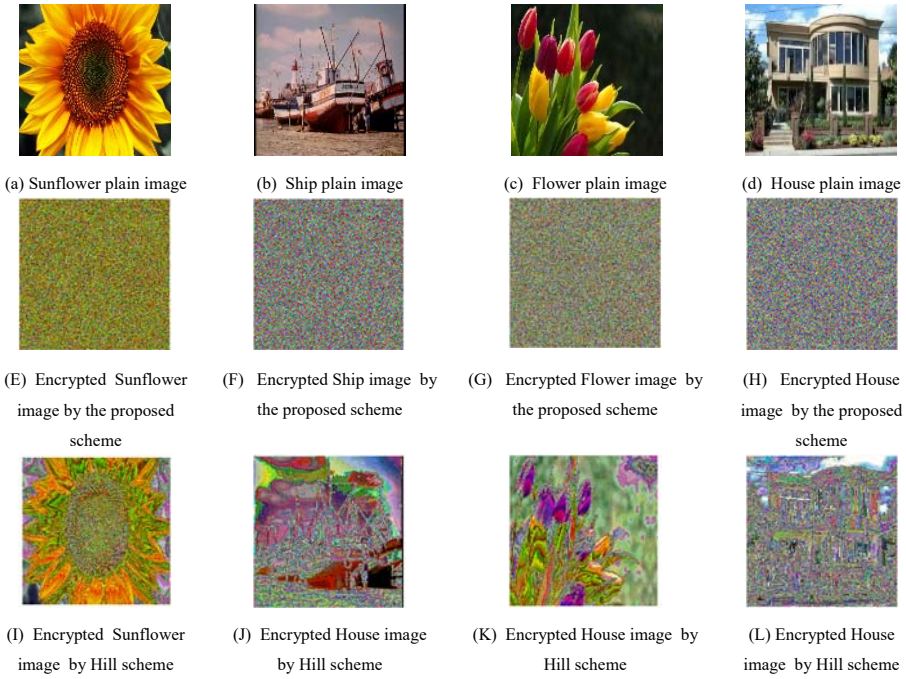


Figure3. Encrypted three channels of Papon color image.

4.1 Quality of encryption:

A comparison of quality between the proposed encryption scheme and the Hill cipher scheme is shown in Figure.4. The four secret images Sunflower, Boat, Flower, and House images shown in Figure.4 (a-d) and their corresponding encrypted images using the proposed algorithm are shown in Figure. 4 (E-H). Also Figures 4 (I-L) show the encrypted images using Hill cipher. It is shown from results that the proposed scheme has a good encryption quality for color images than as in Hill ciphers algorithm.



(a) Sunflower plain image (b) Ship plain image (c) Flower plain image (d) House plain image

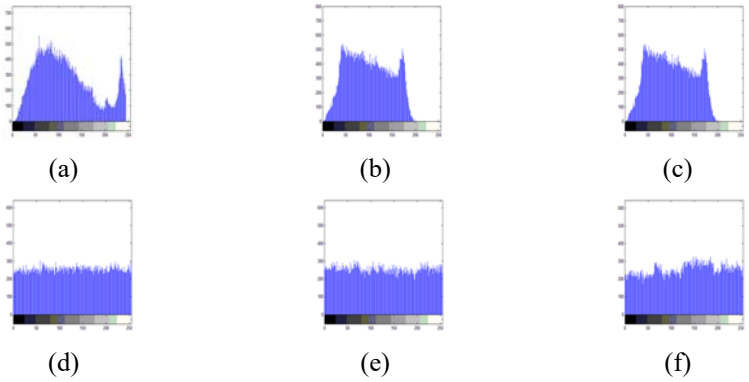
(E) Encrypted Sunflower image by the proposed scheme (F) Encrypted Ship image by the proposed scheme (G) Encrypted Flower image by the proposed scheme (H) Encrypted House image by the proposed scheme

(I) Encrypted Sunflower image by Hill scheme (J) Encrypted House image by Hill scheme (K) Encrypted House image by Hill scheme (L) Encrypted House image by Hill scheme

Figure 4: Quality of the proposed scheme encryption vs AES and Hill cipher encryption scheme.

4.2 **Confusion and diffusion properties:** To prove the confusion and diffusion of the proposed scheme, two statistical analyses are performed by testing. These statistical analyses are as correlations of adjacent pixels between pixels of the ciphered images, and the histogram of the original image and of their corresponding cipher images. These properties allow the scheme to strongly resist statistical attacks.

- **Histogram of the plain and cipher images:** Figure. 5 shows the histogram of the Papon plain red, green, and blue images (shown in Figure.3 (b-d)) and the corresponding ciphered images is shown in Figure.3(e-g) . It is immediate to observe that the histograms of the cipher image are significantly different from the plain image histogram and it is fairly uniform.



(a) (b) (c)

(d) (e) (f)

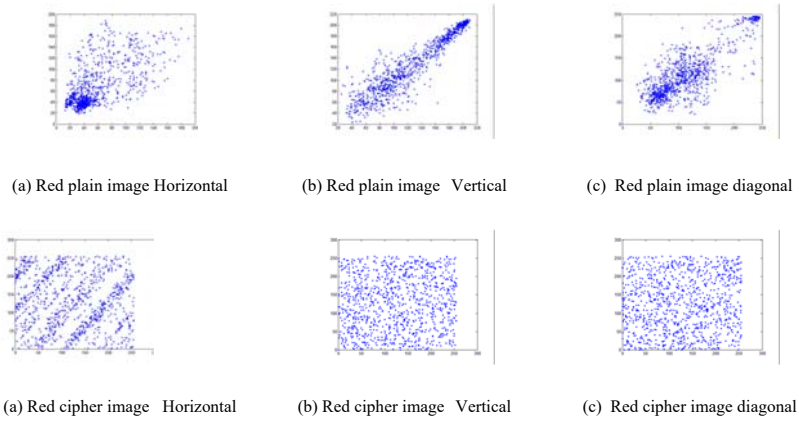
Fig.5: (a-c) Histogram of red, green, and blue plain image, (d-f) Histogram of red, green, and blue corresponding ciphertext.

- **Correlations of adjacent pixels:** In order to test the correlation cipher image, a randomly selected 1000 pairs of two horizontally, vertically, and diagonally adjacent pixels have been selected. The correlation coefficient of each pair of cipher are computed in Table .1. The correlation coefficient for the horizontally, vertically and diagonally adjacent pixels of the four cipher images Sunflower, Boat, Flower, and House images (Figure.4. (E-H)) are shown in table.1. The values of ciphered images correlation coefficient are near to 0.

Table.1: Correlation coefficients of two adjacent 1000 pairs of ciphered images pixels.

	Sunflower cipher image	Boat cipher image	Flower cipher image	House cipher image
Horizontal	−0.0152	-0.0491	0.0180	−0.0152
Vertical	−0.0555	0.00995	−0.0608	−0.0555
Diagonal	−0.0766	−0.0368	0.0023	−0.0766

Finally, Figure.6 presents the correlation distributions of two pair vectors of the horizontal, vertically and diagonal adjacent pixels in the plain blue channel Papon plain image (Figure. (3.c)) and its corresponding cipher images (Figure. (3.f)). As expected, the adjacent pixels in the cipher image are randomly distributed along horizontal, vertical, and diagonal. Nevertheless, for the pixels distribution of horizontal, vertical, and diagonal plain images due to the fact that the those pixels have a very near value. The distribution of adjacent pixels for the ciphered images seems to be random. The proposed scheme is identical in terms of confusion and diffusion properties.



(a) Red plain image Horizontal (b) Red plain image Vertical (c) Red plain image diagonal

(a) Red cipher image Horizontal (b) Red cipher image Vertical (c) Red cipher image diagonal

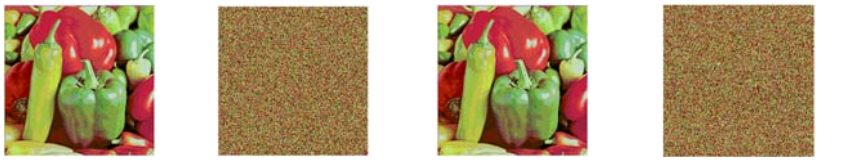
Figure.6: Correlation of the two plain and cipher images

4.3 Sensitivity analysis:

In this section, two means of the sensitivity analysis are measured. The first is the key sensitivity and the second is sensitivity of plaintext to cipher which is known as Differential attack. The key sensitivity means the change rate of the cipher-image pixels if a slight bit of the key is changed. Also, the sensitivity analysis of plaintext to cipher, or differential attacks, tests the influence of changing a single pixel in the plain image on the ciphered image bytes.

For comparing the results, Figure 6 shows the effectiveness of changing only one bit key, or choosing wrong key lead to different result for obtaining the corresponding plain image.

Figure 7 shows the differences between the two ciphered images for two identical images with only one difference pixel. It is shown there is a full difference between two ciphered images.



(a) Plain image (b) Cipher image (c) Recovered image with correct secret key (d) Recovered image with a bit difference key

Figure.7: Image deciphering with correct secret key VS a secret key with a bit difference key

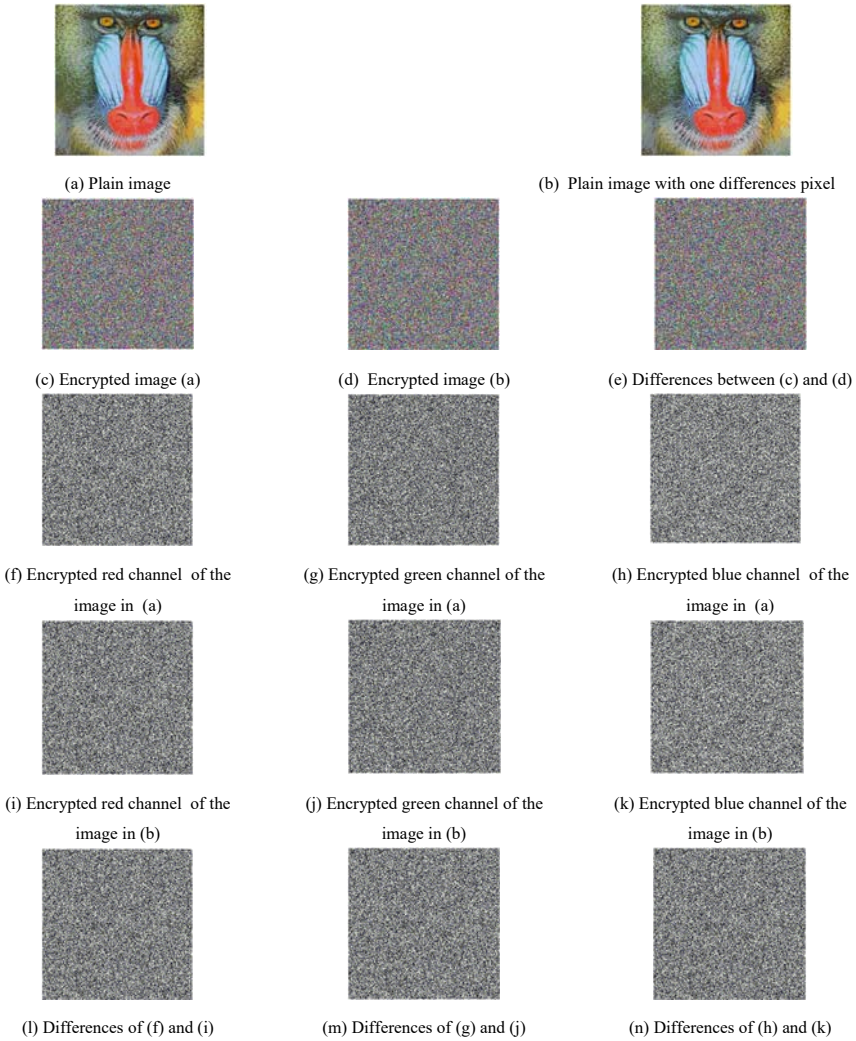


Figure.8: Differences between two encrypted images with only one pixel differences.

5. Conclusion

In this paper, Hill cipher and cellular neural network are combined to be used as new encryption scheme for color images. The proposed scheme depends on two phases permutation and diffusion properties to have a most likely good encryption quality. The results and analysis indicate the proposed system has satisfying a good quality for image encryption and also ensures the sensitively of key and hardness against differential analysis.

REFERENCES

[1] K. Adinarayana Reddy, B. Vishnuvardhan, Madhuviswanatham, A. V. N. Krishna,'A Modified Hill Cipher Based on Circulant Matrices Procedia TechnologyVolume 42012Pages 114-118
[2] Salim M. Wadi, Nasharuddin Zainal 'Rapid Encryption Method based on AES Algorithm for Grey Scale HD Image Encryption', Procedia TechnologyVolume 112013Pages 51-56.
[3] Singh N, Sinha A. Chaos based multiple image encryption using multiple canonical transforms. Opt Laser Technol 2010;42(5):724–31.
[4] KOCAREV L, Lian S, editors. Chaos based cryptography. Springer; 2011.
[5] A.A. Abdo a, Shiguo Lian, I.A. Ismail, M. Amin, H. Diab, "A cryptosystem based on elementary cellular automata ", Commun Nonlinear Sci Numer Simulat 18 (2013) 136–147.
[6] M.Kaur, D.Singh,n, K.Sun, U.Rawat,'Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map', Future Generation Computer Systems. 107 (2020)333-350
[7] Yong Zhang, The fast image encryption algorithm based on lifting scheme and chaos Information Sciences. 520(2020) 177-194.
[8] Y,Sun, Hao.Z, X.Wang, X-qing Wang, P.Yan,'2D Non-adjacent coupled map lattice with q and its applications in image encryption', Applied Mathematics and ComputationVolume 373(2020) 125039
[9] Lili Liu, Qiang Zhang, Xiaopeng Wei, A rgb image encryption algorithm based on dna encoding and chaos map, Comput. Electric. Eng. 38 (5) (2012) 1240–1248.
[10] Zhengjun Liu, Min Gong, Yongkang Dou, Feng Liu, Shen Lin, Muhammad Ashfaq Ahmad, Jingmin Dai, Shutian Liu, Double image encryption by using arnold transform and discrete fractional angular transform, Opt. Lasers Eng. 50 (2) (2012) 248–255.
[11] Nanrun Zhou, Yixian Wang, Lihua Gong, Hong He, Wu. Jianhua, Novel singlechannel color image encryption algorithm based on chaos and fractional fourier transform, Opt. Commun. 284 (12) (2011) 2789–2796.
[12] J.X. Chen, Z.L. Zhu, C. Fu, L.B. Zhang, Y. Zhang, Cryptanalysis and improvement of an optical image encryption scheme using chaotic a Baker map and double random phase encoding, J. Opt. 16 (2014) 125403.

[13] C. Li, K.T. Lo, Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, Signal Process 91 (2011) 949–954.
[14] Li Chengqing, Li S, Zhang D, Chen Guanrong. Chosen-plaintext cryptanalysis of a clipped-neural-network-based chaotic cipher, Part II (ISNN 2005). Lect Notes Comput Sci 2005;3497:630–6.
[15] X. Wei, L. Guo, Q. Zhang, J. Zhang, S. Lian, A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system, J. Syst.Software 85 (2012) 290–299.
[16] M. Kumar, A. lqbal, P. Kumar, A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography, Signal Process.125(2016): 187–202.
[17] X. Huang, G. Ye, An image encryption algorithm based on hyper-chaos and DNA sequence, Multimed. Tools Appl. 72 (2014) 57–70.
[18] He ZY, Zhang YF, Lu HT. The dynamic character of cellular neural network with applications to secure communication. J Commun 1999;20(3):59–67