International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-3, February 2014

Study and Analysis New Algorithm for Effective Cryptographic in Telemedicine Purposes Using Hill Cipher after Modification

Firas Shawkat Hamid , Thakwan Akram Jawad, Ersun Iscioglu

***Abstract*— Nowadays, digital exchanges of medical images are frequently used throughout the world in a fraction of a second via the Internet. These data can be read or modified during their transmission via a non-controlled channel. Therefore, it becomes very important to protect this private information against unauthorized viewers by using cryptography. This work presents a cryptography method that uses the properties of Hill Cipher algorithm for medical images.**

The fast evolution of digital data exchange, security information becomes much important in data storage and transmission. Image, which covers the highest percentage of the multimedia data, its protection is very important. This can be achieved by image encryption. As the use of digital techniques for transmitting and storing image are increasing, it becomes an important issue that how to protect the confidentiality, integrity, and authenticity of image. Each type of data has its own features; therefore various techniques which are discovered from time to time to encrypt the images should be used to protect confidential image data from unauthorized access and to make images more secure. Image encryption techniques scrambled the pixels of the image and decrease the correlation among the pixels, so that we will get lower correlation among the pixel and get the encrypted image. Encryption is used to securely transmit data in open networks. The Hill cipher algorithm is one of the symmetric key algorithms that have several advantages in data encryption. However, a main drawback of this algorithm is that it encrypts identical plaintext blocks to identical ciphertext blocks and cannot encrypt images that contain large areas of a single color. Thus, it does not hide all features of the image, which reveals patterns in the plaintext. Moreover, it can be easily broken with a known plaintext attack revealing weak security. This paper presents a variant of the Hill cipher that overcomes these disadvantages, has been proposed new encryption algorithm using modify the existing Hill cipher to decrease the susceptibility to known plaintext attacks. This is achieved by randomizing the information locations for the whole image. So, even if the attacker can guess the key, the decryption still give false information. Both of Hill image cipher and the proposed modification on it (termed MHill in this paper) are suitable for all images block encryption. The proposed algorithm is carried out via two approaches that is through comparative study and statistical analysis. Results from this comparative have shown that Hill cipher with randomized approach has greatest the Number of Pixels Changed Rate (NPCR) and the Unified Averaged Changed Intensity (UACI) value are two most common

quantities used to evaluate the strength of image encryption algorithms/ciphers with respect to differential attacks and its Correlation Coefficient Factor (CCF) value is the closest to zero for encryption and closest to one for decryption as well as the Deviation Factor. Visually and computationally, experimental results demonstrate that the proposed variant (Hill cipher with randomized approach) yields higher security and significantly superior encryption quality compared to the original one. Testing results between the encrypted and decrypted image and their histogram have shown the algorithm effectiveness.

***Index Terms*—Cryptography, Encryption, Decryption, Modified Hill image Cipher, Hill Cipher with randomized approach, NPCR, UACI, CCF.**

I. INTRODUCTION AND LITERATURE REVIEW

Today web is going towards the multimedia data in which image covers the highest percentage of it. But with the ever-increasing growth of multimedia applications, security is an important aspect in communication and storage of images, and encryption is the way to ensure security. Image encryption techniques try to convert original image to another image that is hard to understand and to keeps the image confidential between users, in other word, it's important that without decryption key no one can access the content. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication; etc. Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons: One is that the image size is almost always much greater than that of text. Therefore, the old system takes more time for encrypting the image data directly. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data [1], [2].

A technique in which secret messages are transferred from one person to another over the communication line, the process is called Cryptography. Cryptography technique needs some algorithm for encryption of data. Cryptography (or cryptology; from Greek κρσπτός, "hidden, secret"; and γράφειν, graphein, "writing", or - λογία, -logia, "study", respectively) is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). data security is a progressively significant difficulty.

Manuscript published on 28 February 2014.
* Correspondence Author (s)
Dr. Firas Shawkat Hamid, Head of Department of Computers Systems in Technical Institute Mosul/ Foundation Of Technical Education/ Ministry Of higher Education and Scientific Research/ Iraq.
Thakwan Akram Jawad, Engineer in Engineering College / Mosul University/Iraq.
Assist. Prof. Ersun Iscioglu, Head of Department of Computer and Instructional Technology Education / Eastern Mediterranean University.Iraq.

A cryptographic algorithm, also called a cipher, is the mathematical function used for encryption and decryption. (Generally, there are two related functions: one for encryption and the other for decryption). Cryptography is the art or research including the values and procedures of changing an intelligible note (plaintext) into one that is unintelligible (cipher text) and then retransforming that message back to its initial pattern [3], [4].

More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, and authentication. The difference between Plain Text and Cipher text is that the Plaintext is information a sender wishes to transmit to a receiver, while Cipher text (or cypher text) is the result of encryption performed on plaintext using an algorithm, called a cipher. Encryption is the process of transforming the image into some other image using an algorithm so that any unauthorized person cannot watch it. Only the person who has a key (anti of that algorithm) can watch that image [5]. Cryptographic algorithms are broadly divided into two categories [6]:

1) Secret key cryptography (symmetric key cryptography): In this, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key, as shown in Figure 1.

2) Public key cryptography, also called asymmetric key cryptography. It used encryption and decryption algorithm pair. With public key cryptography, keys work in pairs of matched public and private keys.

In the present era of Information Technology, transmission of information in a secured manner is the primary concern of all agencies. Security is highly essential, as intruders are very keen to rob the information with all their might and intelligence. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. The objective of this paper is to encrypt an image using a technique different from the conventional Hill Cipher.

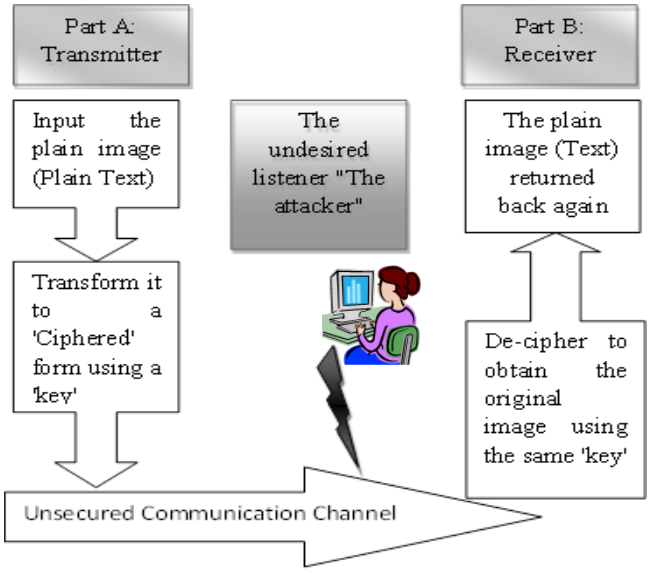

Figure 1 The Symmetric cipher system structure

S. Zhang and M. A. Karim in 1999, have proposed a new method to encrypt color images using existing optical encryption systems for gray-scale images. The color images are converted to their indexed image formats before they are encoded. In the encoding subsystem, image is encoded to stationary white noise with two random phase masks, one in the input plane and the other in the Fourier plane. At the decryption end, the color images are recovered by converting the decrypted indexed images back to their RGB (Red-Green-Blue) formats. The proposed single-channel color image encryption method is more compact and robust than the multichannel methods. This technique introduces color information to optical encryption [7].

In 2000, Yi Kai-Xiang and Sun Xing et a.l give an image encryption algorithm based on chaotic sequence. First, the real number value chaotic sequences using the key value is generated. Then it is dispersed into symbol matrix and transformation matrix. Finally the image is encrypted using them in DCT domain [8].

Shujun Li et al. in 2002, have pointed out that all permutation only image ciphers were insecure against known/chosen plaintext attacks. In conclusion, they suggested that secret permutations have to be combined with other encryption techniques to design highly secured images [9].

Sinha and K. Singh have proposed in 2003 a new technique to encrypt an image for secure image transmission. The digital signature of the original image is embedded to the encoded version of the original image prior to transmission. Image encoding is done by using an appropriate error control code, such as a Bose-Chaudhuri Hochquenghem (BCH) code. At the receiver end, after the decryption of the image, the digital signature can be used to verify the authenticity of the image [10].

In 2004, Maniccam S.S. and Bourbakis N G. proposed image and video encryption using SCAN patterns. The image encryption is performed by SCAN based permutation of pixels and a substitution rule which together form an iterated product cipher [11].

Sinha A. and Singh K. in 2005, proposed an image encryption by using Fractional Fourier Transform (FRFT) and JigSaw Transform (JST) in image bit planes [12].

In 2008, Sastry and Shankar proposed a modified Hill Cipher for with interlacing and iterations. The Use of interlacing iterations in ciphering and decomposition iterations for decryption makes the process complex but secure. Here, interlacing is the exchange of binary bits of the message matrix element. They designed the interlacing and decomposition. According to the researchers, this method designed to be used specifically in saving the biometrics templates to increases the security [13]. Mitra A et al. in the same year, have proposed a random combinational image encryption approach with bit, pixel and block permutations [14].

In 2009, Panigrahy Jena, Korra, and Sanjay Kumar Jena generated algorithm to overcome disadvantages of the other related algorithms. As it was mentioned before, in hill-cipher encryption algorithm, which used self-invertible key matrix, there are the problem of encryption of image with the existing of same color or pattern in the picture, while in advance hill cipher applied an involutory key matrix as encryption the color image can be easily encrypted.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Although AdvHill is a robust and more secure than the traditional Hill algorithm for ciphering images, it failed to return back the images of small objects with wide backgrounds [15]. As well as in the year 2009, H. H. Nien, W. T. Huang, C. M. Hung, S. C. Chen, S. Y. Wu proposed a Hybrid Image Encryption using Multi-Chaos-System,
this method uses hybrid encryption technique for the color image based on the multichaotic-system which combines Pixel-Chaotic-Shuffle (PCS) and Bit-Chaotic-Rearrangement (BCR) and increases the key space of images [16] and in the same year, Zhi-Hong Guan et al. have presented a new image encryption scheme, in which shuffling the positions and changing the grey values of image pixels are combined to confuse the relationship between the cipher image and the plain image [17].
In 2010, Zhu Yu, Zhou Zhe, Yang Haibing, Pan Wenjie, Zhang Yunpeng proposed a method Chaos-Based Image Encryption Algorithm using Wavelet Transform, in this paper the algorithm uses the wavelet decomposition concentrating image information in the high-frequency sub-band image, and then encryption is applied for the sub-band image. After a wavelet reconstruction is introduced in order to spread the encrypted part throughout the whole image. A second encryption process is used to complete the encryption
process [18].
Zhengjun Liu, Lie Xu, Jingmin Dai, Shutian Liu in 2011, proposed an image encryption algorithm based on fractional Fourier transform. A local random phase encoding is introduced into this algorithm. The data at the local area of complex function is converted by fractional Fourier transform [19].
In 2012, Panduranga H T and Naveen Kumar S K tried another strategy for adapting the Hill cipher to be suitable for image cipher. They implied that the key should be of minimum eight characters. Later, all keys elements are replaced by predefined 4 out of 8 code vales. Then it is used as a basic block in self-invertible matrix generator. This research was entitled "Advanced Partial Image Encryption using Two-Stage Hill Cipher Technique" with best results [20]. Somdip Dey in the same year proposed a method, SD-AEI, for image encryption, which is an upgraded module for SD-AEI combined image encryption technique and basically has three stages: 1) In first stage, each pixel of image is converted to its equivalent eight bit binary number and in that eight bit number, the number of bits, which are equal to the length of password are rotated and then reversed; 2) In second stage, extended hill cipher technique is applied by using involutory matrix, which is generated by same password used in second stage of encryption to make it more secure; 3) In third stage, the whole image file is randomized multiple number of times using Modified MSA Randomization encryption technique and the randomization is dependent on an unique number, which is generated from the password provided for encryption [21].
In this paper we proposed algorithm to enhance the Hill cipher so it can be used to cipher images efficiently. The basic concept of the modification is to change the illumination quantization and then randomly change the places of pixels before using the Hill cipher. Each step in this work has is used for a certain purpose to promote the Hill cipher and make it reliable and convenient to be applied on more complicated matrices. In other words, to make Hill cipher suitable for ciphering the images especially for those of small objects lying on unvarying backgrounds. The following sections describe each process of the algorithm. The aim of this work to overcome this kind of security problems in image cipher but using Hill technique preceded by extra steps. As the Hill cipher is the core of this methodology, this algorithm is termed as Modified Hill Cipher (MHill) for simplicity as shown in Figure 2.

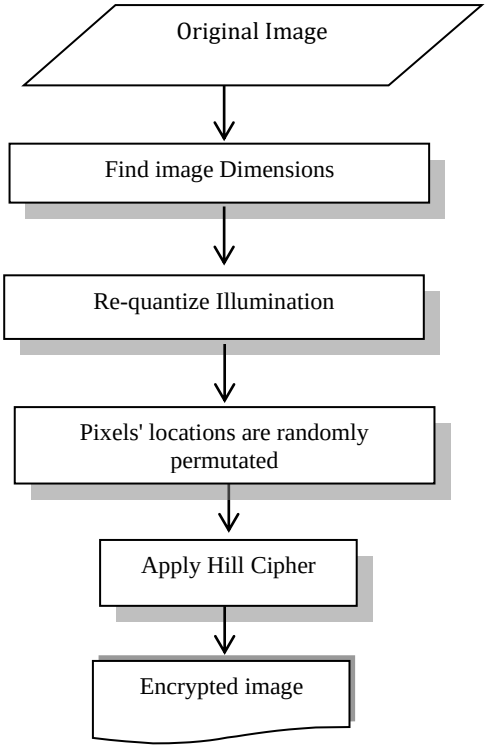

FIGURE 2 THE PROPOSED MHILL CIPHERING ALGORITHM

II. THE CONCEPTS OF IMAGE ENCRYPTION IN TELEMEDICINE

Telemedicine changes the way patients are treated, from the traditional methods of a person care to remote care; it may also improve healthcare access to areas where it was essentially not available in the past. It allows for a virtual communication, using real – time audiovisual information transmitted over, between a patient and a physician at two different sites. Telemedicine totally depends on public network, it is a confluence of Communication Technology, Information Technology, Biomedical Engineering and Medical Science and it is an effective solution for providing healthcare in the form of improved access and reduced cost to the rural patients. Telemedicine can enable ordinary doctors to perform extra-ordinary tasks. Telemedicine enable patients to communicate through video conferencing, audio, images and data. The presence of a network has prompted new problems with security and privacy [22], [23].The main requirement in order to communicate with images and video is a secured and reliable means, so that present situation demands highly secured details of patients. Medical signal is supposed to contain sensitive health information of the patient, due to the advancement in the technologies; securities of the data have become a critical issue.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

New approaches in encryption techniques are required to be developed for effective data encryption and multimedia applications. For future internet applications on wireless networks, besides source coding and channel coding techniques, cryptographic coding techniques for multimedia applications need to be developed [23]. Therefore, in this paper we proposed modern encryption technique.

Image encryption is necessary for future multimedia and Telemedicine applications. Password codes to identify individual users will likely be replaced are biometric images of CT scan and MRI scan.

However, such information will likely be sent over a network. When such images are sent over a network, an eavesdropper may duplicate or reroute the information. By encrypting these images, a degree of security can be achieved. Furthermore, by encrypting noncritical images as well, an eavesdropper is less likely to be able to distinguish between important and non-important information. Image encryption can also be used to protect privacy. An example for image encryption to protect privacy is in medical imaging applications. Recently, in order to reduce the cost and to improve service, electronic forms of medical records have been sent over networks from laboratories to medical centres. According to the law, medical records, which include many images, should not be disclosed to any unauthorized persons. Medical images, therefore, should be encrypted before they are sent over networks [24]-[26].

A. The Difference between Image Encryption and Text Encryption

Text encryption algorithms are not directly implemented to images because image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable [27], [28].

B. Architecture of Image Encryption Model

Encryption techniques are generally categorized into following three [29]-[31]:

1) Position permutation techniques: In this technique the order of the pixels of an image is changed so that the information is invisible.

2) Value transformation techniques: In this the weights and biases of the network are set according to a binary sequence generated from a chaotic system, for encryption or decryption of each signal element.

3) Combination: This technique is combination of both position permutation and value transformation. Position permutation and value transformation can be combined. In this technique first pixels are reordered and then a key generator is used to substitute the pixel values.

III. THE HILL CIPHER FOR IMAGE ENCRYPTION METHOD

Hill cipher can be adopted to encrypt grayscale and colour images, For grayscale images, the modulus will be 256 (the number of levels is considered as the number of alphabets). In the case of colour images, the colour image is first decomposed into (R-G-B) components. Secondly, each component (R-G-B) is encrypted separately by the algorithm. Finally, the encrypted components are concatenated together to get the encrypted colour image [32].

Hill cipher is the first polygraphic cipher. A polygraphic cipher is a cipher where the plaintext is split up into assemblies of adjacent latters of the same fixed extent m, and then each such group is changed into a distinct assembly of m letters. This polygraphic feature expanded the speed and throughput of hill cipher [33], [34].

the Hill cipher did not work efficiently for ciphering images. This fact came from the reality that images sometimes have many repetitive values if it contains low details [32].

It is intended in this work to use the Hill cipher with modifications that lead to proper cipher system making a full use of the advantages of the Hill cipher security.

it is intended to use many different quality metrics in this research. In fact, those metrics, side by side with visual inspection, paved the way to choose the better algorithm from many tried strategies [35].

the Hill cipher cannot encrypt the image perfectly. However, the Hill cipher is used after conditioning it to suite the image characteristics. The powerful attack immunity aspect of the Hill cipher made the researchers keen to adopt it for image ciphering system [35].

This cipher technique was designed by the mathematician Lester Hill in 1929. Hill cipher is the first polygraphic cipher. A polygraphic cipher is a cipher where the plaintext is split up into assemblies of adjacent latters of the same fixed extent m, and then each such group is changed into a distinct assembly of m letters. This polygraphic feature expanded the speed and throughput of hill cipher [32].

The core of Hill cipher is matrix manipulation. For encryption, algorithm takes m successive plain text letters and rather than of that substitutes m cipher letters. Its linear algebra formula is C= K × P (mod m), where C comprises the ciphertext block, P comprises the plaintext impede and K is the key. The key, K is in the pattern of matrix. Thus, for decryption, an inverse key matrix, (K-1) is needed [36].

In Hill cipher, each character is assigned a numerical value that is starting with 0 (zero). The numerical value is illustrated like a=0, b=1,……..z=25 [4, 5]. The substitution of cipher text letters in the location of plaintext letters directs to m linear equation. For m=3, the system can be described as follows [36], [37]:

$$\begin{aligned} C_1 &= (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \bmod 26 \\ C_2 &= (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \bmod 26 \\ C_3 &= (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \bmod 26 \end{aligned} \quad (1)$$

This case can be conveyed in terms of column vectors and matrices. This case can be described as follows:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{bmatrix} K_{11}K_{12}K_{13} \\ K_{21}K_{22}K_{23} \\ K_{31}K_{32}K_{33} \end{bmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \quad (2)$$

We can compose easily as C = KP, where C and P are pillar vectors of extent 3, representing the plaintext and ciphertext respectively, and K is a 3×3 matrix, which is the encryption key.

(3)

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

All procedures are performed mod 26 here. Decryption needs utilizing the inverse of the matrix K. K^{-1} is applied to the ciphertext, and then the plaintext is recovered. In general term we can write as follows [37]:

For encryption: $C = E_k(P) = K_p$

For decryption: $P = D_k(C) = K^{-1}C = K^{-1}K_p$ (4)

IV. THE PROPOSED ALGORITHM FOR MODIFICATION ON HILL CIPHER (MHILL)

Since the Hill cipher is based on matrix multiplication and inverses, it is simply computed and it overcomes the frequency distribution problem of other algorithms used before. This linearity make Hill cipher susceptible even to simple attacks. If an attacker intercepted enough plaintext and cipher text pairs, a linear system could be set up to calculate the encryption matrix [37]. Another problem associated to the Hill cipher's linearity is that the Hill cipher encodes every identical plain image to the same cipher image matrix. These problems arise significantly with images that contain small objects with uniform background [35].

The proposed algorithm (MHill) to enhance the Hill cipher is to randomly change the places of pixels using two small lookup tables. These tables contain the new map for rows and columns separately. The first table contains randomly disordered numbers of the same size of the row as shown in Table 1, while the second table contains randomly disordered numbers same size of the column as shown in Table 2. The following table shows an example:

Table 1: Permutation map for rows of the image

Old Row index	1	2	3	4	5	6	7	…….	R_{max}
New Row index	11	5	22	7	1	16	4	…….	N_1

Table 2: Permutation map for columns of the image

Old column index	1	2	3	4	5	6	7	…….	C_{max}
New column index	19	25	12	30	51	2	28	…….	N_2

Where R_{max} is the maximum row index for the plain image, C_{max} is the maximum column index for the plain image, N_1 and N_2 are random integers.

Each pixel in each layer of the RGB layers is put in a new location depending on those two tables. For instance, according to the example tables above the pixel in location (1,1) is moved to location (11,19) while the pixel in (1,2) is moved to (11,25). This permutation will increase security by increasing the immunity to known-plain text attacks. This is because even if the attacker expected the output of the cipher operation, it would be hard for him to generate the permutation tables.

The random permutation of pixel locations was achieved by MATLAB using the following code:

```
[r c]=size(Image);
 for i=1:r
    for j=1:c
       img(i,j)=Image(new_row(i),new_colomn(j));
    end
end
```

Where (Image) is the input image, (new_row) and (new_colomn) are vectors representing the tables of random permutation for rows and columns respectively.

Although the permutation tables are generated in the sending side, the receiver has to know them as well. Those tables could be altered for each iteration or according to some basis that the transmitter and the receiver agree. Those basis that the sender and receiver can adopt may be time basis or subject basis.

It is clear that decipher is achieved by reversing the cipher procedure. So, to decrypt the ciphered image according to the proposed MHill algorithm, the receiver should apply following steps:

1) The first step in decipher is to calculate the deciphering key, which is the inverse of the key matrix.

2) As the ciphering operation ends with Hill cipher, the decipher starts with Hill decipher. It is the same operation of Hill cipher (Equation 5) except that the key used in decipher is (K_D) rather than (K) and the plain image (P) will be replaced by the ciphered image (C).

$$C = \begin{bmatrix} K_{11} & K_{12} & K_{13} & K_{14} \\ K_{21} & K_{22} & K_{23} & K_{24} \\ K_{31} & K_{32} & K_{33} & K_{34} \\ K_{41} & K_{42} & K_{43} & K_{44} \end{bmatrix} \times \begin{bmatrix} P_{11} \\ P_{21} \\ P_{31} \\ P_{41} \end{bmatrix} (mod\ (256)) \qquad (5)$$

So, if the received ciphered image is (C_R), the output of Hill decipher will be (P_R) according to the following formula (6):

$$P_R = K_D \times C_R \ mod\ 256 \qquad (6)$$

3) The output of this process (P_R) should then recover its original pixel location to reverse the random permutation process in the ciphering. So, the receiver should know the mapping table that was designed in the ciphering side. This operation was implemented simply in MATLAB by the following piece of code, Where (Image) is the output from Hill de-cipher (P_R), (new_row) and (new_colomn) are vectors representing the tables of random permutation for rows and columns respectively.

```
[r c]=size(Image);
 for i=1:r
    for j=1:c
       img(new_row(i),new_colomn(j))=Image(i,j);
    end
end
```

4) The final process of deciphering is return the intensity back to its original quantization.

The following Figure 3 shows the flowchart of the proposed decipher process in the MHill algorithm.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

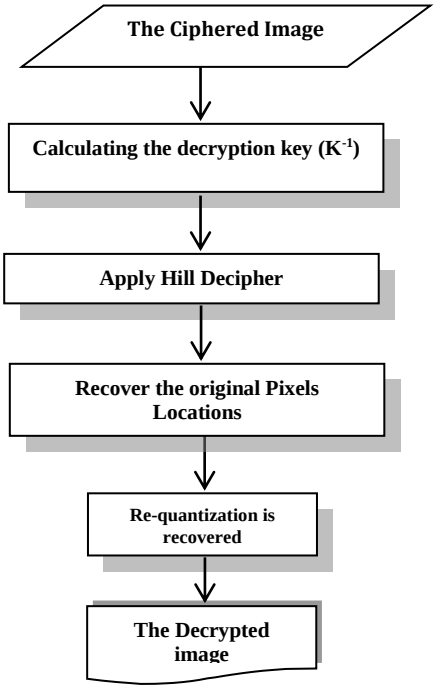

Figure 3: The proposed decipher process of the MHill algorithm.

V.ENCRYPTION MEASURING FACTORS

The visual inspection can prove that the features of the plain image has been removed but it is not enough. Therefore, quantitative evaluation metrics should be used to assess the degree of encryption [21, 22].

The factors that measure the quality of the ciphering techniques can be classified into two families [23]:

The first family measures the ability of the ciphering algorithm to produce an uncorrelated ciphered image. In This family, three metrics, which are the correlation coefficient (CC), the histogram uniformity, and the irregular deviation Factor (IDF), are considered. Where Correlation Coefficient is measured between the plain image and the encoded image while similarity is the correlation between the plain and the decoded images and PSNR is the peak signal to noise ratio of the encrypted image.

The second family evaluates the diffusion characteristics of the encryption algorithm. In this family, two metrics, which are (NPCR) and (UACI), are used. The NPCR is the Number of Pixels Change Rate between the ciphered image (C1) and another ciphered (C2) that came from the same plain image but one pixel is differed. The UACI is the Unified Average Change Intensity between (C1) and (C2). In general, those measurements were improved using the proposed MHill method.

A. The Correlation Coefficient Measuring Factor

The correlation measurement is typically used to measure how two signals are related or similar to each other's. So, it could be said that it can measure the similarity of two different signals. Regarding this project, the correlation coefficient is used to measure the difference of two images [38], [39].

This metric is used to assess the ciphering quality of any image cryptosystem. So that it calculates the correlation coefficient between pixels at the same locations in the plain and the ciphered images [24]. For two dimensional image, the correlation coefficient can be obtained from the equation (7) [38]:

$$C_C = \frac{\sum_m \sum_n (P - \bar{P})\,(C - \bar{C})}{\sqrt{(\sum_m \sum_n (P - \bar{P})^2)\;\;(\sum_m \sum_n (C - \bar{C})^2)}} \qquad (7)$$

Where $\bar{P}$ is the two dimensional mean of the plain image (original) P and $\bar{C}$ is the two dimensional mean of the ciphered image C.

More clearly, Correlation is a measure of the relationship between two variables. If the two variables are the image and its encryption, if the correlation coefficient equals one, that mean they are highly dependent (identical) and the encrypted image is the same as the original image and the encryption process failed in hiding the details of the original image. If the correlation coefficient equals zero, then the original image and its encryption are totally different and this mean the encrypted image has no distinct features and it is highly independent of the original image. So, the success of the encryption process means smaller values of the Correlation Coefficient Factor(CCF), which is measured by the following equation (8) [38]:

$$CCF = \frac{\mathrm{cov}(x,y)}{\sigma_x \sigma_y} = \frac{\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N} (x_i - E(x))^2}\sqrt{\sum_{i=1}^{N} (y_i - E(y))^2}} \qquad (8)$$

$$\text{where } E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (9)$$

x and y are grayscale pixel values of the original and encrypted images. Correlation Coefficient Factor decipher measures the similarity between the plain image P and the deciphered image P' using the correlation coefficient between them. The higher the similarity the better the algorithm.

B. The Irregular Deviation Measuring Factor

The irregular deviation factor measures the quality of encryption in terms of how much the deviation caused by encryption (on the encrypted image) is irregular.

The lower value of the IDF is the better the encryption quality. The steps of calculating this metric are [38], [39]:

- Calculate the absolute difference between the ciphered image and the plain (original) image in equation (10):

$$D = |P - C| \qquad (10)$$

- Calculate the histogram H of this absolute difference matrix, so that:

$$H = histogram(D)$$

- Find the mean value M_H of this histogram in equation (11):

$$M_H = \frac{\sum_0^{255} H}{256} \qquad (11)$$

- Determine the absolute of the histogram deviations from this mean value as follows in equation (12):

$$H_D(i) = |H(i) - M_H| \qquad (12)$$

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

- The irregular deviation factor IDF is calculated as shown in the equation (13):

$$IDF = \frac{\sum_0^{255} H_D(i)}{m \times n} \quad (13)$$

C. The Diffusion Measuring Factor

When it comes to measure the diffusion characteristics in any cipher algorithm, the common metrics usually designed to measure the influence of one-pixel change on the whole image. Two common measures may be used; the Number of Pixels Change Rate (NPCR) and the Unified Average Change Intensity (UACI) [38], [40]. Those metrics are designed as following [40]:

1) Compute two ciphered images CC_1 and CC_2. CC1 is the ciphered form of the plain image. While CC_2 comes from ciphering the same plain image but have only one pixel difference from the first plain image.
2) Obtain the gray-scale form of CC_1 and CC_2. Let $C_1(i,j)$ and $C_2(i,j)$ be the gray scale values of both CC_1 and CC_2 respectively.
3) The UACI measures the average intensity of difference between the two images as equation (14):

$$UACI = \frac{1}{m \times n}\left(\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right) \times 100\% \quad (14)$$

4) To measure the NPCR, first define a matrix D, with the same size as the images C_1 and C_2. Then, D(i,j) is determined from $C_1(i,j)$ and C_2 (i,j), so that:

$$D(i,j) = \begin{cases} 0, & if\ C_1(i,j) = C_2(i,j) \\ 1, & Otherwise \end{cases}$$

The NPCR is defined as equation (15):

$$NPCR = \frac{\sum_{i,j} D(i,j)}{m \times n} \times 100\% \quad (15)$$

When comparing two or more cipher algorithms, the algorithm of the higher values of UACI and NPCR is considered to be better than the others.

D. Execution Time

The execution time is the time required to cipher and/or decipher an image. The execution time depends on the complexity of the applied algorithm and on the computer system that run it. It is obvious that the smaller the execution time is, the better the cipher algorithm.

In this work, the computer that was used in the experiments was DELL Inspiron Notebook PC of Intel® Core ™ i3 2.4GHz CPU. The operating system was Windows 7 Ultimate 32-bit. The application used to simulate the MHill and the Hill cipher was MATLAB version 8.0.0.783 (R2012b).

VI. RESULTS AND DISCUSSION

The results of using the proposed which is termed MHill (Modified Hill) technique in this work was evaluated using different metrics including visual inspection. Those results were compared to the basic Hill image cipher on the same samples.

In our experimental results, several images are evaluated. These images are Lena.jpg as it is the reference image used in image processing research (it does not contain many high frequency components), Brain.jpg and Text.jpg as examples of an image containing very large areas of a single color, and, MRI.jpg as example of an image containing many high frequency components. We illustrate the numerical evaluations for encryption quality of the original Hill cipher and MHill cipher , respectively in Table 3 and the results of the six measuring factors are given in this table. Where CCF_e indicates the Correlation Coefficient Factor encryption measure, CCF_d indicates the Correlation Coefficient Factor decryption measure, *IDF* indicates the Irregular Deviation Factor measure and NPCR indicates the Number of Pixels Changed Rate value and the UACI indicates the Unified Averaged Changed Intensity value. The CCF_e closer to zero is the better; while for CCF_d (Similarity) the closer to one the better, while for *IDF* the smaller is the better and it does not give any misleading results and can be used alone to test the quality of encryption in the field of image encryption. So, if *IDF* agrees with other measuring factors, it will be good judging, otherwise the final decision on measuring the quality of the encryption algorithms will be based on *IDF* which is based on the irregular deviation on each pixel value. For MRI.jpg image as an example, with the smallest *IDF*, the proposed algorithm yields the better encryption. A brain.jpg and text.jpg example of the degree to which original Hill cipher can reveal patterns in the plaintext. Obviously, the proposed method MHill, can encrypt identical plaintext blocks to totally different ciphertext blocks, whereas the original Hill cipher cannot. That is, the proposed method has advantage in hiding data patterns over the original Hill. Visually, MHill is better than the original Hill cipher in hiding all features of the image, specially the image that contains large areas of a single color. In the other hand, the diffusion measurements (NPCR and UACI) show that there is a great progress in the results obtained from the proposed MHill and the Execution time in the Table 3 is the cipher time only. Definitely, the MHill takes more time than the Hill algorithm as it is more complicated.

The Table 3 shows the improvement that was achieved by using the MHill:

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

		Correlation Metrics Family			Diffusion Metrics Family		Other Metric
Sample	Ciphering Algorithm	CCFe	CCFd	IDF	NPCR %	UACI %	Time Execution (Sec)
lena.jpg	Hill Cipher	0.013	0.99	1.98	0.89	0.0002	0.33
	MHill Cipher	0.00016	1	0.37	99.63	33.46	0.39
MRI.jpg	Hill Cipher	0.0396	0.89	0.484	0.0109	0.0042	0.218
	MHill Cipher	0.0068	1	0.476	99.62	33.24	0.24
ECG.jpg	Hill Cipher	0.0859	0.99	0.491	0.0044	0.00168	1.16
	MHill Cipher	-0.0061	1	0.487	99.61	33.7	0.528
Brain.jpg	Hill Cipher	0.571	0.89	0.452	0.0071	0.0046	0.317
	MHill Cipher	-0.0097	1	0.419	94.52	38.57	0.36
Mamogram.jpg	Hill Cipher	0.238	0.915	0.435	0.0133	0.0054	0.147
	MHill Cipher	-0.0113	1	0.431	99.62	33.36	0.196
Text.jpg	Hill Cipher	0.807	0.87	0.63	0.04	0.046	0.0599
	MHill Cipher	-0.026	1	0.59	99.42	32.5	0.072

Table 3: MHill and Hill Quality Tests

The following figures show the resultant ciphering and deciphering with their histogram. It is obvious that the proposed method (MHill) has an advantage over the traditional Hill cipher specially with black text on white background images.

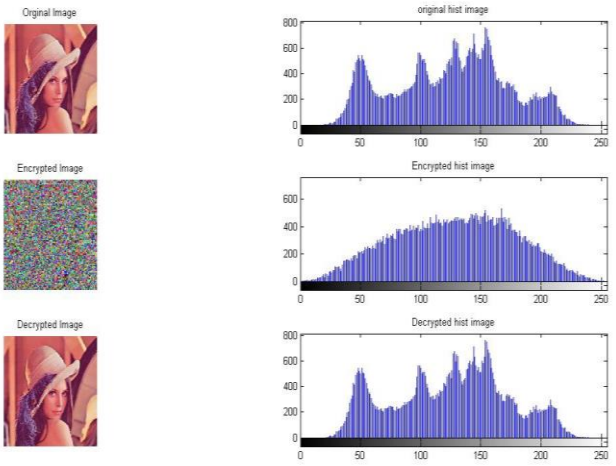

Figure 4.1: Hill cipher results for the sample lena.jpg (Results and Histograms of pixel permutation. (a) Original image. (b) Encrypted image.(c) Decrypted image.)

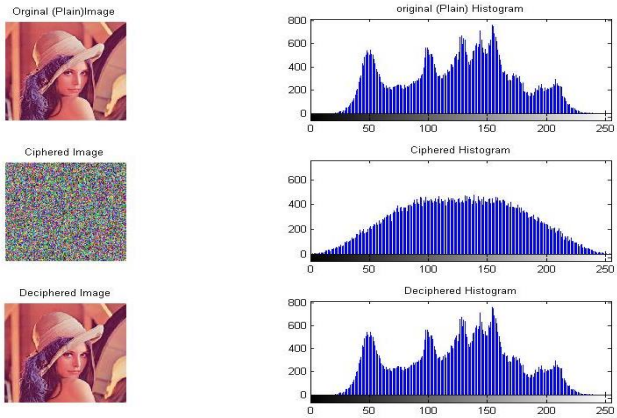

Figure 4.2: MHill cipher results for the sample lena.jpg (Results and Histograms of pixel permutation. (a) Original image. (b) Encrypted image.(c) Decrypted image.)

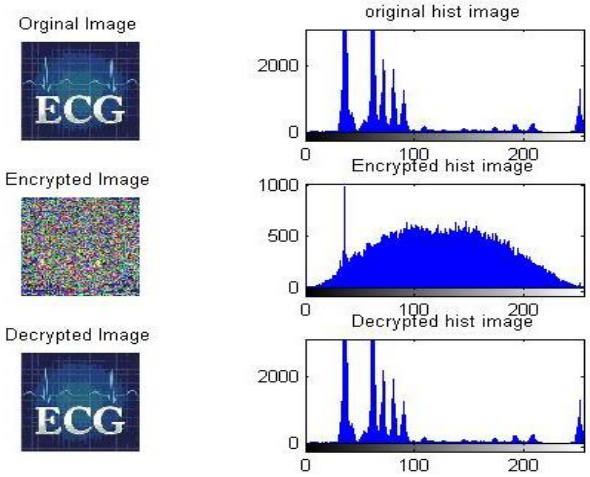

Figure 5.1:Hill cipher results for the sample ECG.jpg (Results and Histograms of pixel permutation. (a) Original image. (b) Encrypted image.(c) Decrypted image.)

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

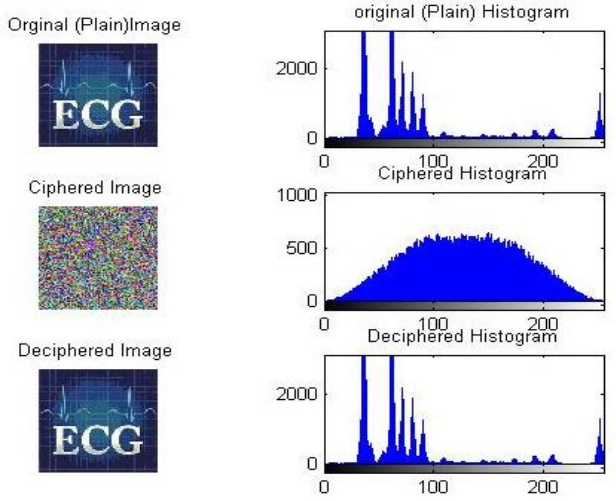

Figure 5.2:MHill cipher results for the sample ECG.jpg (Results and Histograms of pixel permutation. (a) Original image. (b) Encrypted image.(c) Decrypted image.)

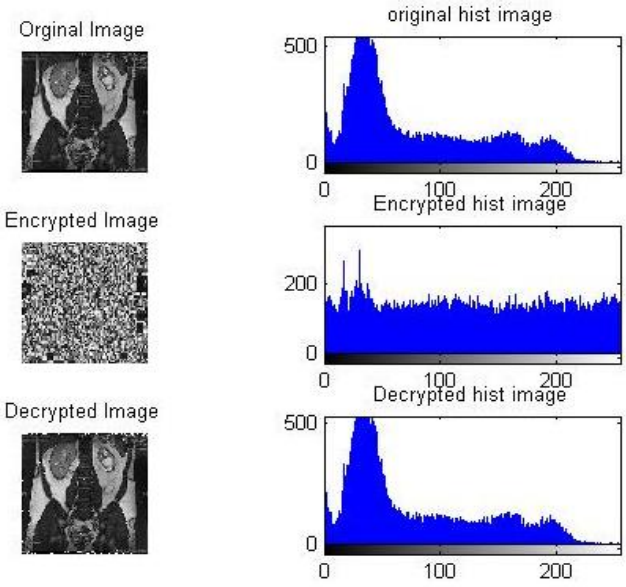

Figure 6.1:Hill cipher results for the sample MRI.jpg (Results and Histograms of pixel permutation. (a) Original image. (b) Encrypted image.(c) Decrypted image.)

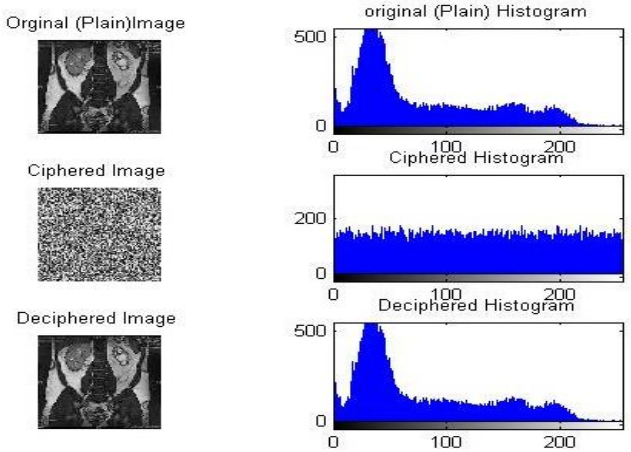

Figure 6.2:MHill cipher results for the sample MRI.jpg (Results and Histograms of pixel permutation. (a) Original image. (b) Encrypted image.(c) Decrypted image.)

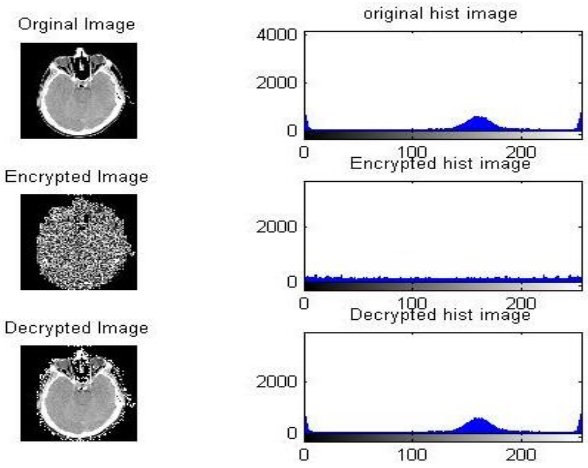

Figure 7.1:Hill cipher results for the sample Brain.jpg (Results and Histograms of pixel permutation. (a) Original image. (b) Encrypted image.(c) Decrypted image.)

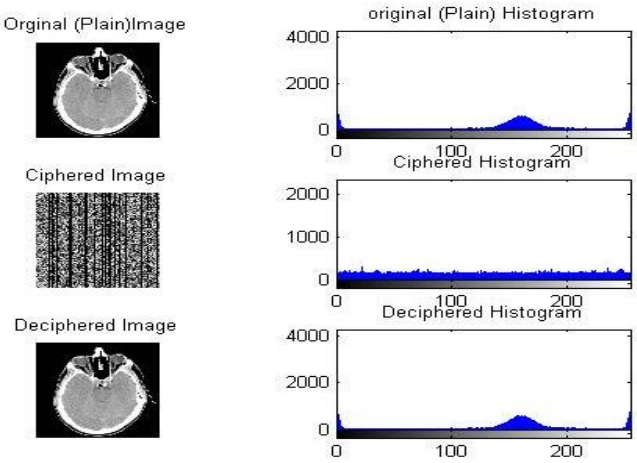

Figure 7.2: MHill cipher results for the sample Brain.jpg (Results and Histograms of pixel permutation. (a) Original image. (b) Encrypted image.(c) Decrypted image.)

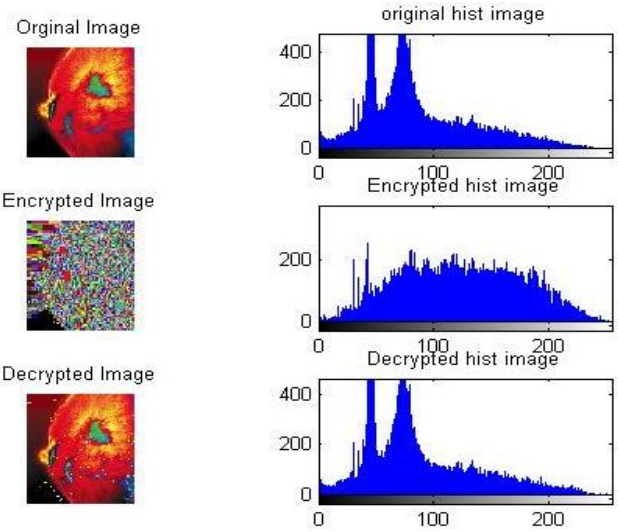

Figure 8.1:Hill cipher results for the Mamogram.jpg (Results and Histograms of pixel permutation. (a) Original image. (b) Encrypted image.(c) Decrypted image.)

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

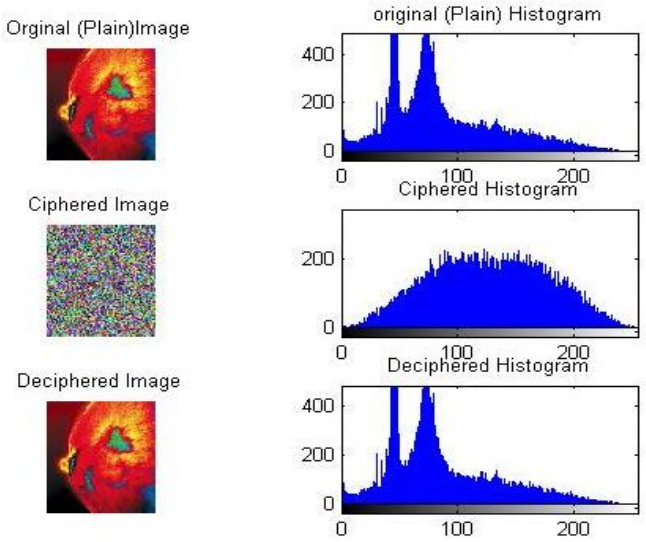

Figure 8.2:MHill cipher results for the sample Breast_Mamogram.jpg (Results and Histograms of pixel permutation. (a) Original image. (b) Encrypted image.(c) Decrypted image.)

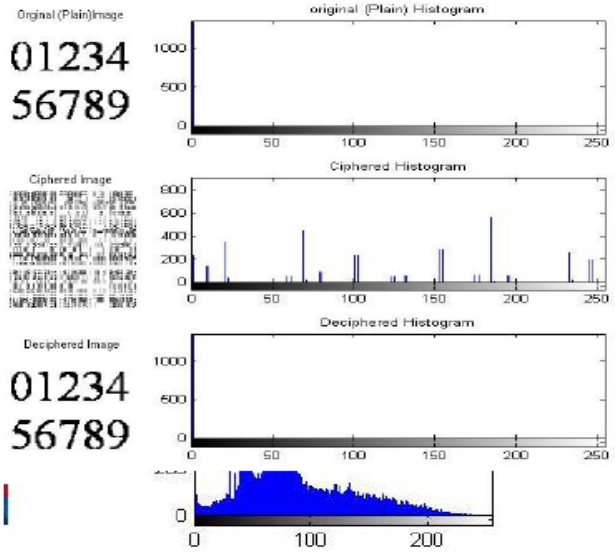

Figure 9.1:Hill cipher results for the sample Text.jpg (Results and Histograms of pixel permutation. (a) Original image. (b) Encrypted image.(c) Decrypted image.)

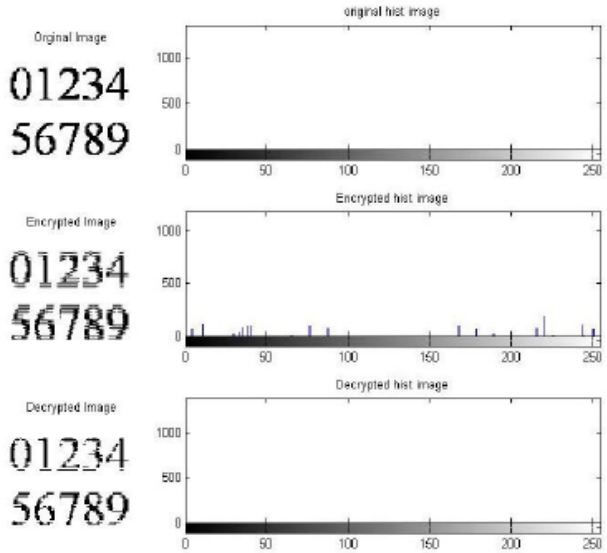

Figure 9.2: MHill cipher results for the sample Text.jpg (Results and Histograms of pixel permutation. (a) Original image. (b) Encrypted image.(c) Decrypted image.)

VII. CONCLUSION

Telemedicine and Cryptography is an emerging field, which is capturing the imagination of all the researchers worldwide. Thus, the scope of enhancements and improvements is enormous. Telemedicine technology uses wireless network for the transmission of medical information or data, so there is a need to provide security of the patient valuable data so that unauthorized user can not access and modify the data. To provide the privacy or security to the information, Hill Cipher algorithm have been developed. We have presented a modified version of Hill cipher. The basic Hill cipher uses a linear operations and modular mathematics and it is based on the fact that its power lies on its security. The ciphering key is a matrix, so the bruit-attacks will be weakened definitely.

However, using this technique to cipher an image faced a problem of the inability for hiding the image details. Many researchers have either tried another types of ciphering techniques or modified it. In spite of the fact that there are other methodologies, the Hill technique still attract researchers because it is the famous symmetric key encryption technique due to its simplicity and security. Roughly, all the Hill modifications are based on adding extra steps before applying it. Those steps usually designed to solve the problem of sustaining of the patterns and details of the image after applying the traditional Hill cipher on it. The proposed MHill algorithm in this research also designed in this way, although it was intended to have less computational expenses.

The proposed MHill strategy, compared with the conventional Hill, gave promising results in sense of producing uncorrelated ciphered images and improving the diffusion characteristics. When it comes to compare the proposed MHill with previous works of other researchers, the first one seems to be better. For example of recent works in 2012, they applied the Hill cipher twice in their system and the maximum NPCR was 97.74%. In opposite to that algorithm is the proposed MHill in this work. In this paper we proposed a new image encryption where Hill cipher is only applied once and the NPCR reaches 99.52% maximum. Thus, the proposed algorithm (MHill) is considered the best for provides significant data (image) ciphering with minimum and maximum Correlation Coefficient Factor (CCF) values with respect to encryption and decryption and maximum NPCR, PSNR in the data set used.

As for the future works can be summarized as follows:

1) the security for the proposed MHill strategy could be upgraded if another random permutation process is added after the last step of the ciphering algorithm. Nevertheless, this extra operation will definitely make the cryptosystem more computationally expensive. The security could be enhanced by adding another extra permutation or increasing the key size.
2) Implementing image encryption with a fractal approach.
3) Application of DNA algorithms in image encryption.
4) Efficient encryption of large block size of data.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

REFERENCES

[1] Bharti Ahuja, Rashmi Lodhi, "Different Algorithms used in ImageEncryption: A review", *International Journal of Computer Science & Engineering Technology (IJCSET)*, Vol. 4 No. 07 2013, pp.: 861-864.

[2] P. P. Dang and P. M. Chau, "Image Encryption for Secure Internet Multimedia Applications," *IEEE Trans. Consumer Electronics*, 2000, vol. 46, no. 3, pp. 395-403.

[3] William Stallings, 2011. *Cryptography and Network Security: Principles and Practices*, Fifth edition, Chapter 2, pp.: 37.

[4] Eskiciogiu,A. Litwin,L " Cryptography and Network Security" *LOS Alamitos,CA: IEEE computer society press*, Issue:1,1987, pp: 36-38.

[5] Pooja Mishra, Biju Thankachan, "A Survey on Various Encryption and Key Selection Techniques", *International Journal of Engineering and Innovative Technology (IJEIT)*, 2013, Volume 2, Issue 7, pp.: 141-145.

[6] Stinson, D.R., 2002. *Cryptography Theory and Practice* (2nd Ed.). CRC Press, Boca Raton, Florida.

[7] S. Zhang and M. A. Karim, "Color image encryption using double random phase encoding," *MICROWAVE AND OPTICAL TECHNOLOGY LETTERS*, Vol. 21, No. 5, 1999, pp.: 318-322

[8] Yi Kai-Xiang and Sun Xing et al., "An image encryption algorithm based on chaotic sequences", *Journal of Computer Aided Design and Computer Graphics*, Vol. 12, No. 9, 2000, pp. 672-676.

[9] Li. Shujun, and X. Zheng "Cryptanalysis of a chaotic image encryption method," *Inst. of Image Process*, Xi'an Jiaotong Univ., Shaanxi, This paper appears in: *Circuits and Systems, ISCAS 2002. IEEE International Symposium* , 2002, Vol. 2, 2002, pp. 708-711.

[10] A. Sinha, K. Singh, "A technique for image encryption using digital signature," *Optics Communications*, 2003, pp. 1-6.

[11] S.S. Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", *Pattern Recognition*, Vol. 34, 2001, pp. 229-1245.

[12] A. Sinha, K. Singh, "Image encrypt ion by using fractional Fourier trans form and Jigsaw transform in image bit planes," *Source: optical engineering, spie-int society optical engineering*, vol. 44, no. 5 , 2005, pp.:15-18.

[13] V.U.K. Sastry and N. Ravi Shankar," Modified Hill Cipher for a Large Block of Plaintext with Interlacing and Iteration", *Journal of Computer Science* 4 (1) , 2008:pp. 15-20.

[14] A. Mitra, Y. V. Subba Rao and S. R. M. Prasanna, " A New Image Encryption Approach using Combinational Permutation Techniques" *World Academy of Science, Engineering and Technology* 14, pp.919–923, 2008.

[15] Saroj Kumar Panigrahy, Debasish Jena,Sathya Babu Korra, and Sanjay Kumar Jena, "On the Privacy Protection of Biometric Traits: Palmprint, Face, and Signature", *Springer-Verlag Berlin Heidelberg*, CCIS 40, pp. 182–193, 2009.

[16] H. H. Nien, W. T. Huang, C. M. Hung, S. C. Chen, S. Y. Wu," Hybrid Image Encryption Using Multi-Chaos-System", *IEEE* 2009, pp.1-5.

[17] G. Zhi-Hong, H. Fangjun, and G.Wenjie , "Chaos - based image encryption algorithm," *Department of Electrical and computer Engineering, University of Waterloo*, ON N2L 3G1, Canada. Published by: Elsevier, 2009, pp. 153-157.

[18] Zhu Yu, Zhou Zhe, Yang Haibing, Pan Wenjie, Zhang Yunpeng,"A Chaos-Based Image Encryption Algorithm Using Wavelet Transform", *IEEE* 2010.

[19] Zhengjun Liu, Lie Xu, Jingmin Dai, Shutian Liu,"Image encryption by using local random phase encoding in fractional Fourier transform domains" *Elsevier, Optik*, vol 123, 2012, pp. 428– 432.

[20] Panduranga H T and Naveen Kumar S K, "Advanced Partial Image Encryption using Two-Stage Hill Cipher Technique", *International Journal of Computer Applications* (0975 – 8887) Volume 60– No.16, 2012.

[21] Somdip Dey, "SD-AEI: An Advanced Encryption Technique For Images", *IEEE 2012, Second International Conference on Digital Information Processing and Communications (ICDIPC2012), Lithuania*, pp. 68-73.

[22] Cherif Moumen, Malek Benslama and Mekhilef Saad, "Cryptography of the Medical Images", *PIERS Proceedings, Kuala Lumpur, MALAYSIA*, 2012, pp.: 42-48.

[23] Vinay pandey , Angad Singh, Manish Shrivastava, "Medical Image Protection by Using Cryptography Data-Hiding and Steganography", *International Journal of Emerging Technology and Advanced Engineering* , 2012, Volume 2, Issue 1, pp.: 106-109.

[24] Ashtiyani, M., Birgani, P.M. and Hosseini, H.M., "Chaos-Based Medical Image Encryption Using Symmetric Cryptography", *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on IEEE, in Damascus*, 2008, pp.: 1-5.

[25] W. Puech, "Image Encryption and Compression for Medical Image Security", *IPTA'08: 1st International Workshops on Image Processing Theory, Tools and Applications, Tunisia*, 2009, ver.1.

[26] Panduranga H T, NaveenKumar S K, "Selective image encryption for Medical and Satellite Images", *International Journal of Engineering and Technology (IJET)*, 2013, Vol 5 No 1, pp.: 115-121.

[27] Abrams, M., and Podell, H. "Cryptography" *Potentials, IEEE* Page No 36-38. Issue:1,Volume: 20, 2001.

[28] Abrams, M., and Podell, H. "Cryptography" *Potentials, IEEE* 2001, Issue: 1, Volume: 20, pp.: 36-38.

[29] Jinn-Ke Jan and Yuh-Min Tseng, "On the security of image encryption method," *Information Processing Letters*, 1996, vol. 60,pp.: 261–265.

[30] Prabir Kr. Naskar,Atal Chaudhuri, "A Secure Symmetric Image Encryption Based on Bit-wise Operation", *International Journal of Image, Graphics and Signal Processing (IJIGSP)*, 2014, Vol. 6, No. 2, PP.: 30-38.

[31] W. Stallings, *Cryptography and Network Security*: Principles and Practice, Prentice- Hall Upper Saddle River, USA, 1999.

[32] Saeednia S. How to Make the Hill Cipher Secure. *Cryptologia Journal*, 2000, 24, pp.: 353-360.

[33] ISMAIL I.A.1, AMIN Mohammed2, DIAB Hossam2," How to repair the Hill cipher", *J Zhejiang Univ SCIENCE A* 2006 7(12):pp: 2022-2030.

[34] "FIPS PUB140-2: Security Requirements for Cryptographic Modules," *National Institute of Standards and Technology*, 2001.

[35] A.V.N.Krishna, K.Madhuravani, " A Modified Hill Cipher using Randomized Approach", *Computer Network and Information Security*, 2012, 5, pp.: 56-62.

[36] V.U.K.Sastry, Aruna Varanasi and S.Udaya Kumar "A Modern Advanced Hill Cipher Involving a Permuted Key and Modular Arithmetic Addition Operation", *Journal of Global Research in Computer Science*, Volume 2, No. 4, 2011.

[37] Ibrahim S I Abuhaiba1 and Maaly A S Hassan, "IMAGE ENCRYPTION USING DIFFERENTIAL EVOLUTION APPROACH IN FREQUENCY DOMAIN", *Signal & Image Processing : An International Journal(SIPIJ)* Vol.2, No.1, 2011, pp.: 51-69.

[38] P.Shanmugam1, C.Loganathan, "INVOLUTORY MATRIX IN VISUAL CRYPTOGRAPHY", *IJRRAS*, 2011, Vol 6, Issue4, pp.: 424-428.

[39] A. Kumar and M. K. Ghose, "Extended substitution-diffusion based image cipher using chaotic standard map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, pp. 372-382, 2011.

[40] Yue Wu, Joseph P. Noonan and Sos Agaian "NPCR and UACI Randomness Tests for Image Encryption", *Journal of Selected Areas in Telecommunications (JSAT)*, 2011,pp: 31-38.

Dr. Firas Shawkat Hamid: Born in Mosul/Iraq in 1972. He obtained his B.Sc. degree in Aviation and Electronic Engineering in 1994, M.Sc. in Electronics and Communication Engineering in 2000 and Ph.D. in Mobile Communication Engineering in 2010. He obtained Consultant Engineer degree in 2010. He is Instructor in CISCO Academic and Head of Department of Computers Systems in Technical Institute Mosul/ Foundation Of Technical Education/ Ministry Of higher Education and Scientific Research/ Iraq. He is interested in the subjects of Computer Networks, Image Processing, ciphering Telemedicine Systems.

and

Thakwan Akram Jawad, Born in Mosul/Iraq in 1965. He obtained his B.Eng. degree in Computer Technology Engineering in 2006 from Technical College of Mosul / Foundation Of Technical Education /Iraq, he is Engineer in Engineering College / Mosul University/Iraq. He is interested in digital image processing, microprocessor and ciphering.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

ERSUN İŞÇİOĞLU, He is Head of Department of Computer and Instructional Technology Education / Eastern Mediterranean University (e-mail: ersun.iscioglu@emu.edu.tr). . He is interested in digital image processing, ciphering.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)