ENCRYPTION OF THE TEXT USING HILL CIPHER AND HIDDEN IN THE DIGITAL IMAGE

Muhmed F. Agbisha[1], Jalal M. Mehalhal[1] and Saed S. Alasttel[2]

[1] *Dept. of Computer Engineering, High Institute-Alkhoms .*
[2] *Dept. of Computer science, Al-Asmarya Islamic University, Zliten-Libya*

ABSTRACT

The use of internet increases for communication and for other aspects. There is a number of cryptography scheme that used to increase security from the passive attack that has more types of attack dangers, This paper discusses the confidential information transfer .This paper, introduces a software-based technique to hide the data in the RGB image , these data are encrypted and decrypted by the Hill Cipher.

Keywords:Cryptography, Hill Cipher, Digital Image, Security.

1. INTRODUCTION

Cryptology [from the Greek *kryptós*,"hidden" and *logos*,"word "] is the science of secure [generally secret] communications. The transmitter and the receiver are able to transform information into a cipher by virtue of a key i.e., a piece of information known only to them.

Cryptography [from the Greek*kryptós*, and*gráphein* to "write"] is the study of the principles and techniques by which information can be concealed in ciphers and later revealed by legitimate users employing the secret key, but in which it is either impossible or computationally infeasible for an unauthorized person to do so. Cryptanalysis [from the Greek *kryptós* and *analyein*, "to loosen "or "to untie"] is the science [and art] of recovering information from ciphers without knowledge of the key.

Cryptology includes both cryptography and cryptanalysis.

An encryption scheme has five ingredients:-

- Plaintext
- Encryption algorithm
- Secret key
- Ciphertext
- Decryption algorithm

The original information to be hidden is called "plaintext". The hidden information is called "ciphertext". Encryption is any procedure to convert plaintext into ciphertext. Decryption is any procedure to convert ciphertext into plaintext.

The plaintext in this algorithm is the text , the Encryption algorithm included the Encrypte and then hide the text in the RGB image, the Secret key is the key that used into crypt the text, the Cipher text is the text hidden in image, the Decryption algorithm included the extract of hidden text from the RGB image and decrypted to the orginal text[3].

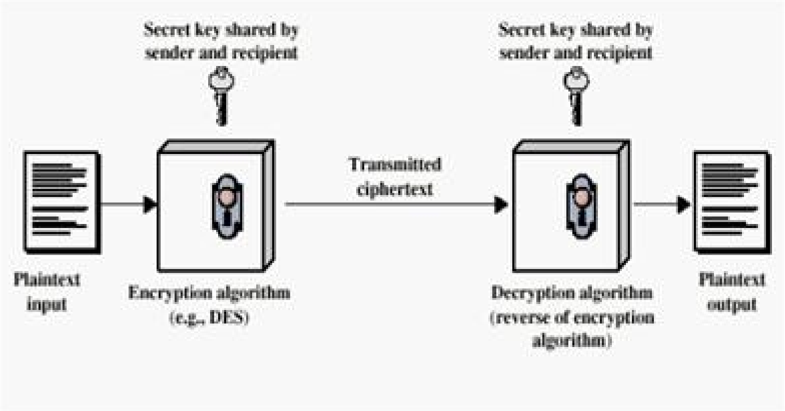

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Fig (1) simplified Model of Conventional Encryption[3]

2. IMAGE PROCESSING

Color image models With the color format, a digital image can record and provide more information than the gray scale format image does. Digital acquisition devices (such as scanners and digital cameras) can separate beams of light into three primary colors- red, blue, and green, through the assistance of spectroscopes and filters. In order to record the color information, we need at least three parameters (e. g. red, blue, and green) to represent a color. We use the color model to represent the color information of digital images. Since we need three parameters to represent a color, those color models must be with a three dimensional format. The models use some mathematical functions to represent a point position (in the three dimensional space) that is assigned to a color. Some color models (RGB, CMY, YIQ, HSI, l1_l2_l3, and L*a*b)[1].

RGB color model

The three primary colors (red, green, and blue) and their combination in visible light spectrum are shown in Fig.1. With different weights, (R, G, B), their combination can indicate different colors. After normalizing the values of R, G, B, we can get the color cube (Fig.2). The colors on the diagonal line, from the origin to the coordinate (1,1,1) of the cube, means the gray-level values.

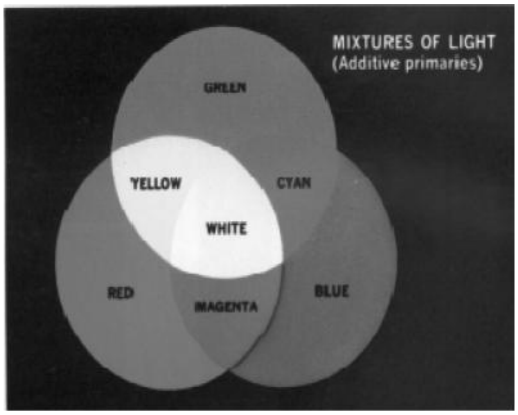


Fig. 2RGB graph of the primary colors [5].

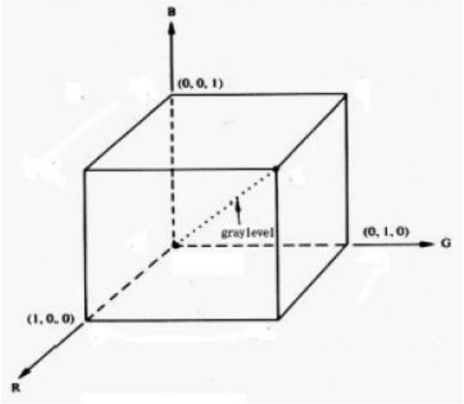
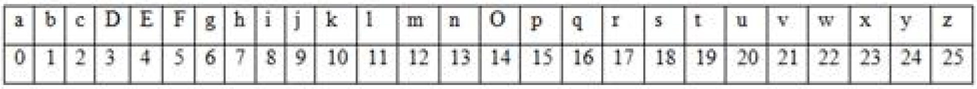


Fig. 3RGB primary color cube [5].

Hill Cipher

It was developed by the mathematician Lester Hill. The encryption algorithm takes m successive plaintext letters and substitutes for them m ciphertext letters. The substitution is determined by m linear equations in which each character is assigned a numerical value [4]:



a	b	c	D	E	F	g	h	i	j	k	l	m	n	O	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

For m=3, the system can be described as follows:

C1=(k11p1+k12p2+k13p3) mod 26

C2=(k21p1+k22p2+k23p3) mod 26

C3=(k31p1+k32p2+k33p3) mod 26

This can be expressed in terms of column vectors and matrices:

C=KP mod 26,

where C and P are column vectors of length 3, representing the plaintext and cipher text, and K is 3x3 matrix, representing the encryption key.
Operations are performed mod 26.
For example, consider the plaintext "payformoney", and use the encryption key

K=

17	17	5
21	18	21
2	2	19

The first 3 letters of the plaintext are represented by the vector (15 0 24). Then K(15 0 24) = (375 819 486) mod 26 = (11 13 18) = LNS. Continuing in this fashion, the cipher text for the entire plaintext is LNSHDLEWMTRW.

Decryption requires using the inverse of the matrix K. The inverse K-1 of a matrix K is defined by K K-1 = K-1 K=I, where I is the unit matrix (1-s on the diagonal, other elements – zeroes). The inverse of the matrix does not always exist, but when it does, it satisfies the preceding equation. In this case, the inverse is

K-1=

4	9	15
15	17	6
24	0	17

This is demonstrated as follows:

K K-1 =

443	442	442
858	495	780
494	52	365

And after taking mod 26 of the elements above, unit matrix is obtained.

In general terms, the Hill system can be expressed as follows:

C=EK(P)=KP mod 26

P= DK(C)=K-1C mod 26 = K-1KP = P

As with Playfair, the strength of the Hill cipher is that it completely hides single-letter frequencies.

Although the Hill cipher is strong against a ciphertext-only attack (opponent has only ciphertext), it is easily broken with a known plaintext attack (opponent has pairs plaintext – cipher text). For an m*m Hill cipher, suppose we have m plaintext-cipher text pairs, each of length m. We label the pairs Pj=(p1j, p2j,…, pmj) and Cj=(c1j, c2j,…, cmj) such that Cj=KPj for 1<=j<=m and for some unknown key matrix K. Now define two m*m matrices X=(pij) and Y=(cij).

3. INTRODUCTION TO MODULAR ARITHMETIC

Suppose k is a positive integer. The remainder when a number is divided by k is called the value of that number modulus k. We usually abbreviate modulus by mod, and write it like this:

- $45 \equiv 5 \pmod{10}$
- $36 \equiv 6 \pmod{10}$
- $36 \equiv 1 \pmod{5}$
- $36 \equiv 0 \pmod{6}$

The method used:

In this paper, the researches uses a way to hide text within a digital image where the text encryption that uses the Hill Cipher is used for the text encryption .

The used technique is the LSB where the least significant bit of each pixel is replaced by bits of the secret till secret message finishes. The risk of information that isuncovered with this method, is susceptible to all ‘sequential scanning’ based techniques ,which threaten its security.

In the image, there are three basic colors red,green and blue. The red color used as pointer to hide the data in other colors or not hide, where after reading the image, the three colors represented by the numbers between 0 to 255.After then converted to binary digit ,the paper took to bits that are the LSB.In the pointer if the bits are 00 then don’t hide this pixel,alsoin the pointer if the bits is 01 then the data is hidden in the two bits that are LSB of green color,also in the pointer if the bits is 10 then the data is hidden in the two bits that is LSB of blue color,also in the pointer if the bits are 11 then the data is hidden in the two bits that is LSB of green color. To increase security, data are hidden . Also the encryption key is hidden in the digital image as shown in the following below:

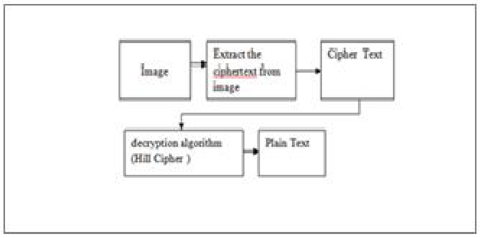
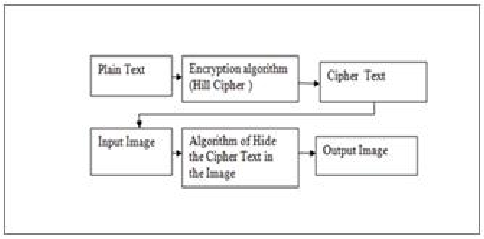
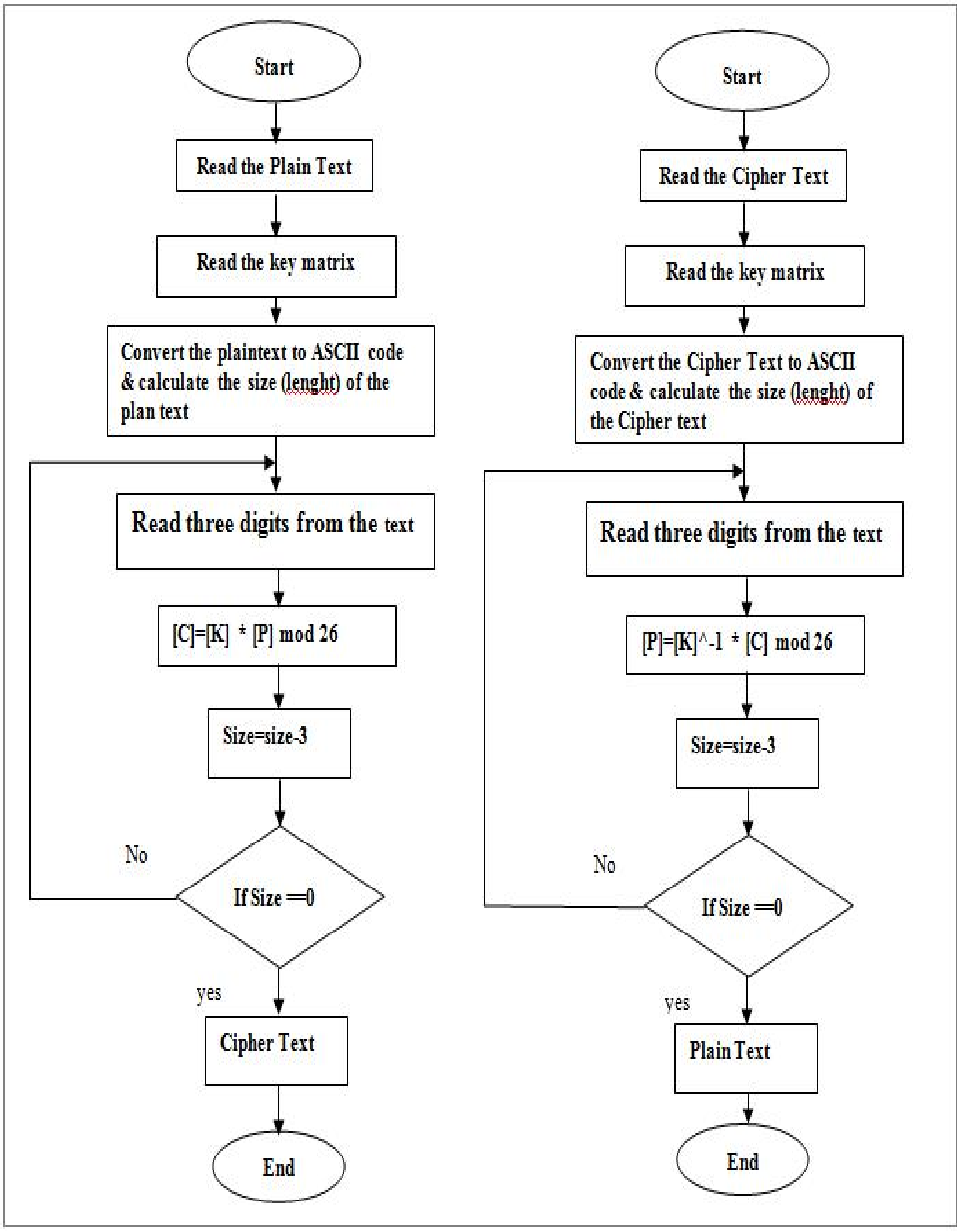


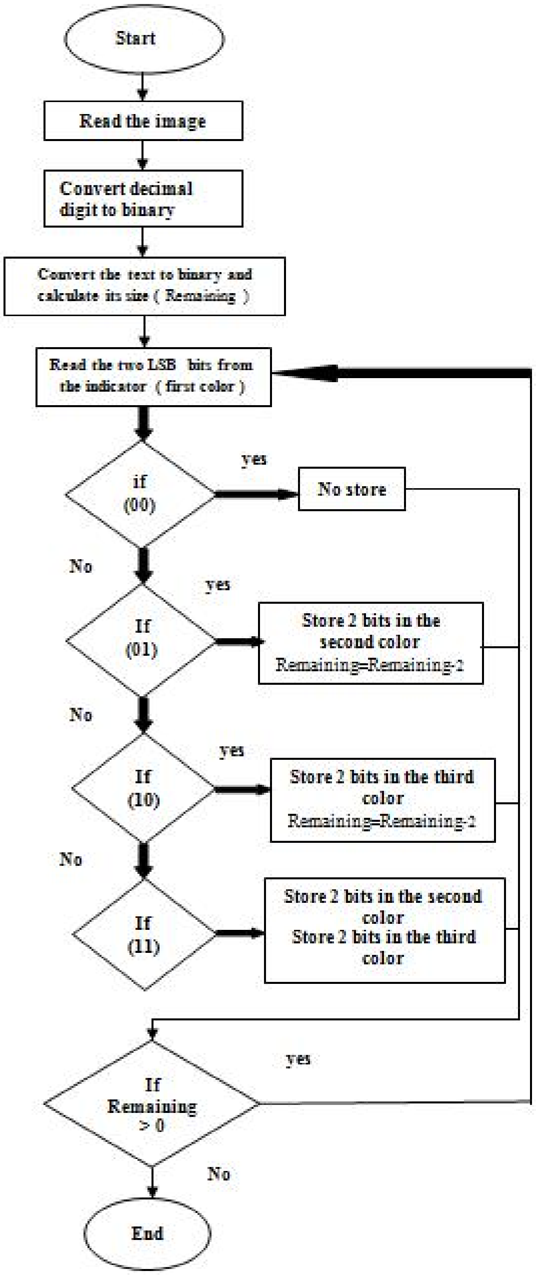
Image
Extract the ciphertext from image
Cipher Text
decryption algorithm (Hill Cipher)
Plain Text


Plain Text
Encryption algorithm (Hill Cipher)
Cipher Text
Input Image
Algorithm of Hide the Cipher Text in the Image
Output Image

Fig(5)graph of extract & decryptionFig(4)graph of encryption & hide


Start
Read the Plain Text
Read the key matrix
Convert the plaintext to ASCII code & calculate the size (lenght) of the plan text
Read three digits from the text
[C]=[K] * [P] mod 26
Size=size-3
If Size ==0
No
yes
Cipher Text
End
Start
Read the Cipher Text
Read the key matrix
Convert the Cipher Text to ASCII code & calculate the size (lenght) of the Cipher text
Read three digits from the text
[P]=[K]^-1 * [C] mod 26
Size=size-3
If Size ==0
No
yes
Plain Text
End

Fig(6) Flowchart of encryption& decryption


Start
Read the image
Convert decimal digit to binary
Convert the text to binary and calculate its size (Remaining)
Read the two LSB bits from the indicator (first color)
if (00)
yes
No store
No
If (01)
yes
Store 2 bits in the second color Remaining=Remaining-2
No
If (10)
yes
Store 2 bits in the third color Remaining=Remaining-2
No
If (11)
Store 2 bits in the second color Store 2 bits in the third color
If Remaining > 0
yes
No
End

Fig(7) Flowchart hiding text in image

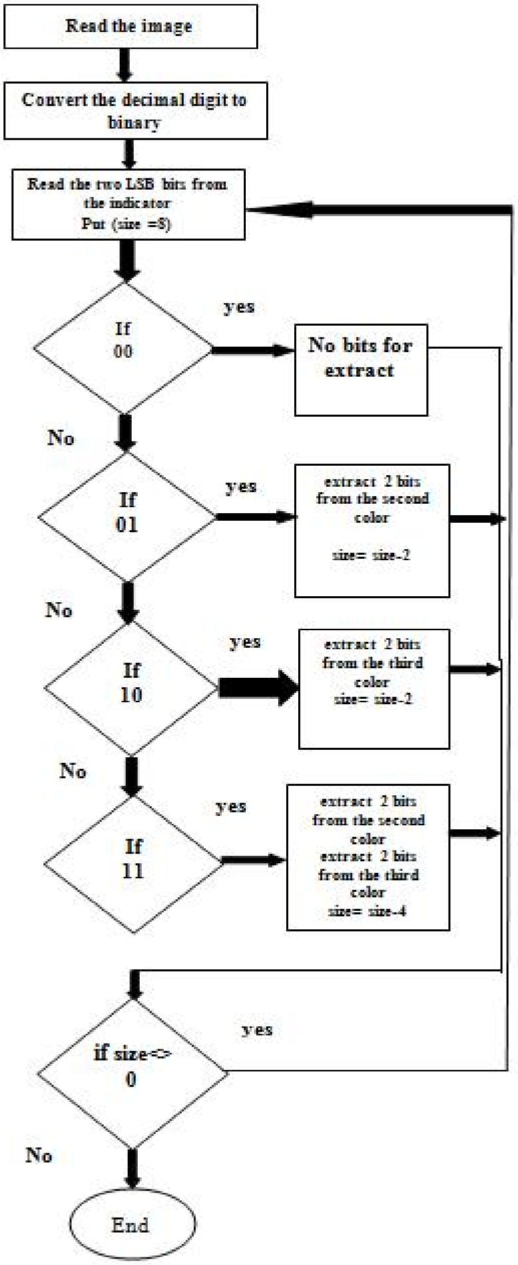
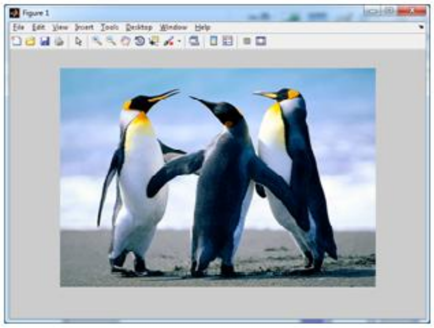

Read the image
Convert the decimal digit to binary
Read the two LSB bits from the indicator
Put (size =8)
If 00
yes
No bits for extract
No
If 01
yes
extract 2 bits from the second color
size= size-2
No
If 10
yes
extract 2 bits from the third color
size= size-2
No
If 11
yes
extract 2 bits from the second color
extract 2 bits from the third color
size= size-4
if size<> 0
yes
No
End

Fig (8) Flowchart extract text from image

4. RESULT

As the ever-increasing demand for the Internet bandwidth is satisfied with new technologies, the amount of information being offered for public access grows at an surprising rate.



Fig(9)An image before imbedding the encrypted data

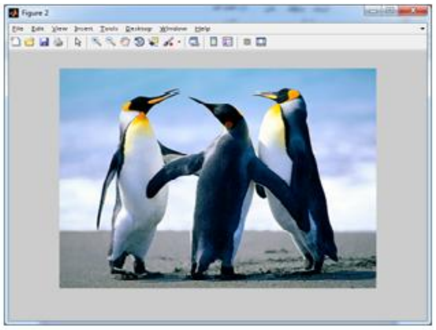
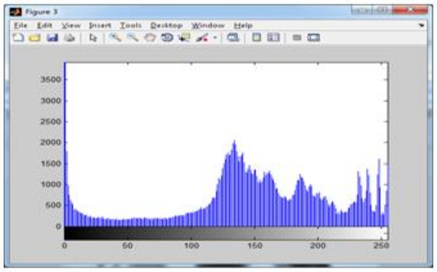
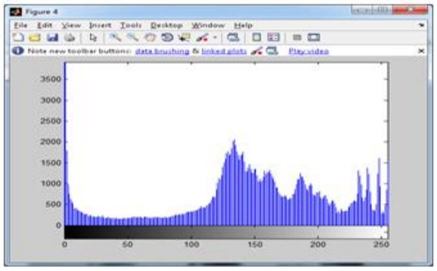


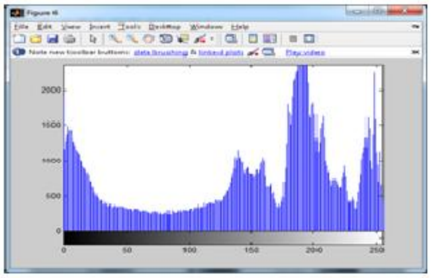
Fig (10) An image After imbedding the encrypted data



Fig(11)Orginal image histogram of red color



Fig(12) modified image histogram of green color



Fig(13)Orginal image histogram of green color

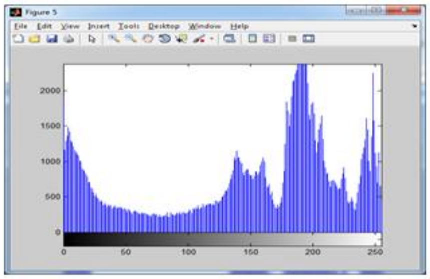
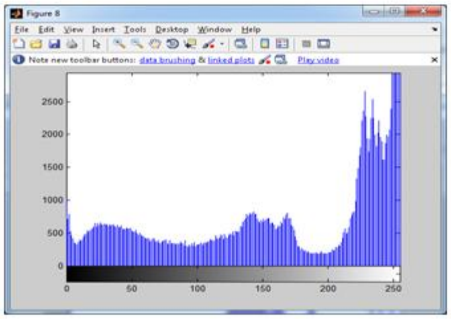
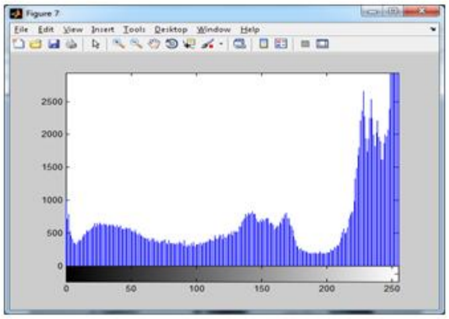


Fig (14) modified image histogram of green color





Fig(15) Orginal image histogram of blue color Fig(16) modified image histogram of blue color

5. CONCLUSION

The goal of information security is to provide an adequate protection for methods of risk information and applying the necessary means to ensure the protection of information and procedures, LSB modification technology provides an easy way to include the information in the pictures, but data that can be decoded easily. The plan proposed in this paper is used to encrypt confidential information before inclusion in the picture. Certainly the complexity of the overall process time increases but at the same time security that have been made in this cost is well_worth.

Data encryption method was used Hill (Hill Cipher), one of the types of compensatory where encryption is used in this way to encrypt more than one character at once.

And follow the encryption method and then concealment were obtained the following results.

1. The image was obtained by the hidden encrypted text without any noticeable changing them.

2. Hide writing conceal the existence of the letter at all and what distinguishes this kind of hidden messages is that they reach their destination in secret completely at odds encrypted messages, that even though it can never be deciphered without the encryption key, it can be identified as a message encrypted.

3. The speed of implementation of the process of concealment, quickly extract the hidden text.

REFERENCE

[1] Gonzalez and Woods. "Digital Image Processing". Prentics Hall 2002. Second Edition.

[2] Saroj Kumar Panigrahy,Bibhudendra Acharya, Debasish Jena.2008. "Image Encryption using Selfe-Invertible Key Matrix of Hill Cipher Algorithm", International Conference on Advances in Computing, Chikhli, india.

[3] Naveen Kumar S K, Sharath Kumar H S, Panduranga H T.Dec 2012." Encryption Approach for Images using Bits Rotation Reversal and Extended Hill Cipher Techniques". International journal of computer Application.

[4] Chris Solomon and Toby Breckon. "Fundamentals of Digital Image Processing" .2011.

[5] WilliamStallings,”Cryptography and Network Security”,Fourth Edition 2006.

[6] Ismail et 2022 al. / J Zhejiang Univ SCIENCE A 2006.How to repair the Hill cipher

[7] Al-Hammami, Ala And Al-Ani, Sad. "Security Data Technology and Security Systems". Wael Publisher 2007.