PICTURE ENCRYPTION BY USING DISCRETE COSINE TRANSFORM (DCT)

Sahera Obaid Sead and Mais'a Abdul Kerim Nasir
Computer Dept/ Science College/ Basrah University

ABSTRACT:

The research aims to proceed the process of encryption and the digital images by using a suggested method which uses the Discrete Cosine Transform and Some logical functions and programmatic applications. The rapid development of the communication network through the Internet and development of the electronic trade with spread of the digital media such as (images, audio, video) which can be got easily, copied, and distributed with another persons names. All these led to the needs of the authentication or copyright.. The suggested technique of transforming the desperate cosine is regarded as one of the important transforming methods and is wide spread, recently in the analytic field and treatment of the digital pictures.

Whenever there was a need to hide images for confidentiality the using transformation of the analyzed pictures prevents, the attacker from restoring the picture unless knowing these methods. For being certain of the efficiency of the suggested method it was tested on a group of images with coloured graduation (RGB) that we enlisted at the end of the research.

Key words

Image , Encryption , Transform , Replacing

INTRODUCTION:

Interest in the treatment of digital image methods stems from two basic fields of application: Improvement of the imaging data to be explained by man and treated with theoretical data for realizing the machine independent manner. One of the applications of treatment of images in the first field was to improve the digital newspaper images that was sent by cable links between London and New York in 1920s, when the time was shortened to transform the images from more than one week into less than three hours. Notwithstanding, the method of the treatment of the digital images, that were sent improved within the last thirty-five years. These improvements exploit the invention of the developed computer and space programs in same time of showing the hidden possibilities in the concepts of image treatments[5].

Since 1964 up to the present time, the field of treatment of images has grown widely in addition to the applications of space program, then the techniques of the digital images treatment is exploited today in various matters that , despite they were irrelevant with each other mostly, they are all need to find methods, capable to improve the imaging data to be explained and analyzed by man, for instance in Medicine which helps to improve and explain the X-ray photos and some other Biological medicine photos. The same techniques or other similar ones are used by geographers in studying the samples of pollution and climax that they get from airplane and artificial satellites. There are some mutual link in the previous examples, it is the result of the treatments which are aim at helping man to explain pictures. The second mall field of application for the treatment of digital images that are mentioned earlier in this research are the matters that deal with the realization of things. In that case the inter concentrated on the proceeding of abstracting data ? images in suitable manners for treatment via computer, the statistics stresses and formalities of transforming
(Furrier) and measuring the distances with multiple dimension which are examples for types of used data in order to be realized by machine for the pictures. As a result of Internet development and the possibility of. anticipation in data via many sharers in world , the growth of Software programs techniques and the Hardware techniques, it is possible now to send and receive many complex data via Internet. In the past, sending was restricted by the written texts via fax, but now it is possible to send and receive various types of fixed and animation images as well as digital multimedia. There are many appeared techniques that can be used in transforming data and information and increasing the need for their protection and thus it became possible to send hidden information within other media such as Sound and vision by using encryption methods which became necessary for making data unreadable by all persons except the authorized one, this is exactly what encryption does[3].

TRANSFORMERS OF IMAGE

The transform theory plays a basic role in the treatment of images because it is interesting point in theory jobs in addition to its practical applications in this field , where there are two dimension transformations an are used for facilitating image treatment and image compression and for improving and restoring images. The image transformers are transforming image data from spatial domain into frequency domain. Techniques of frequency domain are called transform domain which are the raw data transform (image data) with strong link into formalities and with one link or less than to facilitate dealing with it, it is also used to get important information (accurate characteristics) about the image[5]. This operation is characterized by several characteristics the most important one is that it is reversible that is the image which can be transformed and can be reversed to its original form after the transformation process is achieved without any loss in data. We can define the general format for the forward linear transform as that the two dimensions matrix for the image f(x, y) which includes N x N of the following equation(1):

$$F(u, v) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y).\, b(u, v, x, y) \qquad \text{.....(1)}$$

Where:
F(u, v): is the function of (Transform Coefficients).

b(u, v, x, y): is nuclear of forward frequency transform. u, v: frequency domain variables.

u, v= 0,1,2, ..., n-1

Also, we can show the process of inverse transform for transforming the image in transform domain into the original domain as in the following equation(2):

$$F(x, y) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} f(u, v).\ g(x, y, u, v) \quad \text{..(2)}$$

Where

g(x, y, u, v): is the nuclear of frequency reverse transform.

x, y: spatial domain variables[9].

SPATIAL DOMAIN

The term of Spatial Domain refers to neighbor pixels that form the image, **T**he methods of the spatial domain are procedures that work directly on these pixels. The enclosing method in the spatial domain is the easier one when a change of pixels values is accomplished for the image and directly through treatment of pixels or the two dimensions with least significant bit randomly. This method is inefficient towards the possible tasks since it rapidly removes or destroys the spatial digital mark.

FREQUENCY DOMAIN

The techniques of frequency domain are called the techniques of transform domain where there is a division for image factors into three different levels ,The high frequency that human vision system cannot feel. The middle frequency which is the best place for enclosing the digital spatial mark and the short frequency that can be detected by human vision system largely. It has been noticed recently that enclosing data in frequency domain is stronger than enclosing data in the spatial domain, The most common transforms are[8]:

1) Foruier Transform (FT)

Foruier Transform is one of the widest used types, it is one of the basic tools in sciences and modern engineering. The Foruier transform has been developed by (Baptiste Joseph Foruier (1768-1830) for explaining the distribution of pressure and thermo link and since then it has been used in computer imaging which it can analyze the image into balanced group of functions of two dimensions cosine.

2) Discrete Wavelet Transform (DWT)

The Discrete Wavelet Transform is calculated by analyzing the signal into different beams frequency (approximation signal) and detail signal where it includes two groups of function that are called scale functions and wavelet functions. This type appears from transforming with great development in the movement of the commercial images via Internet and the usage of imaging in multi media It became the standard tool for dominating what Foruier Transform has suffered from.

3) Discrete Cosine Transform (DCT)

The Discrete Cosine Transform is one of most important techniques that are used in treatment of images. Here , it could be used for cutting image into blocks ,equally N x N like 8 * 8 the element of the image. The transformation of each mass of the spatial domain into the frequency domain is carried out by using the equation of discrete cosine with two dimensions (2-D- DCT) that are represented by the following equation(3):

$$F(u, v) = 1/4\ C(u)\ C(v)\ [\sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos((2x + 1)\ v\pi \backslash 2n \cos((2y+1)\ v\pi \backslash 2n)] \quad \text{..........(3)}$$

Where

$$C(Z)= \begin{cases} 1\backslash\sqrt{2} & \text{if } Z=0 \\ 1 & \text{if } Z\neq 0 \end{cases}$$

Where z is either u or v
x, y= 1,2 , ……,N-1
While the reverse transform of the cosine gives the following equation(4):

$$F(x, y) = 1\backslash 4 \left[\sum_{u=0} \sum_{v=0} C(u)\, C(v)\, f(u, v) \cos\left((2x+1)\, u\pi\backslash 2n \cos((2y+1)v\pi\backslash 2n)\right]\right| \quad \text{……(4)}$$

Where
u, v= 0,1,2 ,……., N-1

ENCRYPTION

It is the process of protection and the confidentiality of data (both fixed or mobile) by using programs that have the capacity of transforming and translating these data into codes where, unless reaching by persons who are unauthorized, they couldn't understand any of the display codes which will seem to them as mixture of codes and numbers and letters that are obscure, There are two types of technology that are used in encryption which are the Symmetric and the Asymmetric encryption, The difference between them is so simple, but it is important in the level and security degree where in the symmetric encryption, there is encryption of data by using the general number Also, in at the same time the encryption solve and translate the data into its original status by using the same general number[2,4]. Therefore, if any person got that general number or obtained it from the general guide, he would be able to solve the encryption and read these data, If these data are encrypted in Asymmetric encryption technique, then the data would be encrypted by the genera! number, but this cannot be solved and be reached unless getting private key for the owner of the general key that encryption depends upon, The encryption is the process of treatment of the encrypted text in which the meaning of the text is obscure or the process of transforming the plain text into encrypted text is called Cryptogram.

DECRYPTION

It is the reverse process which transform the encrypted text into its original form.

CRYPTOSYSTEM:

It is divided into two parts:
1- Encryption.
2- Decryption.

CIPHER

It is a group of processes that are aim to transform plain text into encrypted text, it is the mathematical function that is used for encryption, and it is the secure modern system that depends on cryptographic key. The value domain which can be taken as cryptographic key is called key space. If M is text space and C is the encrypted text space and K is the cryptographic key space, then[1,6]:

1- Enciphering Algorithm

Ek: M ---- C or Ek(m)=C,where k∈ K , m ∈M and c∈C **……(5)**

2- Reverse Algorithm (Deciphering Algorithm)

Dk: C ---- M or Dk(c)= m, where k∈ K . m ∈ M and c∈C **……(6)**

$Ek^{-1}=Dk$

Dk(c)=Dk [Ek (m)] =m

INTERCEPTOR (OPPONENT)

He is the person who opponents the encrypted text between the sender and the receiver illegally where he doesn't know the used key in cryptographic process ,he cuts the contact or spying or changing the text's content ..Systems of cryptographic keys can be divided into two type depending on cryptographic key they are[7]::

1- Secret Keys Sys tem (Symmetric Algorithm)

In that type of encryption, the cryptographic key and decryption Key which is the same as the following figure.

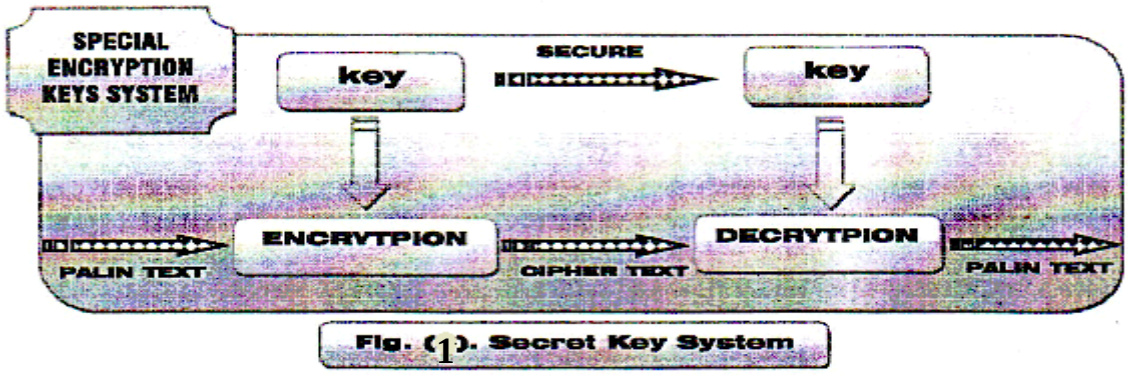


Fig. (1). Secret Key System

2- public Key System (Asymmetric Algorithm)

This type of encryption is very significant is which the used key in encryption is different from that which is used in decryption as in following figure (2).

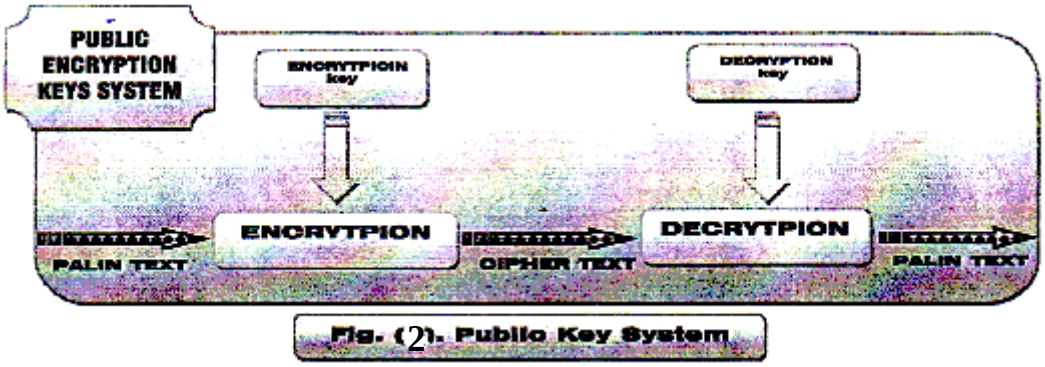


Fig. (2). Public Key System

ENCRYPTION STRENGTH

This depends oh the number of the ranks that form each number, it is measured by bits such as if the number is forms 40 ranks, then the strength would be 40 bit, if the number forms 56 tanks, then the encryption strength reaches 56 bits. Despite the fact, that the available technology in that field can provide the encryption strength, which reaches more than 3000 bits, the USA government forbids up to date handling encryption strength that exceeds 128 bits because it is enough for protecting the electrical trade .It is very important to mention, here, that the required time for the Internet hijackers to be able to decrypt a code with 56 bits is 22 hours and 15 minutes, The required time top decrypt a code of 128 bits strength, by using the recent technology of decrypting, is two trillion years !!! that is because the Internet hijackers in the case of 56 bits need to try 72 quadrillion of attempts (a number with 15 zero) while in case of 128 bits strength the attempts that are required for trial reaches 340 undecellion (a number with 36 zero), thus we hadn't heard till today that a data had been encrypted in such strength which had been decrypted by those professional hijackers we don't think that any body can at least in near future or far future does such a thing. Thus go shop via Internet with relax in condition, you must be certain of the used strength by the site you eager to buy from and be sure of encryption strength by your self[2].

SUGGESTED ENCRYPTION ALGORITHM

The aim of the recent research is to apply a group of mathematics equations and programmatic applications upon multiple levels of images in order to be encrypted as is shown in the following two algorithms:

ENCRYPTION ALGORITHM

Inputs: natural image of BMP type.
Outputs: resulted image from encryption.

According to the following steps:

1- Reading an image of BMP type.
2- Measuring readable image into 512 x 512 pixel.
3- Applications of the factor XOR.
In this process, the resulted matrix would be taken after measuring and applying XOR on it and using the specific key system of encryption as shown in the following equation(7):

$$Ci = Eki(mi) = mi (+) Ki \quad \textbf{.....(7)}$$

Where Ki, mi, ci represents codes or ranks of domiciles that host the (+) encryption which represent the mixer. Then, new values will be added such as (3 xor 2=1), that is (11 xor 10=01). It is known that application of XOR will result in one for different values and zero for the similar values, In order to return these values into its origin in the decryption by inputting the same encryption key system that is used here and apply XQR on it such as returning the value (3) into the file of encryption which is done by (01 xor 10 11) or (1 xor 2=3), the best tools for the encryption of digital values is to use XOR (Exclusive or) which is function that is applicable on all bits that form a number.

4- Separate every level of the three image levels each alone to be able to apply the discrete transforming cosine equation(3).
5- Applying discrete cosine transform on each level of the above levels in order be transformed from the spatial domain into the frequency domain and to be treated programmatically by using equation of two dimensions discrete cosine transform which has been explained earlier.
6- Up-left (tossing) the matrix towards (left-right) which transform the existed values from left to the right and vice versa such as:

7- Cutting all the resulted matrix of the previous step into size mass (32 x 32) in order to be treated in the following step.
8- Replacing the sites of each mass of the resulted mass in step (7) according to the following equations(8):

$$X(i, j) = X(i, 32-j+1)$$
$$X(i, 32-j+1) = X(i, j) \quad \textbf{.....(8)}$$

9- After applying the equations in the previous steps, we will mix the resulted mass and reframed it in a new matrix.
10- Replacing the main diameter elements for the resulted matrix of step (9) with secondary diameter elements for the same matrix to increase the strength of the encryption. The following Block Diagram explain Encryption Algorithm:

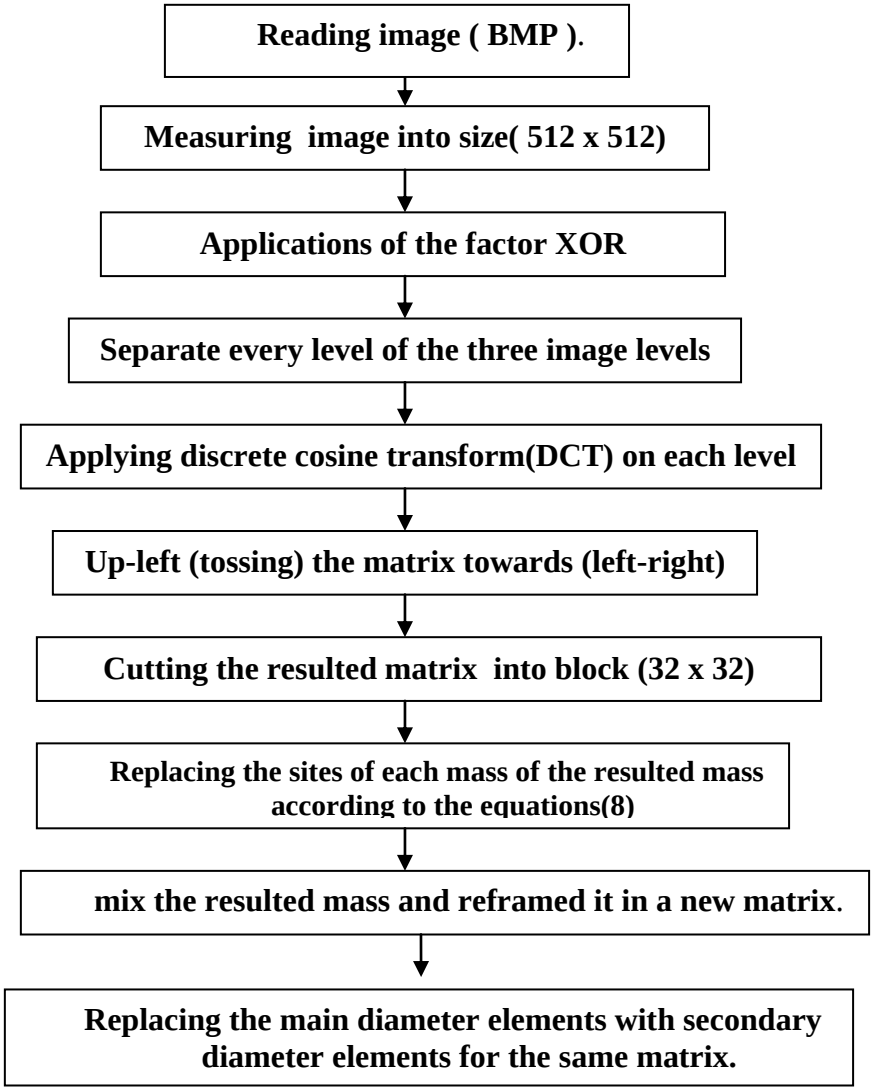


Fig.(3)The Block Diagram into Encryption Algorithm

DECRYPTION ALGORITHM

It is another main process in that system, where it includes similar operations for encryptions of the interlude image but it begins and these operations proceed in reverse direction of the previous operations, when it begins from getting the resulted image of the algorithm of encryption commencing from replacing the main diameters and end up by applying XOR factor.

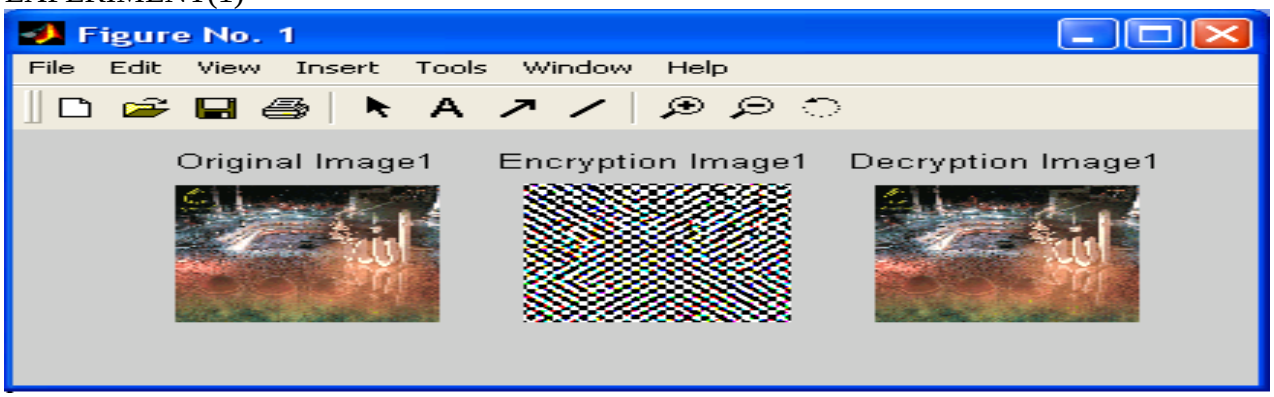
The steps of this algorithm are:

1- Replacing the elements of main diameters for the matrix with elements of secondary diameter for the same matrix.
2- Cutting each matrix into masses of size (32 x 32) in order to be treated in the next step.
3- Replacing all sites of each mass of the resulted mass according to the equations(8)
4- Tossing the matrix towards (left-right)
5- Applying the inverse discrete cosine transform on each level.
6- Gather all three levels from which image was divided into in the encryption algorithm.
7- Applying XOR factor that explained earlier its operation in encryption algorithm and the same used key.
8- Storing the resulting image from decryption with BMP extension.

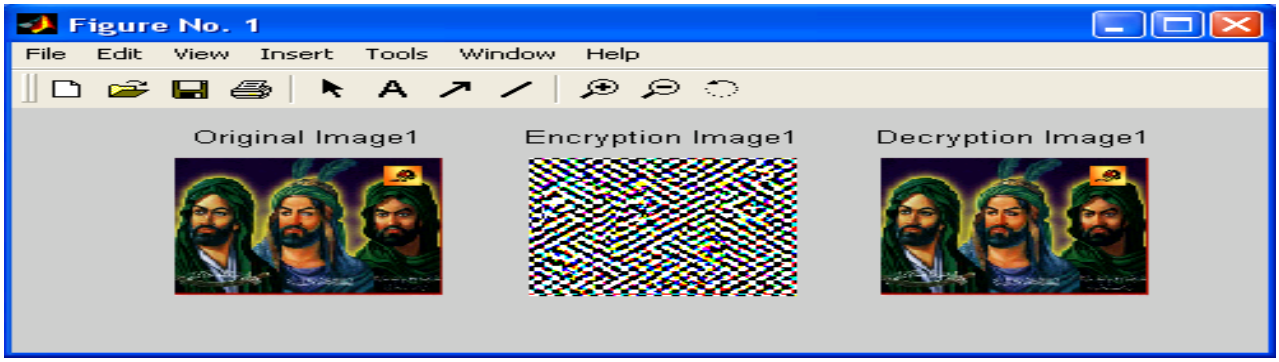
EXPERIMENTAL RESULTS

The experiments were conducted on the digital images in order to test the suggested method for encryption in which the following figures of the original images and encrypted image and the decrypted image, where the experiments showed that the suggested method with secure characteristics suitable in addition that its calculating has few complexity and less infected on the restore images with less influence against the reverse attack.

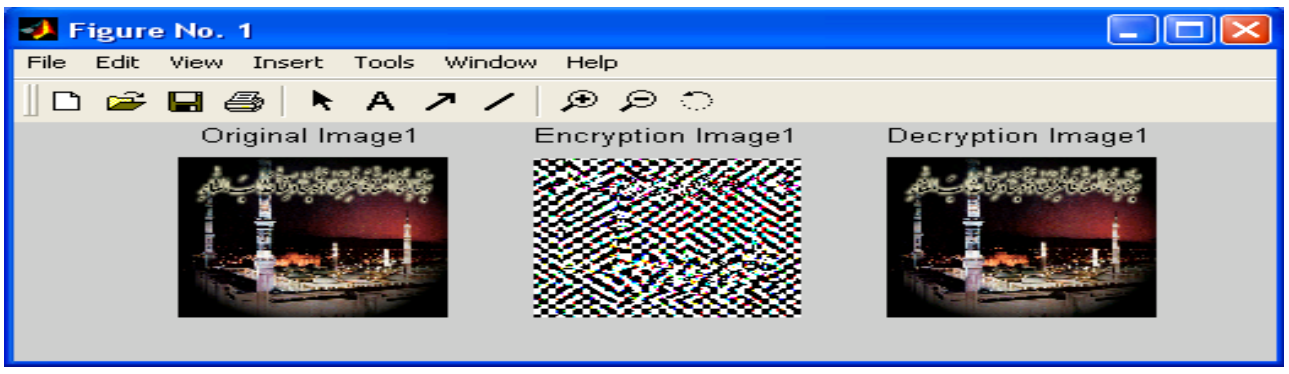
EXPERIMENT(1)



EXPERIMENT(2)



EXPERIMENT(3)



The results compared into the suggested method for encryption by calculate Peak signal-to-noise ratio (PSNR) is the standard method for quantitatively comparing a reconstructed image with the original. For an 8-bit grayscale image, the peak signal value is 255. Hence the PSNR of an M×N 8-bit grayscale image x and its reconstruction $\hat{x}$ is calculated as [10]:

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \qquad \text{.....(9)}$$

where the mean square error (MSE) is defined as:

$$MSE = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\left[x(m,n) - \hat{x}(m,n)\right]^2 \quad \text{.....(10)}$$

Application PSNR on three images previous and be results in the following table(1)

PSNR		Images
Image decrypted	Image original	
33.6531	32.0758	Image1
27.7998	25.3496	Image2
30.9268	30.7158	Image3

Table(1)Application PNSR into images

تشفير الصورة بالاعتماد على تقنية التحويل الجيب تمام المنفصل DCT

ساهرة عبيد سعد وميساء عبد الكريم ناصر

جامعة البصرة/كلية العلوم/قسم الحاسبات

الملخص

يهدف هذا البحث إلى أجراء عملية تشفير للصور الرقمية باستخدام طريقة مقترحة بالاعتماد على تقنية التحويل الجيب تمام المنفصل (Discrete Cosine Transform) وبعض الدوال المنطقية وتطبيقات برمجية . النمو السريع لشبكات الاتصال عبر الإنترنت وتطور التجارة الالكترونية وانتشار الأوساط الرقمية المختلفة مثل (الصور، الصوت، الفيديو) والتي أصبح من السهل الحصول عليها ونسخها وتوزيعها بأسماء أشخاص آخرين كل هذا أدى إلى خلق حاجة ملحة لحماية حقوق النشر واثبات الملكية وغيرها. أن التقنية المقترحة في هذا البحث تقنية التحويل الجيب تمام المنفصل تعتبر من التحويلات المهمة و الواسعة الانتشار في الوقت الحاضر في مجال تحليل ومعالجة الصور الرقمية .

حيث تم أخفاء معلومات الصورة لغرض سرية نقل الصور المحللة ،حيث لا يستطيع المهاجم استعادة الصورة إلا عند معرفته لتلك الطرق. لغرض التأكد من كفاءة الطريقة المقترحة تم اختبارها على مجموعة من الصور ذات التدرج الملونة *(RGB)* والتي أدرجناه في نهاية البحث.

Key words

Image , Encryption , Transform , Replacing

Figure Captions

REFERENCES

1) J.Bone., W.Puech.,M. Dumas.
"Crypto-Compression System for Secure Transfer of medical Images", 2 International Conference on Advances in medical Signal and Information Processing (MEDSIP 2004), September 2004.

2) B.Schneier.,
"Applied Cryptography, Second Edition: Protocols, Algorithm and Source Code in C", John Wiley & Sons, Inc., USA, 1996.

3) W.Stalling.,
'Cryptography and Network Security, Principles and Practice', Third Edition, Pearson Education International, Inc., USA, 2003.

4) A.H ,Tarish.,
Designing and Implementation a stream cipher cryptography system", M. Sc. Thesis, Computer Science Department, University of Technology, 2000.

5) S.E,Umbaugh.,
'Computer Vision and Image processing",
Prentice Inc., USA, 1998.

6) D.Salomon., "Data Compression, the Complete reference', Springer-Verlag, Inc., New York, 1998.

7) Broz Bozowrth, "Symbols, coding and Computers: Principles of Data Security", 1 Printing, 1989.

8) M. Orhan Altan, 'Digital image processing Techniques", Digital Photogrammetry, March 2000.

9) "Digital Image Processing", Rafael C. Gonzales & Richard E. Woods, Addison-Wisily Publishing Company, 1992.

10)M.Rabbani and P.W.jones,"Digital image compression Techniques", VolTT7,SPIE Optical Engineering Press,Bellvue,Washington(1991).