Ibn Al-Haitham Journal for Pure and Applied Science | مجلة إبن الهيثم للعلوم الصرفة و التطبيقية
No. 1 Vol. 25 Year 2012 | 2012 السنة 25 المجلد 1 العدد

Image Encryption Technique Using Lagrange Interpolation

O. Z. Akif

Department of Computer Science, College of Education Ibn Al-Haitham, University of Baghdad

Received in: 11April2011, Accepted in: 22May2011

Abstract

A new proposed technique used to encrypt the private image for secure transfer information. The proposed technique was designed using the Lagrange interpolation polynomial calculation in key generation and in encryption. A three stage for encryption and coding was proposed to complete the encryption of private image. RC6, Quadtree and Xor techniques were used in building the proposed technique. A short time in operation with a good visual encryption view encryption was got from implementing the proposed technique.

Keyword: image encryption, Lagrange interpolation ،image cipher, image coding.

Introduction

With an astounding growth in the field of network technology and multimedia technology, the wide spread dissemination of digital multimedia data is increasing at a fast pace. Increase in distribution of multimedia content over wired/wireless network is due to the applications like video on demand, video telephony, online photo sharing etc. Since the emerging wired and wireless IP networks are open networks, they are vulnerable to eaves dropping. Thus, confidentiality is especially important for secure multimedia distribution over IP based networks. Applications like internet telephony, Internet conferencing, Internet security monitoring and multimedia databases are few examples of audio visual data over IP based networks requiring confidentiality [1].

The security of digital images involves various aspects like copyright protection, authentication, confidentiality and access control. Copyright protection is ensured by embedding a digital watermark, having owner's private information into the original image. This watermark can be extracted from a questionable image when ownership needs to be resolved [1].

On the other hand, confidentiality and access control are addressed by encryption through which only authorized parties having the decryption key can access the encrypted content. Since, eavesdropping can be successfully prevented by the implementing an encryption technique, its use is highly recommended [1].

The traditional systems for visual confidentiality were based on scrambling or encryption techniques. Scrambling techniques are basically simple permutation operation or use of affine transformation in spatial domain. These schemes have high residual intelligibility and hence these low cost scrambling methods become vulnerable to attacks with the increase in computing power of modern computers. With the advancement in digital signal processing, scrambling techniques in the domain of orthogonal transforms, such as DFT, DCT are suggested. Though these new transform domain scrambling techniques have low residual intelligibility than the spatial domains, they are still vulnerable to known plaintext and chosen plaintext attacks. Hence, scrambling alone is not sufficient to make the multimedia data

secure for transmission over IP network. It needs to strengthen by some encryption method to make it robust against various attacks on the transmission channel [1].

Visual cryptography is introduced by first in 1994 Noar and Shamir. Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement [2].

1. Image Encryption

Encryption of multimedia content in an access control system is not simply the application of established encryption algorithms, such as DES (Data Encryption Standard), AES (Advanced Encryption Standard), RSA or IDEA (Ideal Data encryption Algorithm) to the multimedia data bit stream.

These conventional cryptographic algorithms have some clear limitations for multimedia applications. Firstly, they require a lot of computational resources which can be feasible in desktop computers but difficult in low power wireless channels. Secondly, delay is introduced in real time communications using these block based encryption techniques. Thirdly, encrypting the image in spatial domain with these techniques prevents the use of certain advanced processing operations which can be easily implemented in transform domain. Lastly, these conventional encryption algorithms do not consider the structural and statistical properties of multimedia data as they were initially developed for text data. Several other encryption techniques like SCAN based, chaos based, and optics based methods are proposed in the literature.

Due to the use of encryption or decryption process of multimedia contents, its speed is often critical in real time applications. The total encryption and decryption process are computationally demanding and time consuming, thus not suitable for real time communication. One solution to this problem of total encryption in power constrained real time communication is the use of partial encryption providing a certain degree of transparency. Selective encryption is also the requirement of many applications like Pay-TV or IP network, as confidential/total encryption of visual data is not required in such applications. Instead, it requires the content to be transparent to a certain extent to attract possible customers by providing a low quality version of multimedia content.

Only a subset of the entire data is encrypted instead of the complete data stream. The subset should be chosen in such a way that it introduces a desired level of degradation in the multimedia data. Encryption of only a selected portion of the multimedia data stream lowers the computational load both at the user as well as server end. Selective encryption strives for computational complexity rather than for maximum security.

It is best employed in the transform domain as it is easier to identify that what parts of data are critical for security, allowing different levels of security and transparency.

Moreover, it is easier to locate the selected data in frequency domain without any processing overhead.

Selective encryption of images in spatial and frequency domain is pursued by the researchers from the past decade for obvious reasons. A selective/transparent encryption technique was proposed by Droogenbroeck and Raphaël where the sign and magnitude of non-zero DC coefficients and some AC coefficients are encrypted. This technique does not provide high security as plaintext attacks are possible if encryption technique is not chosen carefully and it takes more execution time as, compression and encryption are two different stages.

It gives an obscured image and hence can be used for conditional access over IP based networks. Droogenbroeck extended the idea to multiple encryptions where different sets of

DCT coefficients are encrypted by different content owners. Thomas et al. proposed transparent encryption of the progressive JPEG modes by encrypting the leading AC coefficients instead of the trailing AC coefficients. It was proved that by encrypting the leading coefficients instead of the trailing coefficients, encryption effort can be reduced by a large amount. A scalable lightweight encryption for DCT transformed images was proposed by Yekkala et al., where only selected blocks are encrypted. The selected blocks are those blocks that contain edges, determined using a threshold value and rest of the blocks are left unencrypted.

The protection to the image can be varied by changing the threshold value which is used to identify the blocks containing edges.

The techniques used for selective encryption of images are implemented either in spatial or DCT domain, which has inherent problem of less security and blocking artifacts.

The digital content is scrambled or encrypted in wavelet domain before distribution in such a manner that it gives a degraded view or impression of the image for free to all users while only authorized users can view the clear content. An authorized user can be a person who pays to get the decryption/descrambling key. Conditional access finds its main use when a user browses a catalogue of multimedia files to view the degraded image, to select and then paying the amount to download the desired clear image. The subsequent sections discuss about the proposed work with results and statistics of the method employed [1].

2.Image Coding

The image can be encoded in several ways one of them is theencoding of an image using iterative encoding; this way consists of employing quad tree partitioning to determine all the ranges in the image For each range Ri, the domain Di that maps to it is shrunk by two in each dimension by averaging non-overlapping groups of 2 x 2 pixels. The shrunken domain pixel values are then multiplied by Si, added to Oi, and placed in the location in the range determined by orientation information, this operation the first iteration, normally about 10 iterations is sufficient to give an appropriate approximation for the fixed point. Further iteration does not generally improve the image. Pyramidal decoding is based on decoding a smaller replica of the image first.

A few iterations are subsequently applied to the small image itself, after which the new small image obtained is scaled to the required size to give the output image. The advantage is that less iteration are required on the scaled image to cause a proper convergence. This is expected since the image being iterated is smaller [3].

Hence, the decoding time is significantly shorter. In addition, a better peak-to-peak signal-to-noise ratio (PSNR), defined for a 8-bit grey-scale image as is expected.

$$PSNR = 10.\log_{10} \frac{255^2}{\frac{1}{\#\ pixels}\sum_{i}(a_i - b_i)^2} \quad \text{.....[1]}$$

Generally, all images decoded to a 128 x 128 image at first and then at a size twice larger each time, until the final image size is reached. For example, a 512 x 512 image is decoded at a low-resolution 128 x 128 image, and then the resolution is increased to a 256 x256 images, and finally to a 512 x 512 image. It should be pointed out that fractal encoding has the unique characteristic of using transformations that are resolution independent [4].

3. Quad tree Partition

There are various kinds of partitioning methods to compartmentalize ranges. For example, block-based partition, quad-tree partition, HV partition and Triangular Partition. In this project, we implement quad tree partition. The quad tree partition employs the well-known image processing technique based on a recursive splitting of selected image quadrants, enabling the resulting partition to be represented by a tree structure in which each non

terminal node has four descendants. The partition is constructed by selecting an initial level in the tree (corresponding to some Maximum range block size)and recursively partitioning any block for which a match better than some preselected threshold is not found [4].

In a quad tree partition, a square in the image is broken up into 4 equally sized sub squares, when it is not covered well enough by a domain.

This process repeats recursively starting from the whole image and continuing until the squares are small enough to be covered within

Some specified rms tolerance. Small squares can be covered better than large ones because contiguous pixels in an image tend to be highly correlated. To capture fine details while preserving a high compression ratio, a quad tree partitioning scheme is introduced under the encoding phase. That way, smooth areas can be represented with large range blocks (high Compression (, while smaller blocks are used as necessary to capture the details. During the procedure some ranges will be rejected and subdivided, thus, rendering the corresponding search void. Therefore, the

Maximal range size must not be chosen too large in order to avoid a large number of useless searches. An algorithm that works well for Encoding 256 x 256 pixel images based on this idea can proceed as follows. Choose for the collection D of permissible domains all the Sub squares in the image of size 8, 16, 32, and 64.

The quad tree partitioning allows the encoding scheme to take advantage of using large range blocks in smooth regions of the image, and smaller range blocks in more detailed parts of the image. This procedure also has the positive property of being easy to implement with a fully recursive approach [5].

4. Quadtree Parameters

Once the image is partitioned, we have to know the transform parameters for each partition. This is calculated as follows We can seek S and O to minimize the quantity

$$R = \sum_{i=1}^{n} (s \cdot a_i + o - b_i)^2 \quad \ldots\ldots\ldots\ldots (2)$$

$$s = \frac{\left[n \sum_{i=1}^{n} a_i b_i - \sum_{i=1}^{n} a_i \sum_{i=1}^{n} b_i \right]}{\left[n \sum_{i=1}^{n} a_i^2 - \left(\sum_{i=1}^{n} a_i \right)^2 \right]} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$o = \frac{1}{n} \left[\sum_{i=1}^{n} b_i - s \sum_{i=1}^{n} a_i \right] \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

Where ai is domain pixel and bi is range pixel, s represents “scale” value, o represents “offset” value, we can seek S and O to minimize the quantity [6].

5. The Lagrange Interpolation Polynomial

The problem of constructing a continuously defined function from given discrete data is unavoidable whenever one wishes to manipulate the data in a way that requires information not included explicitly in the data. The relatively easiest and in many applications often most desired approach to solve the problem is *interpolation*, where an approximating function is constructed in such a way as to agree perfectly with the usually unknown original function at the given measurement points. In the practical application of the finite calculus of the problem

of interpolation is the following: given the values of the function for a finite set of arguments, to determine the value of the function for some intermediate argument [7].

5.1 The Problem of Interpolation

The problem of interpolation consists in the following: Given the values yi corresponding to xi, i =0, 1, 2, . . . , n, a function f(x) of the continuous variable x is to be determined which satisfies the equation:

yi = f(xi) for i = 0, 1, 2 . . . , n …..(5)

and finally f(x) corresponding to x = x0 is required. (i.e. x0 different from xi, i = 1, n.)

In the absence of further knowledge as to the nature of the function this problem is, in the general case, indeterminate, since the values of the arguments other than those given can obviously assigned arbitrarily.

If, however, certain analytic properties of the function be given, it is often possible to assign limits to the error committed in calculating the function from values given for a limited set of arguments. For example, when the function is known to be represented able by a polynomial of degree n, the value for any argument is completely determinated when the values for n + 1 distinct arguments are given [7].

5.2 Lagrange Interpolation

Consider the function f : [x0, xn] R given by the following table of values :

x_k	x_0	x_1	...	x_n
$f(x_k)$	$f(x_0)$	$f(x_1)$	...	$f(x_n)$

….(6)

x_k are called *interpolation nodes*, and they are not necessary equally distanced from each other. We seek to find a polynomial P(x) of degree n that approximates the function f(x) in the interpolation nodes, i.e.:

$$f(x_k) = P(x_k);\ k = 0, 1, 2, \ldots, n.$$

The Lagrange interpolation method finds such a polynomial without solving the system.

Theorem: Lagrange Interpolating Polynomial

The Lagrange interpolating polynomial *is the polynomial of degree* n *that passes through* (n + 1)*points* y0 = f(x0), y1 = f(x1), . . .yn = f(xn) . *let:*

$$P(x) = \sum_{j=0}^{n} P_j(x)$$

……(7)

Where

$$P_j(x) \quad y_j \prod_{k=0, k\neq j}^{n} \frac{x - x_k}{x_j - x_k}.$$

……(8)

Written explicitly:

$$P(x) = \frac{(x-x_1)(x-x_2)\cdots(x-x_n)}{(x_0-x_1)(x_0-x_2)\cdots(x_0-x_n)}y_0 + \frac{(x-x_0)(x-x_2)\cdots(x-x_n)}{(x_1-x_0)(x_1-x_2)\cdots(x_1-x_n)}y_1 + \cdots + \frac{(x-x_0)(x-x_1)\cdots(x-x_{n-1})}{(x_n-x_0)(x_n-x_1)\cdots(x_n-x_{n-1})}y_n. \quad (9)$$

Lagrange interpolating polynomials are implemented in *Mathematic* as Interpolating Polynomials[data, var].For the case n = 4, i.e. interpolation through five points, we have:

$$P(x) = \frac{(x-x_1)(x-x_2)(x-x_3)(x-x_4)}{(x_0-x_1)(x_0-x_2)(x_0-x_3)(x_0-x_4)}y_0 + \frac{(x-x_0)(x-x_2)(x-x_3)(x-x_4)}{(x_1-x_0)(x_1-x_2)(x_1-x_3)(x_1-x_4)}y_1 + \frac{(x-x_0)(x-x_1)(x-x_3)(x-x_4)}{(x_2-x_0)(x_2-x_1)(x_2-x_3)(x_2-x_4)}y_2 + \frac{(x-x_0)(x-x_1)(x-x_2)(x-x_4)}{(x_3-x_0)(x_3-x_1)(x_3-x_2)(x_3-x_4)}y_3 + \frac{(x-x_0)(x-x_1)(x-x_2)(x-x_3)}{(x_4-x_0)(x_4-x_1)(x_4-x_2)(x_4-x_3)}y_4 \quad (10)$$

and

$$P'(x) = \frac{(x-x_2)(x-x_3)(x-x_4)+(x-x_1)(x-x_3)(x-x_4)+(x-x_1)(x-x_2)(x-x_4)+(x-x_1)(x-x_2)(x-x_3)}{(x_0-x_1)(x_0-x_2)(x_0-x_3)(x_0-x_4)}y_0 + \frac{(x-x_2)(x-x_3)(x-x_4)+(x-x_0)(x-x_3)(x-x_4)+(x-x_0)(x-x_2)(x-x_4)+(x-x_0)(x-x_2)(x-x_3)}{(x_1-x_0)(x_1-x_2)(x_1-x_3)(x_1-x_4)}y_1 + \frac{(x-x_1)(x-x_3)(x-x_4)+(x-x_0)(x-x_3)(x-x_4)+(x-x_0)(x-x_1)(x-x_4)+(x-x_0)(x-x_1)(x-x_3)}{(x_2-x_0)(x_2-x_1)(x_2-x_3)(x_2-x_4)}y_2 + \frac{(x-x_1)(x-x_2)(x-x_4)+(x-x_0)(x-x_2)(x-x_4)+(x-x_0)(x-x_1)(x-x_4)+(x-x_0)(x-x_1)(x-x_2)}{(x_3-x_0)(x_3-x_1)(x_3-x_2)(x_3-x_4)}y_3 + \frac{(x-x_1)(x-x_2)(x-x_3)+(x-x_0)(x-x_2)(x-x_3)+(x-x_0)(x-x_1)(x-x_3)+(x-x_0)(x-x_1)(x-x_2)}{(x_4-x_0)(x_4-x_1)(x_4-x_2)(x_4-x_3)}y_4 \quad (11)$$

Note that the function P(x) passes through the points (xi, yi), i.e. P(xi) = yi.

For Examples: The Lagrange an interpolating polynomial is given by

$$f_n(x) = \sum_{i=0}^{n} L_i(x) f(x_i) \quad \text{……………………………..…………(12)}$$

where n in $f_n(x)$ stands for the n^{th} order polynomial that approximates the function $y = f(x)$ given at $n+1$ data points as $(x_0, y_0), (x_1, y_1), \ldots\ldots, (x_{n-1}, y_{n-1}), (x_n, y_n)$, and

$$L_i(x) = \prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{x - x_j}{x_i - x_j} \quad \text{……………………………………………..(13)}$$

$L_i(x)$ is a weighting function that includes a product of $n-1$ terms with terms of $j = i$

Let Y = F(x) such that $y_o = f(x_o)$, $y_1 = f(x_1)$, $y_2 = f(x_2)$, … , $y_n = f(x_n)$, then to estimate value of f(x) we use :[8]

x_n	…	x_2	X_1	x_o	x
y_n	…	y_2	Y_1	y_o	F(x)

$$F(x^*) = \sum_{j=0}^{n} f(x_j) \prod_{\substack{i=0 \\ i \neq j}}^{n} \frac{(x^* - x_i)}{(x_j - x_i)} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(14)$$

Example 1: By Lagrange formula , find the value of f(3) and f(5) from the table .

4	2	1	0	X
5	2	1	1	F(x)

Solution:

$$F(3) = \sum_{j=0}^{3} f(x_j) \prod_{\substack{i=0 \\ i \neq j}}^{3} \frac{(3 - x_i)}{(x_j - x_i)}$$

$$= f(x_o) \frac{(3-x_1)(3-x_2)(3-x_3)}{(x_o - x_1)(x_o - x_2)(x_o - x_3)} + f(x_1) \frac{(3-x_o)(3-x_2)(3-x_3)}{(x_1 - x_o)(x_1 - x_2)(x_1 - x_3)} +$$

$$f(x_2) \frac{(3-x_o)(3-x_1)(3-x_3)}{(x_2 - x_o)(x_2 - x_1)(x_2 - x_3)} + f(x_3) \frac{(3-x_o)(3-x_1)(3-x_2)}{(x_3 - x_o)(x_3 - x_1)(x_3 - x_2)}$$

F(3) = 3.5

So by the same way we have F(5)=6 [7].

Inverse Interpolation

As shown, the equation of how to interpolation for function value corresponding to a given independent variable x was addressed. Suppose that, we have now reversed the equation so that we seek to determine on x value corresponding to a given functional value , then the problems becomes inverse interpolation , so we have :

$$x^* = \sum_{j=0}^{n} x_j \prod_{\substack{i=0 \\ i \neq j}}^{n} \frac{(y^* - y_i)}{(y_j - y_i)} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(15)$$

Example: find the value of x* , when y* = 2 ,

5	3	1	Y
2	20	15	x

Solution:

$$x^* = \sum_{j=0}^{2} x_j \prod_{\substack{i=0 \\ i \neq j}}^{2} \frac{(y^* - y_i)}{(y_j - y_i)}$$

$$= x_0 \frac{(2-y_1)(2-y_2)}{(y_0 - y_1)(y_0 - y_2)} + x_1 \frac{(2-y_0)(2-y_2)}{(y_1 - y_0)(y_1 - y_2)} + x_2 \frac{(2-y_0)(2-y_1)}{(y_2 - y_0)(y_2 - y_1)}$$

$$= 20.375 .$$

6. The Proposed System

The aim of this paper is to design and implement an image encryption system. The proposed system build from two three stages: first stage encrypted the image by using the Lagrange interpolation polynomial key generation and XOR operation. In this stage, the Lagrange interpolation polynomial was used to generate the encryption key by using a key numbers. The encryption operation for this stage is by using the XOR logic gate.

The second stage is to encode the encrypted image by using the Quadtree encoding. The resulted parameters (eqns 2,3, and 4) are used in the third stage.

The third stage is encrypted the resulted parameters from the stage two by using the RC6 algorithm. The result s encrypted parameters will encrypted by using the Lagrange interpolation polynomial calculation and key. In this stage, the encrypted key will be used to extract the Lagrange for each encrypted parameters. The encryption operations were applied to the results of encoding operation will keep the image format unchanged. The selection of coding parameters takes to get the secure partial encryption principles of image to reduce the encryption / decryption operation time with high efficient results. Additionally, the encryption/decryption operation is time efficient compared with encoding/decoding operation.

The quadtree encoding method was used due to ability of this method to coding hole image without error and with high speed efficient coding representation.

According to the secure partial encryption principles(in stage 3), the four parameters, i.e., the scaling and offset values Si and Oi for each range, domain that is mapped to it and the orientation information are more suitable for encryption image. In encoding, the image is partitioned into blocks, the fractal transform for each block is determined, the four parameters, i.e., Si, Oi, orientation information, and domains, are encrypted, and all the parameters are multiplexed and stored.

In decoding, the parameters are de-multiplexed, the four encrypted parameters are decrypted, and all the parameters are used to drive the decoding fractal transforms to restore the image depending on quadtree partitions and the symmetry operation to map the domain pixels onto the range pixels.

The RC6 is extended to support a key stream generator for image encryption which can overcome the problem of textured zones existing in other known encryption algorithms [8].

The some features of the RC6[8]:

History of algorithm: RC6 is derived from RC5. It was designed by Ron Rivest et al to meet the requirements of the Advanced Encryption Standard (AES) competition. The algorithm was one of the five finalists, and was also submitted to the NESSIE and CRYPTREC projects. It is a proprietary algorithm, patented by RSA Security.

Key size: The key size of RC6 is 128 bits.

Block size: The block size of RC6 is 128 bits.

Rounds: There are 20 rounds in the RC6 algorithms.

Security level of algorithm: The security margin of RC6 is 2076.

Known attack/threat: Not available so far.

1. The RC6 has 8 stages;
2. Stages 4 to 8 are repeated 20 times;
3. In the third step, the first and the second sub key S0 and S1 are used. Then each round of RC6 uses two sub keys; the first one uses S2 andS3, and successive rounds use successive sub keys. The flow chart of RC6 is as shown in Fig. 2 [8]

Figure 3 shows the block diagram of the proposed system. The steps of the proposed system are:

a. Loading the colored image and extract image: size, length, width, no. of color depth, and name.
b. Encrypt the image using the Lagrange interpolation polynomial key generation and XOR logic gate.
c. Image coding/ decoding using Quadtree.
d. Image coding parameters encryption/ decryption using RC6 algorithm with 128 bit key.
e. Encrypted image coding parameters encryption/ decryption using Lagrange interpolation polynomial.

From the Figure 3, the Lagrange interpolation polynomial is as shown in Figure 4.While the Lagrange encryption / decryption is as shown in Figure 5.

Results

The some results of the proposed system is as shown in figure 6 and 7. The encryption time calculation is as shown in table 1.

Conclusion

In this paper we have proposed new technique for encryption for a private image. This proposed system method given good results in visual encryption image views. In this proposed system, a short time for encryption for three stages in implements and test results. A short time in encryption the image because we select coding parameters scaling(S) and offset(O) and then encrypt this parameter by using the third encryption technique and encryption will not applied to whole image in this stage. Also, in the first stage, the encryption using XOR is very fast due to least complexity of this type of encryption. Thetechnique used for encrypted (RC6) gave good results as discussed previously.

References

1. Kulkarni, N. S. (2008),Balasubramanian Raman, AndIndra Gupta, "SELECTIVE ENCRYPTION OF MULTIMEDIA IMAGES", XXXII NATIONAL SYSTEMS CONFERENCE, NSC , December 17-19.
2. Revenkar, P.S.; AnisaAnjum, W .Z.Gandhare, (2010), Survey of Visual Cryptography Schemes", International Journal of Security and Its Applications, 4(2):April,.

3. Soyjaudah, K. M. S. and Jahmeerbacus, I. "Fractal image compression using quadtree partitioning", International Journal of Electrical Engineering Education39/1.
4.Salam, A. Thajeal,(2010), Secure Fractal Image Based on Quad tree", the Seventeenth Scientific Conference of College of Education,pp.115, May,.
5.BOUKELIF Aoued,(2005)" ACCELERATING FRACTAL IMAGE COMPRESSION BY DOMAIN POOL REDUCTION ADAPTIVE PARTITIONING AND STRUCTURAL BLOCK CLASSIFICATION", 3rd International Conference: Sciences of Electronic,Technologies of Information and Telecommunications,March 27-31–TUNISIA.
6.Yural Fisher Editor,"Fractal Image Compression, Theory and Compression",Chapter 1, 2, 3, 6
7. Khalid Ali Hussien, (2011) ,The Lagrange Interpolation Polynomial For Neural Network Learning, International Journal of Computer Science & Network Security ,11 (3), March.
8. Di Zhu, (2008), Profiling Symmetric Encryption Algorithms forImplantable Medical Devices", MSc THESIS, Faculty of Electrical Engineering, Mathematics and Computer ScienceDelft University of Technology,.

Table (1):The encryption time results

Encryption Time	Image Size	mage Encryption Sample
18.0 sec	600×800	Sample 1
20.0 sec	640×480	Sample 2
24,10 sec	600×800	Sample 3
26,34 sec	600×800	Sample 4
27,00 sec	600×800	Sample 5
10,00 sec	512×512	Sample 6

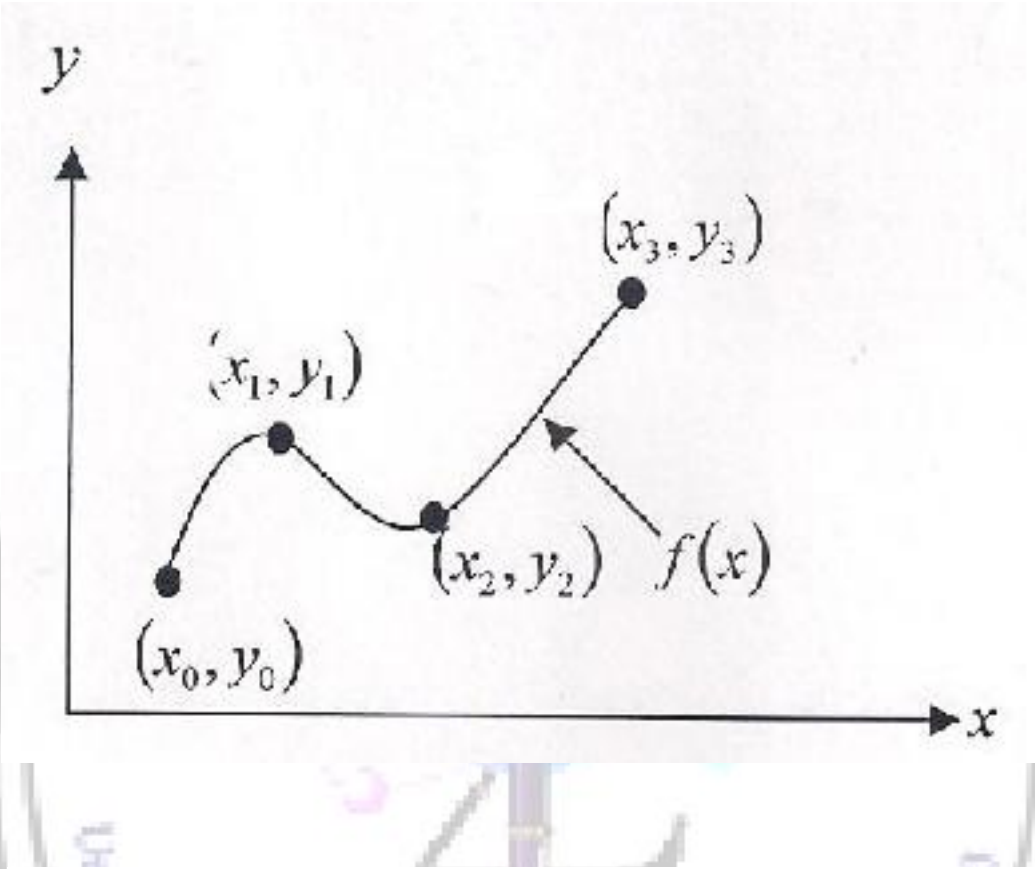


Fig.(1) : Interpolation of discrete data

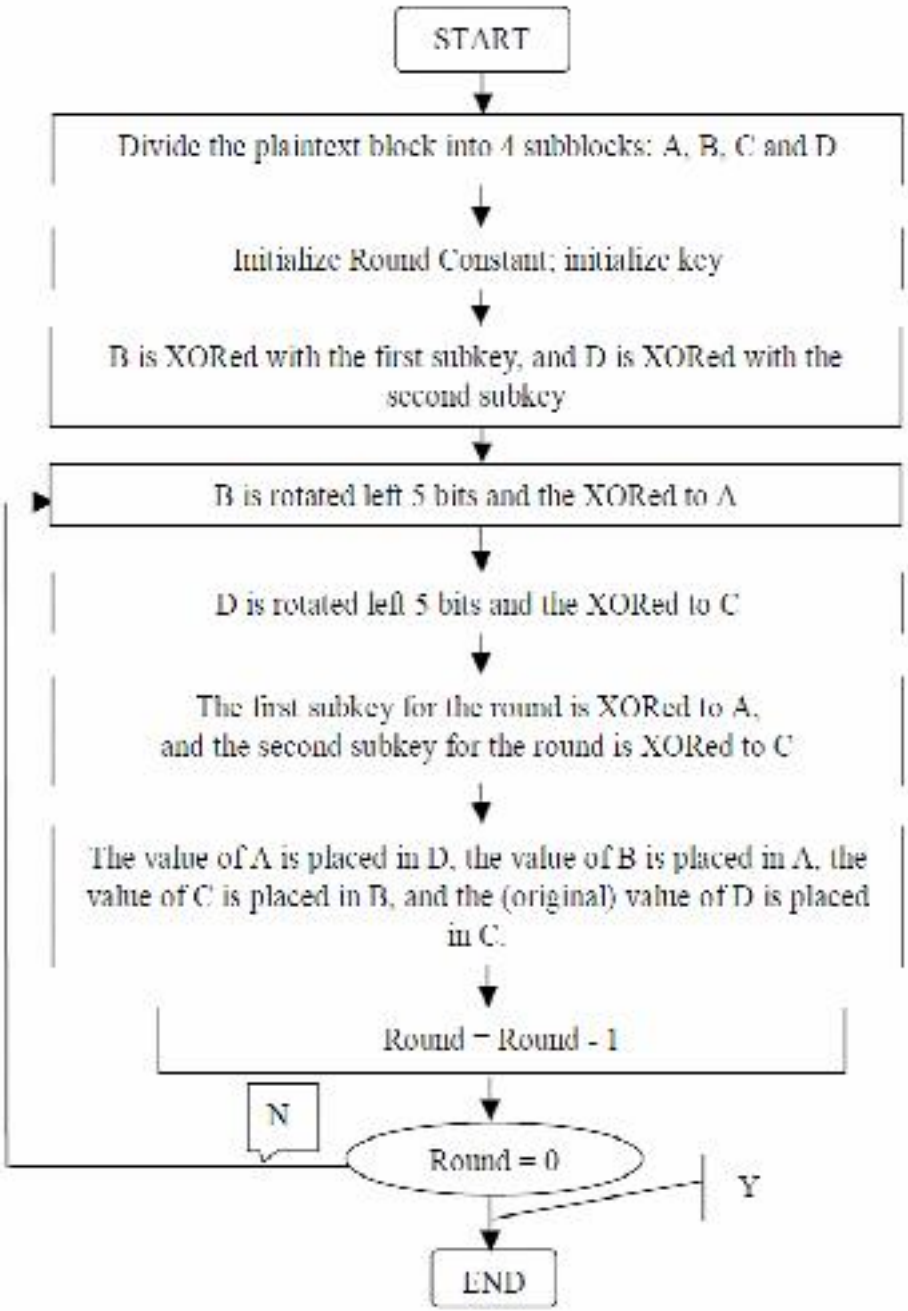


Fig. (2): Flow Chart of RC6 [8]

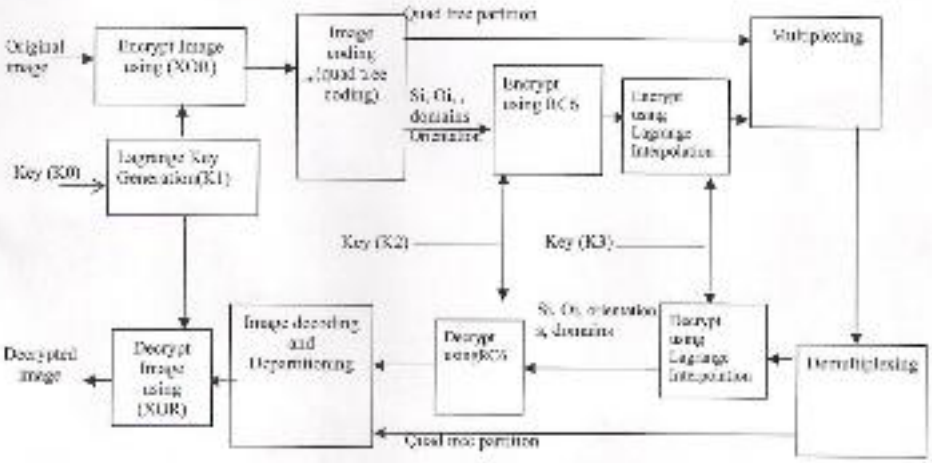


Fig.3 The proposed Image Encryption System

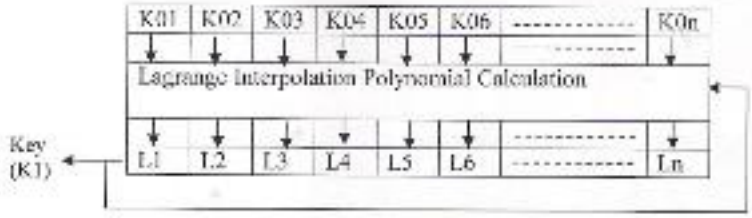


Figure 4 the Lagrange Interpolation Polynomial Key Generation. Note: Li is the Lagrange calculation output and K0i is the element of K0.

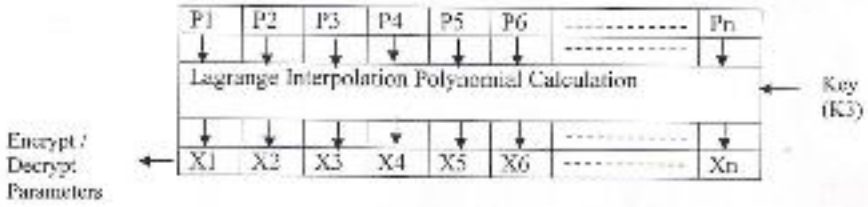
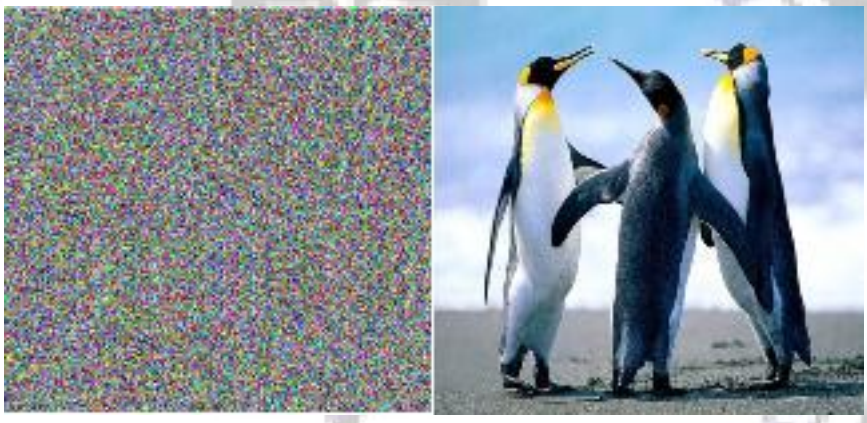


Figure 5 the Lagrange Interpolation Polynomial Encryption / Decryption. Note: Xi is the Lagrange calculation output (encrypt/decrypt results) and Pi is the element of parameters.

(a) original image (b) Encrypted Image by XOR (Stage 1)



(b) Encrypted Image (Stage 3) (c) Decrypted Image

Sample 1
(a) original image (b) Encrypted Image (c) Decrypted Image
Fig.(6): Some Result of proposed system

(a) original image (b) Encrypted Image by XOR (Stage 1)

(b) Encrypted Image (Stage 3) (c) Decrypted Image

Sample 2

Fig.(7): Some Result of proposed system

Ibn Al-Haitham Journal for Pure and Applied Science
مجلة إبن الهيثم للعلوم الصرفة و التطبيقية
No. 1 Vol. 25 Year 2012
العدد 1 المجلد 25 السنة 2012

تقنية تشفير صورة باستخدام استيفاء لاكرانج

عمر زياد عاكف
قسم علوم الحاسبات،كلية التربية ابن الهيثم،جامعة بغداد

استلم البحث في: 11 نيسان 2011 ,قبل البحث في : 22 ايار 2011

الخلاصة

التقنية المقترحة الجديدة المستعملة لتشفير الصور الخاصة لضمان نقل المعلومات السرية . صمّمت التقنية المقترحة باستخدام لاغرانج الاستيفاء لحساب متعدد الحدود في إنشاء المفتاح وفي التشفير. واقترح مرحلة ثلاثية التشفير والترميز لإكمال التشفير الخاص بالصورة.RC6، Quadtree و Xor هي تقنيات استعملت في بناء التقنية المقترحة بوقت قصير في عملية التشفير وعرض مرئي مشفر جيد حصل عليه من تنفيذ هذه التقنية المقترحة.

الكلمات المفتاحية: image encryption, Lagrange interpolation, image cipher, image coding