Lagrange Interpolation and OcTree for 2D-3DImage Encryption

Dr. Haider Kadhim Hoomod
Al-Mustansirya University-College of Education
Computer Science Department
Email: drhjnew@gmail.com

Abstract

A new proposed technique used to encrypt the private 2D-3D image for secure transfer information. The proposed technique was designed using the Lagrange interpolation polynomial calculation for encryption key generation. Three stages for coding and encryption was proposed to complete the encryption of private image.AES algorithm, OcTree and Xor techniques were used in build the proposed technique. A good time in operation with a good visual encryption view encryption was get from implement the proposed technique.

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

المستخلص :

تقنية المقترحة جديدة المستخدمة لتشفير الصور الخاصة ذات البعدين والثلاثة ابعاد لضمان نقل المعلومات السرية . تم تصميم تقنية المقترحةباستخدام لاغرانج الاستيفاء لحساب متعدد الحدود في إنشاء المفتاح التشفير. واقترح مرحلة ثلاثة التشفير والترميز لإكمال التشفير الخاص بالصورة.AES algorithm، OcTtree و Xor تقنيات استخدمت في بناء التقنية المقترحة. بوقت جيدلعملية التشفير وبعرض مرئيمشفر جيد تم الحصول عليه من تنفيذ هذه التقنية المقترحة.

1. Introduction

With an astounding growth in the field of network technology and multimedia technology, the widespread 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 eavesdropping. 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]

2. Image Encryption [1]

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.

3. Advanced Encryption Standard (AES) Algorithm [3]

In January 1997, the National Institute of Standards and Technology (NIST) invited proposals for new algorithms for the Advanced Encryption Standard (AES)to replace the old Data Encryption Standard (DES). After two rounds of evaluation on the 15 candidate algorithms, NIST selected the Irondale as the AES algorithm in October 2000.

The AES algorithm has broad applications, including smartcards and cellular phones, WWW servers and automated teller machines (ATMs), and digital video recorders. Compared to software implementations, hardware implementations of theses algorithm provide more physical security as well as higher speed. Figure2 shows the block diagram of AES algorithm.

The AES algorithm is a symmetric-key cipher, in which both the sender and the receiver use a single key for encryption and decryption. The data block length is fixed to be 128 bits, while the key length can be 128, 192, or 256 bits, respectively. In addition, the AES algorithm is an iterative algorithm. Each iteration can be called a round, and the total

number of rounds, Nr, is 10,12, or 14, when the key length is 128, 192, or 256 bits, respectively.
The 128-bit data block is divided into 16 bytes. These bytes are mapped to a 4x 4 array called the State, and all the internal operations of the AES algorithm are performed on the State.

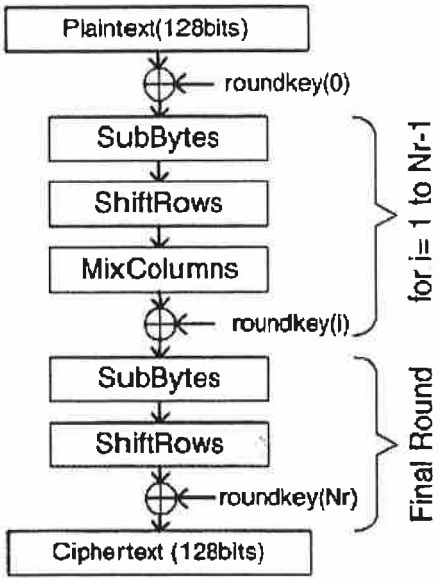


Figure 1The block diagram of the AES algorithm.

4. OcTree Coding [4]

In the literature we could not find a unique definition of an OcTree. Here, we consider an OcTree as a non-uniform but still highly regular and sparse discretization of a domain $\Omega \square R^d$, where d denotes the spatial dimension. To this end, we define an OcTree as a collection of discretization points xj and mesh-sizes hj as shown in figure 2.

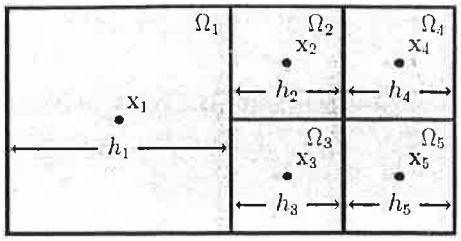


Figure 2: An OcTree discretization S_h in 2D

4.1 OcTree Definition[4]

Let $\Omega = (a_1, b_1) \times (a_2, b_2) \times \ldots \times (a_d, b_d) \subset R^d$ be a rectangular domain and $h \in R$ such that $(b_j - a_j)/h \in N$ for all j. We define an OcTree discretization S_h of with finest mesh-size h as:

$$S_h = \{(x_j, h_j) : j = 1, 2, \ldots, N\} \subset \Omega \times \{h \cdot 2^{\ell} : \ell \in N\} \ldots.(1)$$

such that the sub-domains $B_j := B(x_j, h_j) = \{y : ||x_j - y||_\infty < h_j/2\}$ essentially build a partition of Ω, i.e., $B_j \cap B_k = \emptyset$ for $j \neq k$, and $\bigcup_{j=1}^{M} \bar{B}_j = \bar{\Omega}$.

Furthermore, we make a few auxiliary definitions for neighborhood relations on Oc Trees, regularity of OcTrees, and nested Oc Trees, that will be useful in the following.

For $(x_j, h_j) \in S_h$ the set of direct neighbors is defined by:

$$Adj(x_j, h_j) = \{(x_k, h_k) \in S_h : (x_j, h_j) \neq (x_k, h_k) \text{ and } H^{d-1}(\bar{B}_j \cap \overline{B_k}) \neq 0\} \ldots(2)$$

where H^{d-1} denotes the $(d-1)$-dimensional surface measure.

An OcTree discretization S_h is called regular of m-th order if for all $(x_j, h_j) \in S_h$ it holds $2^{-m} \leq h_j/h_k \leq 2^m$ for all direct neighbors $(x_k, h_k) \in Adj(x_j, h_j)$.

In the following we refer to an OcTree S_h with the implicit understanding ofa first order regular OcTree discretization of finest mesh-size h.

Note that a zeroth order regular OcTree S^0_h is a cell-centered equispaced

discretization of Ω. In other words, S^0_h is the richest possible OcTree of finest mesh-sizes $h_j = h$ given by

$$S_h^o = \left\{(x, h): x_l = (a_l + h(k_l - \frac{1}{2})_{l=1}^d, k_l = 1, \ldots, \frac{b_l - a_l}{h}\right\} \quad \ldots (3)$$

An OcTree discretization $S_h$is nested in an OcTree discretization S'_hif forall (x,η) □$S_h$there exists a (x′, η′) □S'_h, such thatB(x, h) ∩B(x′, h′) = B(x, h).

The finest OcTree $S^0_h$is nested in any other OcTree discretization ofΩ .There are many possible data structures for a given OcTree. Here, the tree is stored as a sparse d dimensional array S. The relative size h_j/h ofeach cell is stored in the upper left corner of the cell. This allows us to use sparse matrix techniques in order to quickly find neighbors which are the major operation in the discretization process.. As a consequence, all that is needed to address a point of the OcTree is the sparse array S.

4.2 OcTree Approximation of Discrete Images[4]

Consider a discrete 2D image with m1 ×m2 pixels. Assume that this image has large regions with low variability. Then such an image can be efficiently represented by an OcTree. An optimal OcTree is the one that would have the least amount of cells for the given image. However, such an OcTree is difficult to find (i.e. exponentially difficult). A central point is that the overall complexity of Algorithm 1 is O(N)where N is the number of pixels in the image. Furthermore, we added at olerance parameter to 1. It is used as a threshold to decide weather the image is almost constant in a certain region. A representative 2D example, an OcTree discretization of a sample image is given in Figure 3 after applied the Algorithm 1.

Algorithm 1 Generate spare array representation S of an OcTree for a 2D image T where regions for color value differences than tol are treated as constant.

$[S] \leftarrow$ `generateOcTreeFromImage`(T, tol)

set $[m_1, m_2] \leftarrow \text{size}(T)$

Initialize $S(1{:}m_1, 1{:}m_2) \leftarrow 1$ and $T_{\min} \leftarrow T$, $T_{\max} \leftarrow T$

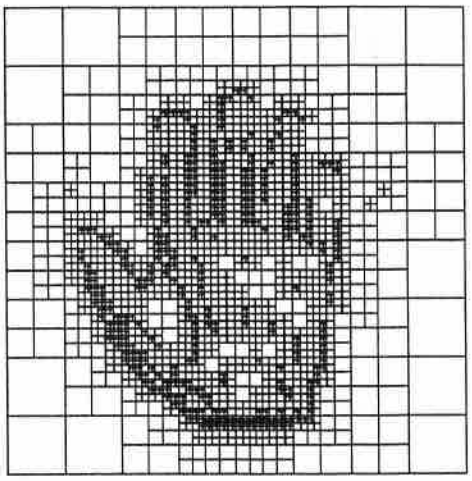
for $s = 2^{[0:\log_2(\min([m_1, m_2]))]}$

- find $(i_1, i_2) \in [1{:}s{:}m_1] \times [1{:}s{:}m_2]$ with $S(i_1, i_2) = s$
- get 4 sub-block indices of the super-block stored at (i_1, i_2) with size $2s$: $\mathcal{I} \leftarrow [i_1, i_1 + s] \times [i_2, i_2 + s]$
- compute minimum and maximum in the super-block: $T_{\min}(i_1, i_2) \leftarrow \min(T_{\min}(\mathcal{I}))$ and $T_{\max}(i_1, i_2) \leftarrow \max(T_{\max}(\mathcal{I}))$
- **if** $T_{\max}(i_1, i_2) - T_{\min}(i_1, i_2) \leq \text{tol}$ **then**
  set $S(i_1, i_2) = 2s$ and $S(\mathcal{I} \setminus (i_1, i_2)) = 0$,
  end if

end for

(a) original image T

(b) OcTree approximation $\hat{T}$



(c) OcTree

(d) absolute error $|T - \hat{T}|$ (scaled)

Figure 3: Approximation of an image with an OcTree (cf. Table 1, tol=15%)

5. The Lagrange Interpolation Polynomial[5]

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.

5.1 The Problem of Interpolation[5]

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 .....(4)

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 representable by a polynomial of degree n, the value for any argument is completely determinate when the values for n + 1 distinct arguments are given.

5.2 Lagrange Interpolation[5]

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

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

....(5)

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:*

$$P(x) = \sum_{j=0}^{n} P_j(x) \quad \ldots(6)$$

Where

$$P_j(x) = y_j \prod_{k=0, k\neq j}^{n} \frac{x - x_k}{x_j - x_k}. \quad \ldots.(7)$$

Written explicitly:

$$P(x) = \frac{(x-x_1)(x-x_2)\cdots(x-x_n)}{(x_0-x_1)(x_0-x_2)\cdots(x_0-x_n)}y_0 + \frac{(x-x_0)(x-x_2)\cdots(x-x_n)}{(x_1-x_0)(x_1-x_2)\cdots(x_1-x_n)}y_1 + \cdots + \frac{(x-x_0)(x-x_1)\cdots(x-x_{n-1})}{(x_n-x_0)(x_n-x_1)\cdots(x_n-x_{n-1})}y_n. \quad (8)$$

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

$$P(x) = \frac{(x-x_1)(x-x_2)(x-x_3)(x-x_4)}{(x_0-x_1)(x_0-x_2)(x_0-x_3)(x_0-x_4)}y_0 + \frac{(x-x_0)(x-x_2)(x-x_3)(x-x_4)}{(x_1-x_0)(x_1-x_2)(x_1-x_3)(x_1-x_4)}y_1 + \frac{(x-x_0)(x-x_1)(x-x_3)(x-x_4)}{(x_2-x_0)(x_2-x_1)(x_2-x_3)(x_2-x_4)}y_2 + \frac{(x-x_0)(x-x_1)(x-x_2)(x-x_4)}{(x_3-x_0)(x_3-x_1)(x_3-x_2)(x_3-x_4)}y_3 + \frac{(x-x_0)(x-x_1)(x-x_2)(x-x_3)}{(x_4-x_0)(x_4-x_1)(x_4-x_2)(x_4-x_2)}y_4 \quad (9)$$

For Examples: The Lagrangian interpolating polynomial is given by

$$f_n(x) = \sum_{i=0}^{n} L_i(x) f(x_i) \ldots (10)$$

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

$$L_i(x) = \prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{x - x_j}{x_i - x_j} \ldots (11)$$

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

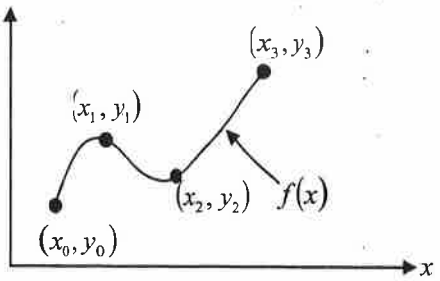


Figure 4 Interpolation of discrete data.

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

$$F(x^*) = \sum_{j=0}^{n} f(x_j) \prod_{\substack{i=0 \\ i \neq j}}^{n} \frac{(x^* - x_i)}{(x_j - x_i)} \quad \text{.....(12)}$$

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

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

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 $F(5)=6$.

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 reverse 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 :

$$x^* = \sum_{j=0}^{n} x_j \prod_{\substack{i=0 \\ i \neq j}}^{n} \frac{(y^* - y_i)}{(y_j - y_i)} \quad \text{.....(13)}$$

6. The Proposed System

The aim of this paper is to design and implement an2D-3D private image encryption system. The proposed system build from two three stages:

a. **First stage:** applied the OcTree to loaded image in order to encoding the private image and extract the Ωi, hi, xi for eachS(i,j) using equations (1-4) and algorithm 1 .
b. Second Stage: encrypted the encoding parameters resulted from OcTree algorithm for private 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.
c. The third stage is encrypts the resulted parameters from the stage two and whole resulted trees by using the AES algorithm. In this stage, the encryption key will generated by using the Lagrange interpolation and will be used in the AES algorithm.

The OcTree encoding method was used due to ability of this method to coding 2D and 3D images without error and with high speed

efficient coding representation. The proposed system will work efficient with two types of image (2D and 3D) but the encoding in 3D images have a little time more than 2D images type.

The AES 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.

Figure 5 shows the block diagram of the proposed system. The steps of the proposed system are:

The encryption phase:

a. Loading the colored image and extract image: size, length, width, no. of color depth, and name.
c. Image coding using OcTree algorithm.
b. Encrypt the coding parameters (Xi, Ωi, Si, and hi) for each space using the Lagrange interpolation polynomial key generation and XOR logic gate.

d. Encrypt the whole coding trees with parameters (encrypted in the above step) using AES algorithm with 128 bit key generated by Lagrange interpolation polynomial.
e. Display the resulted image and save it.

The Decrption Phase:

a. Loading the secure image and extract image: size, length, width, no. of color depth, and name.
b. Decrypt the whole coding trees with parametersusing AES algorithm with 128 bit key generated by Lagrange interpolation polynomial.
c. Decrypt the coding parameters (Xi, Ωi, Si, and hi) for each space using the Lagrange interpolation polynomial key generation and XOR logic gate.
d. Image decoding using OcTree algorithm.
e. Display the resulted image and save it.

The Lagrange interpolation polynomial is shown in Figure 6.

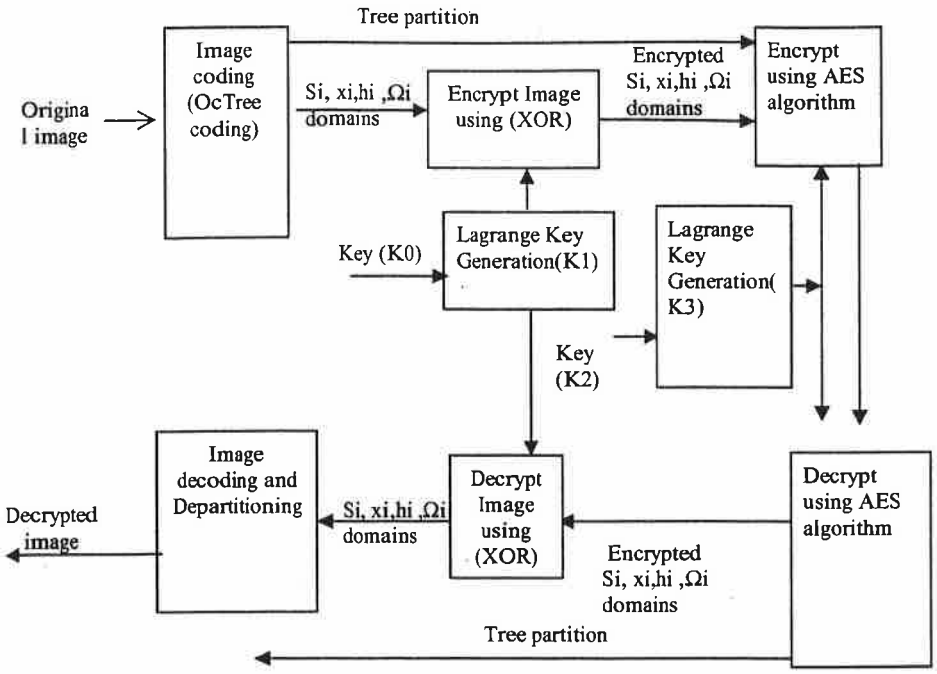


Fig.5 The proposed Image Encryption System

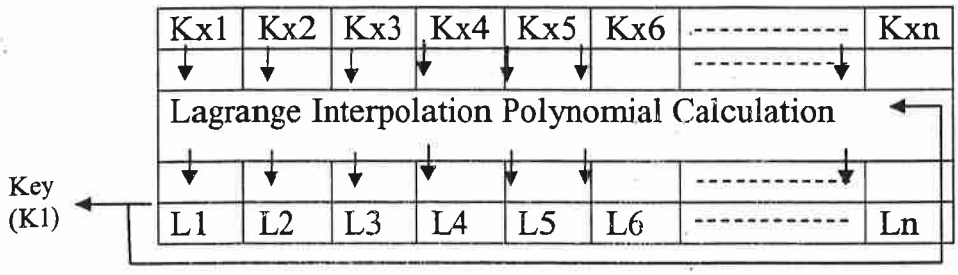


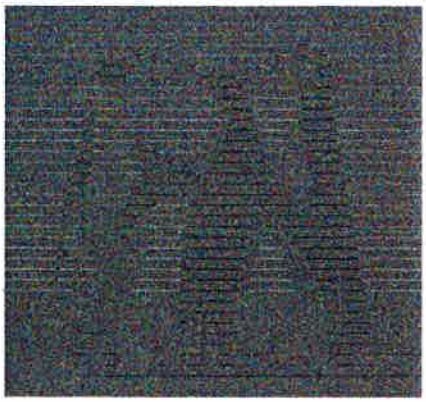
Figure 6 the Lagrange Interpolation Polynomial Key Generation. Note: Li is the Lagrange output key bits and Kxiis the element of Kx(x=0 or 2).

Results

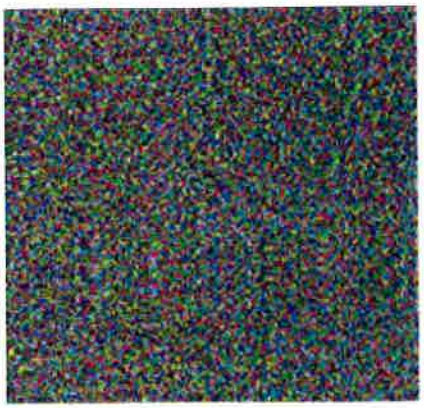
The some results of the proposed system are as show in figure 7,8and 9. The encryption time calculation is as shown in table 1.

Table 1 the encryption time results

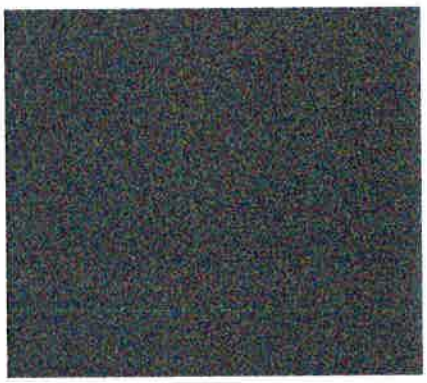
Image Encryption Sample	Image Size	Encryption Time
Sample 1	600×800	18.0 sec
Sample 2	640×480	20.0 sec
Sample 3	600×800	24,10 sec
Sample 4	600×800	26,34 sec
Sample 5	600×800	27,00 sec
Sample 6	512×512	10,00 sec



(a) original image (b) Encrypted Image by XOR (Stage 2)

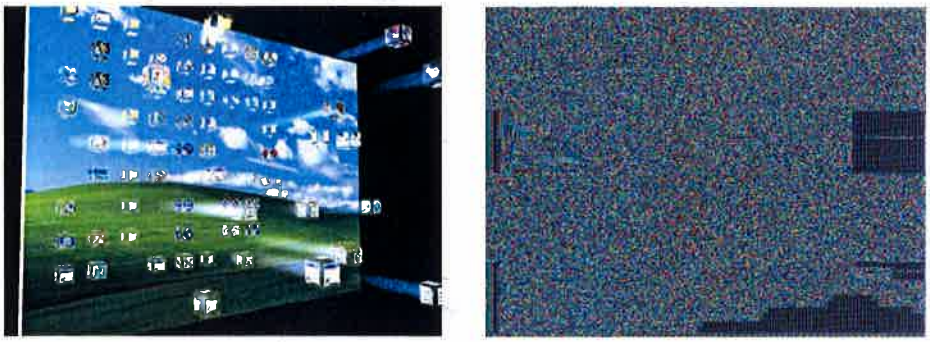



(b) Encrypted Image (Stage 3)(c) Decrypted Image Sample 1
Figure 7 Some Result of proposed system

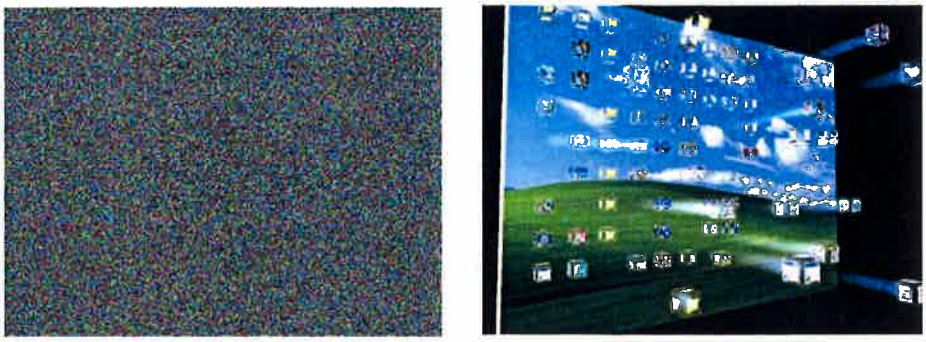



(a) original image (b) Encrypted Image by XOR (Stage 2)

(b) Encrypted Image (Stage 3)(c) Decrypted Image Sample 2
Fig.8Some Result of proposed system



(a) original image (b) Encrypted Image by XOR (Stage 2)



(b) Encrypted Image (Stage 3)(c) Decrypted Image
Fig.9 Some Result of proposed system

Conclusion

In this paper we have proposed new technique for encryption for a private image depending on the encoding technique (OcTree). This proposed system method given good results in visual encryption image views and structure.

In this proposed system, a good speed for encoding and encryption for three stages in implements and test results. The decrypt image lost some of the visual resolution due to encoding (OcTree).

References

[1]Nidhi S Kulkarni, Balasubramanian Raman, AndIndra Gupta, "SELECTIVE ENCRYPTION OF MULTIMEDIA IMAGES", XXXII NATIONAL SYSTEMS CONFERENCE, NSC 2008, December 17-19, 2008.

[2]P.S.Revenkar, Anisa Anjum, W .Z.Gandhare," Survey of Visual Cryptography Schemes", International Journal of Security and Its Applications, Vol. 4, No. 2, April, 2010.

[3]Xinmiao Zhang and Keshab K. Parhi, High-Speed VLSI Architectures for the AES Algorithm", IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 12, NO. 9, SEPTEMBER 2004.

[4] Eldad Haber, Stefan Heldmann and Jan Modersitzki, "An OcTree Method for Parametric Image Registration", Mathematics and Computer Science, EMORY UNIVERSITY, June 9, 2006

[5] Khalid Ali Hussien, "The Lagrange Interpolation Polynomial For Neural Network Learning", International Journal of Computer Science & Network Security ,VOL.11 No.3, March 2011.