Al-Mustansiriyah Journal of Science
Vol. 26, No 1, 2015

journal homepage:www.mjs-mu.com

New Watermark Technique Based on B^+ Tree and Mathematical Morphology

Hala Bahjet Abdul Wahab
Computer Science Department, University of Technology,

A r t i c l e i n f o

Received 28/5/2014
Accepted 29/9/2014

Key words:
Watermark Techniques, Mathematical Morphology, Image Processing, B^+ Tree Indexing, Parametric Polynomial And Lagrange Interpolation.

ABSTRACT

In this paper, a new gray level image watermarking approach based on B+ tree, parametric Lagrange polynomial and morphology operations is proposed. First, the new approach utilizes the B^+ tree to obtain the characteristic compression and efficient store with speed retrieval by building efficient indexing B^+ tree as database for many watermark image positions. Second, the new approach encrypts it by a symmetric encryption algorithm based on robust interpolation polynomial depend on time parameter (t) in its processing called parametric Lagrange polynomial (PLP). Third, it is exploiting the abilities of morphology operation to detect the border of host image objects to use in embedding stage based on different value pixels (DVP) method in order to increase the transparency features to embedding stage. Experimental results show using B^+ tree successful to give the facility to use more than watermark if needed with more flexibility**.** B+ tree produces high level indexing rate with efficient retrieval and solved the ambiguity problem that some embedding methods suffer. And using the B^+ tree with PLP solve time execution problem that appear with PLP when perform only. The proposed approach is invisible and robust against commonly used gray level image processing methods.

الخلاصة

قدمنا في هذا البحث، نهج جديد للعلامة المائية ذات المستوى الرمادي استنادا على الهيكل الشجري B^+ و متعدد الحدود لاغرانج و عمليات التشكل. أولا، النهج الجديد يعمل على الاستفادة من الهيكل الشجري B^+ للحصول على ميزات الضغط وكفاءة تخزين مع سرعة الاسترجاع عن طريق بناء فهرسة كفوءة للهيكل الشجري مثل قاعدة بيانات للعديد من مواقع العلامات المائية. ثانيا التشفير بواسطة خوارزمية تشفير متماثل بالاعتماد على قوة متعدد الحدود لاغرانج التي تعتمد على عامل الوقت (t) في معالجتها وتسمى (Parametric Lagrange polynomial). ثالثا، استغلال قدرات عملية التشكل (morphology) للكشف عن الحدود الموجوده في الصورة المضيف لأستعمالها في مرحلة الطمر أعتمادا على قيم مختلفة للوحده اللونيه (DVP) من أجل زيادة صفات الشفافية في مرحلة التضمين. أظهرت النتائج التجريبية أن أستعمال الهيكل الشجري نجح في الفهرسه على مستوى عالي مع كفاءة الاسترجاع وحل لمشكلة الغموض التي تعاني منها بعض أساليب التضمين. كما ان استخدام الهيكل الشجري مع متعدد الحدود معا نحجت في حل مشكلة الوقت التي كانت تظهر عند تنفيذ متعدد الحدود فقط .النهج المقترح هو غير مرئي وقوي ضد استعمالات طريقة معالجة الصور ذات المستوى الرمادي .

INTRODUCTION

A watermark is a unique or special image that is embedded on a paper or document that consist text or images. The watermark is designed in a way through which appears only when it is viewed by transmitted light or holding it in a particular angle [1, 2, 3]. Watermarks are used to identify the owner of the image/content and to prevent counterfeiting them. But, this was not possible in digital content. The vast growth of Internet has allowed users to copy the digital content and distribute them without control of ownership. Copy protection system is one of the widely used applications of digital watermarking [4]. It can be used either to prevent unauthorized copies of digital media or tracking the source of any data. Digital watermarking techniques provide high security to digital content by allowing only authorized person(s) to modify or detect the watermark [5]. Some recent watermark techniques [6, 7, 8, 9, 10, 11] prevent others from modifying or detecting the embedded watermark in a digital content. Watermarks that are embedded on a digital content should be imperceptible both statistically and perceptually. Once the watermark is embedded in a digital content, it is not possible to retrieve the original content by separating the watermark from the content. The quality of an image should not get affected when a watermarking is embedded to it. i.e., when a watermark is embedded in an image, it should not be visible to the naked eye. Each application might have data with different sizes to be embedded as watermark. The perceptual impact and robustness will be directly affected because of various sizes of data. Possibility is always there for a user to know the exact algorithm to detect and render to inactivate a watermark. Therefore, selecting a unique key for watermarking is the only way to secure it. Now, it is impossible for the unauthorized user to know the exact key even if he/she knows the exact algorithm. This increases the strength or reliability of the watermark. Visible

watermarks are similar the paper watermarks, as the watermarks will be visible to the naked eye. Invisible watermarks are imperceptible and cannot be viewed through naked eye. Numbers of techniques are used to implement invisible watermarking. An invisible watermark can be either robust or fragile. The use of a fragile watermark is important when one wants to verify if the protected media was tampered with or not.

Problem Statement

Robust watermarking is a technique in which modification to the watermarked content will not affect the watermark [1, 12, 13, and 14].

The B-tree was created by [15]. They are general classes of balanced multi way trees which serve as an indexing mechanism for structured data, and are geared in particular towards large paged files. Two classes of B-tree variants were recognized, B^+trees and B*trees, they offer additional properties over the original model**.** B-tree keeps data sorted and allows searches, sequential access, insertions, and deletions in logarithmic amortized time. The B-tree in which is a generalization of a binary search tree in that more than two paths diverge from a single node [16, 17]. B+ Tree is a variation of B-Trees a structure of nodes linked by pointers and anchored by a special node called the root, and bounded by leaves has a unique path to each leaf, and all paths have equal length stores keys only at leaves, and stores reference values in other, internal, nodes guides key search, via the reference values, from the root to the leaves.

The shape of the curve is basically based upon a set of control points that fundamentally describe its properties and its curvature. The algorithms that are used to generate the curves are primarily based on these control points. Thus if the intruder knows the set of control points it may lead to discover the shape of the curves with a trial and error on the method or algorithms that are originally used to produced the curve[21].

The rest of this paper is organized as follows. Lagrange polynomials are presented in section 2. Mathematical morphology are presented in section 3. B^+ tree are presented in section 4. In section 5 the proposed watermark approach is given. In section 6 the Performance Analysis for the proposed approach is presented. Finally, conclusion and discussion are presented in section 7.

Objective of Research

In this paper new approach to generate key watermark by using B+ tree as novel utilization to improvement digital image watermarking algorithms and to get good quality watermarked image for effective watermarking . The proposed approach consist of four preprocessing stage, B+ tree as compression and indexing stage, security stage based on parametric Lagrange polynomial and embedding stage based on methodical morphology.

Related Work

Several researches in the field of Digital Watermark were developed. The presents survey include previous related work to the research objective:

1- Suhad M. Kadhem "Using B+ Tree To Represent Secret Messages For Steganography Purpose"[22]. In this research was suggested approach based on used B+ tree for store the secret massages (that want to be sent) for increased the steganography system efficiency in a manner that prevent redundancy of these massages or even sub massages in order to provide efficient memory usage. Flexibility of the B+ tree gives good result to build many meaningful messages and builds a special dictionary. In this method, there is no ambiguity in retrieving secret message from its code.

2- D.Phani Kumar, G.RoslineNesakumari, S.MaruthuPerumal, "**Contrast Based Color Watermarking using Lagrange Polynomials Interpolation in Wavelet Domain**" [24]. Robust and blind color based watermarking scheme are proposed based on embeds color watermarks in color images using Langrage Polynomial Interpolation (LPI) in wavelet domain. Only a tiny quantity of information is required to extract the watermark key. From the watermark key easily can retrieved original color watermark from the watermarked image. The watermark key was generated by using chaotic mapping technique.

3- G.RoslineNesakumari,Dr.V.Vijayakumar, Dr.B.V.Ramana Reddy ,"**Generation of An Efficient Digital Watermark Key Based on Honey Comb Polynomial Interpolation Approach**" [25]. A new mechanism proposed consists of two stages for efficient authentication based on Honey Comb Polynomial Interpolation (HCPI) and Morphological Border Sorted Pixel Value Difference (MBSPVD) scheme. A simple polynomial interpolation technique on new hexagonal structure called Honey Comb structure (HCS) is used for generating the key of the digital watermark.

Theoretical Background

1- **Lagrangian polynomials**

Lagrange Interpolation formula is one of the most commonly used interpolation functions. When constructing interpolating polynomials, there is a tradeoff between having a better fit and having a smooth well-behaved fitting function. The more data points that are used in the interpolation, the higher the degree of the resulting polynomial, and therefore the greater oscillation it will exhibit between the data points. Therefore, a high-degree interpolation may be a poor predictor of the function between points, although the accuracy at the data points will be "perfect"[18],[19].The Lagrange interpolating polynomials $L_{N,K}$ has degree N and is 1 at $x = x_k$ and 0 at $x = x_j$ where $j \neq k$.

$$L_{N,K}(x) = \frac{(x-x_0)(x-x_1)\dots(x-x_{K-1})(x-x_{K+1})\dots(x-x_N)}{(x_K-x_0)(x_K-x_1)\dots(x_K-x_{K+1})\dots(x_K-x_N)} \quad (1)$$

$$= \frac{\prod_{\substack{j=0 \\ j\neq K}}^{N}(x-x_j)}{\prod_{\substack{j=0 \\ j\neq K}}^{N}(x_K-x_j)}$$

Note that $\prod_{K=1}^{N} K = 1.2.3\ldots N.$

The interpolating polynomial may be written as follows:

$$P_N(x) = \sum_{K=0}^{N} y_k L_{N,K}(x) = y_0 L_{N,0}(x) + y_1 L_{N,1}(x) + \ldots + y_N L_{N,N}(x) \quad (2)$$

It is just a linear combination of the Lagrange interpolation polynomials $L_{N,K}(x)$ with the y_K as the coefficients [20].

2- Mathematical morphology

Mathematical morphological, which started to develop in late of 1990's stand as a relatively separate part of image analysis. The word morphological commonly denoted a branch of biology that deals with the form and structure of the animal and plaints, we use the same word here in context of mathematical morphological as a tool for extracting image component that are useful to represent and description the region shape, such as boundaries . The most basic morphological operations are dilation and erosion. Dilation adds pixels to the boundaries of objects in an image, while erosion removes pixels from object boundaries. In the morphological dilation and erosion operations, the state of any given pixel in the output image is determined by applying a rule to the corresponding pixel and its neighbors in the input image [23].

A- Dilation

The *dilation* process is performed by laying the structuring element B on the image A and sliding it across the image in a manner similar to convolution but the difference is in the operation that is performed. With a dilation operation, all the 'black' pixels in the original image will be retained, any boundaries will be filled, as in figure 1.

$A \oplus B$

1- If the origin of the structuring element coincides with a 'white' pixel in the image, there is no change; move to the next pixel.

2- If the origin of the structuring element coincides with a 'black' in the image, make black all pixels from the image covered by the structuring element.

B- Erosion

The *erosion* process is similar to dilation, but we turn pixels to 'white', not 'black'. As in figure 2 slides the structuring element across the image and then follow these steps:

1. If the origin of the structuring element coincides with a 'white' pixel in the image, there is no change; move to the next pixel.

2. If the origin of the structuring element coincides with a 'black' pixel in the image, and at least one of the 'black' pixels in the structuring element falls over a white pixel in the image, then change the 'black' pixel in the image (corresponding to the position on which the center of the structuring element falls) from 'black' to a 'white'.

$A \Theta B$

C- Border

Border detection is an important function for object identification and is also a critical pre-processing step in image segmentation. Result of the final processed image is obtained by the detection of borders of an image. Mathematical Morphology (MM) is a new mathematical theory which can be used to process and analyze the images. It provides an alternative approach to image processing based on shape concept stemmed from set theory, not on classical mathematical modeling and analysis. In the MM theory, images are treated as sets and morphological transformations which derived from Minkowski addition and subtraction are defined to extract features in images. The structuring element (SE) decides the performance of morphological operation.

$G(A) = (A \oplus E) - (A \Theta E)$ (3)

Where G (A) denote the border of the image A. It is defined as the difference set of the dilation and Erosion [23].

B $^{+}$ Tree

B+ tree is called an index of database, such that each record will be stored in the database, the reference number (and the key) of that record will be stored in the B+ tree. So when we want to reach a certain record, we need to know its key to get its reference number from the B+ tree. When we get the reference number of that record we can retrieve the required record directly. B+ tree is an arranged and balanced tree (see figure 1), and this is why it is so fast in retrieving the required data. B+-trees distinguish internal and leaf nodes, keeping data only at the leaves, whereas ordinary B-trees would also store keys in the interior. B+ tree insertion, therefore, requires managing the interior node reference values in addition to simply finding a spot for the data, as in the simpler B-tree algorithm [15,16, 17].

B+ tree used as a special dictionary for storing data (with their codes) in a manner that prevent redundancy of these data or even sub data in this dictionary (in order to provide efficient memory usage), with Accordance to the following conditions [22]:

1. Store data in this dictionary (if it is not found) and get its unique code (at send process).
2. Retrieve the unique data when we have its code from this dictionary (at received process).

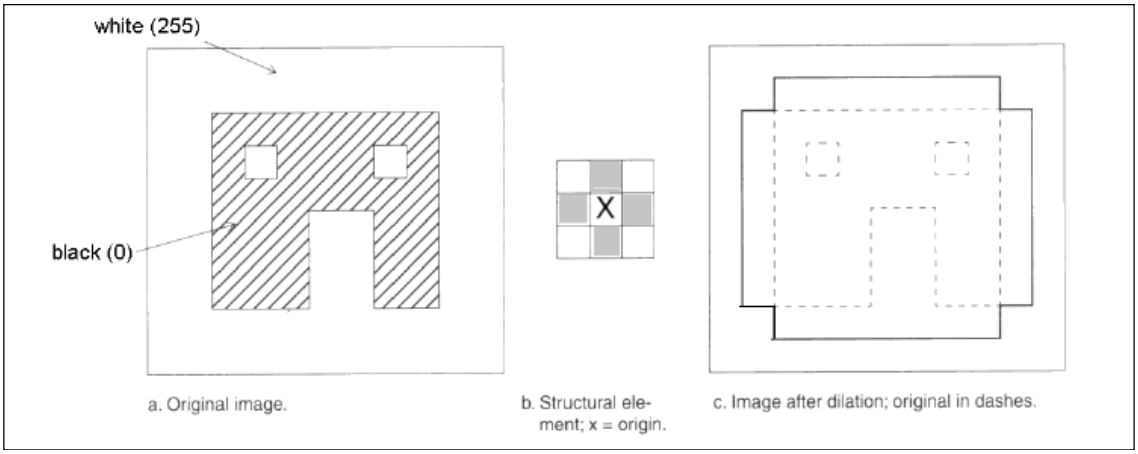


Figure1: Morphological dilation

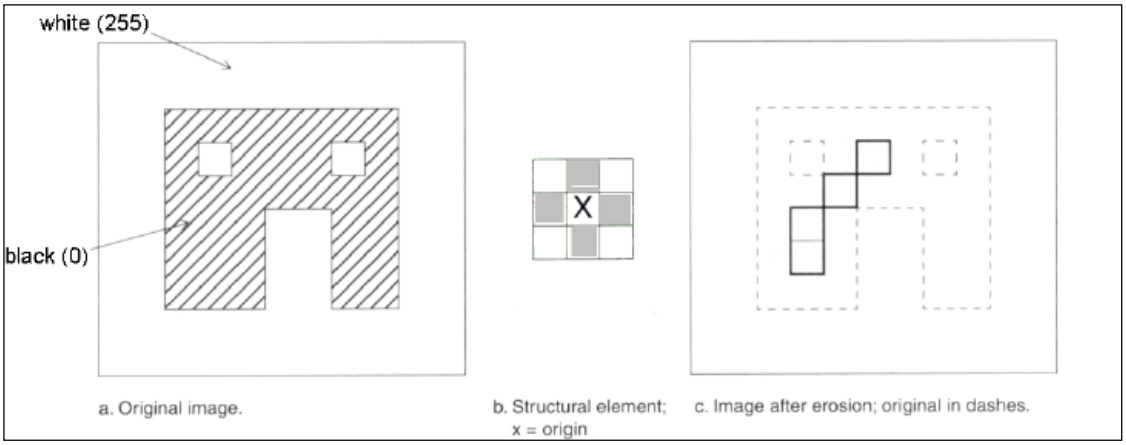


Figure 2: Morphological Erosion.

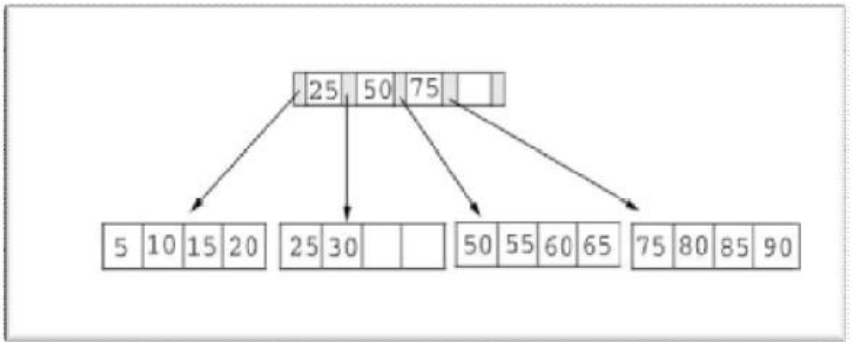


Figure 3: An Example of B^+ Tree.

The Proposed Approach

In the following section descript the main stages for the proposed approach at sender side that shown in figure (4). The proposed approach consists of three main stages. The first stage is Digital Watermark Key generation (DWK), based on sensitive pixel values from watermark image and B+ tree indexing method , Second stage is the security phase based on parametric Lagrange polynomial that represent as encryption stage, and third stage is embedded the encrypt DWT in the host image based on morphology operations.

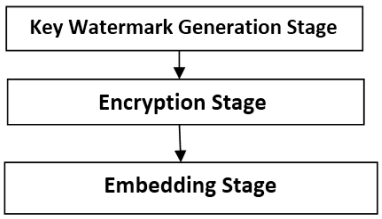


Figure 4: The Main Structure of the Proposed Approach.

1-Key Watermark Generation Stage

A-Preprocessing Operations

Generate watermark key is produce in this paper by using small as possible information that refer to watermark image that agreed between the authorized parties, I.e. the proposed approach starts by selecting the gray image watermark image(secret image) to generate the watermark key.

The preprocessing operations play main role on gray image to extract the positions (x, y) pixels only that contain the same pixels values for example white or black that refers to the main feature of the watermark image to represent the watermark key and store it in matrices (i.e.the proposed approach used the gray level image to reduce the B+ tree indexing size). Preprocessing operations perform on the Pixel Positions Vector (PPV) black or white, PPV divided in sub vectors according to the number of rows in order to preparing the compression operation that perform in B+ tree that illustrated in details in next subsection, figure (5) illustrates the preprocessing operations.

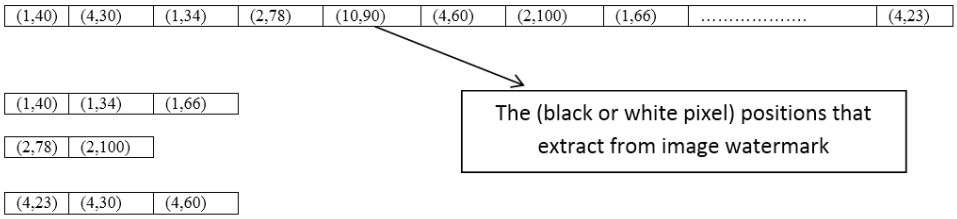


Figure 5: Preprocessing Operations.

B-Compress Operation Based on B+ Tree

B+ tree converts the DWK to small code numbers by investigating from the compression feature that available in B+ tree structure (indexing structure), that was operating in a manner that prevents redundancy of these DWK or even sub DWK in order to provide efficient memory usage.This stage represents by storing the one or more DWKs and getting its unique code based on B+ tree indexing, in order to reach unique codes for every DWK. One of the most important parameters, in this stage represented by ***code counter (n).***

This parameter refers to total number of rows of DWKs those stored in dictionary. The method uses one database(dbase) that represents the dictionary of the secret watermark position images and its corresponding codes, and uses two index trees (Bt1, Bt2) that refer to the same database (dbase). Each new secret image (positions) will be converted to a list of words and these words will be stored in dbase in a manner that prevents the redundancy of these positions or even sub positions. Bt1 is used for storing purpose to check if the row of positions or even sub positions is already found in dbase. So Bt1 use the first position of the row as a key, while Bt2 is used for retrieving purpose, so it uses the code of the position (DWK) as a key. In general the DWK is composed of [word1, word2, …,wordn].

In the following figure (6) shown the B+ tree algorithm to compress DWT to unique cods.

***Algorithm 1*: Compressed the Black pixel position values and get the unique code**

***Input*:** vectors for black pixel positions value after perform preprocessing operation

Output: List of code, Code counters (n).

Process:

Step 1: store the vector for position as matrices I(xi,yi)

Step2: For each row do the following{ store one image watermark position in B+ tree indexing}

2.1 If(row suppose as a (new row)Then do the following

1. Put the first position(x,y) of the row as a key in b+ tree (Bt1),
2. Compute the number of positions in the row
3. give the row a new unique code
4. and use this code as a key for b+ tree (Bt2)

2.2 If (row has points that already found in dbase) Then

- give it a new code
- store it in Bt2 as a key

2.3 If(row has points that already found in dbase except the last point) Then

- store the point in dbase and the reference of the previous point
- store at the previous point the new reference with its specific code ,
- Give it a new code

Step3: *For each row do the following* { store more than one image watermark in B+ tree indexing}

3.1 If (row has some points that are already found in dbase)Then

- Duplicated the common point between new row and dbase
- give its specific code for each point
- Store the point in dbase and the reference of the previous point with its specific code
- Store at the previous point the new reference with its specific code .
- Give it a new code.

Step 4: End

Figure 6: the B+ tree algorithm to compress DWT to unique cods.

2- Encryption Stage.

In this stage , represent a new improvement on watermark key generation technique, based on parametric Lagrange polynomial is use as encrypting function to encrypt DWK instead of traditional Lagrange polynomial to increase the security robust and solve the time execution problem that appear with traditional Lagrange polynomial . Parameterization method use efficient secure parameter (t) that increases the robust and complexity features for key watermark. A parametric Lagrange interpolation suggests the movement of a point through value of time (t), two function (x(t), y(t)). The position of the particle at time (t), increase the security in polynomial generation and for more effort for attacker. Where dealing with Lagrange polynomial from two dimensions (2D) to three dimension (3D) as show in equation below.

$$pi(t) = yi \prod_{k=1,k\neq 1}^{n} \frac{x-tk}{ti-tk} \quad (4)$$

Where:

$$P(t) = \sum_{i=1}^{n} pi(t) \quad (5)$$

The value of (ti) generate by using random generation to get the value of (t) more random and Difficulty guessing by attacker.

t(i)= t(i-1) *a +b (6)

Where a and b integer random value and b change by this equation ((b+2) mod i) to get more randomization for (t) value and prevent redundancy. And increased the isolation of the polynomial coordinates. The value of (t) the same at the sender and receiver just they agree about the initial value of (t (1), a, and b) value to generate the complete value of (t) vector.

That very important note any change in the value (a, b, t(1)) due to change the key generated because it dependent on (t) value. These values provide more flexibility features in key generation process to product different efficient keys.

The DWMK unique code that obtain from algorithm-1 use as inputs to parametric Lagrange polynomial function with pi(t).

In the following figure (7) shown the complete algorithm to generate parametric Lagrange interpolation.

Algorithm -2: Parametric Lagrange Interpolation Method

Input*:* control point of curve (xi,yi) where ***are list of code,.***t, and i=0 t0 n (where n is Code counter (n)),and t(i) than generate by the equation(6)

***Output*:** Digital watermark key (DWMK).

Process:

***Step 1*:** Let x=1

Step2: while (x<=n) do

Step3: let sum=0

***Step 4*:** For i = 0 to n do

***Step 5*:** Let p = 1

***Step 6*:** For j = 0 to n do

Step 7: if i and j are not equal then let

p= p $\frac{x-tk}{ti-tk}$

step8: next j

Step 9: sum=sum + p *xi

Step10: next I; f(x) =sum

Step11: x=x+1

Step 12: End

Figure 7: Generate Parametric Lagrange Interpolation.

3- **Embedding Stage**

Watermark key is embedded in the sorted pixel locations of morphological border pixels on host image using morphology operations to extract the border that illustrated in section (2). This approach overcomes the weak robustness problem of embedding the watermark. The basic PVD method, determines whether the two consecutive pixels belong to an edge or smooth area by checking out the difference value between two consecutive pixels. If the difference value was large, i.e. the two pixels are located in an edge area; more secret data can be hidden here. On the contrary, if the difference value was small, i.e. the two pixels are located in a smooth area; less secret data can be embedded. Therefore, this scheme produces watermarked images that are more similar to the original images than those produced by LSB substitution schemes, which directly embed secret data into the covering image without considering the differences between adjacent pixels for more detail see [23].

Algorithm:" Multi-structure elements morphological border detection"

Step 1: Construct structure elements *Er* of different directions according to the method presented section (C).

Step 2: Use the structure elements got in step 1 respectively to detect the borders Gr *(D)* of original image by morphological gradient border detector.

Gr(D) = (D ⊕E) – (D ⊖E)

Step 3: According to every detected border *Gr (D)* in step 2, use synthetic weighted method to calculate final detected border by:G (D) =$\sum_{r=1}^{m} Wr\ Gr(D)$

Where: G *(D)* is the final detected border of original image, *m* is the number of structure elements and Wr is the weight of different detected border information. It can be calculated by different methods. In this paper, we calculate Wr *by* w = 1/ *m***.**

The proposed watermarking approach which is used to embed the watermark key in the host image is summarized in the following figure (8) that shown an example in the sender side.

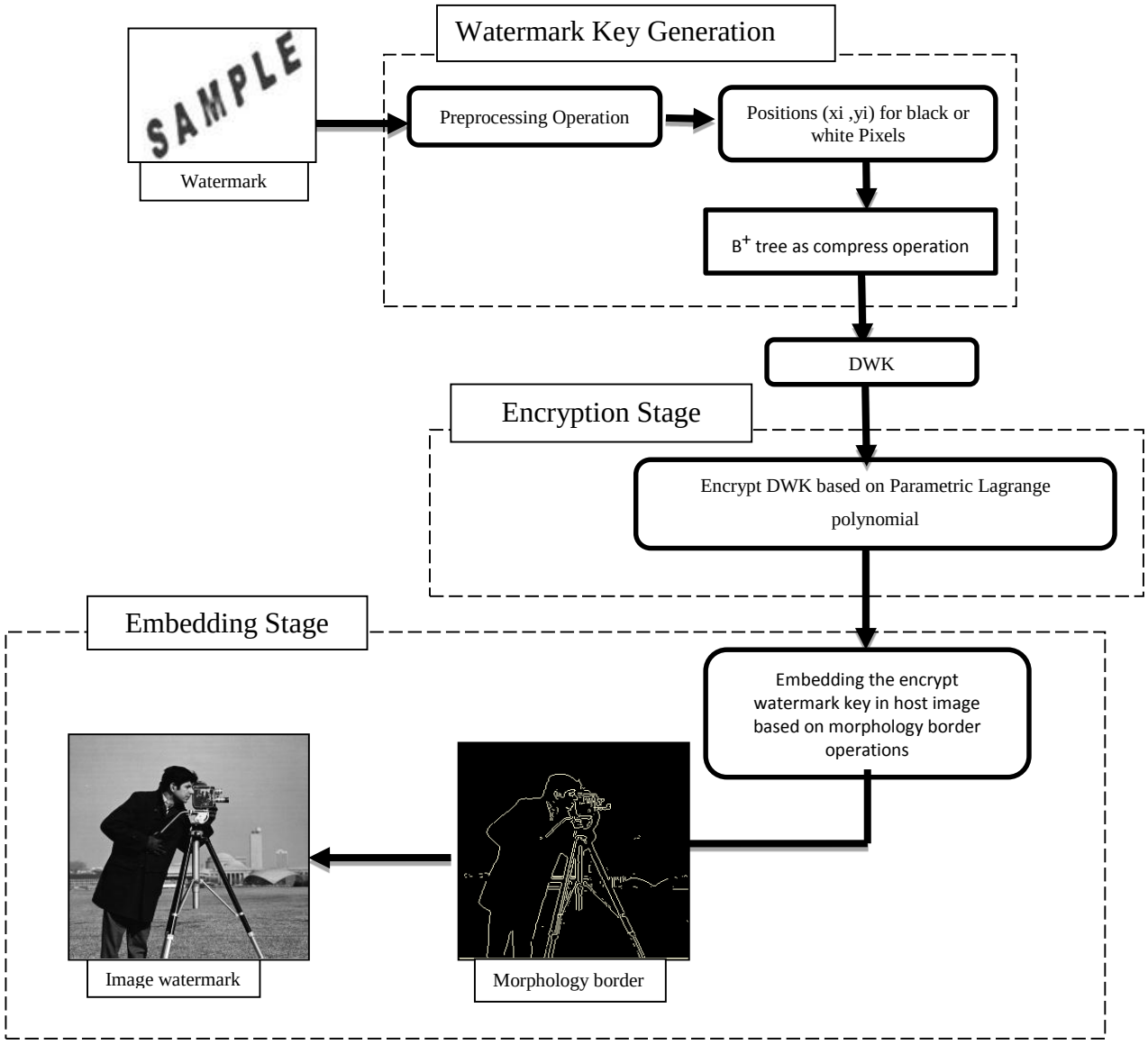


Figure 8: the Proposed Approach in Sender Side.

Algorithm-3: Retrieve the Unique Position White Pixels from List of Code
Input: List of code
Output: vector for whit pixel position

Process:
Step1: For each code in List of code do the following
If(the code is found in Bt2) **Then** do the following
1. Retrieve the term of the last point of the vector that the code refer to it
2. Search in the list of this term on this code
3. Get the length of the row that have the last point, and the reference of the previous point
4. Follow the reference of the previous point with their specific code, and take its point and concatenate it with next point, then follow the reference of its previous point with their specific code and so on, until we get the row.
Step 2: End

Figure 9: The B+ Tree Algorithm to Retrieve the DWK.

Reconstruct Watermark Process

Extraction procedure is a nature blind extraction which uses only host image as input. Morphology operations started on watermarked image extract the DWK. DWT is decrypt using parametric Lagrange polynomial as symmetric encryption key to obtained on sequence of unique codes, apply B+ tree algorithm to speed retrieve the black pixel position for watermark image and reconstruct the watermark. In the following figure (9) shown the B+ tree algorithm to retrieve the DWK.

Example

In the following simple example illustrated the storing with compression features that available in B+ tree to produce compression unique cods (DWT).

- B+ tree store one watermark image positions

Image 1 (position vectors) =
[(1,4),(1,6),(1,7),(1,8)……]
[(2,3),(2,4),(2,5),(2,10),…….]
(1,4)→ 00001 word ([ind(1,4),00011,~0,0,1)])

00010 word ([ind(1,5),00011,00001,0,0)])
00011 word ([ind(1,6), 00100, 00001,0,1)])
00100 word ([ind(1,7), 01000, 00011,0,1)])
01000 word ([ind(1,8), ~0,00100,4,1)]) --- 1

- B+ tree store multi images

Image vector 1= [(1,4), (1,6), (1,7), (1,8), (2,3), (2,4), (2,5), (2,10),……]
Image vector 2= [(1,4), (1,5), (1,6), (2,3), (2,4), (2,5), (2,10), ……]

(1, 4)→
00001 word([ind(1,4),00011,~0,0,1)])
00001 word([ind(1,4), 00010,~0,0,2)])
00010 word([ind(1,5),00011,00001,0,2)])
00011 word([ind(1,6), 00100, 00001,0,1)])
00011 word([ind(1,6), 00100, 00010,3,2)])-------- 2
00100 word([ind(1,7), 01000, 00011,0,1)])
01000 word([ind(1,8), ~0,00100,4,1)])--------1

- **Retrieve process from B+ tree to obtain from positions vector** If code =1 then

Code (1) have 4 points, and will connate them from
1. Ref (01000) is pointer to(00100) that have (1,7) with code 1.

2. Ref (00100) is pointer to two references, Ref(00011) that have (1,6) with code 2 and Ref (00011) that have (1,6) with code 1. B^+ tree will match the code and retrieve the specific point with code 1.

3. Ref(00011) is pointer to (00001) that have two previous references ,Ref(00001) that have (1,4) with code 2 and Ref(00001) that have (1,4) with code. B+tree will match the code and retrieve the specific point with code 1.Code=1,{(1,4),(1,6),(1,7),(1,8)}.
The entire reconstruct process of the proposed approach is as shown in Figure (10).

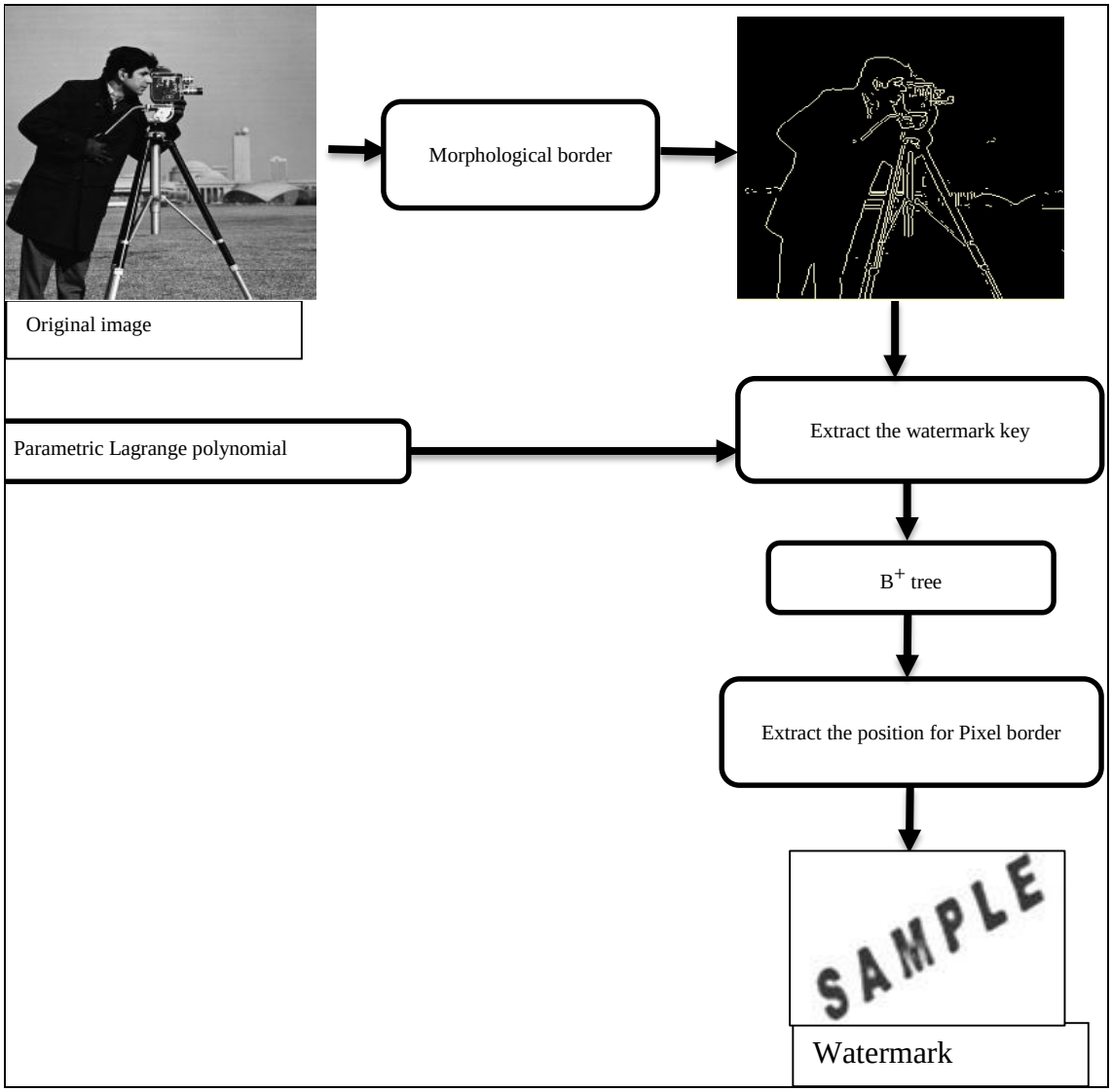


Figure 10: Reconstruct Watermark of the Proposed Approach.

Results and Discussion

The proposed approach is experimented on all 4 images Cameraman, Lena, and lines of size 256×256 of Figure (11). The gray watermark considered for the experiments with different of sizes as shown in Figure (12). Figure (13) represents the boundary images based on morphological boundary algorithm given in stage-2. Figure (14) represents the watermarked images using the proposed approach. The watermark key bits are inserted in the boundary pixel locations. Table (1) shows the Mean Square Error Ratio (MSE), Peak Signal-to-Noise Ratio (PSNR) and similarity tests values for all the 4 images. From the Table (1) it is clearly evident that all the images show high MSE, PSNR and similarity values which indicate high robustness and high quality of image after watermark insertion. Using B+ tree indexing as store and compression stage gave efficient compression data rate from black pixels position of watermark, table(2) shows the indexing ratio to five watermark samples and B^+ tree indexing succeed to reach the following features:-

- Efficient time in storing and in retrieving the DWK
- Solved the ambiguity problem that some steganography methods suffer from.
- Providing high capacity for steganography stage.

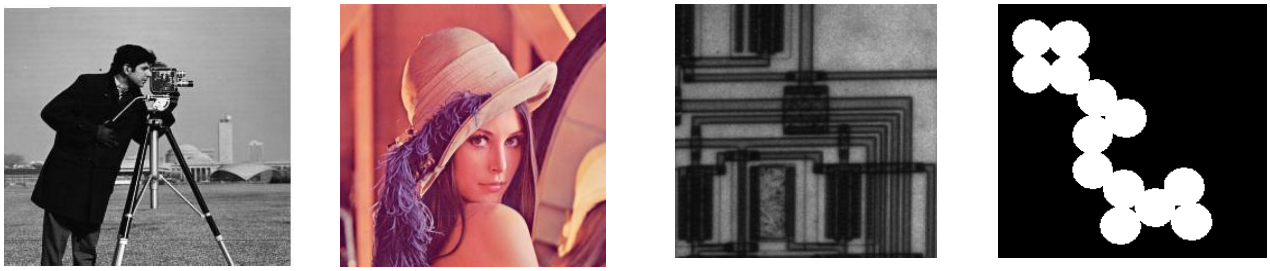


Figure11: The Host Images.

Figure12: The Morphology Images

Sample-1 Sample-2 Sample-3 Sample-4 Sample-5

Figure13: Watermark Samples (Logo).



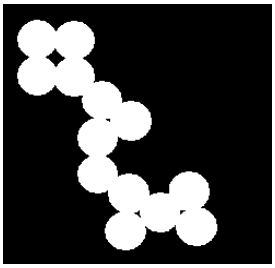



Figure14: Watermark Images.

Table1: Imperceptible Test

Host Image watermark	MSE	PSNR	similarity
cameraman	144.5	58.14	1
Lena	131.34	47.54	1
Lines	94.40	46.63	0.96
Circles	83.86	45.21	0.98

Table 2: B^+ Tree Indexing Ratio.

watermark samples	size	rows	columns	Indexing ratio
Sample-1	3.35 KB	251	201	88%
Sample-2	2.81 KB	290	208	85%
Sample-3	1.10 KB	112	80	89%
Sample-4	4.08 KB	189	267	87%
Sample-5	991 KB	80	113	90%

Table3: Fidelity Criteria for Gray Logo Comparison between Traditional and Proposed Approach

Logo size	Traditional Lagrange			Parametric Lagrange			The proposed approach		
	MSE	PSNR	SIM	MSE	PSNR	SIM	MSE	PSNR	SIM
32*32	24.82	33.23	0.99	40.20	32.08	0.99	46.72	31.52	0.97
50*50	32.1	32.07	0.98	81.84	29.00	0.98	106.7	29.76	0.98
60*60	18.49	35.46	0.99	12.60	37.12	0.99	46.52	31.54	0.96

Table4: Time Executed Comparison between the Traditional and Proposed Approach.

Logo Size	Traditional method Time	Parametric Lagrange Time	The proposed approach
32*32	3.47m	2.17m	0.02m
50*50	6.46m	3.45m	0.04m
60*60	7.01m	3.14m	0.07m

Table 5-1: Gray Logo with 10% Cropping Attack.

Logo size	Traditional method			Parametric Lagrange			Proposed approach		
	MSE	PSNR	SIM	MSE	PSNR	SIM	MSE	PSNR	SIM
32*32	23.95	34.33	0.99	40.20	32.08	0.99	45.72	31.52	0.99
50*50	320.1	32.07	0.89	81.84	29.00	0.98	108.7	27.76	0.95
60*60	18.49	35.46	0.99	12.60	37.12	0.99	45.52	31.54	0.99

Table 5-2: Gray Logo with 15% Cropping Attack.

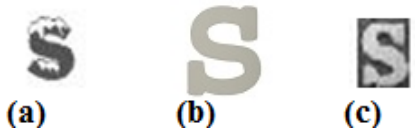
Logo size	Traditional method			Parametric Lagrange			Proposed approach		
	MSE	PSNR	SIM	MSE	PSNR	SIM	MSE	PSNR	SIM
32*32	23.95	34.33	0.99	40.20	32.08	0.99	45.72	31.52	0.99
50*50	320.1	32.07	0.89	81.84	29.00	0.98	108.7	27.76	0.95
60*60	18.49	35.46	0.99	12.60	37.12	0.99	45.52	31.54	0.99

Table 5-3: Gray Logo with Salt and Pepper Attack.

Logo size	Traditional method			Parametric Lagrange			Proposed approach		
	MSE	PSNR	SIM	MSE	PSNR	SIM	MSE	PSNR	SIM
32*32	4773	11.34	0.79	1926	15.28	0.89	45.72	31.52	0.99
50*50	320.1	32.07	0.89	81.84	29.00	0.98	108.7	27.76	0.95
60*60	502.6	21.11	0.87	51.64	31.01	0.97	45.52	31.54	0.99

Security and Analysis

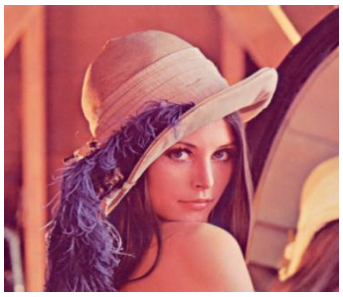
The evaluation the performance for proposed approach based on the security features and comparisons between the proposed approach and traditional method are performed according security robust and time execution. Figure (14) shows the gray logo with different sizes, which use in the test measurements.



(a) (b) (c)

Figure 15: Gray Logo with Size a-(32*32), b- (60*60), and c-(50*50

Figure16: PSNR Comparison



a

b

c

Figure 17: a-Watermark Image, b- 10%Cropping Image, c-15% Cropping Image.

A

b

Figure 18: a-Watermark image, b- Image with Salt and Pepper Attack.

Figure19: The result of extract Logo under salt and pepper attack .

1. Table(3)and figure(16) illustrates traditional to generation watermark key by using Lagrange polynomial without parametric form and give acceptable in MSE, PSNR and the similarity between host image and watermark image, but time execution problem is appear as shows in table (4).
2. In table (3&4) show the results of the proposed algorithm based Parametric Lagrange that provide more robust for watermark generation by adding the secret parameter (t) with decrease the time execution .
3. In table (3&4) show the results of the proposed algorithm using B+ tree indexing succeed to solve the execution time problem and make the key generation so faster and at the same time kept the acceptable results of fidelity criteria .
4. In tables (5-1) and (5-2) shown the result of the cropping attack with 10% and 15% ratios from watermark image appear that the proposed algorithms succeed to stand cropping attack, where the results shown in figures(17and 18) that no change from the standard watermark image, therefore show this algorithm not effective with cropping attacker.
5. In table (5-3) and figure(19) the results shown less effect to the noise(salt and paper attack) than Lagrange interpolation, and some result stayed as same result under the noise that show the robustness of algorithm under attacker.

CONCLUSIONS

This paper was presented a new gray level image watermarking approach that combines between B^+tree, parametric Lagrange polynomial, morphological operations and watermark techniques in order produce an efficient watermark approach. Through the current research work, the following conclusions are derived:-

1- Using B^+tree in proposed watermark approach provide efficient results to reduce amounts of data that embedding in host image. And B+ tree succeed to compress with efficient manner to produce few unique cods about 50% at least from the number of black pixel positions.

2- Using parametric Lagrange polynomial based on time parameter (t) as secret key that agreement between two parties increase the secrecy and integrity and increase the difficulty in front of intruder with consuming time.

3- Combine parametric Lagrange polynomial and B^+tree succeed to solve time execution problem that appear with traditional Lagrange polynomial.

4- The proposed approach robust against noise and cropping attacks with efficient results.

5- The quality of an image not affected when a watermarking is embedded to it. i.e., when a watermark is embedded in an image, it not be visible to the naked eye according test results.

REFERENCES

1- Potdar V., Han S., and Chang E., "*A Survey of Digital Image Watermarking Techniques*", in Proc. of the IEEE International Conference on Industrial Informatics,: 709-716, Perth, Australia 2005.

2- Sameh O., Adnane C., and Bassel S., "*A Fuzzy Watermarking System Using the Wavelet Technique for Medical Images*", International Journal of Research and Reviews in Computing Engineering Vol.1, No.1, March 2011.

3- Hanaa A. Abdallah, Mohiy M. Hadhoud, Abdalhameed A. Shaalan and Fathi E.AbdElsamie, *"Blind Wavelet-Based Image Watermarking*", International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 4, No.1, March 2011.

4- Sumalatha L., Venkata Krishna V., Vinay Babu A., "*Image Content Authentication based on Wavelet Edge Features*", International Journal of Computer Applications Vol. 49– No.23: 0975 – 8887, July 2012.

5- Dr. Eswara Reddy B., Harini P. , MaruthuPerumal S., Dr. VijayaKumar V. , *" A New Wavelet Based Digital Watermarking Method for Authenticated Mobile Signals*", International Journal of Image Processing (IJIP),Vol.5 ,Issue.1 ,2011.

6- G.RoslineNesaKumari , B. VijayaKumar , L.Sumalatha , and Dr V.V.Krishna, *"Secure and Robust Digital Watermarking on Grey Level Images*", International Journal of Advanced Science and Technology Vol. 11, October, 2009.

7- B. Vijaya Kumar,M.Radhika Mani, G. Roseline NesaKumari, and Dr. V. Vijaya Kumar, "*A New Marginal Color Image Water Marking Method based on Logical Operators* ", International Journal of Security and Its Applications Vol. 3, No. 4, October, 2009.

8- Vijayakumar B., Dr. Vijayakumar V., Rosline Nesa kumari G. ,"*A Significant Root Leaf Wavelet Tree (SRLWT) Image Watermarking Technique Based on Tree Quantization*", International Journal of Scientific and Research Publications, Vol.2, Issue 4, ISSN :2250-3153, April 2012.

9- Rosline Nesa kumari G., Sumalatha L., Dr. Vijayakumar V. "*A Fuzzy Based Chaotic And Logistic Method For Digital Watermarking Systems*", International Journal of Scientific & Engineering Researc Publications, Vol.3 , Issue. 6, June 2012.

10- Maruthuperumal S., Rosline Nesakumari G., Dr. Vijayakumar V., "*Complete Qualified Significant Wavelet Tree Quantization for Image Watermarking*", in International Journal of Computer Science and Technology,Vol.3, Issue 2, April-June 2012.

11- Maruthuperumal S., Dr. Rosline Nesakumari G., VijayakumarV., "*Region Based Even Odd Watermarking Method with Fuzzy Wavelet* ", International Journal of computer Engineering & Science(IJCES), Vol. 2 Issue.8 ,August 2012.

12- Chu.W, "*DCT-Based Image Watermarking Using Sub-sampling*", IEEE Trans. Multimedia, 5(1): 34-38, 2003.

13- Rosline Nesakumari G., Rajendran S., Dr. Vijayakumar V., *"Integrated Normalized Content System for Efficient Watermarking",* International Journal of Computer Applications, Vol.53,No.15, Sept, 2012.

14- Jiankun Hu , Fengling Han, "*A pixel-based scrambling scheme for digital medical images protection*", Journal of Network and Computer Applications, Published by Elsevier Ltd.,2009.

15- Jan Jannink, "Implementing Deletion in B+ Trees",Sigmoid Recire,Vol.24,No.1,1995.

16- Gotez, Graefe, *"B-tree indexes interpolation search, and skew",* Chicago Iiinois,USA,2006.

17- Anderson,S,*"B+Trees"*,Freed,1998.Http://bannage,clarku.edu/~achou/cs160/B+Trees/B+Trees.htm.

18- Anthony Ralston and Philip rabinowitz,. " *First Course in Numerical Analysis*", second edition, McGraw-hill Inc, 1978.

19- Shan S.,kuo, "*Computer Applications of Numerical Methods*", Addison wesely publishing company, 1972.

20- Goldman Ron, "*Lagrange Interpolation and Neville's Algorithm*", 2002.

21- Firas Husham Al-Mukhtar, "*Parallel Generation of Non Linear Curves with Computer Aided Application*", PhD. Thesis, Computer & Informatics Information Institute for Postgraduate Studies,2003 .

22- Suhad M.,*"Using B^+ Tree to represent secret Massage for steganography purpous"*,Eng.&Tech. Journal,Vol.28.No.15,2010
23- Chung-Ming Wang a, Nan-I Wu a, Chwei-Shyong Tsai b, Min-Shiang Hwang, "*A high quality steganographic method with pixel-value differencing and modulus function*", the Journal of Systems and Software,2007.
24- D.Phani Kumar, G.RoslineNesakumari, S.MaruthuPerumal, "Contrast Based Color Watermarking using Lagrange Polynomials Interpolation in Wavelet Domain", International Journal of Engineering and Advanced Technology (IJEAT), 2013.
25- G.RoslineNesakumari, Dr.V.Vijayakumar and Dr.B.V.Ramana Reddy, "Generation of An Efficient Digital Watermark Key Based on Honey Comb Polynomial Interpolation Approach", I. J. Computer Network and Information Security, 2013.