IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 04, Issue 02 (February. 2014), ||V2|| PP 52-61

Steganography Using Fractal Images Technique

Prof. Dr. Tawfiq Abdulkhaleq Abbas [1], Hassanein Karim Hamza [2]
[1](Collage of Information Technology, Babylon University, Iraq)
[2](Collage of Information Technology, Babylon University, Iraq)

Abstract: - In this paper, we suggest a new system and effective method for hiding an information in an image by detecting features of the regions of the cover image depending on applying fractal technique on the cover image and then choose the regions that will be hiding within it by using an algorithm determines regions that are fractal in which will be hiding, the fractal technique can be used to hide maximum amount of data in an image without degrading its quality and to make the hidden data robust enough to withstand image processing which do not change the appearance of image.

Keywords: - *Steganography, Digital watermarking, Information Hiding, Information Security, Data Hiding, Cover image, Stego image, Fractal, PIFS, Quadtree, Range, Domain.*

I. INTRODUCTION

Information security plays an important role in all aspects of life, in particular the protection of an organization's valuable resources, such as information, hardware, and software. Therefore, information security is defined as a process of protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption. As no single formula can guarantee full security, there is a need for a set of benchmarks or standards to help ensure an adequate level of security is attained, resources are used efficiently, and the best security practices are adopted [1].

Communication security should not be based on the secrecy of the communication method used. Various cryptosystems have been used to assure the security of transmitted data. In such systems, data is encrypted before transmission and they have been considered as secure systems [2].

There are many ways to provide the security for information and information systems like information hiding (steganography and watermarking), biometric indicators, passwords, and cryptography each one of them has some strong aspects and weak sides [3].

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information.[4].

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication, but it is not the only means of providing information security. In practice, crypto is used to keep secrets secret. It transforms information in such a way that no one other than the intended recipients can read what was actually written [5][6].

Cryptography is based on keys. Secure storage of keys is a crucial non-trivial task. Key management often is the weakest point of many systems [7].

Cryptographic methods are not sufficient to solve all data security related issues. Steganography is the art of hiding information in ways that prevent the detection of hidden messages [8].

II. BASIC PRINCIPLES OF FRACTAL AND STEGANOGRAPHY

Steganography is the science and art of hiding information in deterministic sequence that makes it difficult for any person to expect the existence of information also makes it difficult to extract this information except for intended persons [2].

The word steganography means covered writing, and this word is derived from the Greek words (steganos) meaning (cover) and (graphy) meaning (writing) [6].

Steganography can be defined as the art and science for hiding information in a way to prevent any person from retrieving hiding information without authentication. Steganography is the art of the invisible communication; its purpose is to hide the presence of communication by embedding message into a suitable cover object. Each steganography communication system consists of an embedding algorithm and an extracting algorithm [9].

To accommodate a secret message in a digital cover, the original cover is modified by applying the embedding algorithm, the result is modified cover object that contains the secret message and it is called stego object. To extract a secret message from the stego object, the extracting algorithm works in inverse way than the embedding algorithm, the result is the secret information (message) [9].

Like any security technology, steganography is not perfect and it does not address all security requirements. However, it satisfies most of the requirements of secret communication, sometimes in combination with other techniques such as cryptography. As cryptography and steganography complement each other, it is recommended to use these two techniques together for a higher level of security [2].

Today, steganography is most often associated with the high technologies variety, where information in any file format is hidden within other information in an electronic file. This is usually done by replacing the least important or most redundant bits of information in the original file (bits that are hardly missed by the human eye or ear) with hidden information bits [6].

Steganography can be classified in many ways according to the cover file type, according to how the information have been hidden, and according to the type of the key that used in hiding information.

According to cover file type, steganography is classified into four types which are text, audio, image, and video steganography [10], according to how the information have been hidden, steganography is classified into insertion, substitution, and generation steganography [6], and according to the type of the key used in hiding information steganography is classified into Pure Steganography, Secret Key Steganography and Public Key Steganography [9].

Digital Watermarking is the technique of embedding a secret message or digital logo behind a cover medium. Cover medium can be image, text, audio or video and message can be image, audio or text. Digital watermarking is having its application in the areas of copyright protection and the authentication [11].

Digital watermarking is the process of embedding information into digital cover such that the information (the watermark) can later be extracted for a variety of purposes including copy prevention, Authentication and control. Digital watermarking becomes an active and important area of research. In watermarking applications there is an active adversary that would attempt to remove, invalidate or forge watermarks [12].

Watermarking hides information in media in such a way that it is difficult for anyone to copy this media without authentication, or to protect the ownership of this media in spite of the availability of this media on internet for commercial purposes [3].

According to the human perception, the digital watermarks can be divided into two different types as follows: visible and invisible. Visible watermarks change the signal altogether such that the watermarked signal is totally different from the actual signal, adding an image as a watermark to another image. Invisible watermarks do not change the signal to a perceptually great extent; An example of an invisible watermark is when some bits are added to an image modifying only its least significant bits (LSB) [13].

Each one of these classes has many algorithms to hide secret information, these algorithms differ in many features like: Amount of data, difficulty of detection, and difficulty of removal so, the selection of suitable algorithm to send secret message depends on many factors like the size of the message, and the importance of the message.

The fractal technique can be used to hide maximum amount of data in an image without degrading its quality and to make the hidden data robust enough to withstand image processing which do not change the appearance of image, so this technique can be used for Steganography.

The fractal is one of the patterns which was discovered in 1975 by Benoit Mandelbrot. In recent years, the science of fractal has grown into a vast area of knowledge, with almost all branches of science and engineering gaining from the new insights it has provided. Fractal science is concerned with the properties of fractal objects, usually simply known as fractals. Fractals may be found in nature or generated using a mathematical recipe. The word 'fractal' was coined by Benoit Mandelbrot, sometimes referred to as the father of fractal geometry. Mandelbrot realized that it is very often impossible to describe nature using only Euclidean geometry, that is in terms of straight lines, circles, cubes, and such like. He proposed that fractals could be used to describe real objects, such as trees, lightning, river meanders and coastlines, to name but a few [14].

The formal mathematical definition of fractal is defined by Benoit Mandelbrot. It says that a fractal is a set for which the Hausdorff Besicovich dimension strictly exceeds the topological dimension. However, this is a very abstract definition. Generally, we can define a fractal as a rough or fragmented geometric shape that can be subdivided in parts, each of which is (at least approximately) a reduced-size copy of the whole. Fractals are generally self-similar and independent of scale [15].

The term fractal was coined by Benoit Mandelbrot in 1975 and was derived from the Latin fractus meaning "broken" or "fractured." A mathematical fractal is based on an equation that undergoes iteration, a form of feedback based on recursion [19].

The simplest way to define a fractal is a rough or fragmented geometric shape that can be subdivided in parts, each of which is (at least approximately) a reduced/size copy of the whole. Mathematical, a set of points whose fractal dimension exceeds its topological dimension [15], as example the Sierpinski Triangle in figure (1):

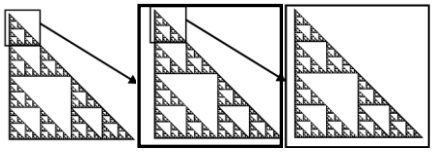


Figure (1) : Sierpinski Triangle illustrate self-similarity fractal.

The notion of fractals refers to an unusual non-Euclidian geometry of self-similar structures looking the same at any scale, the ubiquity of which among natural objects or natural phenomena was discovered during the last forty years [17].

Various attempts have been made to give a mathematical definition of a fractal, but such definitions have not proved satisfactory in a general context. Here avoid giving a precise definition, prefering to consider a set E in Euclidean space to be a fractal if it has all or most of the following features: [18]

- E has a fine structure, that is irregular detail at arbitrarily small scales.
- E is too irregular to be described by calculus or traditional geometrical language, either locally or globally.
- Often E has some sort of self-similarity or self-affinity, perhaps in a statistical or approximate sense.
- Usually the 'fractal dimension' of E (defined in some way) is strictly greater than its topological dimension.
- In many cases of interest E has a very simple, perhaps recursive, definition.
- Often E has a 'natural' appearance.

Human visual performance greatly exceeds computer capabilities, probably because of superior high-level image understanding, contextual knowledge, and massively parallel processing. Human capabilities deteriorate drastically in a low-visibility environment or after an extended period of surveillance, and certain working environments are either inaccessible or too hazardous for human beings. For these reasons, automatic recognition systems are developed for various military and civilian applications. Driven by advances in computing capability and image processing technology, computer mimicry of human vision has recently gained ground in a number of practical applications. Specialized recognition systems are becoming more likely to satisfy stringent constraints in accuracy and speed, as well as the cost of development and maintenance [19].
Hiding of information in fractal image is a difficult process because of the following reasons:

- Fractal's form is extremely irregular, or extremely interrupted or fragmented [15].
- It contains ‘distinct elements’ whose scales are very varied and cover a large range [15].
- A complex structure at any level of magnification [20].
- A non-integer dimension, as we know that the dimension of lines, squares and cubes are respectively 1, 2 and 3. The dimension of a fractal may be 1.342 [20].
- They have a perimeter of infinite length but an area limited [20].

III. THE PROPOSED SYSTEM

The proposed system hides an information (message or image) in an image by detecting features of the regions of the cover image depending on applying fractal technique on the cover image and then choose the regions that will be hiding within it by using an algorithm determines regions that are fractal in which will be hiding, the fractal technique can be used to hide maximum amount of data in an image without degrading its quality and to make the hidden data robust enough to withstand image processing which do not change the appearance of image.

In recent years, the fractal theory has developed rapidly not only in mathematics foundation but also used in many research fields, especially in signal and image analysis, for example, texture analysis of images for recognition, medical images analysis, and physiological signal processing and so on, and has achieved remarkable success in many disciplines.

3.1 The Components of the Proposed System:

In general, the proposed system consists of two basic stages; each stage consists of many steps, as illustrated in figure (2).

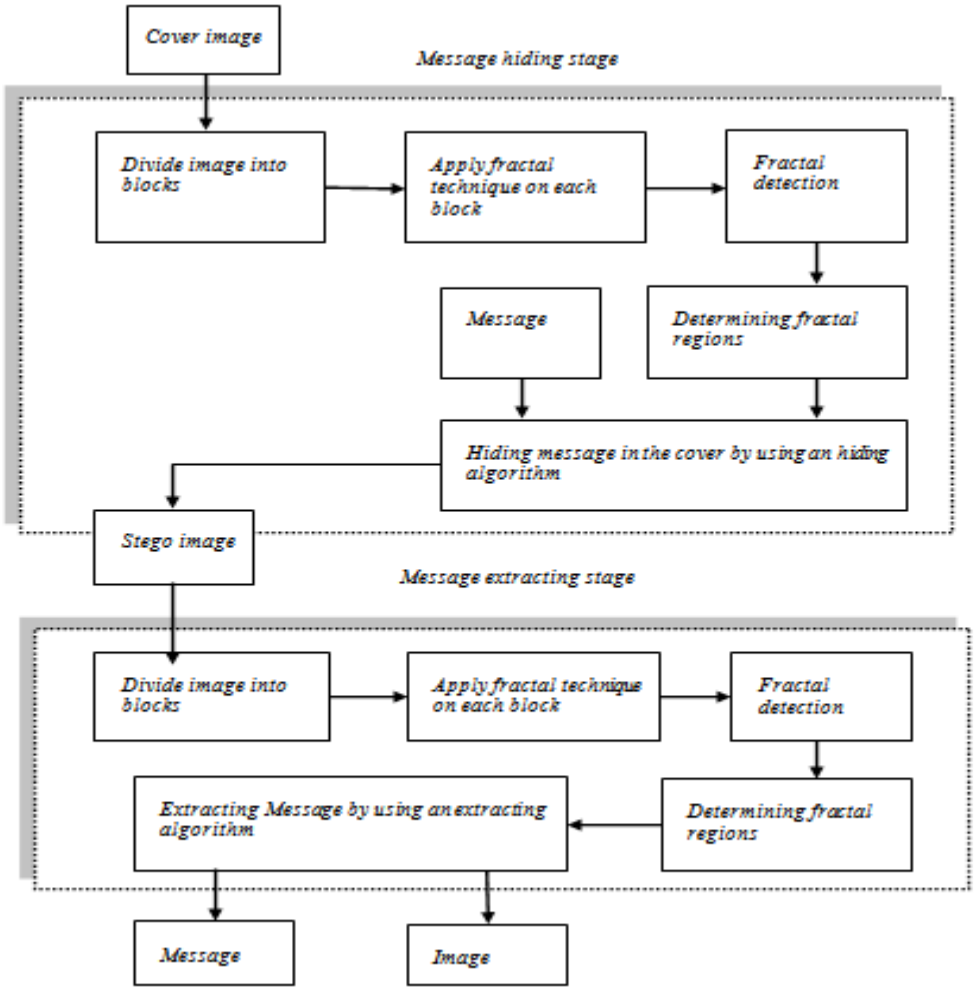


Figure (2): Block diagram of proposed system.

The first stage is used for hiding a message and the second one is for extracting this message. Message hiding in image must be never alter any feature in image, so the original image and stego images must be identical.

The first stage can be divided into the following steps: open an image, divide image into blocks, fractal detection and determining fractal regions to hide the message in them by using an hiding algorithm.

While the second stage cosists of the following steps: open stego image, divide stego image into blocks, fractal detection and determining fractal regions to extract the message from them, Each step will be explained in detail as follows.

3.2 First Stage : Message Hiding Stage:

This stage consists of the following four steps:

3.2.1 Open an image:

Add picture, which are originally fractal image. Choosing an image must be contain fractal because we will hide in fractal. If we want to hide large message then we must be choose an image which contain large fractal size.

3.2.2 Divide image into blocks:

Partition the cover image into blocks are called regions or places, each block is considered as small image then we detection the fractal in each block, size of block is must be greater than 32 pixels because of we can't detection of fractal if size of block less than 32 pixels, in our work we select 48 pixel for size of block.

3.2.3 Fractal detection (PIFSs Construction):

Each sub band (block or sub image or region or place) as a result from Apply splitting (partition) from previous step pass in two stages the first called range is formed from partitioning non-overlapping regions on a sub band and the second called domain is formed also by the subset of a sub band but which may overlap.

For the domain, the image is partitioning into overlapping square, the set D of domains contains all square ranges with sides' size 8, 12, 16, 24, 32, 48 and 64. The domain is twice the range size and then to subsample or average groups of 2 x 2 pixels to get a reduced domain with the same number of pixels as the range.

For the range, the image is partitioning into a non-overlapping squares by using Quadtree Partitioning, if we select a pixel in the image at random, there is a good chance that its immediate neighbors will have the same or similar color. The quadtree method scans the bitmap, area by area, looking for areas composed of identical pixels (uniform areas). where only neighbors on the same scan row are checked, even though neighbors on the same column may also be identical or very similar.The input consists of bitmap pixels, and the output is a tree (a quadtree, where each node is either a leaf or has exactly four children). The size of the quadtree depends on the complexity of the image. For complex images, the tree may be bigger than the original bitmap, resulting in expansion. The method starts by constructing a single node, the root of the final quadtree. It divides the bitmap into four quadrants, each to become a child of the root. A uniform quadrant (one where all the pixels have the same color) is saved as a leaf child of the root. A nonuniform quadrant is saved as an (interior node) child of the root. Any nonuniform quadrants are then recursively divided into four smaller subquadrants that are saved as four sibling nodes of the quadtree. Figure (3) shows a simple example.

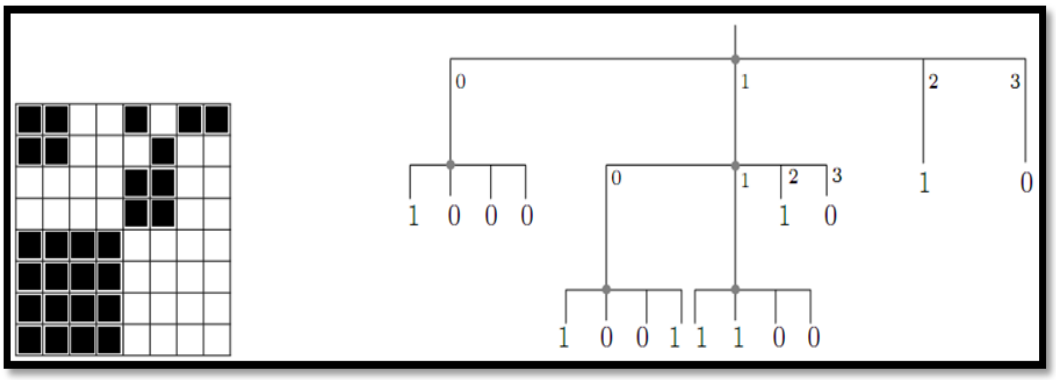


Figure (3) example of Quadtree.

Then, for each range, the algorithm tries to find a domain (larger than the range) that gives the collage error smaller than some preliminary set threshold. If this attempt ends with failure for some ranges then each such range is divided into four. For all newly created ranges the procedure is repeated, i.e. fitting domains are being searched for ranges and if necessary, the non-covered ranges are being broken down. The encoding ends when there are no ranges that remain uncovered or the size of the ranges reaches a given threshold. In the second case, the smallest ranges are paired with domains that do not meet the collage error requirement but are closest to corresponding ranges.

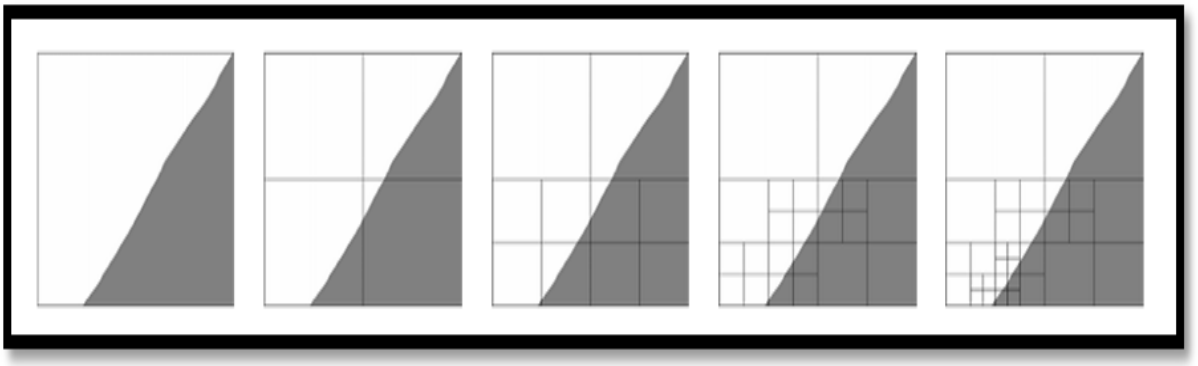


Figure (4) : Quadtree partitioning of a range. Four iterations.

For each Ri search through all of D to find a Di ∈ D which minimizes RMS error ; that is, find the part of the image that most looks like the image above Ri. This domain is said to cover the range. In addition, a square in D has four times as many pixels as a Ri, so we are must subsample average the 2 x 2 sub-squares corresponding to each pixel of Ri.

It means finding a good choice for Di that is the part of the image that most looks like the image above Ri. It means finding good contrast and brightness settings xi and oi for wi. For each Di ∈ D we can compute xi and oi using least squares regression, which also gives a resulting root mean square (rms) difference. We then pick as Di the Di ∈ D with the least rms difference.

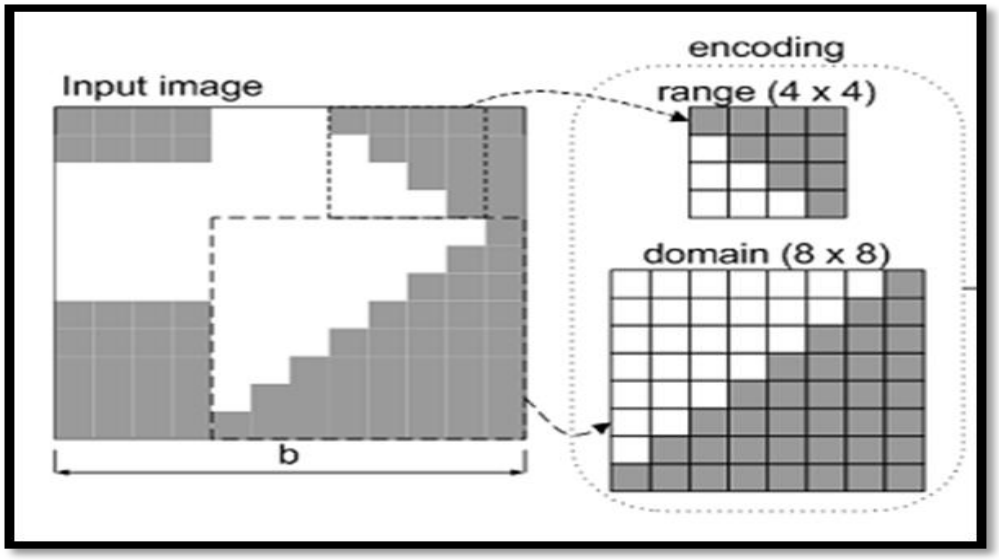


Figure (5) Matching domain and range

And the algorithm (1) describe finding a good choice for Di that most looks like the Ri. The algorithm finds the following parameters oi , si and ti where contrast , brightness and transformation respectively calculate to the output.

Finally, For each block (sub image, region), a set of PIFSs is then constructed. As shown in the figure (6).

Algorithm 1: PIFS Construction algorithm

Inputs: *Image.*

Outputs: *PIFS File.*

Begin

divide the image into overlapping domains $D = \{D_1, D_2, \ldots, D_m\}$ *and disjoint ranges* $R = \{R_1, R_2, \ldots, R_n\}$

"the size of each range is $b \times b$ *and the size of each domain is* $2b \times 2b$*"*

For each range $R_i \in R$

1. *Set* $w_i = null$, $D_i = null$, $j = 1$
2. *for each domain* $D^j \in D$
   - *compare* R_i *with 8 transformations of* D^j.

   " transformations: rotation of Dj by 0, 90, 180, 270 degrees and rotation of the reflection of Dj by 0, 90, 180, 270 degrees"

   - *determine parameters of transformation* w_i^j *that gives minimal distance between* R_i *and* $w_i^j(D^j)$.
   - *calculate* $\delta(w_i(D_i), R_i)$ *distance between* R_i *and* $w_i^j(D^j)$.
   - *if* $\delta(w_i^j(D^j), R_i) > \delta(w_i^j(D^j), R_i)$ *or* $w_i = null$, *then* $w_i = w_i^j$, $D_i = D^j$
3. *Add* w_i *to fractal code*

Figure (6): Fractal detection (PIFS Construction) algorithm.

An encoding of an image consists of the following data:

- The contrast and brightness values si and oi for each range.
- For each range, a domain that is mapped to it.
- The symmetry operation (orientation) used to map the domain pixels onto the range pixels.

3.2.4 Hiding in Fractal Regions:

The proposed system hides an informations (message ,image) in image in places depending on features extracted from image, an image will be subdivided into regions called blocks or places, so each region has features of fractal will be used in hide process, also the number of pixels in these region depends on size of block, also the number of bits in each pixel is 4 bits which are 1 bit in red color, 1 bit in green color and 2 bits in blue color, therefore, each one byte is hidden in two pixels.

Least significant bit (LSB) insertion is one of the methods of embedding secret information in an 'innocent' cover image. For instance, 10101001 is an 8-bit binary number. The last bit in the binary number is the least significant bit because changing it has the nominal effect on the value. The method is based on the fact that change in the LSB information of some area of the image will not be noticeable by the naked eye.

The stego image is the file produced after embedding the secret message in the cover file by using steganography algorithm. The cover image should be a bitmap image, in which the file to be hidden is embedded. The stego image, consisting of the cover image and the secret file, is indistinguishable from the original cover image. By using the LSB insertion method, the software embeds the secret file in a 24-bit bitmap image.

In a 24-bit bitmap, each pixel is represented as 3 bytes – one for red, one for green and one for blue, making up of a 24-bit number. Each color is composed of 8-bit numbers, and the red, green and blue colors/channels create the final color of the pixel. To hide something inside the image, software will replace the LSB of each 8-bit channel of every pixel, with the bits of the file to be hidden. This means the last bit in a byte can be overwritten without affecting the color it appears to be.

3.3 Stage 2: Message Extracting Stage:

In this stage we applying the same techniques used in sections (3.2.1), (3.2.2), (3.2.3) and (3.2.4) for open an image, image splitting and fractal detection, respectively to determine the fractal regions and extract message from them.

This means that the second stage for extracting the message from fractal regions in image consists of the following steps: open stego image, divide stego image into blocks, fractal detection and determining fractal regions to extract the message from them.

When we need to extract message from stego image, we read the first pixel in fractal regions, then from this value we know the length of message which was hidden in image.

IV. EXPERIMENTALS RESUTLS

The proposed system is applied on samples of the images as follows:

Case (1): The cover image is an image with size of (640×480), while the message is an image with size of (60×120), as illustrated in figure (7).

a- Original image *b- Image Partition* *c- Fractal detection* *d- Message* *e- Stego image*

Figure (7): Results of case (1).

The number of pixels in fractal regions (pixels of hiding) are (48384) pixels as illustrated in figure (7) c ,the number of hiding bits in these pixels are (193536) bits, this means (24192) bytes to hide in. Then the image message size must be less than or equal (8062) pixels for color image. In this case, the message size is (7200) pixels, and we can hidden text message with size (24191) characters then extracted them accurately.

Compute fidelity criteria for case 1: Peak signal to noise ratio (PSNR) is (59.5697481912967) and this is an accepted ratio, the larger value of the error metrics (PSNR) implies the better image represents the original images, Another related metric, the root-mean-square error (RMSE) is (0.267949388877825), is found by taking the square root of the error squared divided by the total number of pixels in the image (mean), the smaller value of the error metrics implies the better image represents the original images, Third related metric, the signal-to-noise (SNR) metrics is (451.885680614262), a larger number implies a better image. The SNR metrics consider the stego image g(r,c) to be "signal" and the error to be "noise".

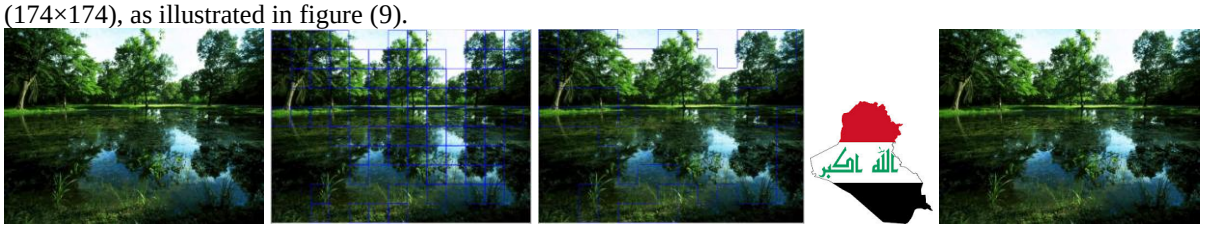
Case (2): The cover image is an image with size of (320×240), while the message is an image with size of (60×54), as illustrated in figure (8).

a- Original image *b- Image Partition* *c- Fractal detection* *d- Message* *e- Stego image*

Figure (8): Results of case (2).

The number of pixels in fractal regions (pixels of hiding) are (23040) pixels as illustrated in figure (8) c ,the number of hiding bits in these pixels are (92160) bits, this means (11520) bytes to hide in. Then the image message size must be less than or equal (3838) pixels for color image. In this case, the message size is (3240) pixels, and we can hidden text message with size (11519) characters then extracted them accurately.
Computing fidelity criteria for case 2: Peak signal to noise ratio (PSNR) is (56.9480874389501) and this is an accepted ratio, the root-mean-square error (RMSE) is (0.362356293354115), and the signal-to-noise (SNR) metrics is (364.110010521544).

Case (3): The cover image is an image with size of (640×480), while the message is an image with size of (174×174), as illustrated in figure (9).



a- Original image *b- Image Partition* *c- Fractal detection* *d- Message* *e- Stego image*

Figure (9): Results of case (3).

The number of pixels in fractal regions (pixels of hiding) are (182016) pixels as illustrated in figure (9) c ,the number of hiding bits in these pixels are (728064) bits, this means (91008) bytes to hide in. Then the image message size must be less than or equal (30334) pixels for color image. In this case, the message size is (30276) pixels, and we can hidden text message with size (91007) characters then extracted them accurately.
Computing fidelity criteria for case 3: Peak signal to noise ratio (PSNR) is (52.9068962272707) and this is an accepted ratio, the root-mean-square error (RMSE) is (0.577025982408938), and the signal-to-noise (SNR) metrics is (162.925005847567).

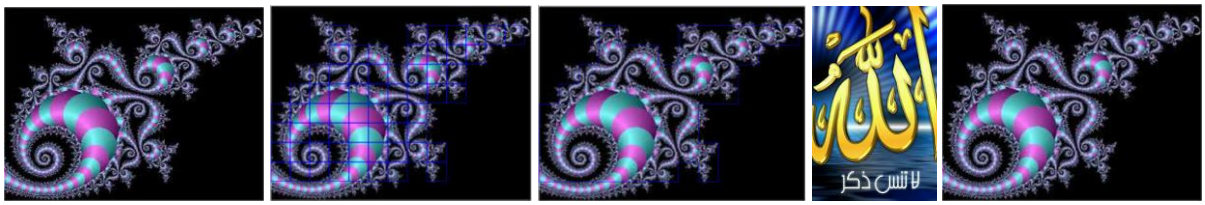
Case (4): The cover image is an image with size of (671×420), while the message is an image with size of (164×180), as illustrated in figure (10).

a- Original image *b- Image Partition* *c- Fractal detection* *d- Message* *e- Stego image*

Figure (10): Results of case (4).

The number of pixels in fractal regions (pixels of hiding) are (198144) pixels as illustrated in figure (10) c ,the number of hiding bits in these pixels are (792576) bits, this means (99072) bytes to hide in. Then the image message size must be less than or equal (33022) pixels for color image. In this case, the message size is (29520) pixels, and we can hidden text message with size (99071) characters then extracted them accurately.
Computing fidelity criteria for case 4: Peak signal to noise ratio (PSNR) is (53.3101670013045) and this is an accepted ratio, the root-mean-square error (RMSE) is (0.550848067755529), and the signal-to-noise (SNR) metrics is (247.438029737723).

Case (5): The cover image is an image with size of (640 × 479), while the message is an image with size of (128×170), as illustrated in figure (11).



a- Original image *b- Image Partition* *c- Fractal detection* *d- Message* *e- Stego image*

Figure (11): Results of case (5).

The number of pixels in fractal regions (pixels of hiding) are (147456) pixels as illustrated in figure (11) c ,the number of hiding bits in these pixels are (589824) bits, this means (73728) bytes to hide in. Then the image message size must be less than or equal (24574) pixels for color image. In this case, the message size is (29520) pixels, and we can hidden text message with size (73727) characters then extracted them accurately.
Computing fidelity criteria for case 5: Peak signal to noise ratio (PSNR) is (55.3440431090345) and this is an accepted ratio, the root-mean-square error (RMSE) is (0.435850978152598), and the signal-to-noise (SNR) metrics is (174.992181931672).

Case (6): The cover image is an image with size of (800 × 600), while the message is an image with size of (165×192), as illustrated in figure (12).

a- Original image *b- Image Partition* *c- Fractal detection* *d- Message* *e- Stego image*

Figure (12): Results of case (5).

The number of pixels in fractal regions (pixels of hiding) are (200448) pixels as illustrated in figure (12) c ,the number of hiding bits in these pixels are (801792) bits, this means (100224) bytes to hide in. Then the image message size must be less than or equal (33406) pixels for color image. In this case, the message size is (31680) pixels, and we can hidden text message with size (100223) characters then extracted them accurately.
Computing fidelity criteria for case 6: Peak signal to noise ratio (PSNR) is (55.7966116765428) and this is an accepted ratio, the root-mean-square error (RMSE) is (0.413722934663606), and the signal-to-noise (SNR) metrics is (326.520449316442).

The following table summarizes the Proposed System Results :

Case No.	Cover image	Size cover image	Message	Size message	Size stigo image	PSNR
1-		640×480 1.17MB		60×120 21.1KB	640×480 1.17MB	59.56
2-		320×240 225KB		60×54 9.54KB	320×240 225KB	56.94
3-		640×480 1.17MB		174×174 89KB	640×480 1.17MB	52.9
4-		671×420 0.97MB		164×180 46.4KB	671×420 0.97MB	53.31
5-		640×479 1.16MB		128×170 63.8KB	640×479 1.16MB	55.34
6-		800×600 1.83MB		165×192 93KB	800×600 1.83MB	55.7

Table (1): the Proposed System Results.

V. CONCLUSION

From the proposed system in this thesis some conclusions were be achieved

1- The number of bits of data that can be stored, depends upon the number of range blocks that have match in domain region. Bigger the range region more is the data that can be stored. But, since range region can not overlap the domain region, on increasing the range region, domain region is reduced which may lead to worse quality of image. So, there is a trade-off between the amount of data and quality of image produced.
2- Increase in tolerance level would allow to use all range blocks so that more data can be stored. However low tolerance is desirable in order to give an image that is visually close to the original.
3- The achieve method conforms the possibility of using PIFS to detection the fractal.
4- In this thesis, a new approach for fractal image detection that uses the compression is presented.
5- Using PIFS in fractal pattern is necessary, because it finds the similarity in the image.
6- A benefit can be got from fractal detection through recognizing patterns which have geographical, environmental, etc., nature. This is based on form of the fractals.

REFERENCES

[1] Safaa Zaman, *Distributed Intrusion Detection System* (Waterloo University, Canada, 2009).
[2] Adel Almohammad, *Steganography-Based Secret and Reliable Communications: Improving Stenographic Capacity and Imperceptibility* (Brunel University, 2010).
[3] Vidyabharati Mahavidyalaya, *Advances in Computational Research* (Amravati University, Amravati MS, India, 2011).
[4] Suman Goyat, A Novel Technique Used For Image Steganography Based On Frequency Domain, *International Journal of Engineering Research & Technology*, 2012.
[5] Dr.D.Vasumathi, M.Surya Prakash Rao, M.Upendra Kumar, Dr.Y.Ramadevi, and Dr.R.Rajeswara Rao, Novel Approach for Color Extended Visual Cryptography Using Error Diffusion, *International Journal of Computer Trends and Technology*, 2012.
[6] Eric Cole, and Ronald D. Krutz, *Hiding in Plain Sight: Steganography and the Art of Covert Communication* (Wiley Publishing USA, 2003).
[7] Zdenˇek ˇR´ıha, *Biometric Authentication Systems* (Masaryk University, 2000).
[8] Kamal Gulat, *Information Hiding Using Fractal Encoding* (School of Information Technology Indian Institute of Technology Bombay,Mumbai, 2003).
[9] Vinay Kumar, and S. K. Muttoo, *Principle of Graph Theoretic Approach to Digital Steganography* (Institute of Computer Applications and Management, New Delhi, 2009).
[10] R.Amirtharajan, Sandeep Kumar Behera, Motamarri Abhilash Swarup, Mohamed Ashfaaq K ,and John Bosco Balaguru Rayappan, *Colour Guided Colour Image Steganography* (School of Electrical & Electronics Engineering SASTRA University Thanjavur, Tamil Nadu, India , 2010).
[11] Ashish M. Kothari, and Ved Vyas Dwivedi, *Video Watermarking Combination of Discrete Wavelet & Cosine Transform to Achieve Extra Robustness* (I.J. Image, Graphics and Signal Processing, 2013).
[12] Dr.M.Umamaheswari, Prof.S. Sivasubramanian, and S.Pandiarajan, Analysis of Different Steganographic Algorithms for Secured Data Hiding, *IJCSNS International Journal of Computer Science and Network Security*, 2010.
[13] Yamuna Govindarajan, and Sivakumar Dakshinamurthi, Quality Security uncompromised and Plausible Watermarking, *International Journal of Image Processing*, 2008.
[14] Paul S Addison, *Fractals and Chaos An Illustrated Course* (Institute of Physics Pub.,1997).
[15] Mandelbrot B.B., The *Fractal Geometry of Nature* (W.H. Freeman and Company,1983).
[16] Apan A., *GIS applications in tropical forestry* (Faculty of Engineering and Surveying The University of Southern Queensland, Toowoomba, 1999).
[17] M. A. lebyodkin, T. A. lebedkina, and A. Jacques, *Multifractal analysis of unstable plastic flow* (New York, Nova Science Publishers,2009).
[18] Kenneth F., *Techniques in Fractal Geometry* (England: John Wiley & Sons Ltd, 1997).
[19] Javidi B., *Image Recognition and Classification Algorithms, Systems, and Applications* (Marcel Dekker, Inc, 2002).
[20] Larry S. Liebovitch, *The NSF Nonlinear Methods in Psychology Workshop* (Florida Atlantic University, USA, 2003).