Commentary

An Improved Data Hiding in Encrypted Images

Aida Laee¹, Masoud Masomei², Hamid Chegini²

¹Telecommunication, of Non-profit Institution of Higher Education, Aba, Abyek, Iran

²Non-profit Institution of Higher Education, Aba, Abyek, Iran

Email address:

aida.laee@yahoo.com (A. Laee), massoud_masoumi@yahoo.com (M. Masomei), Hamidchegini26@gmail.com (H. Chegini)

To cite this article:

Aida Laee, Masoud Masomei, Hamid Chegini. An Improved Data Hiding in Encrypted Images. *American Journal of Networks and Communications*. Vol. 5, No. 5, 2016, pp. 107-114. doi: 10.11648/j.ajnc.20160505.14

Received: September 8, 2016; **Accepted:** September 21, 2016; **Published:** October 11, 2016

Abstract: Nowadays in digital world, safeguarding information is an important phase in transmitting messages and doing trades. The increasing growth of computer networks has caused a lot of changes in life style, occupational activities and organizations. Thus, data security has been one of the essential issues in this area. By connecting a local network to global network, outsiders are likely to have access to the organizations' data. One of the most important challenges about propagating information on internet is to assure inaccessibility of unauthorized people to sensitive information. Various solutions including restricting the use of internet, encoding the data and establishing security have been suggested. To fulfill the security requirements for a safe transaction, operations such as encoding, hiding, etc. are used. Today information is of great importance either in military area or in commercial one. Hence one of the basic needs is to maintain information for transmitting or storing them. Having access to coded information is not possible for unauthorized people and only those having password can decode and use them. Encoding the information is based on the knowledge related to that. On the one hand, hiding is also one of the effective techniques for keeping information since host information is clear and a hidden message may not be discovered. In this study, a new technique is presented for hiding information in encoded images which minimized the error of the previous techniques. In addition, previous techniques have never pointed out to noisy environments and one of the advantages of the introduced technique was to eliminate noise.

Keywords: Storage, Information Security, Encoding, Fractal

1. Introduction

Encoding has a long history and the first application of it dates to 4000 past years in ancient Egypt.

In encoding, transmitting message or information is not done in hiding manner but rather storing information or transmitting message is known. However, only authorized individuals are allowed to retrieve the main information. On the contrary in hiding technique, sending a hidden message is carried out in hiding manner and no one is informed of this except receiver and sender. [9]

In encoding, the content of a text is converted in letter by letter form and in some cases bit by bit and the purpose is to convert the content of a text not the linguistic structure of it. Coding is a conversion process in which a word is replaced by another word or symbol and the linguistic structure of the text is converted.

With the advent of computers and their computational power, encoding knowledge entered the area of computer science and this caused three key changes in encoding issues:

- (1) High computational power provided an opportunity for creating more effective and complicated for encoding.
- (2) Encoding techniques found different applications.
- (3) Previously, encoding was mainly done using alphabets on text data. The advent of computers made encoding done on different information according to bits.

Encoding algorithm refers to any algorithm or mathematical function which is used in encoding protocols due to having the required features in encoding. Encoding algorithm is a comprehensive concept and it is not necessary to use every algorithm of this classification directly for encoding. [12] Only the application of encoding is important.

In communications world, the first question is about illegal propagation of digital products. One of the primary ways to

preserve the owners' rights is using encoding. It may be said that encoding is the most common way to protect digital products and it has faced a lot of advances. Some products are encoded by sender (manufacturer) before delivery and password is only given to legal purchasers of digital products. Then the coded file becomes available through internet for the public. Frauds are not able to use a file without having private password but authorized user can decode and use data by having password.

Fractal term was first developed by Mandelbrot in 1970. He derived this term from Latin word "Fractus" which means a stone broken in an irregular form. [2]

Fractal in its wide definition discusses about processes or shapes which have scalable features. Fractal shapes have a feature that if we change the scale for them, we will obtain a similar shape. Natural and real examples of fractals include human lungs, trees, clouds, mountains and the leaves of some trees like fern. Another definition is based on fractal dimension. On this basis, fractal is a shape that has a non-integer dimension. It means we may have a shape whose dimension is between 1 and 2.

Fractals are mathematical geometrical concepts which have been of interest by the scientists of other sciences during recent years and after Benoite Mandelbrot worked on them and their applications have been demonstrated in physics, chemistry, biology, geology and medicine. [7]

2. Theoretical Foundations of Research

2.1. Well Known Fractals

A) Contour fractal

The simplest type of fractal is contour fractal. Consider a line segment 1 in length. Divide it into three equal parts and eliminate the middle part. Now we have two line segments and their length is one third of initial length. Next, repeat this operation for each remaining line segments. Divide each line segment into three parts and eliminate the middle part. You can write a computer program that can perform these operations sequentially. If we perform these operations many times (computers cannot perform this), we will obtain a form called contour. [3] If we look at the whole shape, we will see a structure which is infinite. If we look at the left or right side of the shape, we will see a structure which is again infinite and at the same time it is quite similar to the whole shape.

Fig. 1. Contour fractal.

B) Sierpinski fractal

One of the most famous fractals was introduced by

Sierpinski, a polish mathematician. Consider an equilateral triangle and each side of it is 2. Connect middle points of the sides and then eliminate the middle triangle. Repeat this for the remaining triangles.

Fig. 2. Sierpinski Fractal.

C) Koch fractal

One of the types of fractals was developed by Helg Fon Koch in 1904. Consider an equilateral triangle. Divide each side into three parts and then substitute two sides in the middle side. If we repeat this in the same way, we will obtain a very beautiful shape called Koch Curve. [11]

Fig. 3. Koch curve.

2.2. Fractal Applications

Fractals have many applications in different sciences. Some of them are:

- (1) In processing signal, fractals are used for compressing images.
- (2) Some chemical processes such as chemical corrosion and bacterial growth are modeled by fractals. An example of computer simulation of bacterial growth by fractals is shown in Fig. 4.
- (3) Fractals are used in solving equations.

- (4) Some of attractive designs made by fractals like in Fig. 5 are used in decorative arts.

Fig. 4. Bacterial growth simulation.

Fig. 5. An example of a design made by a fractal.

2.3. Fractal Geometry

In the first half of 20th century, mathematical objects were considered strange objects which did not have any important application. Mandelbrot was one of the first mathematicians who recognized such strange objects and founded their mathematical root. Mandelbrot used the term fractal for those objects which were analogous at all scales. [3] He has defined fractal in his well-known book “The fractal geometry of nature” published in 1982.

2.4. Euclidean Dimensions

The figure below shows a line, square and cubic which have been divided into parts. The table below shows the relationship between topology (D) and measurement unit and the number of lines, cubic and squares (N). [13]

In general, the relationship between N, L and D is expressed by this formula:

$$N = \left(\frac{1}{L}\right)^D \quad (1)$$

By obtaining log of the two sides of Eq. -1, the formula below is obtained:

$$D = \frac{\text{Log}N}{\text{Log} \frac{1}{L}} \quad (2)$$

Fig. 6. Line- square- cubic.

Table 1. Calculating dimension in Euclidean shapes.

Object	L	D	$N = \left(\frac{1}{L}\right)^D$
Line	$\frac{1}{3}$	1	$\left[\frac{1}{1/3}\right]^1 = 3$
Line	$\frac{1}{4}$	1	$\left[\frac{1}{1/4}\right]^1 = 4$
Line	$\frac{1}{5}$	1	$\left[\frac{1}{1/5}\right]^1 = 5$
Square	$\frac{1}{3}$	2	$\left[\frac{1}{1/3}\right]^2 = 9$
Square	$\frac{1}{4}$	2	$\left[\frac{1}{1/4}\right]^2 = 16$
Square	$\frac{1}{5}$	2	$\left[\frac{1}{1/5}\right]^2 = 25$
Cubic	$\frac{1}{3}$	3	$\left[\frac{1}{1/3}\right]^3 = 27$
Cubic	$\frac{1}{4}$	3	$\left[\frac{1}{1/4}\right]^3 = 64$
Cubic	$\frac{1}{5}$	3	$\left[\frac{1}{1/5}\right]^3 = 125$

In Euclidean geometry, curves include the finite number of segment lines which are one-dimensional. However, using Euclidean dimension is not suitable for fractal curves.

2.5. Fractal Coding Algorithm

In fractal compression, an image is defined by a set of compact plane conversions which describe analogous sections of an image. Fractal coding is based on mathematical results of Iteration Fractal Systems (IFS). [14] By introducing iteration function systems, fractal compression became more

real. In this technique, we first divide the image into blocks in dimensions $N \times N$ which do not overlap each other. Each block is called Range Block or briefly R Block. We consider blocks with dimensions $2N \times 2N$ on the image and call these blocks Domain Block or briefly D Block. On the contrary to R blocks, D blocks overlap each other. After determining these blocks, we find a D block for each R block based on a set of plane conversions in order that collage error would be minimal in the following equation.

1	2
3	4

2	1
4	3

3	1
4	2

1	3
2	4

| | | | |

4	3
2	1

3	4
1	2

2	4
1	3

4	2
3	1

Fig. 7. Eight plane conversions obtained by rotation and inversion.

Since the number of pixels for each D block is four times the number of pixels for each R block, we need to make each D block equal to R block in size using interpolation. W conversion in Eq. 3 is a combination of geometric conversions and brightness.

According to Eq. (4), one pixel in coordinates of grey surface was scaled using geometric conversion parameters and then is replaced by some parameters. The value of it is scaled based on resolution parameter and then is transmitted by brightness parameter. Reducing Eq. 3 has two meanings: first is finding an appropriate D block and second is finding suitable resolution and brightness for W conversion in Eq. (4):

$$w \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} a_i & b_i & 0 \\ c_i & d_i & 0 \\ 0 & 0 & s_i \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} e_i \\ f_i \\ o_i \end{bmatrix} \quad (4)$$

Therefore to obtain fractal conversion for each range blocks from domain blocks, we seek a block that the converted form of it or itself equals to that block after adjusting brightness, resolution and equality in size [10] and in this way, each image block is expressed in terms of another block in the same image and as a result, the entire image is a conversion of the same image. Each of these conversions includes the following components that have to be stored.

- The center of range block
- The number of first point in domain block
- Parameters regarding the conversion of a range to its corresponding domain which includes 6 real numbers a, b, c, d, e, f . Such parameters are determined as follows.

In general, encoding information inside a coded image is better than encoding in an intact image since hackers are likely to decode a coded image at first and thus, there will be less possibility to hack hidden information. To encode an image, there are different techniques which were explained briefly in

$$\text{Collage Error} = \min \|R_i - w(D_{ij})\|^2 \quad (3)$$

We can convert a square by eight methods using rotation and inversion to another square. The figure below shows these eight conversions for a square in dimensions 2×2 and its pixels are marked with numbers 1, 2, 3, 4.

the first chapter. [8] Since the main goal of this paper is to hide and retrieve information with the least error, encoding has been carried out by a random bit string and we will discuss about it in this section.

2.6. Converting an Image into Bit String

The original image is J that has $M \times N$ pixel and every pixel contains eight bits. To encode this image, we first convert its pixels into bits so that a bit string in length $M \times N \times 8$ is obtained. Such conversion is obtained from Eq. 5.

$$J_{i,j}^{(v)} = \left[\frac{J_{i,j}}{2^v} \right] \bmod 2, 0 \leq v \leq 7 \quad (5)$$

In the above equation, $J_{i,j}$ represents the value of pixels in position i, j and $J_{i,j}^{(k)}$ represents V th bit in that pixel.

2.7. Encoding by a Random Bit String

After converting an image into bit, a random bit string having the same length of bits resulting from J image is produced and we represent it by $k_{i,j}^{(v)}$. Encoding is done by XOR between two bit strings and it is shown in the equation below:

$$J'_{i,j}^{(v)} = J_{i,j}^{(v)} \oplus k_{i,j}^{(v)} \quad (6)$$

$J'_{i,j}^{(v)}$ represents the v th bit in i, j which has been encoded. The operator $\oplus$ represents XOR. To convert this bit string into coded pixels, Eq. 7 is used. $J'_{i,j}$ represents the value of pixels in coded image that are in position i, j .

$$J'_{i,j} = \sum_{v=0}^7 J'_{i,j}^{(v)} \cdot 2^v \quad (7)$$

By putting pixels next to each other, the coded image J' is obtained.

2.8. Finding a Block Pair by Homomorphism

To encode information which is in the form of bit string, two pixel blocks of the coded image are required. These two blocks can be selected as adjacent, however to enhance hiding operation, these two blocks are selected as nonadjacent as far as possible. [5]

Homomorphism and finding the pair of blocks are performed both after and before hiding (in receiver and transmitter respectively). Since hiding three cheap bits changes some pixels of the image, the effect of variations in these three bits shall be cancelled to select equal pairs in the receiver and transmitter. [1] For this reason, three variable bits (three cheap bits) are considered as "0".

The resultant image is J_1 . Next, this image is divided into blocks having the same size $b \times b$. In order that blocks can have the greater images, it is better b to be multiples of 4.

Then the block in position p, q is called as $B_{p,q}$. Next, the processes of finding nonadjacent block pairs are presented below:

- (1) The values of pixels in block $B_{1,1}$ are placed in a new block called R .
- (2) The values of pixels in block $B_{1,2}$ are placed in another block called D .
- (3) $\tilde{R}$ is calculated using the equation below:

$$\tilde{R} = SD + O \quad (8)$$

$\tilde{R}$ is the most similar matrix to R and it is built upon D and O and S are obtained from Eqs. 9 and 10:

$$S = \frac{\langle R - \bar{r}I, D - \bar{d}I \rangle}{\|R - \bar{r}I\|^2} \quad (9)$$

$$O = \bar{d} - \bar{r}S \quad (10)$$

Where $\bar{d}$ and $\bar{r}$ are the means of R and D respectively and they are two numbers.

- (4) The difference between the converted form of block D called $\tilde{R}$ and block R is expressed by:

$$X_{1,2} = R - \tilde{R} \quad (11)$$

The distance between the subsequent blocks and block R is calculated according to processes 1 to 4. For the third block this is calculated up to $M \times N$ that and it is known as $X_{1,3}$ to $X_{M,N}$.

- (5) The values of $X_{p,q}$ are arranged in an ascending order and the location of the first obtained value represents a block which has the least variance with block R .
- (6) By cancelling this block pair from the photo blocks J_1 , processes 1 to 6 continue until each block finds its own underlying pair.

The flowchart for the suggested discussions is shown in below.

Fig. 8. Homomorphism.

After block pairs were identified by the introduced method in the previous stage, now we can hide a bit in each block pair of the image J' . Assume that block (1, 1) is corresponding to (p, q) . Each block is randomly divided into two sets.

All processes shall be repeated on transmitter's side to extract hidden information on receiver's side. We must first identify block pairs using homomorphism and then deal with information extraction using smoothness equation after

$$f_{B'}^{i,j} = \frac{1}{s_1 \cdot s_2} \left(\sum_{u=2}^{s_2} \sum_{v=2}^{s_1-1} |p_{u,v} - p_{u,v+1}| + \sum_{u=2}^{s_2-1} \sum_{v=2}^{s_1} |p_{u,v} - p_{u+1,v}| \right), p_{u,v} \in B'_{i,j} \quad (12)$$

$$f_{B'}^{p,q} = \frac{1}{s_1 \cdot s_2} \left(\sum_{u=2}^{s_2} \sum_{v=2}^{s_1-1} |p_{u,v} - p_{u,v+1}| + \sum_{u=2}^{s_2-1} \sum_{v=2}^{s_1} |p_{u,v} - p_{u+1,v}| \right), p_{u,v} \in B'_{p,q} \quad (13)$$

The difference between $f_{B'}^{p,q}$ and $f_{B'}^{i,j}$ is obtained using the equations:

$$f^{i,j} = f_{B'}^{i,j} - f_{B'}^{p,q} \quad (14)$$

For positive and large values of $f^{i,j}$, it is indicated that smoothness level of $B'_{i,j}$ pixel values is reduced and it means that the value of $B'_{i,j}$ pixels is different from that of $B_{i,j}$ (a block of the original image) and $B'_{p,q}$ is quite similar to its original block $B_{p,q}$. In other words, large values of $f^{i,j}$ indicate that the first block in the transmitter contains some variations from the underlying block pair and since variations in the first block are made from each block pair to hide "0", this bit is extracted for large values of $f^{i,j}$. Thus, the value of $B'_{p,q}$ is the same values of the original image and it is just enough to reverse three cheap bits of A_0 set. If $f^{i,j}$ had small values (null values), it would represent matters unlike the above statements. It means that $B'_{i,j}$ is the original block and the bit extracted from this block pair is "1". The extraction of such bit means that $B'_{i,j}$ should not be changed to retrieve this block pair to its main state. However, $B'_{p,q}$ returns to its main state by reversing three cheap bits of A_2 pixel set.

One of the important points in sending the image containing information is noise. [6]

If the transmitted image reaches the receiver with noise, information extraction and retrieval of the original image face some problems and error is maximized. In addition to transmitting image in an environment without noise, transmittance is also investigated in noisy environment so that noise is added to the resultant image after hiding information in a coded image.

In most of the suggested methods, the effect of noise on the transmitted image was not regarded in hiding data in the image. Due to the adjacency of the two sets in which a bit is hidden, the possibility for attacking and finding a hidden bit will be high. For this reason, a set of pixels needed for embedding bits is selected as non-adjacent for having a safer hiding using homomorphism. [4]

3. Result

To extract information, the entire image must be encoded in one place. Given discussions we mentioned in chapter 4, this method requires that each block is compared with all

decoding the image J'' .

Since the smoothness level of one of the two blocks, which had been paired before, is reduced, an equation of smoothness has been used to extract hidden bits.

In general, assume that block (p, q) is corresponding to (i, j) . For blocks $B'_{i,j}$ and $B'_{p,q}$, Smoothness level is determined using the equations below and $f_{B'}^{p,q}$ and $f_{B'}^{i,j}$ will be obtained:

developed blocks in the image to find its own pair. If a part of the image is decoded, bits of that part can be retrieved. This causes the effect of encoding to be positive on hiding in the suggested method. By having a robust code, information extraction is generally prevented. For example, assume that only x block (a small value with respect to the number of image blocks) cannot be decoded. In such circumstances, regardless of retrieval error, only x bit from the main bit string cannot be retrieved for the previous introduced methods, however we can retrieve hidden bit from the rest of blocks. In the suggested method, information extraction faces some problems given that each block is dependent on all the remaining blocks for finding its own pair and even it is sometimes impossible to extract a correct bit.

In the previous methods, the study of results has been carried out on 4 images *Lena*, *Baboon*, *sailboat*, *Splash*. To compare in a better way, these photos are used here. They are shown in Fig. 8.

Fig. 9. From left to right: *Lena*, *Baboon*, *Sailboat*, *Splash*.

The first image shows *Lena* which has been encoded by a random bit string. The second image shows the same coded image after hiding in the transmitter and decoding and extracting information in the receiver. The block size is chosen

16 ($b=16$). By this size, a hidden bit string is completely and correctly extracted and the original image is retrieved.

(a)

(b)

Fig. 10. a) Coded image of Lena b) a retrieved image having size 16.

The diagram of bit error with respect to the size of blocks for the suggested method is shown in the figure below.

Fig. 11. The diagram of bit error percentage with respect to the size of blocks.

The values of error obtained from this method are reduced compared to the method introduced in The results are shown in the diagram 2.

The important point in the two figures above is that the size of blocks is 4 at the beginning while it is 8 for the suggested methods.

The figure below shows an example of comparison for minimizing error of this method compared to the previous methods. This diagram is related to the image *Lena* and white blocks indicate those blocks which have faced an error in extracting bit strings.

(A)

(B)

(C)

Fig. 12. Damaged blocks (A) Zhang method [18] (B) Vienne [19] (C) suggested method.

4. Conclusion

In this study, a new method is introduced for hiding information. in coded images which minimized error from the previous methods up to an acceptable level. Moreover, the

previous methods have never pointed out to noisy environments.

For Gosse noise, the suggested method reduces error well but for pepper and salt noise, error is sometimes reduced and occasionally it is increased compared to the former methods. The reason is that pepper and salt noise changes the amount of pixels with a specific density into maximal and minimal. This change not only produces error while extracting data but also causes blocks not to find their own pairs. As a result, these blocks cause to produce error in two ways and the latter error is not produced for the previous methods.

References

- [1] Busch, Christoph; Funk, Wolfgang; Wolthusen, Stephen: "Digital Watermarking From Concepts to Real-Time Video Applications", IEEE Computer Graphics and Applications, January/February 1999, pp. 25-35.
- [2] Li Yang, Du Sidan: "Research on Wavelet Domain Fractal Coding in Digital Watermarking, Multimedia and Expo", 2005. ICME 2005. IEEE International Conference on, July 2005, p 61-64.
- [3] Kutter, M.; Bhattacharjee, S. K.; Ebrahimi T.: "Towards Second Generation Watermarking Schemes", 6th International Conference on Image Processing (ICIP'99), Kobe, Japan Vol 1 October 25-28 1999.
- [4] Petitcolas, F., R. J. Anderson, M. G. Kuhn (1999). "Information Hiding – A Survey." IEEE Special Issue on Protection of Multimedia Content., Vol. 87, No. 7, pp. 1062-1078.
- [5] Hartung, F., M. Kutter (1999). "Multimedia Watermarking Techniques." Proceeding of IEEE., Vol. 87, No. 7, pp. 1079-1107.
- [6] Cox, I., M. L. Miller (1997). "A Review of Watermarking and the Importance of Perceptual Modeling." SPIE Conference on Human Vision & Electronic Imaging., Vol. 3016, pp. 92-99.
- [7] Wolfgang, R. B., C. I. Podilchuk, E. J. Delp (1999). "Perceptual Watermarks for Digital Images and Video." Proceedings of the IEEE., Vol. 87, No. 7, pp. 1108-1126.
- [8] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding—new paradigm in digital watermarking," EURASIP J. Appl. Signal Processing, vol. 2002, no. 2, pp. 185–196, Feb. 2002.
- [9] J. Tian, "Wavelet-based reversible watermarking for authentication," in Security and Watermarking of Multimedia Contents IV—Proc. SPIE, E. J. Delp III and P. W. Wong, Eds., Jan. 2002, vol. 4675, pp. 679–690.
- [10] J. M. Barton, "Method and Apparatus for Embedding Authentication Information Within Digital Data," U. S. Patent 5 646 997, 2007.
- [11] C. W. Honsinger, P. W. Jones, M. Rabbani, and J. C. Stoffel, "Lossless recovery of an original image containing embedded data," U. S. Patent 6 278 791, 2001.
- [12] B. Macq, "Lossless multiresolution transform for image authenticating watermarking," in Proc. EUSIPCO, Sept. 2000, pp. 533–536. 2010.
- [13] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol. vol. 13, no. 8, pp. 890–896, Aug. 2003.
- [14] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, 2006.