Steganography of Messages using Mandelbrot Fractal

DESAI Hardikkumar V.  
Assistant Professor,  
Naran Lala College of Professional and Applied Sciences, Navsari, India.  
hardik4dreamz@gmail.com

DESAI Apurva A.  
Professor & Head,  
Department of Computer Science,  
Veer Narmad South Gujarat University,  
Surat, India.  
desai_apu@hotmail.com

Abstract

Steganography is a very useful information hiding technique used to communicate secretly. The major advantage of using this technique is that the message which was hidden is not easy to detect. Our research has addressed major aspects of Steganography. We develop new algorithm to achieve Steganography of messages using Mandelbrot Fractal. The algorithm is developed by keeping in mind that the message which was hidden is not easy to detect by naked eye. We have generated histogram for different images to check the distribution of data. Also we checked standard deviation and mean of the images to check the intensity of pixel. We analyze that the image containing stegogramme is not recognized by the naked eye detection, there is not much difference between cover, embedded and cover (post-extraction) image. The paper also focuses on various steganographic techniques like HIDE and SEEKS, JSteg, OutGuess 0.1, OutGuess 0.2, F3, F4, and F5.

Keywords: Steganography, Hide&Seek, JSteg, OutGuess0.1, OutGuess0.2, F3, F4, F5, Fractals, Mandelbrot Fractal

1. Introduction

Internet is an open resource for all, so this technology is very much useful to transmit data from one end to other very easily and speedily. Therefore information security draws attention of researchers, government agencies; law makers, military, intelligence agencies as well as criminals who require uninterrupted communications. They are interested in understanding these technologies and their weaknesses, so as to detect and monitor hidden messages.

1.1 Steganography

The term steganography refers to the art of covert communications. The message is embedded within another object known as a cover work, by tweaking its properties. The resulting output is known as stegogramme. One of the oldest examples of Steganography dates back to around 440 BC in Greek History. Herodotus, a Greek historian from the 5th century BC, revealed...
examples of its use in his work entitled “The Histories of Herodotus”. One elaborate example suggests that Histaeus, ruler of Miletus, tattooed a secret message on the shaven head of one of his most trusted slaves. After the hair had grown back, the slave was sent to Aristagorus where his hair was shaved and the message that commanded a revolt against the Persians was revealed [1].

In modern terms, steganography is usually implemented computationally, where cover work such as text files, images, audio files & video files which are tweaked in such a way that a secret message can be embedded within them.

1.2 Fractals

A fractal is a mathematical set whose patterns are self similar. This means it is "the same from near as from far"[2]. Fractals may be exactly the same at every scale. Fractals are different from regular geometric figures by their fractal dimensional scaling. Doubling the edge lengths of a square scales its area by four, which are two to the power of two, because square is two dimensional. Likewise, if the radius of a sphere is doubled, its volume scales by eight, which are two to the power of three, because a sphere is three-dimensional. A fractal has a fractal dimension that usually exceeds its topological dimension [3] and may all between the integers [4]. Fractals have attracted widespread interest. Virtually every area of science has been examined from a fractal viewpoint, with fractal geometry becoming a major area of mathematics, both as a subject of interest in its own right and as a tool for a wide range of applications. Fractals have also achieved a popular trend, with attractive, highly coloured, fractal pictures appearing in magazines, books, and art exhibitions, and even used for scenery in science fiction films. Further public interest has been generated with the widespread use of computers at home and at school, enabling anyone with a basic knowledge of programming to generate complicated fractal pictures by repeatedly applying a simple operation.

1.3 Mandelbrot Fractal

Mandelbrot Fractals were first described by mathematician Benoit Mandelbrot. He was a French and American mathematician, noted for developing a "theory of roughness" in nature and the field of fractal geometry to help prove it, which included coinig the word "fractal". He later discovered the Mandelbrot set of intricate, never ending fractal shapes, named in his honour. [5] He found geometry to be incomplete. It could not describe the enormous and irregular shape of a mountain. It had no formal representation of the appearance of a cloud. The new geometry that he developed could do all this. It was a description of the beautiful yet irregular and fragmented patterns around us. The term ‘Fractal’ was coined by Mandelbrot from the Latin Fractus, an adjective for the irregular and the fragmented. Essentially, they replicate themselves by fragmentation. Mandelbrot was one of the first to use computer graphics to create and display fractal geometric images, leading to his discovering the Mandelbrot set in 1979. In so doing, he was able to show how visual complexity can be created from simple rules. He said that things typically considered to be "rough", a "mess" or "chaotic", like clouds or shorelines, actually had a "degree of order".[6] His research career included contributions to fields including geology, medicine, cosmology, engineering and the social sciences. Science writer Arthur C. Clarke credits the Mandelbrot set as being "one of the most astonishing discoveries in the entire history of mathematics". [7] Towards the end of his career, he was excellent Professor of Mathematical Sciences at Yale University, where he was the oldest professor in Yale's history to receive tenure. [8] Mandelbrot also held positions at the Pacific Northwest National Laboratory, University Lille Nord de France, and Institute for Advanced
Study and Centre National de la Recherche Scientifique. During his career, he received over 15 honorary doctorates and served on many science journals, along with winning numerous awards. His autobiography, The Fractalist, was published in 2012. Figure 9(a), (b) is an example of Mandelbrot fractal. If we look at a fractal pattern and we see a form; we look closely at a particular region of the pattern and we will see the same form all over again only much smaller this time. And so on it goes, from the largest scales to the smallest. So, the fractals are the repetition of the same structured form.

Figure 1 (a): Mandelbrot Fractal [9] [10]

The Mandelbrot set has its place in complex dynamics; a field first investigated by the French mathematicians Pierre Fatou and Gaston Julia at the beginning of the 20th century. The first pictures of this fractal were drawn in 1978 by Robert W. Brooks and Peter Matelski as part of a study of Kleinian groups. [11] On 1 March 1980, at IBM's Thomas J. Watson Research Center in Yorktown, Heights, New York, Benoit Mandelbrot first saw a visualization of the set. [12]

2. Literature Review

We review different Steganographic techniques like Hide and Seek, JSteg, OutGuess 0.1, OutGuess 0.2, F3, F4 and F5 and other related works regarding steganography are presented. We also presented analysis of various steganography techniques.

2.1 Hide and Seek

Steganography is applicable to all data objects that contain redundancy. People often transmit digital pictures over email and other Internet communication, and JPEG is one of the most common formats for images. Moreover, steganographic systems for the JPEG format seem more interesting because the systems operate in a transform space and are not affected by visual attacks [13]. Visual attacks mean that you can see steganographic messages on the low bit planes of an image because they overwrite visual structures; this usually happens in BMP images. Neil F. Johnson and Sushil Jajodia [14] showed that steganographic systems for palette-based images leave easily detected distortions.

2.2 JSteg

The JSteg algorithm was developed by Derek Upham and is essentially as same as a copy of the Hide & Seek algorithm, because it employs sequential least significant bit embedding. In fact,
the JSteg algorithm only differs from the Hide & Seek algorithm because it embeds the message data within the LSBs of the DCT coefficients, rather than its pixel values [15].

2.3 OutGuess 0.1

In much the same way that embedding the message data sequentially using the Hide & Seek method was not considered very secure, neither was the fact that the JSteg algorithm embedded in the same fashion. The first version of Outguess, designed by Neils Provos [16], improved the JSteg algorithm by scattering the embedding locations over the entire image according to a PRNG on image.

2.4 OutGuess 0.2

Neils Provos [17] created a revised version of the OutGuess 0.1 algorithm, called OutGuess 0.2. It was ensured that the statistical properties of the cover image were maintained after embedding, such that stegograms looks statistically similar to a clean image. This would make it harder for steganalysts to calculate the likelihood that their suspect image is a stegogramme. The algorithm is exactly the same for OutGuess 0.2 as it was for OutGuess 0.1. The difference lies in what happens after the information has been embedded. In OutGuess 0.2, corrections are made to the coefficients such that they appear similar to that of a clean image in terms of frequencies of the values. This is known as statistics aware steganography.

2.5 F3

As an alternative to the OutGuess 0.2 algorithm, AndreasWestfeld designed an algorithm called F3 [18]. It was considered even more secure. The reason for this is that it did not instantiate the same embedding process as the JSteg and OutGuess algorithms. Instead of avoiding embedding in DCT coefficients equal to 1, the F3 algorithm permitted embedding in these regions, at the same time as it would still avoid embedding in zeros and the DCT coefficients. The algorithm still embedded the message data sequentially. Another change with this algorithm was that it did not embed directly in the least significant bits of the DCT coefficients, but instead took the absolute value of the coefficients first, before comparing them to the message bits. If both the absolute value of the coefficient, and the message bit were the same, then no changes are made. If they are different, then the absolute value of the DCT coefficient is reduced by 1. An implication of this however, is that zero values are often created which the decoding algorithm will not be programmed to extract data from. The F5 algorithm worked around this by re-embedding mi when the result is that a zero DCT coefficient is created.

2.6 F4

The main drawback with F3 was the reality that it effectively embedded more zeros than ones as a result of the shrinkage mechanism. This meant that when the statistical properties of the stegograms are examined through its some object of embedding became visible. This is much the same as what happened in the JSteg implementation except a slightly different pattern is derived. In addition to this, steganalysts also found that more odd coefficients existed in F3 stegograms than even coefficients. This now meant that there were two weaknesses that could be examined when viewing the histogram of a suspect image. F4 was developed to remove these properties such that the histogram would appear similar to that of a clean image.
2.7 F5

The F5 algorithm [19] is predominantly the same as the F4 algorithm, at least in terms of its strategy for encoding the message data. However, the F5 algorithm was designed in an attempt to improve on the F4 algorithm by minimizing the disturbance caused when embedding the message data.

The earliest work was done by Davern and Scott (1996) [20], who divide the domain blocks of the image into two sets. They then use standard fractal image compression techniques to select a domain block that matches the range block, however they choose a block from one of the two domain sets depending on whether the data bit they are embedding is a one or a zero.

A. Jacquin (1995) [21], most fractal coding schemes are based on representation by Partition Iterated Function System (PIFS), a solution to inverse problem which was first published by Jacquin. A PIFS differs from IFS in the Individual mappings operating on a subset of image, rather than the entire image.

Pauate et al, Saupe et al, Wotilberg et al, (1997, 1994, 1999) [22, 23, 24], Theoretical background referred to in fractals to generate fractals considers an IFS consisting of a collection of contractive affine transformations. The iteration procedure of applying a number of transforms is terminated when convergence is met i.e. an attractor.

Bas et al, Li C Wang, Liao P et al (1998,2000,2006) [25,26,27], suggested that a great variety of steganographic methods on fractal compression principles are good, but greatest robustness is ensured by means of the methods [26,27] since they directly manipulate the code of compressed image. Building in secrecy increase the given approaches will provide high level of protection.

Lokesh Kumar (2012) [28], in his proposed system cryptographic and steganographic security is combined to give two tier securities to secret data. In proposed scheme secret message is encrypted before hiding it into the cover image which gives high security to secret data. Advanced encryption standard (AES) is used to encrypt secret message and alteration component technique is used to hide encrypted secret message into cover image. Since the resulting perceptual quality of the mixed images is good, it is hardly attracted from eavesdropper by naked eye. Finally we can conclude that the proposed technique is effective for secret data communication.

Rosziati Ibrahim et al (2010) [29], in his proposed a new steganography algorithm with 2 layers of security. A system named SIS (Steganography Imaging System) has been developed using the proposed algorithm. They tested few images with various sizes of data to be hidden. With the proposed algorithm, they found that the stego image does not have a noticeable distortion on it (as seen by the naked eyes). SIS can be used by various users who want to hide the data inside the image without revealing the data to other parties. SIS maintains privacy, confidentiality and accuracy of the data.

Wojciech Frączek et al (2010) [30], suggested that Stream Control Transmission Protocol (SCTP) is a new transport layer protocol that is due to replace TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) protocols in future IP networks. Currently, it is implemented in such operating systems like BSD, Linux, HPUX or Sun Solaris. It is also supported in Cisco network devices operating system (Cisco IOS) and may be used in Windows. This paper describes potential steganographic methods that may be applied to SCTP.
and may pose a threat to network security. Proposed methods utilize new, characteristic SCTP features like multi-homing and multi streaming. Identified new threats and suggested countermeasures may be used as a supplement to RFC 5062, which describes security attacks in SCTP protocol and can induce further standard modifications.

Hemalatha S (2013) [31], observes that two secret images can be hidden in one color image and they can be regenerated without actually storing the image. This approach results in high quality of the stego-image having high PSNR values compared to other methods. However the disadvantage of the approach is that it is susceptible to noise if spatial domain techniques are used to hide the key. This can be improved if transform domain techniques are used to hide the key. The approach is very simple and the security level can be increased by using standard encryption techniques to encrypt the keys.

Sharon Rose Govada et al (2012) [32], he suggested a method is a combination of Word shifting, Text Steganography and Synonym Text Steganography. So we called this as “Three Phase Shielding Text Steganography” This method overcomes various limitations faced by the existing Steganographic algorithms.

Gowtham dhanarasi (2012) [33], suggested a novel method for image steganography using block complexity analysis in wavelet domain. Many researchers have been reported different techniques but all the methods suffer with image quality problem. So in order to achieve good quality.

3. Proposed Algorithm

We present algorithm to hide the image within image, we develop a new algorithm with the use of Mandelbrot Fractal. The algorithm is developed by keeping in the mind that no one can easily detect the hidden image.

3.1 Embedding algorithm

In this approach we take three images showed in figure 2 for the purpose of steganography of text message using Mandelbrot fractal. Image 2(a) is an original image which refers to as cover or carrier image. Text image 2(b) is an image to embed within cover image and image 2(c) is an image of Mandelbrot Fractal which is used to identify location on image 2(a)
First, image 2(c) of Mandelbrot Fractal is generated on Manaal image 2(a) to identify locations in Manaal image 2(a) after that Manaal image 2(a) is splitted into four parts. All pixel values are changed to 8 bit value 11111111 using bit manipulation technique and convert last two bit values to 0 using bitor and bitand operations and make the value 11111100.

Text image 2(b) bit value is changed to 8 bit value 11111111 and these values are divided into four pairs 11,11,11,11. Now, first part of Manaal image 2(a) last two bits 00 are embedded with first pair 1 1 (1 and 2) of Text image 2(b). In the second part last two bits 00 are embed with second pair 1 1 (3 and 4), third part of last two bits 00 are embedded with third pair 1 1 (5 and 6) and the fourth part of last two bits 00 are embedded with fourth pair 1 1(7 and 8). The embedding process is done anti-clock wise to generate a new kid image 3(a) containing stegogramme which looks like original Manaal image 2(a).

![Figure 3 (a): kid Image (With Stegogramme)](image)

[Algorithm 1 – Embedding algorithm to hide message using Mandelbrot Fractal]

**Step 1:** Get the image “A”.
**Step 2:** Generate Mandelbrot Fractal to defined targeted region in Image.
**Step 3:** Change the Pixel value of the targeted region in an Image.
**Step 4:** Make the partition of image in four parts.
**Step 5:** Get the image ‘B’ to embed in image ‘A’
**Step 6:** Separate bits and make pair of two bits in four groups using bit manipulation.
**Step 7:** Join the pairs of image ‘B’ into the change value of image ‘A’ “anticlockwise to generate new image A1 containing stegogramme1”.
**Step 8:** End

**Extracting Algorithm**
In the extraction process we take the embedded kid image 4(a) and recognize targeted region by generating Mandelbrot fractal image 4(b) on kid image 4(a).

![Figure 4(a) - Kid Image (With Stegogramme)](image) ![Figure 4(b) - Mandelbrot Fractal](image)
Firstly, extract last two bits 11 from each part of kid image 4(a). After getting all the values from different four groups of kid image 4(a) in anticlockwise manner and join them together to extract the hided Text image (extracted) 5(a) and compare original image, extracted image and embedded image for the intensity of pixels.

![Figure 5(a) - Text Image (extracted)](image)

**Algorithm 2—Extracting algorithm to extract text using Mandelbrot Fractal**

**Step 1:** Get the embedded image “A1”.
**Step 2:** Generate Mandelbrot fractal to define the locations of stegogramme.
**Step 3:** Extract the embedded pixels and make four groups by changing the value using bit manipulation.
**Step 4:** Pad 1st and 2nd group and 3rd and 4th group.
**Step 5:** Merge all groups derived from previous step.
**Step 6:** Extract the actual message (text) or Image and cover image A1.
**Step 7:** End

**4. Experimental Results**

The results are based on comparison of images and histogram of images. We examine different images for steganography. Over here, we analyze the mean and standard deviation of images to check the intensity of pixel.

Firstly, we hide image (b) within image (a) and new image (c) is generated containing stegogramme. Then we compare cover (carrier/cover) image (a) with image (c) to check whether it is embedded successfully or not. We compare generated histogram to check the data distribution and analyze mean and standard deviation of cover image, embedded image and post extracted image to check the intensity of pixels.

Results are as follows.
Moreover, we find mean and standard deviation of twenty five images to check the intensity of pixels as shown in table (2).

Table 1: Mean and standard deviation of Grass image

<table>
<thead>
<tr>
<th></th>
<th>Mean $\bar{X}$</th>
<th>Standard Deviation $\sigma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cover</td>
<td>Embedded</td>
<td>Cover image Post-Extraction</td>
</tr>
<tr>
<td>249.75</td>
<td>248.80</td>
<td>249.48</td>
</tr>
</tbody>
</table>

Figure 6(a) Grass Image (Carrier/Cover)  
Figure 6(b) Text (Image to Hide)  
Figure 6(c) Grass-em Image (With Stegogramme)
We analyze the mean and standard deviation of images with cover image, embedded image and cover image (post extraction) to find the variance between them. After analysis we find that average mean of cover images is 246.17, average mean of embedded images is 246.15 and average mean of cover image (post extraction) is 244.90. Average standard deviation of cover images is 40.03, average standard deviation of embedded images is 42.35 and average standard deviation of cover image (post extraction) is 42.91.

<table>
<thead>
<tr>
<th>No</th>
<th>Cover</th>
<th>Embedded</th>
<th>Cover image Post-Extraction</th>
<th>Cover</th>
<th>Embedded</th>
<th>Cover image Post-Extraction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>248.53</td>
<td>246.81</td>
<td>248.91</td>
<td>37.72</td>
<td>40.83</td>
<td>39.66</td>
</tr>
<tr>
<td>2</td>
<td>241.22</td>
<td>239.78</td>
<td>239.8</td>
<td>50.48</td>
<td>55.32</td>
<td>55.83</td>
</tr>
<tr>
<td>3</td>
<td>248.62</td>
<td>248.69</td>
<td>251.36</td>
<td>36.21</td>
<td>44.21</td>
<td>36.75</td>
</tr>
<tr>
<td>4</td>
<td>249.52</td>
<td>249.21</td>
<td>247.68</td>
<td>36.81</td>
<td>38.18</td>
<td>37.65</td>
</tr>
<tr>
<td>5</td>
<td>240.78</td>
<td>245.12</td>
<td>230.98</td>
<td>55.63</td>
<td>44.39</td>
<td>63.82</td>
</tr>
<tr>
<td>6</td>
<td>249.68</td>
<td>249.86</td>
<td>249.39</td>
<td>34.86</td>
<td>35.41</td>
<td>36.12</td>
</tr>
<tr>
<td>7</td>
<td>248.53</td>
<td>248.08</td>
<td>248.51</td>
<td>34.28</td>
<td>35.87</td>
<td>36.83</td>
</tr>
<tr>
<td>8</td>
<td>248.56</td>
<td>248.51</td>
<td>248.21</td>
<td>37.48</td>
<td>38.92</td>
<td>38.72</td>
</tr>
<tr>
<td>9</td>
<td>247.89</td>
<td>247.51</td>
<td>241.93</td>
<td>34.61</td>
<td>39.71</td>
<td>41.2</td>
</tr>
<tr>
<td>10</td>
<td>249.09</td>
<td>249.08</td>
<td>238.46</td>
<td>51.38</td>
<td>53.61</td>
<td>56.18</td>
</tr>
<tr>
<td>11</td>
<td>248.78</td>
<td>248.42</td>
<td>248.31</td>
<td>37.62</td>
<td>39.82</td>
<td>39.83</td>
</tr>
<tr>
<td>12</td>
<td>249.63</td>
<td>249.33</td>
<td>249.22</td>
<td>37.19</td>
<td>38.86</td>
<td>41.25</td>
</tr>
<tr>
<td>13</td>
<td>248.91</td>
<td>248.19</td>
<td>248.82</td>
<td>54.12</td>
<td>56.38</td>
<td>57.93</td>
</tr>
<tr>
<td>14</td>
<td>240.92</td>
<td>240.63</td>
<td>232.81</td>
<td>37.67</td>
<td>38.16</td>
<td>39.12</td>
</tr>
<tr>
<td>15</td>
<td>240.74</td>
<td>240.86</td>
<td>240.49</td>
<td>37.61</td>
<td>38.22</td>
<td>39.43</td>
</tr>
<tr>
<td>16</td>
<td>240.56</td>
<td>240.14</td>
<td>240.19</td>
<td>34.81</td>
<td>46.63</td>
<td>47.81</td>
</tr>
<tr>
<td>17</td>
<td>240.24</td>
<td>248.13</td>
<td>248.63</td>
<td>37.59</td>
<td>37.94</td>
<td>37.08</td>
</tr>
<tr>
<td>18</td>
<td>249.72</td>
<td>249.61</td>
<td>249.73</td>
<td>51.39</td>
<td>52.71</td>
<td>51.78</td>
</tr>
<tr>
<td>19</td>
<td>246.52</td>
<td>246.18</td>
<td>246.22</td>
<td>37.81</td>
<td>39.12</td>
<td>39.83</td>
</tr>
<tr>
<td>20</td>
<td>248.12</td>
<td>248.15</td>
<td>248.56</td>
<td>37.78</td>
<td>39.81</td>
<td>32.18</td>
</tr>
<tr>
<td>21</td>
<td>249.54</td>
<td>245.07</td>
<td>245.78</td>
<td>34.29</td>
<td>41.4</td>
<td>41.86</td>
</tr>
<tr>
<td>22</td>
<td>249.78</td>
<td>249.19</td>
<td>249.82</td>
<td>37.19</td>
<td>39.18</td>
<td>39.08</td>
</tr>
<tr>
<td>23</td>
<td>240.46</td>
<td>240.21</td>
<td>240.83</td>
<td>34.57</td>
<td>36.89</td>
<td>36.22</td>
</tr>
<tr>
<td>24</td>
<td>247.19</td>
<td>247.03</td>
<td>247.26</td>
<td>47.69</td>
<td>51.12</td>
<td>50.59</td>
</tr>
<tr>
<td>25</td>
<td>240.76</td>
<td>240.16</td>
<td>240.67</td>
<td>34.12</td>
<td>36.19</td>
<td>36.18</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td>246.176</td>
<td>246.158</td>
<td>244.9028</td>
<td>40.0364</td>
<td>42.3552</td>
<td>42.9172</td>
</tr>
</tbody>
</table>

Table 2: Analysis of images for steganography using Mandelbrot Fractal
5. Conclusions

We have studied various existing steganographic techniques to hide information like Hide & Seek, JSteg, OutGuess 0.1, OutGuess 0.2, F3. The limitations prevailing in those techniques were found. Thereafter, the objectives of the study were set that the embedding process of using sequential least significant bit was meant to be replaced by innovative approach of using fractals to hide information.

It is calculated that, the mean difference between original image and embedded image is 0.02, mean difference between embedded and cover image (post extraction) is 1.25 and mean difference between original image and cover image (post extraction) is 1.27. Further standard deviation difference between original image and embedded image is 2.31, standard deviation difference between embedded and cover image (post extraction) is 0.56 and standard deviation difference between original image and cover image (post extraction) is 2.88.

It was concluded that the image containing stegogramme is not recognized by the naked eye detection, there is not much difference between cover, embedded and cover (post-extraction) image. In the analysis we find mean and standard deviation and concluded that there is very less difference amongst them. That means they remain almost the same.

6. Limitations and Future Work

The research provides an opportunity to go ahead in the field of Information Hiding. The research can be extended by using other fractals for the purpose of steganography. The limitation of our technique is that the size of image to hide should be small in size as compare to size of the fractal used. It may be attempted to overcome. Moreover, the research may be extended by using different carriers (covers) like audio and video.

References


