Digital Image Encoding Scheme using Fractal Approach

Richa Gupta*[1], Deepti Mehrotra[2], Rajesh Kumar Tyagi[3], Rishi Kumar[4]
Amity University Uttar Pradesh[1,2,4] , KIET, Ghaziabad, Uttar Pradesh[3]
Email: richa4483@gmail.com, mehdeepti@gmail.com, profrajeshkumartyagi@gmail.com, rkumar25@amity.edu

Abstract: Image encoding algorithm is a state of art of information hiding using any image as shield. In this paper concept of steganography algorithm and various terms related are defined. The efficiency of the steganography algorithm is improved by using a novel fractal technique. Fractals are self-similar complex image and created by applying a set of affine transformation on image iteratively. In this paper, we propose to exploit the self-similarity present an image to determine the fractal regions. Location of the fractals region present in an image is used to hide information in that region. Proposed algorithm results into good quality coded image and visually it looks exactly like the cover image. This allows the user to hide information without letting the other unauthorized user realize that the image contains a secret message. In this paper, effectiveness of steganography algorithm is analyzed using the fractal technique on various types of images. Further proposed algorithm shows the effect of message size on the quality of coded image.

Keywords: Image encoding, Steganography, Fractal, Message Hiding, Message Retrieving

1. Introduction: Since the early days of communication people around the globe realized the importance of information security to protect the secrecy, consistency, and integrity of data. It was important to develop a mechanism that would restrict the leakage of data to an unauthorized source. Critical data was marked to indicate that it should be protected and stored in a secure environment. The rapid growth and widespread use of data processing raised the need for a secure mechanism for protection of data. There is technology for image encoding like cryptography, steganography and encryption. Encryption protects information, but this protection can be broken with computational power.

Steganography is an old science, and its literal meaning is the practice of concealing messages or information within other non-secret text or data. It can take confidentiality to a new level since it embeds secret information or message within another object, which makes the existence of information in the object practically undetectable. The main objective of steganography is to hide information within another object or message called cover message. The cover message can be plain text, an image, an audio file or a video file [1]. The message that is to be hidden is called secret message which can be plain text, an image, a video or an audio file. Steganography is better than cryptography because the objective of cryptography is to make data unreadable by the third party, whereas the goal of steganography is to hide information from the third party [2].

The earliest work was done by M. F. Barnsley [2], introduced the Iterated Function Systems (IFS) for the first time. It was based on the Self-Similar of fractal sets. He assumed and proposed that objects can be approximated by Self-Similar objects that are generated by the use of IFS transformations. Further Davern and Scott [3], who divided the domain blocks of the image into two parts. Then they apply fractal image compression technique to select a domain block that matches the range block. However, they select a block out of the two domain sets depending on whether the data

978-1-5386-2615-3/18/$31.00 ©2018 IEEE

bit to be embedded is one or zero. There are many methods of steganography on fractal principles that are being described in the literature, but the robustness is ensured by the method used because the method changes the code and quality of an image. Better the hiding algorithm more secure will be the system.

In this paper, the proposed algorithm, works only on bitmap images. In this technique, we find the regions where sharpness is present, which is easier to find in grayscale as compared to RGB or any other colored images [4]. The fractal technique is then determined on the grayscale image to find fractal region. The information is then embedded in these fractal regions, and the generated image is called stego image. The main advantages of this technique are the

2. Fractals: Basic Understanding

Fractals are perpetual self-similar patterns across an infinite scale. They are established by repeating a single process for 'n' number of times. It is an augmenting –symmetry. For every level ranging from the smallest to an infinitely big scale, if the imitation is same it is called as a self-similar pattern. Fractals, its roots can be traced back to 1970s when an IBM mathematician Benoit Mandelbrot [5][6] watched and analyzed a customary geometry to be imperfect. It couldn't clarify depict the enormous and unpredictable state of a mountain. It had no proper representation of the geometry of a cloud. The new geometry that he coined could successfully describe and depict the kind of objects that were earlier undefined [6].

The fractal procedure can be utilized to shroud greatest measure of information in a picture without influencing its quality and to make the concealed information hearty and sufficiently effective to withstand picture preparing which doesn't change the visual appearance of the picture [6], so this strategy can be utilized for Steganography.

amount of information that is to be embedded is equal to the host signal while it is limited to the conventional data hiding techniques. So the unauthorized user will not be able to detect the secret message behind the cover image through naked eye, even if they know that there is secret message hidden behind the cover message it is difficult for the third party to estimate the random image from stego image because random variables are used using transformation of image [2].

The paper is organized as follows: Section 2 and 3 gives an overview of fractals and image steganography respectively. Section 4 encloses proposed algorithm. Simulation results and discussion is presented in Section 5. The paper is concluded in section 6.

Characteristics of the fractal:

1. Exact Self-resemblance – Identical geometry at all scales [7]

2. Quasi Self-resemblance - Small imitations of the entire fractal in a twisted, degraded manner.

3. Statistical Self-resemblance - repeats a pattern in such a manner that numerical and statistical values are maintained [7].

- Emergent properties: It has a fine and detailed structure even at some random points.
- Locally and globally irregular geometry.

The fractal technique can be used to hide maximum amount of data into an image [8]. Data to be protected can be of any type while the cover image must be BMP. The fractal technique allows covering secret information without actually degrading the quality and appearance of the cover image

[9]. Therefore, we have proposed a new method to determine fractal regions in the image and hide maximum data possible than with any other algorithm [10]. The amount of data that can be hidden totally depends on upon the size of the cover image. In fractal image steganography, the model for the authorized user includes side information which can be the password that is used during retrieving of information. While for the attacker the model is without side information or initial parameters. That is information received by the authorized and unauthorized user is asymmetric, which means it is not same for receiver and attacker.

3. **Image encoding using Steganography**

Steganography is an old science its literal meaning is the practice of concealing messages or information within other non-secret text or data. The authorized holder of the message needs to utilize the knowledge of the particular mechanism of steganography that is engrossed to recover the hidden message from the stego image. The goal of steganography is to allow parties to converse without the discourse of information in any form [1]. This characteristic of steganography keeps it aside from cryptography which acts as a medium for private communication between parties, however, can arouse suspicion based solely on its existence. Steganography traced its root right back to its first implementation in 440 BC by Herdotus [3]. Since then steganography has constantly been in use till the present day. Earlier Steganography existed as messages were written on wood covered with wax, written on rabbit's stomachs, or were tattooed on slaves. During World War II, the French Resistance invented invisible ink. Modern steganography came into existence in the year 1985 with the ingression of personal computers [5]. It started with Secreting message within the lowest bit, secreting message with encrypted data or with any random object, concealing a picture that can be uncovered by using basic drawing tools. Chaffing and winnowing - is defined as a cryptographic tool to successfully attain confidentiality while sending data over an insecure passage without using encryption. **Steganalysis**: An attempt to ascertain the presence of steganography requires diligent examination and analysis. The art of unmasking the message hidden by applying steganography is known as steganalysis. The purpose of steganalysis [5] is to detect suspected packages, identify whether it has payload instilled into them and if feasible return the payload. Contrary to cryptanalysis where the existence of secret message is known, steganalysis needs to identify payload from piles of suspected data.

4. The Proposed Algorithm

The proposed algorithm hides a message or information in the form of a plain text or an image within another image by detecting regions using the fractal technique. The image in which the message is to hide is called cover image while the image after hiding secret message is called as stego image [13]. This technique hides the maximum amount of data without degrading the quality of original image. Proposed algorithm is divided mainly into two stages

4.1 First Stage -Message Hiding

The first stage is called message hiding and the second stage is called as message retrieving or extracting stage. These stages are then further subdivided.

Step1. Open an Image**-** Add the picture, which is bitmap image.

Step2. Convert Image into Grayscale Convert the picture into grayscale using equation 1 and 2

$$I_{RGB}=(F_R,F_G,F_B) \quad (1)$$

x = 0.330 FR + 0.587 FG + 0.114 FB. (2)

Step3. Divide image into blocks- Partition the cover image into blocks, blocks are called regions. Initialize , BlockSize = 32 ; The size of the block must be greater than 32 pixels because if cannot detect fractal if the size is less than 32 pixels [10] [13]. We can also take 48 pixels for each block. But in our work, we have taken 32 pixels for each block.

Step 4. Fractal detection- Each subdivided block is called region. Find no of horizontal blocks, no of vertical blocks. Calculate mean and variance of each block, and also the mean variance of the whole image. Compare means of domain and range.

Step5. Hiding- For data hiding, hide data or information in RGB. Hide information in every 3 bits for blue because it is the least visible color, and for red and green hide in 1 bit of every fractal block [14]. The size of the message that is to hide should not be greater than the fractal region.

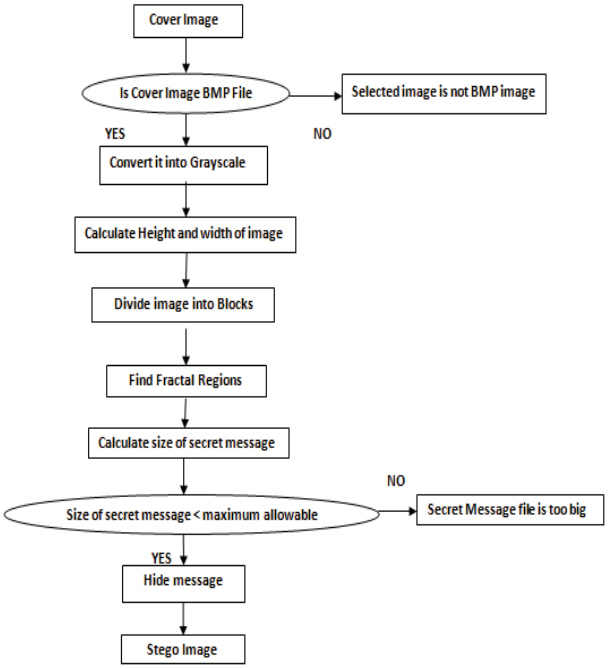


Figure 1. Hiding message

4.2 Second Stage - Retrieving Message

This is the second stage after hiding the message the next step is to retrieve it. We apply the same algorithm as used for hiding. It starts with specifying the path if stego image and location for the output and then the algorithm checks whether the entered image by a user is a stego image or not [13]. The system only works for BMP images and if the entered image is not a BMP, it will display an error and program will terminate. Checks red component of the first pixel for the message and then checks green component of the second pixel with second character .and blue component of the third pixel with 2 bits. And repeat iterations until pixels get exhausted. Since blue color is the most insensitive to eyes 2 bits of blue pixel is used to whereas for both green and blue each 1 bit is utilized.

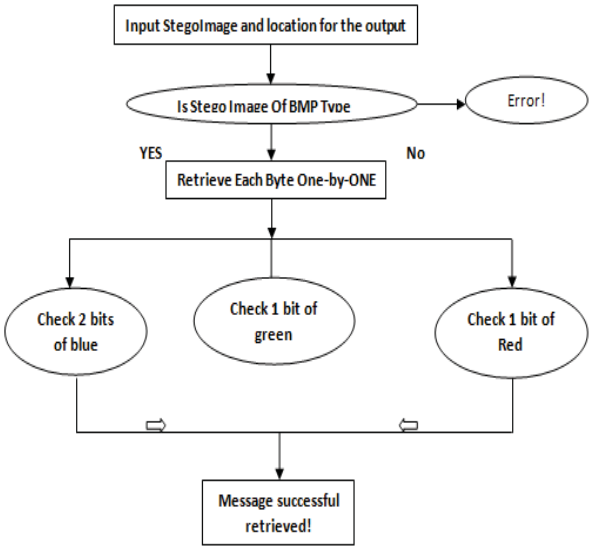


Figure 2. Retrieving message

Performance of algorithm is analyzed using following parameters.

SNR (Signal to Noise Ratio)

$$SNR = P\,signal/Pnoise = \mu/\sigma \quad \textbf{(3)}$$

where **μ** is the signal mean or expected value and **σ** is the standard deviation of the noise [11].

PSNR (Peak Signal Noise Ratio)

$$PSNR = 20\,log10(\mathrm{MAX_i}) - 10\,log10(MSE) \quad (4)$$

$\mathrm{MAX_I}$ is the maximum possible pixel value of the image [12]

RMSE (Root Mean Square Error)

The RMSE of an estimator $\ddot{\theta}$ with respect to an estimated parameter θ is:

$$\mathrm{RMSE}(\ddot{\theta}) = \sqrt{\mathrm{MSE}(\ddot{\theta})} = \sqrt{\mathrm{E}((\ddot{\theta} - \theta)^2)} \quad (5)$$

MAE (Mean Absolute Error)

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|ei| \quad \textbf{(6)}$$

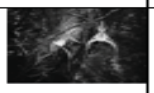
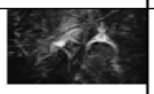
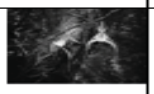
Where, $|\boldsymbol{ei}| = |\boldsymbol{fi} - \boldsymbol{yi}|$, **and** f_i is the prediction and y_i the true value

4. Experimental Results

We have analyzed system efficiency and robustness by taking the type of secret message as one of the parameters and then checking on various aspects of the output image and then comparing the final results.The experiment includes hiding secret message of the type .doc and analyzing the results from the given set of data, we have analyzed three types of image – colored, grayscale, dual-tone keeping the type of message uniform for all the three types and then testing the system by increasing the size of the secret message. The algorithm works for BMP images; it is mandatory for the user to use cover image of type BMP, while the secret message that needs to be hidden can consist of any format.

Table 1. SNR, PSNR, and RMSE of Stego images

Case No.	Original Image	Resolution (H x W) (x)	Stego Image	Size of the stego image	Message type	Message Size (KB)	SNR(dB) (y1)	PSNR (dB) (y2)	RMSE	MAE
	Colored Image									
1		320 X240		320X240	DOC FILE	51	47.275	56.432	0.3845	0.1779
2		320 X240		320X240	DOC FILE	100	47.240	56.397	0.3860	0.1787
3.		320 X240		320X240	DOC FILE	160	47.1852	56.341	0.3885	0.1803
4		320X240		320X240	DOC FILE	231	47.253	56.410	0.3854	0.1788
5.		320X240		320X240	DOC FILE	270	47.242	56.399	0.3859	0.179
6.		320X240		320X240	DOC FILE	309	47.265	56.422	0.3849	0.1786
7.		320X240		320X240	DOC FILE	333	47.292	56.449	0.3837	0.1777

	Grayscale Image									
1		504X284		504X284	DOC FILE	51	40.496	54.888	0.4575	0.2139
2		504X248		504X284	DOC FILE	100	40.5097	54.901	0.4568	0.2134
3.		504X284		504X284	DOC FILE	160	40.4687	54.860	0.4589	0.2140
4		504X284		504X284	DOC FILE	231	40.5242	54.916	0.4560	0.2131
5.		504X284		504X284	DOC FILE	270	40.502	54.8948	0.4571	0.2139
6.		504X284		504X284	DOC FILE	309	40.516	54.908	0.4564	0.2135
7.		504X284		504X284	DOC FILE	333	40.487	54.879	0.45799	0.2140

For Colored image when covered image is a of size 320 X 240 i.e., 230400 byte and secret data size is 333kb i.e., 341870 byte. Maximum size of data that can be hidden is 460800 byte Since the size of secret message is less than the maximum allowable size therefore we are able to hide the secret message. And from the above formula, Peak Signal To Noise Ratio (PSNR) is 56.449db and "this is an accepted ratio", the RMSE 0.3837 and the SNR is 47.292

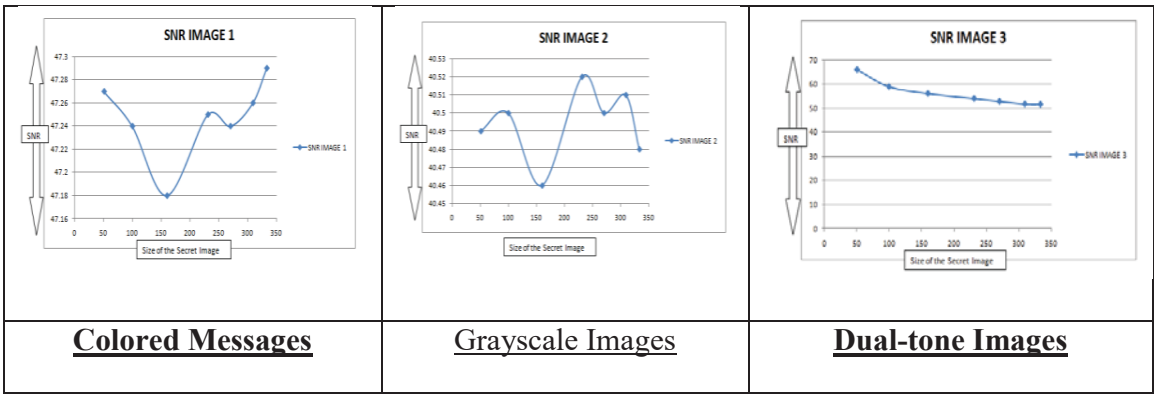
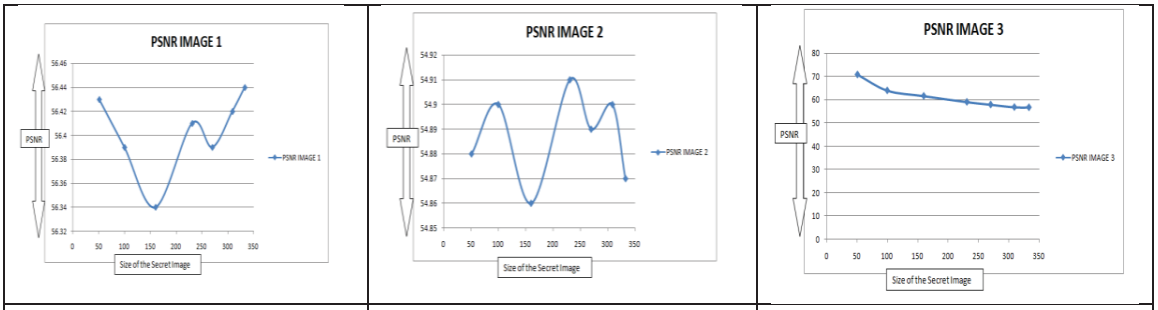


Figure 3. SNR v/s Size of Message

For Grayscale image when covered image is a of size 504X284 i.e., 429462 byte and secret data size is 333kb i.e., 341870 byte. The maximum size of data that can be hidden is 858816 byte. Since the size of secret message is less than the maximum allowable size therefore we are able to hide the secret message. And from the above formula, Peak Signal to Noise Ratio (PSNR) is 54.879db and "this is an accepted ratio" , the RMSE 0.4579 and the SNR is 40.487.



Colored Images	Grayscale Images	Dual-tone Images

Figure 4 PSNR v/s Size of Message

For Dual-Tone Image when covered image is a of size 1293X1480 i.e., 5742454 byte and secret data size is 333kb i.e., 341870 byte. Maximum size of data that can be hidden is 11481840 byte. Since the size of secret message is less than the maximum allowable size, therefore we are able to hide the secret message. And from the above formula, Peak Signal to Noise Ratio (PSNR) is 56.654 dB "and this is an accepted ratio", the RMSE 0.3748and the SNR is 51.772. The PSNR value is highest for Dual-tone Image i.e. 56.654 dB.

5. CONCLUSION

Proposed algorithm uses a new approach called image steganography using the fractal image. The application makes a picture referred as stego picture in which the individual information is inserted which is ensured with a secret key that is profoundly secured. The principle target of the undertaking is to add to a steganography application that gives great security. The proposed methodology gives more security and can shield the message from stego assaults. The picture determination doesn't change much and is practically unimportant when the message is inserted into the picture, and the picture is ensured with the individual watchword. In this way, it is unrealistic for an unapproved individual to harm the information to. Hiding a message with this system eliminates the possibility of a message being identified. If the message is additionally encoded, if found, it should likewise be split(yet another layer of insurance).

6. REFERENCES

[1] J. Kour and D. Verma, "Steganography Techniques –A Review Paper," *Int. J. Emerg. Res. Manag. &Technology*, vol. 9359, no. 35, pp. 2278–9359, 2014.

[2] G. S. Eswari, N. Leelavathy, and U. S. Rani, "Fractal Image Steganography Using Non Linear Model," pp. 2644–2649, 2014.

[3] Hardikkumar V. Desai & Apurva A. Desai, "Image Steganography Using Mandelbrot Fractal," *Int. J. Comput. Sci. Eng. Inf. Technol. Res. (IJCSEITR*, vol. 4, no. 2, pp. 71–80, 2014.

[4] A. M. Al-shatnawi, "A New Method in Image Steganography with Improved Image Quality," *Appl. Math. Sci.*, vol. 6, no. 79, pp. 3907–3915, 2012.

[5] N. Johnson and S. Jajodia, "Steganalysis of images created using current steganography software," *Inf. Hiding*, pp. 273–289, 1998.

[6] C. S. Rawat, S. Meher, and C.

Engineering, “3 A Hybrid Image Compression Scheme using DCT and Fractal Image Compression,” *Int. Arab J. Inf. Technol.*, vol. 10, no. 6, pp. 553–562, 2013.

[7] K. Thamizhchelvy, “a Novel Approach To Generate Fractal Images Using Chaos Theory,” vol. 5, no. 4, pp. 152–157, 2014.

[8] Y. Wu and J. P. Noonan, “Image Steganography Scheme using Chaos and Fractals with the Wavelet Transform,” *Int. J. Innov. Manag. Technol.*, vol. 3, no. 3, pp. 285–289, 2012.

[9] A. Garg, “Article: An Improved Algorithm of Fractal Image Compression,” *Int. J. Comput. Appl.*, vol. 34, no. 2, pp. 17–21, 2011.

[10] Hitashi, G. Kaur, and S. Sharma, “Fractal image compression- a review,” vol. 2, no. 2, pp. 1–4, 2012.

[11] K. Gulati, “Information Hiding Using Fractal Encoding,” no. January, 2003.

[12] D. Omain, “a N Ovel S Ecure I Mage S Teganography M Ethod B Ased O N C Haos T Heory I N S Patial,” vol. 3, no. 1, pp. 11–22, 2014.

[13] T. A. Abbas and H. K. Hamza, “Steganography Using Fractal Images Technique,” *IOSR J. Eng.*, vol. 04, no. 02, pp. 52–61, 2014.

[14] A. S. Nori and A. M. Al-qassab, “STEGANOGRAPHIC TECHNIQUE USING FRACTAL IMAGE By 2 . Information Hiding 3 . Fractals : History and Theory,” vol. 23, no. 1, pp. 52–59, 2014.