STEGANOGRAPHY BASED ON FRACTAL SET

Bubere Arfat , Ravindra Mhatre

Abstract - So as to boost the protection of steganography system, this paper presents a scheme of steganography based on fractal images. This method makes use of fine properties of creation of fractal images, like easy generation, sensitive dependence on their initial condition, information are embedded during creating fractal images by secret information and initial parameters. The receiver can extract secret information by comparing the difference between Stego-Images and Cover-Images recovered with the identical initial parameters. The attackers can't recover the Cover-Images without initial parameters, then don't get secret information. On the opposite hand, the embedding and extracting are unsymmetrical, therefore the scheme has higher security and do well in resisting different steganalysis. Experiments show that the scheme has good imperceptibility and undetectability. The results of this paper have practical significance in extending the study of steganography.

Key Words: Steganography; Julia Set; Fractal images,Steganalysis

----------***----------

I INTRODUCTION

Steganography[1], a way of data hiding, have been employed in various useful applications, e.g., copyright protection, feature tagging, and secret communication. in a very steganography system, information is hided in an appropriate carrier to avoid drawing suspicion to the existence of a hidden message on the premise of the insensitivity of human sense organs and therefore the redundancy inherent in media data (data property redundancy).

Therefore, media with an oversized amount of redundant information are better suited to the carriers because the changes to the carrier thanks to the injection of the payload are imperceptible. The carriers commonly used include images[2-5], videoes[6-8], audioes[9,10], texts[11,12], two dimensional bar codes[13]. Thereinto, steganography in images, especially in natural images, is paramount popular and has been deeply studied.

However, the natural images themself exist as a form of noise, which is able to significantly affect the embedding capacity of the steganography system. To the authors' knowledge, meanwhile, no existing references is anxious about the source of the carrier images. and customarily, the carrier images will be download conveniently from internet by anyone, including the attacker. However, the standard natural images steganography often changed the inherent statistical characteristics the initial carrier images have, especially when the capacity of the data embedded is huge. Therefore, together with the event of the statistcal model of every kind of images, the protection of the natural images steganography has met serious challenge.

Steganography in fractal images will be considered much more secure[14]. Although the fractal images, as a form of non-linear graph, have very complex appearance, they can be easily generated on the premise of the mixture of the nonlinear dynamic system model and therefore the lighting tricks.

- *Author Arfat Aziz Bubere is currently pursuing masters in Information Tecchnology from University of Mumbai, India, PH-9773020605. E-mail: arfatbubere.ab@gmail.com*
- *Co-Author Ravindra Mhatre is currently Professor in University Of Mumbai, India, PH-9967719262.*

Concretely speaking, fractal images will be generated by iterative calculation of a given non-linear model with the initial parameters followed with the particular computer graphic algorithms. No very same fractal images will be generated without initial parameters, whether or not the non-linear model is open. Therefore, to the sender and receiver, the model of steganography system will be considered as a communication model with full side information when both the sender and receiver know the initial parameters, which can be transmitted as passwords in a very reliable signal channel.

While to the attacker, the model will be considered as a form of model without side information or with incomplete side information. In other words, the carrier information in a very fractal images steganography system is asymmetric to the receiver and therefore the attacker. it's different from the natural images steganography system which has the identical side information to the receiver and attacker.

In this paper, a replacement method of fractal images steganography supported Julia set is proposed. In contrast to the algorithm described in ref. 14, the embedding of the secrete information was simultaneous with, while not after, the generation of the fractal images because the secrete data themselves were thought to be the parameters necessary for the generation of fractal images. The structure of the steganography system in fractal images and a detail algorithm are going to be described in Section II and III, respectively. and therefore the experiment results are going to be shown and discussed in Section IV. Finally, some practical and significant conclusions are going to be drawn.

II. STRUCTURE OF STEGANOGRAPHY SYSTEM BASED ON FRACTAL IMAGES

According to the definition and characteristics of the fractal, we proposed a form of structure of steganography system supported fractal images. Fig. 1 shows the block diagram of the procedure of data embedding and extracting supported fractal images. a bit like cryptology, steganography technique also obeys Kerckhoff principle, that means a steganography system should be secure whether or not everything about the system, except the key, is public knowledge. In other words, the safety of steganography is depended on not the algorithm but the key.In our scheme,we took the initia

parameters because the key so the attacker can not generate original carrier image comparable to stegnographic image without the initial parameters, even when the nonlinear model and steganography algorithms is public knowledge. Therefore, just like the symmetric encryption system, the attacker can't detect whether the image contains secret information. As for the knowledge extracting, it's usually the inverse process of the knowledge embedding in traditional steganography system, which is known as the symmetrical mode. While in our scheme, fractal images are used as carriers, and therefore the receiver can generate original image with the key (the initial parameters).

Therefore, the extracting process is asymmetric with the embedding process, which greatly enhances the safety of the system.

III. STEGANOGRAPHY ALGORITHM supported JULIA SET FRACTAL IMAGES

A. Julia set fractal images

Fractal is that the set of some complex points (on the important or complex plane), which form a compact subset. A fractal often has the subsequent features: (1) it's a spectrum line at arbitrarily small scales; (2) it's too irregular to be easily described in traditional Euclidean geometric language; (3) it is self-similar (at least approximately or stochastically); (4) it has a Hausdorff dimension which is larger than its topological dimension (although this requirement isn't met by space-filling curves like the Hilbert curve); and (5) it has a simple and definition.

With the help of tricks, fractal images with visual beauty are often created on the idea of geometry. Plenty of fascinating images are often obtained when the parameters of the nonlinear dynamic system model changes during the generating of fractal images. Julia set is that the maximal set of points that gets mapped onto itself under the function $f(z)=z^m+c\,(m\in C,\ c\in C)$ and is sometimes created with the escape time algorithm.

For simplicity, during this study, we adopted quadratic polynomials of Julia set to make fractal images. The quadratic polynomials are often expressed as $F(Z)=Z^2+C$, where $Z=x+yi$, and $C=p+qi$.

B. Information embedding

The escape-time algorithm takes a clipping area of the complex plane and computes the orbit of every point during this area. Some orbits converges to some fixed limiting value, while some towards infinity as escape-time t increases. If the orbit jump around chaotically everywhere the boundary of some finite region as t increases, the boundary is termed a “Julia Set”.

In this study, we generated fractal images of Julia assail the basis of the escape time algorithm. The secrete information was simultaneously embedded to the photographs creating process. In other words, the embedding process is exactly the creating process, which may be described because the following steps.

Step1. Assume that the scale of fractal image is a×b. Given C=p+qi (initial parameter, saved because the embedded key) , the escape radius threshold R, and therefore the escape time threshold T. Set x_{min}=-1.5, y_{min}=-1.5, x_{max}=1.5, and y_{max}=1.5.

Let

$$\Delta x = (x_{max} - x_{min})/(a-1) \quad (1)$$

$$\Delta y = (y_{max} - y_{min})/(b-1) \quad (2)$$

Complete Step 2-4 for all points (n_x,n_y), where n_x=0,1,…,a-1, and n_y=0,1,…,b-1.

Step2.Given starting values $Z_0=x_0+y_0i$, where $x_0=x_{min}+n_x\times\Delta x$, and $y_0=y_{min}+n_y\times\Delta y$. Set t=0.

Step3. Set $x_{t+1} = x_t^2 - y_t^2 + p$, $y_{t+1} = 2x_t y_t + q$, and t=t+1.

Step 4. Set $r = x_t^2 + y_t^2$

If r>R and t<t, read sequently one bit from the secrete information. If the bit is 0, the pixel (n_x,n_y) is drawn in predefined foreground color. If the bit is 1, the pixel (n_x,n_y) is drawn in predefined background color. Then visit step 2.

If t=T, the pixel (n_x,n_y) is drawn in predefined background color. Then visit step 2.

If r<t, visit step 3.

As we will see from the above algorithm, the colour of each point of Julia set are going to be determined by the secrete information. Moreover, the prevailing probability of 0 or 1 in the secrete information is mostly about 50%, respectively, because the secrete information usually has been encrypted beforehand. Therefore, as a result, the colour of about half Julia Set points will changed from foreground color to background color. this is often why the generated fractal image is blurred and therefore the steganographic fractal image looks different with the image whithout secrete information. so as to solve this problem, we partition the escape time threshold T.

For example, the points of Julia set are considered as important points and not be embedded when t<1/2T and r>R . Embedding only occurred when t>1/2T and r>R.

C. Information extracting

The extracting algorithm is nearly the identical because the embedding algorithm. Complete the step 1 to 3 of the embedding algorithm, then calculate $r = x_t^2 + y_t^2$.

If r>R and t<t, get="" the colour of point (n_x,n_y) and compare with steganographic fractal image. If the colour is that the same, the secrete information is 0, while if the colour isn't the same, the secrete information is 1. If t=T, the colour of point (n_x,n_y) is ignored. Therefore, the essence of this algorithm is extracting the colour information of every point of Julia Set and compared with steganographic fractal image to extract the secret information.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

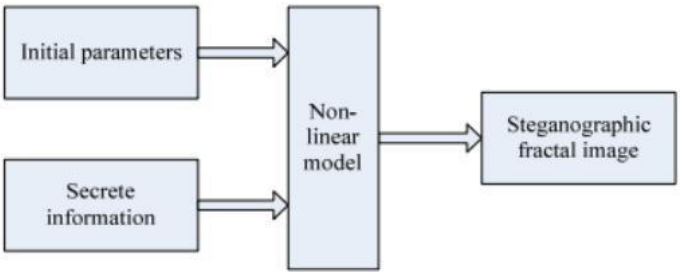
In this study, secrete data were embedded with the algorithm described previously. The initial parameter p'q were set as -0.194 and 0.656, respectively. The escape radius threshold R was set as 400, and therefore the escape time threshold T was set as 1000. Fig. 2 is that the fractal imagewithout steganographic data, Fig. 3 is that

International Journal of Scientific & Engineering Research, Volume 1, Issue 1, Feb 2020
ISSN 2229-5518

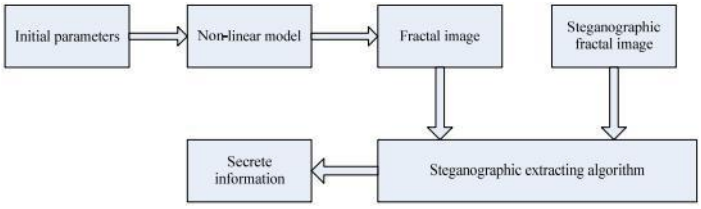
the steganographic fractal image that the escape time wasn't partitioned (embedding capacity is 4K bytes). Compare Fig. 2 with Fig. 3, we are able to find that the fractal image appears "blurring" after being embedded secrete information, which is consistent with the previous theoretical analysis. Fig. 4 is the steganographic fractal image that the escape time threshold T was partitioned (Embedding only occurred when 1000>t>100 and r>R, and embedding capacity is 1K bytes). Fig. 5 is that the steganographic fractal image that the escape time threshold T was partitioned (Embedding only occurred when 1000>t>120 and r>R, and embedding capacity is 855 bytes). it's shown in Fig. 4 and Fig. 5 that escape time threshold T partition can greatly enhance the visual quality of the steganographic fractal image, while the embedding capacity declined, which is incredibly easy to know.

Different from the normal steganography systems based on natural images, the embedder himself doesn't know what quite fractal image are going to be generated within the steganography system supported fractal images due to the non-linear characteristics of fractal. Therefore, the steganoanalyser cannot determine whether the image is embedded secrete information even when the steganographic fractal image like Fig. 3 is open. Moreover, we can adjust the parameters to provide more complex fractal images so more secrete information may be embedded on the premise of higher visual effect. On the other hand, the prevailing steganography analysis algorithms were presented against characteristics of natural images. The features of fractal images are ever changing due to the uncontrollability of the photographs created. Thus the prevailing steganalysis algorithms cannot detect secrete information embedded in fractal images.

V. RESULTS



(a) Information embedding model



(b) Information extracting model Figure 1. Block diagram of digital steganography system

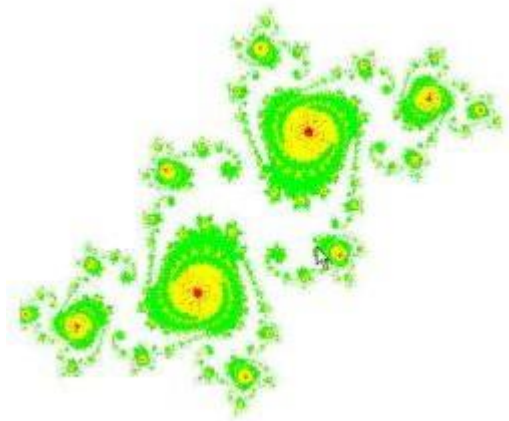


Figure 2. fractal image with no embedded information

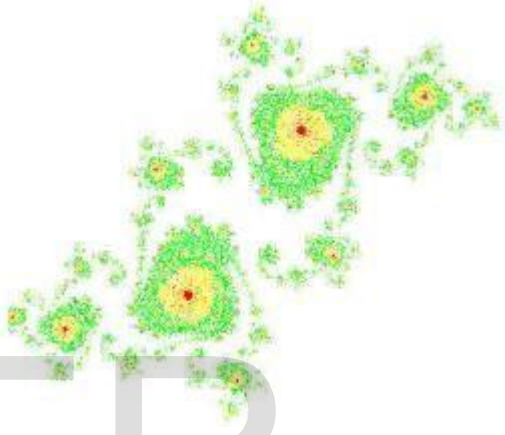


Figure 3. fractal image with embedded information

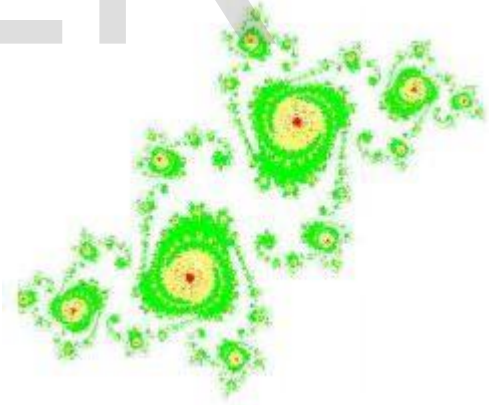


Figure 4. fractal image with embedded information (Embedding when 1000>t>100 and r>400)

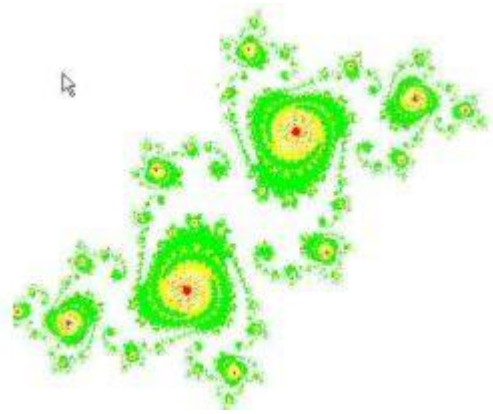


Figure 5. fractal image with embedded information (Embedding when 1000>t>120 and r>400)

VI. CONCLUSIONS

In this study, the fractal images were chosen because the carrier of knowledge hiding thanks to the benefit of generation and changeful characteristics of fractal images. Compared with traditional image-based information hiding methods, the sources of the fractal image carriers are richer, and the method can give better resistance against various steganalysis. However, the beauty, complexity and controllability of the fractal images is poor due to the randomness of generation. Therefore, within the future, we will focus on the way to generate more beautiful fractal image without affecting embedding capacity, including using new non-linear model, changing colour scheme so on.

VII .REFERENCES

[1] F.A.P. Petitcolas, R.J. Anderson, M.G.. Kuhn, "Information hiding - a survey," Proc. of the IEEE, vol. 87, pp. 1062-1078, 1999.

[2] M. Wu, E. Tang, B. Liu, "Data Hiding in Digital Bianry Images," Proc. of the IEEE Int. Conf. On Multimedia and Expositions, New York, 2000, pp. 393-396.

[3] M. Niimi, H. Noda, E . Kawaguchi, "High Capacity and Secure Digital Steganography to Palette-Based Images," Proc. of IEEE International Conference on Image Processing, Sept. 2002, pp.917-920.

[4] Neil F. Johnson, Sushil Jajodia," Steganograpy: Seeing the Unseen," IEEE Computer,pp. 26-34, February 1998.

[5] R.F. Chu, X.G. You, X.W. Kong, X.H. Ba,"A DCT-based Image Steganographic Method Resisting Statistical Attacks," Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing, 2004,pp. 953-956.

[6] F. Hartung, B. Girod , "Watermarking of Uncompressed and Compressed video,"Signal Processing, vol. 66, pp. 283-301, 1998.

[7] H. Noda, T. Furuta, M. Niimi, E. Kawaguchi , "Application of BPCS Steganography to Wavelet Compressed video," Proc. Of International Conference on Image Processing, 2004, pp. 2147-2150.

[8] G.G. Langeiaar, R.L. Lagendijk,J. Biemond, "Real-time Labeling Methods for MPEG Compressed Video," Proc. of the 18th Symposium on Information Theory,1997, pp. 25-32.

[9] Z.J.Wu, W.Yang, Y.X.Yang, "ABS-based Speech Information Hiding Approach," IEEE Electronics Letters,vol. 39, pp. 1617-1619, 2003.

[10] Kaliappan Gopalan, "Audio Steganography by Cepstrum Modification," Proc. of IEEE International Conferenc on Acoustics, Speech, and Signal Processing, 2005, pp. 481-484.

[11] Xin-xin Niu,Yi-xian Yang, " Research on the Algorithm of Text Steganography," Acta Electronica Sinica, vol. 31, pp. 402-405, 2003.

[12] Ji-jun Zhou, Zhu Yang Xin-xin Niu, Yi-xian Yang, "Research on the detecting algorithm of text document information hiding.," Journal of China Institute of Communications, vol. 25, pp. 97-101, 2004.

[13] Xia-mu Niu, Wen-jun Huang Di Wu, Hui Zhang, "Information Hiding Technique Based on 2D Barcode," Acta Scientiarum Naturalium Universitatis Sunyatseni, vol. 43, pp.21-25, 2004.

[14] Hui Lv, Huaxiong Zhang, Xiangjun Weng

[15] , "A Steganography Scheme Based Fractal Images," Journal of Harbin Institute of Technology,vol. 38, pp. 839-843, 2006.

[16] Huaxiong Zhang, Jie Hu, Gang Wang A Steganography Scheme Based on Fractal Images pp results