DSTA 2021 dyn-ta.com
16th INTERNATIONAL CONFERENCE
Dynamical Systems Theory and Applications
December 6-9, 2021, On-line

Fractal techniques associated with steganography

NIKOLAOS NTAOULAS[1], VASILEIOS DRAKOPOULOS[2*]

1. Department of Computer Science and Biomedical Informatics, University of Thessaly, 2–4 Papasiopoulou St., Lamia, Greece [0000-0002-7016-9974]
2. Department of Computer Science and Biomedical Informatics, University of Thessaly, 2–4 Papasiopoulou St., Lamia, Greece [0000-0002-6478-3943]

Abstract: Exploiting the properties of chaotic systems and fractals is a field of great interest and attracted a lot of attention in the last decades as far as steganography and cryptography are concerned. Their dynamic and sensitive properties lead to numerous applications and research gradually increasing through the years. The exploration of the field and the proposed applications is the main purpose of this work, through an effort to classify the main directions and techniques. The wide spread of networking and vast amount of data circulating everyday through internet reveal opportunities and dangers as far as security is concerned. The opportunity arising for steganography is obvious allowing to select various channels to transmit information hidden in a variety of multimedia files. The most frequently used files for steganography are images as there are billions transmitted every day and as they efficiently provide the properties required for hiding information. The main goals of the field, presenting the role fractals and chaos theory play, is robustness, tamper resistance, hiding capacity and perceptual transparency.

Keywords: Fractals, Steganography, Chaos, Information Hiding

1. Introduction

Privacy and Security is of high concern in general and of great importance in Information Systems. Cryptography and Steganography are the vital and fundamental methods in securing information in multiple ways (confidentiality, integrity, authentication, non-repudiation). Since the 5th century B.C. that Herodotus firstly annotates the use of wax tablets as a mean to conceal hidden messages many efforts has taken place to hide information in seemingly innocuous “vessels”. Nowadays, the wide spread of networking and vast amount of data circulating everyday through internet reveal opportunities and dangers as far as security is concerned. The opportunity arising for steganography is obvious allowing to select various channels to transmit information hidden in a variety of multimedia files. While classical cryptography is about concealing the content of messages, steganography is about concealing their existence (Anderson & Petitcolas, 1998). In digital era the hidden message is embedded in some data, normally a multimedia file which is referred to as cover and the result is referred to as stego-file. A secret key referred to as stego-key is employed for the embedding and the corresponding extraction process. Employing a cryptosystem before embedding has become familiar in steganography to enhance security. The main purpose of this work is to point out the techniques that are used in order to exploit fractals and chaos, the robustness and efficiency that is appeared as well as the security issues that arise and how these are handled.

2. Fractal techniques - Applications

The techniques used more in fractal-based steganography vastly rely on the generation of cover images. In (Zhang, Hu, Wang, & Zhang, 2011) the authors use the Julia sets to create images based

on the Escape Time Algorithm. (Thamizhchelvy & Geetha, 2014) use SHA-256 hash function for the text to be hidden before embedding in a fractal image produced with a stego-key as the initial state of the IFS (Iterated Function System) provided by a Fibonacci series initialized by a PRNG (Pseudo-Random Number Generator). Some techniques involve fractal-based compression as well. In (Davern & Scott, 1996), fractal-based image compression techniques identify parts of the image that are most suited for data hiding. (Chang, Chiang, & Hsiao, 2005) employ fractal-based compression to a hidden image and embed it using a PRNG for the DCT (Discrete Cosine Transform) embedding.

Chaotic maps are extensively used in cryptography exploiting their properties. Chaotic maps are found either as a method to encrypt data before embedding or, and mostly, as a source for randomizing the embedding process. In (Enayatifar, Mahmoudi, & Mirzaei, 2009) two logistic maps randomize the selection of the modified pixels in rows and columns, respectively. (Yu, Lifang and Zhao, Yao and Ni, Rongrong and Li, 2010) use the Adaptive LSB (Least Significant Bit) method shuffling the hidden data bits by a logistic map which parameters are produced by a GA (Genetic Algorithm) with PSNR (Peak signal-to-noise ratio) as the fitness function. (Singh & Siddiqui, 2012) proposed a DCT method, embedding in the middle band coefficients, using two sequences deriving from a logistic map to embed a logo image. In (Mishra, Ranjan Routray, & Kumar, 2012) the method uses modified Arnolds cat map to scramble the hidden image and employs LSB method achieving the best result for embedding data in one Bit Plane. (Parah, Ahad, Sheikh, & Bhat, 2017) scale up medical images to produce a cover for watermark and ERP (Electronic Patient Record) which are encrypted using a logistic map and an irritative exclusive-or implementation providing results for robustness of a method embedding in the second least significant bit of the produced cover image. (Gambhir & Mandal, 2020) experiment with the efficiency of multicore processing for an LSB method using logistic map for the encryption of data before and after embedding.

3. Results – Discussion

The most familiar methods take place in the spatial domain altering, substituting or matching the LSB providing highest capacity (up to 4 LSBs can be used in each pixel's color representation). Adaptive methods in the specific domain take advantages of the edge regions or in general Regions of Interest (ROI) which provide less perceivable stego-images. Other methods proposed are in the Transform domain, like DCT, DWT (Discrete Wavelet Transform) and so on, which offer higher robustness. PSNR is the main tool to measure the disruption of a cover image. The noise added to the cover image directly affects its capacity as more information adds more noise. The capacity in most of the cases is evaluated. Moreover, there are methods generating the cover image from scratch, a familiar technique in fractal-based steganography in which the receiver's keys include the process of the image generation. Thus, there is no need for obtaining the cover image, a technique also known as blind steganography. There is an obvious trade-off between capacity and robustness as well as the level of imperceptibility, making capacity and less perceivability valuable for steganography and robustness valuable for watermarking and fingerprinting. The lack of robust information about key space and the keys characteristics is a general problem. As proven, chaotic maps are extensively researched in steganography providing mainly the randomness needed either for encryption of the secret message or the selection of the pixels and coefficients corresponding to the spatial and the transform domain methods. Logistic map is the most studied map useful in producing random sequences and Arnold's cat map is proposed secondly as a way to diffuse the pixels of a secret image taking advantage of the irritation which leads back to the initial image. Recently, research is enriched with more details of their experiments, entropy of colours, homogeneity, contrast etc. added up to the well-known PSNR value as a metric for comparing the cover image with the stego-image. Spatial domain methods are much more prone to attacks, but they trade off the higher capacity they provide in comparison to the transform domain methods.

References

Anderson, R. J., & Petitcolas, F. A. P. (1998). On the limits of steganography. *IEEE Journal on Selected Areas in Communications*, *16*(4), 474–481. https://doi.org/10.1109/49.668971

Chang, C. C., Chiang, C. L., & Hsiao, J. Y. (2005). A DCT-domain system for hiding fractal compressed images. *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, *2*, 83–86. https://doi.org/10.1109/AINA.2005.17

Davern, P., & Scott, M. (1996). Fractal based image steganography. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *1174*, 279–294. https://doi.org/10.1007/3-540-61996-8_47

Enayatifar, R., Mahmoudi, F., & Mirzaei, K. (2009). Using the chaotic map in image steganography. *Proceedings - 2009 International Conference on Information Management and Engineering, ICIME 2009*, 491–495. https://doi.org/10.1109/ICIME.2009.155

Gambhir, G., & Mandal, J. K. (2020). Multicore implementation and performance analysis of a chaos based LSB steganography technique. *Microsystem Technologies*. https://doi.org/10.1007/s00542-020-04762-4

Mishra, M., Ranjan Routray, A., & Kumar, S. (2012). High Security Image Steganography with Modified Arnold's Cat Map. *International Journal of Computer Applications*, *37*(9), 16–20. https://doi.org/10.5120/4636-6685

Parah, S. A., Ahad, F., Sheikh, J. A., & Bhat, G. M. (2017). Hiding clinical information in medical images: A new high capacity and reversible data hiding technique. *Journal of Biomedical Informatics*, *66*, 214–230. https://doi.org/10.1016/j.jbi.2017.01.006

Singh, S., & Siddiqui, T. J. (2012). A Security Enhanced Robust Steganography Algorithm for Data Hiding. *International Journal of Computer Science Issues*, *9*(3), 131–139. Retrieved from www.IJCSI.org

Thamizhchelvy, K., & Geetha, G. (2014). Data hiding technique with fractal image generation method using chaos theory and watermarking. *Indian Journal of Science and Technology*, *7*(9), 1271–1278.

Yu, Lifang and Zhao, Yao and Ni, Rongrong and Li, T. (2010). Improved Adaptive LSB Steganography Based on Chaos and Genetic Algorithm. *EURASIP Journal on Advances in Signal Processing*, *2010*, 1–6. https://doi.org/10.1155/2010

Zhang, H., Hu, J., Wang, G., & Zhang, Y. (2011). A steganography scheme based on fractal images. *Proceedings - 2nd International Conference on Networking and Distributed Computing, ICNDC 2011*, 28–31. https://doi.org/10.1109/ICNDC.2011.13