Image Steganography Scheme using Chaos and Fractals with the Wavelet Transform

Yue Wu and Joseph P. Noonan

***Abstract*—This paper introduces a novel image steganographic method for embedding secret image information into digital images. The proposed algorithm uses a fractal image as the cover image, takes a random-like sequence generated by a chaotic map as the reference for embedded positions, and employs a wavelet transform to realize the embedding procedure. The fractal cover image that can be parametrically generated implies a cover image could be unique in the world. The chaotic logistic map guarantees that the sequence of embedding positions is completely unknown for an adversary and the embedding procedure is almost random-like. The wavelet transform ensures the secret information is only embedded within edges with the least visual distortion. The proposed scheme is tested over different cover images and secret images and simulations results demonstrate its effectiveness and robustness.**

***Index Terms*—Steganography, chaos, fractal, logistic map, wavelet transform.**

I. Introduction

The term steganography [1] originates from the Greek word *steganos* meaning “covered or protected” and *graphein* meaning “to write”. Nowadays, it often refers to the science of “invisible” communication.

Generally speaking, steganography can be classified into two categories: image watermarking and image data hiding. Image watermarking techniques are aimed to provide copyright protection [2-5] and authentication [6, 7]. Image data hiding techniques is aim to camouflage a secret message within a carrier message such that the secret message can be sent without making any notice. This study focuses on data hiding.

There are two kinds of image steganography for image data hiding: spatial-domain based and transform-domain based methods. Spatial-domain based methods embed messages in the intensity of pixels of images directly [8, 9]. Among them, the least significant bit (LSB) method is the most well-known [10-12]. This method embeds the fixed-length secret bits in the same fixed-length LSBs of pixels. This technique is simple and fast but it may cause noticeable distortion when the number of embedded bits for each pixel exceeds three [12]. While transform-domain based methods first transform a cover image into a new domain and then messages are embedded in as the transform coefficients [13, 14].

The proposed method is one of the transform-domain based steganographic techniques. Unlike those related works [15, 16] focusing on hiding the secret message with coding schemes, we directly used the wavelet coefficients to embed the message. In addition, we construct a series of cover images via fractal iterative functions, which guarantee that 1) a cover image can easily regenerated with a given set of parameters; 2) a cover image is almost unique and novel; and 3) a cover image is inaccessible for an adversary without knowing the correct set of parameters. Moreover, based on the fact of the image has different wavelet coefficients when using different wavelets. We use the wavelet function as a part of our shared key to further enhance the security level.

The remainder of the paper is organized as follows: in Section II, backgrounds related to the proposed method are reviewed; in Section III, the proposed steganographic technique is discussed in details; in Section IV, computer simulation results and related analysis are presented; In Section V, we conclude this paper and make discussions on the future work.

II. Backgrounds

Simply speaking, the proposed algorithm uses a fractal image as the cover image, takes a random-like sequence generated by a chaotic map as the reference for embedded positions, and employs a wavelet transform to realize the embedding procedure. More details about the proposed algorithm are discussed in Section III. In the rest of the section, we will briefly review the wavelet transform, the chaotic map and the fractal image.

A. Wavelet Transforms

A wavelet transform is used to divide a continuous-time/ discrete time function into wavelets. Unlike the Fourier transform, which only construct a frequency representation of a signal, the wavelet transform is able to construct a time-frequency representation of a signal. Therefore, the wavelet transform offers very good time and frequency localization.

Mathematically, the Continuous Wavelet Transform (CWT) of a continuous, square-integrable function $f(x)$ at a certain scale $s>0$ and a translation value $\tau\in\Re$ can be defined as Eq. (1), where $\psi_{s,\tau}(x)$ is defined in Eq. (2) [17]. Here $\psi(x)$ is called the *mother wavelet* and $\psi_{s,\tau}(x)$ is called a *daughter wavelet* at scale s and translation τ of $\psi(x)$. To recover the original function $f(x)$, inverse wavelet transform is defined in Eq. (3), where C_ψ is defined in Eq. (4)

Manuscript received April 2, 2012; revised May 9, 2012.

Y. Wu is with the Department of Electrical and Computer Engineering, Tufts University, MA 02155, USA (e-mail: ywu03@ece.tufts.edu).

J. P. Noonan is with the the Department of Electrical and Computer Engineering, Tufts University, MA 02155, (e-mail: jnoonan@eecs.tufts.edu).

and $\Psi(\mu)$ is the Fourier transform of $\psi(x)$. Eqs. (1) to (4) define a reversible transformation as long as the so-callled admissibility criterion $C_\psi < \infty$ is satisfied [18]. In 1989 Fast Wavelet Transform (FWT) is developed and provided a good way of calculating wavelet transforms of a given signal.

$$W_\psi(s,\tau) = \int f(x)\psi_{s,\tau}(x)dx \quad (1)$$

$$\psi_{s,\tau}(x) = \frac{1}{\sqrt{s}}\psi(\frac{x-\tau}{s}) \quad (2)$$

$$f(x) = \frac{1}{C_\psi}\int_0^\infty \int_{-\infty}^\infty W_\psi(s,\tau)\frac{\psi_{s,\tau}(x)}{s^2}d\tau ds \quad (3)$$

$$C_\psi = \int \frac{|\Psi(\mu)|^2}{|\mu|}d\mu \quad (4)$$

One dimensional wavelet transforms can be easily extended to two dimensional cases like images. In two dimensions, a two-dimensional scaling function $\phi(x,y)$ and three two-dimensional wavelets, $\psi^H(x,y), \psi^V(x,y)$ and $\psi^D(x,y)$ are required for the horizontal, vertical and diagonal directions respectively. Each of above four functions is the product of two one-dimensional functions as Eqs. (5) – (8) show, where $\phi(d)$ is the one dimensional scaling function along direction d ; $\psi(d)$ is the one dimensional wavelet mother function along direction d . In this paper, various two dimensional wavelet functions are used to decompose images.

$$\phi(x,y) = \phi(x)\phi(y) \quad (5)$$

$$\psi^H(x,y) = \psi(x)\phi(y) \quad (6)$$

$$\psi^V(x,y) = \phi(x)\psi(y) \quad (7)$$

$$\psi^D(x,y) = \psi(x)\psi(y) \quad (8)$$

B. *Chaotic Maps*

Generally speaking, the chaotic map refers to any map that exhibits some sort of chaotic behavior: any slight change in the initial conditions yields widely diverged outcomes which makes impossible for long-term prediction.

Although chaotic behavior can be observed in many dynamic systems, we focus on the one dimensional logistic map in this paper. Mathematically, a logistic map can be defined as an iterative function in Eq. (9), where r is the parameter and x_0 is used as the initial value.

$$x_{n+1} = rx_n(1-x_n) \quad (9)$$

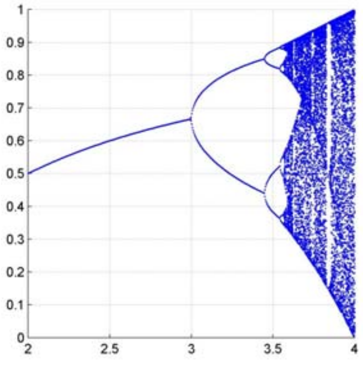

Fig. 1. The chaotic logistic map.

Normally, parameter r is set to $(3.58,4)$ and x_0 is set to $(0,1)$ for keeping the chaotic behavior. In Fig. 1, the x coordinate value represents the parameter value r and the y coordinate value represents the generated x sequences. It is clear to see that for $r \in (3.6,4)$, the map generates random-like x sequences. It is worthwhile to note that sequences with initial value falling in the region around $r = 3.83$ are periodic. In order to avoid trapping the sequence into oscillation, we simply use $r \in (3.9,4)$ in this paper.

The purpose of using the logistic map in the paper is to generate a random-like but deterministic sequence for embedded positions. Therefore, the logistic map can be substituted by any chaotic map.

C. *Fractal Images*

The term fractal was coined by Benoit Mandelbrot in 1975 and was derived from the Latin *fractus* meaning “broken” or “fractured”. Mathematically, a fractal is based on an equation undergoing iterations, which is a form of recursive feedbacks. A fractal usually has the following characteristics as described in [19]:

1) It has a fine structure at any arbitrarily small scale.
2) It is too irregular to be easily described in traditional Euclidean geometric language.
3) It is self-similar or at least approximately similar.
4) It has a simple and recursive definition.
5) Its Hausdorff dimension is higher than its topological dimension.

In this paper, we use the fractal images generated by ‘Ultra Fractal’ [20] as cover images, each of which is uniquely defined by a set of fractal parameters such as type, formula, scale, location, color space etc. In other words, the fractal image can be perfectly restored as long as this set of parameters is known. In ‘Ultra Fractal’ this set of parameters can be saved as a particular file, which can be transported very easily. Therefore, the cover image can be perfectly restored.

III. The Steganographic Algorithm

The proposed steganographic algorithm relies on the wavelet transform and embeds secret data as the wavelet coefficients in a cover image. Here, we assume a cover image is a RGB color image. The flowchart of the proposed steganographic algorithm is sketched in Fig 2. The details of each stage will be discussed in the rest of this section.

A. *Stage I: Transforming Image in Wavelet Domain*

This stage is the start of the steganography. The color cover image C is decomposed in the YCbCr color space and only the Cb component C_{Cb} is used for future processing. This choice of Cb component is heuristic and is selected based on our experiment results. This choice is supposed to achieve a higher covariance between the stego image S and the cover image C than using Cr or Y component.

Later both the C_{Cb} and the secret image I are transformed using wavelet W_1 and W_2 respectively, and become $W_1(C_{Cb})$

and $W_2(I)$. Here W_1 and W_2 are determined by the key and they may or may not be necessarily the same. One benefit of this design is to achieve a larger key space. Unless the correct wavelet mother function W_1 is used, one cannot extract the exact embedded secret information from a cover image; unless the correct wavelet mother function W_2 is used, one cannot restore the secret information from extracted secret information in the spatial domain.

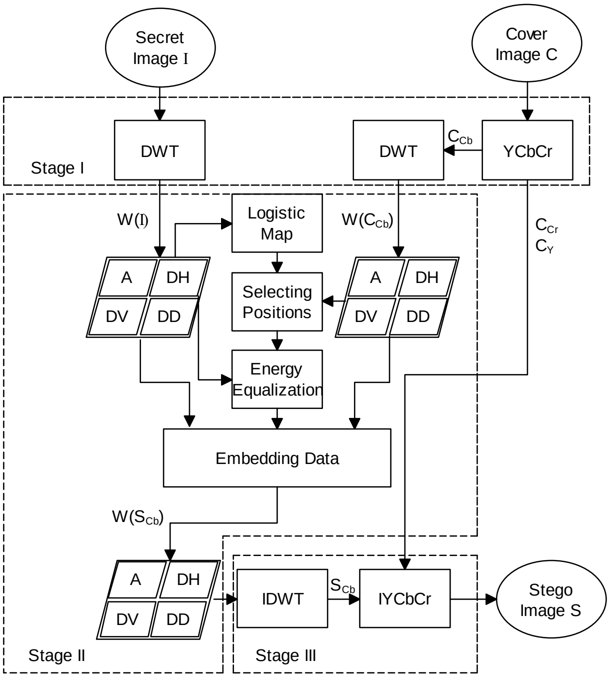

Fig. 2. The flowchart of the proposed steganographic scheme.

B. Stage II: Secret Data Embedding

This stage is the core of the steganography. It embeds the transformed secret image $W_2(I)$ in the transformed cover image $W_1(C_{Cb})$.

First, the initial value x_0 and the parameter value r of the logistic map in Eq. (9) are determined by the key. Based on the number of coefficients in $W_2(I)$, the logistic map generates an equal length chaotic sequence *Seq*. However, this sequence *Seq* has to be quantized before used for extracting wavelet coefficients in $W_1(C_{Cb})$. The number of quantization scales N is calculated via Eq. (10), where $\#(.)$ computes the number of elements and dt rounds the number towards to zero. Then *Seq* is quantized with respect to the bin numbers of the N equal-length bins in $(0,1)$, namely

$$B_1=\left(0,\frac{1}{N}\right],\cdots,B_k=\left(\frac{k-1}{N},\frac{k}{N}\right],\cdots,B_N=\left(\frac{N-1}{N},1\right)$$

Consequently, *Seq* is translated to a random-like sequence Seq_N composed of only numbers from 1 to N.

However Seq_N is still not the sequence which can be used to extract wavelet coefficient in $W_1(C_{Cb})$. Seq_N is calculated for partial sum and the Seq_c is obtained according to Eq. (11). Seq_c is used to extract wavelet coefficients in $W_1(C_{Cb})$. It is worthwhile to note that $W_1(C_{Cb})$ is composed of four regions (see Fig. 2), namely approximation region A (passed by the low-pass filter along y and followed by the low-pass filter along x), horizontal-details region *DH*(passed by the low-pass filter along y and followed by the high-pass filter along x), vertical-details region *VH*(passed by the high-pass filter along y and followed by the low-pass filter along x), and diagonal-details *DD* (passed by the high-pass filter along y and followed by the high-pass filter along x). We keep region A but choose to substitute coefficients in *DH*, *DV* and *DD* by the wavelet coefficients of $W_2(I)$. This is the reason why Eq. (10) contains a factor of $3/4$. In fact, the region A can be considered as the DC component of the image C_{Cb}. Any change in this DC component may lead to big changes in the future. However, *DH*, *DV* and *DD* are more or less about the edge strength of C_{Cb}. Fractal cover images normally have a large number of edges and rely on the DC component of the image to have the fractal-like patterns.

$$N=\left\lfloor\frac{3\times\#(C_{Cb})}{4\times\#(W_2(I))}\right\rfloor \tag{10}$$

$$Seq_c(k)=\sum_{i=1}^{k}Seq_N(k) \tag{11}$$

The selected coefficients in $W_1(C_{Cb})$ are uniquely determined by Seq_c and we named the set of the chosen coefficients as P. Eq. (12) is used as the ratio of energy in set X to that in set Y, where $E(.)$ represents the energy function.

$$R(X,Y)=\frac{E(X)}{E(Y)}=\frac{\sum x^2}{\sum y^2} \tag{12}$$

We then compute $L=R(P,W_2(I))$ and lift wavelet coefficients correspondingly, Consequently, the lifted energy $LE(W_2(I))$ approximately match the energy of the original $E(P)$. Finally, we call these modified wavelet coefficients $W_1(S_{Cb})$.

C. Stage III: Transforming Image Back to Spatial Domain

Parallel to the Stage I, the main task of the Stage III is to inverse transform everything in the wavelet domain to the spatial domain.

$W_1(S_{Cb})$ is inverse wavelet transformed to the spatial domain and becomes the image S_{Cb}. The S_{Cb} is used to replace the original Cb component C_{Cb} for the color cover image C.

Eventually, the component set $\{C_Y,S_{Cb},C_{Cr}\}$ is converted from the YCbCr color space to the RGB color space.

IV. Simulation Results And Discussion

Our computer simulation is run in the MATLAB R2009a environment under Window XP operation system with 3GB memory and Core 2 Quad 2.6GHz CPU.

The key we used in the simulation has the format of $\{x_0,r,width,height,db_C\#,db_I\#\}$, where x_0 and r are used in the logistic map for generating the embedding/ extracting positions; width and height are used to reform the rebuilt secret image; db_C # and db_I # refer the used Daubechies wavelets for the cover/stego image C/S and the secret image I respectively.

Fig. 3 shows the used cover images for simulation. They are all generated from Ultra Fractal [20]. The image can be saved as a parameter file and thus can be easily transported and perfectly restored in other computers installed Ultra Fractal. Here all cover images are at size of 640×480 .

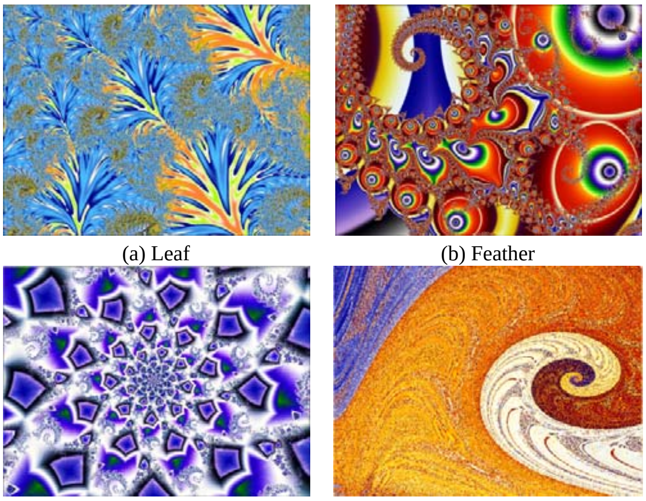
(a) Leaf
(b) Feather
(c) Fragment
(d) Storm

Fig. 3. The cover image generated by Ultral Fractal.

Fig. 4 shows the test secret images in the simulation. The image of 'Tufts Logo' is of size of 128×128 while the image of 'cameraman' is at size of 256×256 .

(a) Tufts Logo
(b) Cameraman

Fig. 4. The test images used in the simulation.

We test all four cover images and they produce more or less the similar results. And thus only the results of fractal cover 'Leaf' are shown in Fig. 5 as an example. Here, we use 'Haar wavelet' for both the cover image and the secret image. From the point view of human visual inspection, the secret image and the cover image are very close to each other. The differences of two images concentrate on the edge pixels, which are very hard to be notice without comparisons. A strong benefit of using this type of fractal images is to largely reduce the risk of known cover image, because all used cover images are synthesized by a set of fractal parameters. If a cover image is not accessible by any unauthorized user, it is then very difficult to differentiate a true fractal image and a fractal image with secret information. Consequently, the security of secret information in the stego image is largely enhanced.

$$RMSE(C,S) = \sqrt{\frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(C(i,j) - S(I,j)\right)^2} \tag{13}$$

$$PSNR = 20\log_{10}\left(\frac{MAX_c}{RMSE}\right) \tag{14}$$

In signal processing, the peaks of the signal-to-noise ratio (PSNR) and the root-mean-square error (RMSE) of the embedding results are two common measurements for evaluating the quality of reconstructed signal. RMSE is defined by the Eq. (13), where C and S represents the cover image and the stego image respectively; m and n refer to the width and height of the image. PSNR can be defined based on RMSE as Eq. (14) shows.

TABLE I: PSNR AND RMSE OF STEGO IMAGES

	Tufts Logo		**Cameraman**	
Cover Image	***PSNR***	***RMSE***	***PSNR***	***RMSE***
Leaf	42.2914	1.9587	35.8950	4.0906
Feather	44.6110	1.4997	38.2453	3.1209
Fragment	43.8974	1.6281	37.4657	3.4139
Storm	41.3414	2.1851	35.5896	4.2370

The PSNR and the RMSE test on the stego image using the proposed method are shown in Table I. It is worthwhile to note that what we exactly calculated is RMSE (C_{Cb}, S_{Cb}) . From Table I, it is easy to see that the cover image with a larger portion of homogenous regions produces a lower RMSE and thus a higher PSNR. This is because no wavelet coefficient has been replaced in the approximation region A , which can be considered as the DC component the image.

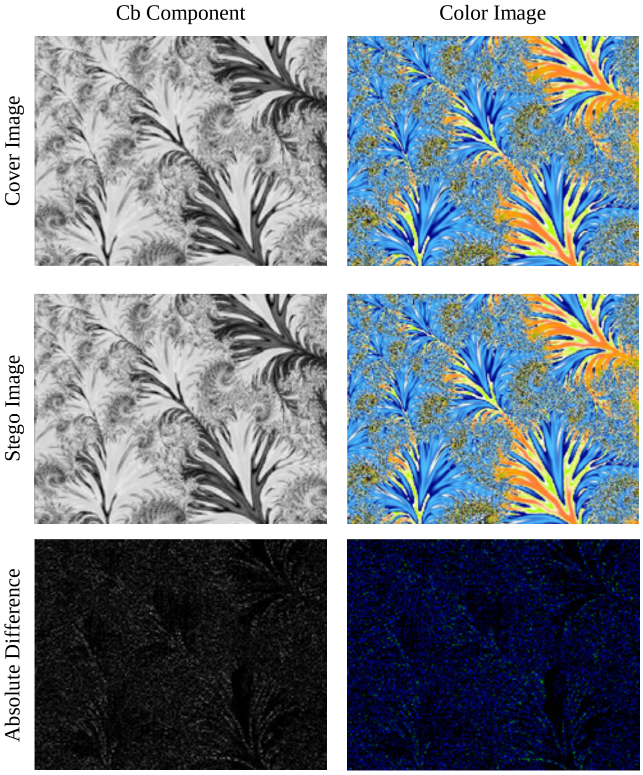

Fig. 5. The comparison of the cover image and the secret image.

We also investigated the influence of using different types of wavelet functions for both the cover image and the secret image. These results are shown in Fig. 6, axis indicates the used wavelet function and '*db*' refers to the Daubechies wavelet family. We tested the Daubechies wavelets (built-in functions in MATLAB) on both the cover image C and the secret image I . x

Recall we used W_1 for the image C and W_2 for the image I . Here 'tree' image is used as the cover image and 'tufts logo' is used as the secret image. The red solid curve is obtained by fixing $W_2 = db1$ while keep changing W_1 ; the blue dotted curve is obtained by fixing $W_1 = db1$ while keep changing W_2. We used the covariance of the cover image C and the stego image S to measure the quality, namely a high covariance value implies a better quality. Generally speaking, the proposed method works well regardless to the selected wavelet. However, different wavelets do produce different performances and a periodic-like curve is observed when changing the wavelet function for W_1. The reason behind this phenomenon is still unknown.

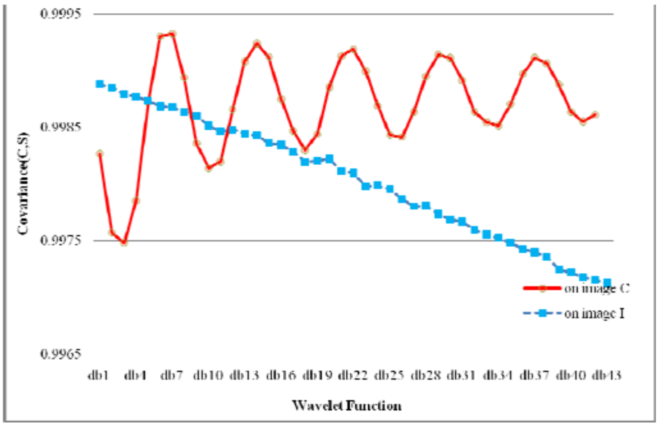

Fig. 6. The influence of using different wavelet function.

V. Conclusions

A new steganographic method based on wavelet transforms and fractal images are proposed. This new method is able to embed the secret image into a fractal cover image without producing noticeable changes. As long as the user has the correct key, the secret image can be extracted from the stego image without knowing the cover image. Although theoretically the attacker is able to sense the positions of the secret image information by comparing the stego image and the cover image, it is very safe for the proposed method. Because the cover image itself is considered to be secure for it is synthesized and can be uniquely expressed as a set of fractal parameters. In other words, the only way for an attacker to obtain the cover image is to use the exactly set of fractal parameters and generate the cover image.

Moreover, the wavelets used to transform the cover image and the secret image provide another level of security. Even in the worst case, the attacker cracked the cover image and knew the secret image positions, but the secret image cannot be decrypted without knowing the used wavelets. Furthermore, since wavelet is a big family of functions, customized wavelets can also be used. One can easily build up a look up table of wavelets and share this table with his/her communicator. If that so, even the brute force attack may fail in finding the correct wavelet function. In future, we will investigate the periodic-like curve in Fig. 6 and try to find out a best wavelet for our scheme if it is possible.

References

[1] D. Kahn, *The Codebreakers: the Story of Secret Writing*: Scribner Book Company, 1996.

[2] L. Zhe-Ming, X. Dian-Guo, and S. Sheng-He, "Multipurpose image watermarking algorithm based on multistage vector quantization," *Image Processing, IEEE Transactions on,* vol. 14, pp. 822-831, 2005.

[3] L. Ghouti, A. Bouridane, M. K. Ibrahim, and S. Boussakta, "Digital image watermarking using balanced multiwavelets," *Signal Processing, IEEE Transactions on,* vol. 54, pp. 1519-1536, 2006.

[4] C. C. Lai and C. C. Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition," *Instrumentation and Measurement, IEEE Transactions on,* vol. PP, pp. 1-3.

[5] C. Bo and S. Hong, "A new robust-fragile double image watermarking algorithm," in *Multimedia and Ubiquitous Engineering, 2009. MUE '09. Third International Conference on*, 2009, pp. 153-157.

[6] L. Chun-Shien and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *Image Processing, IEEE Transactions on,* vol. 10, pp. 1579-1592, 2001.

[7] L. Yao-Chung, D. Varodayan, and B. Girod, "Image authentication based on distributed source coding," in *Image Processing, 2007. ICIP 2007. IEEE International Conference on*, 2007, pp. III - 5-III - 8.

[8] W. Hong, T.-S. Chen, and C.-W. Shiu, "Lossless steganography for ambtc-compressed images," in *Image and Signal Processing, 2008. CISP '08. Congress on*, 2008, pp. 13-17.

[9] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters,* vol. 24, pp. 1613-1626, 2003.

[10] L. Shao-Hui, C. Tian-Hang, Y. Hong-Xun, and G. Wen, "A variable depth LSB data hiding technique in images," in *Machine Learning and Cybernetics, 2004. Proceedings of 2004 International Conference on,* 2004, pp. 3990-3994 vol.7.

[11] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal,* vol. 35, pp. 313-336, 1996.

[12] C.-C. Chang, C.-Y. Lin, and Y.-Z. Wang, "New image steganographic methods using run-length approach," *Information Sciences,* vol. 176, pp. 3393-3408, 2006.

[13] N. Kafri and H. Y. Suleiman, "Bit-4 of frequency domain-DCT steganography technique," in *Networked Digital Technologies, 2009. NDT '09. First International Conference on*, 2009, pp. 286-291.

[14] V. K. Munirajan, E. Cole, and S. Ring, "Transform domain steganography detection using fuzzy inference systems," in *Multimedia Software Engineering, 2004. Proceedings. IEEE Sixth International Symposium on,* 2004, pp. 286-291.

[15] L. Zhang, "Wavelet domain steganography for JPEG2000," in *Communications, Circuits and Systems Proceedings, 2006 International Conference on*, 2006, pp. 40-43.

[16] J. Spaulding, H. Noda, M. N. Shirazi, and E. Kawaguchi, "BPCS steganography using EZW lossy compressed images," *Pattern Recognition Letters,* vol. 23, pp. 1579-1587, 2002.

[17] R. González and R. Woods, "Digital image processing. 2008," Prentice Hall.

[18] A. Grossmann and J. Morlet, "Decomposition of hardy functions into square integrable wavelets of constant shape," *SIAM Journal on Mathematical Analysis,* vol. 15, pp. 723-736, 1984.

[19] H. Peitgen, H. Jürgens, and D. Saupe, *Chaos and Fractals: New Frontiers of Science*: Springer Verlag, 2004.

[20] F. Slijkerman, *Ultra Fractal* 5, 2010.