Stirmark Attack Resistant Fractal Transform-based Information Hiding

Yun Q. Shi, Zhicheng Ni and Nirwan Ansari
Department of Electrical and Computer Engineering
New Jersey Institute of Technology
Newark, NJ 07102, USA
shi@njit.edu, zn2@njit.edu, ang@njit.edu

Abstract

A recently developed fractal transform-based digital image information hiding technique has been further enhanced to resist the well-known StirMark attack. It is semi-blind in that it does not need original images in retrieving embedded information. It has been shown theoretically that the technique is robust against certain geometrical attacks, specifically, translation, scaling and small angle (less than 5 degree) rotation. More detailed test results by StirMark attack are reported in this paper. These results have demonstrated that the technique can resist most of the default StirMark attack functions, including the StirMark randomization and bending, which is a combination of several geometrical attacks followed by other manipulations, and has defeated most of the existing information hiding techniques.

1. Introduction

Information bit hiding has found wide application ranging from copyright protection to anonymous communications. Imperceptibility and robustness of hidden information bits are two major concerns among other requirements. They are known to conflict with each other.

With respect to information embedding, there are two categories of marking methods. One is in the spatial domain and the other is in the transform domain (such as DCT transform and Wavelet transform). There are also two different approaches for information retrieval. One requires the original image to recover the watermark. The other can recover the watermark without the original image. The former is referred to as non-blind, while the latter semi-blind or blind depending on whether the watermark signal is required. If only the embedded mark is needed in retrieval, we call the method semi-blind. This paper deals with still images. The method presented is semi-blind and uses fractal transform.

While watermarking is becoming an intensive research subject in recent years, so is its "rival:" attacking. At the early stage, only normal signal processing procedures and noise corruption were considered for attacking. Afterwards malicious attacks such as collusion and ambiguity attack were included. Recently, geometric attack is the focus of attention. In particular, StirMark has been developed as a benchmark for robustness test purpose [1]. Although some well-designed marking algorithms are able to resist some geometrical attack, it appears that, as a combination of random geometrical attacks together with some other manipulations, the StirMark attack has defeated most of the existing marking algorithms. As a result, great efforts have been devoted to enhancing the robustness of marking algorithms. It is believed that it is this type of interaction between marking and attacking that has advanced and will continue to advance information hiding techniques.

In this paper, we present further improvement of a newly developed digital image information bit hiding technique using fractal transform [2], and its performance in resisting the StirMark attack. With the exception of rotation with an angle larger than 5 degree, cropping 50 and larger, and scale of 2, the proposed technique can survive the default StirMark attack, and almost error-freely recover all embedded information. In particular, it can successfully resist the StriMark randomization and bending, which has been reported to be able to defeat most of the existing information hiding techniques [1]. For instance, the robust blind marking method [3] can successfully resist many testing functions in the default StirMark attacks, but it failed almost completely in passing the StirMark randomization and bending.

Details of the fractal transform based technique is not presented in this paper (Readers are referred to [2]). The basic idea is to relate embedded information bits with the fractal transform coefficients. The latter in turn corresponds to a pattern image. Therefore, by embedding the pattern image into a still image, one can embed the information bits into the image. The paper is organized as follows. Section 2 presents the improvement of the algorithm. Detailed StirMark test results along with the discussion are presented in Section 3.

2. The Improved Algorithm

Compared with [2], some structural modification has been made when inserting and detecting pattern image. That is, the block image, which is used in embedding and extracting the pattern image, has been changed to the

following structure. That is, the distribution of 1 and 0 becomes alternative blocks of 2x2. Compared with the blocks of 1x1 used in [2], this structure makes the algorithm more robust against noise, hence achieving better performance.

1	1	0	0	1	1	…	…
1	1	0	0	1	1	…	…
0	0	1	1	0	0	…	…
0	0	1	1	0	0	…	…
1	1	0	0	1	1	…	…
1	1	0	0	1	1	…	…
…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…

Figure 1: Block Image

3. Experimental Results and Discussion

We have applied the default StirMark attack to evaluate our fractal technique. The test results with Lena image are listed in Table 1, from which some observations are made.

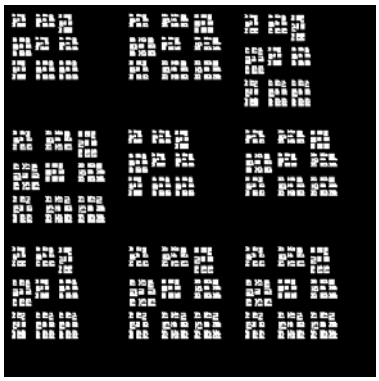

Figure 2. Pattern image (18 bits)

Figure 3: Pattern image recovered before attack

(a) For most of the default StirMark functions, the proposed technique can error-freely recover hidden information bits for both cases of embedding 18 bits and 64 bits, respectively. The bit correct rate for the former case is slightly better than that for the latter. This can be explained with pattern images. The higher the embedded bits, the more detailed the pattern images, and hence the self-similarity measurement becomes more difficult. The pattern image, and recovered pattern images before and after the attack (18 bits) are shown in Figures 2, 3, and 4, respectively.

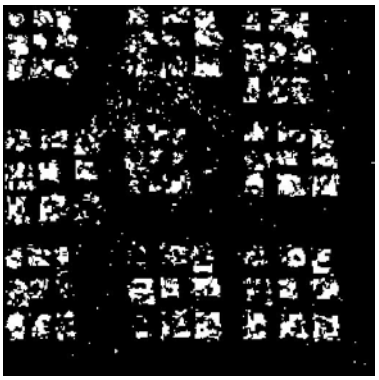

Figure 4: Pattern image recovered after StirMark randomization and bending

(b) According to [1, 3], the StirMark randomization and bending attack has defeated all the existing marking schemes. Therefore, the robustness achieved by the proposed technique against the Stirmark randomization and bending attack seems promising. From Figures 3 and 4, it is seen obviously that the randomization-and-bending attack does not significantly change the similarity measure between these two pattern images. In addition, the error-tolerance adopted in [2] associated with fractal coefficients also contributes to the robustness enhancement.

(c) It is noted that all the embedded information bits can be correctly recovered after a rotation by 5 degree. This performance is rather good. However, as analyzed [2], the bit error rate (BER) will not be zero for rotation with an angle larger than 5 degree.

(d) The algorithm fails for large cropping and scaling, JPEG factor below 15, and some parameters in ratio aspect variation and scaling. Further improvement is being investigated.

4. References

[1] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Attacks on copyright marking systems," *Second Workshop on Information Hiding*, Portland, OR, USA, April 1998.

[2] Z. Ni, E. Sung and Y. Q. Shi, "Enhancing robustness of digital watermarking against geometric attack based on fractal transform," *IEEE International Conference on Multimedia and Expo*, New York, July 2000.

[3] F. Alturki and R. Mersereau, "Robust oblivious digital watermarking using image transform phase modulation," *IEEE International Conference on Image Processing*, Vancouver, CA, October 2000.

Acknowledgement

This work is supported in part by the New Jersey Commission of Science and Technology via NJCMR, and New Jersey Commission of High Education via NJ-ITOWER.

Table 1. StirMark 3.1 Test Results (Lena)

StirMark functions	Correct bit rate % (18 bits embedded) PSNR 34.57 dB	Correct bit rate % (64 bits embedded) PSNR 34.05 dB
base_1_row_1_col_removed	100	100
base_1_row_5_col_removed	100	100
base_5_row_1_col_removed	100	100
base_17_row_5_col_removed	100	100
base_5_row_17_col_removed	100	100
base_2x2_median_filter	30	30
base_3x3_median_filter	100	70
base_4x4_median_filter	100	90
base_cropping_1	100	100
base_cropping_2	100	100
base_cropping_5	100	100
base_cropping_10	100	50
base_cropping_15	100	50
base_cropping_20	100	30
base_cropping_25	100	10
base_cropping_50	x	x
base_cropping_75	x	x
base_FMLR	100	100
base_Gaussian_filtering_3_3	100	100
base_JPEG_10	x	x
base_JPEG_15	x	x
base_JPEG_20	20	80
base_JPEG_25	100	80
base_JPEG_30	100	90
base_JPEG_35	100	95
base_JPEG_40	100	95
base_JPEG_50	100	100
base_JPEG_60	100	100
base_JPEG_70	100	100
base_JPEG_80	100	100
base_JPEG_90	100	100
base_linear_1.007_0.010_0.010_1.012	100	100
base_linear_1.010_0.013_0.009_1.011	100	100
base_linear_1.013_0.008_0.011_1.008	100	100
base_ratio_x_0.80_y_1.00	x	x
base_ratio_x_0.90_y_1.00	100	100
base_ratio_x_1.00_y_0.80	x	x
base_ratio_x_1.00_y_0.90	100	100
base_ratio_x_1.00_y_1.10	100	100

base_ratio_x_1.00_y_1.20	100	100
base_ratio_x_1.10_y_1.00	100	100
base_ratio_x_1.20_y_1.00	100	100
base_rotation_0.25	100	100
base_rotation_-0.25	100	100
base_rotation_0.50	100	100
base_rotation_-0.50	100	100
base_rotation_0.75	100	100
base_rotation_-0.75	100	100
base_rotation_1.00	100	100
base_rotation_-1.00	100	100
base_rotation_2.00	100	100
base_rotation_-2.00	100	100
base_rotation_5.00	100	70
base_rotation_10.00	40	x
base_rotation_15.00	x	x
base_rotation_30.00	x	x
base_rotation_45.00	x	x
base_rotation_90.00	100	100
base_rotation_scale_0.25	100	100
base_rotation_scale_-0.25	100	100
base_rotation_scale_0.50	100	100
base_rotation_scale_-0.50	100	100
base_rotation_scale_0.75	100	100
base_rotation_scale_-0.75	100	100
base_rotation_scale_1.00	100	100
base_rotation_scale_-1.00	100	100
base_rotation_scale_2.00	100	100
base_rotation_scale_-2.00	100	100
base_rotation_scale_5.00	100	75
base_rotation_scale_10.00	40	x
base_rotation_scale_15.00	x	x
base_rotation_scale_30.00	x	x
base_rotation_scale_45.00	x	x
base_rotation_scale_90.00	100	100
base_scale_0.50	100	100
base_scale_0.75	x	x
base_scale_0.90	100	100
base_scale_1.10	100	100
base_scale_1.50	100	100
base_scale_2.00	x	x
base_Sharpening_3_3	100	100
base_shearing_x_0.00_y_1.00	100	100
base_shearing_x_0.00_y_5.00	100	90
base_shearing_x_1.00_y_0.00	100	100
base_shearing_x_1.00_y_1.00	100	100
base_shearing_x_5.00_y_0.00	100	90
base_shearing_x_5.00_y_5.00	100	70
base_stirmark_random_bend	100	100

Note: x denotes that the embedded information bits cannot be extracted.