A study of image authentication based on self-similarity.

Yoko MAEMURA

Summary The conception of copyright protection for digital image is of great interest in recently. Several digital watermarking schemes have an effect on piracy preventing, but they have some degradation of the original images because of the embedded signature. It is therefore necessary to authenticate the digital image with no degradation especially for the works of art. In this paper, the author introduces the conception of the image authentication system using the parameters of fractal coding based on the self-similarity of the image structures and investigates the fundamental properties of this system. The address of best matched domain block, one of the fractal coding parameters shows the information of geometrical correlations between the partitioned images and has marked characteristics depending on each image. The detection rate of the best matched domain blocks can be increased by the optimization of the size of the partitioned image after the manipulations because of the relaxation effect of geometrical distortions.

Key Words: Authentication, Watermark, Fractal Compression, Similarity.

1. Introduction

During the last decade, digital technologies have grown drastically. Digital audio, video and software are widely used not only in office computer but also within home computer and open netwarks. Neverthless one particular problem of digital content is their ability to be easily processed. Several applications of watermarking has been considered by many researchers [1]. Each watermarking application has its own specific requirements. Therefore, there is no set of requirements to be met by all watermarking techniques. Neverthless, some general directions can be given for most of the applications; the mark had to be robust to image compression, quantization, D-A/A-D conversion, filtering, contrast transform and geometric transform. The problem is that the watermarking schemes can not avoid the degradation of the original image because of the embedding marks. It is necessary for the authors who make works of arts desire to distribute their own original images with no marks. The image authentication with no degradation is required in this case. The requirements of this system is also robust to any manipulations.

The fractal code is generated by calculating an Iterated Function System from the image in the fractal compression scheme. This fractal coding parameter (called collage map) is the information of the geometrical correlations between the block images and have marked characteristics which depend on each image. It is therefore useful to apply the collage map for the image authentication.

In this work, the authentication system

using a collage map is considered as one particular scheme to authenticate the image for the authors who desire to distribute the original images with no degradation caused by watermarking. A collage map detected from the image after geometrical translations and classical processed is used for certification of image. The vernam cipher constructed of the binalized mean values of the detected blocks and the content ID are used to certificate the copyright information data for this system. The evaluation of this system is the same as that of watermarking schemes. The results of the weakness of this system against the classical image processing operations and the Stirmark attack [2] are investigated.

2. Fractal Code

The coding-decoding system of the fractal compression is based on the construction of the image. This fractal code, which can be seen as a collage map, extracts the self-similarities of the image. The present approach is based on the block based fractal compression scheme developed by Jacquin [3]. This scheme express the image by a fractal code. It consists in searching an Iterated Function System in the image:

1. An image is partitioned into non-overlapping square blocks called range blocks. The domain blocks which have the same size as the range blocks are extracted from the image.
2. The following step consists in building a fractal code which can be seen as a collage map: we associate with each block R_i of the partition R, the block D_j which is more similar to R_i (except itself). This test of self-similarity consists in minimizing a quadratic error between the block R_i and the affine transformed block D_j.

3. Proposed Method

A collage map indices obtained from the fractal compression scheme mentioned above are composed of the associated block address of partition D, the affine transforms τ, the scale factor s and the offset o parameters for each range blocks. Indeed it is statistically rare to find a block equal to another in an ordinary image except when the image is a fractal image. Contrary to Jacqin's scheme, present scheme dose not use the decoding process, therefore the size of domain blocks or range blocks can be identical. The process of the image authentication is as follows:

1. The original image $f_{org}(x,y)$ $(x=1,\ldots,N; y=1,\ldots,M)$ is partitioned into nonoverlapping square range blocks of size $B_R \times B_R$ pixels; $R_i^{org}(i=1,2,\ldots,n \mid n=N/B_R \times M/B_R)$.
2. $f_{org}(x,y)$ is partitioned into square domain blocks of size $B_D \times B_D$ pixels; $D_j^{org}(j=1,2,\ldots,m \mid m=(N-B_D)/S \times (M-B_D)/S)$.
   S is the searching step cell size.
3. The best matched domain block D_i^{best} is satisfied the following equations for R_i^{org};
   $d(R_i^{org}, D_i^{best}) = \min_{j,\tau,s,o} d(R_i^{org}, D_j)$,
   where $d(R_i^{org}, D_i^{best})$ means the RMS (Root Mean Square) between R_i^{org} and D_i^{best}.
4. $A_{D_i}^{best} \in A_{D_1},\ldots,A_{D_n}$ show the address of D_i^{best} of the original image obtained from the above procedure.
5. The image to be confirmed the authentication is processed by the same procedure as for the original image. The addresses of the best matched domain blocks $A'^{best}_{D_i} \in A'_{D_1},\ldots,A'_{D_n}$

are generated. $A'^{best}_{D_i} \in A'_{D_i}, \ldots, A'_{D_n}$ are compared with $A^{best}_{D_i} \in A'_{D_i}, \ldots, A'_{D_n}$ and the informaiton of the remained block can be detected.

$A^{best}_{D_i}$ is seemed to be robust to image processing such as compression and/or filtering because the most similar domain block is selected for each range block. It is furthermore robust to the geometrical attack added locally because the large size of domain blocks reduces relaxation of the local distortion. However it appears that the quality of fractal codes relies very heavily on block classification and analysis for large size of block. This problem is dealt with an image which is composed of the offset values of a collage map in the preprocessing phase. The mean value of the block is used as an offset value in this method.

The bit pattern of authentication (called authentication data) is generated as the vernam cipher composed of the binalized mean values of the original image data and the bit pattern of content ID (called ID data). ID data and the authentication data are registered and should be in safekeeping at the certification center. The center correlates the ID data deduced from the distributed image with the regestered ID data in the center. The mean value of the block, where the best matched domain block are detected successfully are used for the threshold for the binalization. Therefore, the length of ID data is $B_R \times B_R$.

4. Simulation Results

The original gray scale image "Lenna" (Fig.1) of SIDBA for the simulation. The simulation to evaluate the proposed scheme has been performed by testing robustness against several kind of attack processing: the Stirmark attack as an geometrical transform, jpeg compression, median filtering and random noise adding.

The Stirmark distortion is a attack leading to a geometrical distortion that cannot be modeled by an affine transform on the whole image. The Stirmark 3.0 algorithm has been widely used for the evaluation test for robustness. The system which is robust to the Stirmark attack means that it robust to other processes. Fig.1 and Fig.2 show the original image and the Stirmark attacked image, respectively.

The rate of the remained parameter of collage map after the distortion by Stirmark attack for the various block size are shown in Fig.3. MV, SD and ABMDB are the parameters of collage map, which mean the mean value, the standard deviation and the address of the best matched domain block, respectively in the figures. The rate of the remained parameter is increased in the block size because the distortion locally added by Stirmark is relaxed. The address of the best matched domain block shows the relationship between range and domain. On the other hand, the mean value and the standard deviation are statically obtained. It is therefore that the address of the best matched domain block is more robust than other two parameters. The problem to set the block size large is the large amount of calculation. The mean mask are introduced in preprocessing phase against this problem. The rate of the remained parameter for the various mean mask size are shown in Fig.4. There is no influence of the size of mean masks. The results for the mask size of 2x2 are shown in Fig.5. The similar tendency are seen in this figure.

The simulations have been done for other classical processed images. The rate of the remained parameter are calculated for the different quality of factors with the jpeg compression scheme in Fig.6 with the mean mask size of 2x2. It can be seen that the results for the large size of block is more robust to the jpeg compression than the small one.

The results against the median filtering are shown in Fig.7 with the mean mask size of 2x2. It can be noticed that the results of the address of the best matched domain block is more robust than other parameters This is due to the low pass component of the image can be remained after filtering process.

The results are calculated for the different random noise level in Fig.8 with the mean mask size of 2x2. The large size of block is more robust than the small one except for the standard deviation.

The ID data deduced from the manipulated image are successfully detected for all kind of attack using a majority-logic as seen in Tab.1.

5. Conclusion

The conception of image authentication system using the fractal code based on self-similarity of the image structures has been proposed in this work. The present study indicates that the address of the best matched domain block is more robust than other parameters of fractal code to be used for the authentication. The general framework permits to foresee many perspectives to introduce this characteristics to the watermarking schemes.

References

[1] G.C.Langelaar, I.Setyawan, R.L.Lagendijk, "Watermarking Digital Image and Video Data", IEEE Signal Processing Magazine, Sep, 2000.

[2] M.G.Kuhn, Stirmark, http://www.cl.cam.ac.uk/fapp2/watermarking/image_watermarking/stirmark/, 1997.

[3] A.E.Jacquin, "Image coding based on a fractal theory of iterated contractive image transformations", IEEE Trans. Image Processing, Vol.1, No.1, pp.18-30, 1992.

Fig. 1: Original image.

Fig. 2: Attacked image by the Stirmark (PSNR=17.8dB).

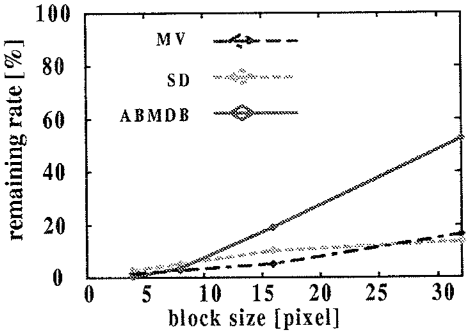

Fig. 3: The remaining rate of collage map data for the block size with no mean mask.

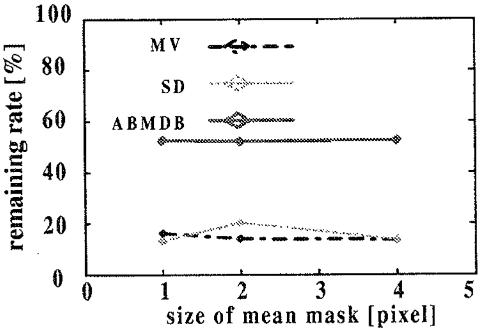

Fig. 4: The remaining rate of collage map data for the different mean mask size.

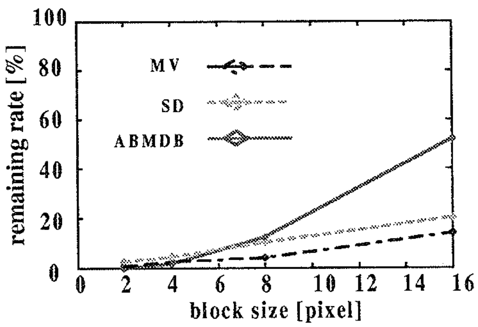

Fig. 5: The remaing rate of collage map data for the block size with the mean mask size of 2×2.

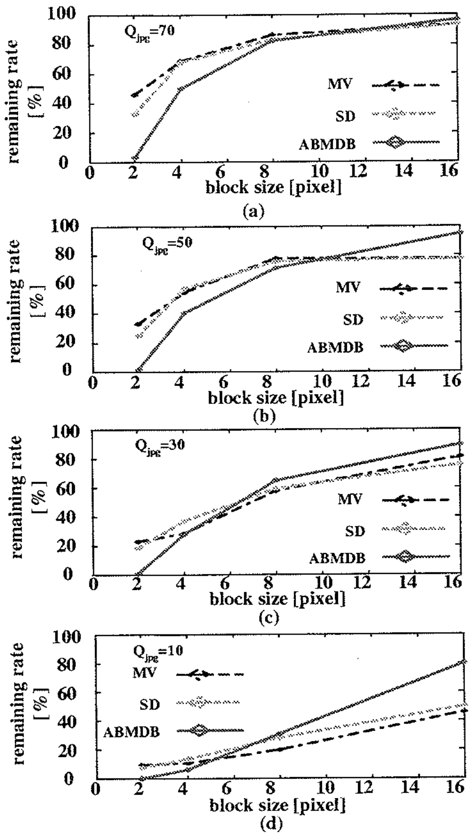

Fig. 6: The remaining rate of a collage map after jpeg compression for the different quarity factors.

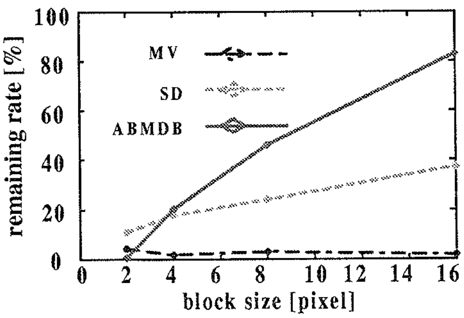

Fig. 7: The remaining rate of a collage map after median filtering(3x3).

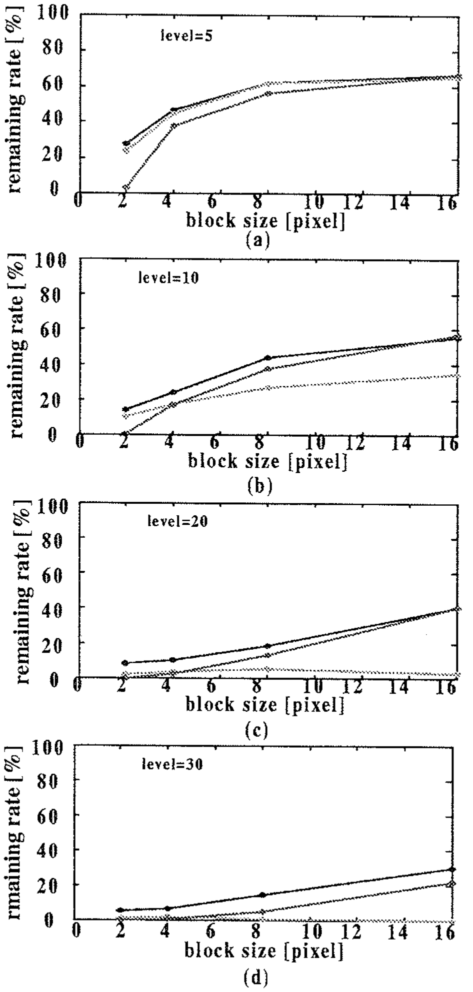

Fig. 8: The remaining rate of a collage map after random noise adding for different level.

Tab. 1: The detection rate of ID data.

Attack	Stirmark	Jpeg	Median	Random Noise
Detection Rate[%]	100	100	100	100