A FRAGILE WATERMARKING SCHEME USING A SIMPLE GENETIC ALGORITHM

Sang-Kwang Lee and Yo-Sung Ho

Kwangju Institute of Science and Technology
1 Oryong-dong Puk-gu, Kwangju, 500-712, Korea

ABSTRACT

In this paper, we propose a fragile watermarking scheme using a simple genetic algorithm. In order to check whether the received image maintains the same attributes as the original image, we exploit block edge characteristics of the image. We use the edge information as a fitness measure in the simple genetic algorithm for message coding. New strings are shuffled randomly and then inserted into the least significant bits of the original image. Experimental results demonstrate that the proposed watermark extraction algorithm can detect any modifications of the original image.

INTRODUCTION

Digital representation of copyrighted materials offers various advantages; however, the fact that an unlimited number of perfect copies can be illegally produced is a serious threat to the right of content owners. Therefore, watermarking is used for owner identification, royalty payments, and authentication by determining whether the data has been altered in any manner from its original form.

The main objective of content authentication is to detect modifications of the data. It can be achieved by so-called "fragile watermarks" that have low robustness to certain modifications such as compression. Among all possible watermarking applications, authentication watermarks require the lowest level of robustness [1].

In this paper, we propose a fragile watermarking scheme using a simple genetic algorithm. We exploit block edge characteristics of the original image to check whether the received image maintains the same attributes or not. The edge information is used as a fitness value in the simple genetic algorithm for message coding. New strings are shuffled randomly and then inserted into the least significant bits of the original image.

WATERMARK INSERTION

The embedding process of the proposed watermarking scheme is shown in Figure 1.

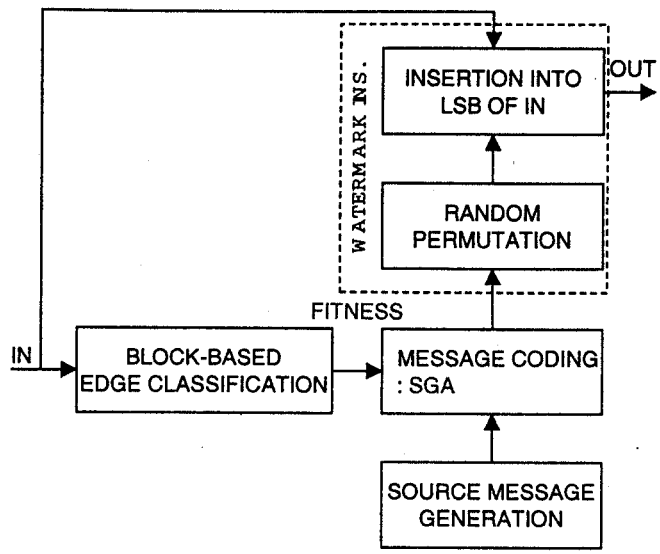

Figure 1: Watermark Insertion Procedure

Inputs to the watermark embedding scheme are the original image, the source message, and the watermark key. In order to exploit block edge characteristics, we use a simple block-based edge classification technique using some DCT coefficients. For example, when the block size is 8×8, we can use $C(0,1)$ and $C(1,0)$, out of 64 DCT coefficients, which represent the vertical and the horizontal edge components, respectively. Based on the two coefficients, we can determine the direction of the edge in each block. The edge classification algorithm is summarized in Figure 2 [2].

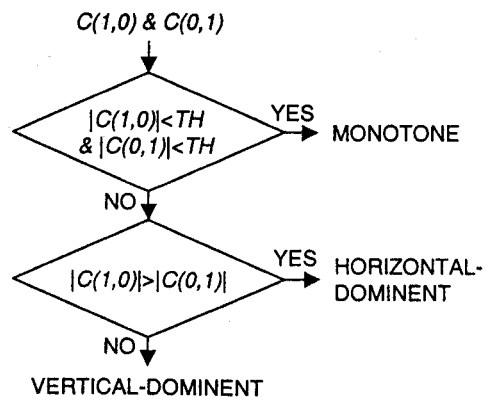

Figure 2: Block-based Edge Classification

The mechanism of a genetic algorithm involves only copying strings and swapping partial strings. The simple genetic algorithm is composed of three operations: reproduction, crossover, and mutation. Reproduction is a process where individual strings are copied according to their fitness values. Copying strings according to their fitness values implies that strings with higher values have higher probabilities of contributing one or more offspring in the next generation.

After reproduction, a simple crossover may proceed in two steps. First, the newly reproduced strings in the mating pool are mated at random. Second, each pair of strings undergoes crossing over as follows: an integer position k along the string is selected at random between 1 and the length less one, i.e., [1, l-1]. Two new strings are created by swapping all characters between positions k+1 and l inclusively.

Mutation is needed because, even though reproduction and crossover effectively search and recombine extant notions, occasionally they may become overzealous and lose some potentially useful genetic material (1's or 0's at particular locations). In artificial genetic systems, the mutation operator protects against such an irrecoverable loss. In the simple genetic algorithm, mutation is the occasional random alteration of the value of a string position [3]. In our work, block edge characteristics play an important role in fitness values of the simple genetic algorithm.

New strings are shuffled randomly and then inserted into the least significant bits of the original image. This shuffling operation forms the secrete key of the insertion algorithm.

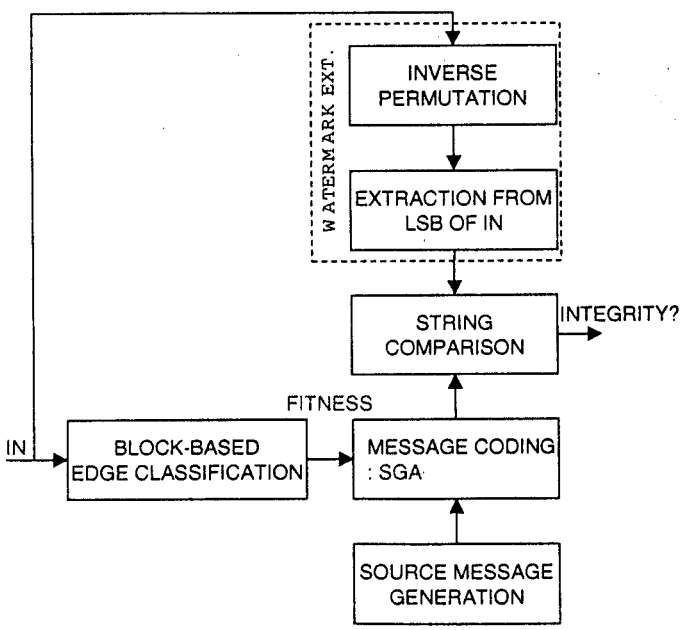

Figure 3: Watermark Extraction Procedure

WATERMARK EXTRACTION

The watermark recovery scheme is depicted in Figure 3. Inputs to the scheme are the watermarked image, the watermark key and the source message. Comparing detected strings with new strings, we can detect modifications of the original image

EXPERIMENTAL RESULTS

In order to evaluate the performance of the proposed fragile watermarking algorithm, we perform computer simulation on test images of size 512×512 pixels. The experimental results are summarized in Table 1.

Table 1: Experimental Results

Integrity?	YES	NO
Unchanged	x	
Unwatermarked		x
Scaled		x
Pixel Changed		x
Cropped		x
Wrong Key		x

The results show that this algorithm can detect if the key is incorrect, or if the image is not watermarked, or if the image is changed in its pixel values.

CONCLUSION

We described a watermarking scheme for authentication. Experimental results show that the proposed algorithm can detect any modifications made to the image. In addition, since the number of the fitness values plays an important role in the robustness of the watermark, this algorithm can be applied to semi-fragile watermarking.

ACKNOWLEDGMENT

This work was supported in part by KOSEF through UFON and in part by MOE through BK21.

REFERENCES

[1] S. Katzenbeisser and F. Petitcolas, *Information hiding techniques for steganography and digital watermarking*, Artech House, 2000.

[2] B. Shen and I. Sethi, "Direct feature extraction from compressed images," *SPIE Storage and Retrieval of Image and Video Databases*, vol. 2670, 1996.

[3] D. Goldberg, *Genetic algorithms in search, optimization and machine learning*, Addison Wesley, 1989.