

Short Paper

Robust Watermark Algorithm using Genetic Algorithm

CONG JIN AND SHI-HUI WANG*

Department of Computer Science

Central China Normal University

Wuhan 430079, P.R. China

**School of Mathematics and Computer Science*

Hubei University

Wuhan 430062, P.R. China

Geometric attacks are among the most challenging problems in present day data hiding. Such attacks are very simple to implement yet they can defeat most of the existing data hiding algorithms without causing serious perceptual image distortion. In this research, we report a novel method to estimate the geometric manipulation. Geometric attacks can very easily confuse the decoder unless it transforms the image back to its original size/orientation, *i.e.*, recover the lost synchronism. To be able to do so, the decoder needs to know how the image has been manipulated, *i.e.*, needs to know geometric transformation parameters. In our approach, the point pattern matching measure is computed for the geometric manipulation. The reference point patterns (*i.e.*, a triple) are computed from feature ellipse of the original image. The point pattern matching is realized by genetic algorithm. The proposed scheme does not require the original image because reference triple information of the watermarked image has been contained in the secret key. Novel method has been proved its robustness to geometric attacks through experiments.

Keywords: digital watermark, reference points extraction, points matching, genetic algorithm, robustness

1. INTRODUCTION

Data hiding [1, 2], the art of hiding information into multimedia data in a robust and invisible manner, has gained great interest over the past few years. There has been a lot of interest in the data hiding research, mostly due to the fact that data hiding might be used as a tool to protect the copyright of multimedia data. A secret message, which is called digital watermark, is an imperceptible signal embedded directly into the media content, and it can be detected from the host media for some applications. The insertion and detection of digital watermarks can help to identify the source or ownership of the media, the legitimacy of its usage, the type of the content or other accessory information in various applications. Specific operations related to the status of the watermark can then be applied to cope with different situations.

Received April 16, 2005; revised June 24, 2005; accepted June 30, 2005.

Communicated by H. Y. Mark Liao.

Geometrical modifications, we refer to all image manipulations that change the image spatially. In this research, we consider geometrical modifications that most image users can apply easily while the value of the image is still preserved. In particular, we focus on the affine transform, which can be defined by a 2×2 affine matrix plus translation. Given the input position (x, y) , the new position (x', y') can be determined by using six parameters in the following model:
$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} x_s \\ y_s \end{pmatrix}.$$

Among all kinds of affine transformation, cropping, rotation and scaling change are those used more frequently in image manipulation. To successfully detect the watermark from the image undergoing geometrical modifications, we need to determine these six parameters so that the inverse transform can be applied to recover the image.

In [3], affine point pattern matching by genetic algorithm is discussed using the partial bidirectional Hausdorff distance [4]. We should use this technique to design the digital watermark algorithm for resisting geometric attacks.

In this paper, a robust watermark algorithm using the literature [3] is researched. Although literature [4] makes use of to genetic algorithm for designing watermark scheme, its purpose is to find the optimal frequency bands for watermark embedding into DCT-based watermarking system. Genetic algorithm also is used in our watermark scheme, but it is used for point pattern matching.

This paper is organized as follows. In section 2, in order to grasp the algorithm as a whole, we firstly introduce the framework for such algorithm briefly. In section 3, the fundamental idea of literature [3] is introduced. In section 4, the embedding secret message processes and the decode method for resisting geometric attacks are described. In them among, the most important problem is the design of the secret key. In section 5, we present experimental results. Finally, section 6 contains conclusions.

2. ALGORITHM FRAMEWORK

Integer $I(i, j)$, $I'(i, j)$ indicate (grayscale or) luminance of the original image I and the watermarked image I' with coordinates (i, j) , $(1 \leq i \leq N_1, 1 \leq j \leq N_2)$, respectively.

In this research, the watermark embedding algorithm is the same as normal embedding method. According to the approaches proposed by Cox *et al.* [5], watermark embedding is achieved by modifying a set of full-frame DCT coefficients of the image. The amount of modification each coefficient undergoes is proportional to the magnitude of the coefficients itself as expressed by the following rule

$$I'(i, j) = I(i, j) + \gamma \cdot W(i, j) \quad (1)$$

where, γ indicates a parameter controlling the watermark strength, and $W(i, j)$ is watermark data.

For better comprehending new algorithm, the framework of this algorithm is firstly given. The algorithms can be represented in the framework shown in the block diagram of Fig. 1.

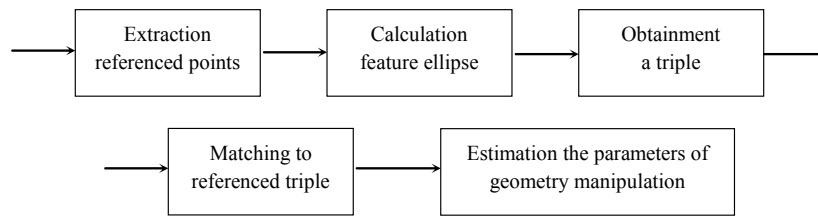


Fig. 1. Building blocks for geometry invariant data hiding.

The five building blocks of the algorithm scheme are:

- To extract the reference points set on watermarked image;
- To calculate feature ellipse of the reference points set;
- To obtain a triple on feature ellipse being called the referenced triple;
- To match between the referenced triple and a triple on tested image through genetic algorithm;
- To estimate the parameters of geometry manipulation.

A detailed discussion of the individual blocks will be deferred in next section.

3. ALGORITHM DESIGN

3.1 Reference Point Set

In order to realize the decoding secret message blindly, we let the referenced triple information of the watermarked image is a part of the secret key. So, before decoding the secret message, the referenced triple information in secret key is decoded at first, and the referenced triple of the watermarked image and any triple of the tested image are matched by genetic algorithm. By using the triple corresponding to the highest value of the fitness function and the referenced triple, the geometric manipulation parameters can be estimated. Therefore, the design of reference triple is a key of this algorithm.

The reference points should satisfy the stability condition, *i.e.*, the reference points should be robustness to compression, filtering, noise adding, *etc.* We know that secure spread spectrum watermark method, proposed by Cox *et al.* [5], has stronger robustness, safety, and transparency. Therefore, we computed full frame DCT coefficients of the image and obtained DCT coefficients between the k th and the $(k + m - 1)$ th according to the magnitude of the DCT coefficients. The points corresponding these DCT coefficients will be reference point denoted by set P .

3.2 Feature Ellipse

Definition 1 [3] (Feature ellipse of a point set) Given a point set $P = \{p_i = (x_i, y_i)^T | i = 1, 2, \dots, m\}$, its feature ellipse is defined as

$$(x - c)^T E^{-1} (x - c) = \frac{1}{\alpha} \quad (2)$$

which α is a positive integer whose value determines the size of the feature ellipse, and $c = 1/m \sum_{i=1}^m p_i$ and $E = 1/m \sum_{i=1}^m (p_i - c)(p_i - c)^T$ are the center point and the second-order center moment of P , respectively.

Obviously the center of the feature ellipse locates in the center of the reference point set. Via adjusting the parameter α , the feature ellipse can be insured to lie into the convex hull of P .

3.3 Reference Triple

Draw three rays from the center c of P , of which each pair forms an angle of 120° . The rays intersect the feature ellipse at three points, which is the expected referenced triplet. A point set is composed by the three points, denoted by P' . Obviously triple locates in the local area around the center of P . For convenience, in this research, we will ensure that one of three rays is vertical.

4. POINT MATCHING BY GENETIC ALGORITHM

For tested image, we obtain its three points set, denoted by Q , using the same method with watermarked image. Any Q compose a triple, denoted by Q' . We adopt genetic algorithm [6] for point patterns matching. For measure the degree of match between two point sets P' and Q' , fitness function is constructed by the partial bidirectional Hausdorff distance [7]. The output of GA is the triple of points which has the highest value of fitness function. Using this triplet and the referenced triplet, the geometric transformation parameters can be obtained.

In GAs, the parameters of the search space are encoded in the form of strings (called chromosomes). A collection of such strings is called a population. An objective and fitness function is associated with each string that represents the degree of goodness of the string. Based on the principle of survival of the fittest, a few of the strings are selected and each is assigned a number of copies that go into the mating pool. Biologically inspired operators like crossover and mutation are applied on these strings to yield a new generation of strings. The process of selection, crossover and mutation continues for a fixed number of generations or till a termination condition is satisfied. An excellent survey of GAs along with the programming structure used can be found in [8].

4.1 Chromosomes

Firstly, the initial population is generated randomly. However, the generating range of chromosomes is not arbitrary but limited to the local area around in the convex hull of Q . Each chromosome consists of a triple of points in test image. Its detailed construction method is serializing coordinates of the three points and coding them into binary codes. As an illustration let us consider the following example.

Three points $T'_1 = (x'_{j1}, y'_{j1})$, $T'_2 = (x'_{j2}, y'_{j2})$ and $T'_3 = (x'_{j3}, y'_{j3})$ are given in test image. Table 1 shows the detailed construction of a chromosome consisting of the three points. Here, each x or y is represented by a binary code. Thus the whole chromosome is a binary sequence.

Table 1. Chromosome coding.

x'_{j1}	y'_{j1}	x'_{j2}	y'_{j2}	x'_{j3}	y'_{j3}
-----------	-----------	-----------	-----------	-----------	-----------

4.2 The Fitness Function

To a chromosome shown in Table 1, the coordinates of the triplet that the chromosome represents are firstly retrieved according to their binary codes. Obviously, if the degree of match between P' and Q' under the transformation can be measured, it is equivalent to evaluating the fitness of the chromosome.

Considering the partial bidirectional Hausdorff distance between point sets P' and Q' the smaller the distance is, the degree of match between P' and Q' is larger. So the fitness function can be selected as the inverse of the partial bidirectional Hausdorff distance $fitness = \frac{1}{a + H_{LK}(P', Q')}$ where a is a positive constant. In order to avoid the denominator is a zero, the partial bidirectional Hausdorff distance is added a .

4.3 Genetic Operators

A pair of chromosome is randomly chosen from the population and is used as the parents to reproduce the offspring. The selection principle is the more chromosome number of its new offspring to the next generation, the bigger fitting function value F_i with the larger probability p_s . The nature choice phenomenon of the biosphere is simulated by $p_s = \frac{F_i}{\sum_{j=1}^i F_j}$.

Crossing operator is obtained after reset the parents facts which are got the selection processing. Crossing processing is performed according to a certain probability, which is called crossing probability p_c . The crossing effect is to produce much better chromosome after combination the generating materials of the parents. Here we adopt commonly used single point crossover operator.

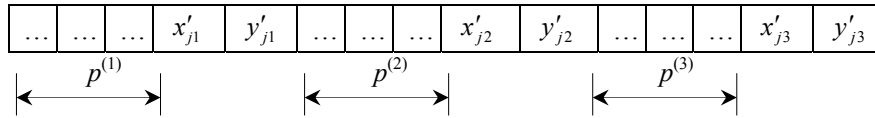
Chromosome is selected from the population using certain probability p_m , and the selected chromosome is overturned after randomly choosing a bit binary system code, *i.e.* 0-1, 1-0.

4.4 Watermark Embedding and Extraction

4.4.1 Design watermark

In our research, watermark is generated by secret key. After referenced triplet obtained, the secret key may be generated. Chromosome consists of reference triple of points in the watermarked image, too. Its construction is the same as Table 1. This chromosome coding is a part of the secret key.

Table 2 shows the detailed construction of a secret key. Here, each x or y is represented by a binary code denoted by $c = \{c_i | c_i \in \{0, 1\}, i = 1, 2, \dots, L\}$, where L is the

Table 2. Construction of the secret key.

length of the binary sequence of each x or y . Usually we use $c' = \{c'_i | c'_i = 1 - 2c_i, i = 1, 2, \dots, L\}$. So c' is a binary polar sequence of $\{-1, 1\}$.

Where $p^{(1)}$, $p^{(2)}$, and $p^{(3)}$ are 2-D pseudo-random binary sequence of $\{-1, 1\}$ with zero mean, generated using the key as the seed. So the whole secret key is 2-D binary sequence of $\{-1, 1\}$ too. This binary sequence of $\{-1, 1\}$ is denoted S . The length of S is N , where $N = \text{Length}(p^{(1)}) + \text{Length}(p^{(2)}) + \text{Length}(p^{(3)}) + 6L = N_1 \times N_2$.

In other words, N equals the size of the original image. There are M binary sequences of $\{-1, 1\}$ the same as size of S using different key as the seed, respectively. Suppose m is a secret message hidden in an original image, where $m = \{b_i | b_i \in \{0, 1\}, i = 1, 2, \dots, M\}$. We let $m' = \{b'_i | b'_i = 1 - 2b_i, i = 1, 2, \dots, M\}$. So m' is a binary polar sequence of $\{-1, 1\}$, too. The watermark will be $W(i, j) = S \cdot m' = \sum_{k=1}^M S_{i,j}(k) b'_k$.

4.4.2 Embedding and extraction

The watermark can be embedded into an original image additively by Eq. (1). A simple detection can be performed using correlation detector. The correlation is calculated as

$$\begin{aligned}
 C_l &= \sum_{i,j} S_{i,j}(l) \cdot I'(i, j) = \sum_{i,j} S_{i,j}(l) \cdot I(i, j) + \gamma \sum_{i,j} S_{i,j}(l) \cdot \sum_{k=1}^M S_{i,j}(k) \cdot b'_k \\
 &= \gamma \sum_{k=1}^M \sum_{i,j} S_{i,j}(l) \cdot S_{i,j}(k) \cdot b'_k = \gamma \sum_{i,j} |S_{i,j}(k)|^2 b'_k, l = 1, 2, \dots, M.
 \end{aligned}$$

In the above deduction, because $S_{i,j}(l)$ is a zero mean pseudo-random binary sequence of $\{-1, 1\}$, and it is independent with $I(i, j)$, term $\sum_{i,j} S_{i,j}(l) \cdot I(i, j)$ is supposedly close to zero. Other terms are all zeros when $k \neq l$ because pseudo-random patterns $S_{i,j}(k)$ are uncorrelated with each other. So secret message can be decoded by $b'_l \approx \text{sign}(C_l)$.

5. EXPERIMENT RESULTS

We consider 256×256 grayscale images. Let Fig. 2 be an original image, and Fig. 3 a secret message. Fig. 4 is the watermarked image for embedding the secret message into Fig. 2 using Eq. (1), when $\gamma = 0.03$.

In the experiments, the parameters of our algorithm are set as, population size $N = 500$, crossover probability $p_c = 0.05$, mutation probability $p_m = 0.02$, two fractions f_l and f_k are all 0.8, and the maximum iterative steps $G_{\max} = 200$. The length of binary code for



Fig. 2. Original image.



Fig. 3. Secret message.



Fig. 4. Watermarked image, when $\gamma = 0.03$, PSNR = 37.3985.

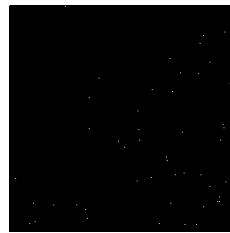


Fig. 5. Referenced points set P of Fig. 4.

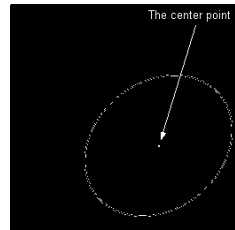


Fig. 6. Feature ellipse of Fig. 5. The center point is (161, 168).

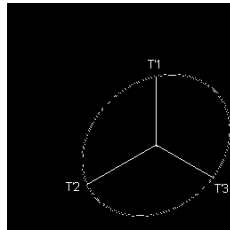


Fig. 7. Referenced triple of Fig. 4. $T_1'(84, 168)$, $T_2'(206, 90)$, $T_3'(198, 232)$.



Fig. 8. Tested image by rotating Fig. 4 according to 5° .



Fig. 9. Referenced points set of Fig. 8.



Fig. 10. Tested image by scaling Fig. 4 according to 75%.



Fig. 11. Referenced points set of Fig. 10.

each coordinate is 8 and the parameter α in Eq. (2) is 2. We obtain DCT coefficients between the k th and the $(k + m - 1)$ th according to the magnitude of the DCT coefficients, where $m = 50$.

In the experiments, because the size of secret message is $41 \times 141 = 5,781$, we produce 5,781 S random matrixes, and its all elements are binary random variable of $\{-1, 1\}$ with zero mean. The size of S equals the size of the original image. According to the watermark design, after some elements of S are replaced by referenced triple, we received new S matrix of the following forms. Every S matrix is like this.

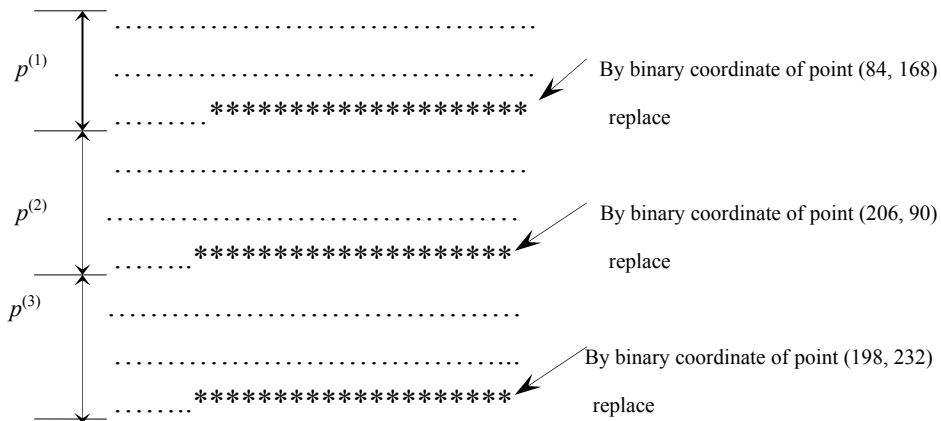


Fig. 12. Form of S matrix.



Fig. 13. Tested image by translating Fig. 4 three pixel positions rightwards and downward respectively.



Fig. 14. Referenced points set P' of Fig. 13.



Fig. 15. Tested image by cropping Fig. 4.



Fig. 16. Referenced points set of Fig. 15.

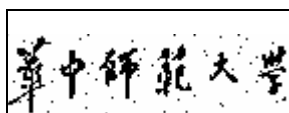


Fig. 17. Decoded the secret message from Fig. 8.

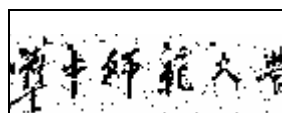


Fig. 18. Decoded the secret message from Fig. 10.

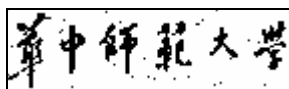


Fig. 19. Decoded the secret message from Fig. 13.

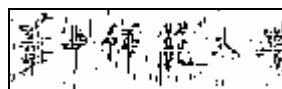


Fig. 20. Decoded the secret message from Fig. 15.

For Figs. 8, 11, 13, and 15, after randomly using new algorithm for 20 times respectively, the best decoded secret messages are Figs. 17-20, respectively.

Here, similarity between original secret message and decoded secret message is simply expressed in terms of the fraction $y = X/N$, where N is the total number of secret message points in both figures and X is the count of points from either secret message that have at least one point from the other secret message in their 3×3 neighborhood. Calculation results of similarity are shown in Table 3.

Table 3. Similarity measure.

Experiment	Similarity
Between Fig. 3 and Fig. 17	0.9510
Between Fig. 3 and Fig. 18	0.9280
Between Fig. 3 and Fig. 19	0.9377
Between Fig. 3 and Fig. 20	0.8485

Table 4. Experiment results.

Attack	Scaling	Rotation	Cropping	Translation
Percentage	83%	100%	85%	87%

Besides above experiments, we let other image be original image selected from USC-SIPI Image Database [9] for testing the new algorithm. We summarize the results in Table 4, where we list the experiment results for each section. To every kind of attack, we make experiment 100 times for over 1,000 images, and data of Table 4 is the percentage of the watermark is successfully decoded. Here, we determine that secret message is decoded successfully when similarity measure is over 0.80.

6. CONCLUSION

In this paper, a blind digital watermark algorithm is design using points matching by genetic algorithm. Characteristics of proposed algorithm include

- (1) The watermark can always be correctly decoded when the cropped part is less than 1/4 of the watermarked image.
- (2) The watermark can always be correctly decoded under the condition that the scale is bigger than 0.615 times; otherwise, the watermark cannot be correctly decoded.
- (3) If image information does not lose when translation, the watermark can always be correctly decoded; otherwise, the watermark cannot be correctly decoded when lose information is bigger than 2/5.

Through experiment we confirm that the blind secret message decoder has the good robustness to rotation, scaling, and translation, cropping attack. It points out a new way for designing the better blind secret message decoder.

REFERENCES

1. M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermark technologies," in *Proceedings of the IEEE*, Vol. 86, 1998, pp. 1064-1087.
2. F. Hartung and M. Kutter, "Multimedia watermark techniques," in *Proceedings of the IEEE*, Vol. 87, 1999, pp. 1079-1107.
3. L. H. Zhang, W. L. Xu, and C. Chang, "Genetic algorithm for affine point pattern matching," *Pattern Recognition Letters*, Vol. 24, 2003, pp. 9-19.
4. C. S. Shieh, H. C. Huang, F. H. Wang, and J. S. Pan, "Genetic watermarking based on transform-domain techniques," *Pattern Recognition*, Vol. 37, 2004, pp. 555-565.
5. I. J. Cox, J. Killian, F. Thomson, and T. Shamoon, "Secure spread spectrum watermark for multimedia," *IEEE Transactions on Image Processing*, Vol. 6, 1997, pp. 1673-1687.
6. D. E. Goldberg, *Genetic Algorithm in Search, Optimization and Machine Learning*, Addison-Wesley, New York, 1989.
7. D. P. Huttenlocher, G. A. Klanderman, and W. J. Rucklidge, "Comparing images using the Hausdorff distance," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 15, 1993, pp. 850-863.
8. E. Saber, A. M. Tekalp, and G. Bozdagi, "Fusion of color and edge information for improved segmentation and edge linking," *Image and Vision Computing*, Vol. 15, 1997, pp. 769-780.
9. USC-SIPI Image Database, <http://sipi.usc.edu/services/database/Database.html>, 1997.

Cong Jin (金聪) graduated for Ph. D. in Institute for Pattern Recognition and Artificial Intelligence, Huazhong University of Science and Technology at Wuhan, P.R. of China, in 2005, and she is currently a professor of computer science, Central China Normal University, P.R. China. Her research interest includes digital watermarking, image processing, and neural networks.

Wang Shihui (王时绘) graduated from the Department of Computer Science, Huanghe University at Zhengzhou, P.R. of China, in 1991, and currently an associate professor of computer science, Hubei University, P.R. China. His research interest includes digital signal processing, computer network, and database.