American Journal of Applied Sciences 4 (6): 405-409, 2007
ISSN 1546-9239

A Main Object-oriented Projective Invariant Image Watermarking Approach

Malik F. Alamaireh
CS Department, Amman Alahleyyah University, Jordan

Abstract: Digital Watermarking is a technology that enables to protect distributed digital content from unauthorized reuse. Robust watermarks must be able to survive a range of geometrical "attacks," such as image resizing, cropping, translation, rotation, scaling, smoothing, filtering, and simplification. In the current paper we extend existing approaches that are based partially on image invariant features; by introducing new image invariant features and exclusively using them. The proposed watermarking method is based on a combination of image processing techniques, theory of geometry, multiple image invariant features, and public key encryption. Experimental results show that the use of such combination of techniques allowed for securing the embedded watermark and for success in image watermark's recovery, if images were exposed to several geometrical attacks.

Key words: Authentication, forgery prevention, digital rights management, piracy

INTRODUCTION

The term watermarking loosely refers to the use of steganography in the application areas of ownership assertion, authentication, content labeling, and content protection. Steganography addresses the problem of hiding information within digital documents. A digital watermark is a distinguishing piece of information that is adhered to a digital document to protect it. This means that it should be very difficult to extract and remove the watermark from a watermarked object[1].

Since watermarking can be applied to various types of data, the imperceptibility constraint will take different forms, depending on the properties of the recipient. In addition, a watermark should possess some desirable characteristics related to robustness, thus it should be resilient to standard manipulations of unintentional as well as intentional nature. Moreover, it should be statistically irremovable, which means, it should be immune against statistical analysis from the attacking point of view. In most watermarking applications embedment of additional information is necessary[2].

One of the most widely considered image watermarking attacks is a class of image manipulations that cause geometric distortion. Most solutions aim at solving geometric distortion due to two-dimensional transformations[1]. Several approaches that counterattack the geometric distortions have been developed: normalization based watermarking[3], invariant domain based watermarking[4], template matching based watermarking, and featured-based watermarking[5,6]. These methods exploit some invariant features for watermark synchronization such as image normalization[4-9]. As a result, such schemes normally require extensive search to recover a template during the detection stage[1].

Every watermarking system consists at least of two different parts: watermark embedding unit and watermark detection and extraction unit. In order to determine how much a certain pixel can be altered so that the resulting watermarked image is indistinguishable from the original, from one side, and to hold enough information, from the other side, the unmarked image is analyzed from the point of view of the human eye sensitivity to changes in flat areas, and its relatively high tolerance to small changes in edges[2].

In literature invariant to a geometrical transform digital image watermarking methods, were proposed. These obtain watermark embedding points based on the invariant theory of collinear points, intersection of a line pairs, image corner points, etc.[8, 9]. These methods rely on image variant features under geometrical alterations; the fact that causes them not to be able to survive a variety of geometrical "attacks".

The current research was aimed to introduce a robust watermarking scheme based on image invariant features against various geometrical attacks such as cropping, transportation, cut, resizing, rotation, and filtering. It was intended to improve the current feature based image watermarking methods.

Corresponding Author: Malik F. Alamaireh, Head of CS Department, Amman Alahleyyah University, P. O. Box 1438, Code 19110, Assalt - Jordan

Overview of the used techniques: The proposed approach makes use of the following techniques: background subtraction, finding the center of area, finding the center of mass, and invariance theory of geometry. Statistical background modeling and subtraction has proved to be a popular and effective class of algorithms for segmenting independently moving foreground objects out from a static background, without requiring any priori information of the properties of foreground objects. In literature many approaches were developed for handling various sources of error, including motion blur, sub-pixel camera motion, mixed pixels at object boundaries, and uncertainty in background stabilization caused by noise, un-modeled radial distortion, and small translations of the camera. These apply Bayesian approach to specifically incorporate uncertainty concerning whether the background has yet been uncovered after identifying foreground objects[10].

The center of area (c_a) is a standard image feature that has many applications in matching the shapes of two closed contours. We can locate the center of area of planar areas using integration. The approach is similar to the one used in the volumes of revolution - that is we consider small strips, and then use integration to add them up. In these problems the planar area is to be thought of as a thin metal plate of uniform density. So the mass is proportional to the area. We already know how to calculate areas, and so we can get the total mass. The total area is equivalent to sum of the individual areas that form the image[11].

To find the center of the area $(\bar{x}, \bar{y})$ of the image we use formulas 1, 2, and 3.

$$A\bar{x} = \int_{\substack{total\\area}} xdA \Rightarrow \bar{x} = \frac{1}{A}\int_{\substack{total\\area}} xdA \quad (1)$$

$$A\bar{y} = \int_{\substack{total\\area}} ydA \Rightarrow \bar{y} = \frac{1}{A}\int_{\substack{total\\area}} ydA \quad (2)$$

$$A = \int_{\substack{total\\area}} dA \quad (3)$$

Where: A- is the total area of an image*;* A_i, x_i, and y_i- are individual parts of the area, their *x*-coordinates, and their *y*-coordinates respectively.

The geometrical center of mass of a 3D object known as its centroid (c_m) is the average location of its weight. In a uniform density body, it coincides with the object's center of mass. The "center of buoyancy" of an object depends only on its geometric shape, independent of its density. The "center of mass" of an object depends on its shape and its density. The center of mass of an object depends on its shape, density, and the external gravitational field. The moment exerted by a body is the same as that would be exerted were the whole mass to be concentrated at the centre of mass. What we shall do is calculate this moment in two ways (M_x, M_y) and thereby locate the centre of mass. To get the coordinates of the centroid we use the fact that these moments are equal to the ones we would get by concentrating the whole mass at the centre of mass[11].

Let the centre of mass be at (x_m, y_m), and let the area of the region be *A,* where: $A = \int f(x)$; A is bounded by the curve *f(x)* and the x-axis. The distance of the centre of mass from the *x*-axis is x_m, and so the moment about the *x*-axis is Ay_m. Similarly that about the *y*-axis is Ax_m. Therefore we have the formulas to find the center of mass:

$$X_m = M_y / A, \quad y_m = M_x / A \quad (4)$$

The cross ratio of four collinear points defined by the invariance theory of geometry does not change under geometrical manipulation[9]. For the points x_1, x_2, x_3, and x_4 that are said to be collinear, the cross ratio relationship of these four points can be computed from the following:

$$R_c(x_1, x_2, x_3, x_4) = \frac{\overline{x_1x_3} \cdot \overline{x_2x_4}}{\overline{x_2x_3} \cdot \overline{x_1x_4}} \quad (5)$$

Where $\overline{x_1x_3}$, $\overline{x_1x_4}$, etc. is the Euclidean distant of segments x_1x_3 and x_1x_4 respectively. The cross ratio is preserved through linear scaling, resizing, reflection, rotation, and translation.

Image watermarking algorithm: The image main object(s) is (are) typically found by using a suitable background subtraction algorithm. In case of recognizing one or more main objects, these will be later subject to applying watermarking. The main object recognition strategy must guarantee recognizing at least one main object in the image to be watermarked.

The proposed method identifies the watermark embedding points in an image based on its invariant geometrical properties. These features are the image main object's center of area (c_a), its virtual center of mass (c_m), and the center of area of one half of the image main object (c_h). To find an image virtual center of mass, its main object is represented as a 3-

dimensional uniform density object in the x, y, z coordinates system as follows: x, y correspond to the two planar image coordinates, z corresponds to the pixel color intensity. A "half" of a main image object may be uniquely identified by drawing a straight line through an image main object center of area and its centroid. Then we can find its center of area (c_h) of an object half is found and a base line (X) is drawn through two image centers (c_a ,c_m), and another straight line (Y) is drawn through image center of area and image half center of area (c_a ,c_h) as shown in Fig. 1. A grid of lines consisting of lines parallel X axis and of lines parallel to Y is constructed such that the distances between neighbor parallel lines are set according to a predefined set of cross ratio values.

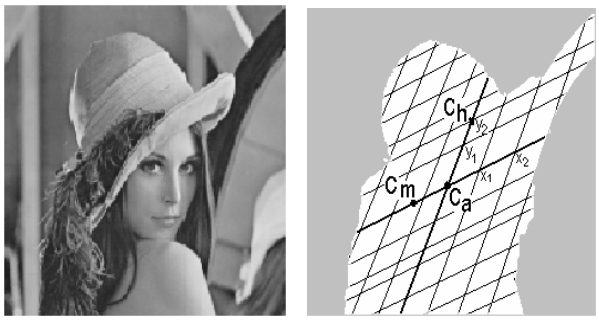

Fig. 1: Calculation of the watermark embedding points.

The proposed image watermarking algorithm is as follows (Fig. 2):

* Define a set of cross-ratio values to be used in subsequent steps (R_c).
* Encrypt the initial watermark using an encryption algorithm and a key[12]:

$$V=E_k(W, k) \quad (6)$$

where: V- a vector of cipher values that correspond to the watermark; *k*- encryption key.

* Define a function that maps (V) of size (n) into a set of (2n) coordinate values such that these values comply with the selected set of cross ratios (R_c). These values will be used to specify the watermark embedding points (x_i, y_i) as follows: $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$ (Fig. 1).
* Find the image main objects by using a background subtraction (BS) algorithm; find the image centroid and the image center of mass for each detected main object of an image to be watermarked. Divide the main object into two parts by drawing a straight line through its center of area and its centroid.
* Compute the watermark embedding points in the image by first drawing a grid of straight lines as mentioned earlier based on the found three image invariant feature points. The points of intersection of the lines of the grid that are located within the main object area are used for embedding a watermark ($p_i=(x_j,y_k)$, $i=1, 2, .., m$). In the case of a collocation of a main object center of area and its center of mass, we apply a square function to the color depth values used as the third dimension of a 3D representation of that main object to move its center of mass far from the center of area.

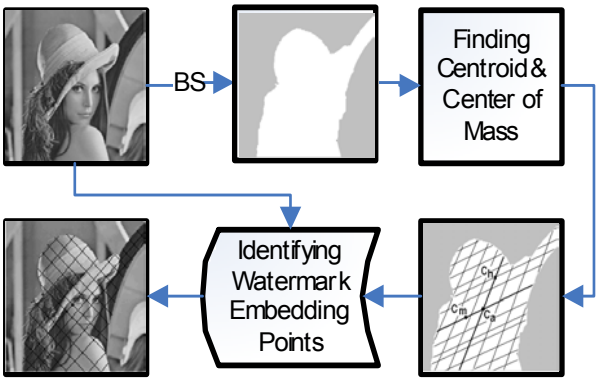

Fig. 2: Image watermarking algorithm

* Embed a watermark pattern bits into those watermark-embedding points obtained from Step 4. Let $p_i=(x_j,y_k)$, $i=1, 2, .., m$, be m watermark embedding points. Given a watermarking pattern bits $wi \in \{-1, 1\}$, $i = 1, 2, \ldots, m$, the watermark embedded image is obtained by using formula 7:

$$p_i^e(x_i, y_i) = p_i(x_i, y_i) + \alpha.w_i \quad (7)$$

Where: $p_i(x_i, y_i)$ is the original image pixel, and (x_i, y_i) is its coordinates, α is a modulation factor.

Watermark detecting algorithm: To detect the embedded watermark from a possibly distorted watermarked image, the watermark embedding locations must be obtained by repeating the steps (1-4) of the watermark embedding algorithm. Then detection is performed by computing formula 8.

$$C(p_i^e, w) = \frac{\frac{1}{m}\sum_{i=1}^{m}\left(\tilde{p}_i^e.\tilde{w}(i)\right)}{\sigma_{p_i^e}\sigma_w} \quad (8)$$

Where $\tilde{p}_i^e$ are watermark embedding points extracted from the watermarked image, $\sigma_{p_i^e}\sigma_w$ are the standard deviation of $\tilde{p}_i^e$, and the standard deviation of the

watermark pattern, respectively. A watermark is detected if the above correlation value is above the predefined threshold. The threshold may be defined, for example, by using certain statistical criteria.

In these experimental results, we demonstrate the effectiveness and utility of our watermarking scheme in the presence of various real world attacks. We used 8 different test images which were embedded with 5 different watermark patterns, each of length m = 1024, by the proposed method.

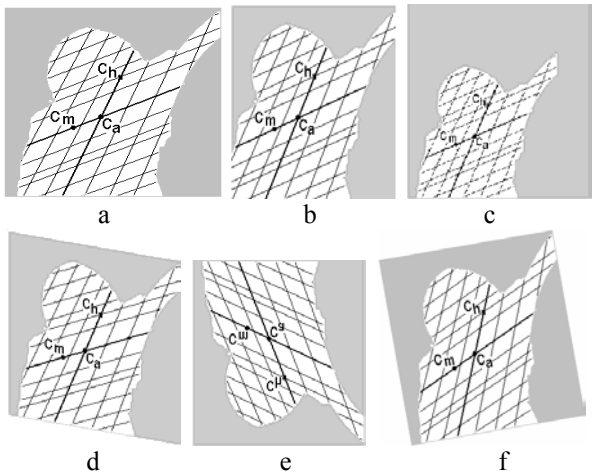

Fig. 3: Geometrical alteration manners
a- Resizing, b- Cropping, c- Translation, d- Skew, e- Reflection, f- Rotation

The watermarked images were tested for watermark recovery after they were rotated, scaled, translated, resized, cropped, skewed, and filtered, see Fig. 3. Image skew and rotation were applied with angle of rotation changing from 1 to 30 degrees. By using the detection threshold of 5 and α = 2.5, the overall false positive detection rate was 0.1 %, while the overall false negative rate was 1.1 %. In all cases, correct detection rate was 98.9% and above.

DISCUSSION

A geometrical attack of a watermarked image may involve one or more of the following: altering the image background (cropping, translation), resizing the image foreground (scaling, resizing, cropping, translation…), and altering the form of its foreground (skewing, rotation, reflection…). Experiments of the proposed method confirm that altering the image background doesn't affect the embedded watermark because it uses image main objects (foreground) for watermark embedment rather than its background. At the same time resizing the image main objects causes the distances between watermark embedding points to be changed while keeping the cross ratio of these distance without any change. This allows for recovering these locations even if an image was attacked. If an image foreground form is skewed, rotated, or reflected, then the locations of the indicated image invariant feature points will be changed accordingly, making it possible to find these points and to recover a watermark by following the same watermark detection algorithm.

In contrast experimental results of Pantuwong 2005[9] show that by using a detection threshold of 3, when planar projection is applied, the overall false positive detection rate was 0.16%, while the overall false negative rate was 1.2%, and a correct detection rate ranging from 98.6 to 92% depending on the used pictures. No results were provided for the cases of cropping, translation, resizing, skew, or reflection. That method was based on image center of area in addition to image corner points and diagonals, which may be altered if the watermarked image is translated or cropped, making the embedded watermark unrecoverable.

In comparison with other methods our watermarking scheme has the advantages of an exclusive use of image invariant features under various geometrical attaches, and a use of a combination of known, and newly defined -by the author- features, background subtraction, invariant theory of collinear and coplanar points, and public key technology. This is very important as most of attacks on image and video watermarks are geometrical, and in our case it allowed for significant improvement of watermarking immunity against geometrical attacks.

CONCLUSION

In the current study, we have presented an enhanced approach for main-object oriented feature-based geometry invariant watermarking. The proposed approach extends the existing approaches of partial use of image invariant features by an exclusive use of these features for image main objects and introducing new image invariant features such as an image centroid. It also incorporates a combination of image processing techniques, invariant theory of geometry, and public key encryption to allow for a construction of a one-way function that is able to verify the private watermark. The experimental results showed a high rate of watermark detection in watermarked images that were exposed to various geometrical alterations. As one might expect, this proved to be robust to changes such as scaling, reflection, translation, skewing, cropping, and rotation.

REFERENCES

1. Pérez-González, F. and J. R. Hernández, 1999. A tutorial on digital watermarking. Proc. 33rd IEEE Annual Carnahan Conf. Security Tech., Madrid, Spain.
2. Chotikakamthorn, N. and N. Pantuwong, 2005. Attacks on feature-based affine-invariant watermarking methods. Proc. 2005. The Fifth Int. Conf. Computer and Information Tech. (CIT'05).
3. Alghoniemy, M. and A.H. Tewfik, 2000. Geometric distortion correction through image normalization. Proc. Int. Conf. Multimedia and Expo, 2000.
4. Oruanaidh, J., T. Pun and Rotation, 1998. Scale and translation invariant spread spectrum digital image watermarking. Signal Processing, 66: 303-317.
5. Pereira, S. and T. Pun, 2000. Robust template matching for affine resistant image watermarks. IEEE Transactions on Image Proc., pp: 1123-1129.
6. Bas, P., J-M. Chassery and B. Macq, 2002. Geometrically invariant watermarking using feature points. IEEE Trans. on Image Proc. 11: 1014-1028.
7. Cox, I. J., M.L. Miller and J. A. Bloom, 2002. Digital Watermarking. Morgan Kaufmann Publishers.
8. Chotikakamthorn, N. and W. Yawai, 2004. Digital watermarking technique for perspective image, Proc. Int. Conf. Control. Automation and Systems 2004.
9. Pantuwong, N. and N. Chotikakamthorn, 2005. Comparative study of two projective-invariant digital watermarking methods using cross-ratios and line intersections. Proc. 2005 The Fifth Int. Conf. Computer and Information Tech. (CIT'05).
10. Hayman, E. and J-O. Eklundh, 2003. Statistical background subtraction for a mobile observer, computational vision and active perception laboratory (cvap). Ninth IEEE Int.Conf. Computer Vision (ICCV'03) 1: 67.
11. Franti, P. and T. Kaukoranta, 1999. Binary vector quantizer design using soft-centroids. Signal Processing: Image Communication, 14: 677-681.
12. Abdel-Hamid, A. T., S. Tahar, and A. El-Mostapha, 2005. A public-key watermarking technique for ip designs proceedings of the design. Automation and Test in Europe Conf. Exhibition (DATE'05) , Universit´e de Montr´eal, Montr´eal, Canada, 1530-1591/05.