# Geometric Robust Watermarking Based on a New Mesh Model Correction Approach

*Ping Dong, Jovan G. Brankov, Nikolas Galatsanos, and Yongyi Yang*

Illinois Institute of Technology
Department of Electrical and Computer Engineering
3301 S. Dearborn St., Chicago, IL 60616, USA

## ABSTRACT

*While geometric attacks are one of the most challenging problems in watermarking, random bending is probably the most difficult to handle among all geometric attacks. In this paper, we present a watermarking scheme based on a new deformable mesh model to combat such attacks. The distortion is corrected using the distortion field (DF) estimated by minimizing the matching error between the meshes of the original and attacked image. A CDMA watermarking method is used for testing the proposed method, which embeds a multi-bit signature in the DCT domain and uses mesh model correction to achieve robustness. Experiments show that the proposed scheme can survive wide range of random bending attacks.*

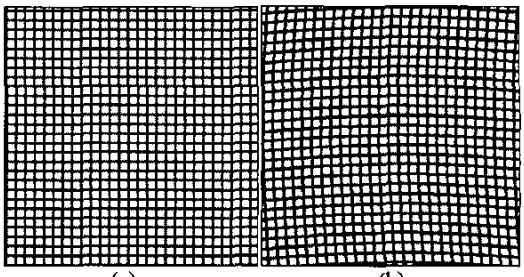
## 1. INTRODUCTION

Geometric attacks are still one of the most difficult problems in watermarking. Such attacks destroy the synchronization of the watermark signals embedded in cover images by introducing global and local changes to the image coordinates. To extract the watermark message correctly, resynchronization is usually a necessary pre-processing step.

Many approaches have been reported to combat the global geometric attacks, such as Fourier-Mellin transform based rotation, scale and translation (RST) invariant watermarking [1][2], and template based affine resistant watermarking [3]. Since global geometric attacks can be modeled by transforms that can be described by a few parameters, for example, the general affine transforms can be modeled by 6 parameters, resynchronization is usually possible through parameter estimation or registration.

Random geometric distortions are much more difficult to correct than distortions caused by RST or affine transforms. The freedom of random attacks can be unlimited theoretically, or too large for any parameter estimation algorithms. One such attack applied by StirMark [4] is demonstrated in Fig.1, where Fig.1(a) shows the rectangular image grid, while Fig.1(b) is the distorted grid by StirMark. Such attacks may cause almost unnoticeable perceptual distortion in the image, but can defeat most, if not all, of the existing watermarking algorithms.

In this paper, we present a watermarking scheme which is robust to random geometric distortions. According to this scheme resynchronization is achieved through a new deformable mesh model for distortion correction. A similar watermarking scheme was proposed independently in [7]. However, the scheme in [7] estimates the distortion field (DF) using the objective function in [6]. In this paper we propose a new objective function to estimate the DF. This objective function consists of two terms. The first term captures the matching error between the original and the attacked watermarked image, and the second term captures the regularity of the DF. This new objective function forces the smoothness of the DF, instead of mesh regularity, so that it can capture effectively the distortion in the attacked image. The estimated DF is then used for distortion compensation. We apply a CDMA based multi-bit watermarking scheme [5] for the embedder, by virtue of its property of high robustness to common signal processing operations. We present numerical experiments that demonstrate the advantages of DF based correction of geometric distortions for watermarking over a range of watermark strengths and geometric distortions. Our numerical experiments also demonstrate that proposed DF estimation approach yields better results than the approach used in [7].



(a) (b)

Fig. 1 (a) Rectangular grid, and (b) grid after attack by random bending.

## 2. MESH MODEL BASED CORRECTION

### 2.1. Mesh model of the Distortion field.

Let $\mathbf{d}(\mathbf{p})$ denote the distortion vector at location $\mathbf{p}$ in the image domain $D$. Let $f_{ref}(\mathbf{p})$ and $f_{targ}(\mathbf{p})$ denote, respectively, the image functions of a reference frame and a distorted frame, also called the target frame. If the distortion is unique (1 to 1) mapping, a perfect

match can be achieved, e.g. $f_{targ}(\mathbf{p}) = f_{ref}(\mathbf{p}+\mathbf{d}(\mathbf{p}))$. In deformation estimation the goal is to estimate $\mathbf{d}(\mathbf{p})$ so that the best match between the frames is achieved.

Next, we introduce the mesh modeling of the DF. The image domain $D$ is partitioned into $M$ non-overlapping mesh elements, denoted by $D_m$, $m = 1,2,\ldots,M$. The DF is then derived from the inter-frame displacements of the associated mesh nodes. Over a particular element $D_m$, the DF can be described as:

$$\mathbf{d}(\mathbf{p}) = \sum_{n=1}^{N} \varphi_n(\mathbf{p})\mathbf{d}_n \qquad (1)$$

where $\mathbf{d}_n$ and $\varphi_n(\mathbf{p})$ are the displacement vector and interpolation basis function associated with node $n$, respectively, and $N$ is the total number of mesh nodes. Note that the support of each basis function $\varphi_n(\mathbf{p})$ is limited only to those reference frame elements $D_m$ associated with node $n$.

Let the nodal positions in the mesh structure of the reference frame be denoted by $\mathbf{P}_{ref} = [\mathbf{p}^1_{ref}, \mathbf{p}^2_{ref}, \cdots \mathbf{p}^N_{ref}]$, and similarly by $\mathbf{P}_{targ} = [\mathbf{p}^1_{targ}, \mathbf{p}^2_{targ}, \cdots \mathbf{p}^N_{targ}]$ for the nodal positions in the target frame. Then the nodal values of DF mesh model are given by:

$$\mathbf{d}_n = \mathbf{p}^n_{targ} - \mathbf{p}^n_{ref}, n = 1,2,\cdots,N \qquad (2)$$

In Fig. 2 we show an example of a distorted mesh element from a reference to a target frame.

### 2.2. Deformation of the mesh

In practice the nodal vectors $\mathbf{d}_n$ in the deformation mesh model in (1) are unknown, and must be determined from the observed data. To estimate the distortion between image frames, a natural approach is to displace the mesh nodes so that the corresponding image intensity function over mesh elements in the two frames achieve the best match in terms of their image values.

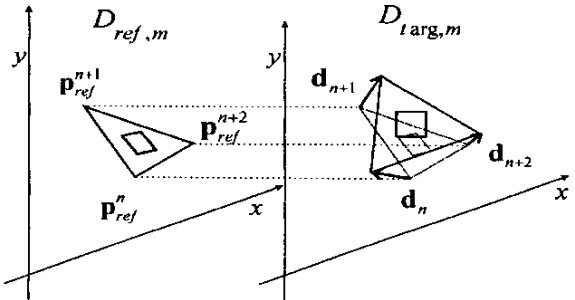



Fig 2. Inter frame displacement estimation using deformable mesh model.

As a matching criterion the following objective function is used:

$$J = \frac{1}{2}\sum_{m=1}^{M}\left[\int_{D_m}\left(f_{targ}(\mathbf{p}+\mathbf{d}(\mathbf{p})) - f_{ref}(\mathbf{p})\right)^2 d\mathbf{p}\right] + \beta E_d \qquad (3)$$

where the first term is the matching error accumulated over all $M$ mesh elements between the two frames [6]. The second term $E_d$ is a measure of DF regularity which we define as:

$$E_d = \frac{1}{2}\sum_{n=1}^{N}\left\|\mathbf{d}_n - \bar{\mathbf{d}}_n\right\|^2 \qquad (4)$$

where $N$ the total number of is mesh nodes in the image, and $\bar{\mathbf{d}}_n$ is the average displacement of the immediate neighboring mesh nodes connected to node $n$. The parameter $\beta$ in (3) controls the trades-off between mesh matching accuracy and the DF smoothness. This penalty term is different from the one in [6] which was used in [7]. The idea of our penalty term is to enforce a smooth DF rather than mesh regularity (evenly spaced nodes). In this application a regular mesh is used for the reference frame. Thus, the effect of this new penalty term is more pronounced toward the image boundaries.

The values of the nodal vectors $\mathbf{d}_n$ are then found numerically by minimizing the objective function in (3) with a gradient descent algorithm. In this paper the optimization algorithm in [6] was modified by applying a line search using quadratic interpolation along the gradient direction [8].

### 2.3. Mesh generation

In our application the DF was independent of the image content and vary smoothly across the image domain. Thus the mesh structure generation was independent of the image content. Specifically, mesh nodes were placed regularly 64 pixels apart in each direction. In addition, to avoid boundary effects, the image was extended by 64 pixels in each direction. The values of those pixels were set to the mean of the whole image.

### 2.4. Deformation compensation

After obtaining the DF estimate the deformation compensation (DC) was performed. This can be represented by the following equation:

$$f_{DC}(\mathbf{p}) = f_{targ}(\mathbf{p}+\mathbf{d}(\mathbf{p})) \qquad (5)$$

## 3. MESH MODEL BASED WATERMARKING SCHEME

### 3.1. CDMA Watermark

Suppose the watermark message is a binary sequence denoted by $m = \{b_i \mid b_i \in \{0,1\}\}, i=1,2,\cdots,L$ where $L$ is the length of the watermark sequence. Usually we use

$m' = \{b'_i \mid b'_i = 1 - 2b_i, i = 1 \cdots L\}$, So $m'$ is a binary polar sequence of {-1,1}. The pseudo-random noise pattern is defined as $P = \{p_{i,j}(k) \mid k = 1, \cdots, L\}$, where $p_{i,j}(k)$ is 2-D pseudo-random binary sequence of {-1,1} with zero mean, generated using the key as the seed. The size of $p_{i,j}(k)$ is the same as cover image.

The CDMA watermark is descried as:

$$w_{i,j} = \sum_{k=1}^{L} p_{i,j}(k) b'_k . \quad (6)$$

The CDMA watermark can be embedded into a cover image additively by

$$\tilde{v}_{i,j} = v_{i,j} + \lambda \cdot w_{i,j} \quad (7)$$

where

$v_{i,j}$ : pixel value of cover image at location $(i, j)$,

$\tilde{v}_{i,j}$ : corresponding pixel values of the watermarked the image at $(i, j)$,

$\lambda$ : a positive coefficient that defines the watermark strength.

A simple detection can be performed using a correlation detector. The correlation is calculated as:

$$C_l = \sum_{i,j} p_{i,j}(l)\tilde{v}_{i,j} = \sum_{i,j} p_{i,j}(l)v_{i,j} + \lambda \sum_{i,j} p_{i,j}(l)w_{i,j}$$

$$\approx \lambda \sum_{k=1}^{L} \sum_{i,j} b'_k p_{i,j}(k)p_{i,j}(l) \approx \lambda \sum_{i,j} b'_l \cdot | p_{i,j}(l) |^2 . \quad (8)$$

In the above derivation, $p_{i,j}(l)$ is a zero mean pseudo-random binary sequence of {-1,1}, and it is independent with $v_{i,j}$. Therefore, the term $\sum_{i,j} p_{i,j}(l) \cdot v_{i,j}$ is close to zero. Other terms are also nearly zero when $k \neq l$ because pseudo-random patterns $p_{i,j}(k)$ are uncorrelated with each other. So the watermark message can be estimated as:

$$\hat{b}'_l = sign(C_l) \quad (9)$$

### 3.2. Watermarking scheme

The deformable mesh model based watermarking system is shown in Fig.3. To demonstrate the idea, we show some results in Fig.4 using an example, where the original image is shown in (a) and the watermarked is shown in (b). The attached image is shown in (c). In (d) the difference between the original and the attacked image is shown, which illustrates the distortion caused by bending using StirMark 3.1. In (e) the regular mesh is overlaid with the mesh generated from the attacked image. From these two meshes, the distortion field can be computed and is shown in Fig.5. The distortion compensated image is shown in Fig.4 (g). In Fig.4 (h) we show the difference between the original and the distortion compensated image. We can see that most of the geometric distortion has been compensated for.

## 4. EXPERIMENTS

A watermark message of 200 bits is embedded into the mid-range DCT coefficients of the Lena image, shown in Fig. 4(a), using the CDMA algorithm detailed in section 3.1. A number of experiments were performed to test the proposed watermarking system. In all the experiments, $\beta = 10,000$ was used and the original non-watermarked image was used as a reference for the distortion correction. The bit error rate (BER) is calculated as the number of incorrectly decoded bits divided by total number of bits in the watermark message. For comparison, the method proposed in [7] which used a mesh regularity penalty was also tested and the value of the penalty term parameter was optimized empirically.

### 4.1. BER vs. bending strength

In this experiment, the watermark strength was fixed at $\lambda$=0.5. The test results are shown in Fig.6. From these results we can see that as the bending strength increases, the BER also increases. Our mesh model based correction is very effective for modest amounts of bending. Furthermore, is clear that the proposed DF estimation approach is more effective than the approach used in [7].

### 4.2. BER vs. watermarking strength

The bending strength was fixed at 5 in this experiment, and watermarking strength $\lambda$ is varied from 0.1 to 1.0. The test results are given in Fig. 7. With the proposed correction nearly error-free decoding can be achieved when the watermarking strength $\lambda$ is close to 1.0. Again, the proposed approach achieves the best performance.

## 5. CONCLUSION

In this paper, a watermarking approach robust to geometric attacks was presented. This approach is based on a deformable mesh model. Although only random bending attacks were considered in our experiments, the proposed system can also be applied to combat other geometric attacks.

## 6. REFERENCES


[1] J. O'Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal Processing*, vol. 66, no. 3, pp. 303-317, 1998.

[2] C. Y. Lin, M. Wu, etc, "Rotation, Scale, and Translation Resilient Public watermarking for images," in *IEEE Trans. on Image Proc.*, vol. 10, no.5, May 2001

[3] S. Pereira and T. Pun, "Robust template matching for affine resistant image watermarks," in *IEEE Trans. on Image Proc.*, vol. 9, no. 6, June, 2000.

[4] F. A. P. Petitcolas. In StirMark 3.1, 1999. http://www.cl.cam.ac.uk/fapp2/watermarking/stirmark/

[5] I.J. Cox, J.Kilian, F.T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. on Image Proc.*, vol. 6, no. 12, 1997.

[6] Y. Wang and O. Lee, "Active mesh-a feature seeking and tracking image sequence representation scheme," *IEEE Trans. Image Proc.*, vol. 3, pp. 610-624, 1994.
[7] F. Davoine, "Triangular Meshes: A Solution to Resist to Geometric Distortions Based Watermark-Removal Softwares", *European Signal Processing Conference*, Tampere, Finland, 2000.
[8] S. Nash and A. Sofer, *Linear and Nonlinear Programming*, McGraw Hill 1996.

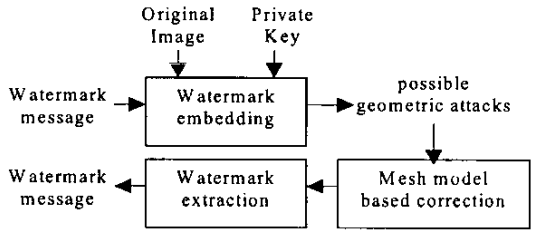



Fig. 3 Mesh model based watermarking system

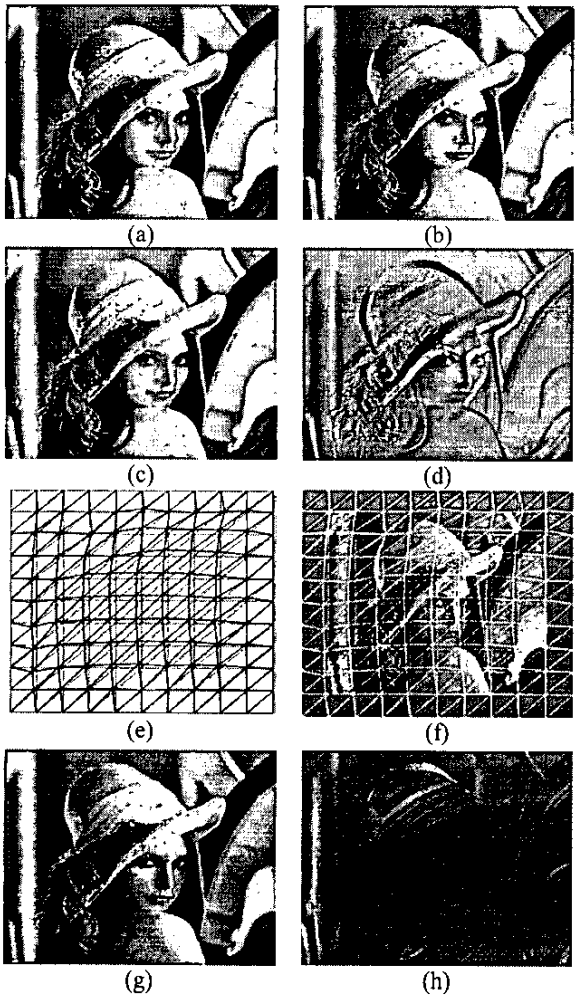



Fig 4. Images to demonstrate the watermarking process (a) Original image (b) Watermarked image with PSNR=38.4dB (c) Attacked watermarked image; (d) Difference between (b) and (c); (e) Regular mesh and mesh generated from (c); (f) Meshes of (e) overlayed on the Leena image; (g) Deformation compensated watermarked image; (h) Difference between (a) and (g).

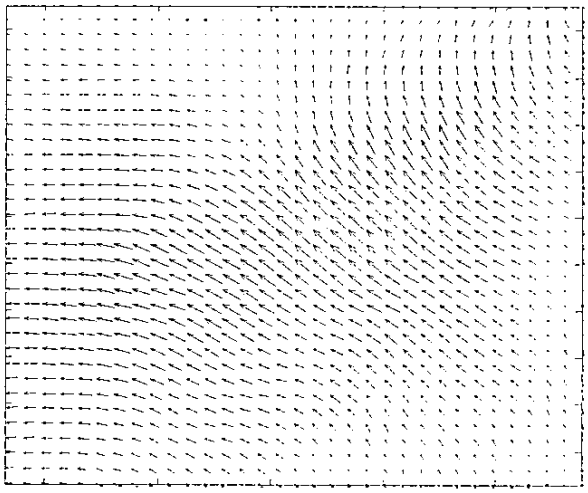


Fig. 5 The estimated distorion field

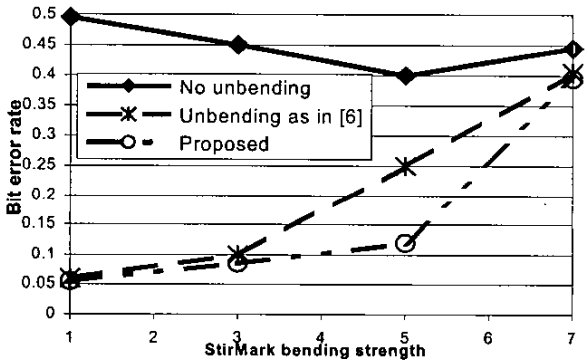



Fig.6 BER vs. random bending strength

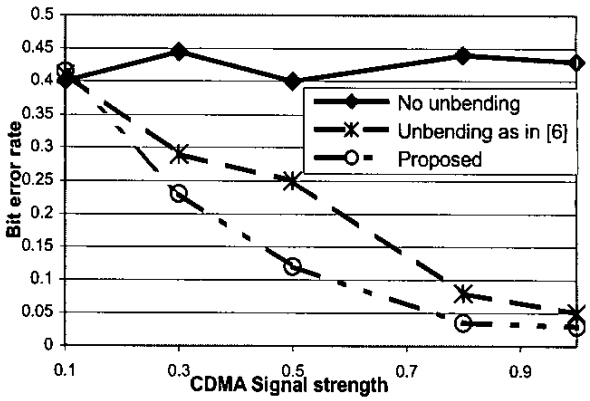



Fig.7 BER vs. watermark strength