WATERMARKING COLOR HISTOGRAMS

Sujoy Roy

School of Computing
National University of Singapore
sujoyroy@comp.nus.edu.sg

Ee-Chien Chang

School of Computing
National University of Singapore
changec@comp.nus.edu.sg

ABSTRACT

In this paper we give a method for watermarking color histograms. Color histograms have been known [3] to be robust to rotations and other geometric transformations. If the watermark can be embedded in such geometry invariant representations it should survive geometric transformations. The difficulty in watermarking color histograms is that they have a non-linear relationship with the pixel representation. Therefore it is not clear how to get a watermarked image given its watermarked histogram. We give a method for watermarking color histograms that uses Earth Mover Distance (EMD) to modify an image to a target histogram. We conduct extensive experiments to test our method.

1. INTRODUCTION

One of the requirements of effective watermarking is that it should be robust to standard signal processing operations and geometric transformations. Although several methods for watermarking have been proposed in the existing literature very few actually satisfy this requirement. Out of the several suggested solutions, the watermarking of geometry invariant features of multimedia data seems to be a promising area to explore. Feature representations give a compact description of multimedia objects and there are a vast range of such features, particularly for images[1], which can be either linear or non-linear representations. Many of the non-linear feature representations, for example, points, edges, histograms etc, have been proved to be robust to several geometric transformations and are thus likely to retain the watermark under such transformations. In this paper we are interested in watermarking one such commonly used feature, namely color histograms.

The problem associated with watermarking such non-linear feature representations, like color histograms is that, it is not clear how to get back the watermarked image from their watermarked feature representations. In other words, watermarking of these non-linear features, although desirable, is not easy to realize. Although some histogram specification techniques may be used it is not clear how to meet the constraint on low perceptual distortion as desired in watermarking and at the same time get an optimized solution for any kind of watermark.

Methods for watermarking histograms of images have been proposed in the existing literature [1, 4]. In this paper we give a general method for watermarking color histograms of images. Our method solves this general problem: given an image I and a target histogram $\widetilde{H}$, we intend to find another image $\widetilde{I}$ perceptually similar to I, whose histogram is $\widetilde{H}$. To minimize distortion between I and $\widetilde{I}$ we use EMD to guide the reconstruction process. Using the above construction, we can easily adapt any known watermarking technique, viz. spread spectrum method, with color histograms. For example, we can embed a random signal directly into the histogram.

Main contribution: In this paper we give an algorithm for watermarking non-linear features of images, namely, color histograms. Our algorithm is based on constrained Earth Mover Distance (EMD) optimization that modifies an image to a target histogram. We conduct extensive experiments to test the efficacy of our proposed method.

2. FORMULATION

Given an image I and a modified histogram $\widetilde{H}$, we are interested to find an image $\widetilde{I}$ which is perceptually similar to I and whose histogram is $\widetilde{H}$. According to this formulation, although the histogram $\widetilde{H}$ can be any histogram, as a special case it can be seen as a modified or watermarked version of the original histogram $H = F(I)$, where $F(I)$ gives the color histogram for the image I. Hence $\widetilde{H}$ can be called the *watermarked histogram* and $\widetilde{I}$ the *watermarked image*.

The modified histogram $\widetilde{H}$ is obtained from H by some watermarking method. Note that under our formulation the watermarking method used is not the concern of this pa-

[1] In this paper we will be explaining all our examples and tests on images. With suitable modifications the same is applicable to other multimedia objects like video and audio.

0-7803-8554-3/04/$20.00 ©2004 IEEE.

per. We are concerned about the reconstruction of the watermarked image.

Remark:

- As $H = F(I)$ is a non-linear function over I, it is not clear how to find a watermarked image $\widetilde{I}$ given the watermarked histogram $\widetilde{H}$, i.e., $\widetilde{I} = F^{-1}(\widetilde{H})$ is difficult to realize.
- how to ensure that the perceptual difference from I to $\widetilde{I}$ is small is also not clear
- the watermarked histograms bin-values can not be negative.

The next section gives a brief review of Earth Mover Distance (EMD) which we use to address the above concerns.

3. EARTH MOVER DISTANCE

The earth mover distance is a distance measure between discrete, finite distributions and can be formalized as the following linear programming problem:

Let $P = (p_1, w_{p_1}), \cdots (p_m, w_{p_m})$ be the original histogram with m bins, where the *bin representative* p_i is a color, and w_{p_i} is the number of pixels in that bin; $Q = (q_1, w_{q_1}), \cdots (q_n, w_{q_n})$ is another histogram with n bins.; and $\mathbf{D} = [d_{ij}]$ the *ground distance* matrix where d_{ij} is the perceptual distance between the representative p_i and q_j. A flow f_{ij} is the number of pixels transferring from p_i to q_j, and the cost of moving a pixel from p_i to q_j is the distance d_{ij}. We want to find the overall flow $\mathbf{F} = [f_{ij}]$ that minimizes the overall cost

$$cost(P, Q, F) = \sum_{i=1}^{m}\sum_{j=1}^{n} d_{ij} f_{ij},$$

subject to the constraints:

$$f_{ij} \geq 0 \quad 1 \leq i \leq m, 1 \leq j \leq n$$

$$\sum_{j=1}^{n} f_{ij} = w_{p_i}, \quad 1 \leq i \leq m$$

$$\sum_{i=1}^{m} f_{ij} = w_q, \quad 1 \leq j \leq n$$

$$\sum_{i=1}^{m}\sum_{j=1}^{n} f_{ij} = \min\left(\sum_{i=1}^{m} w_{p_i}, \sum_{j=1}^{n} w_{q_j}\right),$$

The flow matrix $\mathbf{F}$ tells us how to transform a histogram P to another histogram Q using minimum cost, and thus indicates a way to change the pixel values of the original image to obtain the watermarked image. Because the cost is minimized, the differences between the original and watermarked image will be minimized. The earth mover distance is solved as a transportation simplex problem.

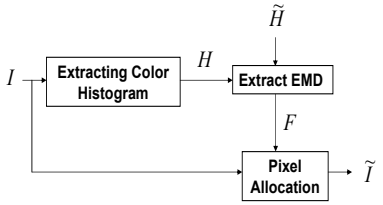


Fig. 1. Schematic diagram of watermark embedding process.

4. PROPOSED METHOD

Our proposed method for watermarking color histograms can be divided into two stages (1) embedding and (2) detection. The embedding stage can be divided into three substages, namely, extracting the histogram from an image, watermarking it to generate a watermarked histogram and then reconstructing the watermarked image. Figure 1 gives a schematic diagram of the watermark embedding process.

Embedding: The 2D-CbCr color histogram H of an image I is extracted. This is watermarked using a spread spectrum technique to give $\widetilde{H} = H + W$, where W is the watermark vector (a Gaussian i.i.d. signal) whose size is same as that of H (details in Algorithm 1). The constrained EMD between H and $\widetilde{H}$ gives a flow matrix F. For discussion on the constraint used refer Section 4.1. Pixels in I are reallocated according to F to get the watermarked image $\widetilde{I}$.

Detection: Given an image I' which has undergone some geometric transformations, the detection process involves finding the correlation between the watermark W and the histogram H' extracted from I'. A watermark is detected (Yes) if the correlation value is greater than a pre-defined threshold i.e. $\sum(H' \cdot W) > \delta$, where δ is the threshold.

4.1. Ensuring Perceptual Similarity

We have to ensure that the distortion between I and $\widetilde{I}$ is small. In our proposed method we achieve this by setting the weights within a band around the diagonal of the distance matrix (refer Section 3) to zero. Note that by enforcing this constraint, triangular inequality is violated. Triangular inequality states that: given a triangle ABC, the distance AB+BC is greater than AC. Therefore, for going from A to C path AC should be preferred over the path

Algorithm 1: Watermarking Color Histograms

Input: Original Image I, 2-D watermarked color histogram $\widetilde{H} = \{\widetilde{h}_{11}, \ldots, \widetilde{h}_{ij}, \ldots, \widetilde{h}_{mn}\}$ where size of $\widetilde{H}$ is m by n.
Output: Watermarked Image $\widetilde{I}$

Step 0: Extract $H = F(I)$, where $H = \{h_{11}, \ldots, h_{ij}, \ldots, h_{mn}\}$ is the 2D CbCr-color histogram of the image I. Normalize H.

Step 1: Note that the watermarked histogram $\widetilde{H}$ was obtained by

$$\widetilde{h}_{ij} = \begin{cases} h_{ij}(1 + \gamma w_{ij}) & \text{if} \quad h_{ij} > 0 \\ h_{ij} & \text{if} \quad h_{ij} = 0, \end{cases}$$

where $W = \{w_{11}, \ldots, w_{ij}, \ldots, w_{mn}\}$ is the watermark, γ is a constant such that $|\gamma w_{ij}| < 1$, $1 \leq i \leq m$ and $1 \leq j \leq n$.

Step 2: Normalize $\widetilde{H}$ and scale it by the number of pixels in the original histogram. Adjust the number of bin values such that $sum(H) = sum(\widetilde{H})$, where $sum(H)$ gives the total number of pixels in image I.

Step 3: Find the EMD between H and $\widetilde{H}$. This gives the flow matrix F between H and $\widetilde{H}$.

Step 4: Use F to generate $\widetilde{I}$ from I by changing the colors in I accordingly.

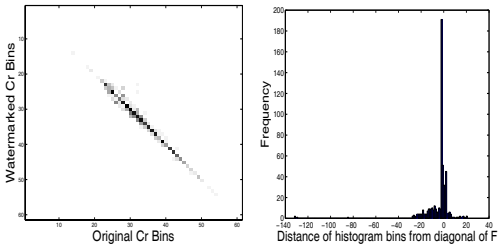
AB+BC. A violation of this rule would involve preferring the path AB+BC over AC. Similarly in a histogram if bin B lies between bin A and C, according to triangular inequality, the EMD (based on transportation simplex optimization) is supposed to prefer a flow from A to C over a flow from A to B and then B to C. In our method we ensure that this is violated and flow from A to B and B to C is preferred. This is because we want exchange of pixels between neighboring bins to take place.

Ideally, the width of the band should be the just noticeable distance (JND). Here, we choose it to be 5 bins based on experimental results. Figure 2(a) shows an image of the flow matrix. Note that the flow takes place mostly within a band around the diagonal of the matrix (Figure 2(b)). Hence, the flow between bins is limited to neighboring colors and this ensures perceptual similarity.

5. EXPERIMENTS

We conducted similar experiments on 100 images to test the robustness of our watermarking method. In this section we perform two experiments. In the first experiment we analyze the watermarking process to generate $\widetilde{I}$. In the second experiment we test the accuracy of our watermarking method to standard manipulations like rotation, scaling, cropping, JPEG compression and additive Gaussian noise.

Experiment 1: Our goal here is to modify the image in Figure 3(a), given the modified 2D-CbCr histogram in Figure 3(d) to get a watermarked image. In our experiment the modified histogram was generated by adding the watermark in Figure 3(e) to the 2D-CbCr histogram (Figure 3(c)) of Figure 3(a). The embedding is done using a simple additive spread spectrum method. We use EMD to the find the flow between the histograms in Figure 3(c) and Figure 3(d). The flow matrix for the Cr-bins is shown in Figure 2(a). Using a constrained EMD optimization ensures that the pixel flow is between neighborhood bins only. Using the flow matrix we modify pixels in the original image to get the watermarked image given in Figure3(b). Note that the original and watermarked image are perceptually similar.



(a) (b)

Fig. 2. (a) Flow matrix F indicating the flow of pixels from I to $\widetilde{I}$. The x-axis and y-axis represent the non-zero Cr-bins of I and $\widetilde{I}$ respectively. Here we have 61 bins. The value at the location $F(i, j)$ gives the flow of pixels between the i^{th} Cr-bin of H and the j^{th} Cr-bin of $\widetilde{H}$. Note that the exchange of pixels is mostly between neighboring bins. (b) Distribution of bin values about the diagonal of F, where "0" on the x-axis indicates the diagonal. To the right is the upper triangle of F and to the left is the lower triangle of F.

	Value	Acc.	Value	Acc.
Rotation	25^o	100	40^o	100
Cropping	20%	100	60 %	95
Scaling	2	100	4	96
Noise (AWGN)	2	100	4	95
JPEG Compr.	+35dB	100	+30dB	92

Table 1. Performance of Color Histogram Watermarking. Detection accuracy (% Acc.) for 100 images rotated by an angle 25^o and 40^o, scaled down by a factor of 2 and 4, cropped by a factor of 20% and 60%, gaussian noise added of strength 2 and 4 and JPEG Compressed with PSNR $+35dB$ and $+30dB$.

Experiment 2: Here we study the behavior of our watermarking method to geometric transformations like rotation, scaling, and other operations like cropping, adding Gaussian noise and JPEG compression. A few examples of transformed watermarked images and their corresponding histograms are shown in Figure 4. In all these cases the watermark was successfully detected. Table 1 gives the performance of histogram watermarking to several amount of

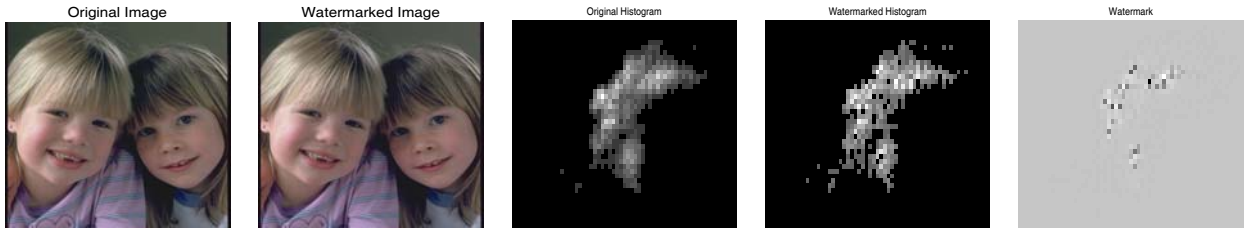


Fig. 3. (a) Original Image (b) Watermarked Image (c) Original Histogram (d) Watermarked Histogram (e) Watermark

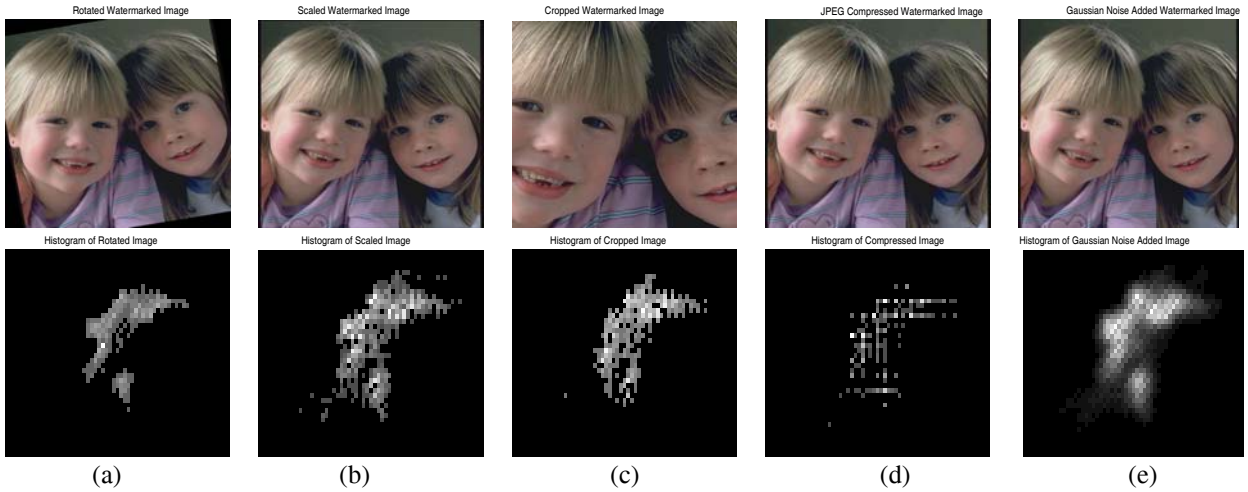


Fig. 4. **Row 1:** (a) Watermarked Image rotated by 10^o. (b) Watermarked Image scaled up by factor of 4. (c) Watermarked Image Cropped by 20%. (d) Watermarked Image JPEG compressed with PSNR $+31.90\ dB$. (e) Gaussian White Noise of strength 2 added to Watermarked Image. **Row 2:** Corresponding (a) Histogram of Rotated Image. (b) Histogram of Scaled Image. (c) Histogram of Cropped Image. (d) Histogram of JPEG Compressed Image. (e) Histogram of Image added with Gaussian white noise.

rotation, scaling, cropping, JPEG compression and additive Gaussian noise on the 100 images. The number of correct detections (correlation value above a predefined threshold) determines the accuracy. The threshold is determined using the formula in [2]. We observe from the experiments that color histogram watermarking works particularly well for rotated, scaled, cropped and gaussian noise added images. Detection accuracy is reasonably good with JPEG compressed images for higher PSNR values.

6. CONCLUSION

In this paper we have given a method for watermarking color histograms. We use a constrained Earth Mover Distance (EMD) optimization to modify an image to a target histogram. The use of constrained EMD helps in ensuring that the image and its watermarked version are perceptually similar. Thus we present a watermarking method that successfully watermarks non-linear features of images.

7. REFERENCES

[1] D. Coltuc and P. Bolon. Color image watermarking in HSI space. In *ICIP*, September, 2000.

[2] A. Piva, M. Barni, E. Bartoloni, and V. Capellini. Threshold selection for correlation-based watermark detection. In *Proceedings of COST 254 Workshop on Intelligent Communications*, 1998.

[3] M. J. Swain and D. H. Ballard. Color indexing. *International Journal on Computer Vision*, 7(1):11–32, 1991.

[4] P. Tsai, Y. C. Hu, and C. C. Chang. A color image watermarking scheme based on color quantization. *Signal Processing*, 84:95–106, 2004.