Robust Watermarking of Facial Images Based in Salient Geometric Pattern Matching

Athanasios Nikolaidis
Ioannis Pitas, Senior Member, IEEE
IEEE Trans. on Multimedia 2000
Outline

- Introduction
- System Overview
- Face Segmentation and Salient Feature Localization
- Watermark construction
- Watermark Embedding
- Watermark Detection
- Experimental Results
- Conclusion
Robust watermarking try to survive in many attacks:
- Geometric transform
- Filtering/Compression

Defects of most of the existing methods
- Customized for some attack resistance
- Can’t survive on most commonly considered attacks
For wider range of attacks

[Maes 98] Digital watermarking by geometric warping
  - Slightly change the geometric feature
  - Line segments watermarks
For wider range of attacks

- [Maes 98] Digital watermarking by geometric warping
  - Slightly change the geometric feature
  - Line segments watermarks

Computationally Feasible?
Point Selection?
Some more defects

- When watermark is embedded on the entire image
  - Scaling, rotation, or cropping may result in destruction of the watermark
  - No salient features is used to detect the watermark (for locating the watermark)
To achieve this

- In this paper, they use some salient pattern matching
  - For a certain class of special interest—frontal face images
- Two important characteristics in this class
  - Contains several salient features (e.g., eyes and mouth)
  - Application on Copyright protection
System Overview

Embed

Frontal Face Image → Feature Detection and Matching → Watermark construction and Embedding → Embedded Image

Detect

Suspicious Image → Feature Detection and Matching → Watermark Matching
Face Segmentation and Salient Feature Localization

Fig. 2. Face segmentation and salient feature localization.
Face segmentation

- Use skin color to detect face
  - On HSV color domain
    - $0 \leq H \leq 25$ or $335 \leq H \leq 360$
    - $0.2 \leq S \leq 0.6$
    - $0.4 \leq V$

- Approximate ellipse of face region
  - Alpha trimmed mean radial basis function
    (Trim some percentage of observation to calculate mean)

\[
\hat{\mu}_k = \frac{N_k - \alpha_k N_k}{N_k - 2\alpha_k N_k} \sum_{i=\alpha_k N_k}^{N_k} X(i)
\]

$X$: data coordinate sorting by the distance to the center
$\mu_k$: kth potential object center
$N_k$: number of data belong to the kth center
Face segmentation

- Use skin color to detect face
  - On HSV color domain
    - $0 \leq H \leq 25$ or $335 \leq H \leq 360$
    - $0.2 \leq S \leq 0.6$

- Approximate ellipse of face region
  - With Alpha trimmed mean radial basis function
    - Trim some percentage of observation

\[
\hat{\mu}_k = \frac{\sum_{i=\alpha_k N_k} X(i)}{N_k - 2\alpha_k N_k}
\]

$X$: data coordinate sorting by the distance to the center
$\mu_k$: kth potential object center
$N_k$: number of data belong to the kth center
Salient Feature Localization

- Eyes and mouth detection
  - Match templates by assuming intensity difference and volume ratio

![Diagram showing eye and mouth templates with parameters r1, r2, r3, c, and ε.](image-url)
Watermark construction

- Generate watermark sequences and then set threshold to be binary sequences

\[ z(n + 1) = \lambda z(n) \mod 2\pi, \quad z(n) \in U, \lambda \in R \quad (10) \]

Fig. 3. (a) The 16 × 16 Peano curve. (b) Watermark produced by raster scan. (c) Watermark produced by Peano scan.
Outline

- Introduction
- System Overview
- Face Segmentation and Salient Feature Localization
- Watermark Construction
- Watermark Embedding
- Watermark Detection
- Experimental Results
- Conclusion
Watermark Embedding

Feature set $\mathcal{F}$

Mass center and embedding region size computation

Scaling and centering

Rotation by $-\theta$

Visual masking

$X_0$ to $X_w$
Watermark Embedding

★ Geometric watermark adaptation
★ Prototype watermark – $2^n \times 2^n$
★ Scaled watermark – $K_1 \times K_2$
★ Nearest-neighbor interpolation

$$K_1 = k \left( x_{(moulh)} - x_{(eyes)} \right)$$
$$K_2 = l \left( y_{(right\_eye)} - y_{(left\_eye)} \right)$$

★ Centered watermark

$$F' = \left\{ F_i, i = 1, \ldots, M \right\} :$$

$$\left( \bar{x}, \bar{y} \right) = \left\{ \frac{1}{M} \sum \sum x, \frac{1}{M} \sum \sum y \right\}$$

★ Rotated watermark

★ Rotated by $-\theta$ with respect to the image center

$x(.)$, $y(.)$ : feature coordinate
$k, l$ : normalizing factors
( control the size of $A_{em}$ so that it covers at least the entire facial region)
Watermark Embedding

Visual masking & Embedding

The watermark image $f_w(x,y)$ is defined as

$$f_w(x, y) = f(x, y)$$

$$(x, y) \not\in A_{rot} \lor ((x, y) \in A_{rot} \land \text{Var}(x, y) \leq T_{var})$$

$$f_w(x, y) = f(x, y) + h \cdot w_n(x, y)$$

$$(x, y) \in A_{rot} \land \text{Var}(x, y) > T_{var}$$

$h$: watermark power

$\text{Var}(x,y)$: local image variance

$T_{var}$: appropriate variance threshold (sufficient large image area)
Visual masking & Embedding (contd.)

- $h$ can be a function of local variance:
  $$h(x, y) = h_{\text{max}} \times s(\text{Var}(x, y))$$
  - $s$ takes values in the range $[0,1]$ (increase monotonically with the variance)

- Frontal facial images that contain mostly homogeneous image regions:
  - Low watermark power
  - Did not employ visual masking
Fig. 8. Salient feature extraction results on original images.

Fig. 9. Salient feature extraction results on watermarked images.

Fig. 10. Amplified difference of watermarked and original images.
Outline

- Introduction
- System Overview
- Face Segmentation and Salient Feature Localization
- Watermark Construction
- Watermark Embedding
- Watermark Detection
- Experimental Results
- Conclusion
Watermark Detection

- The image has first to be segmented
  - Feature set
  - Orientation of the approximated facial region
- The prototype watermark
  - Geometric watermark adaptation.

2009/12/30

Chuan-Shen Hu & Boris Chiou
CMLab, CSIE, NTU
For the detection region $A_{\text{det}}$, the response of a hypothesis testing detector

$$R\left(\hat{f}_w, \hat{w}_n\right) = \frac{1}{N_A} \sum_{(x,y) \in A} \hat{f}_w(x, y) - \frac{1}{N_B} \sum_{(x,y) \in B} \hat{f}_w(x, y)$$

$$A = \left\{ (x, y) \in A_{\text{det}} \mid \hat{w}_n(x, y) = 1 \right\}$$

$$B = \left\{ (x, y) \in A_{\text{det}} \mid \hat{w}_n(x, y) = -1 \right\}$$

$$f_w(x, y) = f(x, y) + h \cdot w_n(x, y)$$

$N_A, N_B$ : the number of pixels of the set $A$ and $B$

This detector expresses the difference of two sample means.
Watermark Detection

- Not to use masking in the detection stage
  - The local variance may have changed significantly due to manipulations.
- Threshold $R_{thr}$ (experimental approach)
  - Detector output is approximated by a normal distribution.
    - Sub-optimal, $f, f_w$ is assumed i.i.d.
  - The pdf of the detector output
    - zero mean (un-watermarked image)
    - $2h$ (watermarked image)
Watermark Detection

If the two distributions have equal variances, the optimal threshold is

$$R_{thr} = \left( \text{mean}_l + \text{mean}_r \right) / 2$$

$\text{mean}_l$ and $\text{mean}_r$ : two distribution means
Outline

- Introduction
- System Overview
- Face Segmentation and Salient Feature Localization
- Watermark Construction
- Watermark Embedding
- Watermark Detection
- Experimental Results
- Conclusion
Experimental Results

White noise

(a) (b) (c) (d) (e) (f) (g) (h)
Experimental Results

Examples (using masking)

The prototype watermark = 128 * 128

\( h = 3 \)
\( \lambda = 1.8 \)
\( T_{\text{var}} = 0.002 \)
Experimental Results

Extended region (without masking)

Fig. 11. (a) Original image. (b) Watermarked image using face region. (c) Normalized detector output.

Fig. 12. (a) Original image. (b) Watermarked image using extended region. (c) Normalized detector output.
Fig. 13. (a) Watermarked image after distortion by multiplicative Gaussian noise with $\sigma = 0.3$. (b) Normalized detector output.
Experimental Results

Fig. 14. (a) Watermarked image after 1:30 JPEG compression. (b) Normalized detector output.
Experimental Results

Fig. 15. (a) Watermarked image after $3 \times 3$ median filtering. (b) Normalized detector output.
Experimental Results

Fig. 16. (a) Watermarked image after rotation by 12°. (b) Normalized detector output.

Fig. 17. (a) Watermarked image after rotation by −5°. (b) Normalized detector output.
Experimental Results

Fig. 18. (a) Watermarked image after scaling by a factor of 1.16. (b) Normalized detector output.

Fig. 19. (a) Watermarked image after scaling by a factor of 1.21. (b) Normalized detector output.
Experimental Results

Fig. 20. (a) Watermarked image after cropping to size 188 x 248. (b) Normalized detector output.
Experimental Results

\begin{table}
\centering
\caption{Detector FRR, FAR for several attacks (common detection threshold = 0.32)}
\begin{tabular}{|l|l|l|}
\hline
\textbf{attack} & \textbf{FRR} & \textbf{FAR} \\
\hline
no attack & $1.3094 \times 10^{-16}$ & $2.1585 \times 10^{-4}$ \\
multiplicative Gaussian noise ($\sigma = 0.3$) & $3.3269 \times 10^{-10}$ & 0.0028 \\
1:30 JPEG compression & 0.0273 & $2.1015 \times 10^{-4}$ \\
motion ($3 \times 3$) & 0.0077 & $3.1819 \times 10^{-4}$ \\
rotation by $12^\circ$ & $7.7982 \times 10^{-5}$ & $9.6364 \times 10^{-4}$ \\
rotation by $-5^\circ$ & $8.4085 \times 10^{-6}$ & 0.0023 \\
scaling by 1.16 & 0.0085 & $4.7922 \times 10^{-4}$ \\
scaling by 1.21 & $1.1913 \times 10^{-4}$ & 0.0536 \\
rotation by $-5^\circ$ and scaling by 1.16 & 0.0016 & 0.0712 \\
cropping ($188 \times 248$) & $2.9899 \times 10^{-5}$ & 0.049 \\
\hline
\end{tabular}
\end{table}

$R_{thr} = 0.32$

FRR = false rejection ratio

FAR = false acceptance ratio

\textbf{Chuan-Shen Hu & Boris Chiou}
\textbf{CMLab, CSIE, NTU}
Outline

- Introduction
- System Overview
- Face Segmentation and Salient Feature Localization
- Watermark construction
- Watermark Embedding
- Watermark Detection
- Experimental Results
- Conclusion
Conclusion & Future work

- A method for embedding and detecting watermarks in color frontal facial images.
  - Color information
    - Good approximation of the skin-colored facial region
  - The prototype watermark was chosen to be a chaotic one.
  - Geometrically adapted watermark
    - Using extracted feature positions and facial region orientation.
  - Robust!!!!

Future work

- Development of more robust techniques for salient feature extraction
- Examination of alternative chaotic generators

Chuan-Shen Hu & Boris Chiou
CMLab, CSIE, NTU
Thank you