

---

# **GEOMETRIC-INVARIANT ROBUST WATERMARKING THROUGH CONSTELLATION MATCHING IN THE FREQUENCY DOMAIN**

**R. Caldelli<sup>a</sup>, M. Barni<sup>b</sup>, F. Bartolini<sup>a</sup> and A. Piva<sup>a</sup>**

**<sup>a</sup> Department of Electronics and Telecommunications  
University of Firenze**

**<sup>b</sup> Department of Information Engineering  
University of Siena**

**Proceedings of the 2000 International Conference on Image  
Processing, Vancouver, BC, Canada, September 10-13, 2000.**

## ATTACKS ON A WATERMARKED IMAGE

---

- ❑ Multimedia can be defined as a **combination** of different types of media (e.g., text, images, audio, video, and graphics) to communicate information in a given application.
- ❑ In the last decade, **digital watermarking** has been studied as a possible tool for copyright protection of multimedia data.
- ❑ A watermarked image may go through either normal audio-visual (A/V) processes or intentional attacks:
  - ❑ Examples of **normal A/V processes**: JPEG compression, and analog-to-digital or digital-to-analog conversion.
  - ❑ Examples of **intentional attacks**: geometric manipulations (e.g., rotation, scaling, and translation).
- ❑ A common strategy for detecting a watermark after geometric manipulations is to embed a **synchronization template** in addition to the watermark.
  - ❑ If a geometric attack has occurred, the template has to be **inverted** before the watermark is detected.
  - ❑ This approach has a number of major drawbacks.
    - ❑ The template has **no informative meaning**.
    - ❑ **Image fidelity** is affected.
    - ❑ Requires **exhaustive** search in watermark detection.

## THE ALGORITHM

---

- ❑ **Embedding**
  - ❑ Take the **luminance** layer of an YUV image.
  - ❑ Compute the **Discrete Fourier Transform (DFT)**.
  - ❑ Select the magnitudes of some DFT coefficients according to a **secret** key.
  - ❑ Modify the magnitudes in such a way to create a **local** peak.
  - ❑ Compute the **average** and the **standard deviation** over a window centered on the point to be changed.
  - ❑ The magnitude of the center coefficient will have a **value** equal to the local average plus  $n$ -times ( $n = 4,5$ ) the standard deviation.
  - ❑ The peaks are arranged in **quadruplets**, with pixels belonging to the same quadruplet being collinear.
  - ❑ Moreover these spikes are posed in such a way that quadruplets are concatenated to form a **chain**.
  - ❑ **Concatenation** is achieved by letting the final peak in each quadruplet to be the initial peak of the subsequent quadruplet of the chain.
  - ❑ The peaks form a **constellation** that represents the watermark and the template.
  - ❑ A very general geometric invariant (the **Cross-Ratio** of four collinear points-*CR*) is adopted to be resistant against complex geometrical attacks.

# CONSTELLATION

---

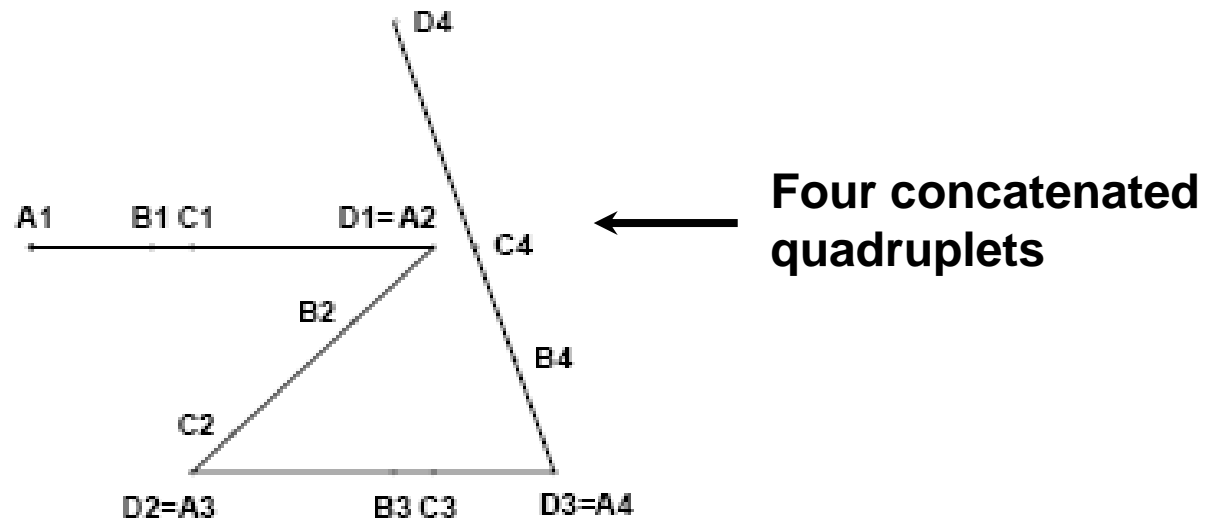


Figure 1. Example of constellation watermark.

## AFFINE AND PERSPECTIVE TRANSFORMATIONS

---

- ❑ CR is invariant under **affine** or **perspective** transformations which cover all the geometric manipulations usually applied to images.
- ❑ An affine transformation is any **transformation** that preserves **collinearity** (i.e., all points lying on a line initially still lie on a line after transformation) and **ratios of distances** (e.g., the midpoint of a line segment remains the midpoint after transformation).
- ❑ Rotation, scaling, and translation are **affine** transformations.
- ❑ A **projective** transformation maps lines to lines (but does not necessarily preserve parallelism).
- ❑ For each quadruplet, the **CR** between its four points is calculated as follows:

$$CR = \frac{\overline{AC} \cdot \overline{BD}}{\overline{AD} \cdot \overline{BC}}$$

where A, B, C and D are the four points of the quadruplet ordered according to the sequence A B C D.

## ORDERING QUADRUPLETS

---

- ❑ The **sequence** of CR's of the ordered quadruplets in the chain represents the secret key of the watermark.
- ❑ The number of **chain branches** can be decided.
  - ❑ The higher the number the more distinguishable the constellation.
  - ❑ On the other hand, the computational burden in the detection step will increase and the image will be more noisy.
- ❑ Note also that the peaks should not be too **evident** in the Fourier domain, otherwise attackers could easily destroy the watermark by removing them.
- ❑ The peaks are introduced in the **medium** frequency range to reach a trade-off between watermark **invisibility** and **robustness**.

**FIGURE 2. WATERMARK INVISIBILITY - 256X256 TEST IMAGE LENA**

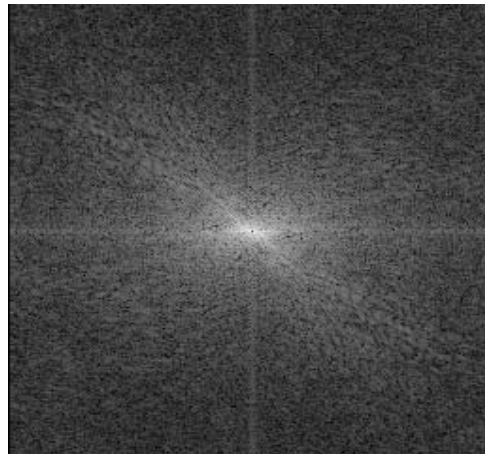
---



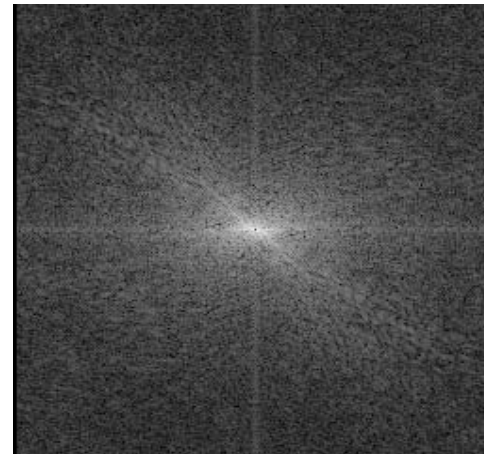
**Original image**



**Watermarked image**



**Magnitudes of DFT coefficients  
of original image**



**Magnitudes of DFT coefficients  
of watermarked image**

## THE ALGORITHM

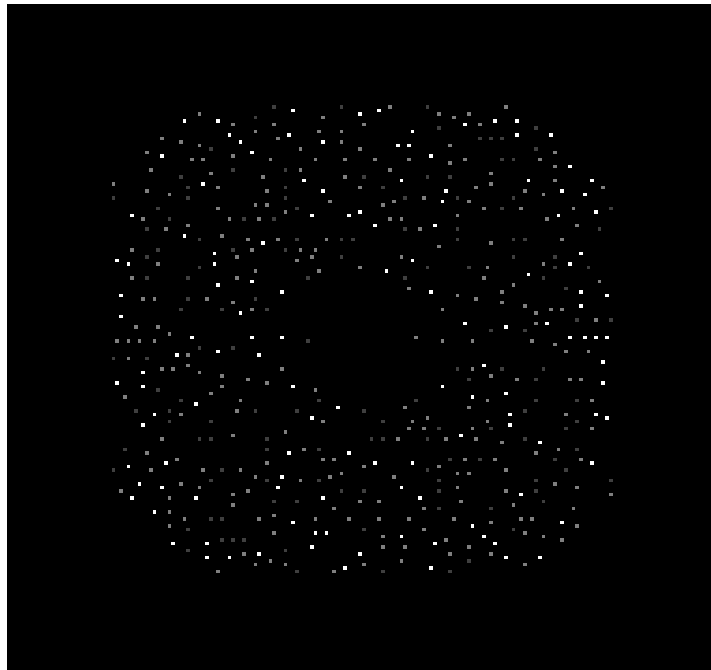
---

### ❑ Detection

- ❑ Take the **luminance** layer of the watermarked YUV image.
- ❑ Compute the **Discrete Fourier Transform (DFT)**.
- ❑ Identify all the **local** maxima through an exhaustive search.
- ❑ If the central coefficient, within a window whose size is equal or smaller than that adopted in the embedding step, is the maximum in the window, this is assumed to be a **peak**.
- ❑ The spikes located in very **low** and in very **high** frequencies are not considered.
- ❑ The watermark is embedded in **middle** frequency range.
- ❑ For an image of size 256x256 about **400** points are generally recovered.
- ❑ This is quite a large number and the watermark is always **well-hidden**.
- ❑ If an attacker wants to **destroy** the watermark, he should modify or delete all these coefficients, resulting in a big loss of image quality.
- ❑ The next step is to check all the existing **quadruplets** of four collinear points, to compute their Cross Ratios and compare them with those characterizing the watermark.
- ❑ If the secret key is known, it is possible to determine which are the correct values of **Cross Ratios** and which is the exact **concatenation** order among those selected.

**FIGURE 3. EXAMPLE OF SPIKES RECOVERED IN THE DFT DOMAIN  
FOR A 256X256 IMAGE**

---



## PROBLEMS

---

- ❑ During detection, there are two issues:
  - ❑ All the **spikes** belonging to the constellation must be extracted.
  - ❑ Just the right watermark, **if present**, has to be detected.
  - ❑ To satisfy the **first** condition, it is sufficient to reduce the size of the extraction window.
  - ❑ However, this **increases** the number of peaks, resulting in a huge amount of possible constellations within the spikes cloud, some of which are likely to satisfy the watermark features.
- ❑ Two different solutions have been considered:
  - ❑ The **first** one is consisted of tolerating loss of some spikes, and consequently of some branches of the chain, without increasing their number, and in carrying out detection resorting to a procedure based on inexact graph matching.
  - ❑ The **second** one relies on the detection of all watermark spikes and on the introduction of some extra constraints or longer chains for the extraction phase.
    - ❑ Obviously this leads to a more **complex** search.
    - ❑ Furthermore, after an image has undergone a geometric transformation, because spikes positions can assume only **integer** values, some **uncertainties** in determining if a point belongs or not to a line and in computing CRs values must be introduced.

## EXPERIMENTS

---

- ❑ Tests against **geometrical** attacks, such as cropping, rotations, scaling, etc., were carried out.
- ❑ In most of the cases, **positive** results were obtained.
- ❑ However, sometimes detection was **missed** and false alarms were **observed**.
- ❑ These two problems can be overcome:
  - ❑ **Missed detection** can be circumvented by developing a safe peaks extraction methodology.
  - ❑ **False alarms** can be prevented by inserting additional and more featuring constraints on the watermark constellation.
- ❑ **Cropping:**
  - ❑ Invariance is obtained by always **padding** the image to the same size before watermark insertion.
  - ❑ Prior to decoding the image is **padded** to the same size, so that frequency sampling is performed with the same step both by the encoder and the decoder.
- ❑ **JPEG compression:**
  - ❑ Up to **60%** of quality factor (Q), the watermark has been correctly and uniquely detected.

## FIGURE 4. WATERMARK ROBUSTNESS TESTS

---



(a)



(b)

- (a) watermarked image cropped at 200x200 and then padded.**  
**(b) watermarked image rotated by -15 degrees.**

## CONCLUSIONS

---

- ❑ A **novel** watermarking technique is presented.
- ❑ **Geometric manipulations** can be prevented.
- ❑ No need for a **reference** template.
- ❑ Some experimental results confirm the **validity** of the approach.
- ❑ There are **implementation problems** that need to be solved.