First wavila challenge: several considerations on the security of a feature-based synchronisation scheme for digital image watermarking

Patrick Bas, Alejandro Loboguerrero

First wavila challenge: several considerations on the security of a feature-based synchronisation scheme for digital image watermarking

Patrick Bas, Alejandro Lobo Guerrero

CNRS,

Laboratoire des Images et des Signaux de Grenoble
961 rue de la Houille Blanche Domaine universitaire
B.P. 46 38402 Saint Martin d'Hères cedex FRANCE

Laboratory of Computer and Information Science
Helsinki University of Technology
P.O. Box 5400 FI-02015 HUT FINLAND

Abstract. This paper presents a study on the security of feature-points based synchronisation watermarking methods. The studied scheme, based on the Harris detector, is presented. An analysis of the feature point detector enables then to draw two different attacks. The first attack called the *competition attack* is performed to lure the detector by increasing the response of neighbouring feature points. The *ranking attack* affects the final ranking which is used to extract the most robust feature points. Examples are given on toy images and the security of feature-based watermarking scheme is afterward discussed.

1 Introduction

It is well known that one major drawback of classical watermarking schemes is the lack of robustness to geometrical distortion. For example, in classical additive (spread-spectrum) methods such as presented in [1–3] and substitutive methods such as presented in [4–7], the image is processed as a classical array of pixels with no reference except the coordinates of each pixel. Consequently if the image undergoes a geometrical transformation, the mark in the image cannot be detected without identifying the transformation.
Using an additive scheme, the correlation cannot be performed because the generated random sequence and the embedded random sequence are not synchronized.
Using a substitutive scheme, the location of the marked components cannot be performed because the initial locations depend on external coordinates; consequently the decoding of the mark is not possible.
Additionally , two levels of geometrical distortions can be addressed:

– The typical geometrical transformation commonly used in image edition such as rotation, translation or cropping. These transformations are applied on the

whole image, and in many ways can be easily represented by a mathematical operation. One basic solution to identify the transformation is to perform an exhaustive detection considering all possible geometrical transformations of the marked image. In this case the computing cost will drastically increase. For example, if we consider only a composition of rotation and scaling operations from 50% up to 200% of the image size, the processing cost is roughly multiplied by 5.4×10^4.

- The other category of geometrical distortions are especially designed to desynchronise the mark without visual changes. M. Khun and F. Petitcolas [8] developed a benchmark called StirMark containing different attacks. One of the first developed attacks of this program is composed of local random geometrical distortions that permits us to defeat many classical watermarking schemes without visible alterations [9].

Different methods have been developed to resynchronize the watermark after geometric transformation. Two of the most popular are the exhaustive search using a correlation function [10] or the use of a template that enables to indicate the location of the watermark[11]. Such schemes often requires an important complexity but it has been showed that they are efficient as long as the number of geometrical transform is a polynomial function of the size of the signal [12].

Recently, content-based watermarking schemes have been proposed to provide another solution to counter geometrical distortions. In this way the location of the mark is not linked with image coordinates, but with image semantics. The problem of geometrical synchronization is solved because the image content represents an invariant reference to geometrical transformations. Content based techniques belongs to second-generation watermarking schemes defined by Kutter *et al* because the image's content is exploited for the embedding of the mark[13].

The goal of this paper[1] is to answer to one of the two questions of the first Wavila challenge [14] which is on the security of synchronisation schemes for digital image watermarking. We study here the security of one category of synchronization schemes called content-based schemes that is widely mentioned in the literature. In comparison with the analysis proposed by Barni [12], a content based synchronisation scheme may be described as template matching synchronisation because the synchronisation relies on the search of *templates*, represented by corner of the image, edges or textures, that are directly provided by the host's content. Additionally , such synchronisation schemes depend on the image's content and therefore can be considered as *public*: features of the image are available to every one. Considering security, this point can be seen as a drawback because the synchronisation information is disclosed to every one [15, 16]. The class of content-based synchronisation schemes will be consequently considered as not secure if it is easily possible to erase the extracted features of

[1] The work described in this paper has been supported (in part) by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT and the National French project Fabriano.

the image without introducing important distortions. In this paper, the security of public feature detectors represented by feature points extractors is analysed. The different strategies to defeat feature points synchronization schemes are explored.

2 Presentation of one feature-point based synchronization scheme

2.1 Description of the whole watermarking scheme

We have decided to investigate the securities issues related to one specific content-based synchronisation scheme [17] which uses a feature point detector to extract the image content. One property of this scheme is that it uses feature points to synchronize the watermark. Such an idea has been also presented in other image watermarking schemes [18–22] or 3D mesh watermarking schemes [23].

The description of the watermark embedding and detection is as follows:

In the embedder side:

1. Detect robust feature points in an image.
2. Generate a triangular tessellation of the image based on the set of feature points.
3. Map a triangular random sequence (the watermark) into each triangle of the tessellation via affine transform.
4. Add the mapped sequence on each triangle.

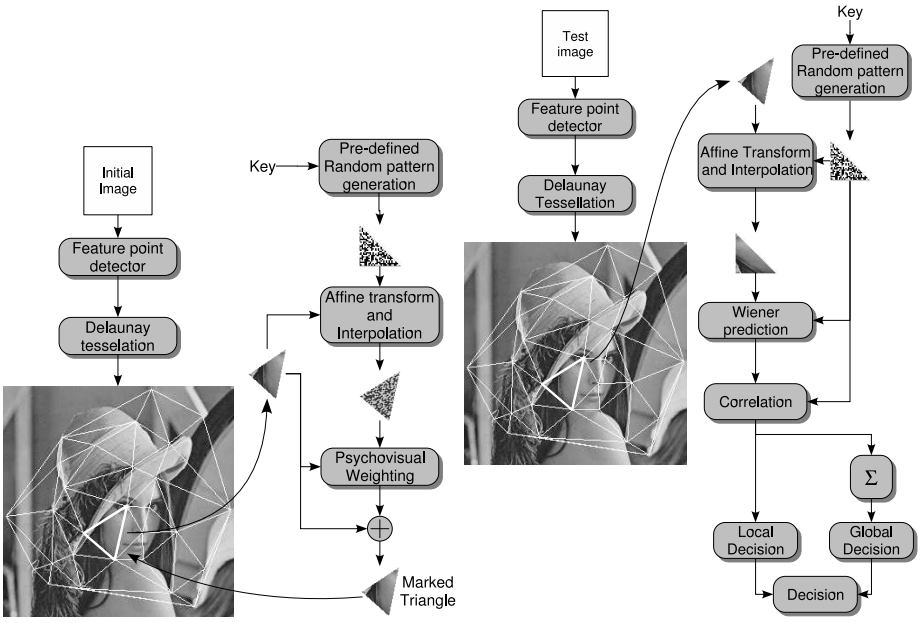
In the detector side:

1. Reconstruct the tessellation.
2. Map each triangle to the shape of the original triangular watermark.
3. Compute the correlation of each mapped triangle with the original watermark.
4. Accumulate the correlations to detect the watermark over the whole image.

The diagrams of the embedding and detection algorithms are depicted on figure 1.

2.2 Description of one feature point detection algorithm

As lot of feature point based synchronisation schemes, the extraction of feature points relies on a modified Harris feature point detector which is described is this section. The whole process of extracting feature points can be summarized in four steps that are described below.



Embedding. Detection.

Fig. 1. Diagrams of the embedding scheme proposed in [17].

Step 1: pre-processing. This step is done because the robustness of the feature point detector, which represents its ability to recover the feature points after geometric transforms or classical image processing processes, depends of the content of the image. Consequently, to increase the robustness of the detector, especially for the heavy textured images, an averaging filter A_n is used as a pre-processing step of the detector.

$$A_n = \begin{bmatrix} 1 \cdots 1 \\ \vdots \ddots \vdots \\ 1 \cdots 1 \end{bmatrix} \tag{1}$$

Step 2: feature points response function. Feature points detectors find salient points in natural images. These points are often located near corners and edges of the image. Feature points were first developed for computer vision and reconstruction [24, 25] but they are also employed in data-base retrieval as a descriptor of the image [26, 27].

The Harris and Stephens response function is used here and is based on a corner detection function created by Moravec [28].

The response function $E_{x,y}$ is calculated for a shift (x, y) from the central point (u, v):

$$E_{x,y} = \sum_{u,v} w_{u,v} |I_{x+u,y+v} - I_{u,v}|^2 \tag{2}$$

where $I_{u,v}$ represents the luminance of the image at the coordinate (u, v). the function $w_{u,v}$ represents a rectangular window centred on (u, v).
Harris reformulated the detection function using a matrix formulation:

$$X = I * [-1, 0, 1] \approx \delta I / \delta x \tag{3}$$
$$Y = I * [-1, 0, 1]^T \approx \delta I / \delta y \tag{4}$$
$$A = X^2 * w \tag{5}$$
$$B = Y^2 * w \tag{6}$$
$$C = (XY) * w \tag{7}$$

where $*$ denotes the convolution product. The new detection function $E_{x,y}$ is then expressed by:

$$E_{x,y} = (x, y) M (x, y)^t \quad \text{with} \quad M = \begin{bmatrix} A & C \\ C & B \end{bmatrix} \tag{8}$$

$E_{x,y}$ measures the significance of the peak of a local cross-correlation function comparing with small shifts. Harris and Stephens gave a new definition of the detector function considering the eigenvalue α and β of the array M. These values are invariant by rotation and if their magnitudes are high, the local auto-correlation function is represented by a local peak.
To avoid computing the eigenvalue of M, the new criterion R is based on the trace and determinant of M:

$$Tr(M_{x,y}) = \alpha + \beta = A + B \tag{9}$$
$$Det(M_{x,y}) = \alpha\beta = AB - C^2 \tag{10}$$
$$R = Det(M) - kTr^2(M) \tag{11}$$

where k is an arbitrary constant.

Step 3: competition. A feature point is afterward represented by a local maximum of the detector response $R(u, v)$. It is important to define the size of the neighbourhood in which the local maximum is computed. If this size is too small, the distribution of the different feature points will be concentrated on textured areas. If the size of neighbourhood is too large, the feature points will become too far from each other.
To obtain an homogeneous distribution of feature points in the image, we chose to use a circular neighbourhood to avoid increasing detector anisotropy. The

centre of the neighbourhood is the considered pixel. To be robust to scaling operations, the circle diameter depends on the image dimensions:

$$D = \frac{w + h}{\gamma} \tag{12}$$

The integers w and h represent respectively the image width and height. The neighbourhood size is quantized by the γ value.

Figure 2 illustrates the influence of the γ parameter.

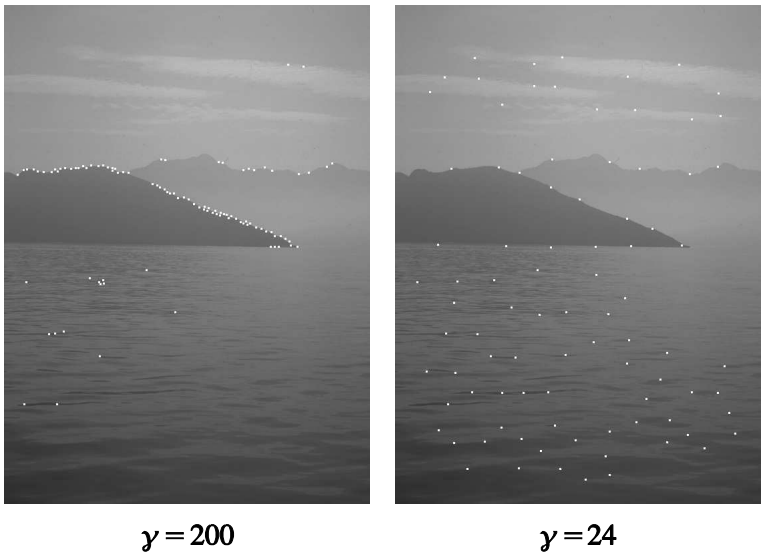


Fig. 2. Influence of the γ parameter.

Step 4: ranking: the selection of N feature points inside the image is finally done by choosing the N most important feature points, e.g. which have the most important values of $R(u, v)$. This last step enables firstly to select the points that have the strongest robustness and secondly to control the number of triangle in the final tessellation.

Overview of the proposed synchronization scheme: an overview of the presented feature detection algorithm is illustrated on figure 3. First the image is pre-processed using a low-pass filter to improve the robustness of the detector. The Harris corner detector function is afterward used. We may approximate this function by a 2D local cross-correlation filter that is applied on the derivate of the image. Then a local competition step is used to tend to an uniform distribution

of the feature points inside the image and finally the N most important feature points are selected using the Harris criterion $R(u, v)$ after the competition process.

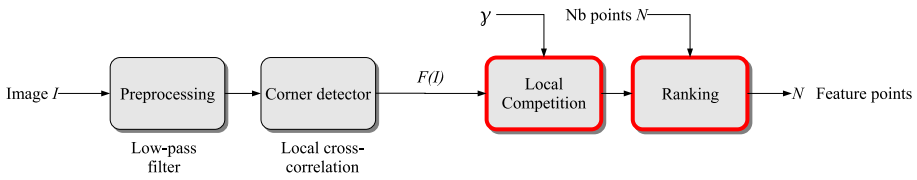


Fig. 3. Overview of a feature-points detector using for watermarking synchronisation

3 Security analysis of the presented feature point based synchronization scheme

The aim of the section is to present the different strategies that can be adopted by an attacker to alter the original triangular tessellation. The goal is to alter the image in such a way that each original triangle of the watermarked image is altered while minimizing the distortion.

3.1 Security considerations related to the Delaunay tessellation

The studied watermarking scheme use the set of feature points to build a Delaunay tessellation. The watermark is afterward embedded in each triangular region of the image. The Delaunay tessellation was originally chosen because it brings interesting properties:

- The tessellation has local properties: if a feature point disappears, the tessellation is only modified on connected triangles. Consequently it is possible to alter the whole tessellation without modifying each feature point that is initial extracted but a minimum number of feature points have to be attacked.
- Each vertex is associated with a stability area in which the tessellation is not modified [29] when the vertex is moving inside this area.

It has been proved that the average degree (number of other feature points connected) of one feature point is less than 6. Consequently, if M triangles are watermarked with a set of N feature points, one need to remove or move at least $N/6$ feature points to alter all the partition. On attacker might for example proceed by first removing the feature points presenting the most important degrees as illustrated on figure 4.

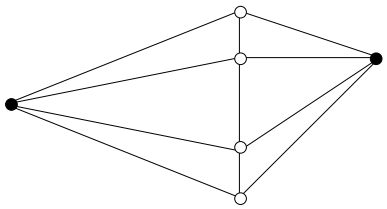


Fig. 4. Example of an optimal attack, the attack will only remove the back vertexes (feature points).

3.2 Analysis

The synchronisation watermarking scheme has been presented in the previous section. It is first important to point out that a feature detector can be considered by definition as a public detector. As far as we know, attempts to find image features that are both secure and robust to geometric distortion are rare [30] and are efficient only for simple geometric transforms such as rotations and scaling operations. We can therefore make the assumption that the attacker can have access to the location of the feature points and that one possible attack is to identify and try to remove feature points that are initially extracted.

The figure 3 outlines the four different modules that composes the presented scheme. The two first modules are equal or similar to 2D FIR filters, one low-pass filter and one filter that acts as a cross-correlation function. They can be considered as an basic pre-processing function whose the output, denoted $R(u, v)$ is used decide is a feature point is present or not.

One simple way to alter the output $R(u, v)$ at a given location (u_i, v_j) is to modify the variance of a bloc centred on (u_i, v_j). This property is due to the fact that the Harris detector is somewhat similar to a local cross-correlation function of the derivate of the signal (or a low-pass version of the signal). Consequently increasing (resp. reducing) the variance of a bloc centred on (u_i, v_j) enables to increase (res. decrease) the output of $R(u_i, v_j)$. In practice, the size of the bloc has to be the same than the size n of the blur filter M_n that is used as a pre-processing step.

One might draw malicious attacks by altering the image in such a way that the output function will afterward lure either the third *competition step* or the fourth step *ranking step*. Both theses last two processes are part of the final decision procedure and the modification of $R(u, v)$ has to be done according to the decision criterion of either the third or the fourth step.

3.3 Attack 1: Lure the local competition

As it as been explained previously the local competition process is necessary to avoid to have huge concentration of feature points (and consequently very small

triangles) in textured areas of the image. We recall that this is done by selecting a feature point if and only if it is a local maximal in a neighbouring window.

Consequently one way to remove a feature point is to increase its related strongest competitor in the window. Basically, if $R(u_k, v_k)$ has been chosen as a candidate to become a feature point because $R(u_k, v_k) > R(u_j, v_j) \forall (i,j) \in \mathcal{N}(u_k, v_k)$ and if $R(u_l, v_l)$ is the second maximum in $\mathcal{N}(u_k, v_k)$, then the attack will consist in altering the image I to create an attacked image I' in such a way that $R_{I'}(u_l, v_l) > R_{I'}(u_k, v_k)$. It is also important to notice that, if the initial difference between $R(u_k, v_k)$ and $R(u_l, v_l)$ is small, the distortion introduced by the attack will be also weak.

3.4 Attack 2: Lure the final ranking

The final step consists in ranking the values of the candidates by choosing the N feature points presenting the most important response values $\{R_1, ..., R_N\}$. Consequently one might want to remove one feature point that is initially ranked with the corresponding response R_i by altering the image is such a way that the feature point after the attack is not in the final ranking and its new response R'_i satisfies $R'_I < R'_N$. This attack can be done by modifying the initial set of feature points in such a way that (1) either their values become greater than R_i or (2) by decreasing R_i such that $R_i < R_{N+1}$. Note however if in one hand strategy (1) will lead to a more important distortion that strategy (2) because a more important number of feature need to be increased on the other hand strategy 2 can be difficult to perform if $R_i >> R_N$ because removing a well defined corner of an image may be a difficult task.

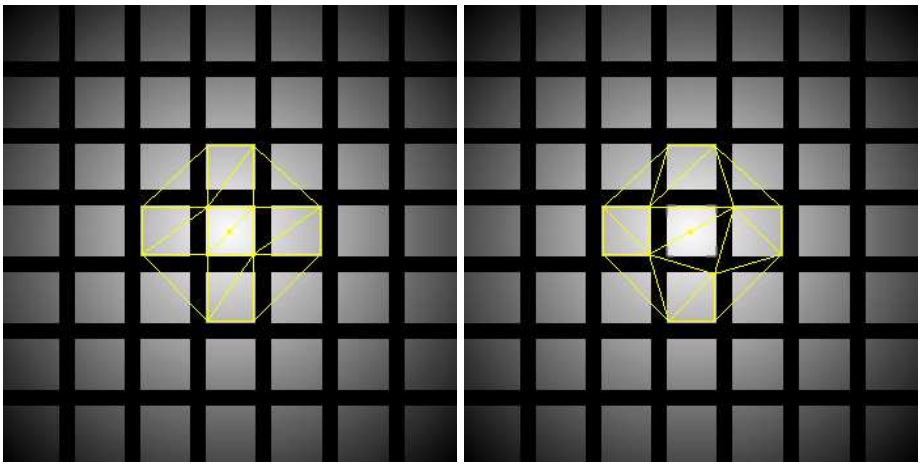
4 Toy examples

The aim of this section is to illustrate the principle of the two attacks that has been mentioned in the previous section. For this purpose we have used two synthetic images, *toy1* and *toy2* that as been specifically build to illustrate the behaviour of the two attacks.

4.1 Attack based on the local competition

The image *toy1*, is an image that contains lot of corners, additionally the function $R(u, v)$ is maximum on the centre of the image and is a decreasing function of the distance from the centre of the image. Figure 5 depicts the image *toy1* and its associated triangular tessellation. Each vertex of a triangle corresponds to a feature point that has been initially detected. We can see that, due to local competition, only one on the four nearest corner is selected. It is always the corner that is the nearest to the centre of the image, this is due to the fact that this point is a local maximum in this case. A successful attack as been performed by locally blurring several corners to decrease $R(u, v)$. Only four feature points, presenting the highest order, have been selected and modified to completely

alter the tessellation of the initial image. In this case, we can also notice that the distortion introduced by this attack is not important, because we have only decreased the variance of the blocks centred on the attacked feature points.

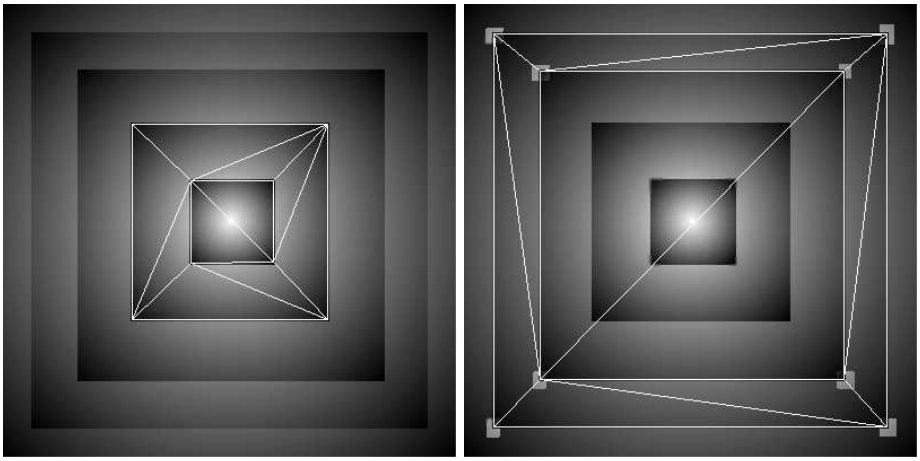


Toy1 image | *Toy1* image after the attack

Fig. 5. Example of the attack based on the local competition.

4.2 Attack based on the final ranking

The image *toy2* has been build in such a way that no *competition attack* is possible because the corners are too far from each other. Consequently only the *ranking attack* is possible. Height feature points have been extracted by the algorithm (see figure 6) and the image has been synthesized in such a way that $R(u, v)$ is a decreasing function of the distance from the centre of the image. The attack has been performed here by increasing the variance of the other corners in such a way that at theses locations, the function $R(u, v)$ becomes greater than in the previous locations. This is done by increasing the variance of the new positions up to have a more important output than for the initial feature point. It is important to notice that such an operation may require an important distortion because each new feature point has to have a more important response than the feature point that is erased. The other strategy that consists in decreasing the response the initially extracted features points was practically difficult to perform on this image.



Toy2 image *Toy2* image after the attack

Fig. 6. Exemple of the attack based on the final ranking.

4.3 Is a feature-point based synchronisation scheme secure ?

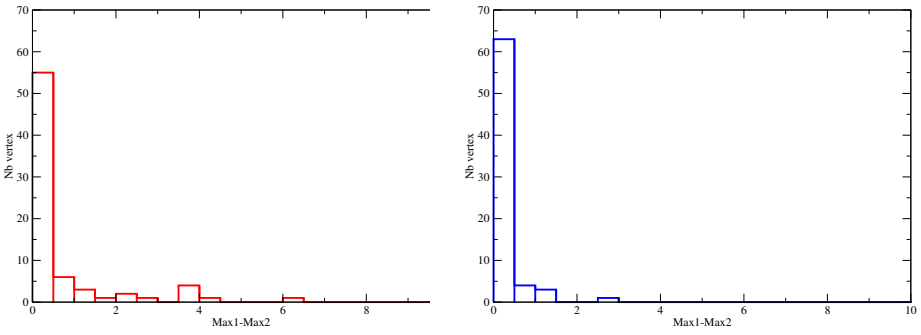
Based on the previous toy examples, we would like to give a preliminary statement on the security of this feature point watermarking scheme. As we have shown, a *competition attack* is efficient if the difference between the first and second maxima is small. In the case of natural images, such a situation happens if the images have important high frequency components. Figure 7 illustrates two different image contents. The left image (lena) is well structured and presents strong corners and only few textured areas. On the contrary, the right image (baboon) is heavy textured and presents high frequencies.

To illustrate the sensitivity of each image to the *competition attack*, figure 8 depicts the histograms of the difference between the first and the second maximum for each extracted feature point. As we can seen, the number of feature point with high differences is more important for the lena image than for the baboon image. Consequently we can assume that the image baboon will be easier to attack than the image lena.

To address the image's sensitivity to the *ranking attack*, figure 9 depicts the normalised cumulative histograms of the output $R(u, v)$ for each possible candidate as a feature point. If for example the extraction algorithm has to select only 10% of the initial set, we can see that it will chose any feature point such that $R(u, v) > 5$ for the image *lena* but $R(u, v) > 1$ for the image *baboon*. If we want to replace all the initial set by the most important non selected feature points, we have to choose candidates having $0.5 < R(u, v) < 1$ for *baboon* and $2.5 < R(u, v) < 5$ for *lena*. Consequently in this case, the necessary distortion will be more important to attack the image lena that to attack the image baboon.

Lena Baboon

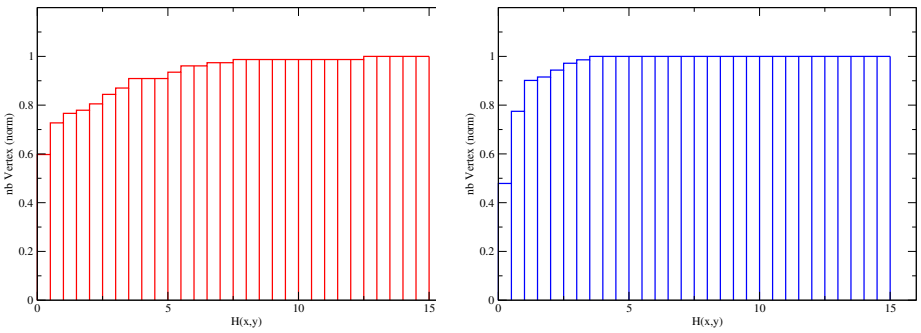
Fig. 7. Examples of two different contents of images: on the right the image *lena* has only small high-frequency components and well defined corners. On the left, the image *baboon* has high frequency and not obvious corners.



Lena Baboon

Fig. 8. Histograms of the difference between the corner detector function $R(u, v)$ for the firt and the second most important values for the images *lena* and *baboon*. For *baboon* the values are in average more concentrated near zero and consequently the *competition attack* is easier.

We finally can state that the security of a feature-point synchronisation scheme is strongly linked with the content of the image and depends on two factors. The security will be more important for images presenting only low frequencies because the competition attack will then be more difficult. The second parameter relies on the distribution on selected maxima and their values have to be as far as possible from the values of the non selected maxima to avoid the rank attack.



Lena Baboon

Fig. 9. Cumulative histograms of the corner detector function $R(u, v)$ for the images *lena* and *baboon*. The values of $R(u, v)$ are more spread for the image *lena* than for the image *baboon* and consequently the *ranking attack* will be easier in the second case.

5 Conclusion and perspectives

We have studied in this paper the security of feature points based synchronisation schemes. Our analysis enables to highlight important conclusions. The major weakness of such schemes is the fact that they are public. Because no key is needed to extract feature points from an image, an attacker may try to remove or move the feature points. However this task is not so easy: we have drawn two types of attack that are possible to erase a feature points: the *competition attack* and the *ranking attack*. We have shown that the distortion that is necessary to perform these attacks will rely on the content of the image: as a global trend, the attack will require a smaller distortion for heavy textured images than for smooth images.

This study addresses only the security of feature-points based synchronisation schemes by the presented methodology can somewhat be extended to other schemes which have a public extractor but with different strategies to lure the content extractor.

Beside this study, it is also important to address the security of other secret content based synchronisation schemes. In the case of synchronisation for images, Delannay *et. al* have presented a feature dependent scheme that is both robust to translations and is claimed to be secret [30]. For audio synchronisation, the concept of informed synchronisation [31] which embeds a secret random sequence at locations that depends on the signal content should also be addressed.

References

1. Tirkel, A., Rankin, G., Schyndel, R., Osborne, C.: Electronic water mark. In: DICTA, Austin (TX), Usa (1993) 666–672
2. Pitas, I., Kaskalis, T.: Applying signatures on digital images. In: Workshop on Nonlinear Signal and Image Processing, Neos Marmaras, IEEE (1995) 460–463

3. Cox, I., Killian, J., Leighton, T., Shamoon, T.: Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing **6** (1997) 1673–1687
4. B.Chen, Wornell, G.: An information-theoretic approach to the design of robust digital watermarking systems. In: Proceedings IEEE-ICASSP'99, Phoenix (Arizona) (1999)
5. Zhao J., K.E.: Embedding robust labels into images for copyright protection. Technical report, Fraunhofer Institute for Computer Graphics, Darmstadt, Germany (1994)
6. Kundur, D., Hatzinakos, D.: Digital watermarking using multiresolution wavelet decomposition. In: IEEE ICASSP'98. Volume 5., Seattle (USA) (1998) 2659–2662
7. Maes, M., van Overveld, C.M.: Digital watermarking by geometric warping. In: IEEE- ICIP'98. Volume II., Chicago (IL, US) (1998) 424–429
8. Petitcolas, F.A., Anderson, R.J., Kuhn, M.G.: Attacks on copyright marking systems. In Aucsmith, D., ed.: Information hiding: second international workshop. Lecture notes in computer science, Springer Verlag, Berlin, Germany (1998)
9. Dugelay, J.L., Petitcolas, F.: Possible counter-attacks against geometric distortions. In Wah Wong, P., Delp, E.J., eds.: EI'2000: Security and Watermarking of Multimedia Content II. Volume 3971 of SPIE Proceedings., San Jose, California USA (2000) 358–370
10. Kalker, T., Janssen, A.: Analysis of spomf detection. In: presented at IEEE-ICIP'99. (1999)
11. Pereira, S., Pun, T.: Fast robust template matching for affine resistant image watermarking. In: International Workshop on Information Hiding. Volume LNCS 1768 of Lecture Notes in Computer Science., Dresden, Germany, Springer Verlag (1999) 200–210
12. Barni, M.: Shedding light on some possible remedies against watermark desynchronization: a case study. In: Proceedings of SPIE, Security, Steganography and Watermarking of Multimedia Contents IV, San Jose, USA (2005)
13. Kutter, M., Bhattacharjee, S.K., Ebrahimi, T.: Towards second generation watermarking schemes. In: IEEE-ICIP'99. Volume I., Kobe (Japan) (1999) 320–323
14. Barni, M.: Wacha: Wavilla challenge. http://www.uoc.edu/symposia/wacha05 (2005)
15. Kalker, T.: Considerations on watermarking security. In: Proc. of MMSP, Cannes, France (2001) 201–206
16. Cayre, F., Fontaine, C., Furron, T.: Watermarking security part I: Theory. In: Proceedings of SPIE, Security, Steganography and Watermarking of Multimedia Contents VII. Volume 5681., San Jose, USA (2005)
17. P. Bas, J.M.C., Macq, B.: Geometrically invariant watermarking using feature points. IEEE Trans. on Image Processing **11** (2002) 1014–1028
18. Dittmann, J., Fiebig, T., Steinmetz, R.: New approach for transformation-invariant image and video watermarking in the spatial domain: self-spanning patterns (ssp). In Wah Wong, P., Delp, E.J., eds.: Electronic Imaging 2001: Security and Watermarking of Multimedia Content III. SPIE Proceedings, San Jose, California USA (2000) 176–186
19. Celik, M.U., Saber, E., Sharma, G., Tekalp, A.M.: Analysis of feature-based geometry invariant watermarking. In: Proceedings of SPIE, Security, Steganography and Watermarking of Multimedia Contents III, San Jose, USA (2001) 261–268
20. Tone, M., Hamada, N.: Affine invariant digital image watermarking using feature points. In: NCSP'05 Honolulu, Honolulu ,Hawaii (2005) 117–120

21. Lu, C.S., Sun, S.W., Chang, P.C.: Robust mesh-based content-dependent image watermarking with resistance to both geometric attack and watermark-estimation attack. In: Proceedings of SPIE, Security, Steganography and Watermarking of Multimedia Contents VII, San Jose, USA (2005)
22. Tang, C.W., Hang, H.M.: A feature-based robust digital image watermarking scheme. IEEE Trans. on Signal Processing **51** (2003) 950–959
23. Alface, P.R., Macq, B.: Feature-based watermarking of 3d objects: Towards robustness against remeshing and de-synchronization. In: Proceedings of SPIE, Security, Steganography and Watermarking of Multimedia Contents VII, San Jose, USA (2005)
24. Boufama, B., Mohr, R., Morin, L.: Using geometric properties for automatic object positioning. Image and Vision Computing **16** (1998) 27–33
25. Faugeras, O., Quan, L., Sturm, P.: Self-calibration of a 1d projective camera and its application to the self-calibration of a 2d projective camera. In: Proceedings of the 5th European Conference on Computer Vision, Freiburg, Germany. (1998) 36–52
26. Loupias, E., Sebe, N., Bres, S., Jolion, J.M.: Wavelet-based salient points for image retrieval. In: Proc. ICIP, to be published (2000)
27. Dufournaud, Y., Schmid, C., Horaud, R.: Matching image with different resolutions. Computer Vision and Pattern Recognition **1** (2000) 612–618
28. Moravec, H.: Obstacle avoidance and navigation in the real world by a seen robot rover. Technical Report CMU-RI-TR-3, Robotics Institute, Carnegie-Mellon University (1980)
29. Bertin, E., Marchand-Maillet, S., Chassery, J.M. In: Optimization in Voronoi Diagrams. Kluwer Academic Publishers (1994) 209–216
30. Delannay, D., Macq, B.: Method for hiding synchronization marks in scale and rotation resilient watermarking schemes. In: Proceedings of SPIE, Security, Steganography and Watermarking of Multimedia Contents IV, San Jose, USA (2002)
31. LoboGuerrero, A., Bas, P., Lienard, J.: An informed synchronization scheme for audio data hiding. In: Proceedings of SPIE, Security, Steganography and Watermarking of Multimedia Contents VI, San Jose, USA (2004) 116–126