Still Image Copy Detection Algorithm Robust to Basic Image Modifications

Karol Wnukowicz [1] , Grzegorz Galiński [1], Rubén Tous [2]
[1] Institute of Radioelectronics, Warsaw University of Technology,
ul. Nowowiejska 15/19, 00-665 Warsaw, Poland,
[2] Computer Architecture Department, Universitat Politècnica de Catalunya,
Jordi Girona, 1-3, 08034 Barcelona, Spain
E-mail: *K.Wnukowicz@ire.pw.edu.pl*

Abstract - *The paper presents a method for content based still-image replica detection. This method uses a compact image signature which depends on image content and is invariant to many widely used image processing techniques, such as lossy compression, resizing, resampling, color enhancements and simple rotations. The signature is designed to be usable in big image database: it has small size (a few dozen bytes), the extraction is fast and the comparison of image signatures is very fast. More than milion of image signatures per second can be compared on a modern PC. Usage of the method within a framework for Digital Rights Infringements Detection in the World Wide Web is also discussed.*

Keywords – *Still image duplicate detection, image signature, search and retrieval, digital rights management*

1. INTRODUCTION

In today's networked audiovisual systems and applications a great deal of audiovisual data is gathered and distributed. The data is often modified during the distribution to meet various requirements of networks, storage capacity, or capabilities of user equipment. Different multimedia devices and networks often need data in specific formats, bitrates, and resolutions – so the data must be transformed according to these needs (e.g. different format is preferred by high resolution printers, HD displays, PC monitors, and mobile phones). This makes the possibility that the same material is stored and distributed in modified versions and various formats. The examples of modifications which may be applied to visual data are rescaling, lossy compression, changing of color depth, and image enhancements such as changing brightness, saturation, blurring or sharpening

The goal of copy detection systems is to allow the detection and localization of all variants of the same multimedia material, including the modified versions. The detection should be fast, reliable, and robust to widely used techniques of adaptation or enhancement of the material.

In this paper a technique for still image copy detection is presented. A practical application of this technique may be, for example, an image copyright protection system, which uses image copy detection module for searching copies of copyrighted images in public networks. Another example is an application of digital photo management. Many users of digital cameras often process their photos in popular image processing applications and multiple (modified) copies of the same photo may be stored in their photo galleries. Copy detection tool would allow users to find photos having different versions in their private photo galleries.

A number of papers investigated the problem of still image copy detection. Some of them proposed techniques which utilize various visual features such as color, shape or texture [1], [2], [3]. Other methods use interest points to index local features [4]. These methods usually produce big descriptions and the searching speed is quite slow, as they use complex distance functions for comparing image features. To be usable for big image repositories containing millions of images, the application of image replica detection should provide:

- fast feature extraction algorithm;
- small size of image feature used for image description;
- fast search algorithm (calculation of the distance between image features);
- high precision and recall.

Recently, the possibility of designing a visual identifier, which can be used for image replica detection, was also investigated by standardization activities of MPEG group [5]. They defined requirements for image signature which can be used for content-based image identification. These requirements contain experimental conditions for two different scenarios: fast algorithm with high success rate for replicas obtained by basic modifications and possibly slower algorithm which will detect image replicas obtained by heavy modifications. Two contributions which fulfill the requirement of basic image signature have been submitted. One contribution use Radon transform [6] to compute features invariant to basic image operations and the second contribution proposes a method based on features computed in concentric circle regions [7].

The work presented in this paper proposes another algorithm which fulfils the requirements of MPEG image signature for basic modifications described in [5] which can be used for fast searching of image replicas in big databases. The detection rate and performance of the proposed image signature is evaluated according to the evaluation criteria described in that document.

The technique presented in this paper is an extension of the work presented in [8] where image is partitioned into fixed number of square blocks. The blocks can be overlapped or not. In each block a local feature is computed and the successive blocks form trajectory of features. Singular energies were used as features of the blocks. The trajectories form a vector of features, and the correlation of vectors between original image and modified copies are very high, so the correlation of the feature trajectories was used to obtain the similarity of two images. The main improvement of the method presented in this paper is that the list of invariant image modifications is extended by basic rotations (90º, 180º, 270º, flip horizontally and vertically). Also some new concepts for extracting the image signature are introduced and evaluated. As a result, the signature has smaller size and the detection rate is better.

The outline of the paper is the following. In section 2 the algorithms for extraction and matching of image signature are described. Experiments and results are presented in section 3. In section 4 the application of replica detection module within the framework for digital rights infringement detection system is described. Section 5 concludes the paper.

2. IMAGE SIGNATURE

2.1. Extraction

The signature obtained by the proposed extraction algorithm is invariant to many common image processing techniques. The signature can be used to detect replicas created by color conversions/enhancements, resizing, simple rotation, lossy compression and applying filters.

The extraction algorithm can be described by the following steps:

1. Image preprocessing:
   - resize image in such a way the shorter edge has 256 pixels;
   - convert the pixel values of image to grayscale;
   - crop the central part of the image of the size 256×256 pixels;
2. Partition image into overlapping blocks $B(x,y)$ of the size 16×16. The blocks are obtained by moving window 16×16 across the image from left to right by 8 pixels and next from top to bottom also by 8 pixels (x,y = 0, 8, 16, 24, 32, 40 ...).
3. Compute features in each local block – 3 features are used: mean level of luminance $Y(x, y)$, mean energy of a block $E(x,y)$ and singular energy of a block $S(x,y)$ which is defined as fractional distribution of the energy in first singular channel, defined by singular directions of image blocks [8].
4. Cluster image blocks to obtain block groups which are rotation-invariant. Rotation invariant means that when the image is rotated (basic rotations) the group is not changed.
5. Compute features for each group of blocks; mean of feature values and standard deviation of features in the groups: $Y_{mean}(i)$, $Y_{dev}(i)$, $E_{mean}(i)$, $E_{dev}(i)$, $S_{mean}(i)$, $S_{dev}(i)$, where i is the id of group of blocks $0 \le i < 120$.
6. Build image signature: the signature is a bit-string built from the feature values. The signature bits are computed for each feature F: if $(F(i+1)) > F(i))$ { $Signature(i) = 1$} else { $Signature(i) = 0$ }, where F is one of features Y_{mean}, Y_{dev}, E_{mean}, E_{dev}, S_{mean}, S_{dev}. The resulting signature is a concatenation of bit-streams obtained for a chosen set of features; the maximum size of the signature if all the features are used is 6*119 = 714 bits.

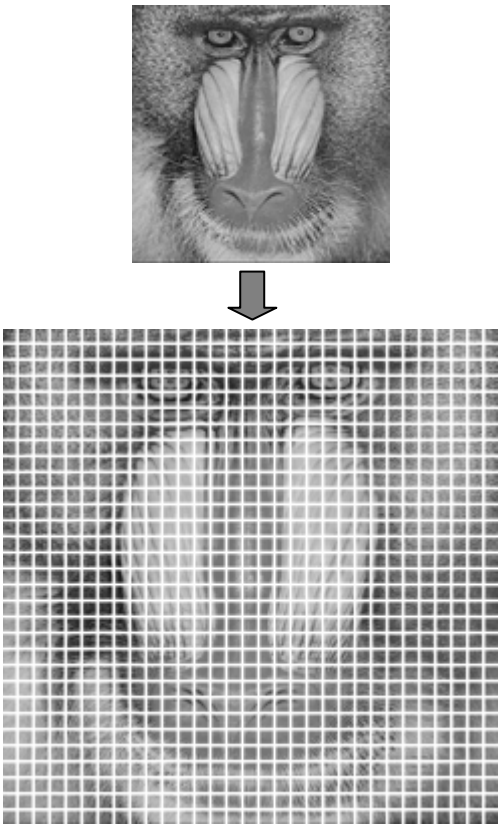

Fig. 1. Illustration of image preprocessing and partitioning into blocks

Figure 1 shows image of Baboon after preprocessing and partitioning (steps 1 and 2 of the algorithm described above). The partitioned image contains overlapping blocks of the size 16×16 pixels.

Figure 2 shows the idea of rotation-invariant block clustering from step 4 and block ordering for building the signature from step 6. The blocks containing the same numbers belongs to the same rotation-invariant groups. The arrows show scan order for building the signature from block-to-block differences of the features. The features for each scan point are mean and deviation of all the features in blocks of the related group (having the same number in the Figure 2). After simple rotation the group does not change, and thus the feature values of the scan points are invariant to such rotations.

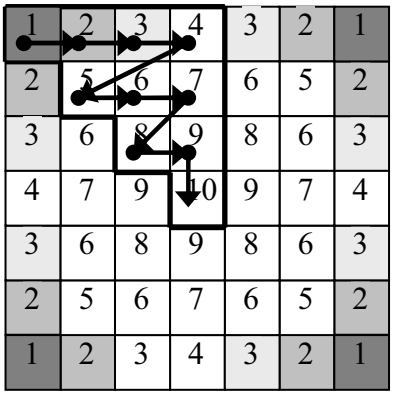

Fig. 2. Block clustering and group ordering for building the signature.

2.2. Matching of signatures and detection of image replicas

Detection of image replicas is performed by matching signatures of two images. The detection system gives binary answer for single matching: an image is a replica or not. For image database the signatures can be extracted and stored. To check if a given image is a replica of any of the images in the database, first signature of the test image is extracted and next it is matched to all the signatures of the images in the database.

The matching algorithm compares bit-streams of two signatures, and the distance is the Hamming distance, which means the number of bits which differ in the two signatures. This can be implemented very efficiently [6] – a few millions of comparisons per second can be performed. The final decision to classify two images as replicas is made by comparing the computed distance with a distance threshold. The threshold is determined experimentally and depends on required precision and recall rates. Lower threshold values will give better precision rate (less falsely detected copies) but the recall rate will decrease (less copies will be detected).

3. EXPERIMENTS AND RESULTS

The detection rate of the image signature has been evaluated using the evaluation criteria and image database defined in Call for Proposals on Image Signature [5]. The experiments consist of two steps. In the first step, operational point for the detection is assigned using a database of independent images (non-replicas). The database contains N=135,609 images and the distances of all image pairs in the database was computed. The number of independent image pairs is: 135,609 * (135,609 – 1)/2 = 9,194,832,636. The operational point is set to obtain false positive rate of the detection equal 0.05 ppm (parts per million). This means that non-replica may be detected as replica in one of 20,000,000 image comparisons. The operational point is set as the threshold for the distance which gives the required false positive rate. This threshold is used in the second part of the evaluation: testing the robustness of the signature.

To test the robustness of the image signature the success rate of the detection is computed corresponding to the operational point 0.05 ppm false alarm ratio obtained in the first part of the experiments. A second image database is used which consist of 10,000 original images. These original images are used to generate modified images with the software provided in [5]. The modifications presented in table 1 are performed on each original image. Up to three modification sets are generated for each modification group using various modification parameters. The success rate is measured for each modification independently. Success rate is defined as the ratio of the number of successfully detected image copies to the total number of image copies.

Table 1. Success rate corresponding to 0.05 ppm false positive rate

Modification	Succes rate [%]	Modification	Success rate [%]
scale to 90%	99.88	noise (16)	98.96
scale to 70%	99.87	noise (64)	97.42
scale to 50%	99.8	noise (144)	96.13
JPEG, q=80	99.98	color 16 bpp	99.1
JPEG, q=60	99.75	color 8 bpp	94.74
JPEG, q=30	99.22	greylevels	99.62
bright. +10%	99.93	hist. equaliz.	61.8
bright. +20%	99.57	auto-levels	99.08
bright. +25%	99.17	flip	100
blur (3)	99.69	rotate 90º	100
blur (5)	99.06	rotate 180º	100
blur (7)	97.86	rotate 270º	100
Average:	97.53		

Table 1 contains the results of success rate obtained for each modification. The signature

consist of concatenated bits of 6 features, the total size of the signature is 714 bits (90 bytes). Average success rate for all modification is 97.53%. The success rate for most modifications is close to the results presented in [6] and [7] except histogram equalization which is worse in our method, but the advantage of our method is faster extraction of signatures.

4. USAGE WITHIN A FRAMEWORK FOR DIGITAL RIGHTS INFRINGEMENTS DETECTION

The algorithm described in this paper will be the basis of the ongoing design and development of architecture to manage Intellectual Property Rights (IPR) related to still and moving images in the World Wide Web, in which the authors are involved. The goal is to develop a fast and robust framework for automatic image replica and digital rights infringements detection in the Web and the Hidden Web (Flickr, Picassa, Facebook, YouTube, etc). The system will allow registered users to upload still images and videos to a central database, along with their related Digital Rights Management (DRM) information expressed with MPEG-21 [9].

The MPEG-21 standard specifies the necessary components to manage multimedia content through the digital value chain, and one of its parts, Part 5 [10], defines a Rights Expression Language (REL) for declaring permissions and constraint of use of digital content. REL licenses declare who has rights over a digital content, and under which circumstances.

The system will crawl the Web in order to find replicas of the users' images, and then, according to the related MPEG-21 metadata, report the corresponding events. The possible applications are detection of copyright-violation or other digital rights infringements, monitoring of royalty payments, detection of illicit content (e.g. child pornography) or statistics.

5. CONCLUSION

In this paper a signature for content-based image copy detection is described. The extraction of the signature is fast and the detection speed is very efficient – millions of signatures can be compared in a second. Also the precision and recall rates are high for many commonly used modifications of images. These properties allow the signature to be applied for the detection of image copies in big image databases and on the Internet, e.g. in the Digital Rights Infringements Detection system. The limitation of the signature is that it cannot detect all possible image modifications, especially heavy cropped images.

ACKNOWLEDGEMENT

This work has been partly supported by the European Network of Excellence VISNET-II (IST-2005-2.41.6), funded under the European Commission IST 6th Framework Program (http://www.visnet-noe.org).

REFERENCES

[1] E. Chang, J. Wang, C. Li, G. Wilderhold. "Rime: A Replicated Image Detector for the World-Wide Web", *Proceedings of SPIE Symposium of Voice, Video, and Data Communications*, November 1998

[2] Y. Maret, F. Dufaux, T. Ebrahimi, "Adaptive Image Replica Detection Based on Support Vector Classifiers", *Signal Processing: Image Communication*, 21(8), 688-703

[3] Y. Meng, E. Chang, B. Li, "Enhancing DPF for Near-replica Image Recognition", *IEEE Computer Vision and Pattern Recognition*, 2003

[4] Y. Ke, R. Sukthankar, L. Huston, "An Efficient Parts-based Near-duplicate and Sub-image Retrieval System", *12th ACM International Conference on Multimedia*, New York, USA, 2004, pp. 869-876

[5] MPEG Video Sub-Group, "Call for Proposals on Image and Video Signature Tools", MPEG Doc No. N9216, Lausanne, Switzerland, July 2007

[6] P. Brasnett, M. Bober, "Visual identifier proposal & evaluation results", MPEG Doc. No. M14225, Marrakech, Morocco, January 2007

[7] W.-G. Oh, A-Y. Cho, I.-H. Cho, W.-K. Yang, J.-W. Lee, D.-S. Jeong, "New proposal and performance results for MPEG-7 VCE-6 basic conditions," MPEG Doc. No. M14523, San Jose, USA, April 2007

[8] K. Wnukowicz, W. Skarbek, G. Galinski, "Trajectory of Singular Energies for Image Replica Detection", *Special VISNET Session at International Conference on Signal Processing and Multimedia Applications*, Barcelona, Spain, July 2007

[9] ISO/IEC, Information Technology – Multimedia framework (MPEG-21) – Part 1: Vision, Technologies and Strategy, ISO/IEC TR 21000-1:2004, November 2004

[10] ISO/IEC, Information Technology – Multimedia framework (MPEG-21) – Part 5: Rights Expression Language, ISO/IEC 21000-5:2004, March 2004