A New Watermarking Attack Based on Content-Aware Image Resizing

A.H. Taherinia
department of Computer Engineering
Sharif University of Technology
Azadi Ave, Tehran, Iran

M. Jamzad

1, 2 taherinia@ce.sharif.edu, 2 jamzad@sharif.edu

Abstract—In this paper, we propose a new method for damaging and destroying robust invisible watermarks using an image resizing technique which is named seam carving. By using this method we are able to resize watermarked images in a content-aware manner so that the synchronization of the embedder and extractor of watermarking system is broken and the watermark detection becomes impossible. In contrast to the available benchmarks like Stirmark, proposed attack does not severely reduce the quality of the watermarked image. Therefore it maintains the commercial value of the watermarked image. We have tested the proposed method to attack 3 recent and robust watermarking methods and the results sound impressive. The NC for all extracted watermarks after applying this attack is lower than predefined threshold 0.4, so they are not detectable. The proposed method is a generic attack which does not consider any knowledge about the underlying watermarking algorithm.

Index Terms—Content-aware image resizing, Image retargeting, Watermarking attacks

I. INTRODUCTION

Digital watermarks have been proposed as a potential method for protection of ownership rights on digital audio, image, and video. Research in this topic has progressed along two paths, while new watermarking technologies are being developed [1-3]; some researchers are also investigating different ways of attacking digital watermarks [4-6]. In fact, as soon as people have tried to develop watermarking technologies, others have attempted to break them. Common attacks to watermarks usually aim to destroy the embedded watermark or to impair its detection.

An attack in watermarking technology is any processing that may impair detection of the watermark. Early attacks, such as random geometric distortions [4] relied on the fact that most watermarking algorithms are based on some form of correlation, which itself requires good alignment properties. Breaking this alignment usually prevents reliable detection.

Current techniques reported in the literature for watermarking benchmarks concentrate mainly on images and can be grouped into two main classes. The first group includes the attacks which attempt to remove the watermark and the other group those which just prevent the detector from detecting them. Random geometric distortions fall in the second category. Attacks in the first category usually try to estimate the original non-watermarked cover-signal, considering the watermark as noise with given statistic. For instance, Langelaar et al. showed that 3×3 median filtering gives a good approximation of original pictures in the case they have been watermarked using spread-spectrum [7]. So far, estimate-and-remove attacks have introduced fairly strong blurring effects but in a recent work that is based on maximum a posteriori watermark estimation and remodulation have given promising results [5].

In case of fingerprinting, another way to remove the watermark is to use copies from different sources and mix them (either by averaging them or concatenating pieces of them like a Mosaic attack [8]) to generate an un-watermarked copy. These are usually referred to as collusion attacks [8].

In this paper, a method for resizing watermarked images in a content-aware manner is presented. The proposed attack not only uses geometric constraints, but considers the image content as well. We use a simple image operator called seam carving [9] that supports content-aware image resizing for both reduction and expansion. A seam is an optimal 8-connected path of pixels on a single image from top to bottom, or left to right, where optimality is defined by an image energy function. By repeatedly carving out or inserting seams in one direction we can change the aspect ratio of an image. By applying this operator in both directions we can retarget the image to a new size. Therefore, synchronization of the embedder and extractor of watermarking system is broken and the detection becomes impossible.

The rest of the paper is organized as follows: in the section 2 content-aware image resizing is discussed and in the section 3 some experimental results is shown. Section 4 is for conclusion.

II. CONTENT-AWARE IMAGE RESIZING ATTACK

For verifying the security and robustness of watermarking algorithms, specific attacks have to be applied to test them. Standard image scaling is not sufficient since it is oblivious to the image content and typically can be applied only uniformly. Cropping is limited since it can only remove pixels from the image periphery. More effective resizing can only be achieved by considering the image content and not only geometric constraints.

The proposed attack only is a generic attack need the watermarked image and is completely free from any pre-assumption on the watermarking algorithm or any other parameters that is used during the watermark embedding procedure.

In [9] Avidan et al. proposed a simple image operator, they named it seam-carving, that can change the size of an image by gracefully carving-out or inserting pixels in different parts.