Int. J. Electron. Commun. (AEÜ) 68 (2014) 644–652

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

journal homepage: www.elsevier.com/locate/aeue

Blind method for rescaling detection and rescale factor estimation in digital images using periodic properties of interpolation

Gajanan K. Birajdar[a,*], Vijay H. Mankar[b]

[a] Priyadarshini Institute of Engineering & Technology, Nagpur 440019, Maharashtra, India
[b] Department of Electronics & Telecommunication, Government Polytechnic, Nagpur 440001, Maharashtra, India

ARTICLE INFO

Article history:
Received 20 October 2013
Accepted 26 January 2014

Keywords:
Image manipulation detection
Resampling detection
Passive authentication
Image interpolation
Discrete Fourier transform (DFT)

ABSTRACT

Availability of the powerful image editing softwares and advancement in digital cameras has given rise to large amount of manipulated images without any traces of tampering, generating a great demand for automatic forgery detection algorithms in order to determine its authenticity. When altering an image like copy–paste or splicing to conceal traces of tampering, it is often necessary to resize the pasted portion of the image. The resampling operation may highly likely disturb the underlying inconsistency of the pasted portion that can be used to detect the forgery. In this paper, an algorithm is presented that blindly detects global rescaling operation and estimate the rescaling factor based on the autocovariance sequence of zero-crossings of second difference of the tampered image. Experimental results using UCID and USC-SIPI database show the validity of the algorithm under different interpolation schemes. The technique is robust and successfully detects rescaling operation for images that have been subjected to various forms of attacks like JPEG compression and arbitrary cropping. As expected, some degradation in detection accuracy is observed as the JPEG quality factor decreased.

1. Introduction

The trustworthiness of images has an important role in many social areas, including: law enforcement, insurance processing, forensic investigation, medical imaging, criminal investigation, surveillance systems, intelligence services, and journalism. For instance, the authenticity of photographs has an essential role in court rooms, where they are used as evidence. Every day newspapers and magazines depend on digital images.

Digital image forgery is the process of tampering the original image in order to change the information represented by an image. There are many ways to categorize the image tampering detection methods based on various image manipulation operations which are surveyed in [1–3]. In the modern age, rapid growth of low cost image processing softwares like Adobe photoshop, GIMP and the advancement in digital cameras has given rise to large amount of doctored images with no obvious traces of tampering, generating a great demand for robust and flexible automatic forgery detection algorithms for verifying the integrity of candidate images. The conventional wisdom that "a photo is fact" is no longer true as visual content can be modified for malicious purposes. Verifying the authenticity of images and detecting traces of tampering requiring no prior knowledge of the image content or any embedded watermarks is an important research field. A good forgery detection algorithm should be passive or blind, requiring no prior knowledge of the image content or any embedded watermarks.

Image forgery detection algorithm aims to verify the trustworthiness of a digital image. Image authentication solution is classified into two types. (1) Active forgery detection and (2) blind or passive forgery detection [4,5]. An active forgery detection technique, such as digital watermarking or digital signatures, uses a known authentication code embedded into the image content before the images are sent through an unreliable public channel. However, this method requires special hardware or software to insert the authentication code inside the image before the image is being distributed. But in real time applications the original image is not available. Passive or blind forgery detection technique uses the received image only for assessing its integrity. The original image has some consistent inherent patterns, which are introduced by the various imaging devices or processing. The tampering may highly likely disturb the underlying statistical property or image consistency of a natural scene image which introduces new artifacts resulting in various forms of inconsistencies. These inconsistencies can be used to detect the forgery.

* Corresponding author at: Pillai HOC College of Engineering & Technology, Raigad 410207, India. Tel.: +91 9224445046.
E-mail addresses: gajanan123@gmail.com, gajanan123@rediffmail.com (G.K. Birajdar), vhmankar@gmail.com (V.H. Mankar).

1434-8411/$ – see front matter © 2014 Elsevier GmbH. All rights reserved.
http://dx.doi.org/10.1016/j.aeue.2014.01.013

In most of the tampered images rotation, rescaling and contrast enhancement are often involved and blind image forgery detection algorithm aims to detect these alterations in image. In copy–paste or image splicing forgery, certain transformations such as scaling, skewing or rotation (i.e. geometrical transformations) are very likely to be used including rescaling frequently. Image rescaling may be accomplished in post-processing using software, and can also be done directly within the camera having a digital zooming function which is achieved with some kind of pixel interpolation. In this paper, we present a method to detect global rescaling and estimate the image rescaling factor based on properties of the zero-crossings of the second difference of the tampered image first described in [6]. The technique is applicable to different interpolation schemes. Results are also presented using different types of input images along with robustness against JPEG compression and arbitrary image cropping operation.

The paper is organized as follows: Section 2 provides a review of related work on this topic. Section 3 describes basics of interpolation and periodicity detection along with properties of the zero-crossings of second difference. Proposed algorithm is presented in Section 4. Section 5 reports experimental results and analysis performed using the UCID [7] database. Finally, Section 6 concludes the paper.

2. Prior work

The resampling process does not leave perceivable artifacts; it causes certain pixels be a linear combination of its neighbours. These pixels are correlated with its neighbours and will appear periodically in the resampled image. These specific periodic correlations between image pixels can be used to detect image manipulation. A M/N resampling of a $1-D$ discrete sequence $x[n]$ involves following steps [8]:

(1) *Upsample:* Create a new signal $x_u[n]$ by inserting $M-1$ zeros after every $x[n]$.
(2) *Interpolate:* Convolve $x_u[n]$ with a low pass filter: $x_i[n] = x_u[n] * h[n]$.
(3) *Decimate:* Collect every Nth sample: $y[n] = x_i[N_n]$, $k = 0, 1, \ldots$

Resampling in two dimensions can be extended in both spatial directions. Different types of resampling algorithms (linear or cubic) differ in the form of the interpolation filter $h[n]$ in step 2. In image processing applications, the most widely used interpolation filters are bi-linear and bi-cubic; hence we investigated the properties of a resampled signal, which uses these filters.

Several passive techniques for image authentication based on resampling detection and rescale factor estimation have been already reported. A method is presented to find the rescaling traces hidden in any portion of an image without resorting to a reference image by using expectation maximization (EM) algorithm in [8]. The EM algorithm estimates the average correlation that is present in the image and subsequently computes the probability of the pixels being correlated to their neighbours. The corresponding correlation probability map (p-map) in the discrete Fourier transform (DFT) domain exhibits periodic peaks that are present due to sampling. This technique is not able to uniquely identify the specific resampling factor. Gallagher [16] proposed a rescaling detection method which exploits periodicity in variance function of their second-order derivative in the interpolated image for detecting the traces of rescaling. This periodicity is computed using DFT of an averaged signal obtained from the second derivative of the investigated signal. Author verified that interpolation makes the signal and its derivatives periodical,

$$V\{D^{(n)}f^{\phi}(x+\mu\Delta_x)\} = V\{D^{(n)}f^{\phi}(x)\}, \quad \mu \in Z \tag{1}$$

where $D^{(n)}f(x)$ be nth derivative of $f(x)$ and V is the variance. From Eq. (1) it is clear that $V\{D^{(n)}f^{\phi}(x)\}$ is periodic over x with a period Δ_x as the sampling rate. This periodicity depends on the interpolation kernel used. The commonly used methods are nearest neighbour, bilinear, bi-cubic and B-spline interpolations. The major limitation of the method is that it cannot be applied to rotated or skewed images.

In [15], a blind and automatic method to estimate scaling factors of some image region of interests (ROI) is proposed based on the fact that interpolated signals and their derivatives contain specific detectable periodic properties. The method also uses radon transformation to find presence of affine transformation. Authors investigated multidimensional relation between the signal and its derivative has a specific periodicity which is present due to interpolation. It is given by,

$$V\{D^{(n)}f^{\phi}(x+\mu\Delta_x, y+\mu\Delta_y)\} = V\{D^{(n)}f^{\phi}(x,y)\}, \quad \mu \in Z \tag{2}$$

Detection of resampling in pixel domain is proposed in [6]. Additionally, frequency domain techniques are employed to localize the portion of the image that has been tampered with. Pixel domain techniques are based on properties of second difference. A binary sequence $p[k]$ is constructed from the sequence of second difference $x''[k]$ to detect resampling as given below,

$$\begin{aligned} p[k] &= 1 \quad \text{if } x''[k] = 0 \\ &= 0 \quad \text{otherwise} \end{aligned} \tag{3}$$

DFT of Eq. (3) will display distinct peaks showing the presence of periodic zeros in the second difference. Another method is based on zero crossings of the second difference of a resampled sequence which exhibits periodicity. The second difference is constructed and zero crossings of the obtained sequence is computed. A binary sequence is constructed using the equation below,

$$\begin{aligned} p[k] &= 1 \quad \text{if } x''[k] > 0 \text{ and } \; x''[k+1] \le 0 \\ &= 1 \quad \text{if } x''[k] < 0 \text{ and } \; x''[k+1] > 0 \\ &= 0 \quad \text{otherwise} \end{aligned} \tag{4}$$

The major limitation of this method is similar to [16]. However, the rescale factor estimation technique is not discussed. We present a method based on Eq. (4) which estimates rescale factor of the resampled image.

A method is investigated to detect resampled imagery which is based on examining the normalized energy density present within windows of varying size in the second derivative of the image in the frequency domain, and exploiting this characteristic to derive a 19-D feature vector that is used to train a support vector machine (SVM) classifier [14]. However the method described just detect the presence of resampling, how to estimate the resampling rate is not described. Another method is presented for detecting interpolation by using the periodicity characteristics hidden among the rows (or columns) of the image [17]. The core of the algorithm is the use of correlation coefficients based on the observation that the correlation coefficients of the row (or column) vectors vary periodically in resampled image. A blind and efficient method which is capable of finding traces of resampling and interpolation based on singular value decomposition (SVD) is proposed in [12,13]. The specific statistical changes brought into the linear dependencies among image pixels and image rows/columns due to tampering are analyzed using SVD. However, both methods detects only resampling and the rescale factor estimation is not possible.

In [11], a technique is developed to detect doctored and manipulated images using three features, the binary similarity measures between the bit planes, the image quality metrics applied to denoised image residuals, and the statistical features obtained from the wavelet decomposition of an image. Image rescaling and