ON RESAMPLING DETECTION AND ITS APPLICATION TO DETECT IMAGE TAMPERING

Prasad S.

Department of Electrical Engineering
Indian Institute of Science, Bangalore, India

K. R. Ramakrishnan

Department of Electrical Engineering
Indian Institute of Science, Bangalore, India

ABSTRACT

Usually digital image forgeries are created by copy-pasting a portion of an image onto some other image. While doing so, it is often necessary to resize the pasted portion of the image to suit the sampling grid of the host image. The resampling operation changes certain characteristics of the pasted portion, which when detected serves as a clue of tampering. In this paper, we present deterministic techniques to detect resampling, and localize the portion of the image that has been tampered with. Two of the techniques are in pixel domain and two others in frequency domain. We study the efficacy of our techniques against JPEG compression and subsequent resampling of the entire tampered image.

1. INTRODUCTION

The advent of digital cameras has made photography easier, and the cheap availability of digital cameras in various forms has made itself an essential household gadget across the globe. As a result several millions of digital photographs are created every day. In addition to this, modern sophisticated photo editing softwares like Adobe Photoshop, GIMP, PaintShop Pro provide user friendly environments to edit digital images. So, images can be easily tampered and can be used in various unethical ways. In this context, it becomes extremely important to validate the originality of digital images.

There are several techniques described in literature to deal with different kinds of tampering. Popescu et. al [1] have noticed that the color images taken using a digital camera has specific kind of correlations among the pixels, due to the interpolation in the color filter array. These correlations are likely to be destroyed, when the image is tampered. Ng et. al [2] have described techniques to detect photomontaging. They have a classifier based on the bi-coherence features of the natural images and photomontaged images. They also have proposed a mathematical model for image splicing [3]. One of the fundamental operations that needs to be done to create forgeries is resizing. It is an operation that is likely to be done irrespective of the kind of forgery (copy move, photomontage, etc.). So, it is of interest to detect resampling in images. Popescu et. al. [4] have described a method to estimate the resampling parameters in a discrete sequence and have shown its applications to image forensics. They have shown that, for a certain type of resampling, some specific samples in a resampled sequence can be written as a linear combination of their neighbouring samples. Those samples are separated by a specific interval. Under certain assumptions, the scalars of the linear combination can be estimated using an expectation-maximization(EM) algorithm. It is this presence of periodic correlations, that gives the evidence of resampling.

In this paper, we further investigate the properties of a resampled discrete sequence and present deterministic techniques to detect resampling.

We call an image *original*, whenever it is acquired out of a digital camera and has not been altered, even in its resolution or size. A *tampered image* is one which is deliberately altered in its content. We call that portion of the image which has been pasted from some other image as *alien* portion.

2. RESAMPLING

A $\frac{M}{N}$ resampling of a 1-D discrete sequence $x[k]$ involves the following three steps [4]

1. *Up-sample*: Create a new signal $x_u[k]$ by inserting M-1 zeros after every $x[k]$
2. *Interpolate*: Convolve $x_u[k]$ with a lowpass filter: $x_i[k] = x_u[k] \star h[k]$
3. *Decimate* : Pick every N^{th} sample: $y[k] = x_i[Nk], k = 0, 1, ...$

Resampling in two dimension is a straight forward application of the above mentioned operations in both spatial directions. In image processing applications, the most widely used interpolation filters are bi-linear and bi-cubic. So, we carefully examine the properties of a resampled signal, which uses these two kind of filters.

3. DETECTING RESAMPLING IN PIXEL DOMAIN

In this section, we first describe the techniques to detect resampling in one dimension and then its extension to two dimensions.

3.1. Properties of the second difference

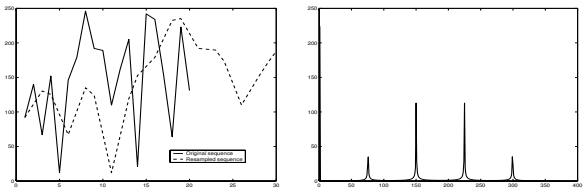
Suppose a sequence has been resampled with a factor $\frac{M}{N} \geq 2$, then the following are observed. Every N samples in the original sequence will get expanded to M samples, with a few original samples retained in the resulting sequence. With $\frac{M}{N} \geq 2$, we are assured of a condition that between every two original samples there are at least two more interpolated samples(Pigeon hole principle).

Let us re-look the pigeon hole principle in our resampling context. Suppose the original sequence had P samples, then once the resampling by a factor M/N has been done, then there are totally (P*M)/N equally spaced samples. When M/N is ≥ 2, this means we have to introduce at least one interpolated sample between every pair of adjacent samples in the original sequence. In case of linear and cubic interpolation kernels, the first difference of the samples between a pair of original samples are equal. So, the second difference will produce a zero at that location. To be more specific, every N^{th} sample in the original sequence will be the M^{th} sample in resampled sequence. Hence, the occurrence of zero is within that interval of M samples. Moreover, the positions at which a zero occurs within the M sample interval is precisely fixed by the numbers M and N. Hence, in every interval of M samples, the second difference produces zero in a periodic pattern. It is this periodicity that characterizes a resampled signal. It is highly unlikely for a natural sequence to display this periodicity.

To detect resampling, a binary sequence $p[k]$ is constructed from the sequence of second differences $x^{''}[k]$, as shown below

$$p[k] = \begin{cases} 1 & \text{if } \left| x^{''}[k] \right| = 0 \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

The DFT magnitude of this binary sequence will display distinct peaks, showing the presence of periodic zeros in the second difference. This is shown in fig. 1



(i) (ii)

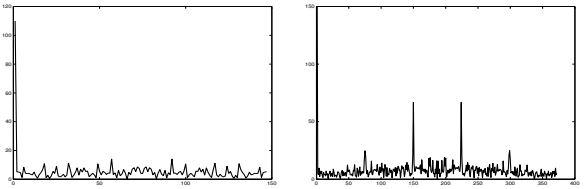
Fig. 1. (i)Plot of the first few samples of a original and 5/2 resampled sequence, and (ii)DFT magnitude of the binary sequence constructed as per (1)

3.2. Properties of the zero-crossings of the second difference

The zero-crossings of the second difference of a resampled sequence exhibits a periodicity that is absent in a non-resampled sequence. This behaviour is consistent for linear, cubic and gaussian smoothing kernels. This fact can be used to detect resampling in discrete sequences. We construct the second difference sequence and find the zero crossings of the obtained sequence. A binary sequence is constructed as per the following conditions.

$$p[k] = \begin{cases} 1 & \text{if } x^{''}[k] > 0 \quad and \quad x^{''}[k+1] \leq 0 \\ 1 & \text{if } x^{''}[k] < 0 \quad and \quad x^{''}[k+1] \geq 0 \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

This binary sequence will exhibit a periodicity, which can be observed by plotting the magnitude of its DFT. The DFT will display distinct peaks, which is absent in case of a non-resampled sequence. This is illustrated in fig.2. In case of sequences, which are composites of a resampled part and a non-resampled part, the DFT of the second difference zero crossings may not be able to produce distinct peaks because of averaging. One easier way to overcome this difficulty is to look at the short time DFTs of the sequence. The choice of the window length of the short time DFT is a heuristic, and the technique is more effective when is window length is less than the length of resampled portion. In our experiments, we varied the window length from 1/16 to 1/2 of the overall length of the sequence, in discrete steps.



(i) (ii)

Fig. 2. DFT magnitude plots of the logical sequences constructed according to (2), corresponding to (i) original sequence, and (ii) 5/2 resampled sequence shown in fig.1 (i)

3.3. Extension to two dimensions

Extending the techniques mentioned in sections 3.1 and 3.2 to two dimensions is straight forward. Each row or column is treated as a 1-d sequence and tested for resampling. The resulting binary sequences are stacked together to form a binary image. The region which has undergone resampling, is visible distinctly. Also, the 2-d DFT magnitude of the resulting image produces distinct peaks, which confirm the presence of resampled region in the image.

4. RESAMPLING DETECTION IN FREQUENCY DOMAIN

In this section, we present two frequency domain techniques.

4.1. Tamper detection using DCT high pass filtering

Whenever an image undergoes up-sampling, the spectra of the image gets periodically repeated. Upon interpolating in spatial domain, the image is lowpass filtered, so as to retain only the original spectra and to remove all the other copies of it. But, all practical filters are non-ideal and hence there is no perfect lowpass filtering. If a resampled image portion is pasted on another image there is an inconsistency in the high-frequency content of the over all image. So, a careful highpass filtering will bring out the differences. A straightforward technique to illustrate this is to compute the block DCT of the entire image, retain only a few high frequency coefficients, and to reconstruct back the image. The reconstructed image clearly marks out that alien portion, which has been pasted onto it. The size of the blocks to compute DCT is generally taken to be 8x8. The number of coefficients to be retained is much of a heuristic. In our work, we experimented by retaining 4x4, 2x2 and 1x1 high frequency coefficients.

4.2. Tamper detection using wavelets

Instead of using DCT and retaining a few high frequency coefficients by brute force truncation, one can analyze images using wavelets. The image is decomposed into an approximation(A) and three details, horizontal, vertical and diagonal(H, V and D). Then, the image is reconstructed using only the diagonal detail coefficients, D and discarding the others. The resampled portion of the image is smoothened by interpolation filter and hence the high frequency content of that region is poor compared to the other regions of the image. So, the reconstructed image clearly distinguishes between the original portion and the tampered portion. The lack of high frequencies is clearly made out in the region that has been resampled. Here again, the usage of a particular wavelet to analyze and reconstruct, is more of a heuristic. In our work, we use biorthogonal 3.5 wavelet for all our experiments.

5. SIMULATIONS AND RESULTS

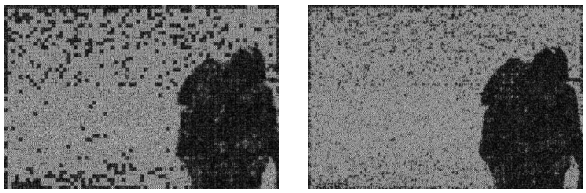
Shown in Fig.3 is a tampered image. The person in the image has been pasted from another image after resampling by a factor of 1.5. We present the results of applying the techniques presented in sections 3.2, 4.1 and 4.2 on this image. To present the result for the technique in 3.1, we use the image in fig.4, where the alien portion has been resampled by a factor 2.1.

Fig.5 (i) and (ii) show the result of applying the DCT highpass technique and wavelet techniques on the test image in fig.3. We clearly notice that the tampered portion is differentiated from other regions in both the images. Also, we note that the result of wavelet method doesn't suffer from blockiness as of DCT method.

Fig.6 shows the results of zero crossing detection method.

Fig. 3. A tampered image: The person in the image has been resampled by a factor of 1.5 and pasted

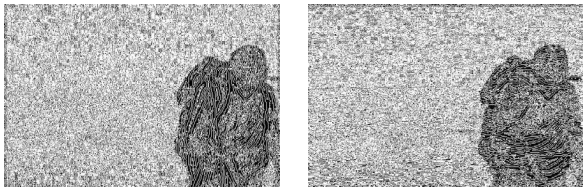
Fig. 4. Another tampered image: The face in the image has been resampled by a factor of 2.1 and pasted



(i) (ii)

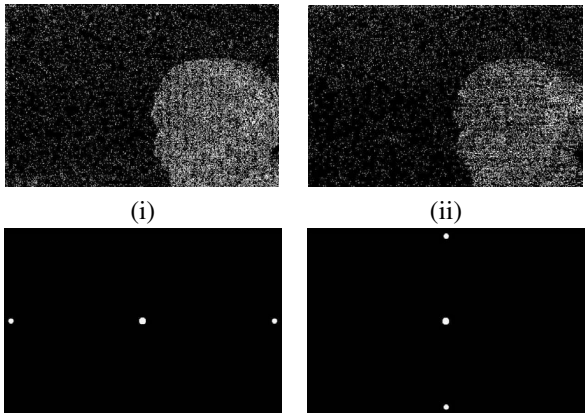
Fig. 5. Result of (i)DCT highpass technique and (ii)wavelet technique applied on image in Fig. 3

Fig.7 (i) and (ii) show the binary image constructed out of second differences of fig.4 according to (1). (iii) and (iv) show the corresponding 2-d DFT magnitude plots, suitably enhanced so that the distinct peaks along the horizontal and vertical directions are visible.



(i) (ii)

Fig. 6. Binary images constructed out of second difference zero crossings method applied on image in fig.4 (i)Horizontal zero crossings, (ii)Vertical zero crossings



(i) (ii) (iii) (iv)

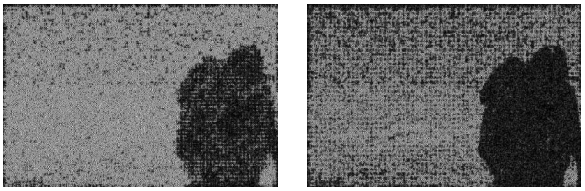
Fig. 7. Binary images constructed out of second difference method applied on image in fig.4 (i)Horizontal differences, (ii)Vertical differences, (iii)Enhanced 2-d DFT magnitude of horizontal differences, and (iv)Enhanced 2-d DFT magnitude of the vertical differences

5.1. Robustness to compression

The above mentioned techniques were also tried on images which are tampered and subsequently JPEG compressed using GNU GIMP. The compression was carried over a range of quality factors. The algorithms perform well for quality factors above 0.85 in GIMP. For factors less than 0.85, the reconstructed images are weak and no conclusive remarks can be made. The results are presented in fig.8

5.2. Robustness to global resampling

In addition to compression, the tampered image may undergo a global resampling. So, the algorithms were tested on tampered images, which are subsequently resampled globally using GNU GIMP. The algorithms perform well for resampling factors above 0.8. The results are presented in fig.8



(i) (ii)

Fig. 8. Result of wavelet technique applied on image in fig.3 after (i) JPEG compressed with a quality factor of 0.85 and (ii) globally resized by a factor of 1.1

6. DISCUSSION

We have presented four new techniques to detect resampling in images. The techniques will distinguish the regions of image that have undergone resampling. If this distinguished portion makes a semantic sense to the observer, then the image can be doubted for being tampered. Moreover, all these four techniques can be combined with complementary techniques such as presented in [5], [6], [1] and [4] to confirm the act of tampering. We are currently working on detection techniques that are more robust to compression and resizing. The work presented here is preliminary and a lot of analysis and experiments need to be conducted. The reader is referred to http://neuronix.ee.iisc.ernet.in/forensics.html for more examples.

7. REFERENCES

[1] Alin C. Popescu and H. Farid, "Exposing forgeries in color filter array interpolated images," *IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3948–3959, October 2005.

[2] Tian-Tsong Ng, Shih-Fu Chang, and Qibin Sun, "Blind detection of photomontage using higher order statistics," in *Proc. of ISCAS*, Vancouver, British Columbia, Canada, May 23-26 2004.

[3] Tian-Tsong Ng and Shih-Fu Chang, "A model for image splicing," in *Proc. of ICIP*, Singapore, Oct 24-27 2004, vol. 2, pp. 1169–1172.

[4] Alin C. Popescu and Hany Farid, "Exposing digital forgeries by detecting traces of re-sampling," *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 758–767, February 2005.

[5] M. K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," in *ACM Multimedia and Security Workshop*, New York, NY, 2005.

[6] Jessica Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery in digital images," in *Proc. of DFRWS*, Cleveland, Ohio, USA, August 5-8 2003.