2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing

A Novel and Secure Image Interpolation Methods for Image Disguise

Shen Wang, Qiong Li, Bian Yang and Xiamu Niu
School of Computer Science and Technology
Harbin Institute of Technology
150001, Harbin, China
xiamu.niu@hit.edu.cn

Abstract—The advent of digital forensic techniques imposes great challenges to the security of image disguise where tampering is involved to conceal the existence of sensitive objects in the source image. As a consequence, image interpolation that is a prerequisite step in image disguise should be adapted to be forensic resistant. This paper proposes a novel and secure interpolation method to facilitate image disguise. As it is reported in the literature, the trace of interpolation can be detected by exploiting the linear relationship among pixels. Therefore, forensic resistant is achieved in this work by breaking the linear relationship among pixels. In particular, genetic algorithm is employed make a balance between forensic resistance and the visual quality of the tampered image.

Keywords: Image Disguise; Digital Forensics; Re-sampling; Genetic Algorithm

I. INTRODUCTION

Protecting the confidentiality of the information is a major concern in information security, and steganography is usually adopted to enforce secure information transmission. However, the embedding capacities of most stego algorithms are quite limited. Therefore, in the case of image transmission, it may be infeasible to embed the whole image that contains some secret objects into the cover image. To tackle this limitation, we propose a novel and secure image transmission paradigm that is referred to as image disguise in this papers. The process of image disguise consists of two steps as illustrated in Fig.1. In the first step, some secret objects are segmented and removed from the source image. Consequently, the regions that contain secret objects are replaced by the objects selected from other images, or filled in via image inpainting methods. It is worth noting that the authorized receiver should be able to recover the secret objects. As a result, we propose to embed the selected secret objects into other regions of the source image. In this way, only a small portion of the source image need to be embedded, which will not impose high requirements on the capacity of the stego algorithm. It should be noted that image tampering is involved in the aforementioned process to conceal the existence of secret objects, and a number of image forensic algorithms have been proposed in recent years to detect the trace of image tampering. Therefore, in order to enhance the security of image disguise, the tampering method in image disguise is expected to be forensic-resistant. As interpolation is usually a prerequisite step in image tempering, our focus is placed on developing a forensic-resistant interpolation method in this paper. To achieve this goal, it is necessary to understand the underlying mechanisms of image forensic algorithms. In this section, we first provide a brief review of several efficient image forensic algorithms. It is observed in [1] that image interpolation will introduce periodic correlations between pixels. Based on this fact, Popescu et al. propose to detect the trace of image tampering by evaluating the correlation between neighboring pixels with the aid of the EM algorithm. The lighting direction is also exploited as a clue for image forensic in [2], as it is difficult to maintain the consistencies in lighting directions of the regions from different source images. However, the lighting direction based scheme is not applied to manipulations where the lighting direction is kept unchanged, such as duplication. A robust and efficient forensic algorithm aiming at detecting duplication is proposed in [3]. In order to enhance the robustness of image forensic against noise and compression, PCA is employed to generate a coarse representation of the image.

As mentioned above, one of the characteristic of interpolation operation is that it will result in the periodic correlations between pixels. Thus, forensic-resistant is achieved in the proposed work by breaking the periodicity of pixel correlations. At the same time, the visual quality of the interpolated image is maintained at a satisfactory level. Different from conventional interpolation methods, the proposed work aims at achieving a reasonable tradeoff between the visual quality of the interpolated image and the confidentiality of the interpolation operation. Therefore, Genetic algorithm[7] is employed in this paper to balance these two conflicting factors. Genetic algorithm can also find extensive applications in multimedia security, such as steganography [6] and digital watermarking [4,5].

The rest parts of this paper are organized as follows. The proposed genetic based interpolated method is elaborated in Section 2. Experimental results are provided in Section 3 to demonstrate the effectiveness of the proposed work. Finally, this paper is concluded in Section 4.

978-0-7695-4222-5/10 $26.00 © 2010 IEEE
DOI 10.1109/IIHMSP.2010.123

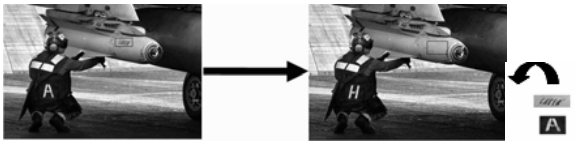

Figure 1. The process of Image Disguise

II. PROPOSED SCHEME

A. Re-sampling Signals and Detecting Re-sampling

In the previous notable work, the digital forging is detected by the trace of the re-sampling. In the creation of digital forgeries, the resize, rotation and stretch always introduce re-sampling into the images. Theoretically, the re-sampling is a process of convolution or filtering. Let X denote a 1-D signal with N elements and the size of re-sampling filter h be $2L$. The re-sampling with factor P/Q is the combination of P times linear interpolation and Q times decimation, where P, $Q \in N$, as shown in Figure .The process can be formulated as:

$$Y = A_{P/Q} X \tag{1}$$

$$A_{P/Q} = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1N} \\ h_{21} & \cdots & \cdots & h_{2N} \\ \vdots & \vdots & \vdots & \vdots \\ h_{M1} & \cdots & \cdots & h_{MN} \end{bmatrix}_{M \times N} \tag{2}$$

where

$$M = \left\lfloor \frac{PN}{Q} \right\rfloor \tag{3}$$

[ ] is rounding operator.

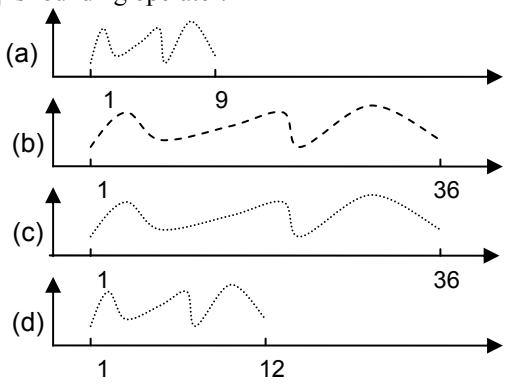

Figure 2. Re-sampling a signal by a factor of P/Q=4/3: (a) the original signal; (b) the up-sampled signal by a factor 4; (c) the interpolated signal; (d) the final re-sampled signal(the down-sampled signal by a factor 3).

In equation 4, h_{ij} is only determined by i, j, P, Q and L.

$$h_{ij} = 1 - \frac{|j - C|}{\sum_{C-L \le j \le c+L} |j - C|} \tag{4}$$

where $C = Qi/P$. Thus, $A_{P/Q}$ is a $M \times N$ banded matrix. For $L \le i \le M - L$, the coefficients of *h* are periodic with period P. If X is a 2-D signal, $A_{P/Q}$ becomes a block matrix. The periodicity of h still exists.

Alin C.Popescu detects the periodicity by EM algorithm[1]. The algorithm includes follow steps:

1. For each pixel y_i, calculate the residual

$$R(i) = \left| y_i - \sum_{k=-N}^{N} \alpha_n(k) y(i+k) \right| \tag{5}$$

2. Calculate the conditional probability

$$P(i) = \frac{1}{\sigma_n \sqrt{2\pi}} e^{-R(i)^2 / 2\sigma_n^2} \tag{6}$$

It is the probability of $y_i \in S$, where *S* is the set of the pixels which are created by re-sampling.

3. Estimate the posterior probability $w(i)$ of $y_i \in S$

$$w(i) = \frac{P(i)}{P(i) + p_0} \tag{7}$$

4. Renew σ_{n+1} and α_{n+1} by the least square method.

After set the initial values p_0, σ_0 and α_0, execute 1-4 steps iteratively until reach convergence. If the image has been re-sampled, the distribution of *w* is periodic. In the Fourier transform domain, peaks appear because of the periodicity.

B. Genetic Algorithm based Interpolation

The trace of re-sampling may be eliminated by changing the pixel values of the image. But the manipulation decreases the image quality. In this paper, we adopt genetic algorithm to a balance. Our genetic method adjusts the pixels in follow steps:

1. The image is divided into $n \times n$ blocks. Consider X as the pixels in the block and h_i is the interpolation filter for the *i*-th pixel.

2. Initialization. Create 100 blocks by changing each pixel in the original block randomly as the initial chromosomes C.
3. Selection. Select the best chromosomes, which maximize the fitness function, as the candidate of crossover. The fitness function considers two aspects, first one is the residual

$$R_{oi} = \sum_i (y_i - h_i * x_i^N) \qquad (8)$$

where x_i^N is the neighbors of pixel x_i. The other aspect is the image quality, which is measured by peak signal noise rate (PSNR). Thus, the fitness function is:

$$Fitness = aR_{oi} + PSNR \qquad (9)$$

where a is the weight used to balance the two parameters.

4. Crossover. Exchange pixels in the blocks with high fitness. If crossover has been applied more than predetermined times, stop the cycle.

III. EXPERIMENTAL RESULT

In the experiments, two 128×128 gray–level images are used as shown in Figure 3(a) and Figure 7(a). Figure 3(b) and Figure 7(b) show the detection results *W* of re-sampling. FFT coefficients *F* of the detection results are shown in Figure 3(c) and Figure 7(c). It is easy to found that *W* are not periodic and there is no abnormal peaks in *F*.

Figure 4(a) shows the image scaled with factor 1.1. Figure 8(a) shows the image scaled with factor 0.9. Figure 4(b) and Figure 8(b) shows the detection results *W* of re-sampling. FFT coefficients *F* of the detection result are shown in Figure 4(c) and Figure 8(c). After scaling, *W* are periodic and peaks in *F* are found.

Figure 5(a), Figure 6(a) and Figure 9(a) show the images manipulated by our algorithm. The PSNR of them are 37.03, 31.5 and 36.8. Figure 5(b), Figure 6(b) and Figure 9(b) shows the detection results *W* of re-sampling. FFT coefficients *F* of the detection result are shown in Figure 5(c), Figure 6(c) and Figure 9(c). It is easy to found that *W* are not periodic and there is no abnormal peaks in *F*. Comparing Figure 5 and Figure 6, we know that the quality could be degraded a little in order to obtain stronger security.

Figure 3. (a) Original image (b) detection result (c) FFT transform of (b)

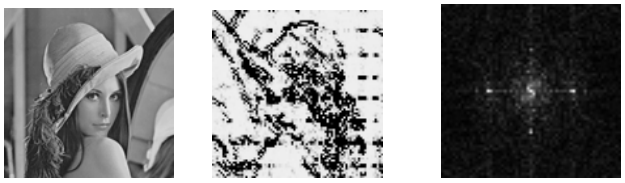

Figure 4. (a) image scaled with factor 1.1 (b) detection result (c) FFT transform of (b)

Figure 5. (a) image manipulated by our algorithm (b) detection result (c) FFT transform of (b)

Figure 6. (a) image manipulated by our algorithm (b) detection result (c) FFT transform of (b)

Figure 7. (a) Original image (b) detection result (c) FFT transform of (b)

Figure 8. (a) image scaled with factor 0.9 (b) detection result (c) FFT transform of (b)

Figure 9. (a) image manipulated by our algorithm (b) detection result (c) FFT transform of (b)

IV. CONCLUSION

A genetic algorithm based image interpolation method is proposed in this paper to facilitate image disguise. Intensive experiments have been conducted to evaluate the effectiveness of the proposed work. As indicated by experimental results, the trace of interpolation is concealed without introducing remarkable degradation on the visual quality of the tampered image.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China (Project Number: 60703011, 60832010, 60671064), the Chinese national 863 Program (Project Number: 2007AA01Z458), and The Research Fund for the Doctoral Program of Higher Education (RFDP: 20070213047).

REFERENCES

[1] A. C. Popescu and H. Farid. Exposing digital forgeries by detecting traces of resampling. IEEE Transactions on Signal Processing, 53(2):758--767, 2005.

[2] M. K. Johnson and H. Farid, "Exposing Digital Forgeries by Detecting Inconsistencies in Lighting", In ACM Multimedia and Security Workshop, New York, NY, 2005.

[3] A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions", TR2004-515, Computer Science.

[4] H. C. Huang, C. M. Chu and J. S. Pan. The optimized copyright protection system with genetic watermarking. Soft Computing, 13(4):333–343, 2009.

[5] H. C. Huang, J. S. Pan, Y. H. Huang, F. H. Wang and K. C. Huang. Progressive watermarking techniques using genetic algorithms. Circuits, Systems, and Signal Processing, 26(5):671–687, 2007.

[6] S. Wang, B. Yang and X. M. Niu. A Secure Steganography Method based on Genetic Algorithm. Journal of Information Hiding and Multimedia Signal Processing, Vol. 1, No. 1, pp. 28-35, Jan. 2010.

[7] D. E. Goldberg. The genetic algorithms in search, optimization and machine learning. Addison-Wesley, 1989.