위변조 검출을 위한 SVD 디지털 이미지 포렌직

송근실*, 김미애**, 이원형***
중앙대학교 첨단영상대학원 영상공학과

SVD-Based Digital Image Forensics for Detecting Tampering

Geun-Sil Song*, Mi-Ae Kim**, Won-Hyung Lee***
Department of Image Engineering,
Graduate School of Advanced Imaging Science Multimedia & Film,
Chung-Ang University
E-mail : *gssong@wm.cau.ac.kr, **kimma@dreamwiz.com, ***whlee@cau.ac.kr

Abstract

The proposed method measures the correlation maps of SVD that are used to interpret data relations and structures between the original image and the distorted image. It seems that the SVD results can be used to assist us in gaining information about covariance structure of two images. This method is able to work in the complete absence of any digital watermark or signature. The effectiveness of this method is seen through testing the robustness against JPEG compression.

I. 서론

The success of the Internet has made it possible to create, replicate, and distribute digital contents without loss of its quality. Moreover digital images can be easily modified and edited because of the availability of powerful image processing and editing software. As a result, it is possible to add or remove important features from an image without leaving any visually obvious traces of tampering. Thus, the detection of digital forgeries has become an important aspect of law enforcement in the court. Digital Watermarking is used to authenticate, validate and communicate information within digital contents. Although digital watermarks have been proposed as a tool to provide useful information about the image integrity and its processing history, the watermark must be inserted either at the time of recording or afterwards by a person authorized to do so.

In this paper, we describe the problem of reliably discriminating between the distorted images from untampered original ones in the absence of any digital watermarks or signatures. The basic idea of our approach is Singular Value Decomposition of the covariance matrix based image processing technique for detection of digital tampering in gray scale image. This method is able to work in the complete absence of any watermark.

II. 본론

The proposed method measures eigenvectors of SVD that is used to analyze data relations between the original image and the distorted image. Let X be the original image of $m \times n$ matrix and let Y be the distorted image of $m \times n$ matrix. The scheme for detection of malicious manipulation with digital gray images using eigenvectors of SVD is presented:

① Compute the average matrix (Ψ) of the two images

.

X and Y, then the result stored in the variable Φ_i:

$$\psi = \frac{1}{M}\sum_{n=1}^{M}\Gamma_n \quad (1)$$

$$\Phi_i = \Gamma_i - \Psi \quad (2)$$

where M is the number of testing images that is the number of X and Y, and Γ is the set of the two images X and Y.

② Calculate the covariance matrix C_{xy}:

$$C_{xy} = \frac{1}{M}\Phi_n\Phi_n^T \quad (3)$$

③ Decompose the SVD of the cross-covariance matrix of the two images X and Y, then the eigenvectors (u_i, v_i) and the corresponding eigen values σ_i should be calculated. The eigenvectors indicate the degree of variance against the average matrix of images:

$$(u_i, v_i) = \frac{1}{M}\sum_{n=1}^{M}\sigma_{ik}\Phi_k \quad (4)$$

④ The difference map is calculated with estimated eigenvectors of the step ④

Ⅲ. 구현

In the results presented in our paper, we applied the measure to 512×512 gray scale images. In order to quantify results from specific forms of digital tampering, we tested robustness against JPEG compression. Fig.1 shows the histograms of the difference map between the original and the distorted images against JPEG compression. Our purpose is to detect if the image has been JPEG compressed and the histograms of the difference maps are computed. If these histograms contain periodic patterns, then the image is very likely to have been JPEG compressed. Each image is JPEG compressed with quality factors 85, and 75.

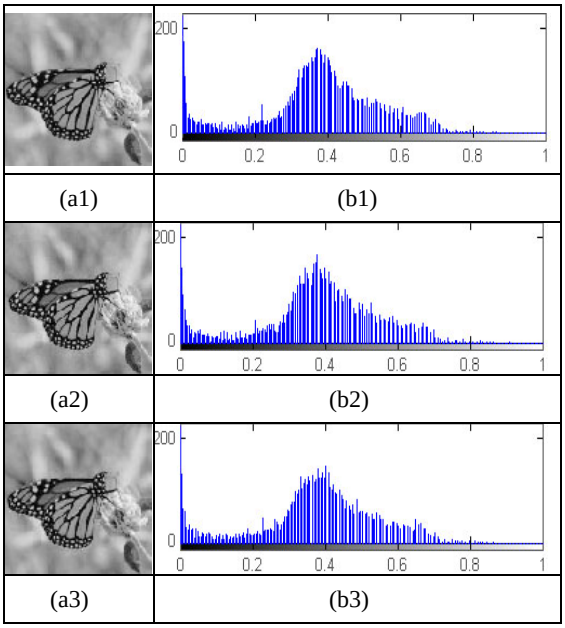

Fig. 1 Shown are original (Fig. 1 (a1) and JPEG compressed images (Fig. 1 (a2) the quality 85 and (a3) the quality 75) and their histograms for compressed JPEG images (Fig1. (b1) to (b3)

Ⅳ. 결론

We described the passive-blind image forgeries detection approaches in the absence of any digital watermark into gray scale digital images. Especially detection of malicious manipulation with digital images is the topic of this paper. We analyzed the histograms for compressed JPEG images using image patch features. As results, .the proposed methods successfully detect the periodic patterns when the distorted image is re-saved in a lossy format, such as JPEG compression. Our hope is that the proposed methods will be needed to reliably expose digital forgeries.

참고문헌

[1] A. C. Popescu and H. Farid, “Satistical tools for digital forensics”, In Proceedings of the 6th Information Hiding Workshop, 05. 2004.

[2] J. Fridrich, D. Soukal, and J. Lukas, “Detection of Copy-Move Forgery in Digital images”, Proc. of DFRWS 2003, 08. 2003.