# An Implementation and Pragmatic Analysis of the Digital Image Forgery Detection Schemes

Hansoo Kim and Joong Lee

***Abstract*—We select the most effective and remarkable schemes among the state-of-the-art digital forgery detection schemes and implement a system based on these schemes. With that, we compare the advantages and limitations of each scheme by experimental analysis. As a result, the detection rate of the schemes is dependent of the parameters of the schemes and the forgery method of the image, although the schemes succeed to detect most of the forged images. Also, a number of forged images are not detected which are off the detection points of the schemes.**

***Index Terms*—Digital image forgery, forgery detection, digital forensics, forensic implementation, forensic practice (alphabetical order).**

## I. Introduction

A picture may worth a thousand words. Like the proverb "seeing is believing", a picture can affect the thought, behaviour, identity, money, and even a life of a person, a society, and a country. With the advent of low-cost and high-resolution digital cameras and sophisticated editing software, digital images can be easily manipulated and altered [1]. Forgery is the process of making, adapting, or imitating objects, statistics, or documents with the intent to deceive or make usually large amounts of money by selling the forged item [2]. We define the term of digital image forgery as the process of modifying the original image obtained from a camera, by splicing (including adding, moving and deleting), blurring, rotating and/or resizing the original image.

Image forgery can be traced back to as early as 1840s when Hippolyte Bayard created the fake image, in which he was shown committing a suicide [3]. Forged images, often leaving no visual clues of having been forged, can be indistinguishable from the original images. As a result, photographs no longer hold the unique stature as a definitive recording of events [1]. Owing to such sophisticated digital image editing software tools, the establishment of the authenticity of a digital image has become a challenging task, encompassing a variety of issues. In this age of illusions, there is a huge question mark over the use of multimedia data as evidence in the courts of law [3].

Digital image forensics, or the digital image forgery detection, is a field that analyses images of a particular scenario to establish credibility and authenticity through a variety of means [3]. It is becoming a popular field that it can compensate human visual inspection which is said to be subjective and unreliable. It also gains its importance because of its potential applications in many domains, such as intelligence, sports, legal services, news reporting, medical imaging and insurance claim investigations [4]. Detecting the traces of resampling forgery by finding a set of periodical samples correlated to their neighbors is proposed [1]. Detecting the image forgeries by CFA (color filter array) demosaicing artifacts is also proposed [5]. Recently, detecting the image interpolation forgeries by differences of the image frequency is proposed [6]. Also, researches have emerged that review a number of state-of-the-art digital image forgeries detection schemes [3], [4], [7], [8].

Among those, we select the most effective and remarkable schemes and implement a digital image forgery detection system based on these schemes. And, we compare the advantages and limitations of each scheme by experimental analysis.

As a result, the digital image forgery detection schemes are dependent of the parameters of the schemes and the forgery method of the image, although most of the schemes succeed to detect the forged images. Also, a number of forged images are not detected which are off the detection points of the schemes.

The rest of the paper is organized as follows. The selected schemes for the implementations are reviewed in Section II. Each scheme is implemented and analysed in Section III. In Section IV, the overall result is stated with conclusion.

## II. Related Work

### A. The Interpixel Correlation [1]

Resampling is defined as processing the original image onto a new sampling lattice [1]. It includes resizing and/or rotating the entire or part of an image, which can be regarded as a partial form of an image forgery. When a digital image is resampled, it introduces specific correlations into the image which when detected can be used as evidence of digital forgery [1], that is, the underlying statistics of an image is altered when it is forged.

$$y_i = \sum_{k=-N}^{N} a_k y_{i+k} \tag{1}$$

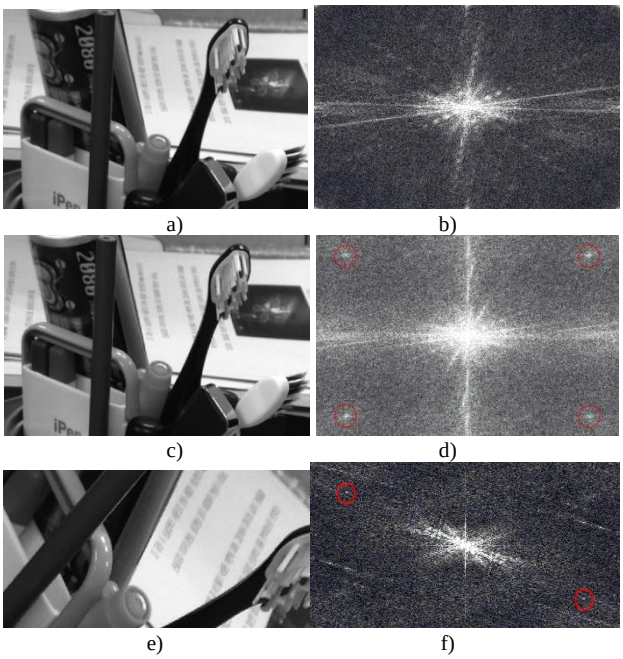
Given a signal that has been resampled by a known amount and interpolation method, it is possible to find a set of periodic samples that are correlated in the same way to their neighbors. The samples satisfy (1), where $y_m$ is the $m$-th sample of the resampled signal, $a_n$ is the $n$-th scalar weight and $N$ is the number of neighbors considered for the

Manuscript received April 2, 2015; revised September 22, 2015. This work was supported by a fund (NFS2015DTB01) from the forensic research program of the National Forensic Service, Korea.

The authors are with National Forensic Service, 10, Ipchunro, Wonjusi, Gangwondo, Korea (e-mail: kutistar@sogang.ac.kr, ljfirst@korea.kr).

correlation.

In order to determine if a signal has been resampled, the Expectation Maximization algorithm (EM) [9] is adopted to simultaneously estimate a set of periodic samples that are correlated to their neighbors, and the specific form of these correlations.



a) b) c) d) e) f)

Fig. 1. An example of the experimental result for the interpixel correlation. a) a genuine image. b) An up-sampled version of a) by 25% using bicubic interpolation. c) A rotated version of a) by clockwise 40°. d) The Fourier transform of probability map of a). e) The Fourier transform of probability map of b). f) The Fourier transform of probability map of e).

The example of the experimental results of the scheme is shown in Fig. 1. In Fig. 1 e) and Fig. 1 f), the red circles denote the abnormal frequencies which are from the pixel value correlated to the neighbors, indicating the image is resampled.

### *B. The CFA Demosaicing Artifacts [5]*

A digital color image consists of three channels containing samples from different bands of the color spectrum, e.g., red, green, and blue. Most digital cameras, however, are equipped with a single CCD or CMOS sensor, and capture color images using a color filter array (CFA). The most frequently used CFA, the Bayer array [10], employs three color filters: red, green, and blue. The red and blue pixels are sampled on rectilinear lattices, while the green pixels are sampled on a quincunx lattice. Since only a single color sample is recorded at each pixel location, the other two color samples must be estimated from the neighboring samples in order to obtain a three-channel color image [11], and the estimated color values are called the CFA demosaicing artifacts.

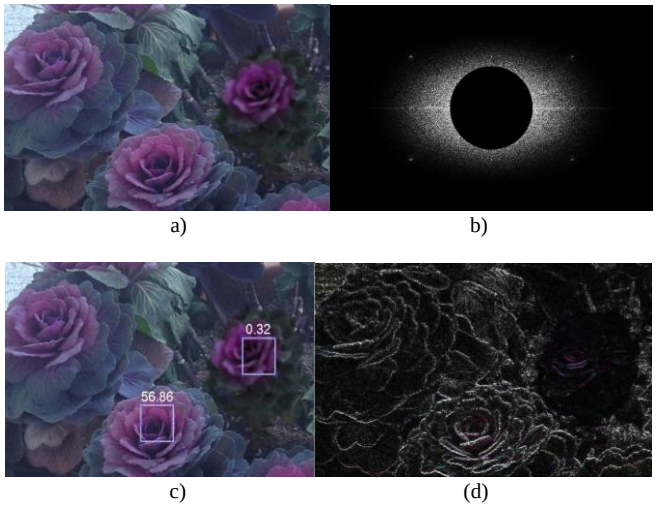
The basic rationale of the scheme is that an image forgery operation alters CFA demosaicing artifacts in a measurable way. The lack of CFA artifacts or the detection of weak CFA artifacts may indicate the presence of forgery [5].

To identify the CFA pattern of an image, the image is re-interpolated with several candidate CFA patterns. For each of these candidate patterns, the Mean Square Error (MSE) between the input and re-interpolated image is computed.

If an image is not forged, it is expected that one of the MSE values out of the 4 computed with each candidate pattern should be significantly smaller than the others. Specifically, the MSE computed for the actual CFA pattern used for the image should be much smaller than the other 3 patterns. If none of the 4 MSE values are significantly smaller than the others, the image may have undergone a post-processing operation which removes the traces of demosaicing. Hence, forgeries such as resizing, recompression, and filtering can be detected through the comparison of MSE values [5].


a) b)

Fig. 2. Experimental results for digital image forgery detection. The four penguins with their shadows are added, enlarged and blurred. a) A result from the CFA demosaicing artifacts. b) A result from the difference of the image frequency map.




a) b) c) (d)

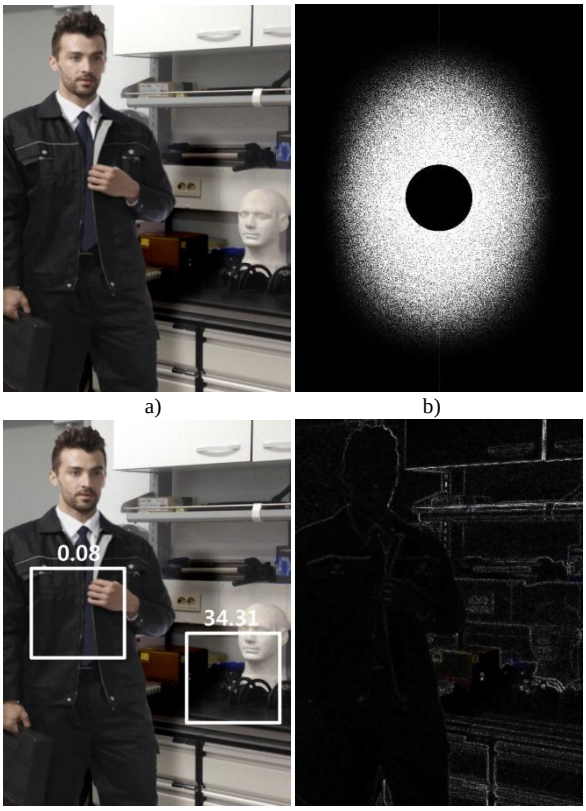
Fig. 3. Experimental results for digital image forgery detection. a) The forged image. The rightmost flower is added, enlarged and blurred. b) A result from the interpixel correlation. c) A result from the CFA demosaicing artifacts. d) A result from the difference of the image frequency map.

Fig. 2 shows an example, where the four penguins with their shadows are added and blurred. In Fig. 2 a), the MSE values from each squared region of the image are shown above or under each region. The MSE values of the forged part are small, while those of the genuine part are comparably large. Note that the MSE values of the forged part are 0.45 and 0.76, while those of the genuine part are 62.88 and 23.33. Thus, the forged part can be detected with the MSE values compared to other regions.

### *C. The Difference of the Image Frequency Map [6]*

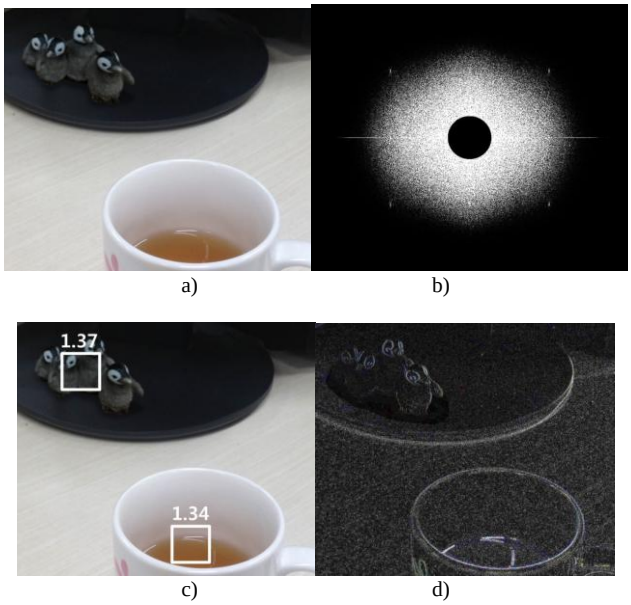
Researches show that most of the image forgery accompany with the blur operation. Blurring is to reduce the image details including noise or sharpness of an image, and it can be regarded as a filtering operation, especially an LPF (low pass filtering). So, if we blur an image by a certain amount and subtract it from the original image, the result of blurred part is small (looks dark) while that of the genuine part is comparably large (keeps the similar look as the original). The difference of the pixel values between the

suspect image and the filtered image is called a map [6]. In Fig. 5 b), the dark area in the map indicates the blurred part, which is the evidence of a forgery.




a) b) c) d)

Fig. 4. Experimental results for digital image forgery detection. a) The forged image. A gentleman with a dark jacket is added, enlarged and blurred. His shadow is also darkened and blurred. b) A result from the interpixel correlation. c) A result from the CFA demosaicing artifacts. d) A result from the difference of the image frequency map.



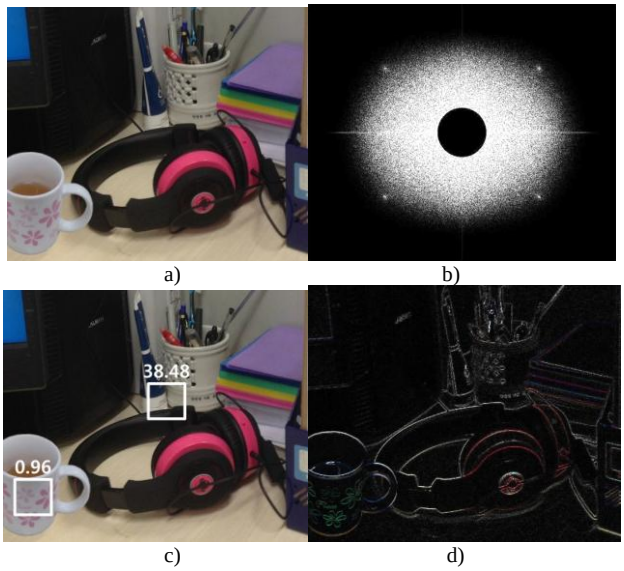

a) b) c) d)

Fig. 5. Experimental results for digital image forgery detection. a) The forged image. The four penguins with their shadows are added, enlarged and blurred. b) A result from the interpixel correlation. c) A result from the CFA demosaicing artifacts. d) A result from the difference of the image frequency map.

## III. Experimental Analysis and Results

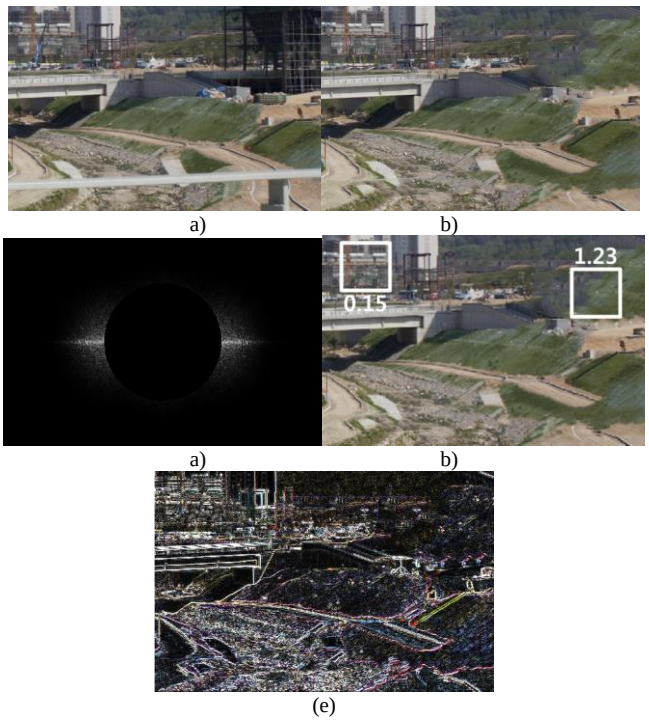
To test and verify the schemes described in Section II, we manually produce forged images. Nikon D100, Canon EOS 5D Mark II and Apple iPhone 5 are used to obtain the original images, and images from Sample Pictures of Microsoft Windows are also used as the original images. Adobe Photoshop CS 5.1is used to make the forged images. Splicing (including adding, moving and deleting), blurring, rotating and/or resizing the original images are applied to make the forged images.

The detection rate of the schemes may depend on the characteristics of the forged images and the forgery methods, so only the qualitative feature of each scheme is evaluated.




a) b) c) d)

Fig. 6. Experimental results for digital image forgery detection. a) The forged image. The white cup with pink flowers on the lower left corner is added, enlarged and blurred with its shadow. b) A result from the interpixel correlation. c) A result from the CFA demosaicing artifacts. d) A result from the difference of the image frequency map.




a) b) a) b) (e)

Fig. 7. Experimental results for digital image forgery detection. a) The original image. b) The forged image. The green hill in the middle is copied and moved to the upper right corner. A road in the lower right corner is cut down in the same way. c) A result from the interpixel correlation. d) A result from the CFA demosaicing artifacts. e) A result from the difference of the image frequency map.

The representative results of the experiments are shown in Fig. 3 through Fig. 7. As shown in Fig. 3, and in most of the cases, all three schemes in Section II succeed to detect whether the suspect image is forged.

However, these schemes have limitations for detecting forgeries that dodge the aim of the schemes. As shown in Fig. 4, the scheme of interpixel correlation fails to detect whether the suspect image is forged. The schemes of CFA demosaicing artifacts and the difference of the image frequency map also fail to detect the forged region of the suspect image and whether the suspect image is forged in Fig. 5 and Fig. 6, respectively.

In addition, the schemes need an intuitive decision for the most part, which the scheme described in Section II is noticeable. In Fig. 4, the forged part in Fig. 4 d) is darker than its nearby area, but it is not easy to tell the difference of the darkness between the gentleman and the shelves on the background. In Fig. 5, the shadows can be easily detected in Fig. 5 d), but it needs careful approach to tell that the penguins are not genuine. Moreover, all three schemes fail to detect the forgery in Fig. 7 case although the forged regions in Fig. 7 a) can be simply detected with naked eyes.

## IV. Conclusion

As the number of digital image forgeries increase fast and its complexity grows, a number of image forgery detection schemes appear to compensate human visual inspection which is said to be subjective and unreliable. The majority of the published detection schemes succeed to detect whether the suspect image is forged, and localize the forged region. However, the schemes are dependent of the parameters of the schemes and the forgery method of the image, thus they still need the human intuition. Moreover, some forged images are not detected which are off the detection points of the schemes.

Our future works include the implementations and verifications of several more detection schemes of digital image forgeries, and build a system that combines the digital image forgery detection schemes which have been proposed up to now. Blind tests of each schemes and a quantitative appraisal for them are also included.

## References


[1] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 758-767, Feb. 2005.

[2] Wikipedia. [Online]. Available: http://en.wikipedia.org/

[3] T. Qazi, "Survey on blind image forgery detection," in *Proc. International Conference on Machine Learning and Cybernetics*, July 2008, pp. 3463-3467.

[4] B. L. Shivakumar and S. S. Baboo, "Detecting copy-move forgery in digital images: A survey and analysis of current methods," *Global Journal of Computing Science and Technology*, vol. 10, no. 7, pp. 61-65, Sep. 2010.

[5] A. E. Dirik and N. Memon, "Image tamper detection based on demosaicing artifacts," in *Proc. 16th IEEE International Conference on Image Processing (ICIP)*, Nov. 2009, pp. 1497-1500.

[6] M. G. Hwang and D. H. Har, "A novel forged image detection method using the characteristics of interpolation," *Journal of Forensic Sciences*, vol. 58, no. 1, pp. 151-162, Jan. 2013.

[7] S. Murali, "Comparison and analysis of photo image forgery detection techniques," *International Journal on Computational Sciences and Applications*, vol. 2, no. 6, pp. 45-56, Dec. 2012.

[8] H. Farid, "Image forgery detection: a survey," *IEEE Signal Processing Magazine*, pp. 16-25, March 2009.

[9] A. Dempster, N. Laird and D. Rubin, "Maximum likelihood from incomplete data via the EM Algorithm," *Journal of the Royal Statistical Society*, vol. 99, no. 1, pp. 1–38, 1977

[10] B. E. Bayer, "Color imaging array," US Patent 3971065, 1976.

[11] A. C. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," *IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3948-3959, Oct. 2005.


**Hansoo Kim** received the B.E., M.E. and Ph.D. degrees in electronic engineering from Sogang University, Korea, in 2002, 2004 and 2014, respectively. He worked as a junior engineer at the Digital Media Research Laboratory in LG Electronics from 2004 to 2005, and as a senior engineer in Nextreaming Corp. until 2006. He is currently a researcher and forensic expert in National Forensic Service, Korea. His research interest and work experience include deep packet inspection, forensic image analysis, application-layer network protocols, home networking, IPv6, multimedia streaming, digital forensics, document analysis, the Internet security and cybercrime.

**Joong Lee** received the B.S., M.S., and Ph.D. degrees in chemical engineering from Kwangwoon University, Korea, in 1994, 1999, and 2004, respectively, and the B.S. degree in computer engineering from Korea Open University, Korea, in 2010. He was with the Electrical and Computer Engineering Department, Temple University, Philadelphia, PA, USA, as a visiting scholar. He is currently a chief of the Digital Technology and Biometry Division, National Forensic Service, Korea. His research interests include questioned documents, image processing, mobile forensics and digital forensics.