IMAGE TAMPER DETECTION USING MATHEMATICAL MORPHOLOGY

Mirei KIHARA, Masaaki FUJIYOSHI, Qing Tao WAN, and Hitoshi KIYA

Dept. of Information and Communication Systems Engineering, Tokyo Metropolitan University
6–6 Asahigaoka, Hino-shi, Tokyo 191– 0065, Japan

ABSTRACT

This paper proposes a tamper detecting method for images using mathematical morphology. The proposed method utilizes the idempotent property of morphological operations rather than fragile watermarking methods. While fragile watermarking methods that must extract the embedded watermark and compare it with the possible watermark to detect tampers, the proposed method detects and localizes tampers by only morphological operations and image subtraction in the spatial domain. Moreover, a visual signature system is proposed based on the proposed tamper detecting method. Experimental results show the effectiveness of the proposed method.

Index Terms— Image processing, Security, Multimedia communication, Authentication, Tampering detection

1. INTRODUCTION

By using high-performance computers and powerful software, the novice as well as the professional easily modify digital images. This advantage introduces malicious tamper of images into our lives. To detect tampering, digital signature [1,2] and robust hash [3] has been used widely, besides non-intrusive methods [4] that does not process images at the image creation.

A digital signature is generated from an image. It needs to be stored and/or transmitted separately from the image itself, but in many cases, separation is undesirable. To overcome this undesirability, methods which hide digital signature into the image itself have been proposed. These methods are refer to as fragile watermarking [5, 6]. These methods, however, require to compare the extracted watermark and possible watermarks to detect tampering, and this process increases computational consumption.

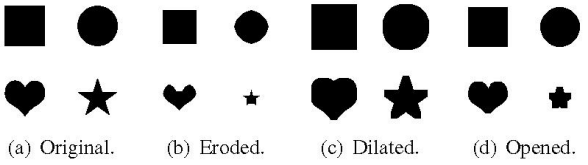
On the other hand, mathematical morphology [7, 8], one of nonlinear processing, has been widely studied in the non security related fields. It is generally used for noise removal or edge detection. This paper focuses mathematical morphology, but for security related problem; image tamper detection.

This paper proposes a novel tamper detecting method for images. The proposed method utilizes the idempotent property of operations in mathematical morphology. Whereas fragile watermarking methods embed, extract, and compare watermarks, the proposed method processes the image by one morphological operation in the spatial domain. Furthermore, the proposed method simultaneously localizes the tampered area. In addition, a visual signature system based on the proposed tamper detecting method is also proposed.

2. MATHEMATICAL MORPHOLOGY

2.1. Morphological Operations for Binary Images

There are two kinds of basic morphological operations called *erosion* and *dilation*.



(a) Original. (b) Eroded. (c) Dilated. (d) Opened.

Fig. 1. An example of dilation, erosion and opening of a binary image by using a 9×9 square-shaped structuring element.

Erosion is defined by the following equation using Minkowski subtraction:

$$A \ominus B^s = \cap\{A - b : -b \in B\}, \tag{1}$$

where A is binary image, B is structuring element (SE), b is unit element of B, and B^s is reflected set of B; i.e. $B^s = \cup_{b \in B}\{-b\}$. To erode A by B, A is firstly translated by $-b$, and then the all translated results are combined by intersection. In general, the erosion operation shrinks the image. The image shown in Fig. 1 (b) is obtained by eroding Fig. 1 (a) by 9×9 square-shaped SE.

To enlarge the image, the dilation is applied, which is defined by the following equation using Minkowski addition:

$$A \oplus B^s = \cup\{A - b : -b \in B\}. \tag{2}$$

To dilate A by B, A is firstly translated by $-b$, and then the all translated results are combined by union. Fig. 1 (c) shows the image obtained through dilating Fig. 1 (a) by a 9×9 square-shaped SE.

By cascading the above mentioned basic operations, further operations are able to be defined. One of them is *opening* that consists of dilation and cascading erosion. It is noted that both basic operations use the identical SE. Opening A by B generates A_B that is given as

$$A_B = (A \ominus B^s) \oplus B. \tag{3}$$

Opening Fig. 1 (a) by a 9×9 square-shaped SE gives Fig. 1 (d).

2.2. Morphological Operations for Grayscale Images

Erosion and dilation for grayscale images are defined by following:

$$(f \ominus g^s)(x) = \min_{x+u \in F u \in G}\{f(x+u)\}, \tag{4}$$

$$(f \oplus g^s)(x) = \max_{u \in G}\{f(x+u)\}, \tag{5}$$

where $f(x)$ is the grayscale image with its domain F and $g(u)$ is zero value held SE with domain G. In erosion, the origin of SE $g(u)$ is put on focused pixel $f(x)$ in domain F, then $f(x)$ is altered with the minimum pixel value in domain G. Dilation is operated in the same way as erosion, but maximum value in domain G is chosen.

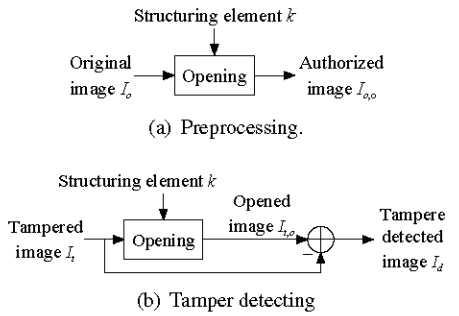


Fig. 2. Block diagram of the proposed tamper detecting method.

Opening of grayscale images is denoted f_g and defined by

$$f_g = (f \ominus g^s) \oplus g. \tag{6}$$

2.3. Idempotence Property of Opening

The morphological opening operations for both binary and grayscale images have algebraic property called *idempotence*:

$$(A_B)_B = A_B, \tag{7}$$
$$(f_g)_g = f_g. \tag{8}$$

Since opening is idempotent, once an image is opened by a SE, the identical image is obtained through opening the opened image by the identical SE.

In the next section, tamper detecting method using the idempotence property of mathematical morphology is proposed.

3. PROPOSED IMAGE TAMPER DETECTING METHOD

3.1. Algorithm

The proposed method consists of two parts as shown in Fig. 2; One is preprocessing and the other is tamper detecting. The algorithm is accomplished according to the following steps.

1. Open original image I_o by SE k to obtain authorized image $I_{o,o}$ as shown in Fig. 2 (a). Generated image $I_{o,o}$ is to be distributed or transmitted.
2. Open image I_t, that is tampered version of $I_{o,o}$, by SE k to obtain opened image $I_{t,o}$. Then, image I_d is acquired by calculate the absolute difference image with the following equation:

$$I_d = |I_t - I_{t,o}|. \tag{9}$$

On account of the idempotence property of opening, once the image had applied the opening operation, no-further change would occur by the repeated opening operations under the conditions that it had opened by the same SE. Existence of dofferemce between $I_{t,o}$ and I_t means that I_t have been tampered with.

Therefore, this method detects tamper by checking I_d's pixel values; I_t is tampered if one or more pixels of I_d have non-zero value. The tampered area can also be detected by this method.

3.2. Variables of the Proposed Method

The proposed method has three variables. Followings can be controlled by regulating each variable.

- Quality of authorized image $I_{o,o}$.
- Tamper detecting ability.

Three variables are described through the next three sections.

3.2.1. Shape and/or Size of the Used Structuring Element

Authorized image $I_{o,o}$ is altered from original image I_o by an opening operation. The alteration depends on the used SE. The shape and/or the size of the used SE are able to be selected by the user, according to the purpose or type of target images.

3.2.2. Area to Apply Opening Operation in an Image

To detect tampers on expressly important part in an image, opening operation need to be done only for the specific area. Size of the area and/or the number of areas to be opened can be chosen flexibly in the proposed method.

3.2.3. Bitplanes to be Opened

An N-bits quantized grayscale image can be regarded as the combined N pieces of binary images. That is, the n-th bitplane ($1 \le n \le N$) of N bits grayscale image I_o can be regarded as an one-bit binary image, and the opening for binary images is able to be used.

Besides, the n_1-th to the n_2-th bitplanes ($1 \le n_1 \le n_2 \le N$) of N-bits grayscale image I_o can be regarded as $n_2 - n_1 + 1$-bits grayscale sub-image, and opening operation for grayscale image is able to be applied.

3.3. Features of the Proposed Method

The proposed method utilizes the idempotent property of the mathematical morphology operation to detect tamper on images. Since opening used in the proposed method is operated in the spatial domain, no transformation such as discrete Fourier transformation, discrete cosine transformation, or discrete wavelet transformation is required. This reduces the computational consumption.

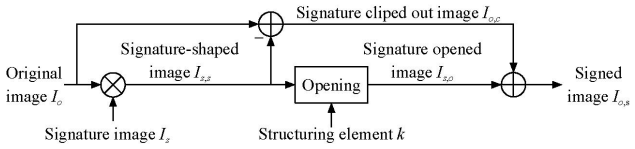
Furthermore, in this method, detection of tamper existence only requires checking whether the absolute difference image has non-zero pixels or not. Moreover, localization of the tampered area is simultaneously done. Whereas, fragile watermarking method requires watermark extraction and comparing the extracted watermark and the embedded watermark to detect tamper existence. It can be bit-by-bit comparison or calculating the correlation between watermarks. In fragile watermarking methods, further operations are needed for tampered area localization.

The proposed method is capable to control the image quality of a preprocessed image and tamper detecting ability by regulating variables. These variables also serve as secret keys. In particular, an SE plays an important role in a secrecy aspect. The shape and the size of an SE are flexible and many kinds of SE patterns can be generated. Attackers, therefore, hardly slip through a detecting system by finding out the used SE.

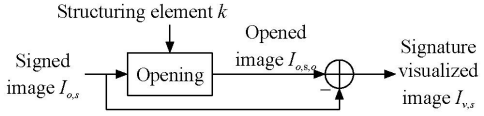
The effectiveness of the proposed method is shown in Sect. 5.

4. FURTHER APPLICATION

In this section, a visual signature system is proposed. The proposed system is based on the image tamper detecting method proposed in the previous section. That is, applying the proposed image tamper detection to visual signature is proposed in this section.



(a) Signature signing



(b) Signature visualizing

Fig. 3. Block diagram of the proposed visual signature system.

(a) Signature image I_s. (b) Signed image $I_{o,s}$ (PSNR: 47.54 dB). (c) Visualized signature $I_{v,s}$.

Fig. 4. An example of visual signature.

4.1. Visual Signature

Visual signature is able to be signed by applying the morphological opening operation to signature area. This signature system utilizes the variable of the proposed tamper detecting method, area to apply opening that is described in Sect. 3.2.2. The block diagram of the proposed visual signature system is shown in Fig. 3.

The signing algorithm is accomplished according to the following steps.

1. Calculate product set of original image I_O and signature image I_S, e.g., Fig. 4 (a), to obtain signature-shaped image $I_{S,S}$. Calculate the difference image of I_O and $I_{S,S}$ to obtain signature clipped out image $I_{O,C}$.
2. Open $I_{S,S}$ by SE k to obtain signature opened image $I_{S,O}$.
3. Calculate union set of $I_{O,C}$ and $I_{S,O}$ to obtain signed image $I_{O,S}$ (Fig. 4 (b)).

Signature image I_S is a binary image having the same size as I_O. Pixel values in signature area are 1's and in other area are 0's in I_S. In Step 1, I_O is separated into signature area $I_{S,S}$ and rest area $I_{O,C}$ by multiplexing I_S and I_O. In Step 2, opening by SE k is only applied to signature area. In Step 3, opened signature area and the other area are combined to generate signed images $I_{O,S}$.

The authentication algorithm is accomplished according to the following steps.

1. Open $I_{O,S}$ by k to obtain opened image $I_{O,S,O}$.
2. Calculate the absolute difference image of $I_{O,S}$ and $I_{O,S,O}$ to obtain visualized signature image $I_{V,S}$ (Fig. 4 (c)).

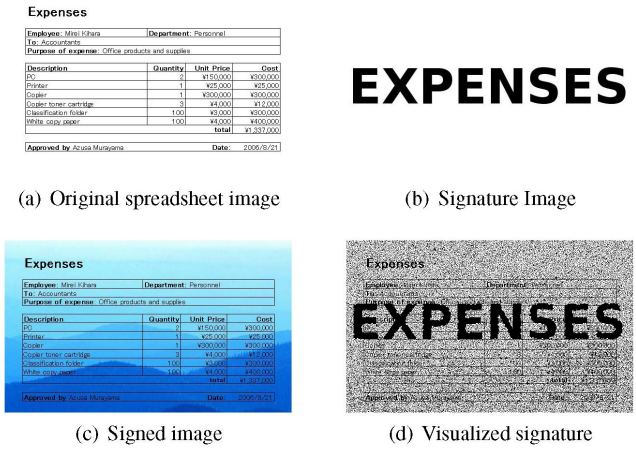
In Step 1, whole area of $I_{O,S}$ is opened by SE k. Signature area of $I_{O,S}$ has already been opened in Step 2 of the signing algorithm, so pixel values in signature area are not changed by this operation because of idempotence. Whereas the rest area of $I_{O,S}$ has not been opened yet, the pixel values are changed. The signature areas in $I_{O,S}$ and $I_{O,S,O}$ have the exactly same pixel values, the signature area in $I_{V,S}$ consists of zero pixels. Besides, the rest area of $I_{O,S}$ differs from $I_{O,S,O}$ from the perspective of pixel values, this area has non-zero pixels. Therefore, the visual signature appears in $I_{V,S}$ in Step 2.

4.2. Visual Signature for Texts Contained Binary Images

In a texts contained binary image, such as a spreadsheet image, pixels on neighboring area hold the same value. This feature introduces two things to be overcome to the visual signature system proposed in the previous section.

One is degrading the quality of signed images. The other is that pixel values in background area lasting the same pixel values are not changed by opening operation. That is, signature signing is hard.

To overcome these problems, insertion of background image is proposed. To insert a background image, extend the binary image to an N-bit image which keeps the original binary image as its most significant bitplane (MSB). An $N-1$-bits background image is inserted to bitplanes of the least significant bit (LSB) to the $N-1$-th bit. Then, morphological opening can be applied to any area and/or bitplanes except for the MSB. Further improvements for randomness of neighbor pixels in a bitplane can be achieved. An example of visual signature on a spreadsheet image is shown in Fig. 5.



(a) Original spreadsheet image (b) Signature Image

(c) Signed image (d) Visualized signature

Fig. 5. An example of visual signature on a spreadsheet image

5. EXPERIMENTAL RESULTS

In this section, two experimental results are shown; one is the image quality of preprocessed images and the other is the tamper detecting ability of the proposed method. Experimental conditions are summarized in Table 1. Lena shown in Fig. 6 (a) is used as original image I_O. Employed SEs, k's, are 1×2 rectangular-shaped, and 3×3 and 9×9 square-shaped as shown in Fig. 7. Tamper is applied to eyes, eyelashes, and eyebrows, of preprocessed Lena $I_{O,O}$ as shown in Fig. 6 (b) and (c).

Fig. 8 shows the preprocessed images $I_{O,O}$ in its left column and detected tampers I_d in its right column. I_d's are processed for easy looking. From Figs. 8 (a), (b), and (c), the qualities of $I_{O,O}$ are affected by the size of the used SEs. The images opened by larger SE

Table 1. Experiment conditions.

Image I_o	Lena (512×512 pixels, 8 bits grayscale)
Structuring element k	1×2 rectangular-shaped, 3×3 and 9×9 square-shaped
Bitplanes	whole 8 bits as grayscale, LSB only as binary
Area	the whole image

(a) Lena. (b) Tamper. (c) Tampered image I_t.

Fig. 6. Conditions of images for experiments.

have lower PSNRs. On the other hand, larger SE is used, clearer tamper existence appears. It is found that the proposed method is capable of controlling the trade-off between the image quality of $I_{o,o}$ and the tamper detecting ability by choosing SEs.

Figure 8 (d) shows that the opening operation for bitplanes is effective to reduce the degradation of the image quality after opening. It is also found that the proposed method controls above mentioned trade-off by choosing the area and/or bitplanes to be opened.

6. CONCLUSIONS

Tamper detecting method using mathematical morphology has been proposed in this paper. The proposed method utilizes the idempotent property of morphology. In addition, visual signature system has been proposed based on the tamper detecting method. Investigation on resilience to lossy compression such as JPEG is a further work.

ACKNOWLEDGMENT

This work has been partly supported by the Grant-in-Aid for Young Scientists (B), No.17700119, from the Ministry of Education, Culture, Sports, Science and Technology of Japan.

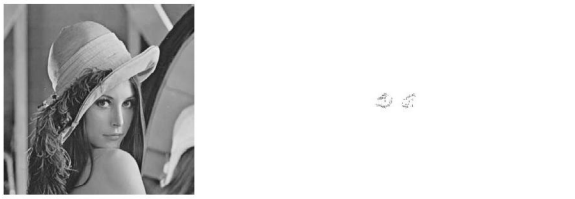
REFERENCES

[1] B. Schneier, *Applied cryptography — protocols, algorithms, and source code in C*, 2nd ed. New York, NY, US: John Wiley & Sons, Inc., June 1996.

[2] Z. Yao and N. Rajpoot, "Radon/ridgelet signature for image authentication," in *Proc. IEEE ICIP*, 2004, pp.43–46.

(a) 1×2 (b) 3×3 (c) 9×9

Fig. 7. Structuring elements, k's, used for experiments.



(a) Whole area, whole 8 bits, and 1×2 rectangular-shaped (PSNR: 39.63 dB).

(b) Whole area, whole 8 bits, and 3×3 square-shaped (PSNR: 31.24 dB).

(c) Whole area, whole 8 bits, and 9×9 square-shaped (PSNR: 23.24 dB).

(d) Whole are, LSB only, and 3×3 square-shaped (PSNR: 51.28 dB)

Fig. 8. Images after opening $I_{o,o}$, the left column, and detected tampers I_d, the right column (I_d's are processed for easy looking).

[3] V. Monga and M.K. Mihçak, "Robust image hashing via non-negative matrix factorizations," in *Proc. IEEE ICASSP*, 2006, pp.II-225–II-228.

[4] A. Swaminathan, M. Wu, and K.J.R. Liu, "Image tampering identification using blind deconvolution," in *Proc. IEEE ICIP*, 2006, pp.2309–2312.

[5] H. Yang, A.C. Kot, and J. Liu, "Semi-fragile watermarking for text document images authentication," in *Proc. IEEE ISCAS*, 2005, pp.4002–4005.

[6] S. Han, H.L. Jin, M. Fujiyoshi, and H. Kiya, "A lossless data hiding in the spatial domain for image tamper detection," in *Proc. IEEE ISPACS*, 2006, pp.760–763.

[7] J. Serra, *Image analysis and mathematical morphology* Academic Press Inc., 1982.

[8] G.R. Arce, *Nonlinear signal processing — a statistical approach* New York, NY, US: John Wiley & Sons, Inc., 2005.