SELECTED PAPER

Morphological Pattern Spectrum-Based Objects Detection for Protecting Privacy

Yuma Murakami, Toshiya Honda, Yuki Yanagihara, Takeshi Kumaki, Takeshi Ogura and Takeshi Fujino

Department of VLSI System Design, Ritsumeikan University, 1-1-1 Noji-Higashi, Kusatsu, Shiga 525-8577, Japan
Phone/FAX: +81-077-599-4167

E-mail: {(ri008085, ri0007hh}@ed, kumaki@fc, togura@se, fujino@se}.ritsumei.ac.jp

Abstract

The growing number of surveillance cameras installed for crime prevention in various city locations capture images that might reveal private information, such as images of human faces, of car license numbers, and of windows, without permission. We previously reported a Hierarchical Masked image Filtering (HMF) technique that can mask and restore such objects in a captured image [1]. The object detection used for masking the privacy-related images uses the Haar-like [2] feature algorithm in the OpenCV library. We have now improved the HMF masking performance by developing a fast object detection method that is used instead of the Haar-like algorithm.

In this paper, we describe HMF based on the morphological pattern spectrum. This pattern spectrum can be used to mask not only a front face image but also a profile image. The use of this HMF reduced the processing time by about 62% compared with that of the Haar-like algorithm.

1. Introduction

While the use of many surveillance cameras has helped to prevent a number of crimes [3], these cameras record images that could reveal private information, such as images of human faces, car license numbers, and windows, without permission. Present surveillance systems [4] make use of masking for protecting privacy against windows and a veranda in a house. However, they sometimes protect privacy at the expense of security. Furthermore, the images provided by the camera are less useful for surveillance. To protect privacy without sacrificing security, mask processing needs to be removable. We have developed a Hierarchical Masked image Filtering (HMF) technique that can mask and restore those portions of captured images that might reveal private information [1]. Methods for detecting objects while allowing private information to be protected has until now made use of the Haar-like algorithm in the OpenCV library. However, to improve HMF masking by detecting objects more quickly, we propose the use of a method based the morphological pattern spectrum.

2. Hierarchical Masked Image Filtering

HMF protects privacy by using an XOR operation between a random number and a pixel value to generate masks for the areas deemed to contain sensitive images. As shown in Fig. 1, pseudo-random numbers are generated from a seed value, i.e., a “key.” An image masked using HMF can be unmasked only by someone with the key, which removes the mask by using an XOR operation. Multiple keys can be used if there is more than one area to be masked. Also, the security of the mask processing can be strengthened by increasing the bit width of the random number. This technique can be applied to a large number of pseudo-random number algorithms. However, safety needs to be considered. We are thus considering the use of a pseudo-random number generation algorithm such as Mersenne Twister [5] or Crypt MT [6].

Figure 1: Hierarchical masked image filtering

This HMF can be used in both surveillance and digital content delivery systems. For example, in surveillance, only the police would have the key needed to unmask a face in an image. Since only the police would have the key, unauthorized people would be unable to unmask a face. In digital content delivery, only people who have paid a fee would get the key and be able to remove the mask.

Dealing with surveillance cameras in a way that balances privacy and security issues has become difficult [7]. Video of people that have been taken without permission should not be viewed even on a monitor. By using HMF processing in a video camera, we can achieve this. We plan to implement small embedded devices such as BeagleBoards [8]. Furthermore, this HMF can be used to hierarchically mask more than one object as shown in Fig. 2. A human face and two monitors are shown in Fig. 2-(a).

The result of masking the face is shown in Fig. 2-(b), and the result of masking the active monitor is shown in Fig. 2-(c). The result of covering the face and the active monitor is shown in Fig. 2-(d). When a mask is applied to several objects, as shown in Fig. 2-(d), the unmask operation restores the image in (a), (b), or (c) in accordance with the authority of the viewer.

Figure 2: Hierarchical masked image filtering

3. Morphological Pattern Spectrum-Based Object Detection

The pattern spectrum [9] is a mathematical morphology based algorithm used to extract the size distribution of target objects contained in an image. Morphological processes, such as opening and dilation, are used for generating the pattern spectrum. In addition to morphological processing, pixel-by-pixel subtraction, area calculation, and the null set assessment process are also needed. Unlike other feature extraction methods, the pattern spectrum process is not affected by rotation or the positioning gap of an image, so it can provide a high level of accuracy.

The pattern spectrum equation is defined by equation (1), where X_{rB} represents the opening operation for image X , with scale r of structuring element B . The “-” denotes pixel-by-pixel subtraction. The same operations are repeated until the condition of null assessment, as shown in equation (2), is met.

$$PS(X, B, r) = \sum_{y \in \text{whole image}} \{X_{rB}(y) - X_{(r+1)B}(y)\} \quad (1)$$

$$\sum_{y \in \text{whole image}} \{X_{rB}(y) - X_{(r+1)B}(y)\} = \Phi \quad (2)$$

On the basis of this process, the morphological pattern spectrum can be used to extract specific features of

objects in the original image (Fig. 3). If a face was hidden, the goal could be to extract an eye, so HMF is applied around the eye.

Figure 3: Morphological pattern spectrum process

Therefore, the structural element used in the processing is an oval close to the shape of an eye.

Here, we want to apply the morphological pattern spectrum to HMF. In accordance with the morphological pattern spectrum, a binary image is generated from the original image. An inter-pixel image is then generated by subtracting the opening image from the binary image. This is shown in Fig. 4. The original image is shown in Fig. 4-(a), a binary one in Fig. 4-(b), and an inter-pixel one in Fig. 4-(c).

Figure 4: Breakdown process of morphological pattern spectrum

The inter-pixel image that remains in the black areas is often the left eye and eyebrows. The black portions in a row are scanned to detect the area to be masked. As shown in Fig. 5-(a), this process starts from coordinates X and Y . The scanning is done from the left to the right along axis X . The Y axis is then scanned from the top to the bottom.

During the scan, while counting the number of black pixels, we look for a solid black portion. The search range can be arbitrarily changed. If we locate a solid black portion, we can assign a pseudo-random number to the surrounding area, as illustrated in Fig. 5-(b). Pseudo-random numbers are entered in the red square. It is also

possible to arbitrarily change the size of the square. Finally, HMF is completed by using an XOR operation between the original and the inter-pixel image, which is assigned a pseudo-random number in the vicinity of the face. Figure 5-(c) shows the results of face masking.

Figure 5: Process of using morphological pattern spectrum to mask face

4. Implementation and Evaluation

This section shows the results of morphological pattern spectrum-based HMF processing using the portable gray map (PGM) format.

First, we focus on treating the human face for protecting privacy. The results of the implementation are shown as follows. The results of the morphological pattern spectrum-based HMF images for face detection are compared with the Haar-like features-based HMF.

The results of masking operation are shown in Fig. 6. Here, Fig. 6-(a) is a picture of the face from the front. Here, Fig. 6-(d) is a profile. For the frontal image, the Haar-like algorithm (Fig. 6-(b)) and the morphological pattern spectrum (Fig. 6-(c)) can mask the face. For the picture of the profile, while the Haar-like algorithm (Fig. 6-(e)) cannot mask the face, the morphological pattern spectrum (Fig. 6-(f)) can do so. The morphological pattern spectrum only has to be used to detect the eye, and the profile is masked by using the XOR operation. To see the accuracy of the masking operation using this pattern spectrum, we went ahead with validation in several images. We focused on the profile of women, and the results are shown in Fig. 7; Fig. 7-(a) is the original image, and Fig. 7-(b) shows the result of the proposed method. Masking was applied around the eyes, and the subject's identity concealed. In Fig. 7-(c) the Haar-like algorithm is used, but the mask is not applied. We then applied mask processing to more than one person, and the results are shown in Fig. 8; Fig. 8-(a) is the original image, Fig. 8-(b) shows the result of the proposed method. Masking was applied around both faces and again the identity of the subjects is concealed. The result of applying the Haar-like algorithm is shown in Fig. 8-(c), and the mask was applied to only one face.

Figure 6: Results of use of face detection technology: (a) and (d) original image, (b) and (e) two results using Haar-like algorithm, (c) and (f) two results using the morphological pattern spectrum

Figure 7: Results of face detection

The proposed method covers solid black areas in the inter-pixel image. In case of the Fig. 4-(c), eyes, a nose and a mouth shapes relatively-large four solid portions. Thus, the whole face is masked by the proposed method in Fig. 6-(c). On the other hand, since a nose and a mouth of the woman in Fig. 7-(b) are unsatisfying the solid-scale condition, the HMF covers only eyes of woman face.

Figure 8: Results of face detection

In the next evaluation, windows were the target for protecting privacy. The result of masking on windows is shown in Fig. 9. Here, Fig. 9-(a) is the original image and the results of the proposed method are shown in Fig. 9-(b).

The implementation results show that windows cannot be viewed.

Figure 9: Result of HMF masking to images of windows

If some objects in the original image have the same shape as structuring element, non-target areas are masked as shown in Figs. 7-(b), and 8-(b). Even with masking, there is no problem in terms of using the image for surveillance because unmasking is easy.

The processing time is now considered. We compare the average processing time of the morphological pattern spectrum and that using Haar-like features, that are used Fig. 6-(c), (f), Fig. 7-(b) and Fig. 6-(b), (e), Fig. 7-(c), respectively. The processing time includes input images, face detection, random number generation, and output image. The implementation environment is as follows.

Table 1: Spec of note PC

OS	Ubuntu11.10
CPU	Core2Duo T7250 2.00GHz
Memory	2GB

The processing time for the HMF based on morphological pattern spectrum and that based on Haar-like features is shown in Fig. 10. The morphological pattern spectrum-based HMF has reduced the processing time approximately 62% compared with that with the Haar-like features.

Figure 10: Speed of processing of morphological pattern spectrum and Haar-like features

5. Conclusion

We proposed the use of the hierarchical masked image filtering method. By using the XOR operation between the random number and the pixel value in the area containing

images, this technology can be used to hide images that might reveal private information. The unmasked image is easily obtained by an XOR operation. The hierarchical masked image filtering method based on the morphological pattern spectrum is proposed. This spectrum can be used to mask not only the image of the front of a face but also the image of a profile. We can do mask processing for a large number of human faces. In terms of the processing time, the morphological pattern spectrum-based HMF has reduced the processing time by approximately 62% compared with that based on Haar-like features.

Acknowledgments

Part of this work has been supported by a Grant-in-Aid for Young Scientists (B) (No. 24710190), Ministry of Education, Culture, Sports, Science and Technology, Japanese government and an Exploratory Research (AS242Z03360H), Adaptable and Seamless Technology transfer Program through targetdrive R & D (A-STEP), Japan Science and Technology Agency (JST).

References

- [1] Y. Murakami, et al.: Implementation and evaluation of image filtering method with authorization for privacy protection, Forum on Information Technology, pp. 495-496, 2011.
- [2] P. Viola, et al.: Robust real-time face detection, Proc. IEEE Int. Conf. on ICCV'01, pp. 511-518, 2001.
- [3] <http://www.shikoku-np.co.jp/feature/tuiseki/217/>
- [4] <http://www.sherlock-holms.com/dp/sh4759.html>
- [5] M. Matsumoto, et al.: Mersenne Twister : A 623 dimensionally equidistributed uniform pseudo-random number generator, ACM Trans. Modeling and Computer Simulation, Vol. 8, No. 1, pp.3-30, 1998.
- [6] M. Matsumoto, et al.: CryptMT3 Stream cipher, new stream cipher designs, Lecture Notes in Computer Science (LNCS), Vol.4986, pp. 7-19, 2008.
- [7] http://www.nichibenren.or.jp/library/ja/opinion/report/data/2012/opinion_120119_3.pdf
- [8] <http://beagleboard.org/>
- [9] Z. B. Rafi'i, et al.: Implementation results and application of real-time morphological pattern spectrum analyzer on cellular-automata hardware, Proc. RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP), pp. 409-412, 2012.