Evaluating Protection Capability for Visual Privacy Information

Yuta Nakashima, *Member, IEEE,* Tomoaki Ikeno, and Noboru Babaguchi, *Senior Member, IEEE*

Abstract

Images are now widely used for various applications like surveillance, entertainment, and communication. They are often accompanied by sensitive information such as people's faces, which can be privacy intrusive. The essential remedy is to remove such information using an image-processing technique (e.g., blurring, blocking out). The effectiveness of removal, however, highly depends on the relationship between viewers and subjects or on the conspicuousness of subjects; viewers might successfully guess subjects' identities from privacy-protected images if the viewers are familiar with the subjects or if the subjects are conspicuous. Through an extensive questionnaire survey, we evaluated the capability of image processing techniques for visual privacy protection, considering these factors.

Index Terms

Privacy protection, image processing, evaluation.

I. Introduction

Images captured with cameras are currently viewed as one of the most important media for wide range of applications, including surveillance, entertainment, and communication. Such images usually contain people's faces that can disclose their identities and thus are highly privacy sensitive. To remedy this privacy concern, television programs, for example, apply image processing (e.g., blurring, blocking out) to filter out sensitive information and avoid violating others' privacy. Recent computer vision technologies enable automatic privacy protection for some applications like video surveillance.

As cameras become more ubiquitous and images become more available through various ways, the chance of such sensitive information being exposed to many people including ones close to the subjects increases. For example, a vast amount of images are now shared through the Internet, which makes these images available to the subjects' friends and family. Some attentive users, therefore, may apply privacy protection to the images manually or with an automatic system available in YouTube [1], for example. Google Street View and video surveillance in a local community (e.g., in a building) are in a similar situation, and privacy protection has been studied for them (e.g., [2]).

The closeness between subjects and viewers can be a critical factor in privacy protection. Considerable prior knowledge on subjects' appearances may make inference of their identities far easier for viewers who are close to them, even if the image is partly filtered. For example, blurring filters out high-frequency components of the image, but sufficient cues for identification might still remain [3]. In addition, for automatic privacy protection, such as [4], [5], computer vision technologies might fail to precisely locate faces and/or bodies, and blocking out might not fully cover sensitive regions. Those who are close to the subjects can successfully guess their identity from such small uncovered regions. Yip and Sinha demonstrated that humans can recognize celebrities' faces in very low-resolution images [6]. Burton et al. showed that faces are more important cues for identification in surveillance videos than gaits or bodies, and concluded that familiar faces, but not unfamiliar ones, can be easily identified [7]. These results imply a negative correlation between familiarity and the capability of visual privacy protection. A good summary of these results can be found in [8].

This raises a crucial question: How well does visual privacy protection work when a subject and viewer share a certain degree of familiarity? We tried to answer this question based on a survey of over 100 participants. This

This work was partly supported by the Japan Society for the Promotion of Science (JSPS) Grant-in-Aid for Scientific Research.

Y. Nakashima is with the Graduate School of Information Science, Nara Institute of Science Technology, Japan.
E-mail: n-yuta@is.naist.jp

N. Babaguchi is with the Graduate School of Engineering, Osaka University, Japan.

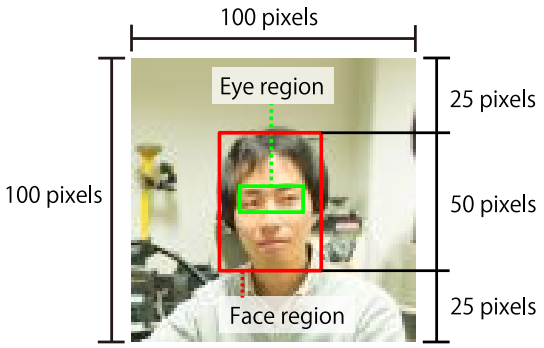

Fig. 1. Specification of face image.

article focuses on visual privacy protection for facial regions using image-processing techniques often used in automatic privacy protection systems. That is, considering several parameters for each image-processing technique or for possible failures in computer vision technologies, we evaluated the capability of image-processing techniques for privacy protection, and sought to clarify the relationship between capability and familiarity. This article is an extended version of our previous work [9], and we added results of statistical tests for clearer interpretation of the survey and some discussion on the factors that affects the privacy protection capability.

II. Image Processing Techniques to be Evaluated

In our survey, we targeted several image-processing techniques that are widely used for visual privacy protection.

- **Resizing.** Many computer vision-based privacy protection systems locate facial regions using background subtraction or face detection [4]. As these technologies are not always perfect, localization might fail, thereby fully disclosing facial regions. In this case, the degree of privacy violation depends on the subject's size, direction, and so forth. Among these factors, resizing corresponds to manipulating the subject's size. Here, we employed bilinear interpolation, and parameter $s \in \{5, 10, 15, 20, 25, 30, 40, 50, 70, 100\}$ specified the width of the resized image.
- **Blocking out facial regions.** Blocking out facial regions covers facial regions with a single color. In an automatic privacy protection scenario, computer vision technologies might fail in locating facial regions precisely, resulting in only a partial block out. We sought to demonstrate the accuracy required from the computer vision technologies to adequately locate and block out faces. Letting w_{F} and h_{F} denote the width and height of the facial region, defined as in Fig. 1, the parameters in this evaluation were vertical shift $n\alpha w_{\mathrm{F}}$ and horizontal shift $n\alpha h_{\mathrm{F}}$, where $n \in \{-3, -2, -1, 0, 1, 2, 3\}$ and $\alpha = 0.125$. Diagonal shifts (top-left to bottom-right and top-right to bottom-left) are the combinations of horizontal and vertical shifts. Figure 2 shows an example facial images after being blocked out.
- **Blocking out eye regions.** Eyes and their surrounding regions are considered one of the most important cues for identification among facial features [10]. Thus, we evaluated the eye-blocking strategy in the same way as the face-blocking strategy. The parameters were vertical shift $n\beta w_{\mathrm{E}}$ and horizontal shift $n\gamma h_{\mathrm{E}}$, where $\beta = 0.15$ and $\gamma = 0.25$, of which examples are shown in Fig. 3. We used the same n as for facial regions.
- **Blurring.** Blurring is one of the most common image-processing techniques used for visual privacy protection (e.g. [11]). Blurring removes high-frequency components of images by applying a smoothing filter. This evaluation employed the Gaussian filter with parameter $\sigma \in \{1, 1.6, 2.2, 2.8, 3.4, 4\}$, which is the standard deviation of the Gaussian function and controls the extent of high frequency component removal. Example images are shown in Fig. 4.

III. Questionnaire

The degree of privacy violation, or the capability of privacy protection, depends on various factors. Among them, our main focus was (i) familiarity between viewers and subjects and (ii) conspicuousness of subjects, both of which were highly subjective factors and determined here using a questionnaire.

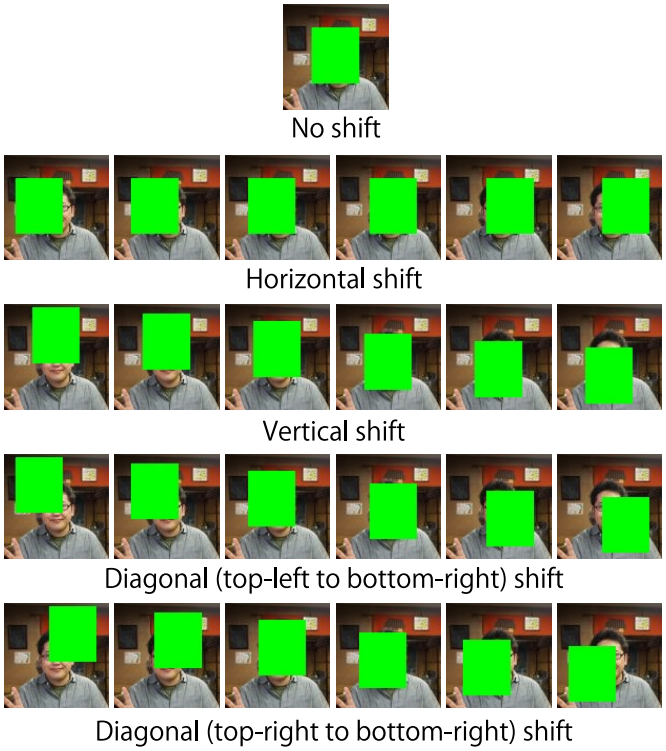

Fig. 2. Example face images for blocking out facial regions. The value of n increases from left to right.

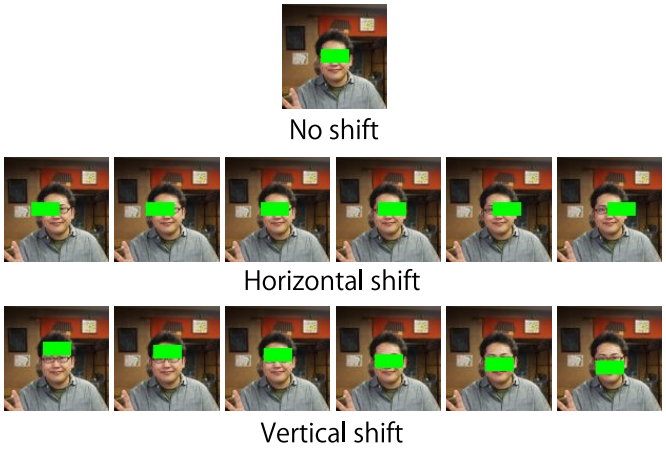

Fig. 3. Example face images for blocking out eye regions. The value of n increases from left to right.

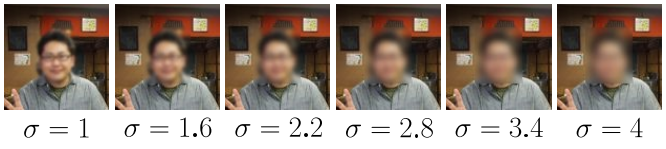

Fig. 4. Example face images for blurring.

TABLE I
DISTRIBUTION OF PARTICIPANTS BY AGE AND GENDER.

	20's	30's	40's	50's
male	12	14	14	13
female	14	13	14	14

- **Familiarity.** As demonstrated in previous research (e.g., [6]), familiarity has considerable effects on our identification abilities. For example, the rate of correct identification of a blurred face is expected to be high when viewers are familiar with the subject. In this evaluation, we assessed familiarity on a 5-point Likert scale. Our questionnaire asked each subject if she/he knew the person, possibly through a television program, and provided textual descriptions as follows: "I have never seen this person before" for 1, "I have seen this person" for 3, and "I'm very familiar with this person" for 5. The original descriptions were in Japanese.
- **Conspicuousness.** Another important factor that can affect the degree of privacy violation is the extent to which the subject is conspicuous. For example, a subject with pink-colored hair is very conspicuous, and might be easily identified even by viewers who are not very familiar with the subject. This factor, which we referred to as conspicuousness, was also assessed on a 5-point Likert scale. Each subject was asked the question, "do you think the person is conspicuous (impressive hair style, facial features, etc., or easily memorable)," with textual descriptions as follows: "Completely inconspicuous" for 1, "Neutral" for 3, and "Very conspicuous" for 5.

One of the difficulties in this evaluation is how to measure privacy violation, or how to measure the capability of privacy protection, because the sense of privacy is highly subjective, varying from person to person and culture to culture. Thus, we required an objective criterion. For face recognition research in psychology, researchers often use the rate of successful subject identification. Accordingly, we defined a similar criterion that we called identifiability.

Identifiability, with respect to each score for familiarity and conspicuousness, was evaluated as follows. First, we collected facial images of subjects of various ages and genders to build a facial image dataset. In this survey, subjects of varying familiarity and conspicuousness levels were required. Some research work used images of celebrities (e.g., [6]), but we consider that this is not appropriate for our survey because of (i) the right of publicity and (ii) difficulty in preliminarily selecting a set of celebrities that makes distributions of familiarity and conspicuousness levels close to uniform distributions. We therefore used images of Japanese politicians on official business, whose right of publicity is considered restricted. In addition, some famous politicians (e.g., Junichiro Koizumi, who is a former prime minister of Japan) are known to most Japanese, and we can easily find a set of politicians suitable for our survey. The images were collected from the Internet and appropriately cropped to fit to our facial image specifications. The number of subjects was 20 (10 males and 10 females), with 20 images for each subject.

The questionnaire sessions were facilitated by a research company, which has a list of potential survey participants who preliminarily and voluntarily registered through the company's website with their occupation, gender, age, etc. In the pre-screening process, the company randomly picked people in the list so that their age and gender distributed uniformly, asking if they can participate in our survey, and recruited some of them. Our participants were in their 20s through 50s, with 53 males and 55 females, 108 in total, and were expected to be familiar with PC because they used one for registration to the list. Table I summarizes the distribution of the participants. We asked the participants to assign familiarity and conspicuousness scores to each of our 20 subjects, providing a facial image from our dataset and the Likert scales.

Each participant was then exposed to a sequence of stimuli. Each stimulus was a facial image that was randomly selected from our dataset, excluding the image used for evaluating familiarity and conspicuousness. An image-processing technique was then applied to the selected facial image with one of the parameter values. For each stimulus, we presented nine facial images, called candidates, one of which contained the subject in the stimulus (but not the same facial image as the stimulus), and the other contained eight randomly selected subjects. Each participant was asked to select the subject in the stimulus from the candidates or answer "I dont know." Figure 5 shows our PC-based interface, with the stimulus in the right pane and candidates with the "I don't know" button in the left pane. For this survey, each participant provided 270 responses (plus 10 responses for another survey), which took about one hour in total.

Fig. 5. PC-based interface used in our survey. Note that the facial images shown in this example are not from our dataset.

After the questionnaire sessions, we aggregated all responses. Let f and c in $\{1, 2, 3, 4, 5\}$ denote the familiarity and the conspicuousness scores, respectively. For a certain image-processing technique, g, with one of its parameters θ, suppose we have $M_f^g(\theta)$ responses for all subjects with familiarity score f, and $L_f^g(\theta)$ responses correctly identified the subject in the stimulus among them. We define the identifiability $I_f^g(\theta)$ for f and g with θ as

$$I_f^g(\theta) = L_f^g(\theta)/M_f^g(\theta). \tag{1}$$

Similarly, the identifiability for the conspicuousness score c is defined as

$$I_c^g(\theta) = L_c^g(\theta)/M_c^g(\theta). \tag{2}$$

Given these responses, we statistically test if faces are identifiable after image processing. Let us assume the identifiability value of a certain type of visual privacy protection with a value of its parameter is constant regardless of participants. Under this assumption, the number of correct responses L, either $L_f^g(\theta)$ or $L_c^g(\theta)$, follows the binomial distribution given the number of all responses. Letting M be the number of all responses, i.e., either $M_f^g(\theta)$ or $M_c^g(\theta)$, the probability of L is computed by

$$\Pr(L|M, \mu) = \binom{M}{L} \mu^L (1-\mu)^{M-L}, \tag{3}$$

where μ is the probability of a correct response. In other words, μ is the true identification value for the population from which the participants are selected. $\binom{M}{L}$ is the binomial coefficient, which gives the number of combinations of L responses from M responses. This equation enables us to compute the probability of L given M and μ. Using this probability, we can compute the so-called p-value for the one-tailed binomial test, where our null hypothesis is that the obtained identifiability value is μ. Under this null hypothesis, we can verify whether the obtained identifiability value is smaller than μ.

So what is μ? In this survey, each question provided participants with ten options. If participants randomly choose one of those ten options, 10% of responses identified correct subjects. If they randomly choose one out of nine candidates (but not "I don't know"), approximately 11% (i.e., $1/9$) of trials are correct. From this observation, we consider that the identifiability value of $1/10$ is a reasonable choice for judging whether visual privacy is protected by the given image processing technique. Therefore, our null hypothesis is that the identifiability value of visual privacy protection is $1/10$ given the score for one of the two factors, and its alternative is that the identifiability value is larger than $1/10$.

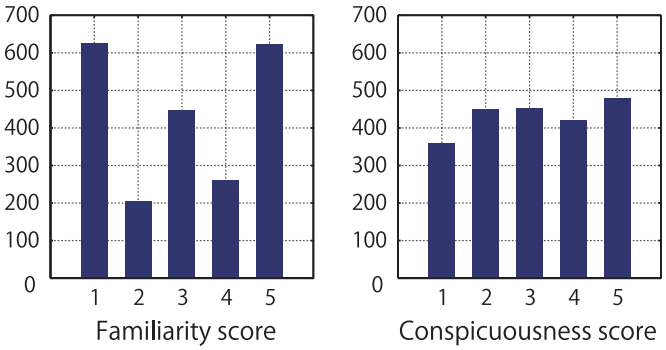

Fig. 6. Distributions of familiarity and conspicuousness scores.

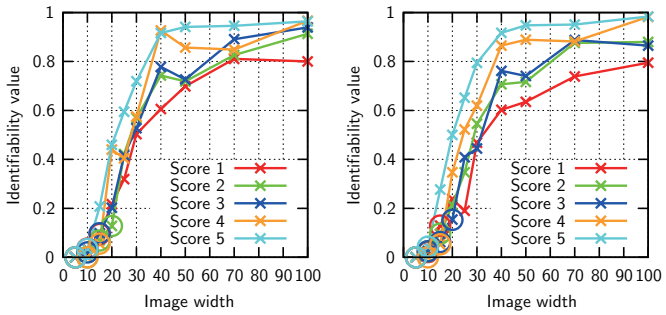

Fig. 7. Identifiability for resizing with respect to familiarity (left) and conspicuousness (right). Points with a circle are parameter values that rejected our null hypothesis. Image width is specified by parameter s.

IV. Results

On the questionnaire for evaluating familiarity and conspicuousness, 108 participants assigned scores to all 20 subjects, which resulted in 2160 total responses. Figure 6 shows the distributions of scores. The distribution for familiarity was concentrated in scores 1, 3, and 5. This indicates that participants felt no need for intermediate scores to represent their familiarity. In contrast, conspicuousness resulted in an almost uniform distribution.

A. Resizing

Figure 7 shows the identifiability values for resized facial images with respect to familiarity and conspicuousness, respectively. Both curves spike from around $s = 15$. These identifiability values seem slightly lower than those reported in [6]. One of the main factors might be the difference in the definitions for identification (choosing one from a set of given candidates in our survey vs. assigning a subject's name to a facial image based on the participant's memory) and subjects used (politicians vs. celebrities). Our results indicate that identifiability shows ceiling effects around $s = 50$ but does not reach 1 even for $s = 100$, because our dataset contained subjects who resemble each other in their facial images. For lower familiarity and conspicuousness scores, the variation among facial images of one subject maintained low identifiability. Even with the image size of 100×100 pixels, the identifiability values for score 1 in both factors are around 0.8, which means the subjects with low familiarity or conspicuousness could not be accurately identified consistently. This result also acts as a baseline of identifiability for each familiarity and conspicuousness score, as parameter value $s = 100$ is the original facial image size in our dataset.

B. Blocking out facial regions

Identifiability for blocking out on facial regions is shown in Fig. 8. Interestingly, comparing horizontal and vertical shifts, the identifiability for the horizontal shift is almost symmetric with respect to n and increases suddenly when $|n| \geq 2$, while that for the vertical shift is less symmetric and changes more gradually. The low identifiability values for the vertical shift when n is larger are because our vertical shift only disclosed a subject's forehead even for the

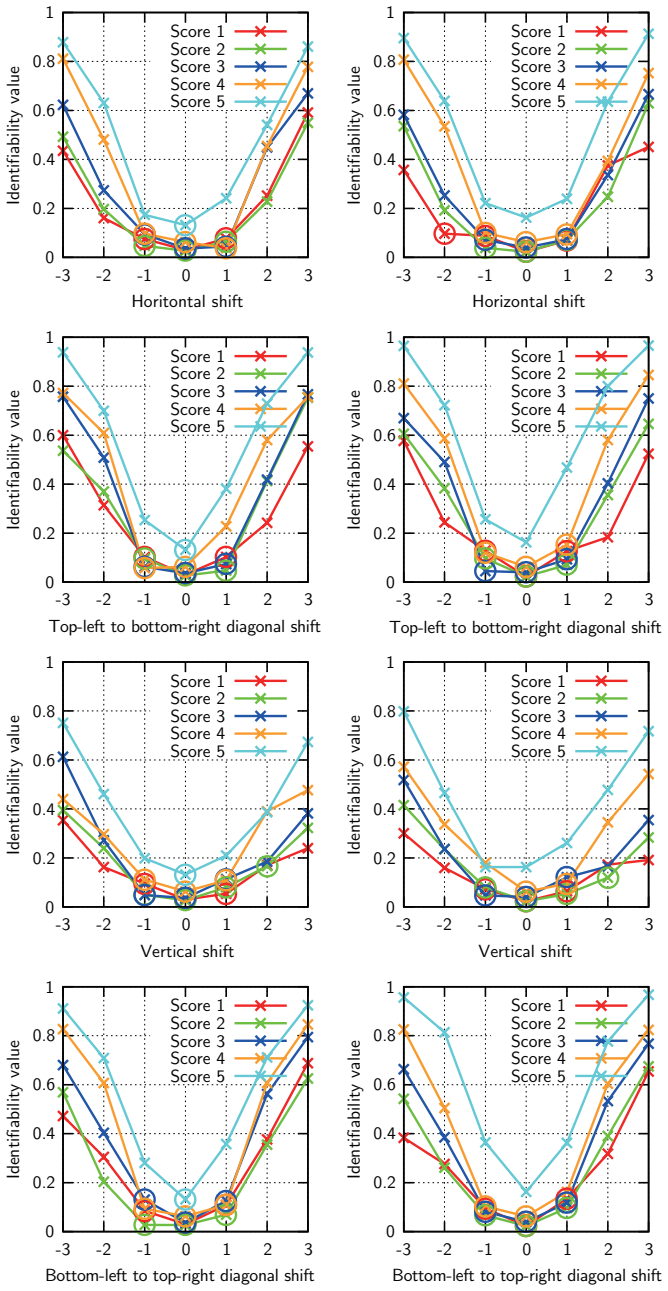

Fig. 8. Identifiability for blocking out facial regions with respect to familiarity (left) and conspicuousness (right). Amount of shift (horizontal axis) is specified by parameter n.

largest n. The relatively low identifiability for $n = -3$ in the vertical shift indicates that subjects' mouth regions are not very informative cues compared to features around the eyes. Identifiability values even for $n = 0$ do not reach zero and increase with familiarity or conspicuousness scores, which may imply that participants could guess identities based on the subject's clothes.

C. Blocking out eye regions

Figure 9 shows the results for blocking out eye regions. Although this image-processing technique is sometimes adopted in some applications, it hardly affected privacy protection capability in our survey. Even for the lowest familiarity and conspicuousness scores, identifiability remains over 0.6 for most cases. A comparison between horizontal and vertical shifts demonstrates that the difference in shift direction almost does not affect the results. It is noteworthy, however, that the difference in conspicuousness appears to yield larger gaps in identifiability than

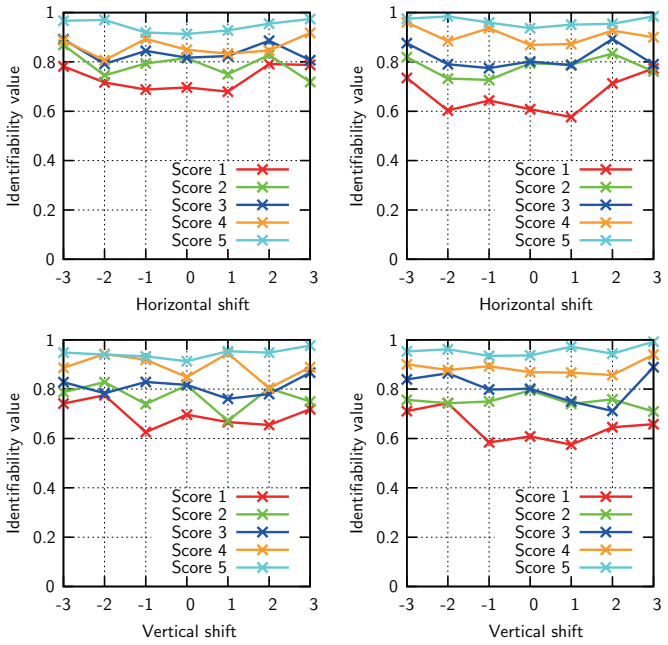

Fig. 9. Identifiability for blocking out eye regions with respect to familiarity (left) and conspicuousness (right). Amount of shift is specified by parameter n. No parameter value rejected the null hypothesis.

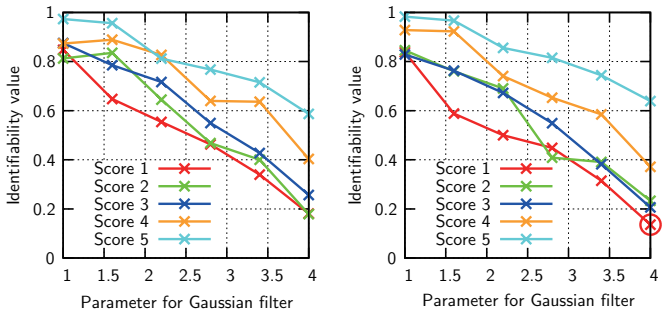

Fig. 10. Identifiability for blurring with respect to familiarity (left) and conspicuousness (right). Parameter for Gaussian filter is specified by σ. Our null hypothesis was rejected only when parameter σ is 4 and a conspicuousness score is 1.

does familiarity.

D. Blurring

The parameter σ for blurring almost linearly decreases identifiability, as shown in Fig. 10. Although blurring is a widely used image processing technique, its privacy protection capability is not ideal. Subjects with highest familiarity and conspicuousness scores obtained identifiability values around 0.6. Blurring also results in a substantial separation among different conspicuousness scores.

V. Discussion

Here, we discuss the correlation between the two factors that affect identifiability and the statistical significance of the results obtained in our survey.

A. Correlation between familiarity and conspicuousness

Before discussing the privacy protection capabilities of the image-processing techniques, we consider the relationship between familiarity and conspicuousness scores obtained in our survey. Observing the identifiability values for each factor, we can hypothesize that familiarity and conspicuousness scores are highly correlated. To verify this

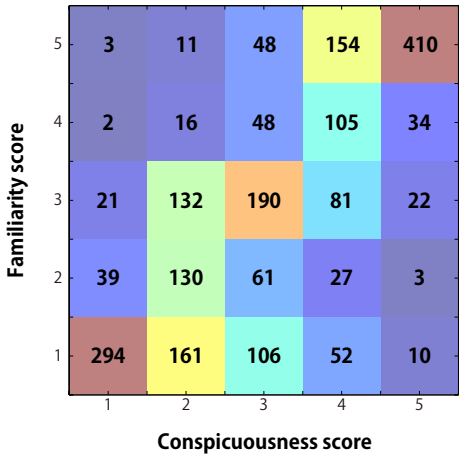

Fig. 11. Conspicuousness-versus-familiarity histogram.

hypothesis, we generated the conspicuousness-versus-familiarity histogram (Fig. 11). This figure shows relatively high numbers of responses in the diagonal elements, which indicates that many participants assigned the same scores to familiarity and conspicuousness. This is significant for familiarity scores "1" and "5," though the other familiarity scores were relatively spread. In contrast, conspicuousness scores for the two extreme familiarity scores appear distributed, but not as much for the other three familiarity scores. In sum, the familiarity and conspicuousness scores appear to be strongly correlated, although responses with the two extreme familiarity scores are spread across different conspicuousness scores.

This might support the wider separation of identifiability values between conspicuousness scores "1" and "5," which is particularly noticeable for blocking out eye regions and blurring. Our evaluation method required participants to choose one face image out of ten options (nine candidates plus "I don't know") that appeared to contain the same subject as the stimulus; thus, conspicuousness appears to more directly affect identifiability, and our survey successfully captured this tendency.

B. Identifiability after image processing

In Figs. 7–10, points with a circle indicate that our null hypothesis is accepted for that parameters with a significance level of 0.05. Other parameter values rejected the null hypothesis, indicating the identifiability value is larger than $1/10$ and thus subjects were identifiable. Figure 7 implies that we must apply visual privacy protection to face images larger than 10×10. This requirement might be slightly relaxed to 15×15 if we can assume that the subjects are not conspicuous or are complete strangers for expected viewers. From Fig. 8, acceptable errors in automatically locating facial regions by computer vision technologies are, in most cases, less than 12.5% of face images. Even when blocking entire facial regions, viewers might accurately guess identities if the subjects are conspicuous. We might need to be more conservative about automatic visual privacy protection. Blocking out eye regions is nearly useless; this technique hardly reduces identifiability values, as indicated in Fig. 9. Face images after blurring, even with $\sigma = 4$, remain identifiable. For secure privacy protection, a blurring kernel at least larger than $\sigma = 4$ is required.

The limitation of our survey is that the way of identifying subjects does not necessarily fit to our actual cognitive process because facial images of candidates can provide prior information on possible subjects, which tends to facilitate the identification. However, our results could bring a guideline to realize stricter protection of visual privacy information.

VI. Conclusion

This article discussed the relationship between visual privacy protection capabilities and two factors, familiarity and conspicuousness. Our survey over more than 100 participants demonstrated that conspicuousness is a more significant factor than familiarity, although the difference is marginal. We also found that blocking out eye regions and blurring are almost incapable of protecting privacy. The requirements for automatic visual privacy protection

are drastic, such that computer vision technologies must find faces smaller than 15×15 and localization errors must be smaller than 12.5% of the facial region. The results presented in this article are beneficial for designing automatic privacy protection, and we hope this work helps to facilitate development in this field.

REFERENCES

[1] YouTube. (2012) Face blurring: when footage requires anonymity. [Online]. Available: http://youtube-global.blogspot.com/2012/07/face-blurring-when-footage-requires.htmlGG

[2] X. Yu, K. Chinomi, T. Koshimizu, N. Nitta, Y. Ito, and N. Babaguchi, "PriSurv: Privacy protecting visual processing for secure video surveillance," in *Proc. of Int'l Conf. on Image Processing (ICIP 2008)*, October 2008, pp. 1672–1675.

[3] C. Neustaedter, S. Greenberg, and M. Boyle, "Blur filtration fails to preserve privacy for home-based video conferencing," *ACM Trans. Computer-Human Interaction*, vol. 13, no. 1, pp. 1–36, 2006.

[4] A. Senior, S. Pankanti, A. Hampapur, L. Brown, Y.-L. Tian, and A. Ekin, "Enabling video privacy through computer vision," *IEEE Security & Privacy*, vol. 3, no. 3, pp. 50–57, 2005.

[5] Y. Nakashima, N. Babaguchi, and J. Fan, "Automatically protecting privacy in consumer generated videos using intended human object detector," in *Proc. the 18th ACM Int'l Conf. Multimedia*, 2010, pp. 1135–1138.

[6] A. W. Yip and P. Sinha, "Contribution of color to face recognition," *Perception*, vol. 31, no. 8, pp. 995–1003, 2002.

[7] A. M. Burton, S. Wilson, M. Cowan, and V. Bruce, "Face recognition in poor-quality video: Evidence from security surveillance," *Psychological Science*, vol. 10, no. 3, pp. 243–248, 1999.

[8] P. Sinha, B. Balas, Y. Ostrovsky, and R. Russell, "Face recognition by humans: nineteen results all computer vision researchers should know about," *Proc. the IEEE*, vol. 94, no. 11, pp. 1948–1962, 2006.

[9] Y. Nakashima, T. Ikeno, and N. Babaguchi, "Quantitative evaluation on effectiveness of privacy protection for facial images," in *IEICE Technical Report, EMM2012-9*, 2012, pp. 59–66.

[10] J. Sadr, I. Jarudi, and P. Sinha, "The role of eyebrows in face recognition," *Perception*, vol. 32, no. 3, pp. 285–293, 2003.

[11] N. Babaguchi, T. Koshimizu, I. Umata, and T. Toriyama, "Psychological study for designing privacy protected video surveillance system: PriSurv," in *Protecting Privacy in Video Surveillance*. Springer Verlag, 2009, pp. 147–164.

PLACE PHOTO HERE

Yuta Nakashima received the B.E. and M.E. degrees in communication engineering from Osaka University, Osaka, Japan in 2006 and 2008, respectively, and the Ph.D. degree in engineering from Osaka University, Osaka, Japan, in 2012. He is currently an Assistant Professor at Graduate School of Information Science, Nara Institute of Science and Technology (NAIST) and a visiting scholar at Carnegie Mellon University. His research interests include video content analysis using probabilistic and statistical approaches. He is a member of the IEEE, the ACM, and the IEICE.
email: n-yuta@is.naist.jp

PLACE PHOTO HERE

Tomoaki Ikeno received the B.E. from Osaka University, Osaka, Japan. He is currently with ALPS ELECTRIC CO., LTD.
email: ikeno@nanase.comm.eng.osaka-u.ac.jp

PLACE PHOTO HERE

Noboru Babaguchi received the B.E., M.E., and Ph.D. degrees in communication engineering from Osaka University, in 1979, 1981, and 1984, respectively. is currently a Professor of the Department of Information and Communications Technology, Osaka University. From 1996 to 1997, he was a Visiting Scholar at the University of California, San Diego. His research interests include image analysis, multimedia computing, and intelligent systems. He received Best Paper Award of 2006 Pacific-Rim Conference on Multimedia (PCM 2006), and Fifth International Conference on Information Assurance and Security (IAS 2009). He is on the editorial board of Multimedia Tools and Applications, Advances in Multimedia, and New Generation Computing. He served as a General Co-chair of the 14th International MultiMedia Modeling Conference (MMM 2008), ACM Multimedia 2012, and so on. He has published over 200 journal and conference papers and several textbooks. He is a fellow of the IEICE, a senior member of the IEEE, and a member of the ACM, the IPSJ, the ITE and the JSA.
email: babaguchi@comm.eng.osaka-u.ac.jp