Anonymizing Face Images by Using Similarity-Based Metric

Tomoya Muraki
Department of Informatics,
University of Electro-Communications
Tokyo, Japan
e-mail: muraki@edu.hc.uec.ac.jp

Shintaro Oishi
Department of Informatics,
University of Electro-Communications
Tokyo, Japan
e-mail: s-oishi@uec.ac.jp

Masatsugu Ichino
Department of Informatics,
University of Electro-Communications
Tokyo, Japan
e-mail: ichino@inf.uec.ac.jp

Isao Echizen
Digital Content and Media Science Research Division,
National Institute of Informatics
Tokyo, Japan
e-mail: ieechizen@nii.ac.jp

Hiroshi Yoshiura
Department of Informatics,
University of Electro-Communications
Tokyo, Japan
e-mail: yoshiura@hc.uec.ac.jp

***Abstract*— Vast numbers of face images are posted and circulated daily on social network and photo-sharing sites. Some face images are linked to the person's name, like those on user profile pages, while others are anonymized due to privacy concerns. If an anonymized face image is linked to a named one, that person's privacy is infringed. One way to overcome this privacy problem is to anonymize face images when they are posted on social networks. However, current face anonymization methods fail to meet two key requirements: being provably secure against de-anonymization and enabling users to control the trade-off between security and usability (similarity to the original face) of the anonymized face images. We are developing a similarity-based method for face anonymization that meets both requirements in those cases where a new face image of a person is to be posted when many face images including those of that person are already posted. The basic idea is to hide the new face image in *s* face images that are equally similar to the face image of the same person. We theoretically demonstrated that the probability of an attacker correctly linking the anonymized face image to an image of the same person is less than 1/*s*. We also showed theoretically and confirmed experimentally, with 150 sample face images, that the larger the *s*, the less usable the anonymized face image. The security of our method holds in spite of future improvements in face recognition tools.**

Keywords-component; privacy, anonymization, face anonymization

I. INTRODUCTION

As social networks are used to exchange not only text comments but also photos, vast numbers of photos are posted and circulating on them. For example, more than 300 million photos are uploaded to Facebook every day [1]. Many photos are also posted on photo-sharing sites, such as Flickr, as well as on various other types of sites, such as dating sites. Many of these photos include face images, and some of these face images are linked to the person's name, like those on user profile pages, while others are anonymized due to privacy concerns. If an anonymized face image is linked to a named one, i.e. it is determined that the two face images are of the same person, that person's privacy is compromised. The behaviours of that person and his or her friends recorded in the anonymized image are now available to his/her other friends, employer, etc. Acquisti et al. showed that anonymized face images uploaded to a dating site can be linked to those in Facebook profiles by using a face recognition tool, so the identities of the dating site users can be compromised [2]. Such privacy risks are becoming greater because of recent improvements in face recognition tools.

One way to overcome this privacy problem is to anonymize face images when posting them on social networks. Methods for face anonymization must be secure against de-anonymization. In addition, they must enable users to control the trade-off between security and usability of the anonymized images because the more the images are

978-0-7695-5008-4/13 $26.00 © 2013 IEEE
DOI 10.1109/ARES.2013.68

anonymized, the less lively and less natural they are. Easy methods for face anonymization use distortion through pixelation and blurring [3][4]. Newton et al. developed an anonymization method that replaces a face image by the average of the k most-similar faces [5]. Bitouk et al. developed a method that replaces a face image with a face image of another person [6]. However, as discussed in Section II, none of these methods meet the two requirements, i.e. being provably secure against de-anonymization and enabling users to control the trade-off between security and usability in those cases where a new face image of a person is posted when many face images including those of that person are already posted. A representative case is that in which a user posts a new face image on the internet where many face images have already been posted.

Our Contribution

We are developing a similarity-based method for face anonymization that has provable security and trade-off controllability in the situation described above. We define the security of face anonymization as the degree to which an attacker cannot link an anonymized face image to an existing face image of the same person. The basic idea is to hide the new face image of a person in $\boldsymbol{s}$ face images that are equally similar to posted face images of the same person. More precisely, the new face image is anonymized so that a posted image of the same person is any one of $\boldsymbol{s}$ or more posted face images most similar to the anonymized face image.

We demonstrated theoretically that the probability of an attacker correctly linking the anonymized face image to an image of the same person is basically less than $1/\boldsymbol{s}$. We theoretically demonstrated and experimentally confirmed, with 150 sample face images, that the larger the $\boldsymbol{s}$, the less usable (i.e. similar to the original face image) the anonymized face image. These properties do not depend on the specific similarity metric used for the anonymization and hold even if the similarity metrics used in the anonymization and attack differ. The security of our method therefore holds in spite of future improvements in face recognition tools. The proposed method is useful not only for face anonymization but also for a wide range of potential applications such as anonymizing voice data and social network profiles.

The structure of this paper is as follows. Section II surveys related work. Section III describes the proposed similarity-based anonymization method. Section IV describes its implementation, and Section V presents the results of our evaluation in terms of security and trade-off controllability. Section VI discusses the remaining security problem and future work. Section VII describes its application to anonymizing other types of personal information, and Section VIII concludes with a brief summary of the key points and a mention of future work.

II. RELATED WORK

A. Privacy Problems with Posting Face Images

Faces of the people in a photo posted on the internet without the names of the people in the photo can be linked with the faces of those people in other photos posted along with the names of the people in the photo, thereby enabling identification of the people in the anonymously posted photo. Acquisti et al. used face recognition technology to compare anonymous face images posted on a dating site with those in Facebook profiles and showed that the Facebook accounts of users of the dating site could be identified [2]. The accuracy of face recognition technology is increasing year by year, so the risk of being identified from a face image is increasing.

B. Anonymization Techniques

Anonymization of personal information is used to reduce the risk of individuals being identified. Here, we describe basic anonymization methods. A typical anonymization method is k-anonymity, in which the values of attributes that contribute to identifying individuals (quasi-identifiers) are equalized within a group of k or more individuals so that it is not possible to identify which individual among the k individuals is represented [7]. The trade-off between the usability of the personal data and security can be controlled by varying the value of k.

k-anonymity is not secure against several attacks. Among such attacks, the homogeneity and background attacks are addressed by methods called "ℓ-diversity" [8] and t-closeness [9] respectively. With anonymization methods such as k-anonymity, ℓ-diversity, and t-closeness, the database administrator must modify all quasi-identifiers throughout the database. For the case in which a user posts his/her face image on the internet, it is not possible for him/her to modify the images that have been posted by other people. It is often cumbersome or undesirable to modify one's own face images that have already been posted in an effort to prevent those images from being linked to a newly posted face image. Thus, these basic methods of anonymization are unsuitable for cases in which a face image of a person is newly posted when many face images including those of that person are already posted.

C. Face Anonymization

The simplest way to anonymize face images is to add blurring or block noise to the image [3][4]. However, these methods detract from the naturalness of the image. Moreover, they are not secure; i.e. methods have been developed for regenerating the original face image from images anonymized by adding block noise [10]. Bitouk et al. developed a method for replacing the face in a photograph with the face of a different person, but this can change the nuance of a photograph, and the rights of the person whose face is used as a replacement must be taken into consideration [6].

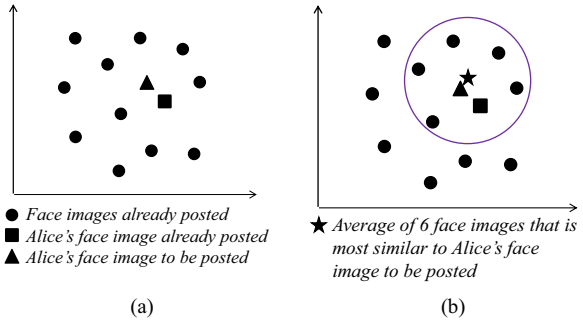


Figure 1. Security problem with method [5].

Newton et al. applied k-anonymity to face images to take privacy into consideration when sharing images from surveillance cameras, proposing a way to control the trade-off between security and usability with these images [5]. This method replaces a face appearing in a monitor camera video with a face that is the average of the k faces that are similar to the original face. However, this method is not secure if a new face image of a person is posted when many face images, including those of that person, are already posted.

The problem with using the average of k faces similar to the original face is illustrated in Figure 1. Alice is planning to post a new face image. One of her face images has already been posted, and there are 11 other posted face images. The new image is similar to the one of Alice already posted since they are of the same person, so they are positioned close to each other in the 2D vector space. A new image is created by averaging the six already posted images that are the most similar to the new image of Alice, as shown in Figure 1 (b). As can be seen from this figure, the average face image is very close to the new image, which is near the already posted image of Alice, meaning that the average image is close to the already posted image. Consequently, if an attacker uses face recognition technology to find several face images close to the average image, he/she will likely find that the already posted image of Alice is the closest one. Thus, this averaging method is not secure.

In short, none of the conventional face anonymization methods can satisfy both requirements, i.e., provable security and trade-off controllability between security and usability.

III. SIMILARITY-BASED FACE ANONYMIZATION

Our proposed face anonymization method both guarantees security and enables control of the trade-off between security and usability.

A. Basic Requirements

For cases in which there is a collection of already posted face images and a new face image is to be anonymized and posted, two requirements must be satisfied.

1) Security against identifying the individual in the face image must be guaranteed.

2) The trade-off between this security and image usability must be controllable.

B. Model

1) Assumptions

Our model is based on two assumptions.

***Assumption 1**: The face images already posted include only one face image of the person whose new face image is to be posted.*

***Assumption 2**: There is an algorithm for computing the similarity of two face images.*

The first assumption is for the simplicity of discussion, and its removal will be considered in Section VI.

2) Definitions

Three basic concepts of our face anonymization technique are defined on the basis of the assumptions above.

***De-Anonymization**: The anonymized face image is linked to the face image of the same person already posted.*

***Security of Face Anonymization**: This is the probability that an attacker attempting to crack the anonymization will fail.*

***Usability of Anonymized Face Image**: This is the similarity between the face image to be posted and the anonymized face image.*

3) Notation

- D: set of face images already posted
- n: number of images in D
- d: face image to be newly posted
- d_a: face image created by anonymizing d (or, d anonymized)
- d': face image in D that is of the same person as in d
- A: algorithm that computes similarity between images
- $A(d_x, d_y)$: similarity between face images d_x and d_y calculated using algorithm A

4) "s-similarity set" of Face Images

Given set D of n already posted face images and algorithm A for calculating similarity, the ***s***-similarity set for arbitrary face image d_x is a subset of D; it is generated using the following procedure.

Step 1. Calculate $A(d_x, d_i)$ *for* i = *1 to* n *and* $d_1, d_2, ..., d_i, ..., d_n \in D$.

Step 2. Select the ***s*** largest values from among the n values, $A(d_x, d_i)$.

Step 3. Form $sim(d_x, s, D, A)$ *as the set of* s *corresponding* d_i.

C. Mathematical Requirements

The two basic requirements given in A can be defined mathematically.

1) Security

The probability that anonymized face image d_a will be linked with the already posted face image d' of the same person is a monotonically decreasing function of s that converges to zero. That is, as s increases, the security against identifying the individual increases. This requirement is given mathematically as $d \in sim(d_x, s, D \cup d, A)$.

2) Usability

The similarity between anonymized face image d_a and the image before anonymization is a monotonically decreasing function of s that converges to zero. Thus, as s increases, usability decreases.

D. Anonymization Steps

An anonymized face image d_a satisfying the mathematical requirements in C is generated by the following steps.

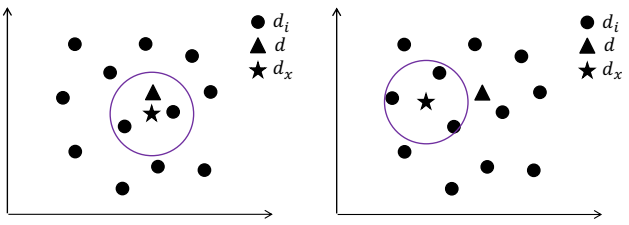
Step 1. Generate a candidate for d_a
Generate candidate d_x for d_a randomly.

Step 2. Determine eligibility
If Requirement (1) below is satisfied for the d_x generated in Step 1, use d_x as the anonymized data, d_a. Return to Step 1 if it is not satisfied.

$$d \in sim(d_x, s, D \cup d, A) \qquad \text{Requirement (1)}$$

Step 3. Output d_a.
Output anonymized face image d_a in place of face image d.

Requirement (1) ensures that the pre-anonymized face image d is within the s-similarity set of the anonymized candidate d_x. For example, showing face images as points in a 2D vector space, with the similarity between images as the inverse of the distance between them, then a d_x satisfying Requirement (1) is shown in Figure 2 (a) and a d_x not satisfying Requirement (1) is shown in Figure 2 (b).



(a) $d \in sim(d_x, 3, D \cup d, A)$ (b) $d \notin sim(d_x, 3, D \cup d, A)$

Figure 2. Candidate anonymized faces that do and do not satisfy Requirement (1).

IV. Implementation

A. Active Appearance Models

We implemented our proposed method using an active appearance model (AAM), which integrates feature point information and appearance information for a face image [12][13]. The AAM was generated using the steps below.

Step 1. Principal component analysis (PCA) was applied to feature point information to compute a shape vector and to appearance information to compute an appearance vector.

Step 2. PCA was then applied to the combination of these two vectors to create a composite face-image vector (hereinafter called "face vector").

B. Face Vector Construction

We used grey-scale images as our sample images. Support for full-colour face images is left for future work. We used 68 points on the face contour and various parts of the face (e.g. eyebrows, eyes, nose, mouth) as face image feature points. The 2D coordinates of the 68 feature points were concatenated into a 136-dimensional vector. PCA was then used to reduce it to an 11-dimensional vector that had a cumulative contribution of 95% or greater. This vector was used as the shape vector.

For the appearance information, we created an appearance vector from the face image appearance values. To keep the sizes of the appearance vectors constant, we normalized them by mapping the face image to an average face shape using piecewise affine texture mapping. For a 260×360 pixel image, this gave a 93,600-dimensional appearance vector, which was then reduced to a 51-dimensional vector by PCA. The shape vector and appearance vector were then concatenated, and PCA was used to create a 30-dimensional vector. This vector was used as the face vector.

C. Anonymization of Face Vector

AAM was applied to the n already posted face images, converting them to n face vectors, $d_1, d_2, ..., d_n$. Anonymization was then applied using these face vectors in accordance with the following procedure.

Step 1. Randomly generate candidate d_x for anonymized face vector d_a.

Step 2. Using algorithm A to compute similarity, generate the s-similarity set for candidate vector d_x. If the d_x generated in Step 1 satisfies Requirement (1), then use d_x as the anonymized face vector d_a. If not, then return to Step 1.

$$d \in sim(d_x, s, D \cup d, A) \quad \text{Requirement (1)}$$

Step 3. Output anonymized face vector d_a

The similarity between two face vectors was computed using algorithm A and the Face Sensing Engine (FSE)

provided by Oki Electric Industry Co., Ltd. [14]. The candidate anonymized face vector d_x was generated as follows. In principle, the candidate must be generated using uniformly random numbers in each dimension of the 52-dimensional vector space. However, using such a method would require generating a very large number of candidates and testing them for eligibility, which would not be practical. Thus, we established a subspace of candidates that satisfy Requirement (1) in accordance with parameter $\boldsymbol{s}$ and generated candidates randomly within this space. We omit a detailed description of this process due to space restrictions.

D. Face Image Construction from Face Vector

From the generated anonymized face vector d_a, we computed the anonymized face shape and appearance vectors and texture-mapped the appearance information onto the shape using piecewise affine mapping, resulting in an anonymized face image.

V. EVALUATION

A. Attacker Model

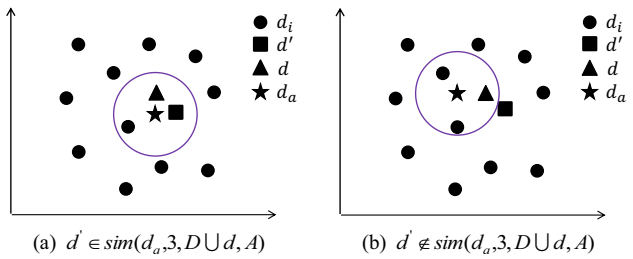
We defined an attacker model for use in evaluating the security of the proposed method. When evaluating an information security method, the algorithm is generally published. Assuming the anonymization method will be published, we can divide potential attackers into two types.

1) Intelligent Attacker

An intelligent attacker is one who attempts to crack the anonymization with a full understanding of the proposed method. He/she first obtains the anonymized face image d_a and each of the images in the face image set D. On the basis of the full understanding, he/she then selects the image in D that is most likely to be d', i.e. the already posted image of the same person.

2) Naïve Attacker

A naïve attacker is one who attempts to crack the anonymization without an understanding of the proposed method. He/she simply computes the similarity between the anonymized face image d_a and each image in D and determines that the image most similar to d_a is d'. Note that we assume for the sake of simplicity that both types of attackers select only one face image as a candidate of d'.



(a) $d^{'} \in sim(d_a,3,D \cup d,A)$ (b) $d^{'} \notin sim(d_a,3,D \cup d,A)$

Figure 3. s-similarity sets of anonymized face images that do and do not include face image of same person.

B. Evaluation of Security

The only information available to an attacker due to publishing the proposed method is that the anonymized face image satisfies Requirement (1). In other words, the original face image falls within the $\boldsymbol{s}$-similarity set for the anonymized image. The original face image d and already published face image d' are of the same person, so the value $A(d,d^{'})$ would be large, and a d_a satisfying Requirement (1) would also be expected to satisfy $d^{'} \in sim(d_a,s,D \cup d,A)$.

However, d_a is generated randomly under Requirement (1), so this second condition is not necessarily satisfied. Figure 3 (a) shows a case in which Requirement (1) is satisfied and $d^{'} \in sim(d_a,s,D \cup d,A)$; Figure 3 (b) shows a case in which Requirement (1) is satisfied and $d^{'} \notin sim(d_a,s,D \cup d,A)$. From this, the probabilities that attackers of each type will be able to crack the anonymization are as follows.

1) Against Intelligent Attacker

Since an intelligent attacker understands the proposed method, he/she will conduct the attack with awareness that $d^{'} \in sim(d_a,s,D \cup d,A)$ or $d^{'} \notin sim(d_a,s,D \cup d,A)$. The attacker first considers the case in which $d^{'} \in sim(d_a,s,D \cup d,A)$. Since anonymized face d_a generated randomly in Step 1 is not based on an artificial design, the probability that any of the $\boldsymbol{s}$ face images in $sim(d_a,s,D \cup d,A)$ is d' is the same, i.e. $1/\boldsymbol{s}$. This means that the probability that an intelligent attacker can match d' to d_a is $1/\boldsymbol{s}$. When considering the case in which $d^{'} \notin sim(d_a,s,D \cup d,A)$, an intelligent attacker needs to search over a wider range (e.g. the $2\boldsymbol{s}$-similarity set) for d'. This means that the probability that an intelligent attacker can match d' to d_a is less than $1/\boldsymbol{s}$.

2) Against Naive Attacker

A naïve attacker decides that the face image with the greatest similarity to anonymized face image d_a is the already posted image d' of the same person. Consider first the case in which $d^{'} \in sim(d_a,s,D \cup d,A)$. The anonymized face image is randomly generated in Step 1, so the $\boldsymbol{s}$ face images in $sim(d_a,s,D \cup d,A)$ each have the same probability of being the most similar. This means that the probability that a naïve attacker can match d' to d_a is $1/\boldsymbol{s}$. Thus, the probability that the naïve attacker correctly selects d' is $1/\boldsymbol{s}$. On the other hand, if $d^{'} \notin sim(d_a,s,D \cup d,A)$, the probability that d' will be selected correctly is zero.

3) Different Algorithms for Calculating Similarity

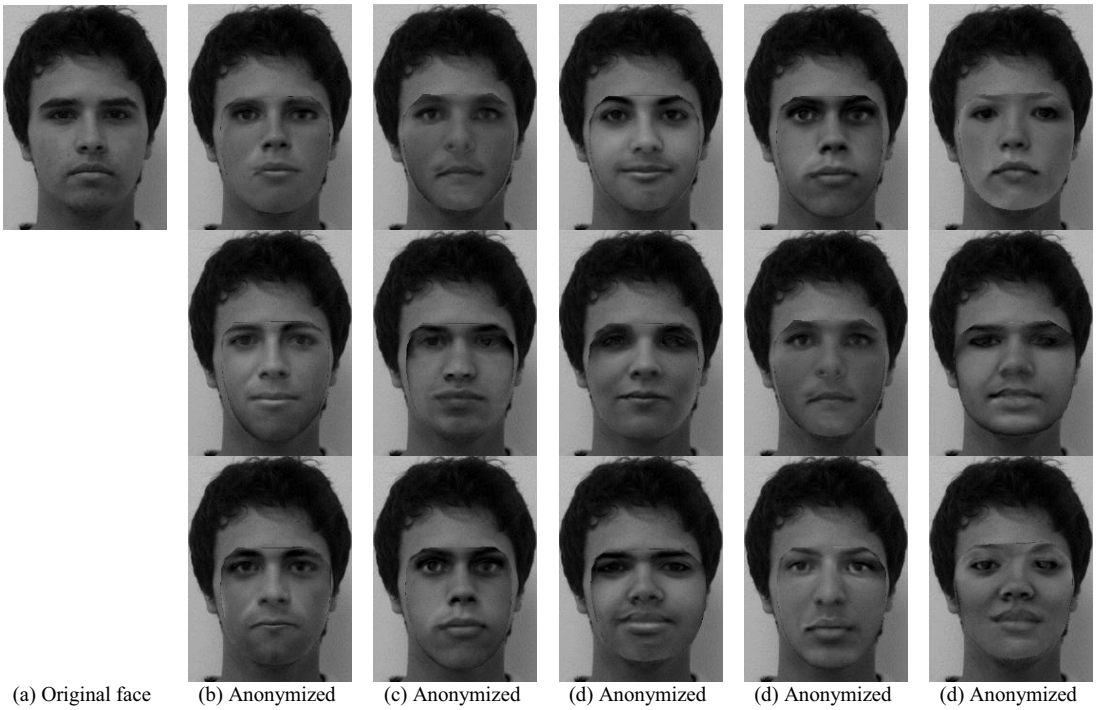
Consider the case in which an attacker uses a different algorithm, A'. Using A' would result in a different $\boldsymbol{s}$-similarity set for the anonymized face image, but since d_a was generated randomly, as it was with algorithm A, there

are still two cases: $d' \in sim(d_a, s, D \cup d, A')$ and $d' \notin sim(d_a, s, D \cup d, A')$. Furthermore, it is still true that any given image within the ***s***-similarity set of the anonymized face image could be the already published face image with the same probability. Thus, reasons 1) and 2) above still apply, and the probability of success for either type of attacker is still 1/***s*** or less. As such, the security of the proposed method does not depend on whether the similarity algorithms used in anonymization and by the attacker are the same or not. Thus, if the similarity algorithms used by attackers become more sophisticated in the future, the probability that the anonymization can be cracked will remain at 1/***s*** or less. The proposed method thus satisfies the requirement for security described in Section III.C.

C. *Evaluation of Usability*

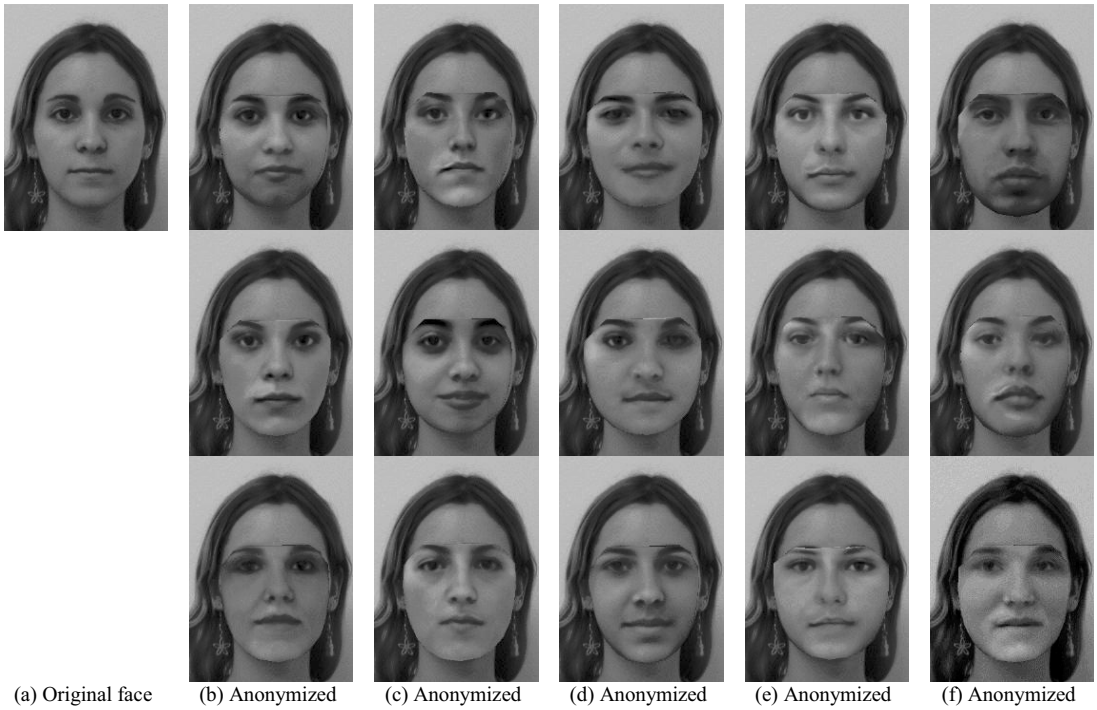
In Step 1, if ***s*** = 1, d_x must be closer to d than any other face image in D in order to satisfy Requirement 1. If ***s*** = 10, d_x only needs to be included in the 10 closest images, and if ***s*** = n + 1 (n is the number of elements in D), d_x can be any distance from d. In this way, as ***s*** becomes larger, the anonymized image d_a becomes more distant from d. Thus, on average, as ***s*** becomes larger, $A(d_a, d)$ becomes smaller, and the usability of d_a decreases.

We evaluated the usability of the proposed method using a database of front-facing face images [15] of 150 men and women (75 each) ranging in age from 19 to 40. For each of the two original faces (shown in Figure 4 and 5 (a)) and for five values of ***s*** (3, 5, 10, 30, and 150), we generated 30 anonymized face images (300 in total). Figures 4 and 5 (b) through (g) show three anonymized face images from 30 images generated for each original face and parameter ***s***. A visual comparison shows that the larger the ***s***, the less similar the anonymized image to the original.We anonymized the face images of two men and two women in addition to those in Figure 4 and 5 (a). The average similarity between each original face image and 30 anonymized face images for each value of ***s*** is plotted in Figure 6. We used the FSE to compute the similarity. As the level of anonymization, i.e. the value of ***s***, increased, the similarity between the anonymized face image and the face image before anonymization decreased. Thus, the proposed method satisfies the requirement for usability described in Section III.C.



(a) Original face | (b) Anonymized face for s = 3 | (c) Anonymized face for s = 5 | (d) Anonymized face for s = 10 | (d) Anonymized face for s = 30 | (d) Anonymized face for s = 150

Figure 4. Original face of MAN01 and anonymized faces for different values of s.



(a) Original face (b) Anonymized face for $s = 3$ (c) Anonymized face for $s = 5$ (d) Anonymized face for $s = 10$ (e) Anonymized face for $s = 30$ (f) Anonymized face for $s = 150$

Figure 5. Original face of WOMAN01 and anonymized faces for different values of s.

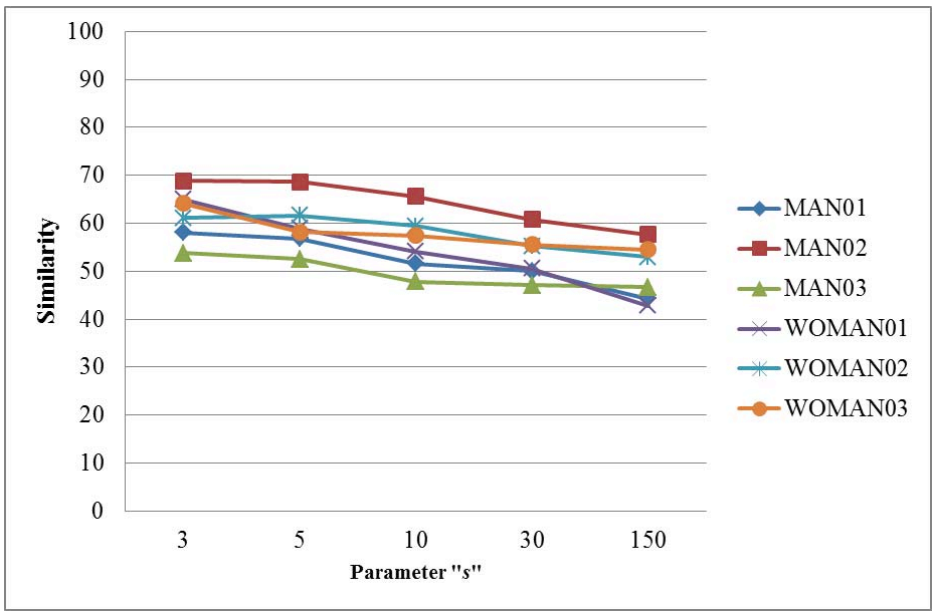


Figure 6. Similarity between original and anonymized face images.

VI. FUTURE WORK ON SECURITY

As explained in Section III.B, we assumed that the set of already published face images D includes only one face image of the person whose new face image is to be published. In reality, however, a person may have published several copies of his/her face image or published several different face images. We also assumed, as mentioned in Section V.A, that the attacker selects only one candidate for d' (an already published face image of the target person). One way to maintain the security of the proposed method without these assumptions is to use a larger s, which would

result in anonymized images that are more secure but less similar to the original image. The use of such images seems natural for situations in which the user has published many images of his/her face and an attacker checks more candidates for breaking the anonymity. Clarifying the security without these assumptions remains for future work. Future work also includes clarifying the security for situations in which the user has published multiple anonymized face images. An attacker taking the intersection of the sets of candidate images may succeed in finding the correct d' with a probability larger than 1/***s***.

A third and more subtle security problem comes from the fact that the distribution of face images in the face space is not uniform. That is, the volume of the subspace for Alice's anonymized face may differ from that for Carol's anonymized face. If these two subspaces intersect and an anonymized face is generated in this intersection, the probability that the original face is Alice's differs from the probability that it is Carol's. Thus, the probability of an attacker breaking the anonymity is not uniformly 1/***s***. Analysis of this problem also remains for future work.

VII. APPLICATIONS

The proposed method could also be applied to other types of data, such as voice data and profile data. Anonymization of voice data is analogous to face image anonymization. For profile data, consider, for example, a case in which a user uses his/her real name in his/her Facebook profile but does not want to use his/her real name in his/her Twitter profile. The user wants to avoid having his/her Twitter profile associated with his/her Facebook profile, but at the same time wants to express some of his/her personality in the Twitter profile. In such a case, the set of published Facebook profiles would be D and would include the user's profile d', and the profile information that the user wishes to publish on Twitter would be d. The proposed method could be used to generate anonymized profile data d_a. The user would be able to control the trade-off between security of his/her personal identity and the usability of the profile information.

VIII. CONCLUSION

Methods for face anonymization must be secure against an attacker linking the anonymized face image to another image of the same person. They must enable users to control the trade-off between security and usability of the anonymized face images. The method proposed in this paper anonymizes a face image so that an image of the same person could be any one of the ***s*** or more existing face images most similar to the anonymized face image. The randomness used in the method guarantees that the probability of an attacker correctly linking the anonymized face image to the image of the same person is 1/***s*** or less. With larger values of parameter ***s***, the anonymized face images can be in wider neighbourhood of the original image and thus less similar to the original and less usable. The relationship between parameter ***s*** and usability was demonstrated through experimentation with 150 sample face images. The security of our method holds in spite of future improvements in face recognition tools. The proposed method is not limited to face anonymization—it has a wide range of potential applications, such as anonymizing voice data and social network profiles.

Future work includes enhancing the security of our method on the basis of more strict analysis of its security, evaluating the method with larger numbers of sample images, and extending the current implementation to handle colour images.

REFERENCES

[1] Facebook, http:// www.facebook.com/.

[2] A. Acquisti, R. Gross, and F. Stutzman, "Faces of Facebook: Privacy in the Age of Augmented Reality," Black Hat USA, 2011.

[3] M. Boyle, C. Edwards, and S. Greenberg, "The effects of filtered video on awareness and privacy," In Proceedings of the ACM Conference on Computer Supported Cooperative Work (CSCW'00), pp. 1–10, 2000.

[4] C. Neustaedter, S. Greenberg, and M. Boyle, "Blur filtration fails to preserve privacy for homebased video conferencing," ACM Transactions on Computer Human Interactions (TOCHI'05), 2005.

[5] E. Newton, L. Sweeney, and B. Malin, "Preserving privacy by de-identifying facial images," IEEE Transactions on Knowledge and Data Engineering, 17(2):232–243, 2005.

[6] D. Bitouk, N. Kumar, S. Dhillon, P. Belhumeur, and S. K. Nayar, "Face Swapping: Automatically Replacing Faces in Photographs," ACM Transactions on Graphics, 27(3):1-8, 2008.

[7] L. Sweeney, "k-anonymity: a model for protecting privacy," International Journal on Uncertainty, Fuzziness, and Knowledge-Based Systems, 10(5):557–570, 2002.

[8] A. Machanavajjhala, J. Gehrke, and D. Kifer, "ℓ-diversity: Privacy Beyond k-Anonymity," In Proceedings of the 22nd IEEE International Conference on Date Engineering, pp. 24-75, 2006.

[9] N. Li, T. Li, and S. Ventakasubramanian, "t-closeness: Privacy Beyond k-Anonymity and ℓ-Diversity," In Proceedings of the 23rd International Conference on Data Engineering, pp.16-20, 2007.

[10] L. Cavedon, L. Foschini, and G. Vigna, "Getting the Face Behind the Squares: Reconstructing Pixelized Video Streams," 5th USENIX Workshop on Offensive Technologies, 2011.

[11] R. Gross, L. Sweeney, F. de la Torre, and S. Baker, "Model-based face de-identification," In IEEE Workshop on Privacy Research in Vision, 2006.

[12] T. Cootes, G. Edwards, and C. Taylor, "Active appearance models," IEEE Transactions on Pattern Analysis and Machine Intelligennce (PAMI'01), 23(6):681–685, 2001.

[13] I. Matthews and S. Baker, "Active appearance models revisited," International Journal of Computer Vision, 60(2):135–164, 2004.

[14] Oki Electric Industry Co., Ltd., "Face Sensing Engine Version4," http://www.oki.com/jp/fse/.

[15] FEI Face Database, http://www.fei.edu.br/~cet/facedatabase.html.