Computers & Security 113 (2022) 102574

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

TC 11 Briefing Papers

A privacy preservation method for multiple-source unstructured data in online social networks

Chenguang Wang[a], Zhu Tianqing[a,*], Ping Xiong[b], Wei Ren[a,c,d], Kim-Kwang Raymond Choo[e]

[a] School of Computer Science, China University of Geosciences, Wuhan, China
[b] School of Information and Safety Engineering, Zhongnan University of Economics and Law, Wuhan, China
[c] Guangxi Key Laboratory of Cryptography and Information Security, Guilin, 541004 China
[d] Key Laboratory of Network Assessment Technology, CAS Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100093 China
[e] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA

ARTICLE INFO

Article history:
Received 24 March 2021
Revised 28 September 2021
Accepted 5 December 2021
Available online 6 December 2021

Keywords:
Image privacy
Privacy preservation
Objective detection
Multiple sources
Unstructured data

ABSTRACT

Significant amounts of data are generated in different formats (e.g., text, audio, and video) in online social networks and from other online sources, which can be mined to facilitate decision-making in different applications. However, it is nontrivial to preserve user and/or data privacy when we are analyzing data from multiple sources, with different characteristics. In this paper, we propose a method to preserve privacy when dealing with data obtained from multiple/disparate sources. Taking images and corresponding text descriptions as examples, we set up different methods and protection scenarios to protect the private information in the data. Our proposed method is also designed to maintain the availability of existing information and links between the two forms to some extent. We then quantitatively analyze the performance of the proposed approach.

1. Introduction

Unstructured data, such as images, videos, or audio, may include a mixture of information from diverse sources. For example, a video may have subtitles and/or audio dubbing, while images may contain tags and descriptions. Such data is generally designed to provide additional information about the object (e.g., video). Such auxiliary knowledge can be used by an attacker to infer further information, such as an individual's identity, location, social connections, and other sensitive information (e.g., unprocessed images may contain GPS information or corresponding text description). When the information is associated and describes the same object in different forms (e.g., identity information in both images and corresponding texts), then there is a real risk of privacy infringement.

Some methods have been proposed to tackle the problem of privacy disclosure across multiple online social networks, such as the paper Aghasian et al. (2017) which proposed a method to measure privacy closure, and Patsakis et al. (2014) to establish distributed scheme for media content sharing. But existing privacy preservation methods are generally designed to deal with single-source information, such as face image de-identification or text encryption. There are still challenges in designing methods that can protect private information contained in different forms with associated information, while also maintaining a certain consistency in the content, which is the focus of this paper.

One associated challenge is how to preserve privacy in correlated content while keeping the content consistency. There are two key sub-challenges to achieving the goal. The first sub-challenge is how to match the sensitive information in these diverse sources. Information from different sources is often presented in different forms. The content of sensitive information is also different. The second sub-challenge is how to define and maintain the utility of the data. Because, the sensitive information exists in various forms in the data, and the definition of privacy information will change due to some factors, like environment, people and so on. It is usually a challenge to evaluate the sensitive information quantitatively. As we aim to protect sensitive information from different sources while preserving the value of this information, we need to define some unified benchmarks to evaluate our results, which can facilitate the quantitative analysis and comparison of our methods. And we also set some metrics to measure the useful information which are retained in the processed data. These benchmarks can also show the privacy preservation effects of our methods, and to ensure the trade-off between privacy preservation and information utilization.

* Corresponding author.
E-mail addresses: cugwangcg@foxmail.com (C. Wang), tianqing.zhu@ieee.org (Z. Tianqing), pingxiong@zuel.edu.cn (P. Xiong), weirencs@cug.edu.cn (W. Ren), raymond.choo@fulbrightmail.org (K.-K.R. Choo).

https://doi.org/10.1016/j.cose.2021.102574
0167-4048/

To tackle the first sub-challenge, we apply objective detection with word tuples to integrate different forms of sensitive information. For the second sub-challenge, in addition to privacy metrics, we define utility metrics to evaluate the consistency rate in different forms of processed information and the utility of the data. Overall, this paper makes the following contributions:

- We propose a solution to realize privacy preservation in both the image and the corresponding text description. At the same time, we can keep the consistency in processed images and corresponding processed texts. This method can be extended to other forms of sensitive data from diverse sources.
- We present different measurement methods for varying preservation methods to tackle the difficulty of the measurement of privacy information and retained information. And these methods facilitate the quantitative analysis of the results of our methods.

The rest of the paper is organized as follows. Section 2 presents the relevant background materials in image privacy, text privacy and mixture data privacy preservation. Section 3 formalizes the problem and scenarios, and introduces our proposed method. Section 4 introduces the related utility and privacy analysis metrics for different methods and scenarios, and Section 5 presents our experiment settings and findings. In the last section, we conclude this paper.

2. Related work

2.1. Image privacy

With the increase of multi-media and various social platforms, a lot of pictures that contain our private information are uploaded or spread to the Internet and cloud. So several works have been done for image privacy preservation. Encryption technology is usually used in image protection, for example, in Shen et al. (2020) authors discuss the image privacy preservation in CBIR. Multiple users can use their own secret key to encrypt the image and the image features to upload to the cloud for the image retrieval. For an image including characters, the facial information of a character often attracts our attention. Facial attributes can be used in bioinformatics statistics, identity recognition and so on. The exposure of attribute information also threats our privacy. Therefore, many people proposed their methods to protect facial attributes and realize privacy preservation. In order to protect biometric attributes in facial images, Terhörst et al. (2019) used noise to transform the image representation. They proposed two types of noise, and realized the binary and continued attribute protection without the foreknown labels.

Machine learning and deep learning technology also help people solve privacy issues related to facial images. Several research are on face de-identification, such as Cho et al. (2020) used Variational Auto-Encoders architecture to change the identity-related facial attributes while preserving the rest facial attributes, like expression, in face images. Mainly change is set in a latent vector, which is a portion of the output of the encoder. Similar to the method in the previous article, Nousi et al. (2020) fine-tuned the latent vector to disturb the identity of character in image while preserving some facial attributes at the same time. And divided the method into two cases of supervised and unsupervised. In Croft et al. (2019) authors used the differential privacy mechanism in a generative model to realize the obfuscation of facial images, which made the similar images more difficult to be re-identification, and provide a higher level privacy guarantee than other facial obfuscation methods. In addition, Chen et al. (2021) propose a GAN-based method to hide the sensitive information for image data.

2.2. Text privacy

In addition to picture information, text information is also a widely available form. The adversary can get the author's identity through the stylometric features and get other attributes from texts. Apart from traditional encryption methods, text documents obfuscation is a method to provide privacy preservation while remaining the utility of text documents. The author's identity is usually regarded as sensitive information. And the document classification can be deemed as the utility. In order to protect the authorship and reserve the utility of text document, Fernandes et al. (2018) used the concept of differential privacy and introduced the distance of two bags of words to generate a new bag of word from the original one. Differential privacy can also be generalized to get many other methods to preserve the utility and privacy in text. For example, Feyisetan et al. (2019) use a generalization of differential privacy, and add noise to the representation of selected words to preserve privacy and utility in text.

Except for the protection of pure text information, some other tasks are often involved in text messages, such as NLP. In order to preserve privacy on these text messages and realize a secure NLP, Lyu et al. (2020) use LDP mechanism and improved coding mechanism to disturb the representation of text, so as to realize the privacy of NLP tasks. And Feng et al. (2020) make the point of two neural network models, and propose a new framework for multi-party interaction to realize privacy preservation.

Some medical information often appears as text. And medical text records usually contain a lot of private information about patients, such as names, diagnostic records and so on. Therefore, to balance the utility and privacy preservation for this kind of textual information, some work has been done. Based on the method of removing Protected Health Information (PHI), authors in Foufi et al. (2017) make some rules to realize privacy protection of the medical text. To improve on the lack of simply removing PHI, and keep the balance between utility and privacy, Li and Qin (2017) use several classifiers to classify the medical text, and use the k-anonymity in the cluster-level.

2.3. Mixture privacy preservation

The information we have now is not only in the form of pictures and texts but can come from different sources, such as human activities, machines and so on. And these data can be presented in different forms, such as text, sound, audio, database and so on. A survey from Zhu et al. (2020) propose a possible way that apply differential privacy to diverse scenarios. Another survey Wang et al. (2018) about privacy-preserving in big data, collecting a series of articles and methods. Multimedia content is usually shown in different forms, such as text, audio and so on. They also contain different types of identity information, like biometric identifiers or non-biometric. Ribaric et al. (2016) summarizes various methods of de-identification of multimedia data. These methods can target one identity attribute or combine with each other to realize the protection of multiple identity attributes. However, these methods do not pay much attention to the relationship between different forms of attributes while implementing protection. Usman et al. (2019) used a multilayer framework to accomplish privacy preservation of multimedia data storage and processing that collected from end-devices. Mainly use the local differential privacy technique and add noise into visual content. Biswas et al. (2019) verify their privacy-preserving method which focuses on K-means clustering in image and text clustering. But the two clusters are mutually independent, without correlation.

Although these works deal with mixed data, many existing methods are aimed at the protection of single form or source data. And some methods do not pay attention to the balance between

data availability and privacy protection. Therefore, this also highlights the significance of our work on the one hand.

3. Proposed privacy preservation method

3.1. Problem definition

The entire system is based on the assumption that we have had multi-source information and the sensitive information has been determined. Just like images and corresponding descriptions, information is presented in different forms by these data. Among them, sensitive information is selected according to different methods and processing scenarios. Although all of this information is very common in our lives, there is currently no privacy preservation tool for them.

Our goal is to find a way to preserve the image privacy and the corresponding description privacy simultaneously. In order to achieve our goal, we need to tackle two main tasks: detection and preservation. In the detection task, we should separately detect images and captions to find the specified objects; The preservation task uses occlusion or substitution methods to deal with detected images and captions, and maintain the utility of the resources.

In this paper, we take human identity, gender and events recorded in pictures as sensitive information, which presents the privacy that we aimed to preserve. In the detection task, faces often reflect a person's identity and gender, and some means of transportation and sports are often related to the event in an image, so we also need to protect objects that represent them. For example, there is an image with a description, and the corresponding text description is "a woman is playing tennis on a tennis court". The preservation task may need to protect the woman's face, original gender and the event "playing tennis" both in the picture and the related description. Fig. 1 shows a mosaic method to realize the protective effect.

3.2. Overview of the method

We divide our method into two tasks. In the detection task, first, we need to detect target objects from images and record objects contained in each image. Second, according to these object records, the method would detect the object related words from corresponding descriptions for each image. The preservation task uses occlusion or substitution approaches to deal with images and text descriptions. Most importantly, the method uses object and word tuples to maintain the consistency between the correlated information. The consistency can be reflected by two perspectives in our method, one is the consistency between detected objects and words, the other is the consistency of the content expressed by images and texts.

In particular, for the substitution process of detected images and captions, we further subdivide the privacy preservation into four scenarios. We marked the four scenarios as S_1, S_2, S_3, S_4, and some examples of these scenarios are shown in Fig. 2. The relationship between the characters and the scene is from strong to weak. These scenarios are described as follows:

- S_1: To protect the identity or gender of people in images, considering the identity and gender of characters as sensitive information. We change the face attributes or substitute the whole face to preserve sensitive information.
- S_2: Replacing objects that have connection with scene and character's behavior, such as replacing a frisbee to a volleyball, when the scene is a court. We hope to eliminate the connection between the characters behavior and the scene to some degree. Characters behaviors recorded in pictures are regarded as sensitive information.
- S_3: To protect the action that happened in images, we substitute an existing action with another action. This scenario further removes the connection between people and the scene.
- S_4: To protect the category of the object in the picture, such as changing people to another category. We use some animals to substitute sensitive objects that we will set.

In addition to providing the privacy protection method, we also described some methods to verify the utility and privacy protection effect of data in various privacy protection scenarios after different processing methods.

3.3. Detection task

The sensitive information we need to detect is different from diverse methods and privacy protection scenarios. And the detec-

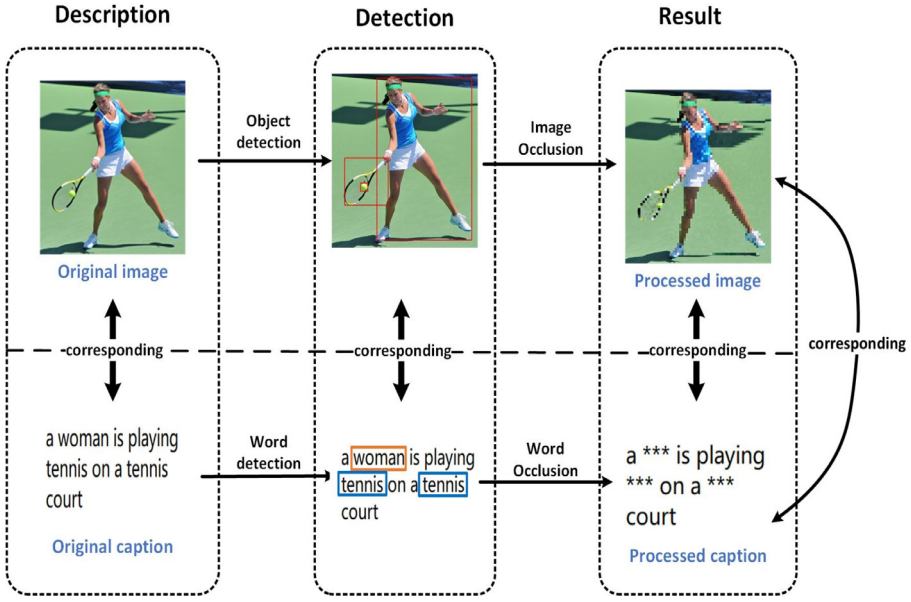


Fig. 1. The example of using occlusion method to deal with the image and the text description. We hope that the detection module's detection accuracy for objects in the processed data is reduced. The final effect is that the character and correlated objects are occluded, and the corresponding caption is also occluded.

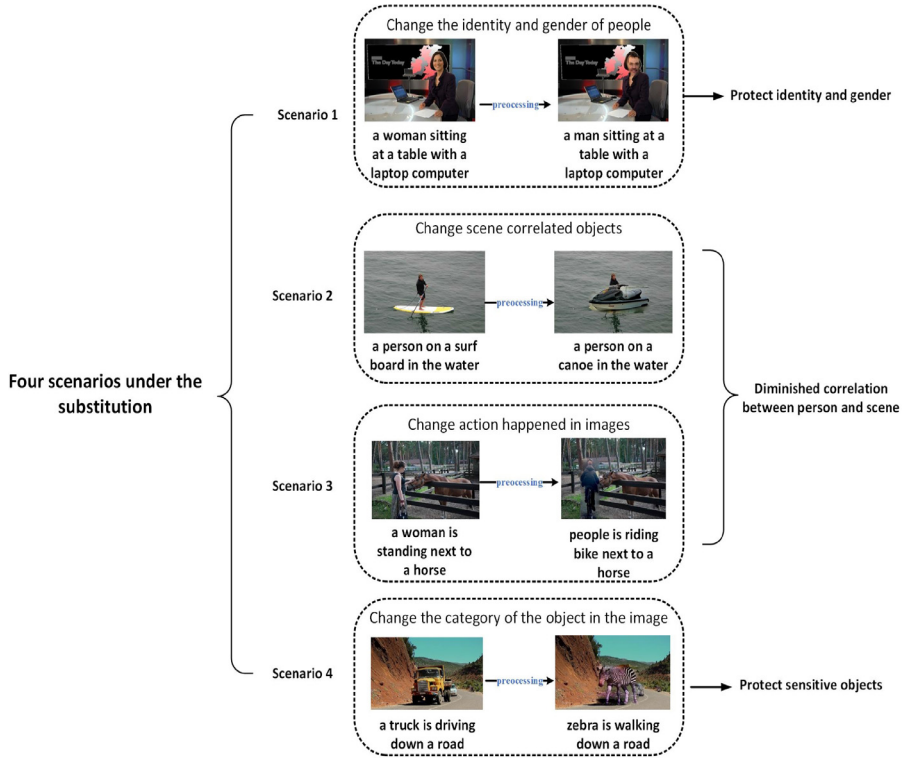


Fig. 2. Substitution examples.

Table 1
Objects and related words.

Object (O)	Word (W)
person	{" man", " woman", "people", " men", " women", "boy", "girl"}
car	{"car"}
motorcycle	{"motorcycle", "riding"}
airplane	{"airplane"}
bus	{"bus", "driving"}
train	{"train"}
truck	{"truck", "parked", "driving"}
parking meter	{"parking meter"}
skis	{"skis", "snow", "slope"}
snowboard	{"snowboard", "snow", "slope"}
sports ball	{"ball", "playing", "soccer"}
kite	{"kite", "flying"}
baseball bat	{"baseball bat", "baseball"}
baseball glove	{"baseball glove", "baseball","glove"}
skateboard	{"skateboard", "skate", "board"}
surfboard	{"surfing", "surfboard"}
tennis racket	{"tennis racket", "tennis", "racquet"}
cell phone	{"cell phone"}
frisbee	{"white frisbee", "frisbee"}

tion task has two parts. One part of the detection task is word detection. The other part is object detection. First of all, we select a set of objects O and a set of words W. The objects in set O are selected by referring to the General Data Protection Regulation (GDPR) Regulation (2016) which is a series of data management rules. And these objects are what we want to protect related to privacy. Each word in set W is associated with the object in set O or can help locate the scene. For example, we want to protect objects like people, and the related words are woman, man, boy, girl and so on. The specific settings of O and W are shown in Table 1.

For object detection, we set a tuple P_O where $P_O = \{o_1, o_m\}$ with each $o_i \in O$. As to word detection, we also set a tuple P_W where $P_W = \{w_1, w_n\}$ with each $w_i \in W$. The specific settings of P_O and P_W for different methods and scenarios are described in tuple setting section.

Through the process of images and descriptions in this task, we can get the detected images I' and detected descriptions D'. The detection methods and the setting of related tuples will be described in detail below.

3.3.1. Tuple setting

For the occlusion method, we set $P_O = O$ and $P_W = W$, the object set O and the word set W are shown in Table 1.

For the first scenario S_1 in substitution method, we set P_O = {person} and the set of words P_W = {"woman", "man"}.

In the second scenario S_2, we set P_O = {frisbee, skis, snowboard, sports ball, baseball bat, baseball glove, skateboard, surfboard, tennis racket, kite} and the words in P_W are the corresponding words to the objects in tuple P_O that refer to Table 1.

For the third scenario S_3 in substitution method, we set P_O = {person} and a set of words P_W = {"in", "on", "next", "down", "at"}, we need to find these prepositions, and substitute the words before these prepositions in word processing.

In the last situation S_4 in substitution method, we set $P_O = O$ and a set of words P_W = {"in", "on", "next", "down", "at"}.

3.3.2. Object detection

According to the object tuple P_O we have set, we need to locate these objects in images. We use the object detection in technology Mask R-CNN He et al. (2017), which can realize classification, object detection and instance segmentation, to get the four coordinates of the target object bounding box. Especially, in the first scenario S_1 for the replacement method, we need to protect facial information. So, we also need to get the position of a person face. For these methods, the number of words corresponding to each object is a lot. Therefore, considering the efficiency of subsequent word detection, we need to record the label of the detected object as a tuple $P_{Ii} = \{o_1, o_n\}$ with each $o_i \in$ tuple P_O for each image.

Table 2
The replacement words for objects.

Object (O)	Word (W)
skis, snowboard	{"snowmobile", "bobsled"}
baseball bat	{"rugbyball", "volleyball",
baseball glove	"basketball"}
tennis racket	
sports ball	{"rugbyball", "barrow", "bucket"}
kite	{"balloon", "parachute"}
skateboard	{"unicycle", "bicycle"}
surfboard	{"canoe", "catamaran"}
frisbee	{"rugbyball", "volleyball", "basketball", "soccer"}

3.3.3. Word detection

After the process of object detection, we can get some tuples like P_{Ii} which represents the sensitive objects in image I_i. According to the word tuple P_W we set before, check whether the words in the tuple P_W exist in the descriptions of images. If words exist, find the location of them. It is easy to implement with the function *find* () in Python, which can return the index of the first occurrence of the substring in the total string if the substring exists in the string.

3.4. Word and image privacy preserving

After detecting the targets in images and descriptions, we hope to realize the privacy preservation. To achieve our goal, we would like to further process the descriptions and images obtained in the second task. The process is divided into word processing and image processing.

3.4.1. Word processing

We have two ways to deal with the descriptions. One is using "***" to indicate protected words that have been detected, which make an effort to block target words. The function *replace* () in Python can help us implement the target and get a new string. After judging the word to be protected in the description according to the detection task, we use "***" to replace the words. This way can satisfy the privacy preservation of captions to some extent, but it also breaks the structure of the sentence.

The other way is using another word to substitute for the protected word. For different privacy preservation in four scenarios which are described above, we set four different tuples T_{S1}, T_{S2}, T_{S3}, T_{S4} to replace the original words in text descriptions. And original words are correlated to some sensitive information.

For the first scenario, we set T_{S1} = {"woman", "man"}. In the second situation, consider the types of objects suitable for different scenes, we set different words for different objects, T_{S2} is shown in Table 2. We also set T_{S3} = {"people is sitting", "people is eating", "people is playing skateboard", "people is playing ball", "people is riding horse", "people is playing frisbee", "people is surfing", "people is riding motorcycle", "people is riding bike", "people is skiing"} and T_{S4} = {"cat is lying", "dog is running", "horse is standing", "sheep is standing", "cow is standing", "elephant is standing", "bear is standing", "zebra is standing", "giraffe is standing"}. After setting these tuples, we use random substitution to randomly select a word from T_{Si}. The replacement method is the same as the first way.

Some sensitive attributes are binary variables, such as gender. Therefore, in the second method of word replacement, we hope that the replacement result of binary variables can meet randomized response, and randomized response is a basic LDP Bebensee (2019) mechanism. We use a tool ldp (0000) to realize the randomized response in the first scenario, to disturb the gender ratio and preserve the gender. For example, "woman" and "man" are two words related to the gender attribute, and we hope that the program has 75% probability to respond with the original word, and 25% probability to respond with the opposing word.

Through the process of descriptions in this part, we can get final descriptions D'.

3.4.2. Image privacy preserving

In the part of image processing, we have two methods to deal with the privacy preservation of images.

The first method is using mosaic technology to protect the detected sensitive object. This method corresponds to the first method in word processing. The mosaic can protect people's identity to some extent.

The other one is using Poisson Blending Pérez et al. (2003) to realize the corresponding protection in images and descriptions. According to the four word tuples T_{S1}, T_{S2}, T_{S3}, T_{S4} in word processing parts, we select four image sets T_{I1}, T_{I2}, T_{I3}, T_{I4} and these images are picture form of the word description in the four word tuples T_{S1}, T_{S2}, T_{S3}, T_{S4}. Before the image fusion, we need to get the mask of the fusion area in image sets T_{I1}, T_{I2}, T_{I3}, T_{I4}. In the object detection section, we have got the four coordinates of the target object bounding box. These four coordinates can help us to determine the center of the replaced object, and use them to determine the size of mask, replacement image and replacement range. We also use random substitution and the random rules are consistent with rules in word processing. For the first situation, the sensitive information we selected was the gender of the characters. In addition to using LDP to disturb the gender ratio, we also use Kazemi and Sullivan (2014) to transform the facial features of the characters, thus blurring their facial features. In order to improve the substitute effect, we use Mask R-CNN He et al. (2017) to get masks of objects and use image inpainting method Yu et al. (2018a,b) to eliminate detected objects.

Then, we can get the final images I'' after a series of processing.

4. Utility and privacy analysis

This section is to verify the usability of the processed images and the effect of protecting sensitive information in images. For different methods and scenarios, we use different verification methods to analyse utility and privacy preservation. Consistency evaluation methods between different data forms are also included in the utility analysis.

4.1. Utility analysis

We use object detection technology in images to realize image utility analysis. We also need to evaluate the consistency of images and text descriptions after processing. According to the four privacy protection scenarios mentioned above, we formulate different evaluation criteria. Let N_{image} be the total number of tested pictures in the current scenario.

In the first scenario S_1 of substitution method, we use the detectability rate R_{d_face} of face and scene similarity rate R_{scene} to verify the usability of the resulting images I'. The face detectability rate R_{d_face} is for characters, and the scene similarity rate R_{scene} is for the scene category which is the non-personal attribute. And the consistency rate was marked as R_{c_gender} to verify the consistency between the gender description contained in the text and the gender of the person in the processed picture. The more similar the scene contained in the image before and after processing, the higher the detectability rate of faces and the consistency rate, the better the image usability. In scenario S_1, the face detectability rate, scene similarity rate and gender consistency rate are defined as:

$$\mathcal{R}_{d\_face} = \frac{\mathcal{C}_{face}}{\mathcal{N}_{image}} \tag{1}$$

$$\mathcal{R}_{scene} = \frac{\mathcal{C}_{scene}}{\mathcal{N}_{image}} \tag{2}$$

$$\mathcal{R}_{c\_gender} = \frac{\mathcal{C}_{same\_gender}}{\mathcal{N}_{image}} \tag{3}$$

The meaning of the parameters in the equation is as follows. We use Arriaga et al. (2017) for face detection, then, we use the face detection model C_{face} to count the number of images that can be successfully detected for face. And let C_{scene} be the number of image pairs that the top 1 scene recognized from the original and processed image is the same. We use a scene classifier Zhou et al. (2017) to achieve scene recognition. For the consistency rate, we use C_{same_gender} to count the number of the processed image and annotation pairs, and deepface Serengil and Ozpinar (2020) is used to realize the gender classification. In these pairs, the gender identified in the image is the same as that contained in the annotation.

For the second scenario S_2 in substitution method, we use scene similarity rate R_{scene} that described in scenario S_1 and the detectability rate of person R_{d_person} to verify the usability of the result I'. And the consistency rate was marked as R_{c_tool} to verify the consistency between the objects contained in the text and those contained in the processed picture. The higher these rates, the better the image availability. We use Mask R-CNN He et al. (2017) and C_{person} to count the number of images that can be successfully detected for a person. Source code of Mask R-CNN built on FPN and ResNet101. And we use a model pre-trained on MS COCO to run object detection on arbitrary images. For the consistency rate, we use C_{same_tool} to count the number of the processed image and annotation pairs. In these pairs, the object described in text is contained in the top 5 object detection results of the image. A transformer object detection tool Chefer et al. (2020) is used for object classification. Then, the person detectability and object consistency are defined as:

$$\mathcal{R}_{d\_person} = \frac{\mathcal{C}_{person}}{\mathcal{N}_{image}} \tag{4}$$

$$\mathcal{R}_{c\_tool} = \frac{\mathcal{C}_{same\_tool}}{\mathcal{N}_{image}} \tag{5}$$

For the third scenario S_3 in substitution method, we also use scene similarity rate R_{scene} and the detectability rate of person R_{d_person} to verify the usability of the result I'. And the consistency rate was marked as R_{c_event} to verify the consistency between the objects contained in the text and those contained in the processed picture. For example, if the text describes a person playing tennis, the picture will contain some related objects, such as a person or a tennis ball or a tennis racket. The higher these rates, the better the image availability. For the consistency rate, we use C_{same_event} to count the number of the processed image and annotation pairs. In these pairs, we can detect objects related to an action from the image, and the action is described in the annotation. Mask R-CNN He et al. (2017) is used for object detection. The consistency rate in this scenario is defined as:

$$\mathcal{R}_{c\_event} = \frac{\mathcal{C}_{same\_event}}{\mathcal{N}_{image}} \tag{6}$$

For the last scenario S_4 in substitution method, we use scene similarity rate R_{scene} and object detectability rate R_{d_object} to verify the usability of images I'. And the consistency rate was marked as R_{c_object} to verify the consistency between the object category contained in the text and the object category in the processed image. The higher these rates, the better the usability. We use C_{object} to count the number of images that can be successfully detected for animals. For the consistency rate, we use C_{same_object} to count the number of the processed image and annotation pairs. In these pairs, the animal object recognized in the image is the same as that contained in the annotation. In scenario S_4, the detectability rate and consistency rate are defined as:

$$\mathcal{R}_{d\_object} = \frac{\mathcal{C}_{object}}{\mathcal{N}_{image}} \tag{7}$$

$$\mathcal{R}_{c\_object} = \frac{\mathcal{C}_{same\_object}}{\mathcal{N}_{image}} \tag{8}$$

And we use scene similarity rate R_{scene} for the evaluation metric of occlusion method about images utility.

4.2. Privacy analysis

In this section, we use privacy metrics to measure privacy protection effectiveness. For the four scenarios of the substitution method, we have two methods of measurement. Let N be the total number of tested pictures.

In the first scenario S_1, when the overall gender ratio contained in the image data is disturbed, and the changed gender ratio is close to the ratio of the random response set by our method, it is considered to have achieved a certain privacy protection effect. We will also test the dissimilarity rate R_{face} of faces before and after processing. The lower the similarity, the better the protection effect. We use C_{face} to count the number of image pairs that the distance of face in image pairs is less than a threshold. The R_{face} is defined as:

$$\mathcal{R}_{face} = 1 - \frac{\mathcal{C}_{face}}{\mathcal{N}} \tag{9}$$

For the scenario S_3, S_4, and occlusion method, we use the dissimilarity rate R_{mse} and R_{ssim} of images to verify the effect of image privacy protection. The higher the dissimilarity, the better the privacy protection effect. During the test processing, we will use two indicators which are MSE and SSIM. The Mean Squared Error (MSE) is a value, and when it is smaller, the images are more similar. And the value is 0 when two images are exactly the same. So, we hope the larger the value of the two images, the better. The Structural Similarity (SSIM) Wang et al. (2004), when the greater the value, the less image distortion. The closer to 1, the more similar the pictures are. We use C_{mse} to count the number of image pairs that the MSE value of face in image pairs is less than a threshold. And we use C_{ssim} to count the number of image pairs that the SSIM value of face in image pairs is less than a threshold. The R_{mse} and R_{ssim} are defined as:

$$\mathcal{R}_{mse} = 1 - \frac{\mathcal{C}_{mse}}{\mathcal{N}} \tag{10}$$

$$\mathcal{R}_{ssim} = \frac{\mathcal{C}_{ssim}}{\mathcal{N}} \tag{11}$$

For the scenario S_2, S_4, and occlusion method, we also use the undetectability rate R_{ud} of original sensitive objects in images to verify the effect of image privacy protection. The higher the undetectability rate, the better the privacy protection effect. We use C_{before_object} to count the number of sensitive objects in original images and use C_{after_object} to count the number of sensitive objects in processed images. And Mask R-CNN He et al. (2017) is used for object detection. The R_{ud} is defined as:

$$\mathcal{R}_{ud} = 1 - \frac{\mathcal{C}_{after\_object}}{\mathcal{C}_{before\_object}} \tag{12}$$

5. Experiment results and analysis

We use a series of experiments to evaluate our methods. First, we will introduce the experimental settings, including the preparation for image data groups with corresponding descriptions and

Fig. 3. Some examples of original images and texts, and the corresponding processed images and texts.

the data used to substitute. Then, we will discuss the experimental result of utility and privacy preservation in different methods and different situations. At the same time, we will also verify the consistency of the image content and the corresponding text content after the method processing.

5.1. Experiment setting

In this paper, for the privacy preservation of images and corresponding text descriptions, we proposed two main methods, which are occlusion and substitution. And for the substitution method, we have four scenarios. So, we set four groups of experiments, and each set of experiments will correspond to the different methods or situations we proposed, named E_1, E_2, E_3, E_4, E_5. Each experiment is described as follows:

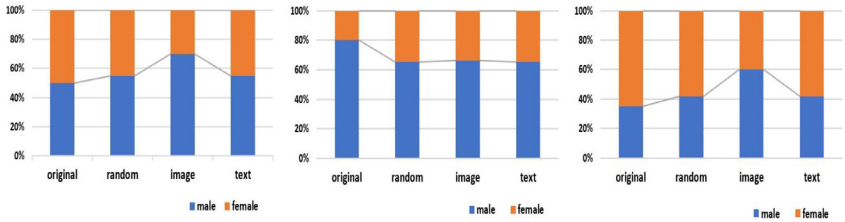
- E_1: This set of experiments is aimed at the substitution method and the first scenario. And we use the substitution method to protect face identity and gender, and the corresponding text is processed with the same method.
- E_2: This set of experiments is aimed at the substitution method and the second scenario, that is, substitute the object we have set, and the corresponding text is substituted by selected words.
- E_3: This experiment corresponds to the substitution method and the third scene. The substitution method is used to protect the characters' actions, and the corresponding text is processed by the substitution method too.
- E_4: For the substitution method and the fourth scene, the substitution method is used to protect the real classification of objects in the picture, and the corresponding text.
- E_5: This experiment corresponds to the occlusion method, the image is protected by occlusion method, and the corresponding text is processed by occlusion method.

5.2. Dataset

5.2.1. Test images and captions

We set different groups of images to evaluate the different methods in different situations. All test images are chosen from the real-world dataset COCO Lin et al. (2014), and each image contains a certain background. And each group's data contains 100 images:

(1) The first set of pictures is used to evaluate in the first experiment E_1. Each image contains a single person, and the gender and the face of the human in the picture can be detected. Three groups of pictures containing different ratios of male and female were set. The ratio of male and female was 1:1, 4:1 and 7:13 respectively.



(a) group1. (b) group2. (c) group3.

Fig. 4. Gender ratio.

Table 3
Proportion of males.

	Original(%)	Random (%)	Image (%)	Text (%)	Image inferred (%)	Text inferred (%)
group1	50	55	70	55	90	60
group2	80	65	66	65	82	80
group3	35	42	60	42	70	34

(2) The second set of images are used to evaluate in the second experiment E_2. Each image contains a person with correlated sports objects, and these objects can be detected.
(3) The third set of images are used to evaluate in the third experiment E_3. Each image contains a single human with an action in progress, and the whole people in the image can be detected. People in these images are doing something, like playing tennis ball, eating food, surfing, riding and so on.
(4) The fourth group is used to evaluate in experiment E_4 and occlusion experiment E_5, and the image can contain one or more people, or not have people just have some objects related to sensitive information.

We use Neuraltalk Karpathy and Fei-Fei (2015) to get the corresponding description of an image. After getting a set of descriptions, we select some images and corresponding descriptions to simulate the mixture of information from real life.

5.2.2. Data to replace

Since the substitution method needs to use data for replacement, we also need to select the corresponding replacement data for different experiments. And these data for replacement are taken as image set T_{I1}, T_{I2}, T_{I3} and T_{I4}. The description of each image set is shown below:

T_{I1}: Because experiment E_1 needs to protect human face identity and gender, we select 100 female faces and 100 male faces from a fake face dataset, and these fake face images are all generated by StyleGAN Karras et al. (2019). These fake faces will be randomly selected to replace the facial features. In addition, according to the word tuple T_{S1} set in word processing, five male and five female fake face images are selected, face masks are obtained by an object contour marking tool VIA Dutta et al. (2016); Dutta and Zisserman (2019). These face images and corresponding masks are taken as the image collection T_{I1} of gender conversion.
T_{I2}: For experiment E_2, pictures containing different objects are selected according to the word tuple T_{S2} set in word processing, and get masks of objects in these images, and these pictures and masks make up the image set.
T_{I3}: For experiment E_3, 10 pictures containing different actions are selected according to the word tuple T_{S3} set in word processing, and get the masks of the person with action area in these images, and these pictures and masks are taken as image set T_{I3}.

Table 4
Some rate results in experiment E_1.

	Dissimilarity	Scene similarity	Consistency
group1	0.69	0.94	0.85
group2	0.70	0.91	0.99
group3	0.69	0.93	0.82

T_{I4}: For experiment E_4, 10 pictures containing different animals are selected according to the word tuple T_{S4} set in word processing, and get the masks of animals in these images, and these pictures and masks are taken as image set T_{I4}.

5.3. Experiment results and discussion

For five sets of experiments, Fig. 3 shows some original images and texts with corresponding processed images and texts. Each group shows the original and processed image with corresponding annotations. The first row shows the example of experiment E_1, we changed the gender both in images and texts. The second row demonstrates some results of experiment E_2, we changed some sports tools, such as changing skis to a bobsled and a skateboard to a unicycle. The third row demonstrates some results of experiment E_3, we changed characters and events, like changing "playing with a frisbee" to "person is riding bike" and changing "throwing a ball" to "playing frisbee". In the fourth row, we show some results that we used animals to substitute sensitive objects in experiment E_4. The last row displays some occlusion results in experiment E_5.

5.3.1. Experiment E_1

We measure the overall gender ratio contained in three image groups. Fig. 4(a)-(c) show the results in terms of the gender ratio. Each figure contains the original gender ratio, the random response gender ratio, the image gender ratio after substitution processed, and the gender ratio in the processed text descriptions. We hope the gender ratio in processed images and processed texts are different from the original images. From the broken lines and columnar proportions in result figures, we can find that there are differences between these proportions. And these differences show our method disturbed the gender ratio in the processed images and texts, and achieves the effect of privacy preservation.

The exact proportions of males are shown in Table 3, which contains the original proportions, random response proportions, processed images proportions, processed texts proportions, inferred proportions from processed images, and inferred proportions from processed images of males.

Table 5
Some quantitative analysis results of experiment E_2, E_3, E_4, E_5.

	Detectability	Scene similarity	Consistency	Undetectability	Dissimilarity (MSE|SSIM)
E_2	0.99	0.73	0.68	0.9	None
E_3	0.92	0.59	0.36	None	0.62|0.75
E_4	0.87	0.35	0.63	0.66	0.55|0.32
E_5	None	0.45	None	0.76	0.18|0.24

We use a random response mechanism, so, the gender ratio in processed images and texts can be used to get the original gender ratio. In our experiment, because of the errors in gender detection module and processed images, there is a certain error between the original gender ratio inferred from the processed pictures and the real gender ratio. But the gender ratio inferred from the processed texts has a great effect to close to the real gender ratio, according to ratio results from Table 3. And we examined the detectability rate R_{d_face} of face in this experiment. We set three groups of images, and the detectability rates are all 100%. And the face and gender detection module has some errors in itself. These results show us that the processed images have great utility.

We also detect the dissimilarity rate R_{face} of face in before and after processed images. We use Facenet Schroff et al. (2015), and set the threshold as 0.9. When the distance of two faces larger than the threshold, we think the two faces are dissimilar. The rates of dissimilarity in three groups are 0.69, 0.70, 0.69.

Then, we detect scene similarity rates R_{scene} in three groups that are 0.94, 0.91, 0.93. Lastly, we detect the consistency rate R_{c_gender} between the gender description contained in the text and the gender of the person in the processed picture. The exact rates in three image groups are 0.85, 0.99, 0.82, which show great effect in consistency. The dissimilarity rate, scene similarity rate and consistency results of the three groups are summarized in Table 4.

5.3.2. Experiment E_2

In this experiment, we measure the detection rate of people, and the person detection rate R_{d_person} is 0.99. Then we measure the similarity of scenes detected from the before and after processed images, the rate R_{scene} is 0.73.

To evaluate the effect in privacy preservation, we measure the undetectability rate R_{ud} of original sensitive objects in images, which is 0.90. This result shows the great effect of our method in privacy preservation.

Finally, we detect the consistency rate R_{c_tool} between processed images and processed descriptions. Because the detection module has some errors, the rate is only 0.68. What's more, some target objects in processed images are too small, that the detection module can not detect the object exactly.

5.3.3. Experiment E_3

In this experiment, we first measure the detection rate of people, and the person detection rate R_{d_person} is 0.92. Then we measure the similarity of scenes detected from the before and after processed images, the rate R_{scene} is 0.59.

To evaluate the effect of privacy preservation, we measure the MSE value. We set the threshold as 1000, and when the value is larger than that, we think two images are dissimilar. And the rate of dissimilarity R_{mse} is 0.62. At the same time, we also evaluate the SSIM value. We set the threshold as 0.7, when the value is lower than it, we think two images are dissimilar. And the rate of dissimilarity R_{ssim} is 0.75. Considering that some images contain a large proportion of background, we choose these two thresholds. These rates show the effect of our method in privacy preservation.

Finally, we detect the consistency rate R_{c_event} between processed images and processed descriptions. The rate is 0.36, the effect is not as good as the effect of experiment E_2.

5.3.4. Experiment E_4

For the fourth experiment, we measure the detection rate R_{d_object} of objects. These objects contain cat, dog, horse, sheep, cow, elephant, bear, zebra and giraffe. The detection rate is 0.87, which shows that the processed images still have some utility. And the scene similarity rates R_{scene} is 0.35.

Then, we also measure the result in privacy preservation. We measure two indicators MSE and SSIM, and the thresholds are the same as the thresholds in experiment E_3. According to the MSE value, the dissimilar rate R_{mse} is 0.55. To the SSIM value, the dissimilar rate R_{ssim} is 0.32. And the undetectability rate R_{ud} is 0.66. Finally, we measure the consistency rate R_{c_object}, and the rate is 0.63.

5.3.5. Experiment E_5

This experiment is aimed at the evaluation of occlusion method. In order to verify the utility, we measure the scene similarity rate R_{scene} which is 0.45.

We still measure the dissimilarity of images referring to the two indicators in experiment E_3. The rates R_{mse} and R_{ssim} are 0.18 and 0.24. Compared to the experiment E_3 and E_4, the result shows that the substitution method in the effect of privacy preservation is better than the occlusion method. We also measure the undetectability rate R_{ud} which is 0.76.

5.3.6. Analysis

The rates of detectability, scene similarity, consistency, undetectability and dissimilarity of experiment E_2, E_3, E_4, E_5 are summarized in the Table 5. For performance, we simply test it under a GPU, and the time for objective detection and instance segmentation for each image is about 0.8 seconds. The average time for image processing and word processing by using a single CPU for 100 pieces of data is 5.64 seconds and 0.05 seconds, respectively. Comparing these experiments, we can find that in scenario S_2 only replacing the objects related to the character's behavior and scene can better balance the effects of image availability and privacy protection. For the experiment E_3, E_4, the usability of the picture will decrease with the increase of the type and area of the replacement items. In addition, in the experiment E_3, E_4, some alternate actions or animals are not very suitable to appear in the background contained in the original picture, and scenario S_2 can better solve this shortcoming.

6. Conclusion

In this work, we proposed methods for privacy preservation for multiple sources information. We not only preserve the privacy of diverse forms data, but also aim to maintain the connection between them. We mainly use occlusion and substitution technologies to implement privacy protection. And we use corresponding occlusion and replacement processing for images and descriptions to maintain the correlation between them. Through various experiments, the result shows that the replacement method maintains the structure of the sentence better than the occlusion method for word processing. In different scenarios and methods, we can find that the processed data can maintain a certain amount of usability and some level of privacy protection. And the substitution method

in the effect of privacy preservation is better than the occlusion method. Although the effect of maintaining consistency between data varies in different scenarios, our method has shown a better effect on data consistency in the gender and identity protection scenarios. And replacing the objects related to the character's behavior and scene can better balance the effects of image availability and privacy protection.

CRediT authorship contribution statement

Chenguang Wang: Conceptualization, Methodology, Writing. **Ping Xiong:** Experiment, Evaluation, Writing-Original draft preparation. **Wei Ren:** Problem definition, Investigation. **Tianqing Zhu:** Methodology, Problem definition, Supervision. **Kim-Kwang Raymond Choo:** Writing, Reviewing and Editing, Solutions.

Declaration of Competing Interest

To represent all authors, I would like to claim the conflict of interests as follows:

1. China university of Geosciences, Wuhan, China.
2. University of Texas at San Antonio (UTSA).
3. Zhongnan University of Economy and Law.

Acknowledgement

The research was financially supported by National Natural Science Foundation of China (No.61972366), the Foundation of Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences (No. KFKT2019-003), the Foundation of Guangxi Key Laboratory of Cryptography and Information Security (No. GCIS201913), and the Foundation of Guizhou Provincial Key Laboratory of Public Big Data (No. 2018BDKFJJ009, No. 2019BDKFJJ003, No. 2019BDKFJJ011). K.-K. R. Choo was supported only by the Cloud Technology Endowed Professorship.

References

Aghasian, E., Garg, S., Gao, L., Yu, S., Montgomery, J., 2017. Scoring users' privacy disclosure across multiple online social networks. IEEE Access 5, 13118–13130.
Arriaga, O., Valdenegro-Toro, M., Plöger, P., 2017. Real-time convolutional neural networks for emotion and gender classification. arXiv preprint arXiv:1710.07557.
Bebensee, B., 2019. Local differential privacy: a tutorial. arXiv preprint arXiv:1907.11908.
Biswas, C., Ganguly, D., Roy, D., Bhattacharya, U., 2019. Privacy preserving approximate k-means clustering. In: Proceedings of the 28th ACM International Conference on Information and Knowledge Management, pp. 1321–1330.
Chefer, H., Gur, S., Wolf, L., 2020. Transformer interpretability beyond attention visualization. arXiv preprint arXiv:2012.09838.
Chen, Z., Zhu, T., Xiong, P., Wang, C., Ren, W., 2021. Privacy preservation for image data: a gan-based method. Int. J. Intell. Syst. (1).
Cho, D., Lee, J.H., Suh, I.H., 2020. Cleanir: controllable attribute-preserving natural identity remover. Applied Sciences 10 (3), 1120.
Croft, W.L., Sack, J.-R., Shi, W., 2019. Differentially private obfuscation of facial images. In: International Cross-Domain Conference for Machine Learning and Knowledge Extraction. Springer, pp. 229–249.
Dutta, A., Gupta, A., Zissermann, A., 2016. VGG image annotator (VIA). http://www.robots.ox.ac.uk/~vgg/software/via/. Version: 2.0.10.
Dutta, A., Zisserman, A., 2019. The VIA annotation software for images, audio and video. In: Proceedings of the 27th ACM International Conference on Multimedia. ACM, New York, NY, USA doi:10.1145/3343031.3350535.
Feng, Q., He, D., Liu, Z., Wang, H., Choo, K.-K.R., 2020. Securenlp: a system for multi--party privacy-preserving natural language processing. IEEE Trans. Inf. Forensics Secur..
Fernandes, N., Dras, M., McIver, A., 2018. Processing text for privacy: an information flow perspective. In: International Symposium on Formal Methods. Springer, pp. 3–21.
Feyisetan, O., Diethe, T., Drake, T., 2019. Leveraging hierarchical representations for preserving privacy and utility in text. In: 2019 IEEE International Conference on Data Mining (ICDM). IEEE, pp. 210–219.
Foufi, V., Gaudet-Blavignac, C., Chevrier, R., Lovis, C., 2017. De-identification of medical narrative data. The practice of patient centered cure 23–27.
He, K., Gkioxari, G., Dollár, P., Girshick, R., 2017. Mask r-cnn. In: Proceedings of the IEEE international conference on computer vision, pp. 2961–2969.
Karpathy, A., Fei-Fei, L., 2015. Deep visual-semantic alignments for generating image descriptions. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 3128–3137.
Karras, T., Laine, S., Aila, T., 2019. A style-based generator architecture for generative adversarial networks. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 4401–4410.
Kazemi, V., Sullivan, J., 2014. One millisecond face alignment with an ensemble of regression trees. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 1867–1874.
local differential privacy library, https://github.com/forestneo/sunDP.
Li, X.-B., Qin, J., 2017. Anonymizing and sharing medical text records. Information Systems Research 28 (2), 332–352.
Lin, T.-Y., Maire, M., Belongie, S., Hays, J., Perona, P., Ramanan, D., Dollár, P., Zitnick, C.L., 2014. Microsoft coco: Common objects in context. In: European conference on computer vision. Springer, pp. 740–755.
Lyu, L., Li, Y., He, X., Xiao, T., 2020. Towards differentially private text representations. In: Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval, pp. 1813–1816.
Nousi, P., Papadopoulos, S., Tefas, A., Pitas, I., 2020. Deep autoencoders for attribute preserving face de-identification. Signal Process. Image Commun. 81, 115699.
Patsakis, C., Zigomitros, A., Papageorgiou, A., Galván-López, E., 2014. Distributing privacy policies over multimedia content across multiple online social networks. Comput. Networks 75, 531–543.
Pérez, P., Gangnet, M., Blake, A., 2003. Poisson Image Editing. In: ACM SIGGRAPH 2003 Papers, pp. 313–318.
Regulation, G.D.P., 2016. Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46. Official Journal of the European Union (OJ) 59 (1–88), 294.
Ribaric, S., Ariyaeeinia, A., Pavesic, N., 2016. De-identification for privacy protection in multimedia content: a survey. Signal Process. Image Commun. 47, 131–151.
Schroff, F., Kalenichenko, D., Philbin, J., 2015. Facenet: A unified embedding for face recognition and clustering. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 815–823.
Serengil, S.I., Ozpinar, A., 2020. Lightface: A hybrid deep face recognition framework. In: 2020 Innovations in Intelligent Systems and Applications Conference (ASYU). IEEE, pp. 23–27. doi:10.1109/ASYU50717.2020.9259802.
Shen, M., Cheng, G., Zhu, L., Du, X., Hu, J., 2020. Content-based multi-source encrypted image retrieval in clouds with privacy preservation. Future Generation Computer Systems 109, 621–632.
Terhörst, P., Damer, N., Kirchbuchner, F., Kuijper, A., 2019. Unsupervised privacy-enhancement of face representations using similarity-sensitive noise transformations. Applied Intelligence 49 (8), 3043–3060.
Usman, M., Jan, M.A., Puthal, D., 2019. Paal: a framework based on authentication, aggregation, and local differential privacy for internet of multimedia things. IEEE Internet Things J. 7 (4), 2501–2508.
Wang, T., Zheng, Z., Rehmani, M.H., Yao, S., Huo, Z., 2018. Privacy preservation in big data from the communication perspective-a survey. IEEE Communications Surveys & Tutorials 21 (1), 753–778.
Wang, Z., Bovik, A.C., Sheikh, H.R., Simoncelli, E.P., 2004. Image quality assessment: from error visibility to structural similarity. IEEE Trans. Image Process. 13 (4), 600–612.
Yu, J., Lin, Z., Yang, J., Shen, X., Lu, X., Huang, T.S., 2018. Free-form image inpainting with gated convolution. arXiv preprint arXiv:1806.03589.
Yu, J., Lin, Z., Yang, J., Shen, X., Lu, X., Huang, T.S., 2018. Generative image inpainting with contextual attention. arXiv preprint arXiv:1801.07892.
Zhou, B., Lapedriza, A., Khosla, A., Oliva, A., Torralba, A., 2017. Places: a 10 million image database for scene recognition. IEEE Trans Pattern Anal Mach Intell.
Zhu, T., Ye, D., Wang, W., Zhou, W., Yu, P., 2020. More than privacy: applying differential privacy in key areas of artificial intelligence. IEEE Trans Knowl Data Eng 0 (0). doi:10.1109/TKDE.2020.3014246. 1–1

Chenguang Wang is currently an undergraduate student at China University of Geosciences, Wuhan, China. Her research interests include privacy preserving, AI security and privacy, and network security.

Zhu Tianqing received her B.Eng. degree and her M.Eng. degree from Wuhan University, China, in 2000 and 2004, respectively. She also holds a PhD in computer science from Deakin University, Australia (2014). She is currently a professor at China University of Geosciences, Wuhan, China. Her research interests include privacy preserving, AI security and privacy, and network security.

Ping Xiong received his BEng degree from LanZhou Jiaotong University, China in 1997. He received his MEng and PhD degrees from Wuhan University, China, in 2002 and 2005, respectively. He is currently the professor of School of Information and Safety Engineering, Zhongnan University of Economics and Law, China. His research interests are network security, data mining and privacy preservation.

Wei Ren is currently a Professor at the School of Computer Science, China University of Geosciences (Wuhan), China. He was with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, USA in 2007 and 2008, the School of Computer Science, University of Nevada Las Vegas, USA in 2006 and 2007, and the Department of Computer Science, The Hong Kong University of Science and Technology, in 2004 and 2005. He obtained his Ph.D. degree in Computer Science

from Huazhong University of Science and Technology, China. He has published more than 70 refereed papers, 1 monograph, and 4 textbooks. He has obtained 10 patents and 5 innovation awards. He is a senior member of the China Computer Federation and a member of IEEE.

Kim-Kwang Raymond Choo received his Ph.D. in Information Security in 2006 from the Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). In 2015, he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He is the recipient of the 2019 IEEE Technical Committee on Scalable Computing Award for Excellence in Scalable Computing (Middle Career Researcher), the 2021 UTSA Carlos Alvarez College of Business Endowed 1969 Commemorative Award for Overall Faculty Excellence and the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, the British Computer Society's 2019 Wilkes Award Runner-up, the Fulbright Scholarship in 2009, the 2008 Australia Day Achievement Medallion, and the British Computer Society's Wilkes Award in 2008. He has also received best paper awards from IEEE Systems Journal in 2021, IEEE Conference on Dependable and Secure Computing (DSC 2021), IEEE Consumer Electronics Magazine for 2020, Journal of Network and Computer Applications for 2020, EURASIP Journal on Wireless Communications and Networking in 2019, IEEE TrustCom 2018, and ESORICS 2015; the IEEE Blockchain 2019 Outstanding Paper Award; and Best Student Paper Awards from Inscrypt 2019 and ACISP 2005.