IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 14, No. 1, February, 2024, pp. 297-308
Journal homepage: http://iieta.org/journals/ijsse

Privacy-Preserving Photo Sharing on Online Social Networks: A Review

M.D. Sajid*, S. Kavitha

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur 522302, India

Corresponding Author Email: sajid24x7@gmail.com

https://doi.org/10.18280/ijsse.140129

Received: 15 October 2023
Revised: 15 February 2024
Accepted: 21 February 2024
Available online: 29 February 2024

Keywords:
privacy-preserving photo sharing, online social networks, social leaks, image tags, privacy settings, and access control

ABSTRACT

Online social networking applications and their services have become an essential part of the human lifestyle. These social services help online users in different ways, such as through social visibility, content sharing, communication, promotions, etc. In the same way, the services of online social networks (OSNs) pose privacy risks for their users. The service of photo sharing in OSNs, in particular, causes leakage of online social users' personal information. It's critical to comprehend previous studies that looked at privacy-preserving photo sharing and whether users have their privacy protected when sharing photos. The goal of this review is to bridge the gap between the growing demand for image sharing via OSNs and individualized privacy requirements. This effort presents a comprehensive analysis of "privacy-preserving" technologies that specifically address contemporary privacy concerns associated with sharing images on online social networks (OSNs). This study presents a comprehensive analysis framework that focuses on the complete lifecycle of image sharing on online social networks (OSNs). This work presented a review framework called Privacy-Preserving Photo Sharing (PPPS) by categorizing previous works into three stages related to online secure photo sharing. Pre-processing, privacy settings, and photo publishing are the stages used in this survey's design to secure photo sharing. This framework aims to tackle the many privacy challenges and propose appropriate solutions in this multidisciplinary domain. During each phase, we analyse common user behaviours connected to sharing, the privacy concerns that arise from those behaviours, and evaluate representative solutions that are proposed by previous works.

1. INTRODUCTION

TA growing number of people are engaging with online social networks due to their popularity. Online social networks have become the most essential thing for internet users. As per 2021 statistics, 4.48 billion people are using OSNs worldwide. On average, six social media platforms are used by each internet user [1]. The OSNs facilitate a few indispensable services, such as online interaction with friends and family, social visibility, content sharing, business promotions, etc. On the other hand, the services of the OSNs may lead to the leakage of the user's private information. OSNs are leaking more personal information, especially in photo-sharing services [2]. The flexibility of photo sharing has significantly improved the social experience for online social users. Online social users can exhibit themselves and engage in active social interaction through the sharing of images because photographing and publishing tasks can be accomplished with a few easy clicks.

The various recent instances of photo content leaks by some of the most well-known online social and photo services, such as Facebook and SnapChat, are an indication that the current methodologies of the service providers are inefficient to preserve the privacy of the users [2-4]. The action of sharing photos by the publishers can cause damage to co-publishers who visually participate in the shared image [5]. It causes privacy loopholes for co-publishers in different ways, such as appearance, geographical region, social gatherings, etc. Based on this literature, this work categorized the privacy leaks in OSNs in two ways, which are described in the following section.

1.1 Typology of the privacy leaks in OSNs

Information leakage in OSNs typically occurs in two ways: based on visual data and context data. The visual data represents sensitive data from the media data, and the context represents the metadata of the posts. The typology of the privacy leaks is differentiated into two parts, as represented in Figure 1. The following section discussed parts of the "privacy leaks" typology in the OSNs.

a) Visual detectable leakage

This type of leakage occurs directly from the media data, especially pictures. The sharing of images is a very common practice in user postings. The publisher's intention is to publish the visual data for better understanding or proofing. But compared to the text data, the visual data may have a greater chance of leaking more sensitive information. This visually detectable leakage can be divided into two categories: object level and overall view level. At the object level, the objects from the shared picture can be detected, such as faces (publisher, co-publisher, unknown), face expressions, body gestures, and other objects (e.g., vehicle registration numbers, personal ornaments, etc.). The overall view object data, such as location, event details, and so on, can be detected at the overall view level [6-15].

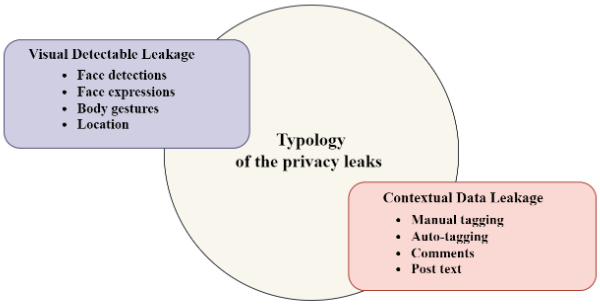


Figure 1. Typology of the privacy leaks

This typology of privacy risk involves two types of data: visually detectable and contextual data.

b) Contextual Data Leakage

This type of leakage occurs based on the context data integration with text posts and media posts. Sometimes, the context of the posts may leak sensitive information to the public. The context data, such as manual tagging, auto-tagging, comments, post text, etc., may cause the leakage of a few aspects of sensitive information (e.g., social connections, mood, activity, etc.). For instance, tagging is the process of integrating other users into the shared posts. Manual or automatic tagging data has the potential to leak social connection information to the public [16-22].

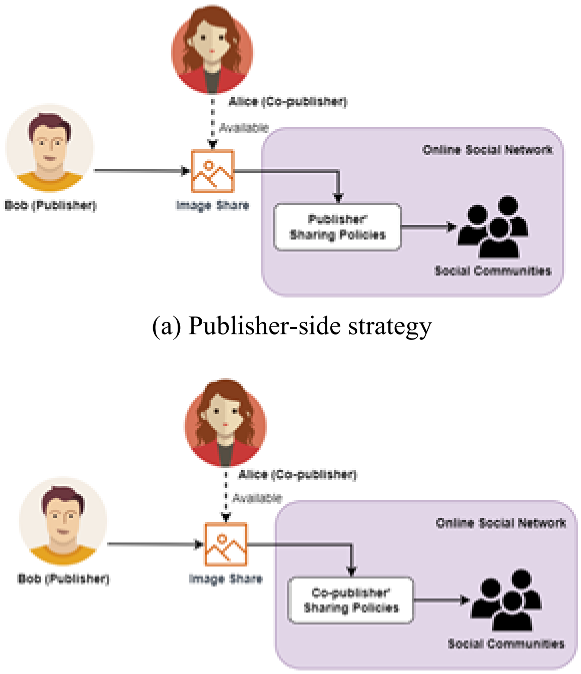
Main contributions

- This study proposed a PPPS-based methodology for analysing secure photo-sharing concepts in OSNs. This framework focuses on the research lifecycle of picture sharing in online social networks (OSNs), such as face identifications, access control, tags, anonymizations, etc.
- This framework encompasses three distinct stages and a range of common human behaviours. Those are image pre-processing, privacy settings, and photo publishing. The privacy challenges are analysed, and sophisticated methods are carefully analysed based on the phases outlined in the framework.
- This study presented a taxonomy of the security problems that come with sharing pictures on OSNs, which can help clarify the privacy of the people being shared. The taxonomy is determined by two distinct approaches: the publisher-side strategy and the co-publisher-side strategy.

The rest of this paper is structured as follows: In Section 2, the strategies of the secure photo-sharing concepts are presented. This section presented a taxonomy of the security problems and solutions of photo sharing, which includes an examination of the ideas and classification of privacy strategies. Section 3 presented previous works related to the three stages of PPPS. This study developed a framework for photo secure sharing by including several solutions, building upon earlier research findings. Each stage focused on distinct strategies for establishing a secure framework for online photo sharing in OSNs. The issues and challenges identified in this review are mentioned in Section 4. Section 5 includes suggested conclusion points.

2. PRIVACY-PRESERVING STRATEGIES

In earlier works, the privacy-preserving strategies of the secure photo-sharing concepts were divided into two parts. These are the publisher-side and co-publisher-side strategies. As illustrated in Figure 2, publisher-side strategies focus on preserving the privacy of the shared data or images from the individuals, friends, family, and other categories in the social networks. Co-publisher-side strategies focus on preserving the co-publisher's presence on the publisher’s shared content.



(a) Publisher-side strategy

(b) Co-publisher-side strategy

Figure 2. Privacy-preserving strategies

In Figure 2(a), the publisher (Bob) is sharing an image, and based on the sharing policies of the publisher, the photo may reach social circles such as friends, family, etc. In this case, the privacy of the co-publishers who participated in the photo was not considered. In Figure 2(b), the publisher (Bob) shares an image, and in that image, Alice (the co-publisher) is there. Based on the co-publisher's sharing policies, the photo may be shared with the public.

a) Publisher-side Strategies

This privacy-preserving strategy focused on the data leakage of the publishers when sharing a photo on the OSN. As represented in Figure 2(a), based on the access or sharing policies of the co-publisher, the photo can be shared to the publisher’s wall. This strategy does not focus on the privacy of the participants in the photo (co-publishers). According to a user's preferences, many studies describe methods for assessing and optimizing access control to better protect their desired privacy. These studies are typically used as an access control mechanism, giving the user a few canonical options (Only Friends, Public, Private, etc.) [23-29]. A few studies used machine learning models to implement design solutions for context-dependent and privacy-aware photo sharing. The suggested models make use of contextual data from the shared images to predict photo-sharing decisions. Contextual information such as location, activity, category, etc. is used to automatically decide which information to share based on user preferences [7, 20, 21].

The majority of research focuses on publisher-side strategies that are implemented based on customized accessibility [23-29]. and auto-access policies [7, 20, 21] for sharing the image. The publisher disseminates the photograph to ensure its availability to the intended recipients. The co-user presents a significant threat to picture privacy as it involves both the direct disclosure of material to the public and the compromise of image privacy.

b) Co-publisher-side Strategies

The main aim of this strategy is to focus on the leakage of information when sharing a photo by the publisher. As represented in Figure 2(b), this strategy does not focus on the privacy of the publishers, it only focused on the participants in the photo (co-publishers). These studies focus on the perspectives of the co-publisher(s). In these studies, researchers used context-dependent access policies such as age, gender, sentiment, etc. [26] and access control mechanisms [27, 28], to share images with co-publishers. Other proposals are also included in this strategy to help with user appearance management for photo sharing through OSNs, where co-publishers' faces blur to mask their appearance. The faces in a shared photo may blur and then become clear depending on the access policies or co-publisher responses [29-34].

This strategy focused on the co-publisher’s privacy in shared photos. These studies depended on access control mechanisms [26-28], and visual obfuscation [29, 30]. The purpose of access control is to utilise identifiable data contained within the shared image in order to grant permissions to all participants involved, rather than solely the publisher. Visual obfuscation is a commonly employed technique for protecting shared images from being seen by unwanted audiences. This is achieved by concealing or eliminating sensitive visual elements through direct manipulation of the image.

Based on previous research, this review framework is intended to categorize the process of secure photo sharing in social networks. This framework is categorized into image pre-processing, privacy settings, and photo publishing stages.

3. REVIEW FRAMEWORK TO SECURE PHOTO SHARING

Based on previous studies, this study designed a framework for secure sharing that addressed different solutions. As illustrated in Figure 3, this framework is designed in three stages: image pre-processing, privacy settings, and photo publishing. Each stage addressed different solutions for developing the secure framework of online photo sharing in OSNs.

3.1 Image pre-processing stage

The main objective of this stage is to identify image context data such as persons, expressions, objects, etc. before sharing the image with OSN. The modules that include this level are the identification of faces, objects, and location attributes.

a) Identification of faces

Recently, the goal of developing biometric features such as facial recognition has become an important factor in many applications. It is also a difficult endeavor due to issues that have consistently affected the accuracy of the results. Pose variations, expression, ageing, and other factors all contribute to difficulty in identifying faces. The researchers have been actively developing algorithms and techniques for identifying faces that are more reliable and accurate. Different methods for identifying faces are used based on different types of inputs, such as color-based, edge-based, feature-based, and so on [35-58]. This functionality is used to identify and distinguish between the publisher, co-publishers, and unknown parties.

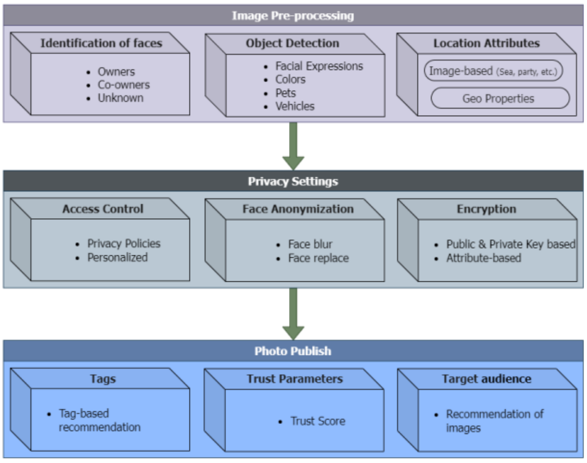


Figure 3. Framework of the PPPS's survey

To identify the faces, Kambi Beli and Guo [22] addressed the problem with face identification when there are significant fluctuations in characteristics such as expression, lighting, and positions. The LBP (local binary pattern) and K-NN (k-nearest neighbor) methodologies are the foundations of this methodology. LBP has emerged as one of the key methods for face identification due to its invariance to target picture rotation.

The approach that was suggested includes three parts. During the first phase, the procedure consists of collecting pictures (also known as training images), extracting features using the uniform Local Binary Patterns (LBP) technique, and then modelling or learning using the histogram of LBP descriptors. The second phase of the procedure is extracting distinguishing characteristics using the uniform LBP technique. This is then followed by classification using the K-NN algorithm with Euclidean distance, which aids in identifying objects or things within the provided images. This proposed K-NN with LBP got 85% accuracy on LFW file. To examine the face identification problem, Arigbabu et al. [29] developed a support vector machine (SVM)-based face recognition system that uses several kernel functions. Bi-cubic interpolation was used in this work to resample images during the pre-processing stage. SVM with soft margins is taken into account in classification models. When the input data cannot be separated linearly, a soft SVM is used and achieved recognition rate to 88% (accuracy).

A comparison study of four techniques: Haar-AdaBoost, LBP-AdaBoost, GF-SVM (Guided Filter SVM), and GF-NN (Guided Filter Neural Network) was carried out by Filali et al. [59] to identify the faces. These methods differ from one another in terms of how data is extracted and trained. Techniques including Haar-AdaBoost and LBP-AdaBoost rely on the boosting algorithm. With cascading classification, this boosting algorithm selects the most efficient classifier. Using a Gabor filter and the other two approaches, GF-SVM and GF-NN, the visual characteristics are extracted to distinguish. In their testing, Haar-AdaBoost showed the best performance compared to other approaches for small-sized images and performed at 60% accuracy for larger images.

Amato et al. [36] proposed a deep face recognition method using an open-set protocol proposed by and based on the CNN (convolutional neural networks) algorithm. This study considered nodal points as distinctive characteristics, encompassing the eyes, nose, and mouth, and their respective distances were taken into account for classification purposes. This work achieved 57% of accuracy in their results and numerous studies using the CNN algorithm for face prediction have been proposed [31, 32]. These works obtained low levels of accuracy using CNN models, but improved performance by including more face images from the user, which is not possible in real-time online social networks. A hierarchical design was proposed by Wang and Deng [60] to define the face recognition (FR) technique. The principles of deep learning and machine learning are combined hierarchically in this work. Deep learning ideas of convolute and pool input were used to extract face features from photos. The nearest neighbor (NN) machine learning algorithm, which is based on distance functions and threshold value comparisons, was used to implement face matching concepts.

b) Object Detection

Object detection helps to understand the image or scene, and it is an advanced visual analysis [37]. This functionality is used to identify the facial expression of the co-publishers and detect the objects that are present in the photo, such as vehicles, pets, etc. The major issues with this object detection are pose variations of viewpoint, deformation, clutter, etc. With improvements in computer hardware and computing power, algorithms that use deep learning to find objects are becoming more common.

Sadaf and Jadhav [11] proposed a three-stage framework, namely, image localization, feature extraction, and classification for the detection of facial expression. This work is proposed to identify facial expressions including surprise, happiness, sadness, etc. by analysing features of eyes, nose and lips using image localization. The DMMA (Discriminative Multi-Manifold) is a method used for image localization by dividing an image into a number of non-overlapping patches. In order to compare patches, Zernike moments were utilised in combination with the KNN (K-nearest neighbour) algorithm and the SVM (Support Vector Machine) algorithm. The support vector machine (SVM) technique attained a maximum accuracy of 96% using Zernike moments [61].

Shahzad and colleagues [62] used Convolutional Neural Networks (CNN) for emotion classification. The simulation findings show that the AlexNet and VGG-16 architectures outperform the SoftMax classifier in terms of support vector machine (SVM) and ensemble classifier performance. The work explained how to use the advantages of Convolutional Neural Networks and other machine learning (ML) approaches to improve the efficiency of emotion recognition applications. This includes extracting learned features from pre-trained convolutional neural networks (CNNs) and applying a range of classifiers. The work's deficiency resides in its inadequate level of accuracy (65%).

Kong et al. [38] proposed a two-stage framework. First, the candidate frame is chosen, and then the frame is changed and put into a category. In order to classify the objects, this work used the CNN algorithm. You Only Look Once (YOLO) is an innovative technique that identifies objects and their regions, as proposed by Redmon et al. [39]. As illustrated in Figure 4, using the input image, this network-based framework creates a S X S grid. The boundary boxes and confidence scores of each box are produced by these grids of the input images. The definition of the confidence score in Eq. (1) states that it is the intersection over union (IOU) of the truth box and prediction box. When no object is identified, the confidence score is zero.

$$Pr(Object) * IOU_{pred}^{truth} \tag{1}$$

In addition, each grid cell forecasts the class probability Pr (Classi | Object) of the grid. Final predictions are encoded based on the confidence values and class probabilities.

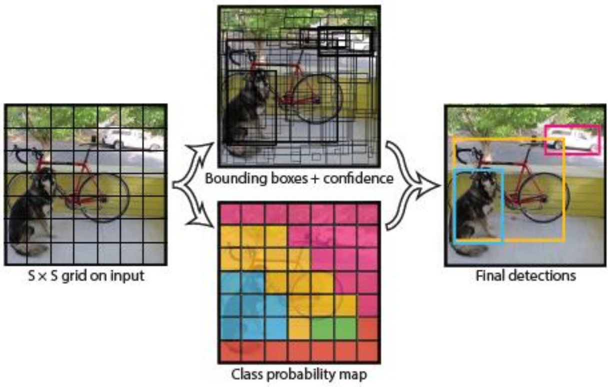


Figure 4. The Yolo model [39]

The input image (S×S grid on input) is processed for identification of various boundary boxes and confidence scores. Based on the class probability map, the final predictions were generated, such as "dog," "car," and "bicycle."

c) Location Attributes

Social networks and geographic data are combined in location-based social networking data. Images can be used to get location-based social data in two ways: based on image data and based on geo-properties. The image-based location extraction module extracts spatial data such as sea, beach, road, etc. The traditional "check-in" indicates a user's geographical action in the real world, residing where the online world and real world connect. Based on "check-in," the direct location properties, or geo-properties (e.g., latitude and longitude), can be extracted [33]. Extraction of location data from shared images is difficult without location-based properties.

The region extraction-based R-CNN (region-based convolutional neural networks) technique extracts candidate regions and transforms the object detection problem into the regional classification problem. A spatial pyramid pooling layer (SPP) [34] is then created to restrict the size of potential processing zones for the R-CNN model. By allowing the use of input images of different sizes, it aimed at overcoming the limitations of traditional convolutional neural networks (CNNs) that employ images of fixed size. This model is utilised for the deformation of location object data from images. This work successfully obtained a processing time and accuracy rate of 93% in its results. The location data can also be extracted from the text of the posts in OSNs. Few works have been proposed to extract location data or perform geo-parsing from OSN posts. Middleton et al. [61] developed an approach to the extraction of location data based on the unstructured text collected from the user’s social media posts.

The work encompasses three primary features: Geoparsing, Location Disambiguation, and Geotagging. Geoparsing utilises methods like named entity recognition (NER) to detect and classify place names and geographical references present in the text. The method of Location Disambiguation may entail the examination of contextual cues, such as surrounding keywords in the content or the user's profile data, in order to ascertain the most probable location. Geotagging refers to the process of associating geographical coordinates with user-generated information, such as social media posts.

Table 1 summarizes previous studies of the stage of image pre-processing. The techniques of the previous studies of the three modules (identification of faces, object detection, and target location attributes) of this stage are discussed in this section.

3.2 Privacy settings

The main goal of this step is to share the photos based on the privacy settings or the rules the user sets for sharing. The modules that are included in this level are access control, face anonymization, and encryption.

a) Access Control

The access control in OSN is a way to regulate the user-specified policies. Based on the access control policies of the users, the OSNs share content according to control settings or find audiences based on the policies. The majority of social networking sites and photo-sharing websites let users manage their privacy through access control. The main issue with this procedure is that users must manually define their sharing policies in a static manner. However, few works have been proposed to address the issue of manual procedures.

Xu et al. [19] proposed a trust-based photo sharing system with a trust score and privacy loss score. Based on the trust and privacy scores, the co-owned photos are shared with or without the co-owner's presence. The trust value is calculated based on the relationship status. The sensitivity score ldjk is calculated based on the trust score tkj of the co-owner and privacy score μ(d)k defined by the publisher, which is defined in Eq. (2).

$$l^{d}_{jk} = f_{loss}\,(t_{kj},\, \mu^{(d)}{}_{k}) \tag{2}$$

where, l represents loss, d represents a sensitive photo, j represents the user, and k represents the value of sensitivity.

Vishwamitra et al. [30] proposed the HideMe framework, which offers an automatic access control system based on a few categories of attributes. This work is concentrated on a co-publisher’s security on shared images. Setting access policies for each co-owned image while sharing may be difficult and time-consuming. Instead of setting the access policies for each image, HideMe developed a policy generator to assist them in making the decision of whether to blur or reveal their faces in shared images. Example: ({t,s,i,a}, decision): ({06/2022, Hyderabad, Everyone, 4m}, blur). The HideMe framework significantly reduces the efficiency of photo sharing procedures and consumes an excessive number of resources. As a result, consumers may consider it risky to use on real-time social networking platforms, reducing its usefulness and efficacy. HideMe requires users to navigate complex settings or take additional actions in order to securely submit images, which may discourage adoption or cause user discomfort.

Yan et al. [12] proposed a system of "Face/Off" that required users to set policies based on their list of friends. This work protects the co-owned presence in the images from the particular targeted audience (restricted users). A "processed" photo that can be displayed differently depending on who is viewing it is the result of this phase. The system will therefore automatically conceal the faces of individuals with restricted access when a photo is accessed. The Face/Off approach may increase complexity and computational cost, particularly for real-time applications requiring real-time processing or platforms with a large number of users. Perturbing facial photos can be computationally demanding, potentially affecting system speed and scalability. Yuan et al. [21] presented a machine learning-based approach for context-dependent and privacy-aware image sharing. This publisher-side strategy used contextual information about the users.

Table 1. A summary of solutions in the image pre-processing stage for secure photo sharing

Module	Technique/s	Summary
Identification of faces	K-Nearest Neighbor [22]	This work addressed the problem of fluctuations such as lighting, positions, etc. This work depended on the K-nearest neighbor algorithm without classification analysis for the identification of faces.
	Support Vector Machine [30]	This work used the SVM algorithm for face recognition with several kernel functions and also addressed gender recognition. But the rate of face recognition is very low.
	Convolutional Neural Networks [30-32]	CNN (Convolutional Neural Networks) has emerged for face identification. The accuracy of the CNN algorithms drops when the input data is smaller.
	Haar-AdaBoost [59]	This study implemented different types of techniques and compared the results. The Haar-AdaBoost technique achieved better performance compared to other techniques. But this work did not address the fluctuation problems in face identification.
Object Detection	K-Nearest Neighbor & Support Vector Machine [11]	The movements of the eyes, lips, etc. are considered for detecting facial expression.
	Convolutional Neural Networks [38]	After identifying the frames of the objects, this work detected objects with the CNN algorithm.
	You Only Look Once (YOLO) [39]	The major purpose of this framework is to address the object detection regression issue. This work devised the YOLO algorithm, which predicts the target region as well as the target category.
Location Attributes	Region-based Convolutional Neural Networks [34]	Visual location characteristics such as sea, park, and so on were identified in this study. However, using these attributes, it is impossible to extract precise location information from the images.

b) Face Anonymization

Face anonymization is the process of removing or blurring the identifiable objects of the targeted users in the shared images. The user experience will be harmed in terms of social sharing purposes, and malicious viewers could readily identify that the image has been modified, which is one of the fundamental concerns of face anonymization [40]. There is a significant loss of visual integrity in the photos processed using the aforementioned conventional technique. On the other hand, some cutting-edge approaches to visual obscuration that make use of contemporary computer vision techniques have the potential to solve the issue.

A GAN-based (Generative Adversarial Net) inpainting method for head replacement was suggested by Sun et al. [41]. Because the faces in social media photographs typically appear in a variety of activities and orientations, realistic face replacement is difficult. This work used GAN in two stages to solve this issue. In order to sensibly capture the head pose, a deep convolutional generative adversarial network (DCGAN) was first built to create facial landmarks from visual context (such as body pose). In the second stage, the face generator was then constructed using a different DCGAN that was conditioned by the derived face landmark. This proposed effort was unable to generate faces efficiently, resulting in a 39% fooling rate.

To obfuscate identification, Sun et al. [42] offer a quantitative face model. The output image produced at this stage is photo-realistic because the obfuscated region has been inpainted with realistic information and the granular features that were absent from the generated 3D morphable model (3DMM) have been added. This methodology involves detecting facial landmarks in the target image, generating a replacement face using a GAN, and blending the replacement face seamlessly into the original image. The success of the face replacement process is strongly determined by the calibre and variety of the training material provided to train the GANs. Insufficient or biassed training data may result in a lack of variation and authenticity in the produced faces, rendering them easily recognised and less compelling.

Li and Lin [43] presented the framework AnonymousNet used to predict facial features. This work used the pipeline model with a convolutional neural network (CNN) and the random forest algorithm. Also, this work extracted deep features from the CNN's fully connected layers and trained random forest classifiers accordingly. After identifying the attributes of faces, this system synthesizes the attributes of the faces in the stage of face obfuscation. For example, gender changing, face color changing, hair color changing, etc.

c) Encryption

Encryption methodologies are used to handle user access to the image data. Based on the shared policies and access control, the data is decrypted and made available to the target users. The issues of encrypting data in a shared image are heavy computation, maintenance of keys, extracting features, etc.

In OSN encryption, Paul et al. [44] explained that public key encryption is the simplest method of implementing encryption. Asymmetric encryption is more expensive than symmetric encryption techniques. Therefore, sharing content with a number of recipients only requires one encryption (symmetric) key to see the original content. A fresh key distribution is not required if the group setting remains the same.

De Salve et al. [45] proposed a symmetric key and an LKH tree-based (Logical Key Hierarchical) model. The LKH model is designed to handle symmetric keys of social groups by utilizing a hierarchical structure. The group owner produces the linked key-tree KT when a social group is started. Each member of the group is paired with a branch of KT, and each branch of KT is associated with a symmetric key. Based on the symmetric key, the content can be encrypted and decrypted by the group members. Dang et al. [46] proposed an encryption methodology for online applications to offer a fusion of attribute-based encryption (AB) with P2P-based programs. For accessing the group data, the ABE encryption used a public key based on the attributes of the target users, such as user role, area, etc. Han et al. [47] implemented ciphertext-policy attribute-based encryption for secure data sharing with data hiding. The attributes, such as department, occupation, relationship, etc., are used for accessing the data. Based on the attributes, the encrypted data is either available or hidden.

Securely generating, storing, distributing, and revoking encryption keys is essential for the implementation of effective encryption methods. Effectively handling encryption keys in real-time OSN applications and user devices can be complex and susceptible to mistakes, which could result in the loss, unauthorized disclosure, or compromise of the keys if not managed appropriately.

Table 2 summarizes previous studies of the stage of privacy settings. The techniques of the previous studies of the three modules (access control, face anonymization, and encryption) of this stage are discussed in this section.

3.3 Photo publish

Photo publish is the final level of the PPPS used to share and recommend images in OSNs. The shared images can be recommended to end users based on tags, trust scores, and target user identification.

a) Tags

The shared images in OSNs need to be tagged with keywords for indexing, distributing, recommendation, searching, etc. This process needs to be protected to prevent the leakage of confidential information. Tonge et al. [9] implemented a collaborative filtering algorithm to suggest privacy-aware tags. The proposed algorithm for tag recommendation is based on the collected image dataset, which comprises images and their tags. For the target image, this system collects the deep features and suggests similar tags (e.g., tag: "women," similar: "girl"). As per the Tag Ranking algorithm, a privacy-aware ranked list of tags is calculated by considering public or private tags.

Tonge and Caragea et al. [49] presented a broad range of image features extracted from pre-trained CNN classification models. This study presented a new way for forecasting photo privacy levels using deep neural networks. The authors use deep learning models' inherent capabilities to autonomously learn about the properties and patterns that indicate image confidentiality. The pre-trained CNN models that are used to extract features are AlexNet, GoogLeNet, VGG-16, and ResNet. In their results, the ResNet model had better accuracy of 88% when compared to other models. In this work, the SVM algorithm was used to figure out how private an image is based on its tags.

Table 2. A summary of solutions in the photo sharing stage for secure photo sharing

Module	Technique/s	Summary
Access Control	Trust-based access control [19]	This work is an automated access control system based on trust parameters. But this work is only concentrated on publisher-side security sharing; there is no privacy for co-owners' presence.
	HideMe [30]	It is a co-publisher strategy, but each co-publisher must set up the access policies for each attribute on their own.
	Face/Off [12]	Targeted-user access control mechanisms and co-publisher strategy It is a basic mechanism that restricts target users.
	Context data based access control [21]	The access control mechanism is based on previous user sharing, learning, and context data analysis. This context-dependent mechanism is more practical for users, but it is a publisher-side strategy.
Face Anonymization	Generative Adversarial Net (GAN) [41]	The goal of this work is to broaden the target population based on the image. This diversification concept is better than obfuscation, but the results of this model are not realistic.
	Hybrid model [42]	GAN and 3D morphable models were used to replace the face with another face. This work implemented realistic information and granular features to replace the face attributes. Only a few attributes, however, were used to replace the attributes.
	AnonymousNet [43]	This work is implemented with the CNN model for identification of face attributes in images by replacing them with other attributes with the Random Forest model. The results of this model are not realistic.
Encryption	Group key encryption [44]	This study implemented decentralization for secure group data management by spreading one encrypted key (symmetric) among a number of recipients. However, the size of the group is not taken into account in this work.
	Logical Key Hierarchical tree-based model [45]	This work used symmetric key encryption mechanisms for social groups. Group members are categorized into multiple branches, and each branch maintains a symmetric key. A group's data cannot be useful to others.
	Attribute-based encryption [46]	Based on the target user's attribute data, the data is decrypted. It is a practical solution for OSN, but heavy computation is required for this type of model.
	CP-ABE [47]	The data can be hidden or decrypted based on the attributes of the target user. This concept is not suitable for social groups.

Squicciarini et al. [50] presented T2P (Tag-to-Protect) tag-driven policy recommender system designed to empower users with personalized privacy settings when sharing images online. The system utilized tags associated with images to recommend appropriate privacy policies based on user preferences and contextual factors. The study presents a new way for forecasting photo privacy levels using deep neural networks. The authors used deep learning models' inherent capabilities to autonomously learn about the properties and patterns that indicate image confidentiality. Thee proposed vertical comparison and CoTag graph cohesiveness methods for recommending the tags for images. The CoTag Graph is designed as a graph to represent the relationship between tags, with each node standing for a different tag and each edge connecting two tags that both appear alongside the same image.

b) Trust parameters

OSN users may share personal information with friends and co-workers, but they are not always entirely aware of the risk of unintended disclosure to different parties, such as adversaries, social bots, spammers, etc. Many trust-based models that work based on trust parameters and trust scores are created to prevent this information leakage. In this methodology, trust parameters are computed using some of the quantifiable user credibility metrics. User credibility is established by factors such as the total number of friends, account age, marital status, gender, etc. that contribute to the user's OSN reputation and level of trustworthiness [8].

For predicting malicious accounts on Twitter, Pramitha et al. [51] implemented a system by comparing it with machine learning models. In this work, for the trust parameters, they considered the content of the tweets, URLs shared in posts, and user attributes such as friend count, status count, date of account creation, etc. This study presumably investigated different supervised machine learning methods employed for the purpose of bot detection, including XGBoost and random forests. In comparison to Random Forest, the XGBoost algorithm outperforms with 89% accuracy. Yu et al. [52] proposed a framework to categorize social activities and investigate how they relate to social picture sharing's fine-grained privacy policies. Examined various features that describe users' social behaviours, including: (1) Relationship types, (2) proximity to the image owner, (3) interest in the user's subject, (4) level of involvement, and (5) social network activity score. They created a kernel function that checks how similar (or close) target users are based on these factors. If the system incorrectly identifies the sensitiveness of data or overestimates user trustworthiness, it may result in erroneous privacy settings, thus affecting user privacy.

Kashani and Hamidzadeh [53] implemented the K-anonymity method, which uses the anonymity method to preserve users' privacy and lower error rates. The main objective of the research appears to be suggesting an approach for selecting features in recommendation systems that safeguards user privacy, employs collaborative filtering methods, and integrates the notion of mutual trust in social platforms. Before using the trustworthiness score, the data, such as gender, job, age, etc., were made anonymous using the k-anonymity method. However, methods such as differential privacy or anonymization might impact the processing demands and perhaps impact the real-time efficiency of recommendation systems.

c) Target audience

Through the creation, description, and uploading of text, photos, and multimedia messages, OSNs produce a significant volume of media content. It is important to recommend the data to social network users. The recommendation concepts on the OSNs help identify trending pictures, popular posts, etc. This section describes the previous work related to identifying the target audience for shared images.

Table 3. A summary of solutions in the photo publish stage for secure photo sharing

Module	Technique/s	Summary
Tags	Collaborative Filtering algorithm [9]	This strategy relies on collaborative filtering to suggest privacy-conscious tags for recently submitted photographs on content sharing services. This concept did not include the sensitivity of the tags.
	Vertical Comparison [50]	The vertical comparison examines the relationships between a tag and each policy-defined access privilege. Based on policy representation, the system identifies private tags.
	Convolutional Neural Networks and Support Vector Machine [49]	This study implemented pre-trained convolutional neural network models to extract the tags and analyze the private tag of the user with support vector machines.
Trust Parameters	XGBoost (eXtreme Gradient Boosting) algorithm [51]	Based on trust parameters such as status, friend count, etc., a spam account detection model is proposed. This work implemented comparative classification results between Random Forest and XGBoost. This work only depends on the profile attributes of the users.
	Kernel Function [52]	This work involved several user variables and implemented a kernel function that assesses the similarity of target users. Different types of attributes are used in this work, but the privacy of the attributes is not considered.
	Confidence-conscious trusted model [53]	To calculate trustworthiness score used confidence-based trust estimate method based on user profile attributes. This work considered limited attributes to calculate trustworthiness.
Target Audience	A collaborative search algorithm [54]	A collaborative search algorithm is proposed for implementing recommendations based on tags. But the recommended results focused on capturing trending images.
	Deep User-Image Feature (DUIF) [55]	Recommend relevant content to users based on user-image features. This work only focused on recommendations and did not mention the privacy of the images or tags.

Hossain et al. [54] proposed a system to recommend personalized trending images to the users of OSNs. To implement a recommendation system, they proposed a collaborative search algorithm. By determining the pairwise cosine similarities, this algorithm only takes into account the similarity between tags and the similarity between individuals. Geng et al. [55] described how traditional recommender systems often struggle to identify representative characteristics of both persons and photos in OSNs. In this work, they proposed the Deep User-Image Feature (DUIF), which transforms the user-image features into low-dimensional feature space to help recommend relevant content to users.

Table 3 summarizes previous studies of the stage of photo publish. The techniques of the previous studies of the three modules (tags, trust parameters, and target audience) of this stage are discussed in this section.

4. ISSUES AND CHALLENGES

As discussed in Section 2, the privacy-preserving strategies of the secure photo-sharing concepts are divided into two parts: the publisher side and the co-publisher side strategies. The majority of previous works rely on publisher-side strategies to protect publishers' privacy while sharing media data. This survey designed a framework to address different solutions for three different models or stages: Image pre-processing, privacy settings, and photo publishing. Image pre-processing, privacy settings, and photo sharing are interrelated components that collectively enhance the confidentiality, safety, and user experience of sharing photos in OSNs. By incorporating these methods into the processes of publishing photos and the features of platforms, users can experience enhanced authority and assurance in handling their digital personas and online information.

In the stage of image pre-processing, we focused on numerous works that rely on face identification, object detection, and the detection of location attributes on the images. Several studies on face recognition have proposed various concepts based on machine learning and deep learning algorithms. A few issues, such as pose fluctuations, expressions, aging, and other factors, have consistently impacted the accuracy of the results of face identification. The K-nearest neighbor [22] and convolutional neural networks [30-32] algorithms produced better results in this area of work. Pose variations, viewpoint, and deformation (cluttered, etc.) are the main issues that reduce the accuracy of the results in object detection. You Only Look Once (YOLO) [39] addressed the many issues of the object detection model. The shared images have the potential to leak location data. Extracting the location data from the images by identifying the location objects is a challenging issue. The R-CNN [34] algorithm identified the visual location attributes such as sea, park, etc.

In the second stage of privacy settings, we identified different security policies for access control, face anonymization, and encryption. In OSN, the user-specified policies are controlled by access control. Users have to manually define their sharing policies in a static way, which is the main issue with this process. In this survey, the context data-based access control [21] mechanism is based on previous user sharing, learning, and context data analysis. This context-dependent mechanism is more practical for users. This model can help with the co-publisher's side strategy. The process of face anonymization involves blurring or removing the recognizable objects of the targeted users from the shared pictures. For this concept, the previous works commonly use the GAN-based (Generative Adversarial Net) inpainting method [41-43]. To manage user access to the image data, encryption techniques are one method. Target users can access the decrypted data based on access control and shared rules. Heavy processing, key maintenance, feature extraction, etc. are problems with data encryption in shared images.

Photo publishing is the final stage, used to recommend the images in OSNs. The images can be recommended to end users based on tags, trust scores, and target user identification. To facilitate indexing, distribution, recommendation, searching, and other functions, shared photos in OSNs must be labeled with tags. To stop the leak of private information, this process must be secured. The works of Tonge and Caragea [49] and Squicciarini et al. [50] presented a secure tag-based image recommendation. Many trust-based models use trust parameters that are computed using some of the quantifiable user credibility metrics. Previous research focused on user profile attributes to calculate trustworthiness scores.

5. SOCIAL MEDIA AND ETHICS

The ethical considerations pertaining to the tools and techniques utilised in social media are complex and have substantial consequences for individuals, society, and the functioning of democracy. The utilisation of social media gives rise to significant ethical dilemmas pertaining to matters such as privacy concerns, algorithmic bias, addiction, cyberbullying, and breaches in data security.

a) Privacy Concern

Social media services frequently gather extensive quantities of user information, encompassing personal details, browsing patterns, and engagements. This gives rise to apprehensions over user privacy and the possibility of misuse or unauthorised acquisition of sensitive data. The Cambridge Analytica scandal, in which private information from millions of Facebook users was collected without their authorization, serves as a prominent illustration of privacy infringements on social media platforms [63].

b) Algorithmic bias

As per Eslami et al. [64], social networking algorithms commonly prioritise information based on user interaction rates, which can lead to the formation of filter bubbles. These filter bubbles only show consumers information that reinforces their existing beliefs and preferences. This can lead to the spread of erroneous or misleading information, the formation of insular societies that reinforce pre-existing attitudes, and the escalation of societal differences.

c) Addiction

Social media platforms use design tactics to maximise engagement among users and amount of time spent on their sites, which can lead to addictive behaviours and harmful effects on mental health. Services like limitless browsing, alerts, and personalised recommendations are intended to catch and hold the user's interest [65].

d) Cyberbullying

Social media platforms face challenges in combating online abuse, hate speech, and cyberbullying while maintaining the principles of free speech and user expression [66].

e) Data breach

As per Lei et al. [67], Social media companies should have strict security protocols to protect user data from unauthorised access, hacker attacks, and data breaches. Neglecting to protect user information can result in significant breaches of privacy and tarnish the reputations of individuals and providers.

6. CONCLUSIONS

This work conducted a survey on privacy-preserving photo sharing on OSNs, with a focus on the online social users' privacy requirements for current OSN image sharing. Based on this survey of OSN photo sharing, this work presented a high-level analysis framework to address a wide range of privacy concerns, issues, and challenges. Using this framework, this work methodically found privacy concerns and surveyed the current solutions in a step-by-step manner. Also, this work explored each intelligent solution's approaches or strategies, outlined its technological features for each stage of the review process, and discussed the issues and challenges in this field. This work will help manage privacy in the modern era by addressing the needs of the growing demand for OSN image sharing and individual privacy requirements. The solutions pertaining to privacy intelligence that were evaluated in this survey are sufficient to form a system that protects, prevents, and applies to social networking sites. This work has the potential to contribute to the establishment of a more sophisticated environment for posting photos on privacy-conscious digital social platforms, where the confidentiality of co-owers is appropriately upheld.

Future developments should give priority to improving user control and clarity regarding privacy configurations and data management procedures. This could involve giving consumers precise authority over the individuals who can see their photographs, along with explicit elucidations of how their data is handled and disseminated by internet platforms.

REFERENCES

[1] Social Media Usage & Growth Statistics (2021). How many people use social media in 2022? (65+ Statistics). www.backlinko.com/social-media-users.

[2] Facebook Exposed up to 6.8 Million Users' Private Photos in Latest Leak - the Verge. (2018). Facebook exposed up to 6.8 million users' private photos to developers in latest leak. www.theverge.com/2018/12/14/18140771/facebook-photo-exposure-leak-bug-millions-users-disclosed.

[3] Zhang, M., Sun, Z., Li, H., et al. (2022). Go-sharing: A blockchain-based privacy-preserving framework for cross-social network photo sharing. IEEE Transactions on Dependable and Secure Computing, 20(5): 3572-3587. https://doi.org/10.1109/TDSC.2022.3208934

[4] Fox News. (2023). Hackers Get Their Hands on 100K 'Deleted' Snapchat Images. www.foxnews.com/tech/hackers-get-their-hands-on-100k-deleted-snapchat-images.

[5] Ilia, P., Carminati, B., Ferrari, E., Fragopoulou, P., Ioannidis, S. (2017). SAMPAC: Socially-aware collaborative multi-party access control. In Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, Scottsdale Arizona, USA, pp. 71-82. https://doi.org/10.1145/3029806.3029834

[6] Bahri, L., Carminati, B., Ferrari, E. (2018). Decentralized privacy preserving services for online social networks. Online Social Networks and Media, 6: 18-25. https://doi.org/10.1016/j.osnem.2018.02.001

[7] Amon, M.J., Hasan, R., Hugenberg, K., Bertenthal, B.I., Kapadia, A. (2020). Influencing photo sharing decisions on social media: A case of paradoxical findings. In 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, pp. 1350-1366. https://doi.org/10.1109/SP40000.2020.00006

[8] Voloch, N., Gal-Oz, N., Gudes, E. (2021). A trust based privacy providing model for online social networks. Online Social Networks and Media, 24: 100138. https://doi.org/10.1016/j.osnem.2021.100138

[9] Tonge, A., Caragea, C., Squicciarini, A. (2018). Privacy-aware tag recommendation for image sharing. In Proceedings of the 29th on Hypertext and Social Media,

Baltimore, MD, USA, pp. 52-56. https://doi.org/10.1145/3209542.3209574

[10] Ilia, P., Polakis, I., Athanasopoulos, E., Maggi, F., Ioannidis, S. (2015). Face/off: Preventing privacy leakage from photos in social networks. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver Colorado, USA, pp. 781-792. https://doi.org/10.1145/2810103.2813603

[11] Shaikh, S.A., Jadhav, D. (2018). Human face detection and facial expression identification. In 2018 Second International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, pp. 956-962. https://doi.org/10.1109/ICCMC.2018.8487651

[12] Yan, C., Li, L., Zhang, C., Liu, B., Zhang, Y., Dai, Q. (2019). Cross-modality bridging and knowledge transferring for image understanding. IEEE Transactions on Multimedia, 21(10): 2675-2685. https://doi.org/10.1109/TMM.2019.2903448

[13] Liu, J., Wang, S., Yang, W. (2019). Sparse autoencoder for social image understanding. Neurocomputing, 369: 122-133. https://doi.org/10.1016/j.neucom.2019.08.083

[14] Liang, Y., Bai, Y., Zhang, W., Qian, X., Zhu, L., Mei, T. (2019). Vrr-vg: Refocusing visually-relevant relationships. In Proceedings of the IEEE/CVF International Conference on Computer Vision, Seoul, Korea (South), pp. 10403-10412. https://doi.org/10.1109/ICCV.2019.01050

[15] Li, Z., Tang, J., Mei, T. (2018). Deep collaborative embedding for social image understanding. IEEE Transactions on Pattern Analysis and Machine Intelligence, 41(9): 2070-2083. https://doi.org/10.1109/TPAMI.2018.2852750

[16] Abraham, A. (2012). Computational Social Networks: Security and Privacy. Springer Science & Business Media.

[17] Zhu, L. (2011). Privacy in context: Technology, policy, and the integrity of social life. Journal of Information Privacy and Security, 7(3): 65-73. https://doi.org/10.1080/15536548.2011.10855919

[18] Shu, J., Zheng, R., Hui, P. (2018). Cardea: Context-aware visual privacy protection for photo taking and sharing. In Proceedings of the 9th ACM Multimedia Systems Conference, New York, NY, USA, pp. 304-315. https://doi.org/10.1145/3204949.3204973

[19] Xu, L., Bao, T., Zhu, L., Zhang, Y. (2018). Trust-based privacy-preserving photo sharing in online social networks. IEEE Transactions on Multimedia, 21(3): 591-602. https://doi.org/10.1109/TMM.2018.2887019

[20] Nadeem, M.S., Franqueira, V.N., Zhai, X. (2019). Privacy verification of PhotoDNA based on machine learning. In Security and Privacy for Big Data, Cloud Computing and Applications, pp. 263-280. https://doi.org/10.1007/s11042-023-15621-5

[21] Yuan, L., Theytaz, J., Ebrahimi, T. (2017). Context-dependent privacy-aware photo sharing based on machine learning. In ICT Systems Security and Privacy Protection: 32nd IFIP TC 11 International Conference, SEC 2017, Rome, Italy, pp. 93-107. https://doi.org/10.1007/978-3-319-58469-0_7

[22] Kambi Beli, I.L., Guo, C. (2017). Enhancing face identification using local binary patterns and k-nearest neighbors. Journal of Imaging, 3(3): 37. https://doi.org/10.3390/jimaging3030037

[23] Hirschprung, R., Toch, E., Schwartz-Chassidim, H., Mendel, T., Maimon, O. (2017). Analyzing and optimizing access control choice architectures in online social networks. ACM Transactions on Intelligent Systems and Technology, 8(4): 57. https://doi.org/10.1145/3046676

[24] Schwartz-Chassidim, H., Ayalon, O., Mendel, T., Hirschprung, R., Toch, E. (2020). Selectivity in posting on social networks: The role of privacy concerns, social capital, and technical literacy. Heliyon, 6(2): e03298. https://doi.org/10.1016/j.heliyon.2020.e03298

[25] Gruzd, A., Hernández-García, Á. (2018). Privacy concerns and self-disclosure in private and public uses of social media. Cyberpsychology, Behavior, and Social Networking, 21(7): 418-428. https://doi.org/10.1089/cyber.2017.0709

[26] Fogues, R.L., Murukannaiah, P.K., Such, J.M., Singh, M.P. (2017). Sharing policies in multiuser privacy scenarios: Incorporating context, preferences, and arguments in decision making. ACM Transactions on Computer-Human Interaction (TOCHI), 24(1): 5. https://doi.org/10.1145/3038920

[27] Sheikhalishahi, M., Stork, I., Zannone, N. (2021). Privacy-preserving policy evaluation in multi-party access control. Journal of Computer Security, 29(6): 613-650. https://doi.org/10.3233/JCS-200007

[28] Yu, L., Motipalli, S.M., Lee, D., Liu, P., Xu, H., Liu, Q., Tan, J., Luo, B. (2018). My friend leaks my privacy: Modeling and analyzing privacy in social networks. In Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies, New York, NY, USA, pp. 93-104. https://dl.acm.org/doi/abs/10.1145/3205977.3205981

[29] Li, F., Sun, Z., Li, A., Niu, B., Li, H., Cao, G. (2019). Hideme: Privacy-preserving photo sharing on social networks. In IEEE INFOCOM 2019-IEEE Conference on Computer Communications, Paris, France, pp. 154-162. https://doi.org/10.1109/INFOCOM.2019.8737466

[30] Vishwamitra, N., Li, Y., Wang, K., Hu, H., Caine, K., Ahn, G.J. (2017). Towards pii-based multiparty access control for photo sharing in online social networks. In Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies, Indianapolis Indiana, USA, pp. 155-166. https://doi.org/10.1145/3078861.3078875

[31] Ma, Z., Ding, Y., Li, B., Yuan, X. (2018). Deep CNNs with robust lbp guiding pooling for face recognition. Sensors, 18(11): 3876. https://doi.org/10.3390/s18113876

[32] Cho, S.W., Baek, N.R., Kim, M.C., Koo, J.H., Kim, J.H., Park, K.R. (2018). Face detection in nighttime images using visible-light camera sensors with two-step faster region-based convolutional neural network. Sensors, 18(9): 2995. https://doi.org/10.3390/s18092995

[33] Gao, H., Liu, H. (2013). Data analysis on location-based social networks. In Mobile Social Networking, pp. 165-194. https://doi.org/10.1007/978-1-4614-8579-7_8

[34] He, K., Zhang, X., Ren, S., Sun, J. (2015). Spatial pyramid pooling in deep convolutional networks for visual recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 37(9): 1904-1916. https://doi.org/10.1007/978-3-319-10578-9_23

[35] Arigbabu, O.A., Ahmad, S.M.S., Adnan, W.A.W., Yussof, S., Mahmood, S. (2017). Soft biometrics:

Gender recognition from unconstrained face images using local feature descriptor. arXiv preprint arXiv:1702.02537. https://doi.org/10.48550/arXiv.1702.02537

[36] Amato, G., Falchi, F., Gennaro, C., Massoli, F.V., Passalis, N., Tefas, A., Vairo, C. (2019). Face verification and recognition for digital forensics and information security. In 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, pp. 1-6. https://doi.org/10.1109/ISDFS.2019.8757511

[37] Sun, G., Ding, S., Sun, T., Zhang, C. (2021). SA-CapsGAN: Using capsule networks with embedded self-attention for generative adversarial network. Neurocomputing, 423: 399-406. https://doi.org/10.1016/j.neucom.2020.10.092

[38] Kong, T., Sun, F., Tan, C., Liu, H., Huang, W. (2018). Deep feature pyramid reconfiguration for object detection. In Proceedings of the European Conference on Computer Vision (ECCV), Munich, Germany, pp. 169-185. https://doi.org/10.48550/arXiv.1808.07993

[39] Redmon, J., Divvala, S., Girshick, R., Farhadi, A. (2016). You only look once: Unified, real-time object detection. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Las Vegas, NV, USA, pp. 779-788. https://doi.org/10.1109/CVPR.2016.91

[40] Xiong, W., Yu, J., Lin, Z., Yang, J., Lu, X., Barnes, C., Luo, J. (2019). Foreground-aware image inpainting. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Long Beach, CA, USA, pp. 5840-5848. https://doi.org/10.1109/CVPR.2019.00599

[41] Sun, Q., Ma, L., Oh, S.J., Van Gool, L., Schiele, B., Fritz, M. (2018). Natural and effective obfuscation by head inpainting. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, pp. 5050-5059. https://doi.org/10.1109/CVPR.2018.00530

[42] Sun, Q., Tewari, A., Xu, W., Fritz, M., Theobalt, C., Schiele, B. (2018). A hybrid model for identity obfuscation by face replacement. In Proceedings of the European Conference on Computer Vision (ECCV), Munich, Germany, pp. 553-569. https://doi.org/10.1007/978-3-030-01246-5_34

[43] Li, T., Lin, L. (2019). Anonymousnet: Natural face de-identification with measurable privacy. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops. https://doi.org/10.48550/arXiv.1904.12620

[44] Paul, T., Famulari, A., Strufe, T. (2014). A survey on decentralized online social networks. Computer Networks, 75: 437-452. https://doi.org/10.1016/j.comnet.2014.10.005

[45] De Salve, A., Mori, P., Ricci, L., Di Pietro, R. (2023). Content privacy enforcement models in decentralized online social networks: State of play, solutions, limitations, and future directions. Computer Communications, 203: 199-225. https://doi.org/10.1016/j.comcom.2023.02.023

[46] Dang, N.T., Tran, H.M., Nguyen, S.V., Maleszka, M., Le, H.D. (2021). Sharing secured data on peer-to-peer applications using attribute-based encryption. Journal of Information and Telecommunication, 5(4): 440-459. https://doi.org/10.1080/24751839.2021.1941574

[47] Han, D., Pan, N., Li, K.C. (2020). A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection. IEEE Transactions on Dependable and Secure Computing, 19(1): 316-327. https://doi.org/10.1109/tdsc.2020.2977646

[48] Tonge, A., Caragea, C. (2019). Privacy-aware tag recommendation for accurate image privacy prediction. ACM Transactions on Intelligent Systems and Technology (TIST), 10(4): 1-28. https://doi.org/10.1145/3335054

[49] Tonge, A., Caragea, C. (2020). Image privacy prediction using deep neural networks. ACM Transactions on the Web (TWEB), 14(2): 1-32. https://doi.org/10.1145/3386082

[50] Squicciarini, A.C., Novelli, A., Lin, D., Caragea, C., Zhong, H. (2017). From tag to protect: A tag-driven policy recommender system for image sharing. In 2017 15th Annual Conference on Privacy, Security and Trust (PST), Calgary, AB, Canada, pp. 337-33709. https://doi.org/10.1109/PST.2017.00047

[51] Pramitha, F.N., Hadiprakoso, R.B., Qomariasih, N. (2021). Twitter bot account detection using supervised machine learning. In 2021 4th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, pp. 379-383. https://doi.org/10.1109/ISRITI54043.2021.9702789

[52] Yu, J., Kuang, Z., Zhang, B., Zhang, W., Lin, D., Fan, J. (2018). Leveraging content sensitiveness and user trustworthiness to recommend fine-grained privacy settings for social image sharing. IEEE Transactions on Information Forensics and Security, 13(5): 1317-1332. https://doi.org/10.1109/tifs.2017.2787986

[53] Kashani, S.M.Z., Hamidzadeh, J. (2020). Feature selection by using privacy-preserving of recommendation systems based on collaborative filtering and mutual trust in social networks. Soft Computing, 24(15): 11425-11440. https://doi.org/10.1007/s00500-019-04605-z

[54] Hossain, M.S., Alhamid, M.F., Muhammad, G. (2018). Collaborative analysis model for trending images on social networks. Future Generation Computer Systems, 86: 855-862. https://doi.org/10.1016/j.future.2017.01.030

[55] Geng, X., Zhang, H., Bian, J., Chua, T.S. (2015). Learning image and user features for recommendation in social networks. In Proceedings of the IEEE International Conference on Computer Vision, Santiago, Chile, pp. 4274-4282. https://doi.org/10.1109/ICCV.2015.486

[56] Dhivakar, B., Sridevi, C., Selvakumar, S., Guhan, P. (2015). Face detection and recognition using skin color. In 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), Chennai, India, pp. 1-7. https://doi.org/10.1109/ICSCN.2015.7219848

[57] Anila, S., Devarajan, N. (2010). Simple and fast face detection system based on edges. International Journal of Universal Computer Sciences, 1(2): 54-58.

[58] Zhang, H., Xie, Y., Xu, C. (2011). A classifier training method for face detection based on AdaBoost. In Proceedings 2011 International Conference on Transportation, Mechanical, and Electrical Engineering (TMEE), Changchun, China, pp. 731-734. https://doi.org/10.1109/TMEE.2011.6199306

[59] Filali, H., Riffi, J., Mahraz, A.M., Tairi, H. (2018). Multiple face detection based on machine learning. In 2018 International Conference on Intelligent Systems and Computer Vision (ISCV), Fez, Morocco, pp. 1-8. https://doi.org/10.1109/ISACV.2018.8354058

[60] Wang, M., Deng, W. (2021). Deep face recognition: A survey. Neurocomputing, 429: 215-244. https://doi.org/10.1016/j.neucom.2020.10.081

[61] Middleton, S.E., Kordopatis-Zilos, G., Papadopoulos, S., Kompatsiaris, Y. (2018). Location extraction from social media: Geoparsing, location disambiguation, and geotagging. ACM Transactions on Information Systems (TOIS), 36(4): 1-27. https://doi.org/10.1145/3202662

[62] Shahzad, H.M., Bhatti, S.M., Jaffar, A., Akram, S., Alhajlah, M., Mahmood, A. (2023). Hybrid facial emotion recognition using CNN-based features. Applied Sciences, 13(9): 5572. https://doi.org/10.3390/app13095572

[63] Boyd, D., Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. Information, Communication & Society, 15(5): 662-679. https://doi.org/10.1080/1369118X.2012.678878

[64] Eslami, M., Rickman, A., Vaccaro, K., Aleyasen, A., Vuong, A., Karahalios, K., Sandvig, C. (2015). "I always assumed that I wasn't really that close to [her]" Reasoning about Invisible Algorithms in News Feeds. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, San Jose, California, USA, pp. 153-162. https://doi.org/10.1145/2702123.2702556

[65] Farajtabar, M., Yang, J., Ye, X., Xu, H., Trivedi, R., Khalil, E., Zha, H. (2017). Fake news mitigation via point process based intervention. In International Conference on Machine Learning, Sydney, Australia, pp. 1097-1106.

[66] Desai, A., Kalaskar, S., Kumbhar, O., Dhumal, R. (2021). Cyber bullying detection on social media using machine learning. In ITM Web of Conferences, p. 03038. https://doi.org/10.1051/itmconf/20214003038

[67] Lei, K., Liu, Y., Zhong, S., Liu, Y., Xu, K., Shen, Y., Yang, M. (2018). Understanding user behavior in Sina Weibo online social network: A community approach. IEEE Access, 6: 13302-13316. https://doi.org/10.1109/ACCESS.2018.2808158