ETDT

Emerging Trends in Digital Transformation

Volume-2, Issue-1, January-March 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-16***

ENSURING IMAGE PRIVACY AND USER TRUST IN SOCIAL NETWORKING PLATFORMS

[#1]REVELLI KISHOR KUMAR, ***Assistant Professor,***
[#2]SHABANA BEGUM, ***Assistant Professor,***
Department of Computer Science & Engineering,
Mother Theressa College of Engineering & Technology, Peddapalli, Telangana.

ABSTRACT: The rapid growth of social media has increased photo sharing, raising concerns about the exposure of personal and sensitive information. When images contain multiple individuals, protecting their privacy becomes essential. This paper presents a trust-based approach for secure sharing of jointly owned photos. The proposed method anonymizes images by masking the identities of individuals at risk, with the level of anonymization determined by the publisher's privacy requirements and the trust level of the recipient. A greedy threshold selection technique is used to balance privacy protection and image usability. Experimental results show that the proposed method effectively reduces the risk of privacy leakage while maintaining acceptable data quality, enabling safer and more reliable photo sharing in social media platforms.

Index Terms*—Social trust, anonymization, privacy preserving, photo sharing, online social networks.*

1. INTRODUCTION

The rapid growth of social networking platforms has transformed the way people communicate, interact, and share personal content online. Among the various forms of shared media, images represent a major portion of user-generated content. While photo sharing enhances social connectivity and user engagement, it also raises significant concerns regarding privacy and data security. Images often contain sensitive visual information such as facial identity, location details, personal relationships, and contextual clues, which may be misused if accessed by unauthorized individuals.

Privacy risks become more complex when a single image includes multiple individuals. In such cases, the responsibility of protecting privacy extends beyond the uploader to all persons appearing in the photo. Unauthorized sharing, identity exposure, facial recognition misuse, and unintended data inference can lead to personal, social, and even financial consequences. As a result, ensuring image privacy has become a critical requirement for modern social networking environments.

In addition to privacy protection, user trust plays a vital role in the continued use of social media platforms. Users are more likely to share content when they feel confident that their personal information is handled securely and that appropriate controls are available. However, traditional privacy settings often rely on manual configuration and do not adequately consider factors such as the sensitivity of image content or the trustworthiness of the recipient.

To address these challenges, there is a need for intelligent mechanisms that can automatically protect sensitive visual information while maintaining the usability of shared images.

DOI: https://doi.org/10.5281/zenodo.19016560

Privacy-preserving techniques such as image anonymization, access control, and trust-based sharing strategies can help balance data accessibility and protection. By integrating privacy management with trust evaluation, social networking systems can reduce the risk of information leakage and improve user confidence.

This paper focuses on developing approaches that ensure image privacy while strengthening user trust in social networking platforms. The proposed framework aims to support secure content sharing by combining privacy protection techniques with trust-aware decision mechanisms, enabling safer and more reliable social media interactions.

2. RELATED WORK

Privacy computing focuses on the use of software techniques to protect personal information while enabling controlled data sharing. With the rapid growth of online photo sharing, several studies have addressed the risk of personal information exposure and the trade-off between privacy protection and the benefits of content sharing.

Early research introduced image-level privacy controls; however, these approaches were limited in handling detailed privacy requirements. To improve protection, face-based access control mechanisms were proposed, allowing visibility restrictions based on the identities of individuals present in an image.

Ilia et al. developed a face recognition–based privacy framework, which was later extended by Vishwamitra et al. to include object recognition along with facial detection, enabling more comprehensive content-aware privacy control. In addition, distributed consensus-based approaches have been explored to improve the efficiency of multi-user privacy decision making for shared images.

Several studies have also examined privacy risks associated with facial features and identity disclosure in social media. These findings highlight the need for automated mechanisms that can incorporate user privacy preferences into image-sharing systems. However, managing privacy becomes challenging when multiple individuals in a photo have different privacy requirements, often leading to conflicts that are difficult to resolve using traditional rule-based methods.

To address observer privacy, approaches such as wearable devices and offline tagging (Offlinetags) have been proposed, allowing individuals to communicate their privacy preferences during image capture. Despite their potential, these methods face practical limitations related to usability and user adoption.

Although significant progress has been made in face recognition and image analysis, accurately interpreting user-generated images in large-scale social networking environments remains a challenge. Many existing solutions are not designed for real-world deployment or intensive usage. Recent studies suggest that contextual analysis, such as identifying individuals who frequently appear together or at the same locations, can improve privacy decision-making.

Based on these limitations, the current work focuses on scenario-level privacy protection, which considers the overall context of image sharing rather than applying rules only to specific faces or individual images. This approach aims to provide more practical and

DOI: https://doi.org/10.5281/zenodo.19016560

scalable privacy management for social networking platforms.

TABLE I
FACTORS ON WHETHER TO SHARE PHOTO

Factors	China	USA	Total
Temporal Factor			
Weekdays 8:00-18:00	84(24.8%)	18(12.2%)	102(20.9%)
Weekdays 18:00-8:00	142(41.9%)	44(29.7%)	186(38.2%)
Weekends	**210(61.9%)**	**122(82.4%)**	**332(68.2%)**
Holidays	**207(61.1%)**	**116(78.4%)**	**323(66.3%)**
Spatial Factor			
Daily outdoor activity	115(33.9%)	13(8.8%)	128(26.3%)
Restaurant	72(21.2%)	24(16.2%)	96(19.7%)
Private gathering(e.g. party)	**237(69.9%)**	**113(76.4%)**	**350(71.9%)**
Worship	76(22.4%)	79(53.4%)	155(31.8%)
Bar or nightclub	95(28.0%)	84(56.8%)	179(36.8%)
Gym	60(17.7%)	24(16.2%)	84(17.2%)
Public transit	54(15.9%)	22(14.9%)	76(15.6%)
Workplace	159(46.9%)	83(56.1%)	242(49.7%)
Hospital	119(35.1%)	**119(80.4%)**	238(48.9%)
Public gathering(e.g. movie)	58(17.1%)	33(22.3%)	91(18.7%)
Other	15(4.4%)	7(22.3%)	22(4.5%)
Total # of Responses	339(100%)	148(100%)	487(100%)

When paired with location-based services, this approach raises concerns about the security of users' private data, including information about their relationships with others, which could increase the precision of face matching. However, this tactic may make handling onlookers more challenging. It can be difficult to decide how many photos to utilize in a deep feature-based method to condense a big face database into a more manageable collection of candidate shots.

3. PRIVACY-PRESERVING PHOTO SHARING

The system overview can be used to define one of HideMe's three potential user roles. The word "photo-uploader" has become popular to describe someone who regularly engages in this type of internet activity. Consider Alice, who regularly posts pictures on different social networking sites. A person who must understand how to protect certain information creates their own privacy restrictions. For instance, Bob's photo-sharing profile. He will be able to limit who can view his images to his pals by accepting Alice's friend request. Alice, the person who uploads the photos, is ultimately responsible for determining her own privacy preferences. An image viewer is anyone who has registered for an OSN and has access to the photos that other users have shared, posted, and discussed. For example, Dave is able to read pictures. He says he wants to view the photo that Alice sent him. In addition, Dave is totally hostile toward Alice yet being polite to Bob. In compliance with company rules, Bob has taken precautions to make sure Dave can't recognize him in the attached photo. In order to preserve Bob's privacy, the HideMe program would conceal his traits before disclosing them to Dave.

DOI: https://doi.org/10.5281/zenodo.19016560

Volume-2, Issue-1, January-March 2026 ISSN: 3107- 4308 Paper ID: ETDT-V2-I1-16

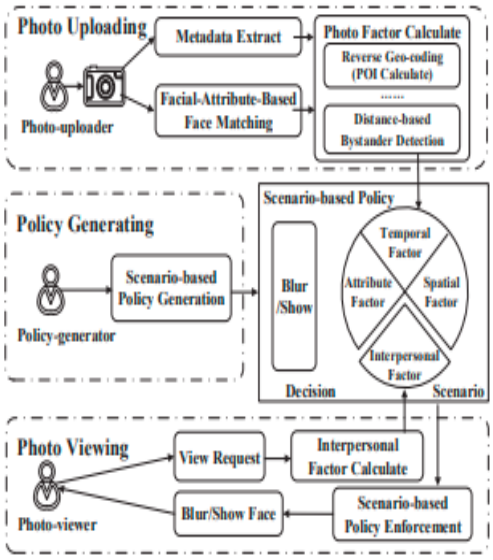

Fig. 1. Data flow of HideMe

As mentioned in Section III-B, our HideMe application can automatically execute the policies of policy-generators, so users don't need to do anything additional before submitting images. This feature will allow both users and remote viewers to meet their privacy needs. Software development consists of three stages: conceptualization, design, and implementation. The process consists of research, design, programming, testing, and maintenance. The three major features of the HideMe website are adding photos, creating rules, and viewing pictures. Figure 1 illustrates this occurrence. HideMe must first organize the face data after gathering image information before calculating the previously stated attributes. HideMe first parses the Exif data, which contains details such as the digital zoom ratio, the focal length in 35mm terms, the date and time of capture, the camera's latitude and longitude, and more. Every time a face is identified in an image, its exact location and dimensions are recorded. To satisfy the needs of multiple clients, we have created a face matching module that considers each person's unique facial attributes. Among other kinds of data, dates, times, locations, and coordinates can all be represented with the help of direct variables. Points of interest (PoIs) and photography distance are important considerations when organizing your photos. Theoretically, the distance information should allow for precise local location identification. Each person in the photo has the option of revealing or concealing their face. However, it could be time-consuming and tiresome to come up with rules for every shot that could be made. HideMe creates hypothetical circumstances instead of rules for each individual photo, allowing policy generators to decide for themselves whether to hide or disclose their facial features. A computer called HideMe is capable of precisely recognizing and extracting faces from pictures. An online social network (OSN) system retrieves matching user identifying information to start the process of assigning identifiable individuals to the context of an uploaded photo. This approach can help policy generators save time by not creating rules for each image separately. Every face in the user-requested photo is subject to restrictions by the HideMe system. HideMe pauses to assess the interpersonal factors between the new user and the photo viewer before allowing them to

DOI: https://doi.org/10.5281/zenodo.19016560

Volume-2, Issue-1, January-March 2026 ISSN: 3107- 4308 Paper ID: ETDT-V2-I1-16

approach a policy generator to request a policy. The way the scenario is customized to meet your needs is what matters most.

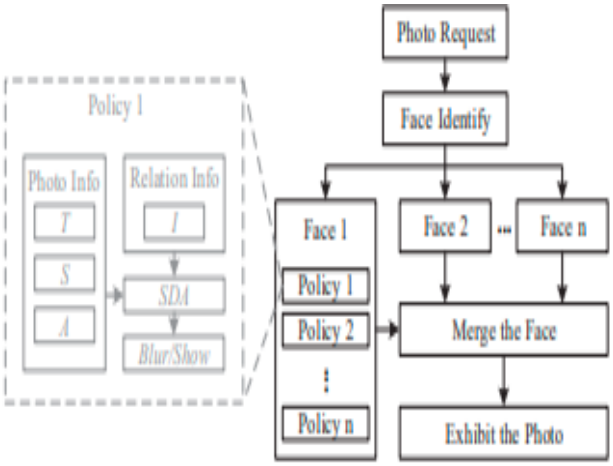

Fig. 2. We'll examine the control's process for choosing and executing the user-defined policy authorizations below. The Hide Me method combines multiple user-facing images into a single image

4. PERFORMANCE EVALUATIONS

collecting data in order to exchange pictures on OSNs. HideMe was tested on an operating system network (OSN) that closely mimics an actual OS network. A significant amount of the data used in this research came from the Stanford SNAP11 dataset and Facebook. With 4,039 nodes and 88,227 edges, the dataset was used to create a basic social network. Using their iPhones, twenty people (shown by red nodes) and their friends (represented by blue nodes) took two thousand pictures in record time. People who are acquainted through acquaintances of acquaintances are shown by white nodes. The obtained user's photo sharing dataset is created by combining facial data and pseudonyms. These characteristics are employed in face filtering. The Facial-attribute Classifier uses the CelebA dataset to train its ABCNN network. The dataset has 202,599 photographs in total, with an average of 20 photos per celebrity out of 10,177 individuals. Ten percent of the images in the CelebA dataset are used for practical applications, twenty percent are used for accuracy assessments, and seventy percent are used for teaching. The CelebA dataset already has forty different facial features with binary labeling. We believe that 16 of the 40 traits would make useful filters, so we decided to investigate them further. We chose to focus on these specific characteristics because there is minimal individual variation in them. We evaluate each hypothetical facial feature's ability to classify face photos in Figure 3(b). These 16 characteristics produce an accuracy percentage of 88.53% on average. We debated sixteen different facial features before settling on "Male," "Young," "Eyeglasses," and "Bald."

DOI: https://doi.org/10.5281/zenodo.19016560

Volume-2, Issue-1, January-March 2026 ISSN: 3107- 4308 Paper ID: ETDT-V2-I1-16

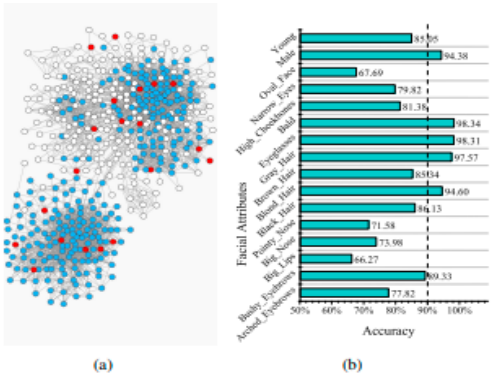

Figure 3 illustrates our photo-sharing OSN, which consists of 500 nodes reflecting facial image filtering properties from the CelebA dataset. Save (a). Because they consistently and accurately identify common traits within a specific domain, these criteria were chosen. According to the results, 98.31% of people with bald areas, 85.04% of young people, 94.37% of men, and 98.34% of those wearing glasses were correctly classified.

A. Evaluations of HideMe

1) An inexpensive laptop that can run the HideMe program is a 1A Thinkpad T430u, which has 16GB of RAM and an Intel Core i7-3517U processor. One way to measure HideMe's effectiveness is to look at how much time users spend uploading and viewing photographs. transferring images to a mobile device or computer. The HideMe software was used to process one hundred participant images that were selected at random. Using face-recognition software, this operation takes an average of 7.5824 milliseconds per image. The time needed to extract and identify photo variables makes HideMe's 2.3 ms completion time much longer than that of the Face/Off app. Unlike data extraction, which takes 7.4763 ms, calculating the distance between two pictures only takes 0.0035 ms. The visual media are the main focus. By taking into account the worst-case situations, the overhead for a collection of one hundred randomly chosen photos—some of which feature blurred faces—is calculated. Figure 4 shows that adding the blur function while viewing the image takes 73 milliseconds. However, we may be able to save 52 milliseconds if we utilize the blur option beforehand.

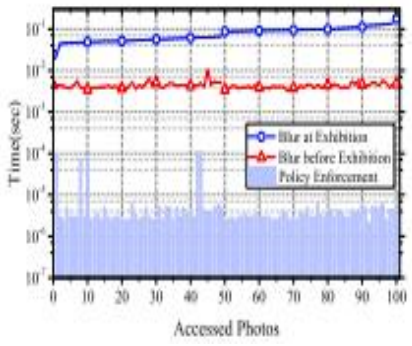

Fig. 4. The total time required for a photo

DOI: https://doi.org/10.5281/zenodo.19016560

Volume-2, Issue-1, January-March 2026 ISSN: 3107- 4308 Paper ID: ETDT-V2-I1-16

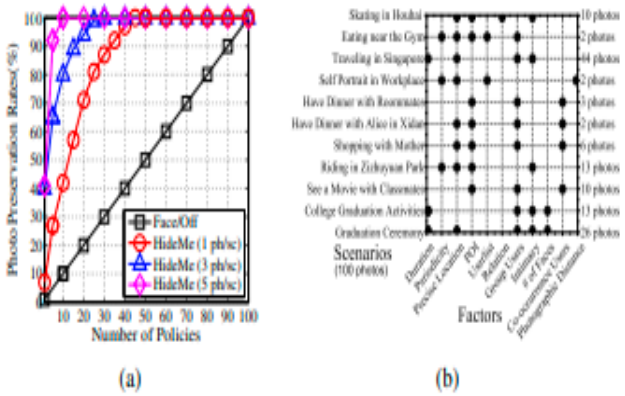

Figure 5: Assessing the effectiveness of rules The alternative policy generating approach is more effective but requires more space because it keeps the picture block associated with each hidden face. When the snap has more than one subject, this picture block is significantly larger than the matching information or tag. The photo preservation rate is the number of photos that have survived. being able to advance and get better.

In this research, we investigate how adding more rules and users affects the system's scalability. We select the test images from a different group of one hundred photos that have three people and five or more facial attributes. Figure 4 illustrates that the amount of policies added results in a delay of roughly 0.008 milliseconds. There is a significant distinction. By asking users to apply policies to a collection of 100 images using either the Face/Off or HideMe methods, the effectiveness of HideMe was evaluated. The results were then compared.

The results show that HideMe outperforms Face/Off. There was a substantial correlation between the number of hypothetical options examined and the policy's magnitude. Figure 5(a) displays three representative participants together with the distribution of 1, 3, and 5 photos across the three situations. HideMe has significantly higher photo preservation rates for shared images than its competitors because of its less stringent criteria. According to Figure 5(b), which depicts the scenario generation process, employing abstracting techniques may improve the success rate of photo preservation.

B.Facial-attribute-based Face Matching We demonstrate the effectiveness of the strategy by applying face filtering to 1,000 randomly selected photos from the CelebA dataset. Approximately 2,071 persons meet the face-matching requirements. This small subset represents barely 20% of the overall population of 10,177. Furthermore, 95% of the 1,000 selected face images had potential matches on the list. Face screening became commonplace. We were able to gauge the effectiveness of face filtering by dividing the faces into two groups.

The first section, "group all," consists solely of headshots. The next step is to give the set a name that appropriately conveys the significance of the selected physical attributes. The "person id" will be allocated to an image of a face that has the attributes Male=-1, Young=-1, Eyeglasses=-1, and Bald=-1. The second half contains sixteen subcategories since each of the four face attributes used for face filtering is assigned a binary value. We will then go over a variety of techniques to improve the efficiency of face matching and filtering. We can determine whether face filtering is more effective than searching the entire database by

DOI: https://doi.org/10.5281/zenodo.19016560

comparing the two methods. To assess the effectiveness of face matching, we employ face filtering and a larger database size.

A random face-matching algorithm was fed one hundred images of CelebA users. Table 2 demonstrates that face screening outperforms face matching when examining the complete database. As database volumes increase, face filtering-based face matching outperforms traditional face matching in every way.

The effectiveness of face-based contests. This research compares a proposed feature-based face matching method with the state-of-the-art face recognition system.

Table 2 Scalability Evaluation Of Face Filtering

Group	The number of persons in the database				
	1000	2000	4000	8000	10000
'group all'	223.57	250.33	296.86	353.98	424.89
facial attributes	193.08	197.63	200.68	226.94	246.42

Table.3 the accuracy comparison: facial-attribute-based face matching v.s. Tencent bestimage

Method	Database: 4000 persons		Database: 10000 persons	
	Time Cost	Accuracy	Time Cost	Accuracy
Facial-attribute-based Face Matching	200.68 ms	95.3%	246.42 ms	94.7%
Tencent Bestlmage	296.86 ms	97.3%	424.89 ms	96.7%

Tencent Best Image uses kNN-approximated deep characteristics to achieve face matching. The Tencent-created Best Image k = 5 facial recognition algorithm was applied in this research. The face traits of 150 randomly selected individuals from the CelebA dataset are compared to those of two different databases, one including 4,000 individuals and the other containing 10,000. Information about 150 participants in the research is stored in two databases. Table 3 demonstrates that the suggested face attribute-based face matching method outperforms Tencent Best Image with only a slight decrease in accuracy. Keep in mind that it will be very beneficial to cut operating time in half if the database size grows, as it would in real-world apps like Facebook.

5.CONCLUSIONS

We developed and introduced HideMe, a privacy-preserving technology for online photo sharing in social networks, and conducted extensive testing. HideMe users utilize visuals to communicate important information. Instead of creating many limitations for every photo, the system provides linked friends with a single setup using a scenario-based access control paradigm. HideMe is a secure site for sharing self-portraits because of its masking capabilities and customizable privacy settings. To help with localization and privacy protection for those in the vicinity, a distance-based algorithm was created. No facial recognition software can match HideMe in terms of effectively concealing users' identity. The evaluation's conclusions indicated that the endeavor was successful.

DOI: https://doi.org/10.5281/zenodo.19016560

REFERENCES

[1] Abokhodair, N., Hodges, A., Vieweg, S.: Photo sharing in the arab gulf: Expressing the collective and autonomous selves. In: Proc. of ACM CSCW 2017

[2] Aditya, P., Sen, R., Druschel, P., Oh, S.J., Benenson, R., Fritz, M., Schiele, B., Bhattacharjee, B., Wu, T.T.: I-pic: A platform for privacycompliant image capture. In: Proc. of ACM MobiSys 2016

[3] Aronov, B., Efrat, A., Li, M., Gao, J., Mitchell, J.S., Polishchuk, V., Wang, B., Quan, H., Ding, J.: Are friends of my friends too social? limitations of location privacy in a socially-connected world. In: Proc. of ACM MobiHoc 2018

[4] Fogues, R.L., Murukannaiah, P.K., Such, J.M., Singh, M.P.: Sharing policies in multiuser privacy scenarios: Incorporating context, preferences, and arguments in decision making. ACM Transactions on ComputerHuman Interaction 24(1), 5 (2017)

[5] Griffin, P.F.: The correlation of english and journalism. The English Journal 38(4), 189–194 (1949)

[6] Guo, Y., Yin, L., Liu, L., Fang, B.: Utility-based cooperative decision in cooperative authentication. In: Proc. of IEEE INFOCOM 2014 [7] Hu, H., Ahn, G.J., Jorgensen, J.: Multiparty access control for online social networks: model and mechanisms. IEEE Transactions on Knowledge and Data Engineering 25(7), 1614–1627 (2013)

[8] Ilia, P., Polakis, I., Athanasopoulos, E., Maggi, F., Ioannidis, S.: Face/off: Preventing privacy leakage from photos in social networks. In: Proc. of ACM CCS 2015

[9] W. G. Mangold and D. J. Faulds, “Social media: The new hybrid element of the promotion mix,” Bus. Horiz., vol. 52, no. 4, pp. 357–365, 2009.

[10] A. M. Kaplan and M. Haenlein, “Users of the world, unite! The challenges and opportunities of social media,” Bus. Horiz., vol. 53, no. 1, pp. 59–68, 2010.

[11] J. A. Obar and S. S. Wildman, “Social media definition and the governance challenge-an introduction to the special issue,” Telecommun. Policy, vol. 39, pp. 745–750, 2015.

[12] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, “Information security in big data: Privacy and data mining,” IEEE Access, vol. 2, pp. 1149–1176, 2014.

[13] N. Senthil Kumar, K. Saravanakumar, and K. Deepa, “On privacy and security in social media a comprehensive research,” Procedia Comput. Sci., vol. 78, pp. 114–119, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050916000211