ISSN No:-2456-2165

Social P Share – A Privacy Preserved Sharing Application

Angel Mary
Student, Dept. of Computer Science and Engineering,
Sahrdaya College of Engineering and Technology,
Thrissur, Kerala, India

Archana P S
Student, Dept. of Computer Science and Engineering
Sahrdaya College of Engineering and Technology
Thrissur, Kerala, India

Deepthi Pradeep K
Student, Dept. of Computer Science and Engineering,
Asst. Professor, Dept. of Computer Science and Engineering

Linnet Tomy
Sahrdaya College of Engineering and Technology
Thrissur, Kerala, India

Abstract:- Development of social media has created a great opportunity for the users to share photos, textual messages or contents and videos to maintain a social connection with each other in Online Social Networks. However, a photo may contain rich information like Identity of the person, number plates etc. which makes it easier for malicious viewer to interfere in these sensitive information. Sharing a photo involves multiple users, so the publisher should take into account of the privacy of all related users. The main aim of this paper is to anonymize the photo so the users who may experience privacy loss due to the photo sharing will not be identified. We use Haar Cascade which is a machine learning based approach where a lot of positive and negative images are used to train the classifier. This technique is used to detect the faces and number plates. A User Identification Lock is provided before sharing or posting a content so as to ensure whether the photo or other textual information is posted by the actual owner or not. This project ensures the users personal information and other important contents are not violated.

Keywords:- *Anonymization, Online Social Networks, Haar Cascade.*

I. INTRODUCTION

Online media empowers individuals to associate with one another by making and sharing data, which has become a significant piece of our everyday life. Users of online media services make a tremendous measure of data in types of text posts, advanced photographs or recordings. Such client produced content is the soul of online media, However, user produced content typically includes delicate data, which implies the sharing of such substance may affect their security.

Some well-known online communication services, for example, Instagram, Facebook, and Pinterest are fundamentally intended for photo sharing. Contrasted with literary information, photographs can convey more itemized data to the watcher, which is dangerous to the person's protection. Additionally, the foundation data contains in a photograph might be used by a malicious watcher to deduce one's data. On the great side, it is more helpful for a user to shroud their informative data, without harm by anonymization.

In this paper, we study the protection issue brought by photograph sharing up in Online Social Networks (OSNs). Security strategies in OSNs are about how a user's data will be investigated by the specialist cooperator called the service provider, and through which techniques a user can control the extent of data sharing. Most OSNs offer a security setting capacity to their clients. A user can indicate, typically depend on his associations with others, where clients are permitted to get to the photograph the user shares. It should be noticed that the photograph shared by a user may relate or may affect other users.

In recent years, face recognition has been criticized and is considered to be the most promising application in the field of image analysis. Face detection can be regarded as an important part of the face recognition operation. Mandatory computing resources are concentrated in the image area containing the face. Due to differences in the posture, expression, position and direction of the face, skin color, the existence of the lens, camera gain and image resolution, the process of recognizing the face in the image is very complicated.

Object recognition is one of the computer technologies that processes image processing and computer vision and interacts with the recognition of object instances (such as faces, buildings, trees, cars, etc.). The main purpose of the face detection algorithm is to determine whether there is a face in the image. OpenCV is a library with programming functions mainly for real-time computer vision. OpenCV is a multi-platform library, we can use it to improve real-time computer vision applications. The focus is on image processing; video recording and analysis, including facial recognition and object recognition functions. People can automatically recognize faces every day without any effort. Although this seems to be a very simple task for us, it is difficult for the computer because there are many variables

that affect the accuracy of the method, such as: lighting changes, low resolution, occlusion, etc. In computer technology, face recognition is basically the task of identifying people based on their photos. In the past two decades, it has become very popular, mainly due to the newly developed technology and the high quality of modern video/cameras. Local Binary Pattern is very powerful operator that characterizes the pixels in the image by setting a threshold for the neighborhood of each pixel and treating the result as a binary number. Combining LBP with histogram, we can use a simple data vector to represent facial images.

II. PROBLEM DEFINITION

Social platforms have grown to play a vital role in our day to day life. Online interpersonal businesses and organizations OSNs, like Facebook, Google and other social media platforms are normally meant to make capable people to component individual and open facts and make social associations with companions, colleagues, individuals having like-position, family, or even with outsiders. To be careful that user's truths, direction on top of things has changed to a head element motive of OSNs. Be that it can finally end up the evidently eternal record as soon as some photograph/picture is posted. Late results may be risky, people may also utilize it for diverse sudden purposes. For example a published or posted may also find the mafia courting of with any big names.

Users switch the image and tag different people no matter the truth that they're keen or now no longer inclined to be a chunk of transferred photo/content. At the factor whilst different people are labelled the condition, seems to be greater convoluted. The client posting or transferring the photo is genuinely subconscious of the results that emerge for the person who is included in the picture. Right now no person can prevent such unavoidable condition. We really need to manage these activities to restrict the risks of images being labelled or transferred. Rather than forcing obstacles over such occurrences or increasing security, locations like Facebook and Instagram are urging people to get into such matters more.

III. RELATED WORK

The authors Lei Xu and Ting Bao briefly explained the Trust Based Privacy Preserving Photo Sharing in Online Social Network. Social media enabled people to create huge information in the form of texts, images, videos etc. and privacy is a main concern. This approach was implemented to deal with the privacy concerns that happen while sharing photos in OSN platforms. For this the anonymization technique was used i.e. the original photo is anonymized so the users will not be identified from the anonymized photo and does not suffer much privacy loss.

The trust here was evaluated based on the level of users privacy loss. The user who wants to share the photos will be temporarily held by the service provider. The service provider estimates the privacy loss that has brought to the stakeholder due to the sharing of photo is totally based on the trust relationship between the users. The trust values utilized between the users determine whether their privacy will be protected or not.

Authors D. Ko, S. Choi, J. Shin, P. Liu and Y. Choi discussed the method Structural Image De-identification in Privacy Preserving Deep Learning. This approach deals with the data leakage that happens when deep learning models are trained in a shared environment. Structural image de-identification is a vector driven approach which is used for privacy preserving deep learning on object classification. This prevents an unauthorized personnel to access the private information existing in a training image data.

In this method the structural shape is modified so it will not be easily recognized by human. They used the vector graphics file concept ie, the original image is transferred into vector graphics file. The operation involves three main steps. First step is the Vectorization ie, transformation of original raster image into vector graphics file. Second step is the position OPE, where OPE(Order Preserving Encryption) is partially applied on vector graphics file. The last step is Rasterization. In this the position shifted vector graphics file is transferred into de-identified raster graphics image. In order to measure the performance of this approach, authors used GPU server. Then for deep learning performance evaluation CIPHER-10 was used. From this approach we observed larger the size of original raster graphics image is, the more accurate the classification of vector graphics image is. When the photo length is greater than 8x8, then the safety of this technique is a good deal and stronger against few attacks.

Tianliang Liu and Junwei Wan Luo discussed Sentimental Analysis for brief Graphics Interchange Format Using Visual-Textual Fusion. Studies show that mostly, textual messages are used for sentimental analysis. Video understanding and the gap between texts and videos are the two primary roles of sentiment analysis for short annotated videos. Authors elaborated an effective and integrated sentiment Analysis scheme with Visual Sentiment Score and textual Sentiment Score and combined both of them for the ultimate result. Visual Sentiment Score calculation is done by VGG-16 and C3D network for representation of visual of the given short GIF and passes it to the Convolutional Long Short-Term Memory network. Textual Sentiment Score is calculated by Key Information Extraction and thereafter by Textual Sentiment Perception. It was shown to enhance and improve the visual sentiment representation and efficiently work with the complicated parameters of the visual-textual sentiment function for large amount of upcoming short annotated GIF videos. Various experiments and evaluations were validated to find the accuracy and performance of the proposed method.

The new individual acknowledgment in close to home photographs technique neal2 is clarified by Seong Joon Gracious, Rodrigo Benenson. With the appearance of interpersonal organizations and ready to take picture

catching through modest computerized gadgets, clients share huge measure of individual photographs through on the web. Consequently, perceive individuals in close to home photographs is significant test for PC vision. For human recognizable proof errand, be that as it may, conventional focal point of PC vision has been face acknowledgment and passerby re-ID. Individual acknowledgment in online media photographs sets new difficulties for PC vision, including non-helpful subjects (e.g., in reverse perspectives, strange postures) and incredible changes in appearance. In this strategy new situation neail2, is a blend of neail and deepID2 that emphasis on the time and appearance hole among preparing and testing tests. neail2 is utilizes five signals that is head,face, upper body ,scene and full body.

Two head prompts prepared with additional information hcacd; hcasia is an adjusting open face perceiving informational index and Ten trait prompts hpipa11, upeta5 is utilized for long haul characteristic acknowledgment. Here we construct a basic individual acknowledgment structure that take five highlights from numerous picture areas like full body, chest area, face, head and scene. We present a top to bottom examination of the significance of various highlights as indicated by time and perspective generalizability. All the while, we confirm that our straightforward methodology accomplishes edge result on the PIPA benchmark, ostensibly the biggest online media-based benchmark for individual acknowledgment to date with assorted stances, perspectives, social gatherings, and occasions.

IV. PROPOSED SYSTEM

The proposed system is a privacy-protected photo sharing web application for safe photo uploading to an online social network. The rich data contained in a photograph makes it easier for a vindictive observer to infer sensitive information about the person depicted in the photograph. In order to prevent such situation, we used the technique called Anonymization of images.

We implemented a web application mainly focusing on safer photo uploading by anonymizing the person's face that is recognized through face recognition who feel it inappropriate to post his/her photo in an OSN platform. Anonymization is done here using OpenCV. The detailed functioning of the project is expressed below.

A. Face Recognition

Face acknowledgment is that the errand of distinguishing an all-around identified item as a known or obscure face. Face recognition is a simple task for humans. Our inward highlights (eyes, nose, mouth) or external highlights (head shape, hairline) utilized for a fruitful face acknowledgment. In Face acknowledgment measure, it can choose somebody's face from a group, remove the face from the rest of the scene and contrast it with an information base of put away pictures. so as for this software to figure, it's to understand the way to differentiate between a basic face and therefore the remainder of the background. Face recognition software is predicated on the power to acknowledge a face then measure the varied features of the face.

Local Binary Patterns Histogram algorithm (LBPH) for face recognition is predicated on local binary operator and is one among the simplest performing texture descriptor. They're getting used in entrance control, surveillance systems, Smartphone unlocking etc. We use LBPH to remove highlights from an info test picture and match them with the countenances in framework's information base. It is broadly used in face acknowledgment on account of its computational straightforwardness and discriminative force. The LBPH algorithm may be a part of OpenCV.

B. Anonymization

Anonymization is securing private or delicate data by deleting or scrambling identifiers that associate a person to put away information. Anonymization is the way toward transforming information into a structure that doesn't recognize people. Since sociology is worried about society and human conduct, an anonymization technique to secure the personality of members is basic to moral examination. Similarly, as with assent, arranging anonymization prior to undertaking information assortment produces both better educated assent and a less asset escalated cycle of information anonymization.

Generally, anonymization applies to two sorts of identifiers: immediate and roundabout. Direct identifiers are the undeniable factors like name, address, or phone numbers, which explicitly feature a member. Aberrant identifiers when sorted out could likewise uncover a person, for instance, by cross-referring to occupation, business, and area. First the course records are stacked for the face given for face recognition utilizing Haar cascade identifiers. The face indicator will give you the bouncing box (x, y)-directions of a face in a picture. We then, at that point utilize this data to extricate the face return on initial capital investment itself.

Figure 1: Detection of the face.

Figure 2: Anonymized Image

ISSN No:-2456-2165

Apply the face blurring technique using OpenCV to anonymize the person's face. Using the original *(x, y)*-coordinates from the face detection (i.e., 2.), we can take the blurred/anonymized face and then store it back in the original image as shown in Figure 2 (if you're utilizing OpenCV and Python, this step is performed using NumPy array slicing).The face in the original image has been blurred and anonymized at this point the face anonymization pipeline is complete.

C. Anonymize on Tagging

When you take a fresh photograph with your phone and upload it to social media, it is able to recognize the people in the photo and suggests that you tag them. To begin with, it is the ability to identify a person's or a pet's face. You won't be able to tag someone if you have a part of a face, a silhouette, a strange side angle, or any other shot where a person appears but their face isn't immediately recognizable. The photo uploaded will be held temporarily by the service provider and identify the person through the face recognition technique. After recognizing and then predicting, the recognized users will be tagged automatically. After the tagging, each user that is recognized will receive a request whether to allow posting or to not or an option to anonymize the face. If the person find it revealing he/she can reject further making the image blurred i.e. anonymized.

Figure 3: Accept/Reject the tagged photo.

In Figure 3 shows the image of the tagged person's account notifying whether to accept or reject his photo which is uploaded by another person. If the person clicks accept, the image will be posted in the same way or if it is rejecting the image will be further anonymized.

V. PROJECT DESIGN

A. Architectural Design

The Figure 4 shows the Detection of faces using KNN Classifier and Face Recognition using LBPH Face Recognizer, as Face recognition is one of the main ways to recognize a person based on the facial features provided in the image. When the face is identified, it will be predicted. LBPH algorithm is a part of Open CV.

After the above process Anonymization of Image using the Anonymization Technique is done. Here photos will be anonymized if the recipient find their photo revealing any personal or any sensitive information.

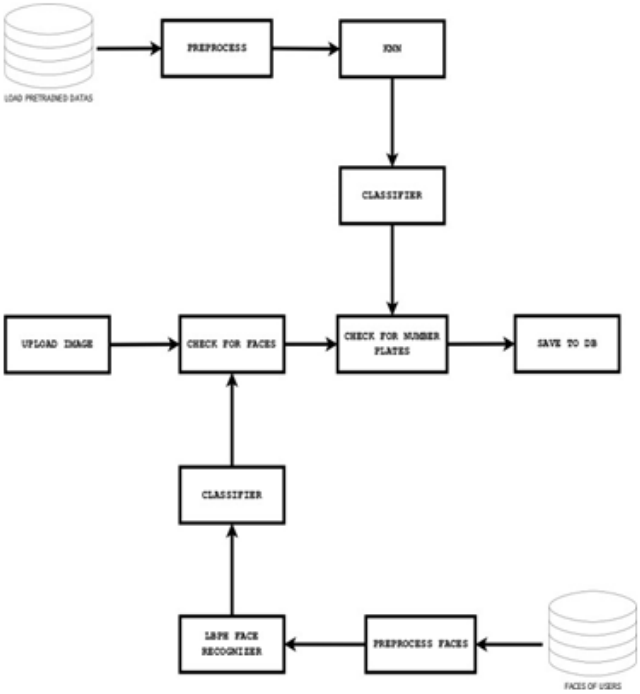

Figure 4 : Architectural Design of the proposed System

B. Flowchart

The given Figure 5 is the flowchart of the proposed system. If the user is new to the application, he/ she will have to undergo the registration process which include giving the required details and an image that can be used for user recognition. If already registered then the user can directly login to the application by face recognition of the user. The faces detected will automatically get stored in the database. When the user gets identified he/she will get the access to the application.

During image uploading, again the user is being recognized in order to make sure that it is done by the actual user and continue posting the image. The faces of the image will be detected and recognized by the service provider and a message will be sent to those who are tagged on. If the person accepts the photo will posted, if not that portion of the image will be anonymized. By this process, we could develop a very secure and trust-based privacy preserving mechanism, where the rich information of the image can be hidden from the public to avoid any intruder to manipulate or misuse.

ISSN No:-2456-2165

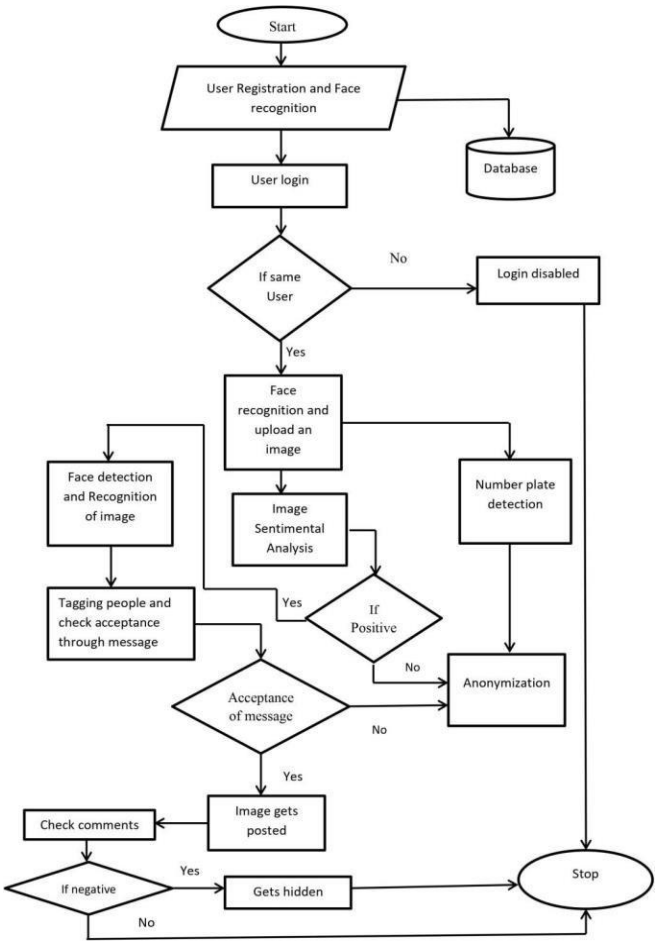

Figure 5 : Flowchart of the proposed system

VI. RESULT

Final result is the anonymization of the necessary image. The image gets anonymized once the user of the account rejects the image since he/she finds the image revealing personal identification. The blurring can be adjusted accordingly as shown in the Figure 6. Finally, the user can protect their face and avoid malicious attack.

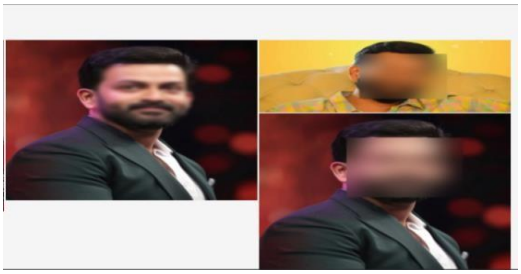
Figure 6 : The anonymized image

VII. CONCLUSION

Sharing co-owned photos in online social networks face many privacy issues. To deal with such a privacy issue, proposed system consists of a privacy-preserving photo sharing mechanism. We mainly focus on the information exchange between the publisher and the receiver. Since in practice, users usually share a photo with multiple users at the same time, we hope to investigate the one-to-many situation in future work. There are many existing methods of adjusting the threshold in order to detect the loss of confidentiality and determine the trust value. One of these threshold adjustment methods can be considered greedy method, because publishers prefer to choose the threshold that allows them to get the maximum instant spend. Due to the correlation between the loss of confidentiality and the trust value, the choice of the current threshold will affect the future profit of the publisher. In future work, we'd like to investigate how to modify the tuning method so as to achieve a better result in finding the privacy loss a user had faced.

REFERENCES

[1]. L. Xu, T. Bao, L. Zhu and Y. Zhang,"Trust-Based Privacy-Preserving Photo Sharing in OnlineSocial Networks," in IEEE Transactions on Multimedia, vol. 21, no. 3, pp. 591-602, March2019.

[2]. D. Ko, S. Choi, J. Shin, P. Liu and Y. Choi, "Structural Image De-Identification for Privacy-PreservingDeepLearning,"inIEEEAccess,vol.8,pp.1 19848-119862, 2020.

[3]. T. Liu, J. Wan, X. Dai, F. Liu, Q. You and J. Luo,"Sentiment Recognition for Short Annotated GIFs Using Visual-Textual Fusion," in IEEE Transactions on Multimedia, vol. 22, no. 4, pp. 1098-1110, April2020.

[4]. Fiesler,M.Dye,J.L.Feuston, C. Hiruncharoenvate, C. Hutto, S. Morrison, P. Khan pour Roshan, U. Pavalanathan, A. S. Brackman, M. De Choudhury, and E. Gilbert, "What (or who) is public?: Privacy settings and social media content sharing," in Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, March 2017, pp.567–580.

[5]. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in Proceedingsofthe 18th ACMInternationalConference on World Wide Web, April 2009, pp.521–530.

[6]. S. K. N, S. K, and D. K, "On privacy and security in social media a comprehensive study," Procedia Computer Science, vol. 78, pp. 114 – 119, 2016, 1st Interna- tional Conference on Information Security and Privacy 2015.

[7]. H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," December 2011, pp. 103– 112.

[8]. J. M. Such and N. Criado, "Resolving multi-party privacy conflicts in social me- dia," IEEE Transactions on Knowledge and Data Engineering, vol. 28, no. 7, pp. 1851–1863, July 2016.

[9]. J. Yu, B. Zhang, Z. Kuang, D. Lin, and J. Fan, "IPrivacy: Image pri- vacy protection by identifying sensitive objects via deep multi-task learn- ing," IEEE Trans. Inf. Forensics Security, vol. 12, no. 5, pp. 1005–1016,May2017.

[10]. A.K.TongeandC.Caragea,"Imageprivacypredictionusin gdeepfea-tures,"in Proc. 13th AAAI Conf Artif. Intell., 2016, pp.4266–4267.

[11]. Oasis Labs' Dawn Song on a Safer Way to Protect Your Data. Accessed: Jan. 3, 2020. [Online]. Available: https://www.wired.com/story/ dawn-song-oasis-labs- data-privacy-wired25/
[12]. R. Gilad-Bachrach, N. Dowlin, K. Laine, K. Lauter,
[13]. M. Naehrig, and J. Wernsing, ''Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy,'' in Proc. Int. Conf. Mach. Learn., 2016, pp.201–210.
[14]. L. T. Phong, Y. Aono, T. Hayashi, L. Wang, and S. Moriai, ''Privacypreserving deep learning via additively homomorphic encryption,'' IEEE Trans. Inf. Forensics Security, vol. 13, no. 5, pp. 1333–1345, May2018.
[15]. A. Al Badawi, J. Chao, J. Lin, C. F. Mun, J. J. Sim, B.
[16]. H. M. Tan, X. Nan, K.M.
[17]. M. Aung, and V. R. Chandrasekhar, ''The AlexNet moment for homomorphic encryption: HCNN, the first homomorphic CNN on encrypted data with GPUs,'' 2018, arXiv:1811.00778.
[18]. M. Tanaka, ''Learnable image encryption,'' in Proc. IEEE Int. Conf. Consum. Electron.-Taiwan (ICCE-TW), May 2018, pp.1–2.
[19]. W. Sirichotedumrong, T. Maekawa, Y. Kinoshita, and
[20]. H. Kiya, ''Privacypreserving deep neural networks with pixel-based image encryption considering data augmentation in the encrypted domain,'' in Proc. IEEE Int. Conf. Image Process. (ICIP), Sep. 2019, pp.674–678.
[21]. A. Krizhevsky and G. Hinton, ''Learning multiple layers of features from tiny images,'' in Proc. Citeseer, 2009, p.7.
[22]. A. Krizhevsky, I. Sutskever, and G. E. Hinton, ''ImageNet classification with deep convolutional neural networks,'' in Proc. Adv. Neural Inf. Process. Syst., 2012, pp. 1097–1105.
[23]. A. Rozsa, E. M. Rudd, and T. E. Boult, ''Adversarial diversity and hard positive generation,'' in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops, Jun. 2016, pp. 25–32.