IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

Maintaining Privacy on Photo Sharing

Rajat Agrawal[1], Karan Gidwani[2], Dakshayani Kamble[3], Maheshwari Chaudhari[4]

Student, Computer Dept., SAE Kondhwa, Pune, India [1-4]

Abstract: Photo sharing refers to the transfer or publishing of a user's digital photos online and the website which provides such acquaintances offer services such as hosting, uploading, sharing and managing of photos through online system. This function provides the upload and display of images through the websites and applications. The usage of online photo galleries including photo blogs is increased. The photo sharing term can be set up and managed by individual users. It means that other users can view but not essentially download the photos, users being able to select different copy-right options for their photos. Unfortunately, it may reveal users privacy if they are permitted to post, comment, and tag a photo liberally. Communication feature on social network is not secured. Users can not send confidential message through social chat. To address these problem, this project proposes an efficient facial recognition system that can recognize everyone in the photo. Online photo sharing applications have become popular. To share photos with a range of people, it provides users various new and innovative alternatives. The photo sharing feature is incorporated in many social networking sites which allow users to post photo for their loving ones, families and friends. Encryption technique is applied for communication between users. AES algorithm is implemented for encrypting chat. For users of social networking sites such as Facebook, this system focuses on the privacy concerns and needs of the users, at the same time explores ideas for privacy protection mechanisms. By considering users current concerns and behaviors, the tool can be designed as per the user's desire which they can adopt and then can be motivated to use.

Key words: Social network, Photo Privacy, Secure Multi-Party Computation, Collaborative Learning.

I. INTRODUCTION

With the huge popularity of sharing and the vast usage of social networking sites users unknowingly reveal certain kinds of personal information. Social-networking users may or may not have the idea of getting their personal information will be leaked or could profit the malicious attackers and may perpetrate significant privacy breaches. With the extravagancy of technology and services sharing of news, photos, personal taste and information with friends and family has led to an ease. But along with this user privacy should also be taken into consideration. An issue related to privacy with Facebook users has been constantly appearing on international press either because of the company privacy policy or because of user's unawareness of content sharing consequences. Even if the individuals in a photo are not explicitly identified by photo tags, the combination of publicly available information and face recognition software can be used to infer someone identity. These kinds of problems are defined as collateral damage: users unintentionally put their own privacy or their friend's privacy at risk when performing events on SNSs such as Facebook. Encryption is provided for chat application. Security should be provided for communication. User is able to send message in encrypted format. Receiver will receive encrypted file and key. Using key, file can be decrypted and original content is displayed. Even if the individuals in a photo are not explicitly identified by photo tags, the combination of publicly available information and face recognition software can be used to infer someone's identity. These kinds of problems are defined as collateral damage: users unintentionally put their own privacy or their friend's privacy at risk when performing events on SNSs such as Facebook.

II. RELATED WORK

N. Mavridis, w. Kazmi, and p. Toulis. Buddies with faces: how Social networks can beautify face popularity and vice versa. In Computational social community evaluation, computer communications and networks. Springer London, 2010. Study the records of photograph Sharing on social networks and suggest a three realms model: "a social realm, wherein identities are entities, and friendship a relation; 2d, a visible sensory realm, of which faces are entities, and co-prevalence in pix A relation; and third, a physical realm, in which bodies Belong, with physical proximity being a relation." They show that any nation-states are pretty correlated. Given facts in a single realm, we are able to give an amazing Estimation of the connection of the other realm.

Z. Stone, t. Zickler, and t. Darrell. Toward big-scale face recognition using social community context. Stone, t. Zickler, and t. Darrell. Autotagging fb: Social network context improves photo annotation. In computer vision and sample recognition workshops, 2008. The contextual statistics inside the social realm and cophoto dating to do computerized for. They define a Pairwise Conditional Random Area (CRA) version to locate the top-quality joint labeling via maximizing the conditional Density. Especially, they use the present classified pics as the education samples and combine the photo co-occurrence information and baseline for rating to enhance the accuracy of face annotation.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

k. Choi, h. Byun, and ok.-a. Toh. A collaborative face popularity Framework on a social network platform. In automated face gesture reputation, 2008. Speak the distinction between the traditional for system and the for gadget this is designed specifically for osns. They point out that a custom designed for gadget for each person is predicted to be an awful lot greater accurate in his/her own picture Collections.

J. Y. Choi, w. De neve, k. Plataniotis, and y.-m. Ro. Collaborative Face recognition for improved face annotation in personal photo Collections shared on online social networks. Multimedia, ieee Transactions on, 13(1):14–28, 2011. Propose to use multiple personal for engines to Work collaboratively to improve the recognition ratio. Specifically, they use the social context to select the suitable Fr engines that contain the identity of the queried Face image with high probability.

D. Rosenblum. What each person can recognize: the privacy risks of social Networking web sites. Protection privacy, ieee, five (3):40–forty nine, 2007. The privateness leakage caused by the terrible get entry to control of shared facts in web 2.0 is properly studied.

C. Squicciarini, m. Shehab, and f. percent. Collective privacy management in social networks. In proceedings of the 18th international convention on global wide internet. Acme. Propose a recreation-theoretic scheme wherein the privateness rules are collaboratively enforced over the shared statistics. Each person is capable of outline his/her privacy coverage and publicity policy. Handiest while a picture is processed with owner's privateness coverage and co-owner's publicity coverage could it be published.

III. COMPARISON OF EXISTING AND PROPOSED SYSTEM

The comparison between the existing system and the proposed system by considering different parameters is shown in the table below. The existing system provided most of the functionality, but the proposed system is more secure and preserves the privacy of the owner and the co-owner of the photo.

Sr. No.	Parameter	Existing system	Proposed system
1	Auto tag	Yes	Yes
2	Privacy of photo	No	Yes
3	Notification while photo uploading	No	Yes
4	Face detection	Yes	Yes
5	Face recognition	No	Yes
6	OTP generation while log in	No	Yes
7	OTP generation while photo uploading	No	Yes

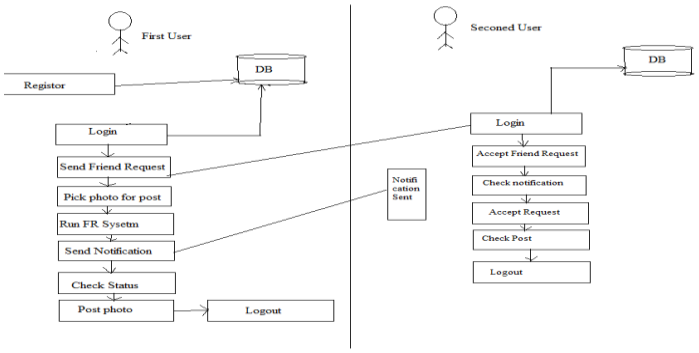
IV. PROPOSED WORK

A. Problem Statement

To propose a facial recognition system for preserving privacy of photo sharing that can recognize everyone in the photo which enables each person in a photo be alert of the posting action and participate in the decision making while posting the photo.

B. System Architecture

A precise structure is been designed to make the end-users attentive of the posting mechanism and to be keenly aware in participating in the photo posting and decision making criterion for which Facial Recognition (FR) mechanism is used. Limitation may occur over the number of photos which will be utilized as the training set if more privacy setting is done. In order to overcome this problem and for training set for FR system we would utilize the private photos of users which would differentiate the photo co-owners without affecting their privacy.



IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

A distributed consensus based method is developed which would protect the private training set and even reduce the computational complexity. Our contributions to this work when compared with previous work are mentioned below:
• The ability to find the precise owners of shared photos automatically framework and along these lines keep the spillage of the security of the people

V. ALGORITHM

We have proposed Harr cascade algorithm. In this the photo is provided by the owner to for
A set of train images. This algorithm detects faces in the photo and crops it into Rectangle. This images are stored as train images.

Algorithm

1: Store positive and negative images to train the classifier.
2: Extract feature= _(pixel in black area)- _(pixel in white area)
3: If image I is a face yi = 1, if not yi= -1
4: Assign a weight wi1
= 1=N to each image I.
5: Renormalize the weight so that it sum to 1.
6: Apply feature to each image, then find the optimal threshold and polarity _j ; pj to minimize the weighted classifier error.
7: Calculate the weak classifier
8: Compute the final classifier,h(x)
9: Train classifier and select best features

AES algorithm

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
Begin
   byte state[4,Nb]
   state = in
   AddRoundKey(state, w[0, Nb-1])
   for round=1 to Nr-1
      SubBytes(state)
      ShiftRows(state)
      MixColumns(state)
      AddRoundKey(state, w[round*Nb, round+1)*Nb-1])
   end for
   SubBytes(state)
   ShiftRows(state)
   AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1)
   Out = state
end
```

VI. PROJECT MODULES

Technique used for implementation of the proposed system are given. It consists of following modules.
1. Friend request
2. Picking close friends
3. Sharing photo
4. Generate OTP
5. Face Detection and Feature extraction
6. Check policy status
7. Post or block

Mathematical Model

_ System S= (x, f, D, M, e_n)
_ Initial State (x): Uploaded photos for training images
_ Final state (f): Success or Failure
_ Input (D):
D= (I, Pi(x), Vk(x))
_ Output (M):
M= Set of users satisfying privacy policy and exposure policy

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

_ Algorithm (e_n):
$M= P_i(x) \setminus V_k(x)$
Where, i, k- users uploading photo
I- Set of users on co-photo
$P_i(x)$ - Privacy policy of user x.
$V_k(x)$ - Exposure policy (Private data)

VII. CONCLUSION

Photograph sharing is a standout amongst the most prominent highlights in online informal organizations, for example, Facebook. Sadly, thoughtless photograph posting may uncover protection of people in a posted photograph. To check the protection spillage, we proposed to empower people possibly in a photograph to give the consents previously posting a co-photograph. We planned a security saving FR framework to recognize people in a co-photograph. The proposed framework is highlighted with low calculation cost and classification of the preparation set. Hypothetical examination and investigations were led to demonstrate viability and proficiency of the proposed plot.

REFERENCES

1. N. Mavridis, w. Kazmi, and p. Toulis. Friends with faces: how Social networks can enhance face recognition and vice versa. In Computational social network analysis, computer communications and networks, pages 453–482. Springer london, 2010.
2. Z. Stone, t. Zickler, and t. Darrell. Toward large-scale face Recognition using social network context. Proceedings of the ieee, 98(8):1408–1415., z. Stone, t. Zickler, and t. Darrell. Autotagging facebook: Social network context improves photo annotation. In computer Vision and pattern recognition workshops, 2008. Cvprw'08. Ieee Computer society conference on, pages 1–8. Ieee, 2008.
3. K. Choi, h. Byun, and k.-a. Toh. A collaborative face recognition Framework on a social network platform. In automatic face gesture Recognition, 2008. Fg '08. 8th ieee international conference on, Pages 1–6, 2008.
4. J. Y. Choi, w. De neve, k. Plataniotis, and y.-m. Ro. Collaborative Face recognition for improved face annotation in personal photo Collections shared on online social networks. Multimedia, ieee Transactions on, 13(1):14–28, 2011.
5. D. Rosenblum. What anyone can know: the privacy risks of social Networking sites. Security privacy, ieee, 5(3):40–49, 2007.
6. C. Squicciarini, m. Shehab, and f. Paci. Collective privacy management in social networks. In proceedings of the 18th international Conference on world wide web, www '09, pages 521–530, new York, ny, usa, 2009. Acm.
7. K.-B. Duan and S. S. Keerthi. Which is the best multiclass svm method? An empirical study. In Proceedings of the 6th international conference on Multiple Classifier Systems, MCS'05, pages 278–285, Berlin, Heidelberg, 2005. Springer-Verlag.