PHOTO AND VIDEO SHARING PRIVACY BASED ON MULTICLASS CLASSIFIER IN OSN

Miss.Devyani P Khambekar[1]
[1] *PG Student,Computer Engineering,SND COE & RC,Yeola,Maharashtra,India*

ABSTRACT

In this modern era, youth's get attracted towards social networking site. Every day they share some post, photos, videos, tagging etc. in social networking domain. Sharing such data requires security. The system is aiming to provide security to such shared data based on the content of post. In this system it is providing a mechanism that enables the user to participate in decision making activity of his/her photo and video sharing on any user's wall. It is providing decision making policies panel to the user using which user can give authority of sharing data to certain users.The system is applying filters on image and video sharing. An efficient FR algorithm is used by system to automatically identify the user from shared videos & images. By analyzing picture present in shared image or video and user policies decision can be taken to share or block the content. To indentify user we are using users profile picture dataset. It will evaluate the system performance on huge dataset and can calculate accuracy of the system. It provides policies for decision making in which user can specify authority to share data with certain users. By using FR-technique our system can automatically detects users shared images and videos.

Keywords*: Image processing, video processing, FR technique, Social network, photo privacy*

I. INTRODUCTION

Recently, there are no regulations with sharing of co-photos, on the contrary, social network service providers like Facebook are encouraging users to post co-photos and tag their friends in order to get more people involved. According to Facebook Statistics average user creates 90 pieces of content each month, whereas more than 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) are shared each month. A social network is a media to interact and share content with people but having lot of risk of privacy. Consider the scenarios like what if the co-owners of a photo are not willing to share that photo? Is it a privacy violation to share this co-photo without permission of the co-owners? Should the co-owners have some control over the co-photos? Some mishaps can happen by applying photo-shop effects on certain users photograph.

To provide privacy policies and decision control to the user on shared items in OSN is required. We are providing a mechanism to provide automatic face recognition in photo and shared videos using FR system. Photos and/or videos will get automatically blocked of user provide privacy policies.

Social networking is going viral day by day and posted data spreads in small amount of time [2][4]. Sometime unnecessary data get viral. Data may contain text, images and videos. Vulgar text posting on wall may corrupt the social image of user. In case of image posting, if user image is shared without his consent then that may cause breach of privacy. Also videos shared without user permission having user face, then that tends to the breaching of privacy of user. Hence this area should be focused. A system that provide blocking of automatic photos/videos on OSN as per the user privacy policies. These photos and videos are automatically getting identified without generating tags [5]. To identify photos and videos in social network and apply policy filter. Sharing multimedia data is most popular and regular trend in recent online social network.

The Proposed project idea is to design Client – server application for the concept is in scope of this project. Also to enhance privacy policy to next level is also in scope statement [9][11]. Using filtering policy video, group images, texts are filtered. To provide facility to user so that he can establish social network for himself by sending and accepting friend requests. We are implementing this system to provide control panel and facility to user so that he can manage his privacy settings. To provide facility in such way that he can filter unnecessary images from his wall. To provide facility, so that he can filter unnecessary video from his wall. To provide facility in such a way so that he can filter unnecessary text from his wall.

II. RELATED WORK

In [2], Altman's privacy regulation theory is discussed. It states that, privacy is a term that is dialectic and dynamic which has control on accessing but it can be dynamic. It expands privacy level of other group. They defined an analysis of the privacy such as dynamic, dialectical and traditionally universal process.

B. Carminati, E. Ferrari represented a rule-based access control for social networks. An author discussed about WBSN is an access control model. It specifies policies based on type of data and belief of relationship. SNMS is a Social Network Management Systems, it allow users to explain whether specific information. It is a simple approach having straightforward approach still they are not flexible enough in denoting authorized users because they may grant access to non-authorized users.

J. Y. Choi, W. De Neve discussed about collaborative face recognition system. It Improves face annotation in personal photo collections shared on OSN[4]They described key idea behind an OSN that are ideally correspond to real-world activities, for that they are evaluating the correlation between the personal context models of the OSN members, and hence accuracy of event-based image annotation can be improved significantly. Only for retrieving images, this paper, mainly personalize image search, a tag-based query.

K. Choi, H. Byun, and K.-A states a collaborative face recognition framework on a social network platform [5], they discussed difference between a stand-alone based system and a social network based system. A novel collaborative face recognition technique is established, to neglect the redundant tagging by sharing the identification information for efficient update under the social network platform.

P. A. Forero, A. Cano did an empirical Study which describes methods of multiclass those are competitive with each other. There is no clear superiority of one method over another.

These methods are namely, WTA SVM, MWV SVM, Pairwise coupling etc.

These methods are highly approved as the best kernel discriminate methods for solving challenges in multiclass.

B. Goethals, S. Laur, H. Lipmaa, [7], represents standard cryptographic techniques known as private scalar product protocol and proved that this technique is more secure, Optimization technique is used to make result of proposed system more efficient.

L. Kissner and D. X. Song , suggested Privacy-Preserving Set Operations [8], Set Operations Using Polynomial Representations and Operations with Encrypted Polynomials techniques are proposed. This technique is used for solving privacy issues in OSN:

Proposed system describes two standard adversary models such as, honest-but-curious adversaries and malicious adversaries. Authors were design efficient methods to enable privacy preserving computation of the union, intersection, and element reduction multi set operations.

The structure and function of complex networks [9], proposed by M. E. Newman et al to reviews on structure and function of social networked systems. This paper works on real networks such as, Internet, the World Wide Web, social networks, collaboration networks, citation networks, and a variety of biological networks. Authors determine behavior and function of the networked systems.

L. Palen. discussed about Unpacking “Privacy” for a Networked World. They represented researchers and practitioners to understand the better privacy by unpacking the more specific statements. For dong this they were forming privacy regulation theory that is developed by social psychologist Irwin Altman.

Authors described that how privacy management process is conducted in the presence of information technology.

Collective privacy management in social networks [11], this paper described a simple mechanism to promote truthfulness, and that rewards users who publish co-partnership. Authors integrate their design with inference techniques; these techniques are free users from the burden of manually selecting privacy preferences for each picture. They were also showing a proof-of-concept application that is implemented in the context of Facebook.

Toward Large-Scale Face Recognition Using Social Network Context Technique Used: MRF [12] this paper introduced, MRF technique. MRF is used for face recognition. In this technique a large photo collection are on the web. Resulting, a practice of users can produces large labeled image, to reduce enrollment burden.

Z. Stone, T. Zickler et al.[13], tends to improve a recognition performance. This proposed method integrates an image data with social network background in a conditional random field model. For implementation of system this paper uses, a technique such as, CRF model (Conditional Ramdom Fields). It will be most effective technique when social network background is available for all of the people who appear in a photographer’s photos, but this information may not be available from Facebook for many reasons.

This paper, expect that their context-based labeling technique would perform far better with complete access to Facebook’s data.

K. Thomas, C. Grier [14] observes that how the lack of multi-party privacy controls for shared content can undermine a user’s privacy. For process purpose threat model is used to classify properties of user information.

It unthinkingly exposed due to privacy conflicts. They were assuming some parties involved are marketers, political groups, and monitoring agencies who have the resources, sophistication, and motivation to glean as much information from social networks as possible.

P. Viola and M. Jones [15], represents some techniques used to gain the privacy on OSN as, object detection, speed of the Final Detector, Image Processing, scanning the Detector etc. This system uses, object detection technique for minimizing computation time to achieve high accuracy. This system designed to construct a face detection system. Data sets include many face conditions such as, illumination, scale, pose, and camera variation.

III.PROPOSED SYSTEM

Following fig. 1 represents the proposed system architecture. There are five module presented in proposed system diagram such as,

1. Video Processing
2. Facial Recognition system
3. Collaborators supervised learning
4. Apply policy filter
5. Auto user blocking.

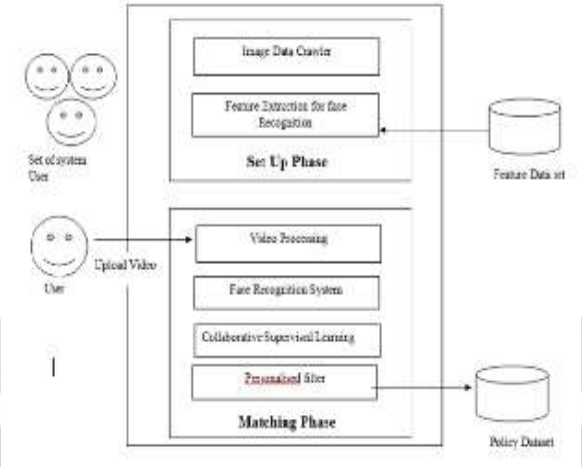


Figure 1: System Architecture

Step 1: Video Processing:
Video is a collection of successive n frames .We are applying algorithm to get 'n' images from the uploaded video. These images are passed to the following filters.

Step 2: Collaborators supervised learning:
In photo or video more than 1 person can present and hence our classifier needs to figure out exact classification for this we are using multi-class classification system.

Step 3: Apply policy filter:
We are providing privacy policies Pi(x) and set of exposure policy Vi(x) to each user i.

Step 4: Auto user blocking:
Based on the photos and videos present in shared data of other user and access policies of that user are responsible for taking a decision of sharing data on OSN.

IV.ALGORITHMS
1. Classifier Computation Algorithm:
To develop a system for photo / video matching we follow pipelined strategy. We first build a friend hierarchy then find match for first level hierarchy that is self to friend paring: {self, friend}. If no match found then e will go to the next step of hierarchy, i.e. friend of friend: {friend, friend}
Following algorithm shows the working of classifier.
Input:
'ui' friend hierarchy,
Uploaded post image Pu_i, access policy data set AC
Output:
Post matching decision.
Processing:
Step1: get 1st level node list
Step2: for each node in 1st level list
Get profile photo data set Xi
Compare 'ui' image with whole data set using one against all strategy.
if Pu_i matched with Xi

Check access policies Aci
if 'ui' not belongs to Ac_i
Block post
Break the execution
Step 3: get 2nd level node list
Step 4: for each node in 2nd level list
Get profile photo data set Xi
Compare 'ui' image with whole data set using one against all strategy using FR matching algorithm
if 'ui' matched with Xi
Check access policies Ac_i
if 'ui' not belongs to Ac_i
Block post
Break the execution

2. FR matching Algorithm:
Input:
Image dataset I, P-iamge ,Tr as Treshold
Output:
Face matching result
Processing:
Step1: obtain face images I1, I2... IM
Step 2: represent every image Ii as a vector Ti
Step 3: Ti is an N*N x1 vector, corresponding to an NxN face image I.
Compute the average face vector y:
Step 4: subtract the mean face:
Qi= Ti-Y
Step 5: compute the covariance matrix C:
Step 6: compute the eigenvectors ui of A-AT
Step 6.1: consider the matrix AT-A (MxM matrix)
Step 6.2: compute the eigenvectors 'vi' of AT -A
Step 6.3: compute the M best eigenvectors of AAT: 'ui' = Av_i
Step 7: keep only K eigenvectors
Step8: Compute Tp , Yp and Qp for P-image
Step 9: compute M = min Qp-Q
Step 10: if min m=Tr
Face matched

V.MATHEMATICAL MODEL
Set Theory:
S = I, O, F
I = {I1, I2, I3, I4, I5}
I1 = user details
I2 = user photo
I3= image post
I4= video post
I5= filter policy
O = {O1, O2, O3, O4}
O1 = friend list
O2= feature list dataset
O3= filtered post
O4 = block list
F = {F1, F2, F3, F4, F5, F6, F7, F8, F9, F10, F11, F12, F13}
F1 =Register
F2 = Login
F3 = find friends
F4 = Manage Friend list
F5 = Add profile photo

F6 = supervised learning
F7 = video preprocessing
F8 = training data retrieval
F9 = find friend hierarchy
F10 = feature extraction
F11 = recursive matching
F12 = match policy
F13 = auto blocking

VI.EXPERIMENTAL RESULTS

To implement this system I have used java-jdk 1.7. To store database mysql 5.3 is used. A web based application is created using apache tomcat5.7 and jsp-servlet.

Dataset Used:

For Profile dataset I have used online fake profile generator.
URL: http://www.fakenamegenerator.com/order.php

Using this generator I have generated 125 records with multiple attributes like:<name, age ,gender ,city, occupation, company name, etc.

For profile picture I have used face recognition database.
We have randomly selected 1000 images from this database for profile pictures.
URL: http://www.face-rec.org/databases/
We have randomly mapped entries for friend network using a java program.

For testing photos are created in photoshop by collecting multiple faces together.

1: Time

a) Text Filtering

Text message is get filtered as per the number of categories: vulgar, Violence, offensive and hate. Text message is then filtered using sentiment polarity count. The statement is get discarded if it has negative polarity.

Message statement count	Time(in Sec)
20	4.2
40	7.24
60	11.67
80	16.64
100	21.64

Table 1: Text filtering

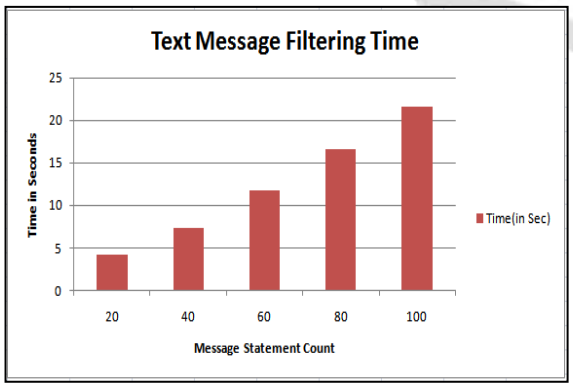


Figure 2: Analysis of text filtering

b) Image and Video Filtering

i) Training dataset Creation:

For Training dataset creation user need to upload photos. These photos are first preprocessed and cropped the faces from it. These faces are resized and converted in pgm format.

Number Of Images	Time(in Sec)
20	5.23
40	11.53
60	17.32
80	22.52
100	29.32

Table 2: Training dataset creation

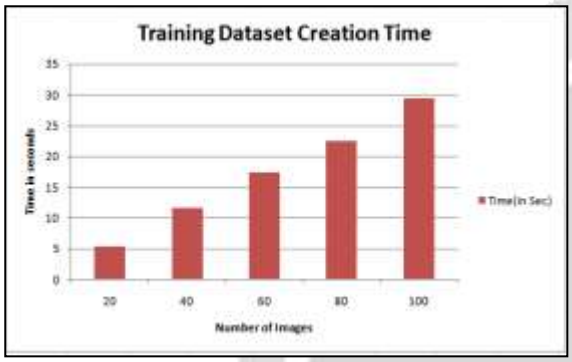


Figure 3: Analysis of Training dataset creation

ii) Testing:

To filter post, first friends and friend of friends of post sender is identified. Then training dataset is selected with respect to friend and friend of friend list.

1: Single photo matching:

Single photo is matched with dataset containing own, friends and friends of friends photograph.

Photo	**Training Time**	**Testing Time**
Own Photo	1.45	1.19
Friend Photo	2.53	3.3
Friend of Friend Photo	3.32	6.2

Table 3: Single photo matching

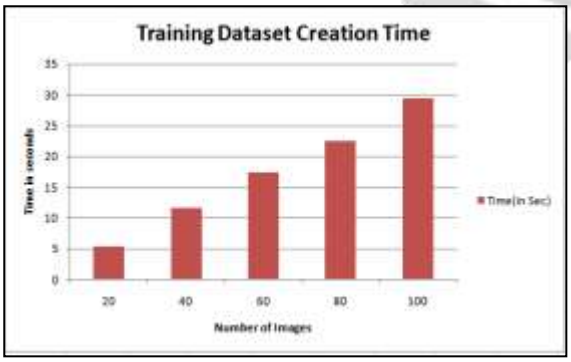


Figure 4: Analysis of Single photo matching

2: Group photo Matching:

From the uploaded post faces are cropped and all faces are matched with the training dataset as per user's friend list and friend of friend list.

Number Of faces	Testing Time
2	5.13
4	9.32
6	13.95
8	18.53

Table 4: Group photo matching

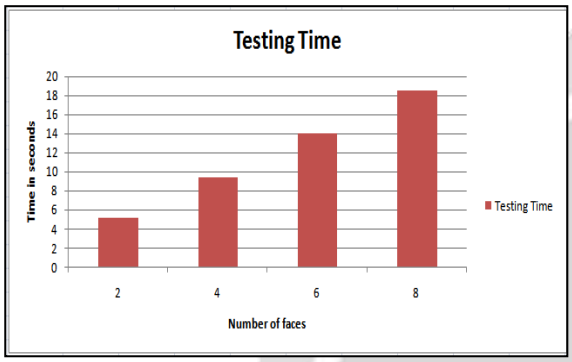


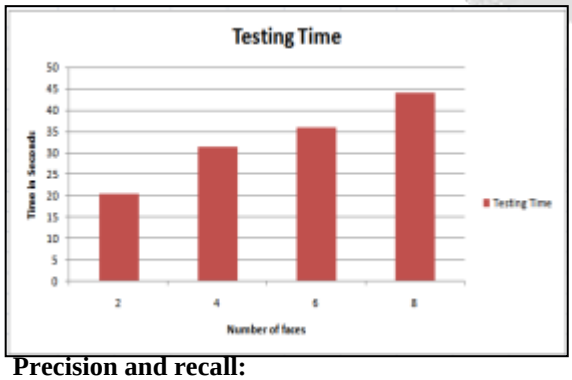
Figure 5: Analysis of Group photo matching

3: Video Matching:

Video is preprocessed and mapped into 20 frames irrespective of video size. Each frame is treated as a single image. And processed like image matching.

Number Of faces	Testing Time
2	20.34
4	31.32
6	35.95
8	43.94

Table 5: Video photo matching



Precision and recall:

Precision and recall is calculated after multiple test cases. We have categorized the result in true positive, false positive and false negative categories.

Precision is evaluated as:

Precision = (true positive)/ (true positive + false positive)
Recall = (true positive)/ (true positive + false negative)

1] Text:
Following is the graphical representation of precision and recall when text messages are posted as comment. In this scenario text processing is carried out using neive bays classifier and sentiment analysis by polarity count and accordingly text message is get posted or blocked. Text processing is done and particular text message is categorize in following categories.
A] Vulgar B] Offensive C] Violence D] Hate E] Negative and F] Neutral
If text is not neutral or positive then it will not appear on user's wall.
Following graph shows the precision and recall details when text messages with mentioned categories are given.

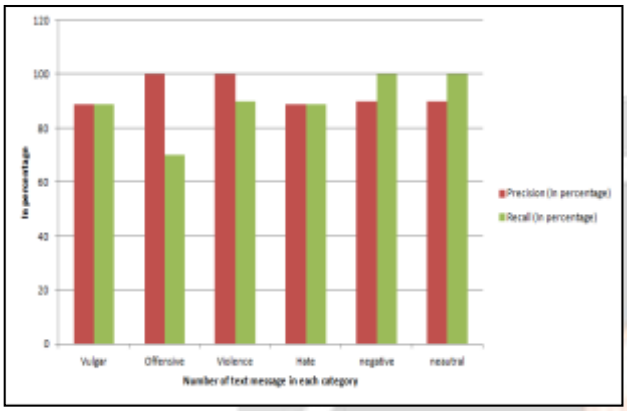


Figure 7: Precision and recall for text filtering

2] Images:
Following is the graphical representation of precision and recall when images are posted as comment. In this scenario image matching is carried out and based on privacy policies these images are posted or blocked.

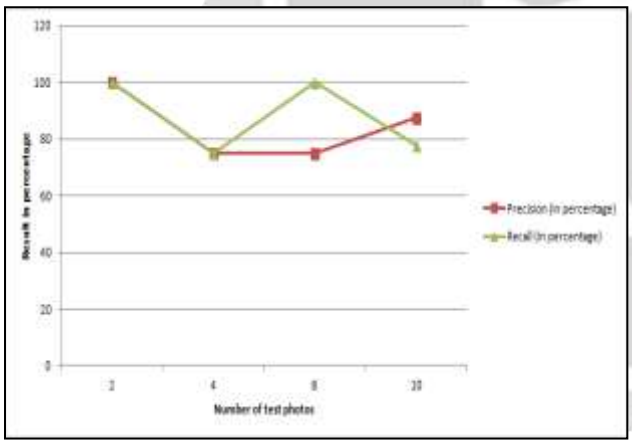


Figure 8: Precision and recall for image filtering

3] Videos:
Following is the graphical representation of precision and recall when videos (in MP4 format) are posted as comment. In this scenario video is converted into frames and faces are extracted from frames and based on privacy policies these videos are posted or blocked. In this processing extracted faces are matched with the friend's or friend of friend's profile picture and based on privacy policies decision is taken whether videos should be blocked or posted. Following graph shows the precision and recall details when videos are given as a comment.

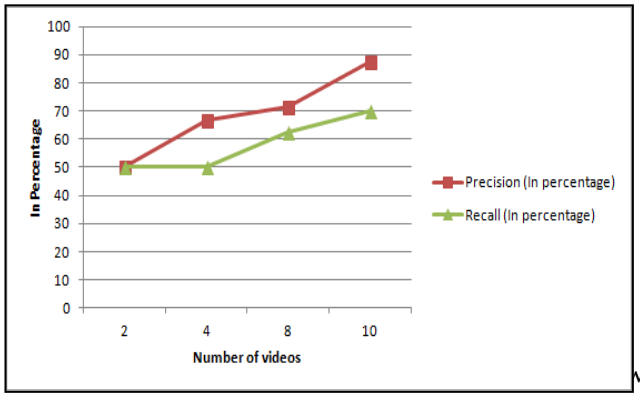


Figure 9: Precision and recall for video filtering

VII. CONCLUSION

In this research I propose to establish private photos set of the own user. And these private photos are used to model a personal FR system based on social background. Training data set i.e. set of private photos of user are distributed over the network could be defined as typical secure multi-party computation problem as well as to achieve the efficiency and privacy it proposes novel concurrence based approach.

REFERENCES

[1] My Privacy My Decision: Control of Photo Sharing on Online Social Networks Kaihe Xu, Student Member, IEEE, Yuanxiong Guo, Member, IEEE, Linke Guo, Member,IEEE, Yuguang Fang, Fellow, IEEE, Xiaolin Li, Member, IEEE
[2] I. Altman. Privacy regulation: Culturally universal or culturally specific? Journal
of Social Issues, 33(3):6684, 1977.
[3]B. Carminati, E. Ferrari, and A. Perego. "Rule-based access control for social networks", In R. Meersman, Z. Tari, and P. Herrero, editors, On the Move to Meaningful Internet Systems 2006.
[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):1428, 2011.
[5]K. Choi, H. Byun, and K.-A. Toh. A collaborative face recognition framework on a social network platform, In Automatic Face Gesture Recognition, 2008IEEE International Conference on, pages 16, 2008.
[6]P. A. Forero, A. Cano, and G. B. Giannakis. Consensus-based distributed support vector machines. J. Mach. Learn. Res., 99:16631707, August 2010.
[7] B. Goethals, S. Laur, H. Lipmaa, and T. Mielik?inen. On private scalar product computation for privacy-preserving data mining, In Proceedings of the 7th Annual International Conference in Information Security and Cryptology, Springer-Verlag, 2004.
[8]L. Kissner and D. X. Song. Privacy-preserving set operations. In V. Shoup, editor, CRYPTO, volume 3621 of Lecture Notes in Computer Science, pages 241257.Springer, 2005.
[9] M. E. Newman. The structure and function of complex networks, SIAM review,45(2):167256, 2003.
[10] L. Palen. Unpacking privacy for a networked world. pages 129 136. Press, 2003,
[11] A. C. Squicciarini, M. Shehab, and F. Paci. Collective privacy management in social networks. In Proceedings of the 18th International Conference on World Wide Web,
[12]Z. Stone, T. Zickler, and T. Darrell. Toward large-scale face recognition using social network context. Proceedings of the IEEE, 98(8):14081415.
[13]Z. Stone, T. Zickler, and T. Darrell. Autotagging facebook: Social network context improves photo annotation. In Computer Vision and Pattern Recognition Workshops, 2008, CVPRW08. Computer Society Conference on, pages 18,2008
[14]K. Thomas, C. Grier, and D. M. Nicol. unfriendly: Multi-party privacy risks in social networks. 2010.
[15] P. Viola and M. Jones. Robust real-time object detection. In International Journal of Computer Vision, 2001.