IJCSN - International Journal of Computer Science and Network, Volume 6, Issue 6, December 2017
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

My Privacy My Authorization: Control of Photograph Sharing in Online Social Media

[1] Nirajkumar Kunturkar; [2] Dr. S.N.Kakarwal

[1] PG Student, P.E.S. College of Engineering
Aurangabad, Maharashtra, India

[2] Professor in CSE Department, P.E.S. College of Engineering
Aurangabad, Maharashtra, India

Abstract - Image sharing is the new cool feature which is successful in ruling Online Social Networks (OSNs). Unknowingly, it may expose users' privacy if they can post, comment, and tag a photo without any restriction. In this paper, we are attempting to address this issue and study the scenario when a user shares a photo containing individuals' other than himself/ herself (referred as co-photo for short). To refrain the possible privacy leakage of a photograph, we are suggesting an approach to entitle everyone in a photo to acknowledge the act of image posting and enable them to be a decisive authority on the photo sharing. To achieve this feat, we require coherent facial recognition (FR) system to identify everyone in the photo. However, as the need of the privacy concerns in people increases it may limit the publicly available photos to train the FR system. To deal with this trauma, we suggest an approach to consider private photos to design personalized FR system which can be trained to recognize possible co-owners without compromising their privacy. With our suggested approach, we think the computational complexity will reduce as we are not relying on the photos available on social platform for the training purpose but instead asking users to provide their photos from their gallery which is reliable source and the private training set is also not exposed on the platform to maintain secrecy about this dataset.

Keywords - *Online social networks, FR system, Open social, privacy.*

1. Introduction

The Internet has become associate part of the lives of individuals these days. OSN [1] have become integral part of our daily life and has deeply changed the way people connect with each other, in turn meet social needs, the needs for information sharing, respect, appreciation and social interactions. It is also the root of the existence of social media that individuals put more content including photos, without any hesitation. Unknowingly once something like a photo is posted online, it becomes a long-lasting record, which may be used for the things one did not expect.

Most existing FR systems have been developed using a centralized FR approach [2]. This includes traditional FR application domains such as video surveillance and national security. A centralized FR system relies on a single FR engine for performing FR operations (e.g., subject identification or subject verification [3]).

2. Literature Survey

In [4] A. Acquisti given that online interpersonal firms like Friendster, Myspace, or the Facebook have learned exponential development in enrolment as of late. These systems give connecting with proposes that to association and correspondence, however furthermore raise protection and security issues. In this study authors tend to overview a stratified example of the individuals from the Facebook (an informal community for schools and secondary schools) at a USA instructional exercise foundation, and contrast the review information with information recovered from the system itself. R. Gross look for fundamental demographic or behavioral varieties between the groups of the system's individuals and non-individuals; authors tend to investigate the effect of protection issues on individuals conduct; tend to contrast individuals' unequivocal mentalities and genuine conduct; and that were archived the adjustments in conduct after security related information presentation. Authors find that partner individuals protection issues are exclusively a powerless indicator of his participation to the system. Moreover, security included individuals be a piece of the system and uncover pleasant measures of private information. Some deal with their security issues by believing their capacity to deal with the information they supply furthermore the outer access to that. Nonetheless, authors tend to furthermore acknowledge evidence of individuals misguided judgments with respect to the net group's real size and creation, and regarding the perceivability of individual's profiles.

In [5] S. Ahern, D. Eckles, N. S. Good stated that as sharing individual media online becomes simpler and wide unfold, new privacy disorders emerge - as soon as the chronic nature of the media and related context displays important points regarding the bodily and social context for the duration of which the media matters were created [6]. In a very first-of-its-kind be trained, authors tend to make use of context-conscious camera phone instruments to seem at privacy alternatives in mobile and online percent sharing. S. King, M. Naaman, R. Nair. Here mentioned that the way of expertise evaluation on a corpus of privacy picks and associated context know-how from a real-world procedure, we are likely to check relationships between vicinity of percent's capture and system privateness settings [8]. Their expertise analysis leads to more queries that eventually are likely to examine by way of a set of interviews with fifteen users. The interviews reveal normal themes in privateness concerns: protection, social speech act, identification and convenience. Finally, they are inclined to spotlight many implications and opportunities for type of media sharing functions, together with mistreatment earlier privateness patterns to discontinue oversights and mistakes.

The M. Ames and M. Naaman expressed in [1] Why do individuals tag? Clients have generally abstained from explaining media, for example, photographs - both in desktop and versatile situations - despite the numerous potential uses for comments, including review and recovery. Authors research the encouragement for comment in Flickr, a well-known online photograph sharing framework, and Zonetag, a camera phone photograph catch and comment instrument that transfers pictures to Flickr. In Flickr, comment (as literary labels) fills both individual and social needs, expanding motivators for labeling and bringing about a moderately high number of comments [3]. Zonetag thusly, makes it less demanding to tag camera phone photographs that are transferred to Flickr by permitting explanation and proposing significant labels quickly after catch. A subjective investigation of Zonetag/Flickr clients uncovered different labeling designs and rising inspirations for photograph explanation. We offer a scientific classification of inspirations for comment in this framework along two measurements (sociality and work) [7], and investigate the different elements that individuals consider while labeling their photographs. Our discoveries propose suggestions for the plan of computerized photograph association and sharing applications, and in addition different applications that join client based explanation.

Here Photograph sharing has turned into a favored element of the numerous on-line long range interpersonal communication destinations. A. Besmer and H. Lipford. shared ideas in [8] as a few of the introduction sharing applications on these destinations, empower clients to comment on photographs with individuals who are in them. Assortment of specialists have analyzed the social uses and protection issues with on-line introduction sharing locales, however few have investigated the security issues with presentation partaking in interpersonal organizations. In this paper, they begin by looking at some of the discoveries from a progression of center groups on presentation protection inside the person to person communication area. They tend to then devise a substitution system to help presentation security strengthen these discoveries.

3. System Architecture

Keeping enemies from accumulating noteworthy measures of client information is a noteworthy test for interpersonal organization administrators said by J. Bonneau, J. Anderson, and G. Danezis in [6]. As we analyze the trouble of gathering profile and diagram data from the well-known long range interpersonal communication website Facebook and report two noteworthy discoveries. To begin with, we depict a few novel routes in which information can be separated by outsiders. Second, we exhibit the productivity of these strategies on crept information. Our discoveries highlight how the present security of individual information is conflicting with client's desires of protection.

4. Proposed System

In this paper, we tend to plan to empower folks conceivably in an exceedingly photograph to allow the consents before posting a co-photograph [9]. We tend to be printed a security protective framework to tell apart folks in an exceedingly co-photograph. The planned framework is highlighted with low calculation expense and classification of the preparation set. Hypothetic investigation and analyses were directed to indicate adequacy and proficiency of the planned arrange. We tend to expect that our planned system would be very useful in making certain clients' security in photograph/picture sharing over on-line informal communities. Then again, there reliably exist exchange off within the middle of protection and utility [10]. For example, in our prototype application, the co-photograph should be post with consent of all the co-owners. Dormancy conferred during this procedure can extremely influence end-user's expertise of sharing and privacy concerns pf photos [1].

The ideal scenario for face detection would be one in which only front images were involved. The feature occlusion of images is given as the presence of elements like beards, glasses or hats introduces high variability. Faces can also be partially covered by objects or other faces [2]. We extract the features by facial expression by calculating facial features which also vary greatly because of different facial gestures. Imaging conditions also affect the quality of image as different cameras and ambient conditions affecting the appearance of a face.

The proposed system architecture diagram of our system is shown in appendix at the end of this paper. When user wants to upload a photo, he requests for photo to be shared on OSN, in our case let say on Facebook. The system takes the photo and extracts the features of the faces in the photo. A Facial Recognition algorithm is needed to identify faces in the photo. Once the faces in the photo are identified we can point out the individuals which are in turn are the co-owners of the photo. The decision to specify partially relies with them too; as they are getting exposed publicly. The co-owners can decide the policy to be assigned to the photo. The aggregated policy specified by them is assigned to the photo.

Each image in the database is compared with sample image which is getting uploaded. The comparison happens pixel by pixel. Each pixel in the sample image is compared with the identified stored image. Based on the matching a potential score is derived. Based on the previous experience a threshold can be decided. If score of the image is greater than the threshold we can consider it as a positive sample and improve our recognition learning system. Those photos where matching is less than threshold is considered as negative samples.

According Classifier Computation Algorithm, there are two steps to build classifiers for each neighborhood: firstly, find classifiers of {self, friend} for each node, then find classifiers of {friend, friend}. Notice that the second step is tricky, because the friend list of the neighborhood owner could be revealed to all his/her friends. On the other hand, friends may not know how to communicate with each other. For this consideration, when building classifiers of {friend, friend}, all the local training results are send to the neighborhood owner, who will coordinate the collaborative training processes by forwarding local training results to right collaborators. In this manner, friends need not to know who they are working with and how to talk with them.
Comparing the photos in a considered database is seamlessly effortless and much less complex. When we consider the whole OSN comparing the photos for identity is cumbersome job. For that we can use suggest approach which reduces the search space and still does not lose the context of the goal.

5. Evaluation

Our system works in 2 steps. We have taken test images from the users' phone gallery. This data is not exposed on platform. It is completely kept private. Using Voila-Jones algorithm, we can classify samples as positive and negative samples. Only positive samples are considered as training data-set. First step is face detection and second step is face recognition. The user on OSN platforms like facebook are not mandated to share only pictures of friends or images of friends. User can share images other than facial images like flowers, monuments, structures or his own fact of interest. In-order to exclude images other than faces, Viola-Jones algorithm with Haar-Cascade classifier is used.
For the training purpose, all the images in user's private photos are considered. Using Haar-Cascade algorithm samples which are not faces are excluded. The samples with faces are called positive samples and rest are considered as negative samples. These positive samples are taken as users training dataset. The collective of all the users face positive samples form the total training data set. One important point, all the images must have same size and the faces are placed at center. A probe image is then compared with face data.

Algorithm 1: Viola Jones Algorithm

1. Store positive and negative images to train the classifier

2. Extract feature = sum (Pixel in black area) – sum (Pixel in white area)

3. If image I is a face y^i = 1, if not y^i = -1

4. Assign a weight W^i = 1/N to each image I

5. Renormalize the weight so that it sums to 1

6. Apply feature to each image, then find the option threshold and polarity $\Theta_{j,}$ P_j 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

Algorithm 2: Face-Recognition algorithm using Eigen Method

1. Prepare the data of the faces constituting the training set (Y) should be prepared for processing

2. The faces must be of same size and must be centered.

3. Represent every image as a vector Γi

4. The average matrix Ψ is calculated, then substracted from the original faces (Γ) and the result is stored.

5. Covariance matrix is calculated according to

C = $\frac{1}{M}\sum_{n-1}^{M} \phi_n \phi_n^T$

6. Compute eigenvectors for the covariance matrix. In this step eigenvectors and the corresponding eigenvalues are calculated.

8. Normalize eigenvectors so that they become unit vectors i.e. of length 1

9. From all the eigenvectors select highest small part eigenvalues. Eigenfaces with low eigenvalues can be omitted.

10. For classification of image, transform the image into its eigenface components.

11. Calculate the Euclidian Distance between weight vectors, and if the distance lies within some threshold the face is labelled against that.

First the faces constituting the training set (ϒ) are prepared for processing. The average matrix Ψ must be calculated, then substracted from the original faces (Γ) and the result stored in the variable i :

$$\psi = \frac{1}{M} \quad (1)$$

$$\phi_i = \Gamma_i - \psi \quad (2)$$

In the next step the covariance matrix C is calculated according to

$$C = \frac{1}{M}\sum_{n-1}^{M} \phi_n \phi_n^T. \quad (3)$$

After calculating the covariance matrix, the eigenvectors and eigenvalues for the covariance matrix are calculated. Once the eigenfaces and eigenvalues are got, the principal components are selected. From the eigenvectors calculated only few of them are selected.
The higher the eigenvalue, the more characteristic features of a face do the eigenvector describe. After M' eigenfaces μ_i are determined, the training phase of the algorithm is finished. Now comes the classification of the training image. The classification works in two steps. First, the new image is transformed into its eigenface components. The resulting weights form the weight vector Ω_{new}^T

$$w_k = \mu_k^T\ (\Gamma_{new} - \Psi)\mathrm{k} = 1 \ldots M' \quad (4)$$

$$\Omega_{new}^T = [\omega_1, \omega_2, \ldots.\omega_{M'}] \quad (5)$$

The Euclidean distance between two weight vectors d (Ώ$_i$, Ώ$_j$) provides a measure of similarity between the corresponding images i and j. If the Euclidean distance between Γ_{new} and other faces exceeds - on average - some threshold value Θ, one can assume that Γ_{new} is no face at all. d (Ώ$_i$, Ω$_j$) also allows one to construct" clusters" of faces such that similar faces are assigned to one cluster.

5.1 Implementation Details

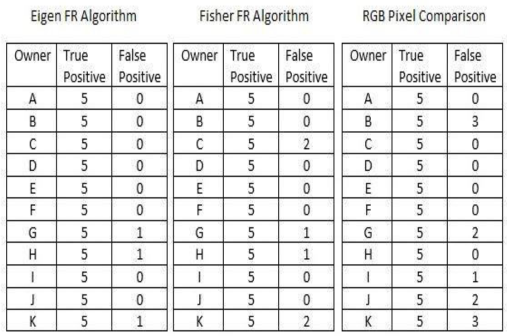
Our prototype application is a web-app, implemented in JSP servlet. We have tried to mimic the basic functionality of finding people and making friends like facebook. We use OpenCV, JavaCPP library to carry out face detection and above stated algorithm for face recognition. On launching the web-app, we can create users, the existing user can login. After logging in, a greeting message and the profile picture will be shown with a greeting message. User can upload photos for sharing, can change his profile picture.

Running in the setting mode, the program is working towards the establishment of face data used for training. For this purpose, the set of photos X_i are selected also the profile photos which user had uploaded till date are considered. For the neighborhood β_i, we have considered all the people available on the platform. This is just for this prototype. We can use the neighborhood algorithm but, as we are working on the small set of people connected on the platform, we are considering everyone on the platform as a neighborhood. For all the users on the platform, we have taken 10 photos per user for collaborative training. On these photos face detection algorithm is executed, and positive samples are extracted. From these positive samples only, the faces from the positive samples are extracted. These extracted faces are used as classifier for face recognition against the sample image getting uploaded.

In the working mode, user can choose to share the photo Xi by selecting the upload photo option. Before sharing we ask users to choose the group from the existing created groups with whom they want to share the photo. When the button "Check" is pressed, co-owners of Xi are identified, then notification along with X are send to the co-owners to request permissions. If all of them agree to post the photo, it will be posted on the wall of the group selected at the time of upload. If any of the co-owner choose not to share the photo and rejects the request; the photo is not shared at all. For now, we are allowing to share photo only within 2 groups. We can extend that to as many groups as we want later. In this sense, in current system, users could specify their privacy policy, but their exposure policies are either everybody on earth or nobody depending on their attitude toward x. By allowing the photos to share in groups we can expand selection to group of selected people. People outside of the shared groups cannot see the photos shared in those groups. If any new dataset comes up as private data for user, setup mode is to be invoked.

5.2 Performance Analysis

We have studied face recognition ratio against the number of connections, number of photos and number of strangers. We have used Haar-Cascade algorithm for face detection stated above Algorithm 1 and Algorithm 2 for face recognition. For the performance evaluation, we have used "Face Recognition Data, University of Essex, UK" database; which is commonly known as Face94 Database. For training we considered total 11 users. Each user is mandated to provide 10 images with various facial expressions; which makes training data set of 110 images in total. In Face94 Database, total there are 153 users' photos are available; each user 20 images. For testing the efficiency of the system, we have used rest of 5 images for testing of the selected 11 users. For identification of strangers in the system, we have used rest if the users' photos for testing. These images are referred as imposters in rest of the paper.



Eigen FR Algorithm

Owner	True Positive	False Positive
A	5	0
B	5	0
C	5	0
D	5	0
E	5	0
F	5	0
G	5	1
H	5	1
I	5	0
J	5	0
K	5	1

Fisher FR Algorithm

Owner	True Positive	False Positive
A	5	0
B	5	0
C	5	2
D	5	0
E	5	0
F	5	0
G	5	1
H	5	1
I	5	0
J	5	0
K	5	2

RGB Pixel Comparison

Owner	True Positive	False Positive
A	5	0
B	5	3
C	5	0
D	5	0
E	5	0
F	5	0
G	5	2
H	5	0
I	5	1
J	5	2
K	5	3

Fig.2 Evaluation using various techniques of FR

In fig.2 we have stated the analysis of FR we got for different face recognition techniques. We have used same training dataset in RGB Pixel comparison, fisher and our system which uses eigen method for FR; detailed in Algorithm 4 above. For the privacy of individual appearing as a co-owner in a photo, can well be preserved if the FR engine identifies correctly who all are appearing in a photo. All the three FR techniques are tested against the images we have used for testing our system. The evaluation shows the result of correctly recognized faces (True Positive Rate) and the incorrectly recognized faces (False Positive) rates. We have determined true positive rate if, known image correctly identifies the person against the training data set. If the technique identifies the person when an imposter image is given, then the test is said to be false positive test. In Fig 3. we show the recognition ratio of true positive rates. Fig 3. shows the comparison in graphical representation of the TP of Fisher, Eigen and RGB Pixel Comparison techniques. We have found that when there are no imposters all of the three systems can achieve very high recognition rate when the number of users are 11.

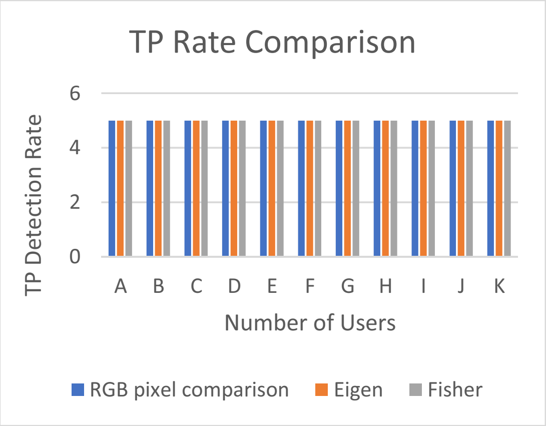


Fig 3. TP Rate Comparison of Face Recognition Algorithms

For the recognition of co-owner, number of users and the iterations it takes is same. If the number of users are increased, then the number of iteration needed for face recognition will increase.

Another criterion to measure the performance of the system is false positive rate. It is important to recognize the correct owners of the image. But if there are false positive recognition, it may reveal the test image to unwanted person. This is another threat of the persons privacy. Also, if the wrong user approves the request of photo sharing, then the actual user's exposure policy is at question. For these reasons, a low positive rate is expected.

If there are no strangers, the false positive rate would be determined by how accurately system recognize the user. If there are strangers, then the misclassification would result in false positive rate. Fig 4 illustrates the false positive rate. For getting the false positive results, we have used the face94 database. As stated above, only the 11 users are considered for training the face data. So, we are left with plenty of users from the standard database as strangers. We have taken 20 users for testing the false recognition. We have considered the false positive rate if any of the images taken for testing recognizes wrong face and labels from the user from the training data. For most of the users our system did not recognize the user which is intended behavior.

We observed in these methods, there are false recognitions. We have tried different thresholds, but these are the best results we could see. The more the users, higher is the chance of recognizing the user as a stranger.

We have tested the systems with group photo as well. In a group photo we have taken 2 people together in a photo. While testing the group case scenario we have used same database, face94 db. We have merged 2 individual photos in a single photo. The faces appearing in a photo were mix of different possible combinations of imposters and known faces. In some photo, people from training set may appear or one known and other imposter or both imposter appeared together.

We tested our system for identification of strangers appearing in a photo/co-photo. For this aspect of test, we calibrated our system with 30 users in total. These 30 photos of individuals are fed to the system as a single photo or a mix of both strangers appearing in a single photo or one stranger and one known user (appearing in the training dataset) image. As stated above if the system identifies any stranger in the appeared in a photo sharing the system will not allow sharing of that photo. When we say a user is a stranger, we mean that face is not identified from the scope of training dataset.

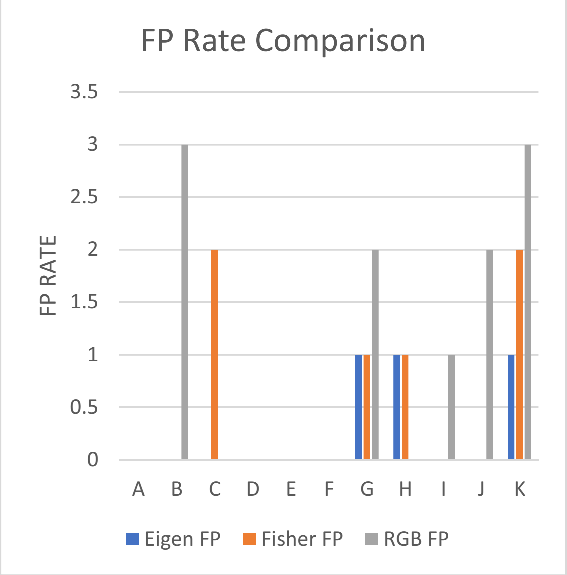


Fig 4. FP Rate Comparison of Face Recognition Algorithms

The test results of stranger detection using Face94 db with 30 users in total are detailed in Fig. 6 when one or more users appear together in a photo.

	Eigen	Fisher	RGB Comparison
Stranger Detection (in %)	90	80	65
FP in (%)	10	20	35

Fig 5. Evaluation of stranger detection

From the observation of the tests we conducted with 30 strangers we got these results. In total in our approach, using Eigen algorithm 3 users were recognized incorrectly. Wherein 6 and 11 users were detected incorrectly. The table above gives the idea of the false recognition rate. From this if we consider percentage of stranger detection:

Stranger Detection = 100 – (Percentage of FP)

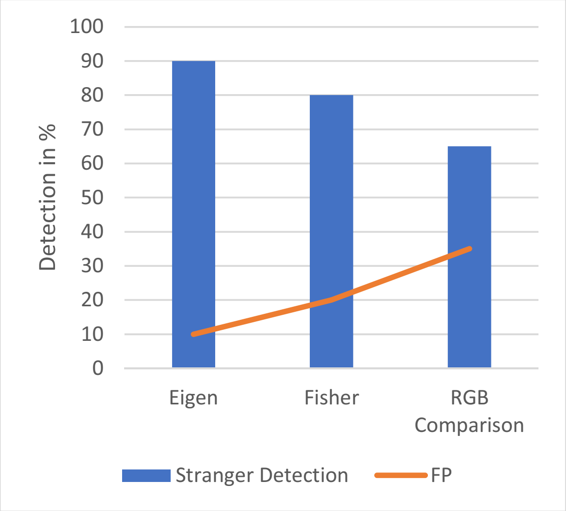


Fig. 6. False Positive ratio and stranger detection ratio

We detailed about performance of how we can identify everyone in a photo. After the recognition of who all appear in a photo, we ask the co-owner to approve the request to share that photo. If all the co-owners in a photo agree, a photo is shared in a group, specified at the time of sharing, by owner user. Users who are not part of those groups won't be able to see the photo this adds extra layer of security for getting exposed. In a facebook we can share a photo in group and if group is private only member of group can see the photo. Host user can use this functionality to share the photo. But, it is obvious that there might be cases where the group owner has selected a group, a set of people with whom co-owner does not want to share that photo. In [11] an approach is suggested, where a social-clique is used to identify clique for automated privacy control. This uses random tags used in photo and forms the clique. However, it is seen that people who appear in some photos may not concerned about the data, always. To improve the clique finding technique, the user given tags are considered. We can use the knowledge of co-owners and the probability of them appearing in a photo together and giving permissions to share the photo in a specific group, as input criteria to detect the social clique to determine automated privacy policy. We believe so because our co-owners are actual users who are appearing in a photo together and not the tags owner has given to a photo.

By allowing a photo to share in a specific group/groups, the privacy of getting exposed is maintained. The co-owner can decide whether they are the same people, to access a photo getting shared. It is seen that users find it difficult to select the user from the list of friends list individually and allow them access. At the same time, we can expect a scenario where all users in a group may not be relevant to access the photo or somebody who isn't part of group needs to access the photo. It is seen that the people in groups on online social network belong to either to same community, age group, relation, family, social interaction, institute, office, friends or hangouts. People post photo from mostly these locations. Hence chances of being all of them together is more; still not guaranteed. We assume it is easy to add/remove somebody from a group than selecting users from the long friend lists.

6. Conclusion

Photo sharing is amongst the top activities on online social networks such as facebook and it has got lot of popularity in recent times. Unfortunately, and unwillingly careless photo post, may reveal individual's privacy appearing in a photo. To get rid of the privacy concern, we have proposed an approach which enables everyone appearing in a photo to give permission before photo is getting posted publicly on a platform. We have designed a privacy preserving FR system to identify each individual in a photo. This system has pure confidentiality of the photos used for training. We have carried out experiment with standard database to show the effectiveness and the capability of the system to protect the privacy of the user. The analysis carried out shows the efficiency of the system; with the Face94db we observed that the identification of a user when his photo is given to the system it identified the user correctly in all of the three Eigen, RGB pixel comparison and fisher algorithms correctly. All of the test data for 11 users; 5 photos each recognized correctly. However, the accuracy of RGB pixel comparison was least in the recognition of a face incorrectly. When 30 stranger users with 5 photos each were taken, for this test the FP count was 3, 6 and 11 for Eigen, Fisher and RGB FR algorithms. For stranger detection we observed that Eigen algorithm out-performed the Fisher and RGB pixel comparison algorithm with accuracy 90%, 80% and 65% respectively. The deliberate framework is highlighted with low calculation expense and classification of the guidance set. We tend to anticipate that our system be very valuable in making detailed customers' security in image sharing over online informal communities.

Also, we have added extra layer of security by allowing the photo sharing in a specific group. In the context, the exposure policy of the user is not compromised. In exiting approach, if all owners agree to post a photo, the photo is available publicly. Our approach would help users to maintain balance between privacy and exposure policies. However, this has a latency which can affect in the end-user's experience of OSNs. Our future work could be to improve the performance of the system and working towards making dynamic groups and sharing the photo with an individual rather than group of people.

7. Appendix

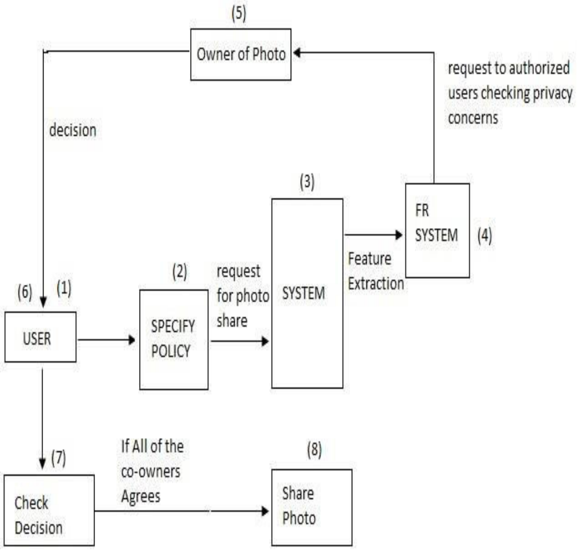


Fig 7. System Architecture

8. Acknowledgments

We are appreciative to commentator for their significant recommendations furthermore thank the college powers for giving the obliged base and backing. We are thankful to **University of Essex, UK** for making face94 database accessible to carry out the experiments.

References

[1] M. Ames and M. Naaman. Why we tag: Motivations for annotation in mobile and online media In V. Shoup, editor, CRYPTO, volume 3621 of Lecture Notes in Computer Science, pages 241–257. Springer, 2005.

[2] 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] L. Kissner and D. X. Song. Privacy-preserving set operations. In V. Shoup, editor, CRYPTO, volume 3621 of Lecture Notes in Computer Science, pages 241–257. Springer, 2005.

[4] A. Acquisti and R. Gross. Imagined communities: Awareness, information sharing, and privacy on the Facebook. MCS'05, pages 278–285, Berlin, Heidelberg, 2005. Springer-Verlag.

[5] Over-exposed? Privacy patterns and considerations in online and mobile photo sharing.
S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair. Trends Mach. Learn., 3(1):1–122, Jan. 2011.

[6] J. Bonneau, J. Anderson, and G. Danezis Prying data out of a social network OTM 2006 Workshops, volume 4278 of Lecture Notes in Computer Science, pages 1734–1744. Springer Berlin Heidelberg, 2006.

[7] M. E. Newman. The structure and function of complex networks. SIAM review, 45(2):167–256, 2003.

[8] A. Besmer and H. Lipford. Tagged photos: Concerns, perceptions, and protections. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '10, New York, NY, USA, 2012. ACM.

[9] 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.

[10] Z. Stone, T. Zickler, and T. Darrell. Toward large-scale face recognition using social network context. Proceedings of the IEEE, 98(8):1408–1415.

[11] Hakan Yıldız, Christopher Kruegel. Detecting Social Cliques for Automated Privacy Control in Online Social Networks.

Nirajkumar Kunturkar received B.Tech. from COEP, Pune university in Information Technology. At Present he is pursuing M.E. in department of Computer Science and Engineering, P.E.S. College of Engineering, Aurangabad, MS-India.

S. N. Kakarwal received Ph.D., M.E. and B.E. degree in Computer Science and Engineering. She Presently working as Professor in Department of Computer Science and Engineering, P.E.S. College of Engineering, Aurangabad, MS-India. Her research interests include Image Processing, Pattern Recognition and Artificial Neural Network. In these areas, she has published 28 research papers in leading Journals, National and International conferences proceedings. She has bagged 3 Best Paper Award.