My Privacy My Decision Control Of Photo Sharing In Online Media

Diwakaran M[1], Dr D Surendran[2] Dr.V Anandkumar[3]

[1]Assistant Professor , Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore , diwakaran910@gmail.com
[2]Professor Department of Computer Science and Engineering, KPR Institute of Engineering and Technology, Coimbatore
[3]Professor, Sri Krishna College of Engineering and Technology, Coimbatore,India, anandkumar@skcet.ac.in

ABSTRACT –

In today's world, most of the people utilize Online Social Networks (OSN) to mingle with people of their interest. Various new and innovative photo sharing features attract many users and kindle them to post several photos. The user has the privilege of posting any photo on his/her profile and share it with a range of people. Unfortunately, it may leak user's privacy if others are allowed to post, comment, and tag a photo freely. To address this issue we have proposed a system that would notify OSN users, if any of their friends post a content that involves them. The Face Recognition (FR) system extracts facial features of the user's friends and gets trained. If the user's friend posts a photo that includes people other than himself/herself, then that photo is fed into FR system. The system detects all faces in the photo, locates facial details and compares with the faces of the other friends in the list.

Keywords - Online Social Networks, FR System, Notification, Privacy, Feature Extraction, Feature Match

1. INTRODUCTION

Social media has quickly become an essential foundation for communication across multiple generations. The interaction among varied set of people through Online Social Network is immense. It's used for various purposes like interconnecting with friends and extended family, for networking career opportunities, finding like-minded beings across the world to express their thoughts, insights, and emotions. Social Networking enhances many business opportunities. Online Social Networking offers many fancy options of posting and sharing one's thoughts and happiness through photos and videos in social media. This has become a regime for many. Hence, the number of posts posted on the social network has grown large over the period of time. In the past two decades, social media usage and the data shared through it has grown up exponentially. Many data get shared with many people. However many of us are not aware of the target viewers of the shared post and the impacts it can create. Any content, be it textual or visual, when shared among people, becomes a record. It shall remain undisturbed and may reveal details about the person and the associated person in the post directly or indirectly. Since normal OSN users are careless about the content and the target viewers, privacy becomes a question. Social media gives information about a person's life knowingly or unknowingly. Knowingly when they sign up, they input their information such as birthday, city, and other information and then choose their profile's privacy setting. While this has the potential to be the base for many severe privacy attacks, much more information is shared unknowingly. Depending on the details in photos being shared on social media, it is clear that the average person is more at risk to threats like identity theft, cyber stalking, and more. When users share pictures of themselves and friends, usually taken with a smart phone, it also uploads the metadata for that picture. Metadata reveals data about data. In this case, data about pictures shared to social media. It includes more important information which can be used to track down a specific individual. This information includes the cameras identifier number, the GPS Coordinates of where the photograph was taken and more. All this information is unknowingly entered into the metadata when the picture is created. This creates an issue for users who share media without knowledge of this occurring. The exploitation of a single shared photo can result in an adversary.

Privacy becomes a primary requisite, before the users indulge in socialism. There are many privacy policies provided by the Online Social Networks for each of their user to protect their data from unknown people and to curb the privilege of other people from accessing their photos, videos or posts. Most of the privacy policies and settings are intensely concentrated only on the restrictions of others on the user's private account. No policy involves the privacy of the user's friends or circle involved in the content shared by the user. Anyone can post a photo of any user without their knowledge. Only if they're tagged, the concerned person would come to know about the post. Depending upon their willingness, it shall remain on the public wall or removed from it.

Let's consider a situation where-in the person in the photo is unaware of the post being shared. This situation might result in a privacy breach. To give each user, their privilege of their contents over other's post is demandable. We gave thoughts to this situation and proposed a solution for the same. The solution aims at making the users get notified about the posts involving their presence in the photos. Just getting notified does not fully satisfy our privacy needs. Some counter action on the post must be taken.

We propose a system where a person on the Online Social Network site posts a group-content or any other content that involves other than himself then, the faces in the group content must be recognized and detected. The detected faces must be checked across the facial features of their friends. If the features match, then the friend is recognized and intimated about the post. A notification that can both act as an alert and as a response collector will be sent to the recognized friends in the group content. Depending upon their willingness to share their content on the social media, the post will be shared as such or the person's face will be blurred and get posted. Initially while any person gets added to the user's friends circle, few images are collected and maintained privately. These images act as training dataset and would train the face recognition system for further computation. The facial recognition system initially pre-processes the dataset. The facial identities are noted and the Euclidean distance between each facial feature is measured. When a test set is passed to the system, the facial details and the measure between them are calculated and compared. If a match is found, then that system recognizes and alerts the person.

2. PREVIOUS WORK

[1] Mavridis et al. study the statistics of photo sharing on social networks and propose a three realms model: "a social realm, in which identities are entities, and friendship a relation; second, a visual sensory realm, of which faces are entities, and co-occurrence in images a relation; and third, a physical realm, in which bodies belong, with physical proximity being a relation." They show that any two realms are highly correlated. Given information in one realm, we can give a good estimation of the relationship of the other realm. In Stone et al., for the first time, propose to use the contextual information in the social realm and co-photo relationship to do automatic FR. They define a pairwise conditional random field (CRF) model to find the optimal joint labelling by maximizing the conditional density.

[2] In 2009, Jonathan Anderson proposed a paradigm called Privacy Suites :

It allows users to easily choose suites of privacy settings that can be created by an expert using privacy programming or can be created through exporting them to the abstract format or through existing configuration UIs. A Privacy suite can be verified by a good practice, a high level language and motivated users which then can be then distributed to the members of the social sites through existing distribution channels

[3] Privacy and Security Issues in Online Social Networks by IkramUd Di:

The advent of online social networks (OSN) has transformed a common passive reader into a content contributor. It has allowed users to share information and exchange opinions, and also express themselves in online virtual communities to interact with other users of similar interests. However, OSN have turned the social sphere of users into the commercial sphere. This should create a privacy and security issue for OSN users. OSN service providers collect the private and sensitive data of their customers that can be misused by data collectors, third parties, or by unauthorized users. In this paper, common security and privacy issues are explained along with recommendations to OSN users to protect themselves from these issues whenever they use social media.

3. PROBLEM STATEMENT AND PROPOSED SYSTEM

Nowadays we are able to share any photograph we to like on OSNs, whether the photograph contains people (a co-photo) other than themselves or not. Presently there's no restriction with sharing of co-photos. On the contrary, social network service suppliers like Face book want to elaborate on the privacy problems over the period. Privacy is considered a state of social withdrawal. In consent with Altman’s privacy regulation theory, privacy may be a dialectic and dynamic boundary regulation method wherever privacy isn't static however “a selective management of access to the self or to ones group”. During this theory, “dialectic” refers to the openness and closeness of self to others and “dynamic” means that the specified privacy level changes with time.

Disadvantage of existing system:

1. Presently there's no restriction with sharing of co-photos. On the contrary, social network service suppliers like Facebook are encouraging users to post co-photos and tag their friends so as to attract a lot of folks.
2. Unfortunately, on most current OSNs, users do not have any management over the details leaked outside their profile page.
3. People are unaware of their photos being posted on their friend’s profile.

Proposed system:

1. We propose a privacy-preserving, distributed and collaborative training system. In our system, we ask each of our users to establish a private photo set of their own, ensuring to make use of it only for the FR system. We use these private photos to build personal Face Recognition engine based on the specific facial context.
2. We have proposed a novel consensus based approach that would efficiently deal with the privacy of the users.
3. All the faces in the photograph are recognised. Each person’s facial specifications are verified with the FR system, which has student the facial specifications of the user’s friends.
4. User’s friends on the photo are identified and a request notification is sent to their profile for them to decide on uploading the photo.
5. If no negative response is collected, the photo will be posted with no modification.
6. If at all any person rejects, the identity of that particular person in the photo is blurred.

4. SYSTEM ARCHITECTURE

The purpose of this architecture is to explain the working of the project “MY PRIVACY MY DECISION”. The system explains few processes that are both superficial and submissive. The photos collected from each friend while including a person to one’s friends circle, is used as a training dataset. This is fed into a face recognition system, where the photo is split into n-array matrix. All unwanted things other than the facial details are exempted. Details that is necessary to detect and recognize a face alone is collected and fed to the system. Unique measure between the facial details helps the system to learn and find when a test data is passed. Each person is given a unique label say a name for the feature. When any matching face is recognized, the system responds us with the labels fed.

If any user tends to share a group picture, if any person other than the user is involved, then each face is recognized from the groupie and is pre-processed to check with our FR system. The pre-processing involves the same steps involved with training dataset. The facial details once extracted from the pictures are cross checked with the previously trained images. If any match found, then the system responds with the label of the face.

When faces from our friend list are recognized on the photo, a notification is sent to the user regarding the actions the post was exposed to. These are the key processes that run throughout our proposed system.

The system architecture and the flow of data in this research is depicted in 4.2 which essentially gives a sense of data movement from one module to the other and the various essential components the project will need.

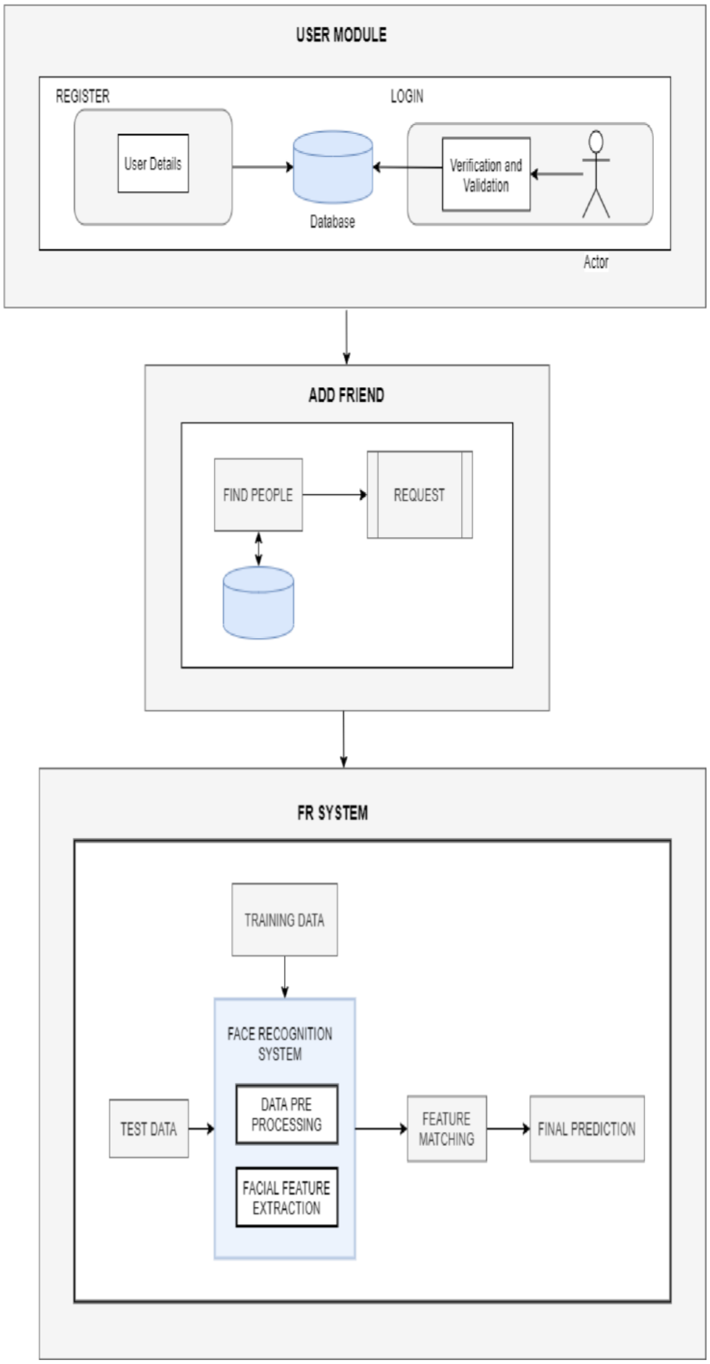
USER MODULE
REGISTER
LOGIN
User Details
Database
Verification and Validation
Actor
ADD FRIEND
FIND PEOPLE
REQUEST
FR SYSTEM
TRAINING DATA
FACE RECOGNITION SYSTEM
DATA PRE PROCESSING
FACIAL FEATURE EXTRACTION
TEST DATA
FEATURE MATCHING
FINAL PREDICTION

Fig 4.1

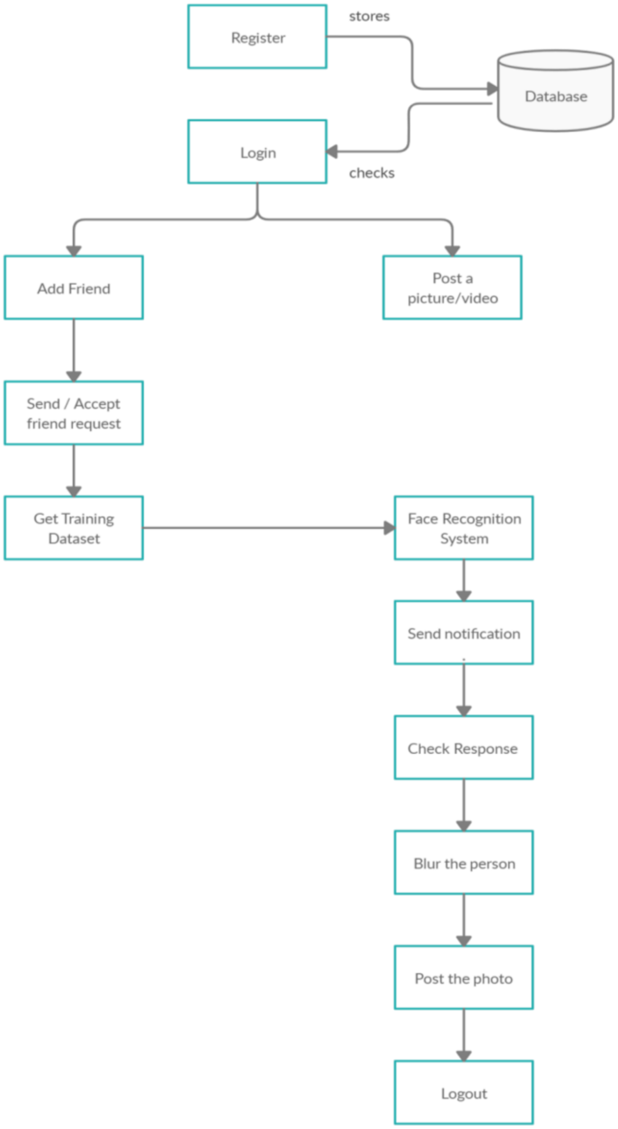

Fig 4.2

5. SYSTEM DESIGN

The process of recognising face from the uploaded photo and sending a notification to the concerned user is done through various modules. The modules involved are as follows:

5.1 User module:

In a socially connected society of people, social networking helps us connect and communicate to all our lost and known contacts. This simulation portal requires a Registration and a Login module that allows the user to access the portal. Registration is one of the primary modules in any system. User details such as Name, age, Date of Birth, Email ID, password, etc are collected and stored in a database. It also prompts the user to create a profile by uploading their personal photo that is later used to train the system. When a user logins to the system, the credentials are verified and validated with the details stored in the database. Once the user is validated, he/she is given access to use the Online Social Network. They are given access to view contents shared to them by their friends, view public contents, add friends and post contents.

5.2 Add friend module:

Once the user registers and logins to the portal, he/she is given the privilege to access the Online Social Networking portal. The registered users can connect with their friends, families, like minded individuals and people of their interest. Based on the connection, details and their friends circle, people who are likely to be known to the person shall be suggested. The user shall request any person to add into his/her circle. That request will be sent to the concerned person intimating the user's interest. It's the choice of the individual to accept or ignore the request. If the user is accepted to be in the person's circle, then the person's profile and posts are made visible. All privacy settings are applicable only to those not in their circle. The user shall comment, tag and share the friend's content if applicable.

5.3 Face recognition module:

Posting group photos in social media may leak co-persons in the posts' privacy. In order to address this scenario when sharing a photo containing individuals other than himself/herself, we provide a mechanism to enable each individual in a photo be aware of the posting activity and participate in the decision making we provide a privacy option where in the co-persons in the post get detected automatically through a facial recognition (FR) system. The FR system recognises everyone in the photo by extracting features.

The photo which is being uploaded is detected for faces and results in coordinates of the location where the face is detected. These coordinates are used to match with the trained data set that is obtained from the profile picture that is being uploaded at the time of profile creation. The faces are tested against the friends data set and the co-owners of the photo are identified by feature extraction and the notification is send to the detected friends.

5.4 Notification module:

When each people in the group content such as photo is located and detected, faces are compared with the already trained faces of their friends. If any face matches with the trained faces, then that person on the friend list, whose faces have been detected are notified about the post. Any person can share any content on his/her wall. But if that content is related to some other person, then it's the right of that person on the post to be notified about it. This module serves the purpose of acknowledging the breach of the user's content without their consciousness. An alerting notification is sent to the user and it remains visible on the user's page.

6. CONCLUSION AND FUTURE WORK

When most of the people use Online Social Networks to socialize, then there is a need to provide enough privacy policies that would prevent privacy leakage. The designed portal will let user know when others post their photos, without user's knowledge. The system reads the photo and learns all facial specification. The photo is fed into the trained system. It then recognizes all the faces in it. It compares and predicts the faces based on the similarity of facial features and labels them. Any unknown person in the photo is automatically blurred, preserving the privacy of the unassociated circle. Our system finds and recognizes people with high accuracy and correctly predicts the faces. It works efficiently with less latency. However the current system is designed only for the close circle. Hence the system will be widened to next circle of people, say friends of friends. A responsive GUI that will result in blurring the user's identity will be included thereby ensuring the user's control over the post. These will eventually increase the privacy and control over their photos.

REFERENCES

[1] Mavridis et al. *Study the statistics of Photo Sharing on social networks and propose a three realms model*.

[2] Jonathan Anderson in 2009, proposed a paradigm called *Privacy Suites*.

[3] IkramUd Di, *Privacy and Security Issues in Online Social Networks*.

[4] MichelleMadejski :The Failure of Online Social Network Privacy Settings.

[5] NahierAldhafferi, Charles Watson and A.S.M Sajeev: Personal Information Privacy Settings Of Online Social Networks and Their Suitability For Mobile Internet Devices.

[6] Privacy Settings in Online Social Networks -- Preferences, Perception, and Reality.

[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, 2015. SpringerVerlag.