Research Paper
Volume : 5 | Issue : 8 | Special Issue August-2016 • ISSN No 2277 - 8179

Social guard – A secure photo sharing innovative in online social networks

Engineering

KEYWORDS: Index Terms—Collaborative learning, EigenFace algorithm, SVM, Symmetric encryption, Joint privacy control, Exposure policy.

Ashitha R N — PG Scholar, Computer Science and Engineering Vedavyasa Institute of Technology Karad parampa, Malappuram

Ginnu George — Asst.Professor, Computer Science and Engineering Vedavyasa Institute of Technology Karad paramba, Calicut

ABSTRACT

Photo sharing is a recent feature provided by online social networks. The users get attracted with this feature and shares different photos including their selves and others. However, this may violate the user privacy. I.e., any users can share any other's photo without their permission. To avoid this, a new system is introduced which consists of a face recognition system. Users in a group photo will be identified by the system and send notification about the photo posting. The photo publishing is a joint decision. The face recognition system uses Support Vector Machine (SVM) concepts for data classification. The latency of the photo sharing can be reduced using an extra layer of alert mechanism. The data storage is secured using encryption mechanism.

I. INTRODUCTION

Nowadays any photo can be shared on OSNs, regardless of whether this photo contains other people (is a co-photo) or not. There is no restriction 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. However, the problem arises when the co-owners are not willing to share their photos and hence it becomes a privacy violation. If the privacy over Online Social Networks is too restricted, the user will feel lonely or isolated. On the other hand, if the actual level of privacy is smaller than the desired one, the user will feel over-exposed and vulnerable.

Unfortunately, on most current OSNs, users have no control over the information appearing outside their profile page. The lack of joint privacy control can inadvertently reveal sensitive information about a user. To mitigate this threat, OSN users are asked to specify a privacy policy and an exposure policy. Privacy policy is used to define group of users that are able to access a photo when being the owner, while exposure policy is used to define group of users that are able to access when being a co-owner. These two policies will together mutually specify how a co-photo could be accessed.

The new social network- social guard is introduced to avoid all the problems of group photo sharing over social networks. The new approach makes the photo sharing more secure in a privacy preserving manner. The system uses face recognition method to recognize each face in a group photo and send notification to each user in that photo. The photo publishing is a joint decision, which must be approved by all the members in that photo.

To construct an FR system, Support Vector Machine concepts along with EigenFace approach is used. The following sections will explain more about the FR system concepts and techniques.

Support Vector Machines (SVMs) are a set of related supervised learning methods used for classification and regression. They belong to a family of generalized linear classifiers. In another terms, Support Vector Machine (SVM) is a classification and regression prediction tool that uses machine learning theory to maximize predictive accuracy while automatically avoiding over-fit to the data. Support Vector Machines (SVMs) are formulated to solve a classical two class pattern recognition problem. SVM can be adapted to face recognition by modifying the interpretation of the output of a SVM classifier and devising a representation of facial images that is concordant with a two class problem. A multi class SVM will be constructed by combining number of two-class SVM classifiers.

This chapter has given an overview about Face Recognition using SVM and its need and scope in privacy and security in Online Social Networks. In modern world, impact of Social networks are increased and hence the security aspects. A new online social network which emphasizes privacy and security in photo sharing is proposed in this work.

Further chapters discuss the related work, existing system with its drawbacks, proposed system and conclusion.

II. RELATED WORK

In [1], Andrew Besmer et al. conducted study on photo tagging in social networks. Increased access to a person's photo has led to these images being used for purposes that were not intended. The study suggest a number of design options, based on that photo owner and co-owner can take the decisions jointly. However, it consists of manual process of tagging and un-tagging.

Nithya Sara Joseph in [2] describes privacy setting for a shared data including multiple users and proposes a system in which collaborative management of shared data is included. However, a potential owners can be identified only when he is tagged and the privacy settings are manual.

Kai-Bo Duan et al. in [3] conducted a study on identifying the best multi class SVM method. The different multi class SVM methods discussed are:

- One-versus-all method using winner-takes-all strategy
- One-versus-one method using max-wins voting
- One-versus-one method using pairwise coupling strategy

The study proves that the one-versus-one method using pairwise coupling strategy uses Platt's posterior probabilities to give better results comparing other two methods and has significantly smaller mean values of test error.

In [4], Divyarajsinh et al. describes the common methods like holistic matching method, feature extraction method and hybrid methods used for Face recognition. The paper also discuss about the applications of Face Recognition system including Security, Image Database investigations, Surveillance etc. Current FR systems use hybrid methods, which is a combination of both holistic and feature extraction methods. Generally 3D Images are used in hybrid methods.

Radhika S. Fulzele et.al. [5] in 2015 conducted a survey on message filtering from OSN user walls. The study proposes a system in which users directly can control the posted messages on their wall. Filtering rules are applied over unwanted messages that prevent vulgar

messages. However, this method is applicable to text data only.

Justin Becker et.al. in [6] conducted a study on privacy risks in online social networks. They proposed a tool called PrivAware, a tool to detect and report unintended information loss in online social networks. The tool provides users with the steps necessary to improve their overall privacy measurement. However, one of the suggestions provided by the tool to eliminate the security threat is, to remove the friend having common attribute, which may affect the social relationship.

Vinay Hiremath et.al. in [7] conducted research to develop computational models to identify the faces, which are relatively simple and easy to implement. The Eigenface approach is used with Principal Component Analysis (PCA) algorithm for the recognition of the images.

P.Latha et.al. in [8] propose a neural based algorithm to detect frontal views of faces. The dimensionality of face image is reduced by PCA and the recognition is done by the Back propagation Neural Network (BPNN). However, neural network based face recognition is not that popular because of the fact that neural networks require large set of training sample compared with SVM for getting the correct output.

Kurt Thomas et.al. in [9] examine how the lack of joint privacy controls over content can inadvertently reveal sensitive information about a user including preferences, relationships, conversations, and photos. However, major limitation is, there is no method of automatically identifying the individuals in a post/image. The system works based on manual tagging.

Kaihe Xu et.al. in [10] study the scenario when a user shares a photo containing individuals other than him/her. To curb the privacy leakage, the proposed system helps to enable individuals potentially in a photo to give the permissions before posting a co-photo, with the help of an FR system. However, since the co-photo could only be post with permission of all the co-owners, latency introduced in this process will greatly impact user experience of OSNs.

III.PROBLEM STATEMENT AND HYPOTHESES

The proposed methodology focuses on an improved technology for providing privacy over co-photo sharing in social networking sites by reducing the latency that may occur during this process. The system is an Online Social Network, Social Guard; that includes a Face recognition system along with an additional layer of notification.

A. FR SYSTEM WITH SOCIAL CONTEXTS

Social contexts contain a large amount of useful information which could be utilized as a priori knowledge to help the facial recognition. There are three realms for the study of social contexts. The three realms include a social realm, in which identities are entities, and friendship a relation; a visual sensory realm, of which faces are entities and occurrence in images a relation; and a physical realm, in which bodies belong, with physical proximity being a relation. With the priori distribution, while trying to recognize people on the co-photos, the FR engine could focus on a small portion of 'close' friends.

B. FR SYSTEM

Consider user i has a private training set of size. From the private photo set, a user detects and extracts the faces on each photo with the standard face detection method. For each face, a vector of size p is extracted as a feature vector. These feature vectors are used in constructing binary classifiers. A multi-class classification system is constructed by combining several binary classifiers together.

One-against-all method

It uses winner-take-all strategy. A data point would be classified under a certain class if and only if that class's SVM accepted it and all other classes' SVMs rejected it. This strategy consists of constructing one SVM per class, which is trained to distinguish the samples of one class from the samples of all remaining classes. Usually, classification of an unknown pattern is done according to the maximum output among all SVMs.

It constructs n binary classifiers for each of n classes. The goal of each binary classifier is to distinguish one class from the rest with a decision function. Hence, the ith decision function fi is trained by taking records from user i as positive samples and the records from all the other users as the negative samples. When a testing record x comes, if fi concludes that it belongs to class i, x is labeled as class I.

One-against-one method

The method uses max-voting-win strategy. The "one against one" strategy, also known as "pairwise coupling", "all pairs" or "round robin", consists in constructing one SVM for each pair of classes. It constructs n (n-1)/2 binary classifiers, in which each classifier is aimed to distinguish two classes. The idea is that if any two classes can be distinguished, then any of them can be identified. Hence, classifier uij is constructed by taking records from i as positive samples and records from j as negative ones. When a new record x comes, if concludes that x is in class i, then the vote of class i is added by one. After testing all the n (n-1)/2 classifiers, x is assigned to the class with the largest voting value.

C. CLASSIFIER REUSE FOR SVM STRATEGIES

There is a classifier computation algorithm, which is used to compute the classifiers from a social site. The basic notations include user i as the initiator when Xi is used as the positive training samples and user j as the co-operator when Xj is used as negative samples. For a node i in friendship graph, Bi denotes its one hop neighbors.

Classifier computation algorithm
Input: Users in social network
Output: Classifier list

1. Initialize classifier list as null for all the users.

2. For each user I, do

3. Check each user j in the neighbourhood of I,

4. If (uij) is not in the classifier list, do face recognition for the user using EigenFace method.

5. Set uij = - uji (Classifier reuse)

6. Add uij in the classifier list i or j based on the +ve or –ve result in the face recognition system

7. End if loop and for loops.

8. Now check for each user pair in the neighbourhood of I, (k,j ; K != j)

9. If ukj is not in the classifier list, do face recognition for the user using Eigenface method.

10. Else, request the trained set result from user j

11. Add ukj in the classifier list.

12. End

According to this Algorithm, there are two steps to build classifiers for each neighbourhood: firstly find classifiers of {self, friend} for each node, then find classifiers of { friend, friend}.

The existing system sends notification to the co-owners of a photo before publishing it on the web. The co-owners will be identified using the Face recognition method. The co-owners are then allowed to accept or reject the photo posting decision. Even though this system prevents the problems occurred due to privacy violations in a

group photo sharing, it fails in some situations, where the publishing will wait for the decision of co-owner forever. This increases the latency in photo publishing and hence reduces the social media experience of user. Therefore the proposed research work focuses on an improved version of existing system in which an additional layer of notification will be added. This will reduce the latency that can occur in photo sharing and hence improve the photo sharing experience of social media users.

IV. SYSTEM OVERVIEW

This section presents the detailed description of the system. The system is an Online Social Network „Social Guard that includes an additional layer of notification, which sends mobile message as well as the mail to the registered mobile number and email of the co-owner of that photo, if he is not responding to a group photo request even after a specified time period. The system also consists of a symmetric encryption mechanism for the confidential data stored in the database to make it little more secure. For this purpose, Rijndael algorithm is used. With the new layer of notification system, the latency of photo sharing can be reduced to an extent and hence provide a secure way of photo sharing with enhanced privacy.

A. STEPS IN PROCESS

Profile creation and training set adding

Profile creation is the first step of the entire process. The user will be asked to compulsorily register his correct email and mobile number during the registration process. Once the profile picture is added, it will be converted into a set of feature vectors. This resulted image will be stored in the system even after changing the profile picture. For the new profile picture, a new feature vector will be added.

Face recognition and Eigenface method

When a new group photo is posted, the system will recognize each person in that picture by comparing it with the training samples. The method used for this face recognition is Eigenface method.

Classifier computation and photo post request

The classifier computation will be done based on the classifier computation algorithm. The algorithm finds the list of friends and friend's friends in a privacy preserving manner. The notification will be send to those people in the classifier list.

Notification to the registered mobile and email

This module works based on the user behavior. Once a photo post request is send, the system will start counting for the days. If there is no response even after 2 days, the message will be send to the registered mobile and email alerting about the photo sharing. If there is no response even after 4 days, the photo will be published on the wall, leaving a message saying the photo is posted. The alert mechanism is added to make the users curious about their photo privacy, even though not an active user of social networks.

B. ALGORITHM FOR THE ALERT MECHANISM

Input: Classifier List C from the classifier computation algorithm [10]

1. Check if the user Cij selects the „Allow notification option from his privacy settings.

2. If yes, count the time from the moment of photo posting.

3. If no response for 2 days, send mail and message.

4. Count the time till it reaches 4 days.

5. Publish the photo and send alert saying photo is posted.

6. End if loop

7. If 'Allow notification' is set to 'No', notification send to all users in {C-Cij}

8. End

C. EIGENFACE METHOD

The task of facial recognition is discriminating input signals (image data) into several classes (persons). Input signals are highly noisy (e.g. the noise is caused by differing lighting conditions, pose etc.), yet the input images are not completely random and in spite of their differences there are patterns which occur in any input signal. Such patterns, which can be observed in all signals, could be - in the domain of facial recognition - the presence of some objects (eyes, nose, mouth) in any face as well as relative distances between these objects. These characteristic features are called eigenfaces in the facial recognition domain (or principal components generally).

The algorithm for the facial recognition using eigenfaces is basically described below. First, the original images of the training set are transformed into a set of eigenfaces E. Then the weights are calculated for each image of the training set and stored in the set W. Upon observing an unknown image X, the weights are calculated for that particular image and stored in the vector WX. Afterwards, WX is compared with the weights of images, of which one knows for certain that they are face.

V. PERFORMANCE ANALYSIS

For the strategy of one-against-all, each user j in Bi are associated with a binary classifier fj(.) by making j initiator and {k€ Bi, k!= j} co-operators. Denote Di the degree of user i, there will be Di +1 classifiers and each classifier involves Di + 1 users. The cost to build one classifier is hence O(nE Ta^{Dd}) where O(nE) is the cost of local SVM training with n training itemsTa is number of iterations to converge and^{D}is the average degree for a node in friendship graph. Hence, total cost in one neighbourhood is O(nE $Ta^{D}2$)

For the strategy of one-against-one, ½($\overline{D(D}$ +)) systems need to be trained. The cost for each binary system with 2 users is O(nE To), where O(nE) is the cost of local SVM training with n training items, To is number of iterations to converge. Hence, total cost in one neighbourhood is O(nE $To^{D}2$).

Comparing two strategies, intuitively, To should be much smaller than Ta, because less data is considered. Another factor makes one-against-one strategy appearing is that the classifiers can be reused among mutual friends. In comparison, classifiers cannot be reused in the one-against-all strategy because they are trained with different co-operators.

A. NETWORK WIDE PERFORMANCE

The project is simulated a real life social network with the small world network. In a small world network, there are 3 input parameters: the total number of vertex N, the average node degree and rewire probability p. It uses dataset of 28 different people each one with 20 different facial images as the data. The database of "Face Recognition Data, university of Essex, UK" is used to assign training set for each simulated users. Test user profile is created for around 20 people and then added profile photos.

Fig 1.a shows the average number of iterations, which are increasing with the number of participants. In this simulation, each user has 20 training samples and each sample is a vector of 20 features.

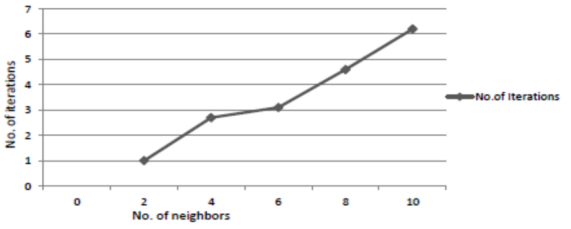

Fig 1.a.The average iterations against the number of neighbours

The figure shows that for the large number of neighbors, the number of iterations required increases.

B. FACIAL RECOGNITION PERFORMANCE

In this subsection, recognition ratio against number of friends is studied. Standard face detection using OpenCV forum is used for face detection and Eigenface is used to extract features and vectorize the training image. The performance is measured using the false positive rate. A false positive recognition will reveal the test image to the wrong person. Thus, a low false positive rate is desirable.

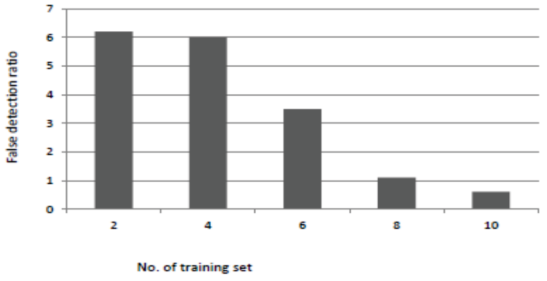

Fig 1.b.False detection ratio

The figure 1.b shows that as the number of training samples increases, the system gives better result by reducing the false detection ratio. The main advantage of this system is that it gives better result with comparatively less training samples.

I. EVALUATION

The system is evaluated with two criteria: network-wide performance and false detection ratio. This section describes the implementation details of the system.

II. IMPLEMENTATION

In the proposed methodology, the face recognition system first creates a feature vectors from the profile pictures added. This result will be stored in a folder called „Trained Images . For face detection, OpenCV library 2.4.6 is used and Eigenface method is used for face recognition.

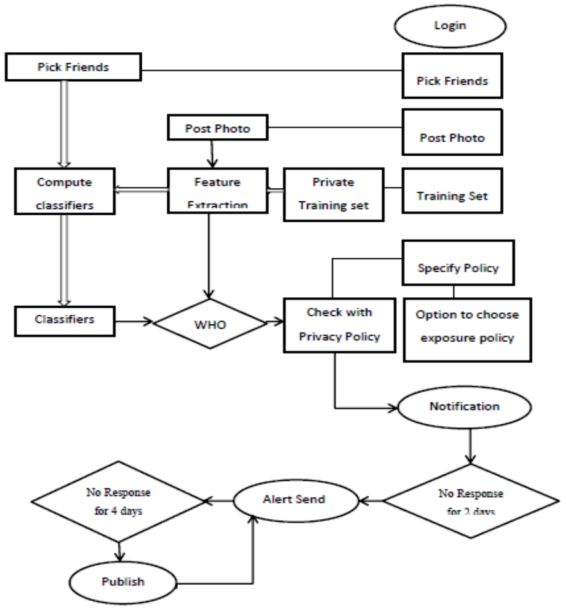

Fig.3 System Architecture

The figure shows the architecture of the social guard. The user will specify the friends by inviting them and accepting their friend request. Once they are friends, the person 1 will get the notifications of the photos which he included and shared by person 2. For this purpose, the person 1 must choose the privacy and exposure policy. The person 1's other friends who are not friends with person 2 can also get notification if they are present in that particular photo. If all agree to post the photo, the photo will be published on the owner's page like a normal photo. A thread will start running throughout the process, once we open the system. This will check for co-owner's response once the notification sent. If the time goes beyond the specified time limit, the alert mechanism will send a mail and message to the co-owner.

VIII. CONCLUSION AND DISCUSSION

The revolutionary changes in Internet have introduced new features in Online Social Networks. These new features are the key factors for the popularity of these sites. One of the main features of social network is the photo sharing feature. Anyone can share any photos over internet without any limitation. Some websites even allow tagging someone in a photo, which means a virtual link to some other's space or 'wall'. The unlimited photo sharing over internet may reveal the identity of person. Current features allow the user to share any photos including other individuals without asking their permission. This is actually a privacy violation.

This research work proposes a social network with improved privacy. The user will be notified if someone shares his/her photo. The photo will be published only if the person in that photo is allowed to share his/her photo. The module is implemented using a face recognition system along with the alert mechanism. The face recognition system uses eigenface algorithm to recognize faces in a group photo and notify that users.

The alert mechanism is implemented to regain the social media experience of user on photo sharing, by reducing the latency that can be introduced by the notification system. The proposed method gives accurate result with less rate of false detection ratio.

The future works will be moving the data storage to a cloud based server.

IX. REFERENCES

[1.] A.Besmer and H. Richter Lipford, "Moving beyond untagging: photo privacy in a tagged world" in SIGCHI conference on human factors in computing systems, pages 1563-1562, New York, NY, USA, 2010.

[2.] [2] Nithya Sara Joseph, "Collaborative data sharing in online social network resolving privacy risk and sharing loss" in IOSR Journal of Computer Engineering, volume 16, issue 5, Ver. VI (Sep-Oct. 2014), PP 55-61.

[3.] Kai-Bo Duan and S. Sathiya Keerthi, "Which Is the Best Multiclass SVM Method? An Empirical Study", MCS 2005, LNCS 3541, pp. 278–285, 2005

[4.] Divyarajsinh N. Parmar and Brijesh B. Mehta, "Face Recognition Methods & Applications" in Int.J.Computer Technology & Applications,Vol 4 (1),84-86.

[5.] Miss. Radhika S. Fulzele and, Prof. Vipul Dalal, "A Survey on an Intelligent System for Unwanted Message Filtering from OSN User Wall", in International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015.

[6.] Justin Becker and Hao Chen, "Measuring Privacy Risk in Online Social Networks" in web 2.0 security symposium, 2009

[7.] Vinay Hiremath and Ashwini Mayakar, "Face Recognition Using Eigenface Approach"

[8.] P.Latha, Dr.L.Ganesan and Dr.S.Annadurai, "Face Recognition using Neural Networks" in Signal Processing: An International Journal (SPIJ) Volume (3): Issue (5)

[9.] Kurt Thomas, Chris Grier and David M. Nicol, "unFriendly: Multi-Party Privacy Risks in Social Networks" in PETS'10 Proceedings of the 10th international conference on Privacy enhancing technologies pages 236-252 VVIT Secure photo sharing innovative in social networks Dept. of CSE 50 M Tech 2014 Admission

[10.] Kaihe Xu, Yuanxiong Guo and Linke Guo, "My Privacy My Decision: Control of Photo Sharing on Online Social Networks" in IEEE Transactions on Dependable and Secure Computing (Volume:PP , Issue: 99)

[11.] D. Rosenblum, "what anyone can know: the privacy risks of social networking sites" in security privacy, IEEE, 5(3):40-49, 2007

[12.] M.Turk and A. Pentland, "Eigenface for recognition" journal of cognitive neuroscience", 3(1):71-86, 1991

[13.] J. C. Platt, N. Cristianini, and J. Shawe Taylor, "Large margin dags for multiclass classification" in Advances in Neural Information processing systems 12, pages 547-553, 2000

[14.] www.wikipedia.org

[15.] www.shervinemami.info/faceRecognition.html