International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 10 (2018) pp. 7360-7363

Privacy Monitoring and Restriction Algorithm

Abhind A[1]
Bharati Vidyapeeth's College Of Engineering
New Delhi, India.

Sagar[3]
Bharati Vidyapeeth's College Of Engineering
New Delhi, India.

Harmeet Kaur Bawa[2]
Bharati Vidyapeeth's College Of Engineering
New Delhi, India.

Shilpa Gupta[4]
Bharati Vidyapeeth's College Of Engineering
New Delhi, India.

Abstract:

For any social media application, such as Facebook, YouTube or Whatsapp, the major concern lies in securing a user's personal content. When a user shares their media online, they may want certain parameters to protect their content from becoming a social property at the behest of the user's privacy. Privacy Restriction System works by identifying facial features of a user from videos and maps them to a previously maintained database of user images for identifying the particular user. This user is then intimated about the video being shared on the particular social media and asks for consent of being circulated to mass. If accepted, the video can be circulated among the mass, otherwise, the video will be flagged and not be allowed to circulate further, as well as be removed from the social media site.

Keywords: Face Recognition, Image Mining, Video Recognition, Database Mapping, Social Media, Privacy Control

INTRODUCTION

Social Media started a trend of sharing, sharing images, videos, files and simply, data. With that came the need of protecting that data from unwanted hands. Security has become a primary issue with the advancement of technology. Media shared online can be stolen for obtaining private information, harassment, abuse, for one's amusement, copying data to proclaim as one's own, et al. Even if images are protected by the application from downloading, they can be recorded by recording the screen or by taking screenshots, and even if not that, then using another device to record that data.

Hence, this system works at the backend of the system i.e. instead of blocking content that is reviewed manually by designated people or flagged by users, all the review is done by the system.

Privacy Restriction System works by providing privacy at the user level of applications by actively monitoring uploads or shares by users. A database is maintained by the application which contains information of user such as images of the face and basic details such as name, email address and linked phone number, which may be obtained by the application itself or central databases of the government. Facial features such as eyes, nose and lips are mapped to the pixel vector values stored in the database.

RELATED WORK

Since the beginning of human civilization, humans have been actively involved in identifying and recognizing each other and objects we see around us. This nature has transferred from humans to machines as automation sets in. Identification has become a primary motive for automated systems as they are deployed for security, privacy and authorization. They have even been employed as systems for people with disabilities by providing face and facial muscle recognition techniques. A very notable example would be the facial muscle recognition system developed by SwiftKey for Professor Stephen Hawking. The software has been a very successful development in the field of facial recognition as even minor twitching of a muscle can be used to interpret a message of the Professor. Another exemplary work which must be quoted is of Facebook's face tagging feature. This feature helps users by self-tagging images of humans appearing in the photographs the user uploads. It matches several features of a human face mapped by Facebook's algorithm and compares them with the extracted features of the uploaded profile pictures of that person identified by the algorithm for tagging. This also has been extended to provide facial recognition for logging into accounts, all happening at real time. Apple's face recognition has been touted to be the best ever. Thus, the solution needed by today's generation not only needs to be viable for usage, but be fast paced and highly accurate to allow fully automated systems. This system uses the likes of the facial recognition system but while integrating it to an online social networking platform. Due to increase in the number of hate crimes, violence, racism, trolling, personal attacks, impersonations, phishing, etc. several applications have devised algorithms to combat such problems, such as YouTube's bots which flag videos with abusive words or inappropriate images, similarly with Facebook.

Humans can easily distinguish between other humans they see based on several features such as the face of a person, body structure, height and gait, but expecting a computer to identify humans requires training similar to what human brains do. Humans learn to recognize and distinguish by noting key spectral features of another human by learning the face built, body built, eye color, nose structure, lips, etc. and similarly a

computer is trained to identify and map the distinct features of a human such as eyes, nose and lips. This is done by identifying boundaries of the features of the human, such as identifying the facial boundaries. As a human brain stores the images of a human for recognition, the same is done for a computer system, only by storing the facial features in a database for easier management. [1]

While it is estimated that a human can recognize 100 – 1500 faces in a lifetime but a facial recognition system can be capable of recognizing an infinite number of faces.

Requirements for a satisfactory facial recognition system are:

- Ambient lighting conditions
- Clarity of image
- Granularity of image
- Number of images taken
- Orientation of image
- Face coverage
- Absence of sunglasses or eye patches
- Maintenance of database
- Efficient mapping algorithm

Ambient lighting conditions are required for improving the facial recognition so as to illuminate key features to be mapped, which includes appropriate natural or artificial lighting which can illuminate the entire face or at least be 35% visible partially. [1, 2]

Image granularity plays a key role since high image granularity refers to low clarity of image and hence eigenfaces would be difficult to map. Eigen face mapping requires shades of dark and light of the image to be created into a matrix for recognition. Hence, low clarity would map the face to the wrong human's image. [1, 3]

The number of images taken matters the most since appropriate Eigen faces are then created from the taken images so as to increase the face mapping efficiency as well as improve matching speed. Thus, if a person was to upload a video with his/her face at different angles, the algorithm would still be able to map the person. [4]

Orientation of image refers to the side of the face that is visible. Usually databases are maintained with the frontal face map but this algorithm will be implementing side faces [6] to increase efficiency.

Glasses are acceptable in this algorithm but since it takes the eyes, nose and mouth, sunglasses and eye patches cover the eye which makes it impossible to detect one of the required [7] unique traits for matching.

Database maintenance needs to be managed time to time due to the size of such a system's database. Mismanagement can cause mismatches to occur more frequently.

Efficient database mapping technique is needed so as to match the correct Eigen face of the scrutinized face with the database stored Eigen face.

THEORY

Privacy Monitoring and Restriction Algorithm consists of six parts namely:

- Video Retrieval
- Video Scanning
- Face Detection
- Face Recognition
- Face Tracking
- Informing The Victim

The algorithm takes time sliced video frames from input video then applies the face detection algorithm for cropping out the faces based on the different white and black shades in the image. Then it applies recognition algorithm on the cropped image based on the data from image database after successful recognition it constantly tracks the face in the video to get the duration for which the particular face was in the video.

The following are the steps involved in the algorithm:

Video Retrieval:

- The video is retrieved from the backend of the system, i.e. where the application is hosting the content of its application, the server.
- Users upload videos onto applications which gets stored on the application's server. This step of the algorithm retrieves videos from the server.

Video Scanning:

- The video is scanned to detect human faces in the first run. This step is for identifying human presence only.
- The time frames where human presence is detected are time sliced to reveal still images from the video.

Detection and storing:

- Face detection using Viola-Jones algorithm, in this algorithm a slider window is used over an image to find dark-light regions to detect face in the image. The ratio of the image remains unchanged but the size can vary depending upon the size of the face.
- This step consists detection of facial features and then storing the detected features in the database for future recognition.
- This step uses matrices for storing of the dark and light region values for identifying the faces of the human.

Recognition and tracking:

- The video is taken as input and detection algorithm is applied to it, after successful detection of face, recognition algorithm is applied to the detected face.
- Recognition algorithm consists of PCA i.e. Principal Component Analysis, to find a match in the database. This technique is also used in image compression. It is a way of identifying patterns in data, and expresses the data in the way that highlight their similarities and difference.
- The PCA of the image in dataset and input is measured and the difference between them is calculated, the

image with the least difference is the result for the face recognition.

- After successful recognition the software tracks the face in the video and will calculate the time period for which the face was shown in the video.
- Kanade-Lucas-Tomasi KLT algorithm is used for tracking, this algorithm needs at least two points for tracking, the points are supplied by Shi Tomasi corner algorithm.
- Shi Tomasi corner algorithm provides the corner points and KLT algorithm tracks those points.

Informing the victim:

- This step takes the contact information of the recognized face and then informs the same about the video being posted by unauthorized person.

If the victim's video was published without his permission they victim can flag the video in the system and the video would be removed from the online platform.

RESULTS AND DISCUSSION

The face detection phase has been completed with 80% accuracy pertaining to ambient light conditions, multiple face detection and mapping. The 20% chance of failure may arise due to dull lighting, hair covering the face, eye patches, sunglasses, etc.

The following table represents the success and failure rates of detection:

Test cases:

This project will be further implemented on a server to create a prototype that will be locally hosted to run on an android application to test the complete algorithm's working. This algorithm has been successfully tested on real time mapping and detection for single as well as multiple faces.

Local Dataset Results:

$$Success\ Rate\ = \frac{Number\ of\ test\ cases\ matched\ successfully}{Total\ Number\ of\ Test\ Cases}$$

$$Success\ Rate\ = \frac{15}{20} = 75\%$$

$$Failure\ Rate\ = \frac{Number\ of\ test\ cases\ not\ matched}{Total\ Number\ of\ Test\ Cases}$$

$$Failure\ Rate\ = \frac{5}{20} = 25\%$$

Global Dataset Results:

$$Success\ Rate\ = \frac{Number\ of\ test\ cases\ matched\ successfully}{Total\ Number\ of\ Test\ Cases}$$

$$Success\ Rate\ = \frac{75}{100} = 75\%$$

$$Failure\ Rate\ = \frac{Number\ of\ test\ cases\ not\ matched}{Total\ Number\ of\ Test\ Cases}$$

$$Failure\ Rate\ = \frac{25}{100} = 25\%$$

The global dataset has been obtained from AT&T which contains well illuminated photographs of a set of humans.

These photographs were first preprocessed using our algorithm. Preprocessing steps are:

- Crop images by recognizing presence of a face
- Obtain boundary points of face
- Analyze facial features to obtain shade differences
- Plot shade differences in matrix
- Obtain eigenfaces

Adding images to the database:

- MATLAB requires images to be added into the software
- Add directory containing images to MATLAB

CONCLUSION

This project can successfully perform the following steps of the created algorithm:

- Video Retrieval
- Video Scanning
- Face Detection
- Face Recognition
- Face Tracking
- Informing The Victim

The algorithm can take time sliced video frames from input video to apply the face detection algorithm for cropping out the faces based on the different white and black shades in the image. Then it applies recognition algorithm on the cropped image based on the data from image database after successful recognition it constantly tracks the face in the video to get the duration for which the particular face was in the video.

REFERENCES

[1] Park, B. and Lee, J. (2014). High Efficient Viola-Jones Detection Framework for Real-Time Object Detection. Journal of IKEEE, 18(1), pp.1-7.

[2] K. T. Talele, S. Kadam, A. Tikare, Efficient Face Detection using Adaboost, "IJCA Proc on International Conference in Computational Intelligence", 2012.

[3] T. Mita, T. Kaneko, O. Hori, Joint Haar-like Features for Face Detection, "Proceedings of the Tenth IEEE International Conference on Computer Vision", 15505499/05

[4] T. Ahonen, A. Hadid, M. Peitikainen, Face recognition with local binary patterns. "In Proc. of European Conference of Computer Vision", 2004.

[5] J Lu, K. N. Plataniotis, A. N. Venetsanopoulos, Face recognition using LDA-based algorithms, "IEEE Neural Networks Transaction", 2003.

[6] M. A. Turk and A.P. Pentland, Face recognition using eigenfaces, "Proceedings of the IEEE", 586-591, 1991.

[7] I. Kukenys, B. McCane, Support Vector Machines for Human Face Detection, "Proceedings of the New Zealand Computer Science Research Student Conference", 2008.

[8] L. Wiskott, M. Fellous, N. Krger, and C. Malsburg, Face recognition by elastic bunch graph matching, "IEEE Trans", on PAMI, 19:775–779, 1997.

[9] M. M. Abdelwahab, S. A. Aly, I. Yousry, Efficient WebBased Facial Recognition System Employing 2DHOG, arXiv:1202.2449v1 [cs.CV].

[10] W. Zhao, R. chellappa, P. J. Phillips, Face recognition: A literature survey, "ACM Computing Surveys (CSUR)", December 2003.

[11] G. L. Marcialis, F. Roli, Chapter: Fusion of Face Recognition Algorithms for Video-Based Surveillance Systems, Department of Electrical and Electronic Engineering- Univ- ersity of Cagliari- Italy.

[12] A. Suman, Automated face recognition: Applications within law enforcement. Market and technology review, "NPIA", 2006.