Security in Artificial Neural Network Based Face Recognition

Mohammad Fahim Akhtar

Research Scholar (Computer Science), CMJ University, Shillong, Meghalaya

Abstract— Facial recognition technology is growing rapidly and at the same time interest in face recognition systems is increasing constantly. Face recognition systems are the computer-based security system which helps to identify the specified individuals by using the surveillance cameras. Face recognition systems use complex algorithms to compare the faces which were observed by the camera with the database of individual photographs. This paper discusses about the artificial neural network based face recognition systems and its security issues and threats.

Keyword — Face Recognition System, Computer Based Security System, Artificial Neural Network, Face Detection

----------♦----------

1. FACE RECOGNITION SYSTEM:

The face is considered as the primary focus of attention and also it plays a major role in conveying the identity and emotion of a person. Face recognition in machines are becoming very important because of the wide ranges of the law enforcement applications and commercial purposes which include human computer interactions, access control, forensic identification, image and film processing and security systems. Face recognition system is one of the computer visions that have capacity to identify the human face from the database images automatically (Baker and Matthews, 2001).

The facial recognition process may start its operation by collecting the face image from the specified security cameras (Adini, Moses, and Ullman, 1997). Then the facial recognition system measures the point of nodes on face such as shape of cheekbones, distance between the eyes, tip of the nose, and other distinguishable features. Then the facial recognition system compares these nodal points with the nodal points of images from the database to find out the match (EPIC, 2006). Face recognition system is currently being employed by different businesses and government in order to improve the security.

The following figure illustrates the generic configuration of face recognition system.

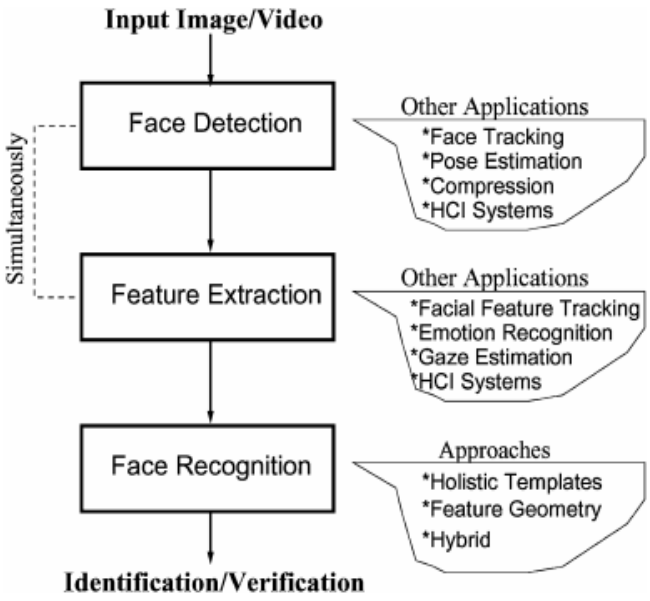

Figure: Configuration of a Generic Face Recognition System.

Source: Zhao et al (2003), Face Recognition: A Literature Survey, ACM Computing Surveys, Vol. 35, No. 4, December 2003, pp. 399–458.

Face recognition systems are mainly used in:

- Airports
- Public Transportation
- ATMs (Automated Teller Machines)
- Law Enforcements
- Railway Stations
- Criminal Investigation
- Casinos, Clubs, Sport Arenas
- Financial Agencies
- Banks requiring high security
- Personal Security - Home video surveillance systems

The problem that arises before the face recognition process is the face detection which identifies the face in a given image. The face detection code will start its operation by searching the face in all aspects without any omission by scanning the given image and also in all possible scales. The face recognition process is one of the difficult tasks. Face recognition system will take several steps to recognize the face such as face detection, face model resize, edge removal and comparison.

The following table illustrates the typical applications of the face recognition.

Areas	Specific applications
Entertainment	Video game, virtual reality, training programs
	Human-robot-interaction, human-computer-interaction
Smart cards	Drivers' licenses, entitlement programs
	Immigration, national ID, passports, voter registration
	Welfare fraud
Information security	TV Parental control, personal device logon, desktop logon
	Application security, database security, file encryption
	Intranet security, internet access, medical records
	Secure trading terminals
Law enforcement and surveillance	Advanced video surveillance, CCTV control
	Portal control, postevent analysis
	Shoplifting, suspect tracking and investigation

Table: Typical Applications of the Face Recognition

Source: Zhao et al (2003), Face Recognition: A Literature Survey, ACM Computing Surveys, Vol. 35, No. 4, December 2003, pp. 399–458.

2. ARTIFICIAL NEURAL NETWORK

The term artificial neural network was derived from neural network and it is one of the data mining techniques. The neural networks are the machine learning technique and it have ability to perform as like the human brain. The neural networks are mainly used to find the patterns in data or model the complex relationships between the inputs and outputs. The neural networks are interconnected group of artificial or natural neurons and also it uses the computational or mathematical model for the image processing. The artificial neural network is very challenging and also interesting biometric technique for identifying the specified individuals by the facial features (F´eraud et al, 2002).

This study discusses about the face recognition with artificial neural network. Artificial neural network is the artificial intelligence and it is emerged with wide range of applications in the data processing and pattern recognition. A neural network learns to recognize the given faces. The artificial neural network uses various algorithms to recognize (identify) the face. There are various factors that must be observed or identified during the face recognition process was image conditions, eye localization, pose, face localization, quality check, preprocessing, facial expressions, training set, feature extraction and absent and presence of structural components (Li and Chellappa, 2001). Artificial neural network based face recognition provides the fast and accurate face recognition and also it takes short processing time and high recognition time.

The following figure illustrates the features that used for the face recognition.

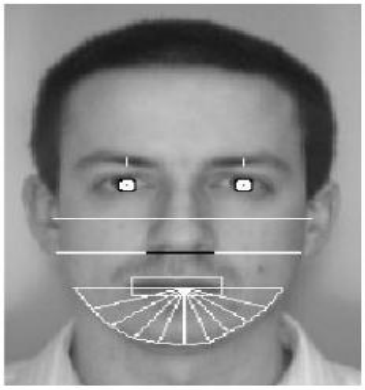

Figure: Geomentric Features for Face Recognition

Source: Brunelli R and Poggio T (1993): Face Recognition: features Vs templates, IEEE Transactions on Pattern Analysis and Machine Intelligence, 15(10):1042-1052.

Face recognition based on artificial neural network may uses different methods and techniques such as: Holistic methods such as: Principal-component analysis (PCA), Eigenfaces, Probabilistic eigenfaces, Group Based Adaptive Tolerance (GBAT), SVM, Feature lines, ICA, Evolution pursuit, and Fisherface algorithm/subspace LDA. Feature-based methods such as: Convolution Neural Network, Dynamic link architecture, Pure geometry methods and Hidden Markov model. Hybrid methods such as: Modular eigenfaces, Shape-normalized, Modular eigenfaces and Component-based.

3. HACKING FACE RECOGNITION SYSTEM:

Face recognition systems are also facing security issues and this is because of hackers. Generally, face recognition using for log-in option in laptop are mostly affected by security issues. Attackers have possible chances for breaking the face-recognition technologies in laptop by using the digitized images of the specific user. Today most of the researchers consider that, face recognition systems are not suitable for the secure log-on purposes and face authentication (log-in) can be easily fooled.

Most of the users use face authentication as a secure option instead of logging in with a password and username. Here, user simply sits in-front of the camera on the system and it will capture the image of the user's face and compare its features with the image that previously stored by the user. Access will be granted to the user, only if the images match. Here, the hackers play their role to attack the system. Face-recognition algorithms do not find the difference between the real face and digitized image (Vijayan, 2009). Because the algorithms, process the digital information which was sent by the camera and it is possible to attack the software with image of the registered user of that system.

The hacker will obtain the photo of the user and make editing with lighting with the help of image-editing tools. The hacker, who wants to attack the system unlikely to know that how the image that stored in the system looks like and so the hacker will take time to find out the different viewpoints and lighting to fool the face-recognition technology. Attacker need to have an experience with regeneration and image editing to attack the system successfully. This type of attack is possible even when the user have set highest security setting in the face-recognition software. The face-recognition technology becomes dangerous when it compromises to the hackers. The attacker will have possibilities to attack the system without the knowledge of real user and also real users ever have no chances for knowing about it. There are trade-offs between convenience and security and the users must balance it to avoid the unnecessary issues of security.

4. THREATS IN FACE RECOGNITION SYSTEM

Face recognition automatically pick up the faces in photographs and helps to identify who it is and if it is not new. Today, face recognition is a cornerstone to identify the individual among groups. In U.S, government organizations are using the facial recognition software to identify the sensitive public locations like airports and the citizens in motor vehicles. It is essential to note the difference between defeating face recognition and defeating face detection. Defeating face recognition means stopping the camera from matching the person by altering the physical features of that person and distances between them (Padania, 2012). Defeating face detection means stopping the camera from recognizing the face (usual patterns).

The following figure illustrates the different face images with different styles.

Figure: Facial Images with different styles

Source: CVDAZZLE (2012), Camouflage from Computer Vision, retrieved on 4th December 2012 from http://cvdazzle.com/

The applications of face recognition technologies ensure security in modern society. Programs that use the biometrics face recognition is to uniquely identify the individuals in order to combat expedite border crossings, identity fraud and dispense social services. For example: In India, the process of biometrics enrolling with more than 1.2 billion people for the purpose of social inclusion and

this to issue the UID (unique number) to the individual and this will serve like their unique identity and they can use it to interact with commercial service providers or government (Atick, 2011). Biometrics is not only the application or program that protects the integrity and also it provides trust for verifying the claimed identity. Within the family of biometrics, the face recognition occupies the special position.

Wearing fake teeth, inserting nose plugs and chewing tobacco can defeat the face recognition. In addition to these, smiling also makes the facial recognition to be more difficult. For this reason, there is a "no smile" policy for the passport photos. While considering the face recognition system for security, it is essential to consider face recognition system as only one of the overall security.

The following figure illustrates the different types of facial with masks.

Figure: Facial Images with Masks

Source: CVDAZZLE (2012), Camouflage from Computer Vision, retrieved on 4th December 2012 from http://cvdazzle.com/

5. CONCLUSION

It is concluded that, in past few years, face recognition is a technique which is developed rapidly. Human face is playing an important role in social interaction. Face recognition system has several algorithms and methods to identify the particular face. Face recognition system performs several operations like face detection, edge removal, quality check, facial expressions, eye localization, pose, etc. Most of the people use face recognition as an authentication purpose such as entrance of university, post office and public place etc. This paper explores the false acceptance rate (FAR) and false rejection rate (FRR). The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. In case of similarity scale, if the person is imposter in real, but the matching score is higher than the threshold, and then s/he is treated as genuine that increases the FAR and hence performance also depends upon the selection of threshold value.

The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

The user must reconsider to use face recognition for

secure log-in purposes, until the problem has been solved.

It is concluded that, face recognition system is mostly

used in airports, banks and other financial institutions to avoid the unsecured people. In addition to these, this research concluded that, face recognition system must be improved in order to perform security while it is used for authentication purposes as like the fingerprints. We hope this paper can provide the readers a better understanding about face recognition, and we encourage the readers who are interested in this topic to go to the references for more detailed study.

6. REFERENCES

1. Padania A (2012): How to Defend Yourself Against Facial Recognition Technology, retrieved on 4th December 2012 from http://www.pbs.org/mediashift/2012/06/how-to-defend-yourself-against-facial-recognition-technology170.html

2. Vijayan J (2009): Digital pictures can fool the built-in systems, retrieved on 4th December 2012 from

http://www.computerworld.com/s/article/9128264/Laptop_face_recognition_tech_easy_to_hack_warns_Black_Hat_researcher

3. Atick JJ (2011): Face Recognition in the Era of the Cloud and Social Media: Is it Time to Hit the Panic Button?, retrieved on 4th December 2012 from http://findbiometrics.com/face-recognition-in-the-era-of-the-cloud-and-social-media-is-it-time-to-hit-the-panic-button-2/

4. EPIC (2006): Electronic Privacy Information Center, "Face Recognition History", EPIC.org, 10 October 2006 http://www.epic.org/privacy/facerecognition

5. F´eraud R, O. Bernier, J.-E. Viallet, and M. Collobert (2002): A fast and accurate face detector based on neural networks. IEEE Transactions on Pattern Analysis and Machine Intelligence, 23(1):42–53, 2002

6. Y. Adini, Y. Moses, S. Ullman, (1997): "Face Recognition: the Problem of Compensating for Changes in

Illumination Direction", IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 19 No. 7, pp. 721-732, 1997

7. Li B. and Chellappa, R. (2001): Face verification through tracking facial features. J. Opt. Soc. Am. 18.

8. Brunelli, R., and Poggio, T., "Face Recognition: Features versus Templates", IEEE Trans. Pattern Anal. Machine Intell., vol. 15, pp.1042-1052, 1993.

9. Chellappa, R., Wilson, C.L., and Sirohey, S., "Human and Machinr Recognition of Faces: A Survey", Proc. IEEE, vol.83, pp.705-741, May 1995.

10. Reuters News, "Computer Security Threat On Rise – U.S. Survey", March 7, 1999.