International Conference on Applied Soft Computing Techniques ICASCT-18-2018

RESEARCH ARTICLE OPEN ACCESS

Survey on Biometric Security System to Secure Data

Bhagyashri Budhe, Mrs. Rashmi Jain
(Computer Science & engineering, Rajiv Gandhi College of Engineering, Nagpur.
Email: bhagyashribudhe1216@gmail.com)
(Computer Science & engineering, Rajiv Gandhi College of Engineering, Nagpur
Email : rashmil_jain@gmail.com)

Abstract:

Security is the basic requirement for the today's world. Everything is connected to internet and there is a basic need for the confidentiality of data. If someone stole user's credentials, then he/she will able to access personal data of user. System security only depends upon credentials. So, in this paper we proposed a system based on Biometric authentication where a real time image is captured and compare with our database image. Biometric authentication provides secured platform to protect our confidential data. For more security of credentials of user, we are using encryption and decryption algorithms. Biometric authentication is done by the help of detection of faces using two algorithms viola Jones and point matching algorithms. This paper also deals on security with the help of encryption and decryption by 3DES algorithm

Keywords — Data Encryption Standard, Triple DES, Face recognition, Face detection

I. INTRODUCTION

The usage of Biometric Technologies in Access Control System (ACS) has grown in the last few years, mainly because they offer big advantages over traditional ACS such as radio frequency cards (RFID) or Personal Identification number (PIN) codes. This is due to an all-around realization that the most important assets companies should preserve its information it is the core element that provide values today's corporate panorama. It is common to see available prebuild ACS at sale; that any person or company can use it as is. But, there is a very common problem with these types of systems, as they are a closed box with no prospect of adaption and often incompatible with pre-existent systems running at those companies. So, we are going to follow a research work on current technologies use in ACS, identifying their advantages as well as their gaps, in order to achieve a fully open system capable of total integration with an existing infrastructure. Biometric technology uses different kind of techniques for authentication or different characteristics of human like their fingerprints, Hand geometry, iris, face, retina. Here in our paper we are proposing biometric authentication Using face detection.

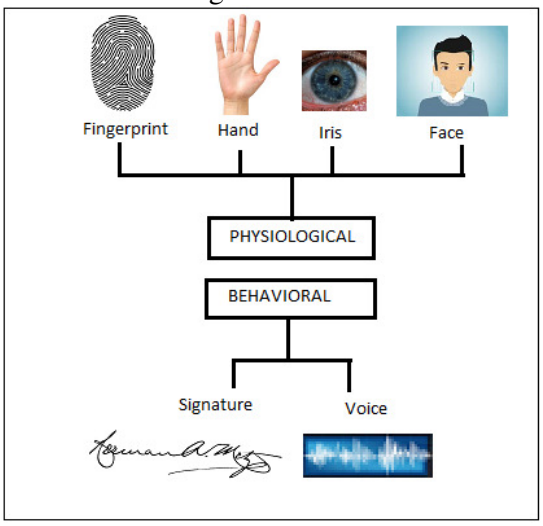

Fig. 1: Types of Biometrics

There are few characteristics of human body that is not feasible to use for the biometric authentication [12]. After collecting all pros and cons we came up with the solution that we can use these five parameters for authentication. They are

Fingerprints: Fingerprint is the pattern of valleys and ridges on the surface of finger prints. They are

different from person to person and also different between fingers on that person, making it one of the most.

Retina: It is considered to be the most secure biometrics as it examines the vascular configuration of the eye. It is next to impossible to replicate and also very stable during someone's lifetime although susceptible to some diseases like diabetes or glaucoma.

Face:On a daily basis face recognition is clearly the most common biometric used by humans in order to identify one another. Facial recognition can be made either by getting the location and shape facial attributes as well as their spatial relations or by making overall analysis of the face image.

Here in this paper we are proposing a very secured biometric system using encryption and decryption techniques. Triple DES encryption and decryption techniques is used to make the credentials secure from the outside user.

A. DES: (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It is based on the IBM proposed algorithm called Lucifer. DES became a standard in 1974. Since that time, many attacks and methods recorded that exploit the weaknesses of DES, which made it an insecure block cipher.

B. 3DES: An enhancement of DES, the 3DES (Triple DES) encryption standard was proposed. In this standard the encryption method is similar to the one in original DESbut applied 3 times to increase the encryption level.

II. LITRATURE SURVY

Over the years many contributions were done to the field of face detection and recognition. G. Yang came up with Multiresolution rule method. This knowledge based method used the structural nature of the face for detection [4]. Feature based method uses the facial features [5][6], skin color [7][8]and combined multiple features [9]of the face for better accuracy and detection speed. In order to increase the detection speed, the accuracy is sacrificed. For this, a steady and uniformly scaled images using template matching method was employed. Predefined face templates [10] and deformable templates [11] were incorporated which was completely based on the International Journal of Computer Trends and Technology (IJCTT) – volume 25 Number 1 – July 2015 ISSN: 2231-2803 http://www.ijcttjournal.org Page 55 template (a predefined structure) without using learning. Appearance based methods gives faster detection speeds, more accurate results and adaptive nature that could distinguish a face from a non-face in any environmental conditions. Neural networks [12] is commonly used model for getting the desired results.A very fast and accurate approach to detect an object was devised by viola and Jones[18] in the year 2001. Nowadays, this method is used in cell phone cameras, security perimeters and also in our paper we are detecting face using viola jones method. Due to the use of Haar features and adaboost machine learning computational speed increased. And within a millisecond a face can be detected in a frame. Further improvements were done by Lienhart and Maydt [19] in the year 2002.In this method, firstly, the value of all pixels in greyscale images which are in black accumulated. Then, they subtracted from the total of white boxes. Finally, the result will be compared to the defined threshold and if the criteria is met, the feature considers a hit.

In [20], we see that if an image of a random size contains a face of a person, it must be known by a face detector. One way to solve the problem is using classification of binary which has a particular classifier is made to reduce the risk of misclassification. Since we can't know the real previous probability for a particular picture to have a face, in order to achieve an acceptable performance, the specific algorithm must reduce both the false negative and positive rates.

This goal needs a specific arithmetic set of what differentiates faces of people apart from other things. These features can be known with Adaboost, a new committee learning algorithm which depends on a group of classifiers that are too weak to form a stronger thing through a mechanism of voting. Generally, if a classifier is too weak, it can't meet a previously set target of classification in terms of errors.

III. ALGORITHM COMPARISON TABLE

Name	Description	Advantages	Disadvantages
1.Data Encrypt-ion Standard-d (DES)	**DES** uses a 56-bit key and runs through 16 cycles of 48-bit sub keys. When decrypting the data, the exact reverse operation is performed, using the same algorithm. The same key is used for the entire process.	56-bit key is used in encryption and there are 256 possible keys. A brute force attack on such number of keys is impractical.	Hardware implementations of DES are very fast; DES was not designed for software and hence runs relatively slowly.
2. Triple Data Encryption Standard (3DES)	**3DES** expands the size of the key by running the algorithm in succession with three different keys. It makes 48 passes through the algorithm. The resulting key is 168 bits; this can be hard to implement, so there is also a two-key option provided in 3DES that runs through a method called **Encrypt-Decrypt-Encrypt**	It has the proven reliability and a longer key length that removes more attacks that can be used to reduce the amount of time it takes to break DES.	It may not be strong enough to protect data for very much longer.
3. Advanc-ed Encrypt-ion Standa-rd(AES)	AES, is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. Brute force attack is the only effective attack known against this algorithm	It uses higher length key sizes such as 128, 192 and 256 bits for encryption. Hence it makes AES algorithm more robust against hacking.	AES in counter mode is complex to implement in software taking both performance and security into considerations.

VI.CONCLUSION

This proposed face detection biometric system using viola jones technique for detection of face and point matching algorithm is very efficient and highly secure system as it uses the triple des system for authentication. Thus the proposed system is able to produce an accurate and secure result. Also the face detection technique used in this paper requires less computational time and low error rate. It is secure, simple and efficient method for checking the authentication.

REFERENCES

[1] Hsu, Rein-Lien, Mohamed Abdel-Mottaleb, and Anil K. Jain. "Face detection in color images." Pattern Analysis and Machine Intelligence, IEEE Transactions on 24.5 (2002): 696-706.

[2] A.S. Georghiades, P.N. Belhumeur, D.J. Kriegman, From few to many: illumination cone models for face recognition under variable lighting and pose, IEEE Trans. Pattern Anal. Mach. Intell. 23 (6) (2001) 643–660.

[3] Mayank Chauha and Mukesh Sakle. ―Study & Analysis of Different Face Detection Techniques.‖ International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 1615-1618.

[4] G. Yang and T. S. Huang, ―Human Face Detection in Complex Background,‖ Pattern Recognition, vol. 27, no. 1, pp. 53-63, 1994.

[5] T.K. Leung, M.C. Burl, and P. Perona, ―Finding Faces in Cluttered Scenes Using Random Labeled Graph Matching,‖ Proc. Fifth IEEE Int'l Conf. Computer Vision, pp. 637-644, 1995.

[6] K.C. Yow and R. Cipolla, ―Feature-Based Human Face Detection,‖ Image and Vision Computing, vol. 15, no. 9, pp. 713-735, 1997.

[7] J. Yang and A. Waibel, ―A Real-Time Face Tracker,‖ Proc. Third Workshop Applications of Computer Vision, pp. 142- 147, 1996.

[8] S. McKenna, S. Gong, and Y. Raja, ―Modelling Facial Colour and Identity with Gaussian Mixtures,‖ Pattern Recognition, vol. 31, no. 12, pp. 1883-1892, 1998

[9] R. Kjeldsen and J. Kender, ―Finding Skin in Color Images,‖ Proc. Second Int'l Conf. Automatic Face and Gesture Recognition, pp. 312- 317, 1996.

[10] I. Craw, D. Tock, and A. Bennett, ―Finding Face Features,‖ Proc. Second European Conf. Computer Vision, pp. 92-96, 1992

[11] A. Lanitis, C.J. Taylor, and T.F. Cootes, ―An Automatic Face Identification System Using Flexible Appearance Models,‖ Image and Vision Computing, vol. 13, no. 5, pp. 393-401, 1995.

[12] H. Rowley, S. Baluja, and T. Kanade, ―Neural NetworkBased Face Detection,‖ IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no. 1, pp. 23-38, Jan. 1998.

[13] Sharifara, Ali, et al. "A general review of human face detection including a study of neural networks and Haar feature-based cascade classifier in face detection." Biometrics and Security Technologies (ISBAST), 2014 International Symposium on. IEEE, 2014.

[14] Zhengming Li; Lijie Xue; Fei Tan, "Face detection in complex background based on skin color features and improved AdaBoost algorithms," Progress in Informatics and Computing (PIC), 2010 IEEE International Conference on , vol.2, no., pp.723,727, 10-12 Dec. 2010.

[15] Campadelli, Paola, Raffaella Lanzarotti, and Chiara Savazzi. "A feature-based face recognition system." Image Analysis International Journal of Computer Trends and Technology (IJCTT) – volume 25 Number 1 – July 2015 ISSN: 2231-2803 http://www.ijcttjournal.org Page 61 and Processing, 2003. Proceedings. 12th International Conference on. IEEE, 2003.

[16] Yang, Ming-Hsuan, David J. Kriegman, and Narendra Ahuja. "Detecting faces in images: A survey." Pattern Analysis and Machine

Intelligence, IEEE Transactions on 24.1 (2002): 34- 58.

[17] Xiaowei Zhao, Xiujuan Chai ,"Context Constrained Facial Landmark Localization Based on Discontinuous Haar-like Feature" International Conference on Computer Vision (ICCV2013),2013. [18]

[18] Paul Viola, Micheal Jones, "Rapid object detection using a Boosted Cascade of Simple features" CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION, 2001 .

[19] Lienhart and J. Maydt. An Extended Set of Haar-like Features for Rapid Object Detection. IEEE ICIP 2002.

[20] Yi Qing Wang, 'An Analysis Of The Viola – Jones Face Detection Algorithm', Image Processing On Line, 2014, v0.5.