ISSN (Print): 0974-6846
Indian Journal of Science and Technology, *Vol 11(26), DOI: 10.17485/ijst/2018/v11i26/130560, July 2018* ISSN (Online): 0974-5645

Integrated Anthropometric Approach for Ceaseless Authentication

S. Sheeba Rani[1*], J. Janet[2], S. Balakrishnan[2] and K. Sujatha[3]

[1]Department of Electrical and Electronics Engineering, Sri Krishna College of Engineering and Technology, Coimbatore – 641008, Tamil Nadu, India; sheebaranis@skcet.ac.in

[2]Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore – 641008, Tamil Nadu, India; janetjude1@rediffmail.com, balkiparu@gmail.com

[3]Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore – 641008, Tamil Nadu, India; sujatha.ssps@gmail.com

Abstract

Objectives: To model a novel ceaseless client validation method to authorize the client regardless of their body position before the capturing system. The system ceaselessly validates the client with their various soft anthropometric parameters such as (e.g. wearables and skin) in addition to hard biometrics. **Methods/Statistical Analysis:** The proposed system mechanically stores in the soft anthropometric parameters each time the client logs in and integrate the anthropometric parametric features along with the conventional face traits for verification thus fusing the combination of hard and soft biometric attributes to attest a client ceaselessly. The methodology comprises of various modes such as initialization, validation and regeneration. **Findings:** Various samples of facial colour features and user's cloth colour features are used as soft biometrics in this system for authorization. The experimental results of AR show the extensive improvement over the existing methods. **Application/Improvements:** This methodology eliminates the challenges faced in face recognition due to different expressions and postures, lighting effects. Thus the key discriminating features are authenticated using hard and soft biometrics thus making it a high secure technology.

Keywords: Authorization, Biometrics, Color Histogram, Face Recognition, Fusion

1. Introduction

Authentication of the client plays an important role in computer and network system's security. In practice, even though token-based methods and knowledge-based methods are well known, they suffer with security weakness problems. Passwords, the commonly used metric can be misused in several ways (suits well for smart cards also). To get around these problems, a variety of authentication procedures for login are available which includes text password, graphical password, public key procedure and authorization using biometric features. All the login strategies face a standard drawback i.e. they attest the client solely at primary login attempt and don't re-authenticate the client till he/she logout. This might cause security issues not just for high security system, however conjointly for private computers in an exceedingly general workplace atmosphere. To deal with this problem, the system should ceaselessly monitor the client and attest the client even after initial login. Various research groups on client validation in ceaseless mode have been published extensively. These approaches use the conventional biometric attributes. Though these systems provide good results they suffered with low access of biometric features. To address this problem, soft metrics like client's face colour, hair colour and dress colour can be used. Those systems face issues below matters wherever all the staff having common dress code as

*Author for correspondence

uniform. So as to deal with on top of issues, a replacement frame work is proposed that uses strong face recognition for primary login attestation and registers the soft statistics of client, monitors the client supported registered features and verify the client in regular interval of time to make sure for continuous authentication and to supply re-authentication.

2. Literature Survey

Biometrics is defined as the recognition of an entity established on the traits pertaining to bodily functions and mannerisms[1]. Soft biometrics is a package of unique characteristics to provide information about an entity. In[2] captured the anthropometric features using a sensor interfaced with finger print scanner and mouse layout set up in a camera console to feature the facadic features of the client which proved to give efficient validation results provided there was abundance of such traits. In[3] proposed a face recognition method to detect the face by considering scale and orientation[4]. Used feature selection technique to reflect the client typing behavior by using n-graph, but the systems requires high level of training[5].

3. Methods Used

3.1 Biometrics Based Anthropometric Feature Extraction

Anthropometric attributes are the traits that gain insight into data about the individual, but using them; it is less distinctiveness and lacks permanence to distinguish between two people. These attributes can be enlisted as color of the eye and hair, body mass weight and height, ethnic origin and tattoo marking, burn scars etc. They do not include the ample discriminatory details to totally validate the client. However, in this frame work, soft biometric has been used to monitor client who logged in, here it acts as like a session key.

4. Proposed System

Combination of hard and soft biometric attributes is used to attest a client ceaselessly is proposed in this work. This proposed system, primarily attest the client by face recognition and registering a fresh template based on client's cloth colour and face colour for continuous monitoring. Just in case of any deviation in soft attributes then immediately the system will verify hard attributes. If both traits differ, system treats client as imposter and moved to logoff state. When the system finds authorized client, by verifying hard biometric traits, allows the client by re-authentication to continue. The workflow for the proposed system is shown in Figure 1.

4.1 Mode 1 - Validation Initialization

As a first step in this proposed work, strong face recognition for primary login attestation for client is used. The flowchart for face recognition is shown in Figure 2.

4.1.1 Exposure of the Face

When the client sits before the system the webcam application runs automatically and a snapshot of the running videos is taken. That image is then passed to the lighting compensation and colour space transformation block where skinny and non skinny layers are separated and the RGB to YCbCr colour space transformation is being done. Now the image is in the pipeline for the third block where skin colour detection takes place. Then high frequency noises are removed by using a low pass filter (a 5 × 5 mask) to identify skin colour blocks. Next is with the help of features like mouth, eyes and height to width ratio are determined for each candidate block. Then mouth and eye detection takes place and at finally a true face is determined.

4.1.2 Discovery of Face Traits

The Cropped image of client's face is initially disintegrated into various orientation and scale responses by convolving multi-scale and multi-orientation Gabor filters. Then neighbouring relationship not only in image

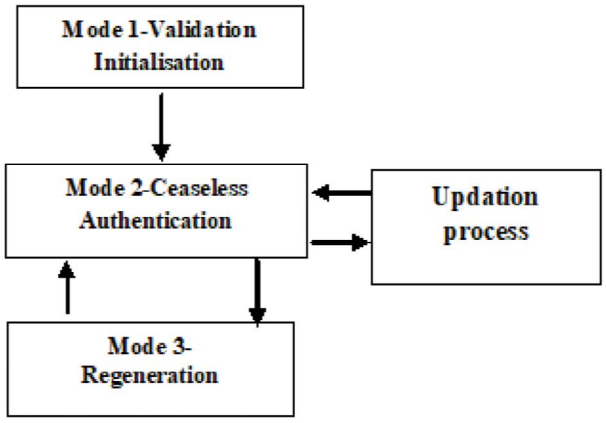

Figure 1. Modes of operation.

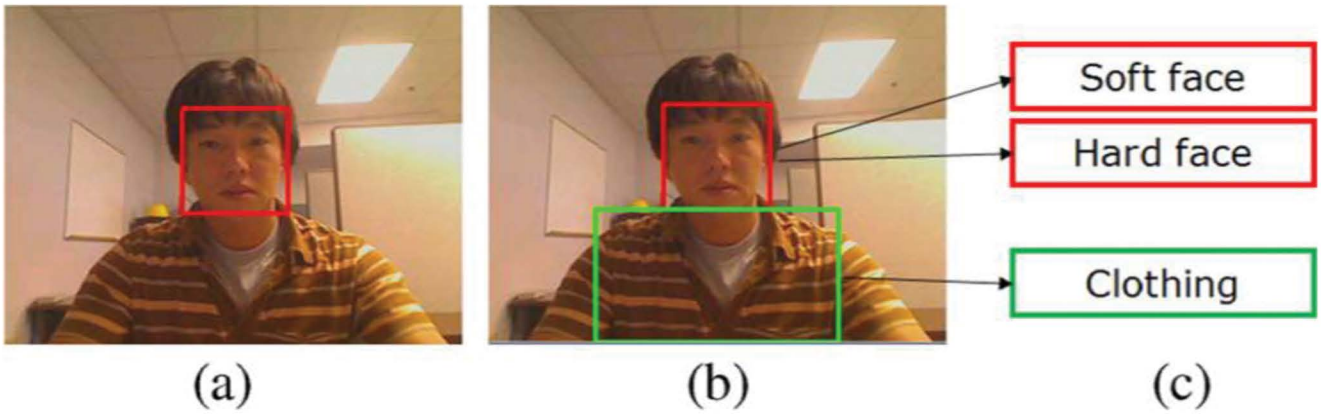

Figure 2. a) Mode 1, b) Mode 2 and c) Mode 3.

space, but also in different scale and orientation responses are described with the help of local binary pattern analysis and thus forming third order Gabor volume based LBP. The length of the histogram vector is reduced by the effective formulation of E-GV-LBP. By this method, details from various domains are discovered to provide a face representation for recognition process. Discriminant classification can then be performed based mostly upon weighted histogram intersection techniques and results whether the client is authenticated client or not.

4.1.3. Confinement of Body and Pattern Conscription

The position and external of the client's body are estimated. Histograms are computed for client's face color and dress color and attributes of client's face are calculated during login session and then are kept as enrolment templates. RGB shade spaces are computed to 3D sixteen bins so as to get the color statistical feature of costume and facade shade.

4.1.4. Mode 2 - Validation

Immediately after login session, ceaseless authentication procedure should start. The system authenticates the client continuously without cease with the help of the "soft face" and "clothing" and enrollment templates are registered during initial login authentication step. At any time the system acknowledges that the client is not present in the front of the console and then the system status should change to enrollment template update process. The continuous attestation procedure consists of identification of face & body and calculation of similarity as important steps.

- Identification of client's façade and physique using tinted statistical imaging. Based on the histogram details obtained during primary login, the system tracks the face and the body separately and then the similarities S_{facade} and S_{wear} are calculated separately. Face recognition process is carried out in every 10 seconds.
- Figuration of Likeness. The system calculates the final similarity S_{ceas}. (S_{facade} + S_{wear}). If this value is below a threshold T_{cont}, then the system is because of ambient illumination changes or due to client's missing presence before the workstation.

4.1.5. Mode 3 - Regeneration

At instances of similarity S_{ceas} is less than Tceas. Then the system should go for template update process. This procedure contains two major steps.

- Detection of illumination changes. Whenever the S_{ceas} is less than T_{ceas}, the system checks whether the client is present in front of the console or not and is there any illumination changes. Ion to identify the occurrence of illumination change, workout the difference image just before and after the time when $S_{ceas} < T_{ceas}$. If the distinction image shows intensity variations everywhere in the image, it can be concluded that there has been an occurrence of illumination change.
- Enrollment template updation. Once an illumination change is identified, we updation of the client's biometric template should be done to maintain successful continuous authentication within the changed operating environment.

5. Experimental Results

Whenever the client is not present before the workstation, the structure should go for relogin authentication process. During this flow, the structure will be secured and attempts to identify the client and re-validate the same autonomously. If in case the set up identifies the client as genuine and re-validates the client, then system jumps on to ceaseless authentication process again. The similarity score is used for relogin authentication. When a pretender tries to switch the legitimate client, small variation in the soft biometric values will be identified and it leads the set up to re-login the validation process. In this mode of operation, the client has to supply genuine soft and hard biometrics. Hence, the re-login validation is the unique methodology of deterring session hijacking which is proposed in this research.

6. Conclusion

This proposed system uses soft biometrics along with hard biometric features for ceaseless client authorization. This system registers a fresh template at every instance when the client logs in, which sanctions consent to the system to employ the hard and soft anthropometric features effectively for ceaseless client validation. Facial colour features and client's cloth colour features are used as soft biometrics in this system for authorization. This system is more powerful in relation to the posture of the client in the front of the system and it conjointly has the aptitude enrolment guide update and relogin authentication. This continuous authentication procedure makes use of both hard and soft biometric attributes for relogin authentication which leads to high security.

7. References

1. Qinghai G. Online teaching: Do you know who is taking the final exam? Fall 2010 Mid-Atlantic ASEE Conference. 2010; p. 1–6.
2. Jain AK, Dass SK, Nandakumar K. Can soft biometric traits assist client recognition? Proceedings of SPIE, Biometric Technology for Human Identification. 2004; 5404:561–72. Crossref.
3. Sim T, Zhang S, Janakiraman R, Kumar S. Continuous verification using multimodal biometrics. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2007; 29(4):687–700. PMid: 17299225. Crossref.
4. Lei Z, Liao S, Pietikainen M, Li SZ. Face recognition by exploring information jointly in space, scale and orientation. IEEE Transactions on Image Processing. 2011; 20(1): 247–57. PMid: 20643604. Crossref.
5. Solami EA, Boyd C, Clark A, Ahmed I. User-representative feature selection for keystroke dynamics. 5th International Conference on Network and System Security. 2011; p. 229–33. Crossref.
6. Sujatha T, Sangeetha T, Balakrishnan S, Susila N. Honey/sugar template based on biometric protection using bloom filter. International Journal of Pure and Applied Mathematics. 2018; 119(12): 1143–55.