International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 6 (2015) pp. 15457-15474

http://www.ripublication.com

File Security Using Neural Networks Induced Facial Recognition

Dr.V.Dhanakoti, S.U.Abinandhanan And R.Jaya Ganthan
Department of Computer Science and Engineering
Valliammai Engineering College
Chennai, India.

Abstract

In the past decade significant promotions in several biometric techniques have been propelled. But file security is a field where the implementations of the biometric technologies are seldom done. In today's file-dependent operating systems laden era, the security of files is compromised for a certain level. The compromise is not necessary, as biometrics can be applied to file security too. Biometrics with machine learning and neural networks impose high level of learning with some compromise in the accuracy of detection of biometric values. Face recognition with neural networks and in current use has Principal component Analysis as its primary algorithm, which can be manipulated to include machine learning. The Modified component Analysis in this system proposes a concept where the training set is constantly manipulated with elimination of less accurate faces and inclusion of more accurate faces, which makes the detection rate to increase in a gradual manner, as human faces change in a fashion proportional to time, and the faces do not revert back in time.

Introduction To Bio-Metrics

In this internet era, disguise and eavesdropping have increased. The security stands central to all these problems. The concept of authentication provides this security which process helps in identifying the user. Various ways of providing authentication are: using knowledge (such as passwords and PIN), using tokens (like security token and smart card) or using biometric. The implementations of passwords cannot guarantee high security and it is difficult to manage passwords for many systems. Similarly, the usage of tokens requires specialized hardware and infrastructure support.

Biometric authentication process is found to be the most fool-proof in providing security. It cannot be easily stolen or duplicated. It can also defend social engineering attacks. Most network companies use biometric as authentication to protect their

products. The companies providing e-commerce solutions use biometrics for high level security. Biometrics effectively prevent unauthorized attempts and preserves non-reputation in information security [1]

This paper is outlined as follows. Section II Provides information on biometric modalities and classifies the multi-biometric systems. Section III provides research works in areas of faces recognition. Section IV discusses on the proposed modifies algorithm which introduces elimination of Eigen values. Section V presents conclusion and also future work.

Biometric Techniques

Biometric-systems use physical features and even behaviors of a person. Physical characteristics include fingerprints, iris, face or hand geometry. Similarly behaviors are voice, signatures and other keystroke dynamics [1].

Biometric authentications done by single personal characteristics are affected by the performance problems like noisy data (Ex: voice recognition system fails when the user has sore throat), intra-class variations (i.e the variation in received and original data), non-universality and spoof attack. Because of this motive, the multiple personal characteristic biometric systems are admired [2]. Multiple personal characteristics involves more than one biometric features co-related with one another. It also joins different features such as iris, face image and finger print (or) fingerprint and faces image or spoken password and face image [3][4].

The merits of multi-modal biometric system are impoverishing false acceptance rate (FAR) by imposing the matching accuracy. It also impoverishes false non-match rate, false recognition rate and false rejection rate. It also vanquishes the non-universality problem. One biometric trait compensates another biometric trait if a human failed to enroll using one trait. It enhances the quality of data (i.e.) removes noisy data [4].

Biometric Modalities

Face recognition Biometrics

In Fig.1 shows Face recognition biometric method that uses following two approaches to identify person.

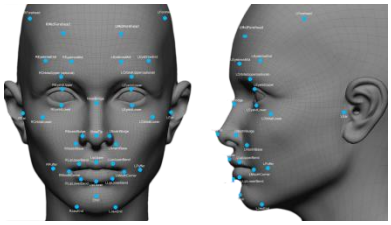

Figure 1: Face Recognition Biometrics

- The first approach uses some basic components such as eyes, nose, lips and relate them with their shape and spatial relationships between them [1].
- In second approach, the image of the face is treated as weighted combination of numerous canonical faces [1].

Fingerprint Biometrics

Fingerprint biometric also helps to identify a person. It is well known that even identical twins have different fingerprints. It consists of valleys and ridges. Minutiae points helps in matching process by identifying position and corresponding orientation of few critical points. Fig.2 and Fig.3 represents the pattern of customer's fingerprints.

Figure 2: Fingerprint Biometric

Figure 3: Fingerprint

Plain Arch and tented Arch

Plain Arch has ridges on a side, which eventually rises towards the centre and ends at the opposite side. It is represents in fig.4.Tented arch is similar to plain arch but here the ridges makes an angle. It has some loop characteristics as in Fig.5

Figure 4: Plain Arch

Figure 5: Tented Arch

Radial Loops and Ulnar loops

The right slants loop or Ulnar loop flow towards the little finger whereas the left slant loop or radial loop pattern flow towards thumb. It is represented in Fig.6 and Fig.7

Figure 6: Radial Loop

Figure 7: Ulnar Loop

Plain Whorl

This pattern consist of two deltas and atleast one ridge which forms a complete pattern of circle, spiral or oval. The imaginary line which is drawn in the inner pattern between deltas will cross or touch minimum one ridge as shown in Fig.8

Figure 8: Plain Whorl

Central Pocket Loop Whorl

Central pocket loop whorl pattern has an hindrance against line of loop at right angles or atleast one backward curve. In the inner pattern the inner backward ridge, is not cut or touched by the imaginary line in between two deltas as shown in Fig.9

Figure 9: Central Pocket Loop Whorl

Double Loop Whorl

There are two different loop formations differentiated in double loop whorl. It comprises of two difficult and unique sets of shoulders and two deltas as in Fig.10.

Figure 10: Double Loop Whorl

Accidental Whorl

Accidental whorl pattern is connected with atleast two deltas. It combines two or more characteristics pattern types keeping out the plain arch. There are some unusual patterns as represented in fig.11 [1].

Figure 11: Accidental Whorl

Iris Biometrics

The iris is a pigmented area of eye that remains identical throughout the part of human life. The white region of eye, sclera and the pupil is coupled on both sides. This authentication method proves to be more precise method. Every iris is unique hence artificial irises such as contact lenses can be detected [1].

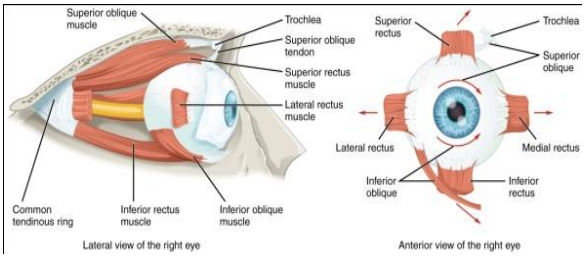

Figure 12: Iris

Gait Biometrics

Gait represents the way a person walks. It is highly helpful in surveillance scenarios because it recognise a person easily at a some distance .It is represented in Fig.13 [1].

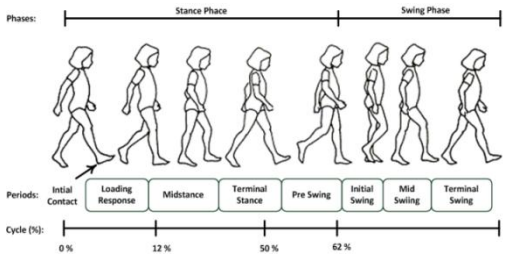

Figure 13: Gait Biometrics

Thermal Imaging

It is similar to hand vein geometry. In this method, the vein pattern in wrist or face is captured using infrared light source and a camera as represented in Fig.14 [1].

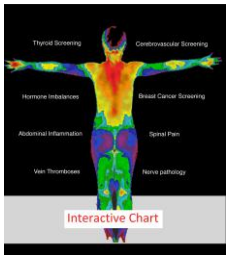

Figure 14: Thermal Imaging

Ear Shape

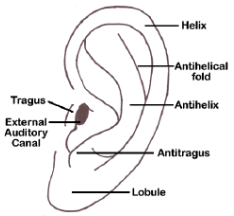

Figure 15: Ear Shape

Ear shape biometric is applied in law enforcement. The image of ear is acquired by Optophone (verifier to identity ear shape). It is a handheld device which uses a flash and a camera to capture a set of ear images in Fig.15 [1].

Palm Print Biometrics

Humans have different palms. Similar to fingerprints, palm has valleys and pattern of ridges along with wrinkles and principal lines. It does not require high resolution scanner to take palm image in Fig.16 [1].

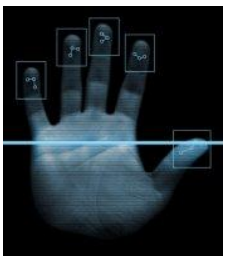

Figure 16: Palm Print Biometrics

Retina Biometrics

Retina is a nerve present behind the eye. It sends some pulses to brain via optic nerve. It is more precise and dependable than other biometric methods. It is difficult to capture the retina image. low intensity infrared light is enough to scan the retina pattern. The vascular information reflection is also noted down as in Fig.17 [1].

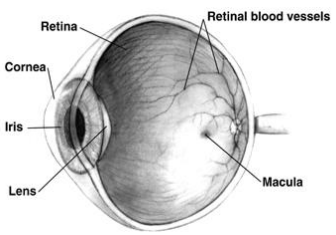

Figure 17: Retina

Signature Biometric

Handwritten signature can be used to recognise a person. Compromising the signature is tough as the biometric system compares stroke, speed pen pressure and shape. It is represented in Fig.18

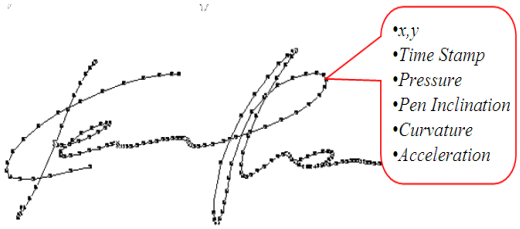

Figure 18: Signature Biometric

Body Odour

Body Odour from part of body that are non-intrusive are sensed. Human body odour consists of chemical called volatile. A template is created from these volatile extracted from the body as in Fig.19 [1].

Figure 19: Body Odour

Keystroke Dynamics

Keystroke (Fig.20) dynamic identifies a person by way of typing. The system monitors continually or during the log in time. It is easy, because a software package is enough [1].

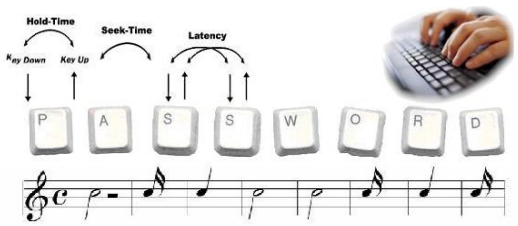

Figure 20: Key Dynamics

Fingernail Bed
The skin beneath the fingernail (Fig 21) is used in this type of biometric systems [1].

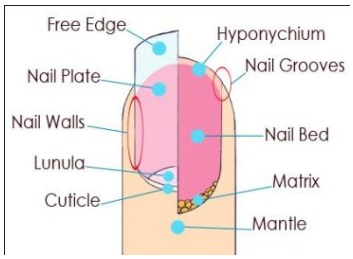

Figure 21: Fingernail Bed

Classification of Multi-Biometric Systems

Multi-Sensor Systems
Multi-sensor systems use different sensors to obtain the single image of the user. For Ex: sensor level fusion is a technique that integrates capacitive and optical sensors to obtain fingerprint.

Multi Algorithm Systems
Multi algorithm systems use many algorithms for single biometric. The technique such as rank level, score level and feature level matching technique are used to integrate them. It is a cheaper system as there is no extra device required. The system is complicated because of use of secural algorithms.

Multi Instance System
Multi instance systems employ multiple occurrence of a single biometric. For Ex:- if a person's iris is to be recognised then both the right and left irises are scanned. This system is cost effective, since a single sensor can be used to obtain the images.

Multi Sample Systems
Multi sample systems capture samples of single biometric feature. For Ex:- In capturing the image of front face, this system captures both the right and left profiles also.

Multi Modal Systems
It is efficient to use systems that capture additional features to authenticate a person. For Ex:- An authentication can involve features such as voice and face. Features that are uncorrelated physically such as face and fingerprint provides better results. Since multiple features require multiple sensors, the system is expensive to install.

Hybrid Systems

Hybrid systems combine several multi biometric systems. Ex:- fingerprint recognition algorithm can be integrated with palm recognition algorithm. They are also called a multi algorithmic system (or) multi modal system.

Related Work on Biometrics

Reported work on face recognition biometric

The several face recognition methods and algorithms fails to handle image misalignment, light intensity variation collusion and vigorous check. The images such as multi spectral /gray scale, video / image frames captured using multiple / single camera, whether objects are at varying distance etc….. Are the parameters used to compare when related works are surveyed.

Instead of using flash method, a projector illuminations method to recognise a face is explained by Andrew Wagner et al.[5]. The image is tested by using methods like off-the-shelf detector, spare representation based classifier (SRC), iterative alignment, and light intensity variation is supported in this method. But it is limited to 2D images and fails to handle contiguous occlusions. The accuracy of 92.2% from CMU multi PIE database and 93.7% from extended Yale-B database result is reported.

A technique using video frame to recognize and detect a person's face is proposed by E.Garcia Amaro et al [6]. Viola-Jones face detector is used by this technique. A high resolution image of the face can be captured using this method for better result. The accuracy of locally weighted learning (LWL)-78.3%, decision tree (DT)-85% and Naive Bayes classifier – 100% and K- Nearest neighbor -98.3% is achieved from the test result.

With the help of saliency maps, the unconstructed outdoor backgrounds can be used to detect face at a distance. This is introduced and explained by Ahmed El Barkouky et al [7]. The Voila-Jones face detector used in testing saliency maps are combined with skin tone and facial characteristics by using a method called score fusion. 87% of true positive (TP) rate and 79.3% count on false positive test result is obtained.

Local shape analysis and texture checks the liveliness of a person's face. This is dome to identify face spoofing proposed by J.Maatta et al [8]. Fusion techniques such as weighted score level combines features of face extracted by Histogram of oriented gradients (HOG), gavor wavelets and local binary pattern. The accuracy of about 0.999 using NUAA database area under curve and 1.1% in equal error rate and 100% with Yale database from test result is obtained.

A face detection scheme introduced by Hanuma Teja.M [9] uses single camera to capture line object. Images discrete cosine transformation (DCT) energy monitors pupil movements and eye blinking to test the liveliness. The image gets rejected if the object is not lively.

When a face in video is to be detected, the liveliness of the face is checked. This is presented by Younghwan Kim et al [10]. Algorithm used is based on similarity. There is 100% accuracy and no fake is reported.

A solution across multi spectral illuminations for face detection is devise by Zhiwei Zhang et al [11]. For this purpose an algorithm called regularized transfer booting is used by this method. A satisfactory report of result with 850nm and 650nm spectrum is obtained.

Demographic information of a person and facial marks (e.g. Scars, moles, freckles etc.,) can be used for face recognition. This is developed by Unsang Park et al [12]. The performance of information retrieval and image matching can be improved by this method. An accuracy of about 92.02% and EER of about 3.839% is reported on results on mugshot database and FERET.

A scheme to identify a user with the help of facial video data is presented by Norman Poh et al [13]. This is used by banks. Facial characteristics such as mugshot image are used by this scheme. Comparison of parts based versus holistic image, set based facial recognition versus frame based is done by this method. It is evident that part based approach is better than holistic on BANGA database.

Face verification can be done by convolutional neural network. And a method for face detection is discussed by Ihor paliy et al [14]. Gray scale images are used for testing. Increases accuracy rates in face detection and high speed can be observed after CMO test.

A novel technique to identify facial component landmark is discussed by B.A.Efraty et al [15]. It comprises of fast wavelet algorithms. Adaptive bag of words descriptors combined with cascade boosted classifiers and multi resolution Isotropic analysis. Low failure rate is reported in multi PCE database.

Proposed System

File security is a field which is less secure than what is needed for the current technological environment. The existing systems use normal encryption techniques using passwords, which can easily be bypassed. Even though the password is unknown, the security can be bypassed by using techniques like phishing and brute force. They can be protected by simple algorithms, but still, if the password is known by any third person, the security can still be breached. Our system encourages the concept of security for a file which belongs to, and can be accessed by only authenticated people. The system also proposes a higher security level ring that compliments the security of password protected encryption. It also acts as a monitoring system in addition to the security system.

Working

When a user needs to access a protected file, the user enters the username and password. When the password does not match, any sort of read or write access to the file is denied. If the passwords match, then the process runs in the foreground, meanwhile in the background the

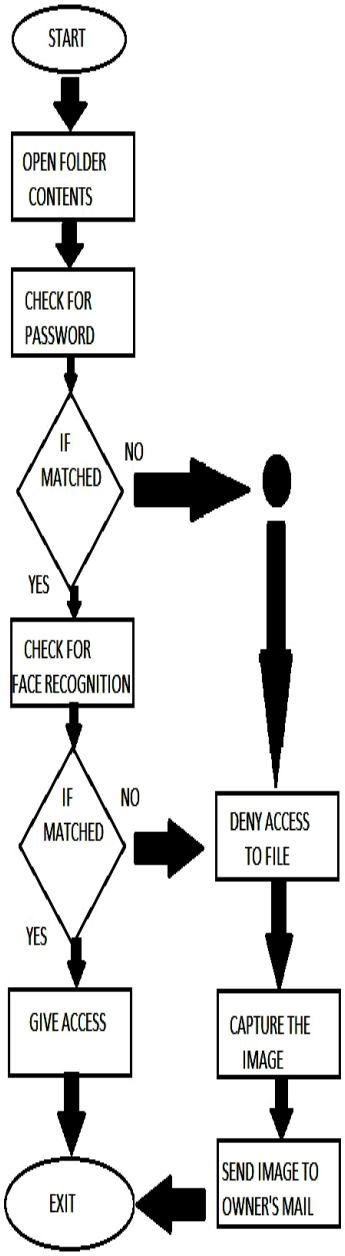

Figure 22: Architecture Facial Recognition

system recognizes the face of the user through the web-cam. If the face matches that of the owner, then the program grants access to the user. If in case the faces do not match, the access is simply denied, and the picture of the user is sent via a server of the software to the mail of the owner of the file, and also an SMS prompt is issued to the phone number of the owner of the file.

Face Image Preprocessing

The image with the face is preprocessed to an optimal level to achieve a smooth and uniform face image. Lighting defects are removed by converting to gray-scale. The size of the image is reduced as per the uniformity constraints specified by the algorithm which is used. The lighting affects the determination of the facial shape, so filters are applied so that the face shape is perfectly extractable.

Figure 23: Face Image Preprocessing

Binarization

The preprocessed face image is subjected to Binarization, which extracts the features of the face by converting the face into a feature-specific image.

Figure 24: Binarization

Binarization is done by specifying thresholds to specific localities in the image of the face and assigning binary values to the pixels by determining the histogram variations when compared to the threshold.

Face Extraction

The binarized image is subjected to face extraction by making the processed image as a matrix. The matrix values correspond to the pixel intensity values in the coordinate.

The size of the matrix is proportional to the accuracy of the extraction, but it also increases the space and time complexity. The matrix is stored as the extracted face.

The feature extraction is done using the PCA algorithm. Let there be R face images in the training set. Each image Xi is a 2-D array of any size m× n of intensity values. The image can be converted into a vector D where D = m× n pixels, and, Xi = (xi1, xi2… xiD).

The pixel rows of the image are arranged as per the vector formation. The training set image is defined by X = (X1, X2… XR) $\subset R^{D\times R.}$

The covariance matrix is defined as follows: This is the mean image of the training set. The dimension of the covariance matrix Γ is D × D. Then, the Eigen values and eigenvectors are calculated from the covariance matrix Γ.

Let Q = (Q1, Q2… Qr) $\subset R^{D\times R}$

The proposed system eliminates the training image from the training set; whenever an image is found to be matching (Euclidean distance is lower than the threshold). The training set is analyzed and the training image with the greatest Euclidean distance is flagged every time(X_m). It is eliminated whenever a new image is found to be lower than that of the threshold Euclidean distance in Eq.1.

$$\Gamma = \frac{1}{R}\sum_{i=1}^{R}(Xi - \bar{X})(X_i - \bar{X})^{\gamma} \quad (1)$$

$$= \Phi\Phi^{\gamma}$$

$$\text{Where } \Phi = (\Phi 1, \Phi 2, \dots\dots, \Phi_R) \subset \Re^{D\,x\,R}$$

$$\bar{X} = \frac{1}{R}\sum_{i=1}^{R} X_i \; -: \frac{1}{R}\sum_{i=1}^{R} X_m$$

Neural Network Architecture

Figure 25: Image through Neural network architecture

There are three layers in the neural network, namely, input layer, output layer, and a hidden layer in the middle. Each of these layers are composed of neurons and they have weights which can be assigned and modified. The path in which they communicate with each other when a sample face is encountered determines the

recognition of the face. A training set consisting of the face values of the owner of the file is submitted to the algorithm. The accuracy grows with the increase in training set.

Face Recognition

When a user tries to access the file, the face is compared to the training set using the extracted featured. They are both compared and if the Euclidean distance between the neuron is found to be lower than that of the threshold, the face is determined to be the same.

1. For every person, there are N images in the training set. The unknown K (K< N) has to be found which are the sub clusters from the image space spanned by the N training images.
2. In the beginning, the whole of the training set is assigned to be N distinct clusters. Let k = N.
3. The inter cluster distance is computed d(i, j) with the help of the equation:Eq.2
   $d_{i\neq j}(i, j) = \| Ci - Cj \|$; i, j = 1,2,…., k (2)
   C_i and C_j are the i^{th} and j^{th} clusters which is the Euclidean standard.
4. The two nearest clusters C_i and C_j are computed by the equation:Eq.3
   $d_{min}(i, j) = arg_{i,j} \min\{d(i,j)\}; i, j = 1,2,….,N, i\neq j$
5. The average of two clusters is found and a new cluster is formed and the value k is set as k = k-1.
6. Steps 3 and 5 are repeated until k becomes K.
7. All the steps are repeated for all the other subjects in the training set.

Comparison With Traditional Principal Component Analysis

When compared with traditional Principal Component Analysis(PCA), the Modified competent analysis(MCA) showed significant levels of increase in the recognition accuracy over a training set of ten people with random training images and test images varying from Straight, Tilted, Turned and Low light conditions.

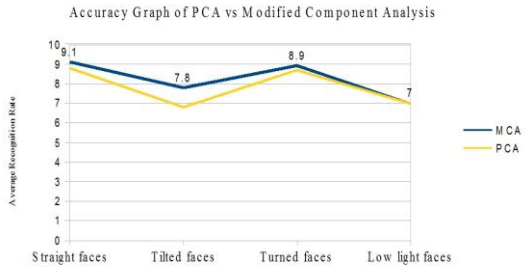

Figure 26: Accuracy Graph of PCA Vs Modified Component Analysis

Except low light conditions where the accuracy level matches with that of the PCA, all other conditions showed an average increase of accuracy. The straight face condition saw an average increase from 8.8 – 9.1, tilted faces 6.8 – 7.8 and turned

faces from 8.7 – 8.9. Low light faces remained 7 for both the algorithms. Fig.27 shows, File Security Using Neural Networks Induced Facial Recognition

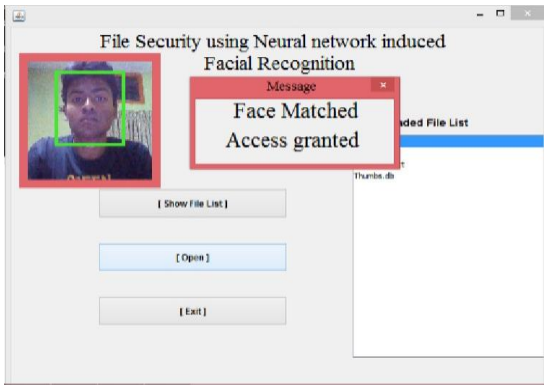

Figure 27: File Security Using Neural Networks Induced Facial Recognition

Conclusion

The existing machine learning approach for facial recognition fails to settle for more, as intelligence incorporated does not allow forced memory loss, as it is architectured like our natural neural network. The increased accuracy in output is far more important than the space and time complexity compromised. The modified component analysis incorporates forced elimination of the training images with higher euclidean distance values leading o an increase in the accuracy of the recognition of the face. This forced elimination accounts for an increase in the detection of accuracy of the face of the subject. This is due to the virtual decrease in the average of the euclidean distance of the trining image of the subject. So, as the accuracy is increased, this leads to a promising reduction in the false recognition rate and rejection rate of the subjects image than the previous algorithms.

References

[1] Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov A, Minkyu Choi, “Biometric Authentication: A Review”, International Journal of u- and e- Service, Science and Technology, Vol.2, No.3, Page.13-27, 2009.

[2] Young Ho Park, Dat Nguyen Tien, Eui Chul Lee, Sung Min Kim, Ho Chul Kim, "A Multimodal Biometric Recognition of Touched Fingerprint and Finger-vein", International Conference on Multimedia and Signal Processing, ISBN: 978-0-7695-4356-7/11 IEEE, Page 247-250, 2011.

[3] Ashraf A.Darwish, Walaa M.Zaki, Omar M.Saad, Nadia M.Nassar, Gerald Schaefer, “Human Authentication using Face and Fingerprint Biometrics”, Second International Conference on Computational

Intelligence, Communication Systems and Networks, ISBN: 978-0- 7695-4158-7/1O IEEE, Page 274-278, 2010.

[4] Naveena Marupudi, Eugene.John, Fred Hudson, "Fingerprint Verification in Multimodal Biometrics", ISBN: 1-4244-0359- 6/06 IEEE, Page 130-136, 2006.

[5] Andrew Wagner, John Wright, Arvind Ganesh, Zihan Zhou, Hossein Mobahi, Yi Ma, "Toward a Practical Face Recognition System: Robust Alignment and Illumination by Sparse Representation", IEEE Transactions on Pattern Analysis and Machine Intelligence, ISBN: 0162-8828112, Published by IEEE Computer Society, Vol.34, No.02, Page 372-386, 2012.

[6] E. Garcia Amaro, Nuno-Maganda, M.Morales-Sandoval, "Evaluation of Machine Learning Techniques for Face Detection and Recognition", ISBN: 978-1-61284-1325-5112 IEEE, Page 213-218, 2012.

[7] Ahmed EL-Barkouky, Ham Rar, Aly Farag, "Face detection at a distance using saliency maps", ISBN: 978-1-4673-1612-5/12 IEEE, Page 31-36, 2012.

[8] J.Maatta, A.Hadid, M.Pietikainen, "Face Spoofing detection from single images using texture and local shape analysis", Institute of Engineering and Technology(IET) Biometrics, Vol.1, Issue.1, Page 3-10, 2012.

[9] M.Hanuma Teja, "Real-time Live Face Detection using Face Template Matching and DCT Energy Analysis", International Conference of Soft Computing and Pattern Recognition(SoCPaR), ISBN: 978-1-4577- 1196-1I1l1 IEEE, Page 342-346, 2011.

[10] Younghwan Kim, Jang-Hee Yoo, Kyoungho Choi, "A motion and similarity based Fake Detection method for Biometric Face Recognition Systems", IEEE International Conference on Consumer Electronics (ICCE), ISBN: 978-1-4244-8712-7/111 IEEE, page 171-172, 2011.

[11] Zhiwein Zhang, Dong Yi, Zhen Lei, Stan Z Li, "Regularized Transfer Boosting for Face Detection Across Spectrum", IEEE Signal Processing Letters, Vol. 19, No.03, ISBN: 1070-9908 IEEE, Page 131-134, 2012.

[12] Unsang Park, Anil K. Jain, "Face Matching and Retrieval Using Soft Biometrics", IEEE Transactions on Information Forensics and Security, ISBN: 1556-6013 IEEE, Vol.5, No.03, Page 406-415, 2010.

[13] Norman Poh,Chi Ho Chan, Josef Kittler, Sebastien Marcel, Christopher Mc Cool, Enrique Argones Rua, lose Luis Alba Castro, Mauricio Villegas, Roberto Paredes, Vitomir Struc, Albert Ali Salah, Nikola Pavesic, Nicholas Costen, "An Evaluation of Video-to-Video Face Verification, IEEE Transactions on Information Forensics and Security", ISBN: 1556-6013 IEEE, Vol.5 No.4, Page 781-801, 2010.

[14] Ihor Paliy, Anatoly Sachenko, Yuriy Kurylyak, Ognian Boumbarov, Strahil Sokolov, "Combined Approach to Face Detection for Biometric Identification Systems", IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications Rende, Haly, ISBN: 978-1-4244-4881-4/09 IEEE, Page 425-429, Page 21-23, 2009.

[15] B.A.Efraty, M.Papadakis, AProfitt, S.Shah, I.A.Kakadiaris, "Facial Component-Landmark Detection", Computational Biomedicine Lab, University of Houston, TX, USA, Page 278-285.