Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Multimodal Biometric Authentication Using Face, Speech and Fingerprint Feature

Shaveta, Naveen Kumari
Punjabi University Regional centre of IT and Management,
Mohali, Punjab, India

Abstract—A lot of research has been done on biometrics. This paper represents the brief survey on biometrics and its modalities. It consists of the comparison between the parameters that have been used in the proposed work life face, finger prints and speech. In the paper the survey is followed as a consequence and specifies the strong technique using finger, face and speech. To overwhelm the weakness of the Uni- modal Biometric techniques, there is destitution of Multimodal biometric techniques. In the context of a given system and application, the presentation of a user's biometric feature involves both biological and behavioral aspects. A number of biometric traits have been developed and are used to authenticate the person's identity, this survey follows as a Consequence and specified way the importance of a strong multimodal biometric technique using face, fingerprint recognition and enhanced speech features.

Keywords— Biometric, Finger, Face, Speech, Modalities, Identification, Verification

I. INTRODUCTION

1.1 Biometric

"Biometrics" means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual. The application which most people associate with biometrics is security. However, biometric identification has eventually a much broader relevance as computer interface becomes more natural. Knowing the person with whom you are conversing is an important part of human interaction and one expects computer of future have the same capability [1].

A number of biometric traits have been developed and are used to authenticate the person's identity. The idea is to use the special characteristics of a person to identify him. By using special characteristics we mean the using the features such as face, iris, fingerprint, speech biometric etc.

The method of identification based on biometric characteristics is preferred over traditional passwords and PIN based methods for various reasons such as: The person to be identified is required to be physically present at the time-of-identification. Identification based on biometric techniques obviates the need to remember a password or carry a token. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics. A biometric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below [2].

1.1.1 Identification - One to Many: Biometrics can be used to determine a person's identity even without his knowledge or consent. For example, scanning a crowd with a camera and using face recognition technology, one can determine matches against the database

1.1.2 Verification - One to One: Biometrics can also be used to verify a person's identity. For example, one can grant physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retinal scan.

Biometric authentication requires to compare a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, the one captured during a login). This is a three-step process (Capture, Process, Enroll) followed by a Verification or Identification process. During Capture process, raw biometric is captured by a sensing device such as a fingerprint scanner or video camera. The second phase of processing is to extract the distinguishing characteristics from the raw biometric sample and convert into a processed biometric identifier record (sometimes called biometric sample or biometric template). Next phase does the process of enrollment. Here the processed sample (a mathematical representation of the biometric - not the original biometric sample) is stored / registered in a storage medium for future comparison during an authentication. In many commercial applications, there is a need to store the processed biometric sample only. The original biometric sample cannot be reconstructed from this identifier.

The input to the adaptive filter is a noise signal w1 (n) that is highly correlated with the additive disturbance, w(n), but is uncorrelated with the clean signal s(n). (One can think of w1 (n) as being derived from a sensor located at a point in the noise field where the signal is undetectable.) The reference signal w1 (n) is filtered to produce the output 6(n) that is an estimate of the additive noise w(n).

This output is then sub- traced from the noisy signal x(n) to produce the system out- put z(n). The system output is used to control the adaptive filter and is an estimate of s(n). Provided s(n) is uncorrelated with both w1 (n) and w(n), and the adaptive filter is adjusted to give a system output z(n) that has the least possible energy, then z(n) is a best least-squares fit to the clean signal s(n).To prove this, in proposed system note that the power in z (n) is given by E(Z'(Y1)) =E(s'(n) + (w(n)- c;(n))2 + 2s(n)(w(n) - G(n))) where E(.) denotes expected value. Now since the noise terms and the signal s(n) are assumed uncorrelated, E(2 (n)) =E(? (n)) t E((w(n) - G(n))'). Since the signal energy is a fixed quantity for the frame of interest, minimizing the output energy yields min ~(z' (n)) =E(? (n)) + min ~((w(n)

- G(n))'). Thus, when the noise canceling filter is adjusted so that (z(n)) is minimized, E((w(n) - $(n))2 is also minimized. The filter output $(n) is then a best least-squares estimate of the primary noise w(n). Moreover, when E((w(n) - $(n))') is minimized, E((z(n) - ~(n))' is also minimized since z(n) - s(n) = w(n) - 6(n). Thus, z(n) is a best least-squares estimate of the clean signal.

1.2 Biometric Modalities

Biometric modality refers to a system built to recognize a particular biometric trait. Face, fingerprint, hand geometry, palm print, iris, voice, signature, gait, and keystroke dynamics are examples of commonly used biometric traits. In the context of a given system and application, the presentation of a user's biometric feature involves both biological and behavioral aspects. A brief introduction of these common biometrics modalities is given below –

1.2.1 Face

Face recognition is a non-nosy technique, and facial pictures are most likely the most widely recognized biometric trademark utilized by people to make an individual recognition. Static or video images of a face can be used to facilitate recognition. Modern approaches are only indirectly based on the location, shape, and spatial relationships of facial landmarks such as eyes, nose, lips, and chin, and so on. Signal processing techniques based on localized filter responses on the image have largely replaced earlier techniques based on representing the face as a weighted combination of a set of canonical faces [1, 2]. Recognition can be quite good if canonical poses and simple backgrounds are employed, but changes in illumination and angle create challenges. The time that elapses between enrolment in a system and when recognition is attempted can also be a challenge, because facial appearance changes over time [2].

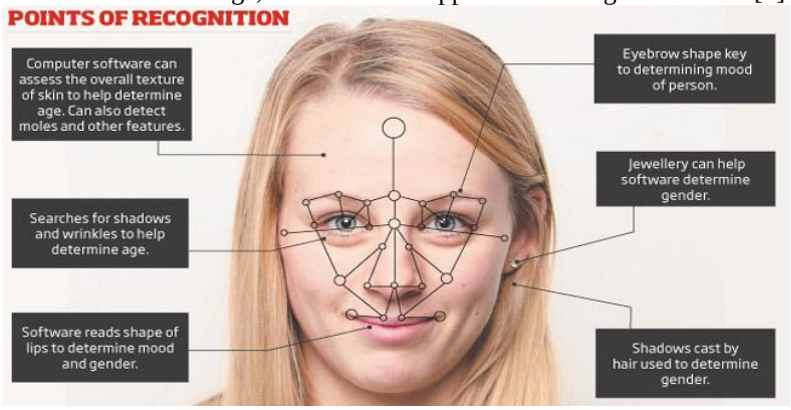

Fig.1.1 Face Recognition [14]

1.2.2 Fingerprint

Fingerprints—the patterns of ridges and valleys on the "friction ridge" surfaces of fingers—have been used in forensic applications for over a century. Friction ridges are formed in uteri during fatal development, and even identical twins do not have the same fingerprints.

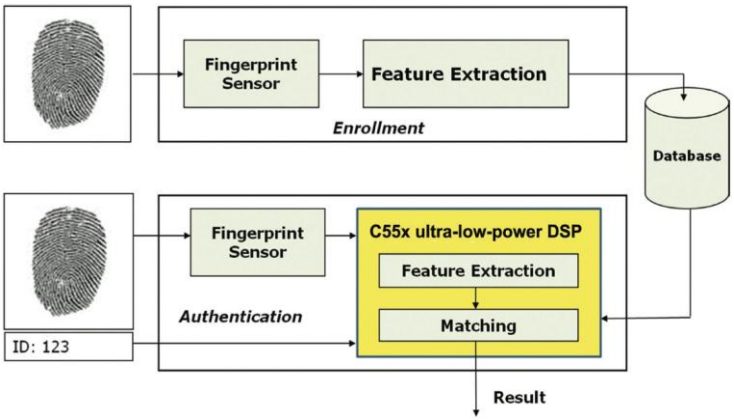

Fig.1.2 Fingerprint Recognition [15]

The recognition performance of currently available fingerprint-based recognition systems using prints from multiple fingers is quite good. One factor in recognition accuracy is whether a single print is used or whether multiple or ten prints (one from each finger) are used. Multiple prints provide additional information that can be valuable in very large scale systems. Challenges include the fact that large-scale fingerprint recognition systems are computationally intensive, particularly when trying to find a match among millions of references. Unique mark recognizable proof is a standout amongst the most remarkable and plugged biometrics [3].

1.2.3 Iris

The proposed systems are living in the age, in which the demand on security is increasing greatly. Consequently, biometric recognition, which is a safe, reliable and convenient technology for personal recognition, appears. Iris recognition is the procedure of perceiving an individual by dissecting the irregular example of the iris. The computerized system for iris recognition is generally youthful, existing in patent since just 1994 [4]. The iris is a muscle inside the eye that directs the extent of the student, controlling the measure of light that enters the eye. It is the shaded parcel of the eye, and the coloring is focused around the measure of melatonin color inside the muscle. Despite the fact that the coloration and structure of the iris are hereditarily connected, the example subtle elements are most certainly not []. The iris creates amid pre-birth development through a methodology of tight shaping and collapsing of the tissue film. Before conception, degeneration happens, bringing about the understudy opening and the iris framing arbitrary, one of kind examples. Despite the fact that hereditarily indistinguishable, an individual's iris is novel and structurally different, which takes into account them to be utilized for recognition purposes? This technology makes use of physiological or behavioral characteristics to identify individual. A biometric system is a pattern recognition system including acquiring the biometric feature from individual, extracting the feature vector from the raw data and comparing this feature vector to another person's feature vector.

1.2.4 Speech

Speech is a combination of both physical and behavioral biometrics traits. The features of an individual's voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in the synthesis of the sound. Physical characteristics of behavior part of speech change with the age, because of some medical conditions such as cold etc. A text-dependent voice recognition system is based on the utterance of a fixed predetermined phrase i.e. password. A text-independent voice recognition system recognizes the speaker independent of what she speaks. A text-independent system is more difficult to design than a text-dependent system but offers more protection against fraud. Speech recognition is most appropriate for phone-based applications but there are chances of degradation of speech signal due to quality of microphone and communication channel [4].

II. PARAMETERS USED

In order for us to determine the accuracy of any biometric system, in proposed system have to measure the error rates. There are two key error rates in biometrics, false acceptance rate (FAR) and false rejection rate (FRR).The FAR is a measurement of how many impostor users are falsely accepted into the system as "genuine" users. The FRR is a measurement of how many genuine users are falsely rejected by the system as "impostors"

FAR (False Acceptance Rate): The False Acceptance Rate (FAR) is the frequency that anon-authorized person is accepted as authorized and is calculated as follows

$$FAR = \frac{N_{fs}}{N_f} \quad \text{..... Eq. 1}$$

Nfs = Number of successful fraud attempts against a person

Nf = Total Number of fraud attempts against a person

The false acceptance rate, or FAR, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. FAR only provides half the information. When selecting a biometric solution, in proposed system needs to find out what the False Rejection Rate (FRR).

FRR: The False Rejection Rate (FRR) is the frequency that an authorized signature is rejected and is calculated as follows:

$$FRR = \frac{N_{qr}}{N_{fq}} \quad \text{.....Eq. 2}$$

Nqr = Number of rejected verification attempts for a qualified person

Nq = Total Number of verification attempts for a qualified person

The features of dynamic signature are subject to statistical fluctuations. Therefore, the recognition systems are designed with a built-in acceptance threshold. If it is high FAR decreases and FRR increases. The false rejection rate, or FRR, is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. So when a biometric solution provider claims to have a very low FAR, it is very important to find out what is the FRR at this 'low' FAR. Then depending upon the application one needs to evaluate whether the FAR & FRR ratio is acceptable for the application. In a practical scenario a low FAR & a high FRR would ensure that any unauthorized person will not be allowed access. It would also mean that the authorized people will have to put their finger on the device several times before they are allowed access.

III. RELATED WORK

Eshwarappa (2008) this paper developed a robust bimodal biometric person authentication system using speech and signature biometric features. Speaker based uni-modal system is developed by extracting Mel Frequency Cepstral Coefficients (MFCC) and Wavelet Octave Coefficients of Residues (WOCOR) as feature vectors. The MFCCs and WOCORs from the training data are modeled using Vector Quantization (VQ) and Gaussian Mixture Modeling (GMM) techniques. Signature based uni-modal system is developed by using Vertical Projection Profile (VPP), Horizontal Projection Profile (HPP) and Discrete Cosine Transform (DCT) as features. Score level fusion is employed for the development of bimodal biometric person authentication system.

Radfar,M.H (2009) This paper present that In most current model based single channel separation techniques, it is assumed that the recording conditions are identical in the training phase and application phase. In this paper, in proposed system consider a general case in which training data and application data have different levels of energy and a technique is proposed to estimate the sources' gains which are required for the separation process. In proposed system use the period gram of the speech signal as the selected feature for separation such that the sources' gains are estimated in terms of normalized period grams of the sources and the mixture. The proposed technique is compared with a state-of-the-art technique which uses AR modeling of the speech signal and maximum likelihood for estimating gain and separating the sources. Experimental results show that our technique not only outperforms this technique in terms of SNR results and gain estimation accuracy but also reduces computational complexity.

Gamliel (2009) Author wants to say that a new perceptual time varying model for non-stationary analysis of speech signals is presented. some researchers have already shown that the time varying linear prediction coding model that was applied to speech signals increases the recognition performance of automatic speech recognition (asr) systems. this improvement has been achieved due to the incorporation of the speech dynamics information in the model. Another work, perceptual linear prediction (plp) analysis of speech, has shown that a modified estimation of the auto correlation function (acf) of stationary speech frame yields major improvement to the recognition rate. the presented model, perceptual time varying linear prediction (ptvlp) analysis of speech, adopts the perceptual concepts, of how to estimate the acf, into the ptvlpmodel. This research shows that the proposed ptvlpmodel is more accurate, robust to noise and achieves better recognition rates than plp and tvlpc over wide snr range.

Crichton, R.G (2010) Author proposed that the linear prediction model of speech production is reviewed and its various formulations are related. Algorithms are presented for efficient fixed-point analysis and synthesis, together with their execution times, on a small computer. The properties of the model are discussed, and the acoustic-tube analogue is developed. This forms the basis of a system currently being used for deaf speech training. The system is described, and results and experience gained from the initial evaluation period are discussed.

Dr. S. Ravi (2013) Author describe that for the last decade of year major promotions have propelled in various biometric techniques. This paper outlines a review on various biometric authentication modalities, their merits and demerits. It also discusses comparative analysis of biometric advancement in the face, fingerprint recognition, iris feature areas. To overwhelm the weakness of the Unimodal Biometric techniques, there is destitution of Multimodal biometric techniques. This paper also states a few multimodal biometric techniques and their pitfalls. This survey follows as a consequence and specified way the importance of a strong multimodal biometric technique using face, fingerprint recognition and enhanced iris features.

Sabato Marco Siniscalchi (2014) Author proposed that Model adaptation techniques are an efficient way to reduce the mismatch that typically occurs between the training and test condition of any automatic speech recognition (ASR) system. This work addresses the problem of increased degradation in performance when moving from speaker-dependent (SD) to speaker-independent (SI) conditions for connectionist (or hybrid) hidden Markov model/artificial neural network (HMM/ANN) systems in the context of large vocabulary continuous speech recognition (LVCSR). Adapting hybrid HMM/ANN systems on a small amount of adaptation data has been proven to be a difficult task, and has been a limiting factor in the widespread deployment of hybrid techniques in operational ASR systems. Addressing the crucial issue of speaker adaptation (SA) for hybrid HMM/ANN system can thereby have a great impact on the connectionist paradigm, which will play a major role in the design of next-generation LVCSR considering the great success reported by deep neural networks ANNs with many hidden layers that adopts the pre-training technique on many speech tasks. Current adaptation techniques for ANNs based on injecting an adaptable linear transformation network connected to either the input, or the output layer are not effective especially with a small amount of adaptation data.

IV. PROBLEM FORMULATION

The pursuits of knowledge on the diverse biometric system envisage single biometrics feature is not sufficient to provide secure authentication. This dictates the importance of multi-modal system. Most of the multi-modal techniques are lacking in security aspect. Previous work presented the feature level fusion scenario with face and fingerprint modalities, using Gabor filter bank to extract the features individually but still this work is lacking in some another way like this is not used for low resolution images. By using this filter time complexity increases because size increases. Their features properties are also not properly define due to which it does not give proper acceptance.

V. PROPOSED WORK

In this work firstly images are taken of face, speech and fingerprint, and then features are extracted of respective. After the feature extraction fusion is done. Optimized features are then matched with the database and recognition is done. In the end parameter evaluation is done.

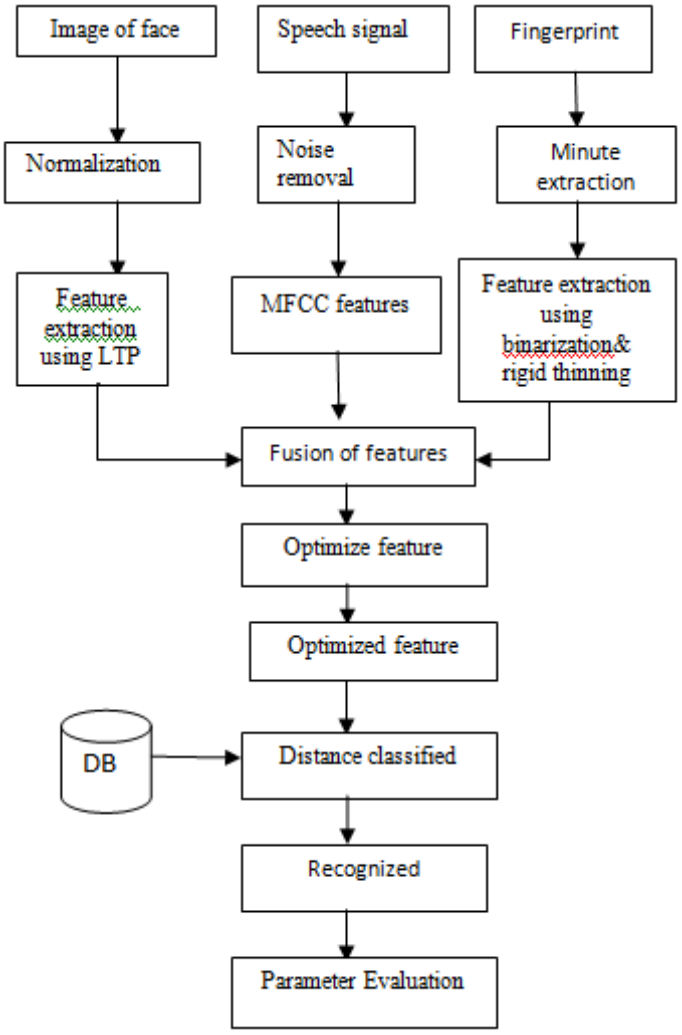

Fig. 1 Flow Chart of Proposed System

VI. RESULTS AND DISCUSSIONS

The proposed system presented the comparative study on the Multimodal biometric system incorporating face recognition, Finger print recognition and speech matching. The performance Evaluation is done on surveyed works with different Parameters and existing methods. Various issues related to Uni-modal and multi-modal biometric systems are discussed, Summarizing it can be ensured that better accuracy, security and performance can be achieved by developing multi-modal biometric systems using face, fingerprint and speech features.

TAßLE1. BIOMETRIC PARAMETERS

1	**Universality**	Each person should have the characteristic
2	**Uniqueness**	Is how well the biometric separates individuals from another
3	**Permanence**	Measures how well a biometric resist aging and other variance over time
4	**Collectability**	Ease of acquisition for measurement
5	**Performance**	Accuracy, speed and robustness of technology used
6	**Availability**	Degree of approval of a technology
7	**Circumvention**	Ease of use of a substitute

Table 2 shows experimental comparative analysis of different biometric traits with respect to the parameters listed in Table I. Table 3depicts performance comparison of different biometric technologies based on parameters like EER, FAR and FRR. The survey study put forth the importance of multi biometric system and also affirms the enhanced performance is achieved using multimodal biometric comprising of fingerprint, face and speech features, since this method has better edge over others.

TABLE 2 EXPERIMENTAL COMPARATIVE ANALYSIS OF BIOMETRIC TRAITS

	Biometric Parameters

Biometrics	Universality	Unique-Nance	Permanence	Collectab-ility	Performance	Availability	Circumvention
Face	High	Low	Med	High	Low	High	Low
Finger	Med	High	High	Med	High	Med	High
Speech	Med	Low	Low	Med	Low	High	Low

TABLE 3, Performance comparison of biometric technologies based on EER (equal error rate), FAR (false acceptance rate), FRR (false rejection rate)

TABLE 3 PERFORMANCE COMPARISON OF BIOMETRIC TECHNOLOGIES

Biometrics	EER	FAR	FRR
Face	NA	1%	10%
Finger	2%	2%	2%
Speech	6%	2%	10%
Multi-modal	1%	0%	1%

VII. CONCLUSIONS

This paper represents the comparative study of all the multimodal biometric system concluding face, finger and speech. Various biometric modalities are discussed including the parameters which have been used in the proposed work. Concluding that more accuracy and security is found using all these parameters in a biometric system.

REFERENCES

[1] Crichton, R.G "Linear prediction model of speech production with applications to deaf speech training", IEEE *Conf. on Electrical Engineers*, 2010, PP 865 – 873.

[2] C. Fookes, S. Denman, R. Lakemond, D. Ryan, S. Sridharan and M. Piccardi, "Semi-Supervised Intelligent Surveillance System for Secure Environments", *IEEE Conf. on Industrial Electronics (ISIE)*, 2010, pp 2815 – 2820.

[3] Dr. S. Ravi "Multimodal Biometric Approach Using Fingerprint, Face and Enhanced Iris Features Recognition", *IEEE Conf. on International Conference on Cireuits*, Power and Computing Technologies, 2013, pp 1143-1150.

[4] Daniela Moctezuma, Cristina Conde, Isaac Martín de Diego and Enrique Cabello "Incremental Learning with soft-Biometric features for People Re-Identification in Multi-Camera Environments", *IEEE Conf. on Digital Image Computing: Techniques and Applications (DICTA)*, 2013, pp 1 – 7.

[5] gamliel, o. "perceptual time varying linear prediction model for speech applications ",*IEEE Conf. on Acoustics, Speech and Signal Processing*, 2009, PP 4601 – 4604.

[6] Mohamed Soltane and MimenBakhti, "Soft Decision Level Fusion Approach to a Combined Behavioral Speech-Signature Biometrics Verification", International Journal of Signal Processing, Image Processing and Pattern Recognition, 2013, pp 3-10.

[7] Min-Gu Kim, Hae-Min Moon and Sung Bum Pan, "Framework of Human Identification using Multi-Modal Biometrics", International Journal of Multimedia and Ubiquitous Engineering , 2012, pp 5224 – 5227.

[8] Prof. M.N. Eshwarappa, Prof. (Dr.) Mrityunjaya V. Latte, "Bimodal Biometric Person Authentication System Using Speech and Signature Features*", IEEE Conf. on Bimodal Biometric Person Authentication System Using Speech and Signature Features*, 2008, pp 1 - 6.

[9] Radfar, M.H "Gain estimation in model-based single channel speech separation" *IEEE Conf. on Machine Learning for Signal Processing*, PP 1 – 5, IEEE 2009.

[10] Simon Denman, Alina Bialkowski, Clinton Fookes and SridhaSridharan, "Determining Operational Measures from Multi-Camera Surveillance Systems using Soft Biometrics*", IEEE Conference on Advanced Video and Signal-Based Surveillance*, 2011, pp 462 – 467.

[11] Sabato Marco Siniscalchi "Hermitical Polynomial for Speaker Adaptation of Connectionist Speech Recognition Systems" *IEEE Conf. on Audio, Speech, and Language Processing*, 2014, pp 2152 – 2161.

[12] Simon Denman, Clinton Fookes, Alina Bialkowski, SridhaSridharan, "Soft-biometrics: Unconstrained Authentication in a Surveillance Environment", *IEEE Conf. on Digital Image Computing: Techniques and Applications*, 2009, pp 196 – 203.

[13] Yukari Koga, Yasushi Yamazaki, MasatsuguIchino, "A Study on the Surveillance System Using Soft Biometric Information", *IEEE 2nd Global Conference on Consumer Electronics (GCCE*), 2011, pp 23-33.

[14] https://goo.gl/C0VcJr

[15] https://goo.gl/PQHSTP

