Advances in Computational Research
ISSN: 0975-3273 & E-ISSN: 0975-9085, Volume 7, Issue 1, 2015, pp.-194-196.
Available online at http://www.bioinfopublication.org/jouarchive.php?opt=&jouid=BPJ0000187

# FACE LOCKS PASSWORD FOR DATA SECURITY IN MOBILE DEVICES - INHERENCE BASED AUTHENTICATION

**WAGH U.B.***

Computer Science, VSS College, Jalna - 431 213, MS, India.
*Corresponding Author: Email- ujjwala_wagh4@yahoo.co.in

Received: December 18, 2014; Revised: January 05, 2015; Accepted: January 15, 2015

**Abstract-** Forgotten password is a serious problem for users. The root of the problem is a tradeoff between memorability and security. Simple password are easy to remember but easy to crack; complex password are hard to crack but hard to remember. A newly proposed alternative based on the psychology of face lock.

**Keywords-** Inherence authentication, Biometric Encryption, Biometric Encryption Algorithm, Face Recognition, Face Detection, Face Detection Using Biometric

**Citation:** Wagh U.B. (2015) Face Locks Password for Data Security in Mobile Devices - Inherence Based Authentication. Advances in Computational Research, ISSN: 0975-3273 & E-ISSN: 0975-9085, Volume 7, Issue 1, pp.-194-196.

## Introduction

Face unlock for mobile devices, which uses more information than frontal face information only based on a pan shot of the device around the user's head and intends to be more secure and usable than current mobile device unlocking approaches. Our approach requires a mobile device with a front side camera and integrated gyroscope sensor, as it conceptually uses data recorded by cameras and sensors during a pan shot.

**Table 1-** Security Comparison Features

| Biometric | Finger print | Face Lock | Hand Geometry | Voice |
|---|---|---|---|---|
| Barriers To Universality | Hand / Finger Impairment | None | Hand Impairment | Speech Impairment |
| Collectability | Medium | High | High | Medium |
| Acceptability | Medium | High | Medium | High |
| Potential for circumvention | Low | High | Medium | High |

The aim of our approach is to increase security over current mobile device authentication approaches and still retain a high usability by a fast authentication approaches, our approach requires more information than a available in a photo or video of a face from a single perspective.

When using inherence based authentication, users authenticate by providing information about something they are, such as biometric information (e. g. fingerprint, face lock, iris grain, DNA), or with implicitly derived factors, such as certain behavioral pattern (e. g. within gait or keyboard usage) which do not involve secret knowledge. We propose a variant of face unlock which is more robust and more secure against photo attacks than using frontal face information only. Our approach is based on our previous work and uses all face information available from a $180^0$ stereo camera pan shot around the user's head, which the user can take by simple panning the mobile phone with one arm in a half circle around the head. Using the mobile device's stereo camera, we record stereo images - a left/right pair of grayscale images - from multiple perspectives of the user's head. We record images instead of a video stream as they are usually of higher quality. For obtaining range images- grayscale images, in which the brightness represents the distance from the camera to the object - out of the recorded pair of stereo images, a stereo to range algorithm is applied. Then the grayscale and range images both get used for authentication.

## Inherence Authentication

A biometric is defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. Statistically analyzing these biological characteristics has become known as the science of biometrics. These days, biometric technologies are typically used to analyze human characteristics for security purposes. Five of the most common physical biometric patterns analyzed for security purposes are the fingerprint, hand, eye, face, and voice.

Biometric identification consists of two stages: enrollment and verification. During the enrollment stage, a sample of the designated biometric is acquired. Some unique characteristics or features of this sample are then extracted to form a biometric template for subsequent comparison purposes. During the verification stage, an updated biometric sample is acquired. As in enrollment, features of this biometric sample are extracted. These features are then compared with the previously generated biometric template.

Many systems have been developed for implementing biometric identification and authentication. Even for a single biometric, such as the fingerprint, there are many different methods used to create the biometric template.

### Biometric Encryption

There are various methods that can be deployed to secure a key with a biometric. One method involves remote template matching and key storage. The biometric image is captured and the corresponding template is sent to a secure location for template comparison. If the user is verified, then the key is released from the secure location. This provides a convenient mechanism for the user, as they no longer need to remember a Pass code. Unfortunately, this implies that the cryptographic key will be retrieved from the same location in a template each time a different user is authenticated by the system. Thus, if an attacker could determine the bit locations that specify the key, then the attacker could reconstruct the embedded key from any of the other users' templates.

Biometric Encryption refers to a process of secure key management. Biometric Encryption does not directly provide a mechanism for the encryption/decryption of data, but rather provides a replacement to typical pass code key-protection protocols. Specifically, Biometric Encryption provides a secure method for key management to complement existing cipher systems. Although the process of Biometric Encryption can be applied to any biometric image, the initial implementation was achieved using fingerprint images.

### Biometric Encryption Algorithm

### Image Processing

In contrast to feature-based biometric systems, the Biometric Encryption algorithm processes the entire fingerprint image. The mechanism of correlation is used as the basis for the algorithm.

### Correlation

A two-dimensional input image array is denoted by *f*(x) and its corresponding Fourier transform (FT) mate by F(u). Here x denotes the space domain and u denotes the spatial frequency domain. The capitalization of *F* denotes an array in the Fourier transform domain. Note that although the arrays defined here are two dimensional, only a single parameter, i.e. x, is used as the array variable to simplify description of the process. A filter function, H(u), is derived from an image, *f*0(x), where the subscript 0 denotes an image obtained during an enrollment session. The correlation function, *c*(x), between a subsequent version of the input, *f*1(x), obtained during verification and *f*0(x) is formally defined as

$c(X) = {}^{\infty}{}_{-\infty} f_1(V) f_0^*(X+V)dv$, where * denotes the complex conjugate. In a practical correlation system, the system output is computed as the inverse Fourier transform ($FT^{-1}$) of the product of $F_1(u)$ and $F_0^*(u)$, i.e. $c(x) = FT^{-1}\{F_1(u)F_0^*(u)\}$

Where $F0^*(u)$ is typically represented by the filter function, *H*(u), that is derived from *f*0(x). For correlation-based biometric systems, the biometric template used for identification/authentication is the filter function, *H*(u). Normally in the correlation process the filter function *H*(u) is designed to produce a distinctive correlation peak (which approximates a delta function) at the output of the system. Furthermore, a scalar value can be derived from the correlation plane (Kumar and Hassebrook), and used as a measure of the similarity between *f*1(x) and *f*0(x).

### Face Recognition/ Face Unlock

With face unlock, the mobile device unlocks for authorized users by recognizing their face, observed by a built-in camera. The core component of face unlock therefore is face recognition, which is used to distinguish between different people by their biometric facial information. First, the device records the user's face with a device integrated camera. Next, face detection and segmentation are used to find the face position in the recorded images and extract the face from the image to a smaller image only showing the face (e. g. rectangular crop area). Finally, face recognition is performed on extracted faces in order to distinguish between users.

Users performing a face unlock with [Fig-1a] the user presenting her face to the camera and [Fig-1b] the camera recorded face image.

**Fig. 1-** Performing a face unlock **(a)** and the camera recorded face image **(b)**

In terms of duration and usability, face unlock can conceptually be faster than the classical authentication approaches (PIN, password, unlock pattern) and other presented biometric authentication approaches (speaker and gait recognition). As with the other biometric authentication approaches, face unlock is not prone to shoulder surfing or similar attacks and the user do not have to remember an unlocking secret with face unlock.

Besides these advantages, face unlock approaches are conceptually prone to the shoulder surfing attack, with which an attacker spoofs the authentication by presenting a photo or video of the legitimate user to the camera Only using frontal perspective biometric facial information for face unlock – which is the case for most of the currently existing face unlock approaches

### Face Detection

Most existing authentication Approaches based on biometric face information conceptually feature a face detection, face segmentation and face recognition module.

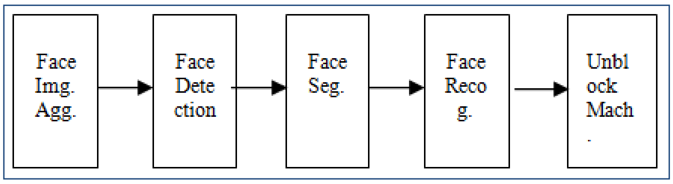

**Fig. 2-** Face detection

Face detection, segmentation and recognition as frequently used core components of a face unlock tool chain. The first module (face detection) is used to localize faces in recorded images. For mobile device unlock based on biometric face information, there is only one face to find (face localization) in the regular cases. The second module (face segmentation) extracts faces localized by the face detection module from recorded images to separated, smaller images. In most cases, the face segmentation module is integrated into the face detection module and not mentioned separately, as it is very simple (such as cropping the image to the rectangular area the face was found in). The final module (face recognition) checks the user's identity based on the segmented face images in order to decide on authentication.

Propose a mobile device face unlock approach using Haar-like feature based face detection, a local binary pattern based filter to achieve illumination invariance and likelihood ratio feature verification for face recognition .implement and evaluate an face unlock system for mobile devices using studio photographs – although they don't describe their test data or the used face detection and recognition approach in detail.

### Face Detection using Biometric

Face detection based on biometric/geometric facial features uses knowledge about the alignment of human face elements, such as position of eyes, nose, mouth, ears and eyebrows, the face contour or brighter/darker skin areas caused by shadows of the face surface structure. As these approaches need face related features in order to find a face by design, they conceptually cannot be applied to problems other than face detection without major modifications. Further, when detecting faces from different perspectives, likely different biometric features have to be derived – this results in structural different face detectors for different perspectives. Group face detection approaches based on biometric/geometric facial features in three further classes: low-level analysis, feature analysis and active shape models. Low-level analysis based face detection derives visual features from the image pixels. This includes edges, differentiation between grayscale and color pixels or - if a video is available – changes of pixels between frames.

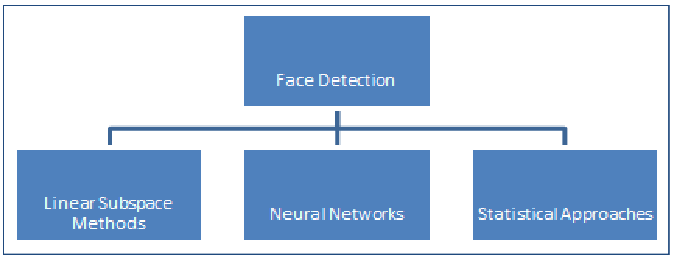

**Fig. 3-** Face Detection Approaches by Hjelmas and low

Using geometric features and view-based (appearance-based) face recognition. Geometric feature based face recognition incorporates the knowledge about geometric alignment of human face elements, such as eyes, nose, mouth, eyebrows and ears or the face contour. From this geometric alignment biometric features are derived, which further are used for face recognition.

### Conclusion

Mobile device face lock unlocking approach which uses all data available from recording a mobile device pan shot around the user's head. Our approach is intended to on the one hand increase the level of security which is realistically applied in practice during unlocking, while on the other hand retaining high usability due to fast usage and not requiring the user to remember an unlocking secret.

An inherence based approach in contrast to a knowledge based approach. In comparison to face unlocking approaches using frontal face information only, our initial implementation uses a smart phone with gyroscope sensor and built-in camera in order to evaluate feasibility of a mobile device pan shot face unlock.

**Conflicts of Interest:** None declared.

### References

[1] Lindell S.D. (1995) *SPIE's 1995 Symposium on OE/Aerospace Sensing and Dual Use Photonics*, 20-34.

[2] Stoianov A., Soutar C. & Graham A. (1999) *Optical Engineering*, 38(1), 99-107.

[3] Kumar B.V.K. & Hassebrook L. (1990) *Applied Optics*, 29(20), 2997-3006.

[4] Lee H.C., Ramotowski R. & Gaensslen R.E. (2010) *Advances in fingerprint technology*, CRC press.

[5] Findling R.D. & Mayrhofer R. (2012) *Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia*, 275-280.

[6] Hjelmås E. & Low B.K. (2001) *Computer Vision and Image Understanding*, 83(3), 236-274.

[7] Tresadern P.A., McCool C., Poh N., Matejka P., Hadid A., Levy C., McCool C. & Marcel S. (2012) *IEEE Pervasive Computing*, 99.

[8] Tronci R., Muntoni D., Fadda G., Pili M., Sirena N., Murgia G., Ristori M. & Roli F. (2011) *IEEE International Joint Conference on Biometrics,* 1-6.

[9] Tao Q. & Veldhuis R. (2010) *IEEE Transactions on Instrumentation and Measurement*, 59(4), 763-773.