A Watermarking Technique to Improve the Security Level in Face Recognition Systems: An Experiment with Principal Component Analysis (PCA) for Face Recognition and Discrete Cosine Transform (DCT) for Watermarking

Mohd Rizal Mohd Isa, Zaharin Yusoff
Computer Science Department
Faculty of Defence Science and Technology
National Defence University of Malaysia
Sungai Besi Camp 57000 Kuala Lumpur
Malaysia
Email: rizal@upnm.edu.my, zarinby@gmail.com

Salem Aljareh
School of Engineering,
University of Portsmouth, Portsmouth,
United Kingdom

E-mail: salem.aljareh@port.ac.uk

Jacey-Lynn Minoi
Faculty of Computer Science and
Information Technology
Universiti Malaysia Sarawak
94300 Kota Samarahan, Sarawak
Malaysia
E-mail: jaceylynnminoi@gmail.com

***Abstract* — This paper presents a proposal for a suitable and viable combination of a face recognition system and a watermarking system, with a watermarking technique that will ensure the authenticity of the data being transmitted in the face recognition system, which will then enhance its level of security. The proposed combination is a PCA—DCT system.**

Keywords — Biometric systems; Face recognition systems; Principal Component Analysis (PCA); Discrete Cosine Transform (DCT)

I. INTRODUCTION

Biometrics is a relatively new domain in information security technology [1]. It determines the identity of a person based on his/her biophysical features (e.g. face, fingerprint, palm-print, and iris), or behavior features (e.g. signature, voice, and gaits). Various biometric systems have been developed during the past few decades, such as automated fingerprint recognition systems (AFRS), iris recognition systems, and face recognition systems, and they have been successfully deployed in a wide range of applications, including access control, attendance control, customs checking, etc. Compared with traditional token based security systems, biometric systems are much friendlier and more difficult to cheat because biometric traits are unique to every person and are permanent throughout his/her life.

Although biometric techniques offer reliable methods for personal identification, they do suffer from several security problems. A study reported in [2] analyzed threats in biometric systems and listed them out into eight classes. As an example, one kind of attack may take place when the scanner captures the biometric traits and sends them to the feature extraction module for further processing. At this location, the transmission channel is vulnerable to several threats, such as eavesdropping attack, replay attack, man in the middle attack, and brute force attack. For instance, during the raw data transmission between the said modules, the biometric traits can be intercepted and the attackers can 'replay' the biometric traits directly to the feature extractor and effectively bypass the scanner. Countermeasures to such attacks include transmitting data over encrypted channels, the use of symmetric or asymmetric keys, digital signatures, and Timestamp/Time to Live (TTL) tags.

Figure 1 depicts the components of a typical biometric system, where the biometrics data of the Subject captured by a Sensor is to be matched with one of the authorized Objects stored in a database. The core component is made up of a Feature extraction module and a Matcher that compares the features extracted from the Subject and those from an Object. A match will result in an Approval status sent to the Application device, else a Rejection.

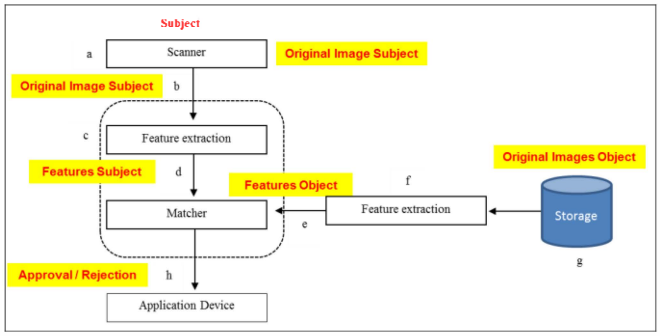

Fig. 1. Typical components of a biometric system and possible locations for interception and reintroduction of data

As mentioned, there may be attacks on a biometric system, where data may be intercepted (stolen), manipulated, and then reintroduced into the system to achieve Approval. Figure 1 can also be seen as the typical components of a face recognition system, where the Sensor device is a Scanner, and the Object database is a Facial database. More significantly, the figure shows the possible locations where data may be intercepted as well as reintroduced, namely the 8 points a, b, c, d, e, f, g, h (hence a total of 8x8 = 64 possible situations). The figure also shows the possible types of data that may be intercepted and/or reintroduced. Measures to increase the level of security of biometric systems will have to secure these 8 points, both in terms of blocking entry, as well as to ensure the authenticity of the data being transmitted.

978-1-5090-0412-6/16/$31.00 ©2016 IEEE