Biometric Encryption™

Colin Soutar, Danny Roberge[‡], Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar[†]

Bioscrypt Inc. (formerly Mytec Technologies Inc.),

5450 Explorer Drive, Suite 500

Mississauga, ONT

L4W 5M1

www.bioscrypt.com

[‡]currently with Forensic Technologies Inc.

[†]Department of Electrical and Computer Engineering, Carnegie Mellon University

The content of this article appears as chapter 22 in ICSA Guide to Cryptography, edited by Randall K. Nichols, McGraw-Hill (1999)

1 Introduction

1.1 Biometrics

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.

The use of biometric characteristics as a means of identification is not a new concept. By 1926, law enforcement officials in several U.S. cities had begun submitting fingerprint cards to the FBI in an effort to create a database of fingerprints from known criminals. Human experts in the law enforcement field were subsequently able to manually match fingerprint samples collected at a crime scene against the prints in this criminal database. Years of research in developing accurate and distinctive fingerprint classification schemes made these manual matching processes feasible by drastically reducing the required database search space. Various fingerprint classification schemes are discussed in Lee and Gaensslen. In the early 1960's the FBI invested a large amount of time and effort into the development of automated fingerprint

identification systems. This automation of biometric identification for law enforcement purposes coincided with the development of automated systems for non-forensic applications, such as high-security access control. Fingerprint identification systems have been deployed in access control systems since the late 1960's. During the 1970's a biometric product based on measuring the geometry of the hand was introduced in a number of access control applications. Interest in biometric identification eventually moved from measuring characteristics of the hand to include characteristics of the eye. In the mid-1980's the first system that analyzed the unique patterns of the retina was introduced while, concurrently, work was being performed to analyze iris patterns.

In the 1990's, research continues on developing identification systems based on a wide variety of biometric patterns, such as the traditional biometrics mentioned above (i.e. fingerprint, hand geometry, iris, and retina), along with the development of voice, signature, palm print, and face recognition systems. A few new, innovative approaches are also being examined for biometric analysis, such as ear shape, DNA, keystroke (typing rhythm), and body odor.

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.

It is convenient to distinguish between the two main objectives of biometric systems: *identification* and *authentication*. Biometric identification is the process of matching an individual to one of a large set of system users, whereas biometric authentication simply verifies that the individual is who he or she claims to be. Law enforcement applications typically require the process of biometric identification. For example, a typical law enforcement application would seek to determine the identity of an individual who has left a latent fingerprint at the scene of a crime. The law enforcement official would enter the collected fingerprint and match its template against all the stored templates in the criminal record fingerprint database. This process may also be termed a one-to-many search. Alternatively, in the process of biometric authentication the user submits an identity claim to the system. Thus, only one biometric template is retrieved from the database of users and compared with the verification sample. Authentication is typically used in circumstances where access is being controlled, whether physical access to a room or building, or access to

an electronic system such as the logon to a computer system. Biometric authentication thus processes a one-to-one match rather than a one-to-many search. For both the identification and the authentication systems, a threshold will generally be used to determine the match between templates. The setting of this threshold determines the discrimination sensitivity of the system.

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. For example, law enforcement has traditionally used a method of extracting and comparing *minutiae* points from the fingerprint. Minutiae points are locations where a fingerprint ridge ends or splits in two. Other fingerprint characteristics are sweat pore location, ridge density, and distance between ridges. In other systems, the entire fingerprint image may be processed to implement a pattern recognition process, such as correlation.

1.2 Merger of biometrics with cryptography

With the proliferation of information exchange across the Internet, and the storage of sensitive data on open networks, cryptography is becoming an increasingly important feature of computer security. Many cryptographic algorithms are available for securing information, and several have been discussed previously in this book. In general, data will be secured using a symmetric cipher system, while public-key systems will be used for digital signatures and for secure key exchange between users. However, regardless of whether a user deploys a symmetric or a public-key system, the security is dependent on the secrecy of the secret or private key, respectively. Because of the large size of a cryptographically-strong key, it would clearly not be feasible to require the user to remember and enter the key each time it is required. Instead, the user is typically required to choose an easily remembered passcode that is used to encrypt the cryptographic key. This encrypted key can then be stored on a computer's hard drive. To retrieve the cryptographic key, the user is prompted to enter the passcode, which will then be used to decrypt the key.

There are two main problems with the method of passcode security. First, the security of the cryptographic key, and hence the cipher system, is now only as good as the passcode. Due to practical problems of remembering various passcodes, some users tend to choose simple words, phrases, or easily remembered personal data, while others resort to writing the passcode down on an accessible document to avoid data loss. Obviously these methods pose potential security risks. The second problem concerns the lack of direct connection between the passcode and the user. Because a passcode is not tied to a user, the system running

the cryptographic algorithm is unable to differentiate between the legitimate user and an attacker who fraudulently acquires the passcode of a legitimate user.

As an alternative to passcode protection, biometric authentication offers a new mechanism for key security by using a biometric to secure the cryptographic key. Instead of entering a passcode to access the cryptographic key, the use of this key is guarded by biometric authentication. When a user wishes to access a secured key, he or she will be prompted to allow for the capture of a biometric sample. If this verification sample matches the enrollment template, then the key is released and can be used to encrypt or decrypt the desired data. Thus, biometric authentication can replace the use of passcodes to secure a key. This offers both convenience, as the user no longer has to remember a passcode, and secure identity confirmation, since only the valid user can release the key.

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 passcode. This method would work well in a physical access application where the templates and keys may be stored in a secure location physically separated from the image capture device. In this scenario, the communication line must also be secured to avoid eavesdropper attacks. However, for personal computer use, the keys would likely be stored in the clear on a user's hard drive, which is not secure.

A second method involves hiding the cryptographic key within the enrollment template itself via a trusted (secret) bit-replacement algorithm. Upon successful authentication by the user, this trusted algorithm would simply extract the key bits from the appropriate locations and release the key into the system. 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. If an attacker had access to the enrollment program then he could determine the locations of the key by, for example, enrolling several people in the system using identical keys for each enrollment. The attacker then needs only to locate those bit locations with common information across the templates.

A third method is to use data derived directly from a biometric image. Bodo proposed such a method in a German patent. This patent proposed that data derived from the biometric (in essence, the biometric template) are used directly as a cryptographic key. However, there are two main problems with this method. First, as a result of changes in the biometric image due to environmental and physiological factors, the biometric template is generally not consistent enough to use as a cryptographic key. Secondly, if the cryptographic key is ever compromised, then the use of that particular biometric is irrevocably lost. In a system where periodic updating of the cryptographic key is required, this is catastrophic.

An innovative technique for securing a key using a biometric has been developed by Mytec Technologies Inc., based in Toronto Canada. The solution developed by Mytec does not use an independent, two-stage process to first authenticate the user and then release the key. Instead, the key is linked with the biometric at a more fundamental level during enrollment, and is later retrieved using the biometric during verification. Furthermore, the key is completely independent of the biometric data, which means that, firstly, the use of the biometric is not forfeited if the key is ever compromised, and secondly, the key can be easily modified or updated at a later date. The process developed by Mytec Technologies is called Biometric Encryption™. During enrollment, the Biometric Encryption process combines the biometric image with a digital key to create a secure block of data, known as a Bioscrypt™. The digital key can be used as a cryptographic key. The Bioscrypt is secure in that neither the fingerprint nor the key can be independently obtained from it. During verification, the Biometric Encryption algorithm retrieves the cryptographic key by combining the biometric image with the Bioscrypt. Thus, Biometric Encryption does not simply provide a yes/no response in user authentication to facilitate release of a key, but instead retrieves a key that can only be recreated by combining the biometric image with the Bioscrypt.

Note that 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 passcode 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. The majority of this chapter therefore deals only with fingerprint images. The application of the Biometric Encryption algorithm to other biometrics is briefly discussed in the section entitled Biometric Encryption using other biometric templates.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.