Biocryptography

Increasing the protection of biometric templates

by Ravi Das

Why does the subject of biometrics receive so much attention? It is because a piece of our individual self is being extracted and literally further examined under a microscope. As a result of this, there is increased fear and mistrust amongst the public about the safety and protection of their biometric information and data, or 'biometric templates'. While these templates possess a reasonable level of entropy, there is still a strong need to protect them even more. In this two-part article, Ravi Das explains how the principles of cryptography and biometrics can be used together to provide maximum security for those biometric templates.

***Ravi Das** is a technical writer for BiometricNews.net, an independent publisher and leading source of news and information about the Biometrics Industry. Ravi holds a Master of Science Degree in Agribusiness Economics from Southern Illinois University and a Master of Business Administration (specialising in Management Information Systems) from Bowling Green State University.*

Imagine, if you will, a spectrum of security technologies, from one end to another. Somewhere in this spectrum lies the technology known as 'biometrics'. To some degree or another, most people have heard about security tools and devices, such as firewalls, routers and network intrusion devices, but biometrics is the one technology that receives the greatest scrutinisation from the private sector, the academic community, the government, and most notably, the public.

The reason for this is that a piece of our individual self, either physiological or behavioural, is being extracted, and quite literally further examined under a microscope. As a result of this attention, there is an increased fear and mistrust (as well as a certain level of apprehension) amongst the public about the safety and protection of the biometric information and data which is being stored in the devices themselves and in their respective databases. These pieces of information and data are known as 'biometric templates'. Although the templates themselves possess a reasonable level of entropy - meaning that they cannot be easily cracked or hacked into, there is still a strong need to protect them even more. One of the prime reasons for doing this is to try and quell the fear of potential misuse and mishandling of the biometric templates.

This two-part article will examine a solution to further protect biometric templates, a solution known as 'biocryptography'. It consists of four sections:

1. the scientific concepts of what a biometric template really is (in particular fingerprint recognition and iris recognition templates).
2. an introduction to (bio)cryptography, and some of its components (such as symmetric and asymmetric cryptography).
3. a review of how the concepts of cryptography can be used to increase the protection of fingerprint and iris templates in three different types of network environments.
4. conclusions and implications for further research.

The first two sections will be discussed in this issue. Section 3 and 4 will appear in the next issue of the Journal.

Biometric templates

Apart from the social perspective of the need to protect biometric templates, there is also a need to fortify the security of biometric templates from a technical perspective. Before this is discussed, it is important to define what a biometric template really is. First, a biometric sample has to be obtained: an image from a distinct characteristic such as someone's fingerprint, eye or hand, or even a voice recording. This image (or multiple images) becomes a master profile - and it is from this, that the unique features of a fingerprint or an eye, a hand or a voice are extracted, and then converted into a mathematical file. This file can be anything from a binary mathematical file to a statistical model. These mathematical files - not the images which were extracted and created - are known as the biometric templates. To illustrate the exact nature of biometric templates, two types of templates will be examined: fingerprint recognition templates and iris recognition templates.

Fingerprint recognition templates

Three steps can be distinguished in fingerprint recognition. The first step is known as 'image acquisition'. In this part of the process, a user places his or her finger on a platen or scanner, which is located on top of most fingerprint recognition devices.

The optical sensor then captures numerous images of the fingerprint. During this stage, the goal is to capture images of the centre of the fingerprint, which contains many unique features. All of the captured images are then converted into black and white images.

The second step in fingerprint recognition is the location and determination of unique characteristics of the processed fingerprint image. The fingerprint is composed of various 'ridges' and 'valleys' which form the basis for the loops, arches, and swirls that you can see on your fingertip. The ridges and valleys contain different kinds of breaks and discontinuities. These are called 'minutiae', and it is from these that the unique features are located and determined. There are two types of minutiae:

- ridge endings: the location where the ridge actually ends;
- bifurcations: the location where a single ridge becomes two ridges.

The third step in fingerprint recognition is that of template creation, based on the unique features found in the minutiae. The location and position, as well as the type and quality of the minutiae are factors taken into consideration in the template creation stage. This template then becomes a binary, mathematical format, which is a series of zeroes and ones (for example, 0100110000110o). Again, it is not the image that is stored, but the binary file, which is subsequently used for verification and identification.

Iris recognition templates

Iris recognition is very similar to fingerprint recognition, with the main difference that there is no direct contact required with a platen and its corresponding sensor. The iris is the coloured region between the pupil and the 'sclera', the white of the eye. The fibrovascular tissue of the iris is connected to the muscles of the pupil, which will help to contract and dilate the pupil. When the iris is exposed to a beam of near-infrared red light, many unique characteristics are exposed, such as the trabecular meshwork (which causes the radial pattern of the iris), arches, crypts, coronas, and many types and kinds of 'zigzag' patterns.

To capture an image of the iris, the user looks into a camera as far as nine inches away, with which high-resolution grayscale images are captured. Using software, any extraneous features, such as eyelashes, glare and eyelids are removed from the image. The unique features as described above are then located and extracted, and their spatial orientation within the iris are converted into vectors. From this point, using high-level mathematics known as the Gabor Wavelet theory, these vectors are converted into an IrisCode. This IrisCode becomes the iris template: a binary mathematical file.

Critical areas for biometric templates

A question which often gets asked is: "What will happen if my biometric template gets stolen or hacked into?" Not much, if you think about it. After all, what can a hacker do with a series of zero's and one's and/or a probability curve? Furthermore, each biometric vendor has their own proprietary, mathematical enrolment and matching (meaning, verification and identification) algorithms, so taking a template and entering it into another system is simply not feasible. But, if one were to dig deeper at a technical level, biometric templates are just like any other technology: prone to failures, hacking, theft and, to a certain degree, reverse-engineering.

There are four critical areas where biometric templates are most at risk from hacking and theft:

1. Just after a template has been created, including the verification and the enrolment template.
2. In the database (the actual database depends upon the specific biometric technology being used).
3. In client server network topology (where clients connect to a server and send it all their data for handling or routing): during the transmission of biometric templates from the biometric system to the central server, where the biometric database resides.
4. In a hosted environment, where the biometric template database resides with a third party.

An introduction to (bio)cryptography

The science of cryptography provides the means to increase the protection of biometric templates at these critical junctures. It is the science of scrambling information and data which is in transit across a network medium, and then descrambling it at the receiving end into a decipherable format. That way, if the scrambled information and data were to be intercepted by a third party, it would be of no use, unless they possess the keys for descrambling the information. But one has to keep in mind that cryptography is much more complex than this, and it makes heavy use of complex mathematics in order for the required solution to be stronger. The goal of this section is to introduce some of the very basic concepts of cryptography, as well as provide an introduction to the protocols which are being used today.

Whenever we send a message to an intended recipient - whether it is by e-mail, instant message, or even just a text message from our smartphone, this message

is often sent as a 'plaintext', or 'cleartext'. This means that the actual message is being transmitted to the intended recipient in the way it was originally constructed by the originator of the message. Thus, the only true way to protect the information being sent is to scramble it, in other words, 'encrypt the message'. This encrypted message is now known as the 'ciphertext'. The reverse of this process is known as 'decryption', with the end result being a message that the intended recipient can read.

Biocryptography

These concepts of scrambling and descrambling can be very easily applied to biometrics. This is known as 'biocryptography'. The biometric templates are protected by scrambling and descrambling keys while they are stored in the database, or in transit across a network. The biometric template (such as the fingerprint or iris recognition template) can be seen as the plaint text, or the 'plaintext biometric template'. When the fingerprint or iris template is encrypted, it can be seen as the 'cipher biometric template', and when it is decrypted, it becomes the decrypted 'plaintext biometric template'.

Functions of cryptography

Cryptography has to provide the following three functions in order for it to be truly effective:

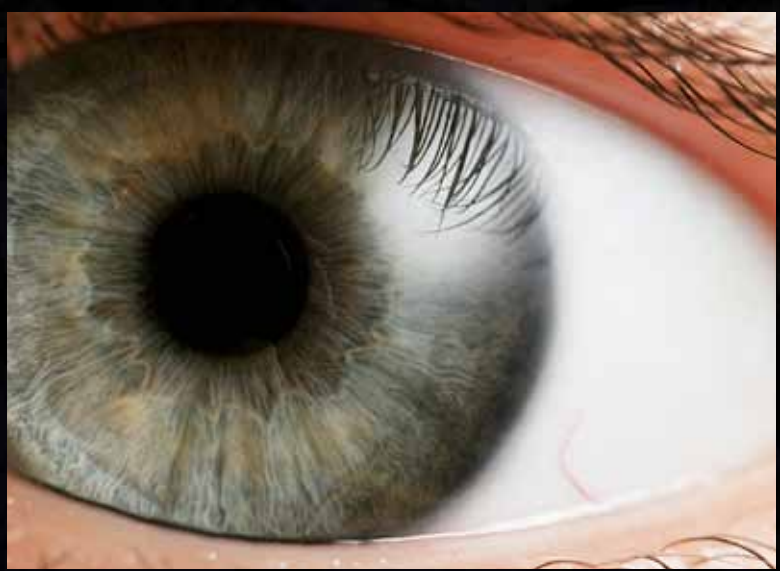
1. Authentication
   The receiver of the message (or the plaintext biometric template) should be able to completely verify the origin of it.
2. Integrity
   The message in transit (or the plaintext biometric template) should not be modified in any way or format while it is in transit (for example, replacing a fingerprint biometric template with an iris biometric template in order to spoof the biometric system).
3. Non-repudiation
   The sender of the plaintext biometric template should not falsely deny that they did not sent that particular template originally.

Mathematical algorithms

However, all of this is not possible without the use of 'ciphers' or cryptographic algorithms - mathematical functions which allow for the encryption and decryption of the plaintext biometric template while it is in transit across the network medium. A component which is central to these mathematical algorithms is a so-called 'key'. It is the key itself which is used to lock up the plaintext biometric template (or to encrypt it) at the point of origination, and it is also used to unlock that same template at the receiving end.

The key itself is a series of mathematical values - obviously, the larger the value, the harder it is to break it, while in transit. The range of possible mathematical values is referred to as the 'keyspace'. There are many types of keys used in cryptography, such as signing keys, authentication keys, data encryption keys and session keys. The number of keys which are generated depends primarily upon the mathematical algorithms used. In the world of cryptography, there are two primary types of algorithms:

1. symmetric algorithms
2. asymmetric algorithms (or Public Key Algorithms)



Symmetric algorithms

With symmetric algorithms, the key system consists of the encryption key and the decryption key. Because the same key is used to encrypt and decrypt the plaintext biometric template, they can be broken down very easily, and the information and the data can be very easily tapped into, and consequently hijacked. As a result, the use of symmetric-based algorithms possesses inherent risks and dangers, as the primary security here depends solely upon the key which is being used. If anybody divulges the secrecy behind the key, the security of it is 100% compromised.

Asymmetric algorithms

The alternative to the symmetric cryptography is asymmetric cryptography. In this process, two keys are generated: one for the encryption and one for the decryption of the plaintext biometric template. The encryption key is known as the 'public key', and the decryption key as the 'private key'. The security strength is much greater than that of the symmetric algorithms, not only because two keys are being used, but also because the decryption key cannot be computed from the encryption key.

Mathematical hashing functions

To further fortify the strengths of public key cryptography, mathematical hashing functions are used to protect the integrity of the plaintext biometric template - a critical function of cryptography. For example, when the plaintext biometric template is received at its destination, the hashing function is included with it. If the values within the hashing function have not changed after it is has been computed by the receiving end, then one can be assured that the plaintext biometric template has not been changed or altered in any way. To prove the validity of the hashing functions, it should be noted that they can be calculated in only one direction (for example, going from the sending point to the receiving point, where they are computed), but not visa versa (for example, going from the destination point to the origination point).

Public Key Infrastructure (PKI)

In businesses and corporations all over the world today, it is the asymmetric approach which is most commonly used, especially for client server network topologies, given its superiority over the symmetric approach. One of the most popular, or commercial forms of the asymmetric cryptography is known as 'Public Key Infrastructure', or 'PKI' for short. It has been around for quite some time (since the 1970's), and will be used in our example in the next section of this article, which will bring together the concepts of fingerprint/iris recognition templates and cryptography.

In the next issue of the Journal, this article will be continued with a review of how the concepts of cryptography can be used to increase the protection of fingerprint and iris templates in three different types of network environments. Also, conclusions will be given and implications for further research.

›› to be continued in KJD&I 39