# BIOMETRIC ENCRYPTION

**Vishaka Singh**

*Dept. of computer Science,RKGIT(W),Ghaziabad(India)*

## ABSTRACT

*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.*

***Keywords -- Biometric Product,*** **Matching Process**

## I INTRODUCTION

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 fingerprints 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 tothe 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 conveniences, 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.

## II 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. A general overview of correlation, as it relates to Biometric Encryption, is given in the following section. More detailed

discussions of correlation and its applications are given in the references by Goodman, Steward and VanderLugt. 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, f0(x), where the subscript 0 denotes an image obtained during an enrollment session . 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. Such a correlation peak can easily be identified in a correlator system, and its position can be used to track an object of interest, see Hahn and Bauchert. Furthermore, a scalar value can be derived from the correlation plane (Kumar and Hassebrook), and used as a measure of the similarity between f1(x) and f0(x). The process of correlation provides an effective mechanism for determining the similarity of objects, and has been successfully used for fingerprint authentication (Stoianov et al). In the next section, it will be demonstrated that the process of correlation can also be used as the basis for the Biometric Encryption algorithm.

## III. SYSTEM REQUIREMENTS

The objective of the Biometric Encryption algorithm is to provide a mechanism for the linking and subsequent retrieval of a digital key using a biometric such as a fingerprint. This digital key can then be used as a cryptographic key. The important system requirements that apply to a key retrieval system using a fingerprint are distortion tolerance, discrimination and security.

• Distortion tolerance is the ability of the system to accommodate the day-to-day distortions of the fingerprint image. These distortions are due to behavioral changes (positioning, rotation, and deformation), as well as environmental (ambient temperature and humidity) and physiological (moisture content) conditions. A key retrieval system must be able to consistently produce the correct key for the different expected versions of a legitimate user's fingerprint.

• Discrimination is the ability of a system to distinguish between all of the system users' fingerprints. An attacker should produce an incorrect key when the attacker's fingerprint is combined with a legitimate user's filter.

• Security of the system means that neither the digital key, nor the legitimate user's fingerprint, can be independently extracted from any stored information.

To satisfy these three constraints simultaneously, the process of correlation was used as a mechanism for linking and retrieving the digital key. As discussed above, correlation is normally used to provide a single scalar value which indicates the degree of similarity between one input image, f1(x), and another, f0(x), that is represented by the filter function, H(u). The process of Biometric Encryption, on the other hand, needs to extract more information than a simple yes/no response from the system. In fact, Biometric Encryption is designed typically to output 128 bits of information to be used as a cryptographic key. Thus, it is not immediately evident how the process of correlation can be applied to this procedure. However, it is known that the process of correlation can be used to design filter functions that are tolerant to distortions in the input images; see Kumar, or Roberge et al. This distortion tolerance property of the correlation filter is critical to the implementation of Biometric Encryption. Instead of designing a filter function, H(u), which produces a simple output pattern, c(x), which

approximates a delta function, the process of Biometric Encryption produces a more sophisticated output pattern. This output pattern is linked during enrollment with a particular digital key, and subsequently regenerated during verification to retrieve the same digital key.

Design of the filter function The filter function will be optimized for the following two requirements: that it consistently produces the same output pattern for a legitimate user, and that it is tolerant to distortions present in the input images. To provide a degree of distortion tolerance, the filter function is calculated during an enrollment session using a set of T training images, where $T \geq 1$. Denote the T images of the fingerprint by {f01(x), f02(x), f0T(x)}, where the subscript 0 denotes a training image. The filter function that will be constructed using these images is denoted by H(u). Note that we may refer to complex-valued functions such as H(u) independently by their magnitude and phase components, denoted by |H(u)| and () uHie φ , respectively. The output pattern produced in response to f0t(x) is given by c0t(x) and the E-3: Identification code creation A requirement of the Biometric Encryption algorithm is that an incorrect key should be produced when an attacker uses the system with another user's Bioscrypt. In fact, it is convenient to further constrain the system such that an incorrect key is never released from the algorithm, but instead a verification failed message is passed to the cryptographic system. This will avoid the cryptographic system making wasteful attempts at decryption using an incorrect key. Therefore, a key validation scheme is required for the process. Obviously the key, k0, itself cannot be stored in the Bioscrypt for comparison with the key generated at verification. Instead, a combination of standard encryption and hashing algorithms is used to produce a derived identification code, id0. During verification, a corresponding identification code will be similarly derived from the retrieved key, k1. Comparing the identification code created during verification with that created during enrollment allows the system to determine if the key retrieved during verification is correct.

The method used for key validation is as follows. Using the input N-bit key, k0, as an encryption key, encrypt S bits of data. Next, hash the encrypted text using a one-way hash function to create an identification code, id0. Store this identification code in the Bioscrypt.

The S bits, to be encrypted, can be any S bits that will be available at both enrollment and verification. Also, these S bits should be different for each user in order to provide the key validation procedure with maximal security, see Schneier. Given these constraints, we use S bits from the stored filter function, Hstored(u), as it is available during both the enrollment and verification procedures. Also, because Hstored(u) is the product of fingerprint information and a random array, it will be distinct for each user. Therefore, we use the first S bits of Hstored(u) as input data to the encryption algorithm.

The choice of encryption algorithm and hash function is independent of the Biometric Encryption process. These algorithms are required simply for creation of the identification code, and the main concern in the choice of these algorithms is that they are secure. Good examples to use are Triple-DES as the encryption engine and SHA-1 as the hash function (Schneier).

The lookup table and id0 are now appended to Hstored(u) to complete construction of the Bioscrypt, which can be stored on any conventional storage medium.

Verification The objective of the verification procedure is the successful retrieval of the N-bit key for a legitimate user.

With reference to figure 22-2, a set of biometric images is acquired from the system user and combined with Hstored(u), the lookup table, and id0, from the Bioscrypt, to retrieve and check the validity of an N-bit key. If this key is found to be correct, it will be passed on to the cryptographic system.

With reference to figure 22-5, it is observed that the image processing stage of verification is very similar to the corresponding stage of enrollment. As in enrollment, T fingerprint images are acquired from the system user. Fourier transforms are performed on the images and the terms A1(u) and D1(u) are calculated. Using Hstored(u) retrieved from the Bioscrypt, the output pattern, c1(x), is calculated according to equation 22-19, and is then passed to stage V-2 of the verification procedure to retrieve the N-bit cryptographic key.

The verification pattern, c1(x), will be used to retrieve the cryptographic key. Clearly, the similarity of the output patterns, c1(x) and c0(x), significantly affects the discrimination capabilities of the system. It is therefore interesting to compare the generation of c1(x) and c0(x) for legitimate users and attackers, and to understand how this affects the discrimination of the system.

The magnitude information from the attacker's fingerprints is not equivalent to that derived from the legitimate user. Therefore, the weighting of the contribution of the phase values is not properly moderated. Furthermore, the phase information derived from the attacker's fingerprints does not cancel the enrollment phase information which was implicitly stored in Hstored(u). Thus, both the magnitude and phase terms derived from the attacker's fingerprint affect the generation of c1(x), producing a pattern that is significantly different from the legitimate user's c0(x) pattern. Thus, the key retrieved from this pattern will not match the key linked to c0(x) during legitimate user enrollment.

Concatenate the real and imaginary parts, as in the enrollment stage E-2, to create a verification template of dimension 128×64. Binarize each value, as in E-2, to create a binarized verification template (the equivalent of the binarized enrollment template). 3. Use the lookup table to extract the constituent bits of the binarized verification template that are required for the key. Define k1 as an N-element vector. For the nth element of k1, sum the L bits of the binarized verification template whose indices are specified by the nth column of the lookup table. The nth element of k1 is set to 1 if the sum of these bits is greater than L/2, and it is set to 0 otherwise. In other words, a decision by majority is used to assign the parity of the nth bit of k1. 4. Determine the validity of the retrieved key. This process is described in the following section on verification stage V-3. 5. If k1 is found to be the correct key, release it into the system. If k1 is found to be incorrect, return to c1(x) and extract a 64×64 portion of c1(x) that is offset from the center by one pixel. Continue to repeat steps 2 to 5 of the retrieval algorithm with all portions of c1(x) that are one pixel offset from the center, then continue with all portions that are two pixels offset from the center, and so on, up to approximately sixteen pixel offsets. If at any point the key retrieved is found to be correct, cease the algorithm and release k1. If the key is found to be incorrect for all pixel offsets, release a verification failed message.

Note that step 5 of the key retrieval algorithm is required to accommodate relative translations of the input fingerprints between enrollment and verification. We find that, in general, a search of one quarter of the input aperture, or ±16 pixels in an array of dimension 128×128, is sufficient.

V-3: Key validation Step 4 of the retrieval algorithm requires that a key, k1, be checked for validity. This key should be released only if it precisely matches k0, the key linked to the output pattern during enrollment. To check the validity of k1, we calculate an identification code, id1, and compare it with the stored id0. The identification code, id1, is calculated the same way as id0 was during enrollment stage E-3, i.e. using k1 as an

encryption key, encrypt the same S bits of the stored filter function, then hash the encrypted text to produce id1. The identification code, id1, is then compared with id0. If id1 = id0, then k1 = k0, with high probability (Schneier), and k1 can be released to the cryptographic system. If id1 ≠ id0, then k1 ≠ k0 and either a verification failed message is released, or the retrieval algorithm continues with the next pixel offset of c1(x). Biometric Encryption using other biometric templates Although the Biometric Encryption algorithm was developed primarily for use with image-based biometric templates, the process can also be applied to other biometric templates. This can be achieved simply by representing the non image-based biometric template as an image array. For example, a minutiae-based fingerprint template can be represented as an image array by embedding a code referring to each minutiae type at the appropriate location in a two-dimensional array, thereby creating a map of the minutiae points. This array can then be input to the Biometric Encryption algorithm, as described above for fingerprint images. Using a minutiae-based rather than an image-based template may have the added advantage of producing a rotation invariant system, assuming the original minutiae template contained information about the relative orientation of the minutiae.

For some other biometric types, different considerations may modify the algorithm. For example, images of the iris or retina can easily be aligned using the center of the eye's pupil as a reference point. Thus, for these types of images, the Biometric Encryption process is not required to be translation invariant. Therefore, transforms other than the Fourier transform may be appropriate, such as the Gabor transform, which was originally used in the algorithm for iris identification developed by Daugman. Also, the distortion tolerance requirements of the filter function may be relaxed for biometrics other than fingerprints. The majority of the distortions present in fingerprint images is due to the skin deforming on contact with a glass or metal surface. For other biometrics, such as the iris or retina, there typically is no direct contact between the biometric and the system. Therefore, less distortion will be present in these biometric images, and the distortion tolerance of the filter can be decreased either by adjusting α in equation 22-11, or by completely removing the magnitude terms in equations 22-15 and 22-18. This will typically make the system more secure by improving the discrimination capabilities of the system.

## IV. CONCLUSION

Biometric Encryption is an algorithm for the linking and retrieval of digital keys, which can be used as a method for the secure management of cryptographic keys. The cryptographic key is generated independently from the Biometric Encryption algorithm and can be updated periodically via a re-enrollment procedure. The convenience and security provided by Biometric Encryption will undoubtedly help to promote more widespread use of cryptographic systems.

## REFRENCES

[1] Albert Bodo, "Method for producing a digital signature with aid of a biometric feature", German patent DE 42 43 908 A1, (1994).

[2] J. Daugman, "High confidence visual recognition of persons by a test of statistical independence", IEEE Trans. on Pattern Analysis and Machine Intelligence 15, 1148-1161, (1993)

[3] J.W. Goodman, Introduction to Fourier Optics, McGraw-Hill, (1968).

[4] W.B. Hahn, Jr., and K.A. Bauchert, "Optical correlation algorithm development for the Transfer of Optical Processing to Systems (TOPS) program", Proc. SPIE 1959, 48-54, (1993).

[5] B.V.K. Vijaya Kumar, "Tutorial survey of composite filter designs for optical correlators," Applied Optics, 31, 4773-4801, (1992)

[6] B.V.K. Vijaya Kumar and L. Hassebrook, "Performance Measures for Correlation Filters", Applied Optics, 29, 2997-3006, (1990).

[7] H.C. Lee and R.E. Gaensslen, Eds., Advances in Fingerprint Technology, CRC Press, New York: Elsevier, (1991).

[8] AbhijitMahalanobis, B.V.K. Vijaya Kumar and David Casasent, "Minimum average correlation energy filters," Appl. Opt. 26, 3633-3640, (1987).

[9] Danny Roberge, Colin Soutar and B.V.K. Vijaya Kumar, "Optimal correlation filter for fingerprint verification", Proc. SPIE 3386, 123-133, (1998).

[10] Ph. Réfrégier, "Optimal trade-off filters for noise robustness, sharpness of the correlation peak, and Horner efficiency," Opt. Lett. 16, 829-831, (1991).

[11] Bruce Schneier, Applied Cryptography, 2nd Ed., John Wiley & Sons, Inc., New York, (1996).

[12]Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar, "Biometric Encryption™ using image processing", Proc. SPIE 3314, 178-188, (1998).

[13]Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar, "Biometric Encryption™ - Enrollment and Verification Procedures", Proc. SPIE 3386, 24-35, (1998).

[14] E.G. Steward, Fourier Optics: an introduction, Ellis Horwood Limited, (1983).

[15] D. Stinson, Cryptography: theory and practice, CRC Press Inc., Boca Raton, (1995).

[16]Alex Stoianov, Colin Soutar, and Al Graham, "High-speed fingerprint verification using an optical correlator," Proc. SPIE 3386, 242-252, (1998).

[17] A. VanderLugt, Optical Signal Processing, John Wiley & Sons, Inc., (1992).