Eduard Nabokov

FICT

IP-52

What is Cryptography?

- *How does it influence on cyber crime nowadays?*
- *What is biometric encryption?*
- *How important is security in Internet?*

ABSTRACT

In the last decade of computer security, using biometrics for various types of security problems has become more and more popular. The uniqueness of biometrics for any specific human being makes the identification system more secure. Biometrics is widely used in person identification and verification. Biometrics as such poses few security risks. Combining cryptography with biometrics is a new research area. This technique proves to be more secure. We basically deal with the use of keystroke dynamics, speech and 2D biometric data (such as fingerprint, palmprint, face, etc) as various biometric approaches or techniques. We will discuss privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of Biometric Encryption over other uses of biometrics.

Keywords : Biometric encryption, cryptography, security, key generation

INDEX

Background

Identification and authentication requirements are steadily increasing in both the online and offline worlds. There is a great need on the part of both public and private sector entities to know who they are dealing with.

The current security model for:

- the verification of identity
- protection of information
- authorization to access premises or services

is based on using ***a token.***

This token may be:

- ***a password or shared secret*** (something you know)
- ***an identity card*** (something you have)
- ***a biometric*** (something you are)

In all of these cases, the details of the token are held by a third party whose function is to authorize and at times allow the transaction to proceed if the details of an individuals token match those stored in a database. The biometric is increasingly viewed as the ultimate(finalize) form of authentication or identification, supplying the third and final element of proof of identity. Accordingly, it is being rolled out in many security applications.

1. Growing Public Awareness and Interest

Biometrics are expected to add a new level of security to applications, as a person attempting access must prove who he or she really is by presenting a biometric to the system. Such systems may also have the convenience, from the users perspective, of not requiring the user to remember a password.

There is evidence of growing public awareness and interest in the use of biometrics.
Border Security Control: Perhaps the most visible (and controversial) use of biometrics is taking place in the transportation sector. Identification requirements at airports and border crossings may now involve the collection and processing of travellers' fingerprints, facial images, and iris patterns. Increasingly, machine readable travel documents such as ***passports, drivers licenses and other identity or travel cards*** may also contain biometric data or images. Frequent travellers who apply for and pass extensive background checks may use their biometrics for speedy passage through customs and immigration.

Payment Systems: We are seeing increasing uses of biometrics by the private sector for enhanced convenience services, such as "pay 'n' go" systems that allow enrolled customers to pay for groceries or gasoline using only their finger — at times, an enormous convenience.

Access Control: One of the most widespread uses of biometrics has been for physical and logical access to secure areas or resources (e.g. to a database of medical records) In such circumstances, biometrics can enhance security by helping to ensure that access to sensitive resources is strictly restricted to authorized individuals.

2. A Biometrics characteristics

"Biometrics" refers to automatic systems that use measurable, physical or physiological characteristics or behavioral traits to recognize the identity, or verify/authenticate the claimed identity of an individual. The examples of biometric characteristics that have been used for automated recognition include fingerprints, iris, face, hand or finger geometry, retina, voice, signature, and keystroke dynamics.

These systems are based on the following steps: a biometric sample is taken from an individual, for instance, a fingerprint. This physical characteristic may be presented by an image. Often data are extracted from that sample. These extracted data constitute a *biometric template*. The biometric data, either the image or the template or both, are then stored on a storage medium. The medium could be a database or a distributed environment, such as smart cards. These preparatory phases together constitute the process of *enrollment*. The person whose data are thus stored is called the enrolee.

The actual purpose of the biometric system is only achieved at a later stage. If a person presents himself to the system, the system will ask him to submit her biometric characteristic(s). The system will then compare the image of the submitted sample (or the template extracted from it) with the biometric data of the enrole. If the match succeeds, the person is then recognised and the system will "accept" him. If the match does not succeed, he is not recognized and he will be "rejected."

3. Problems with using Biometrics for Identification Purposes

It is important to bear in mind that the collection of biometric samples and their processing into biometric templates for matching is subject to great variability. Simply put, no two samples will be perfectly identical. Facial recognition technologies, for example, are notoriously prone to variability due to different lighting conditions, angle, subject movement, and so forth. This is the reason, for example, ***that we are asked not to smile in our passport photos***. Among the various biometric types, irises seem to be the most accurate and consistent.

As a consequence, live biometric samples can be at some variance with stored reference samples, making comparison, matching and identification an inexact process. In other words, biometric systems do not have 100 per cent accuracy. When the biometric system cannot perform a proper match and (incorrectly) rejects a legitimate user, this is called a false reject, and the user must typically resubmit one or more biometric samples for further comparison by the system.

Other challenges for a biometric system are speed (the system must make an accurate decision in real time), and security (the system must be resilient against attacks).

So far, we have presented a straightforward technical discussion of the critical concepts of FAR(false acceptance rate) and FRR (false rejection rate).

But, because people usually only have two thumbs, two eyes, and one head, it is nearly impossible to change these if and when the related biometric data become compromised. In this sense biometrics operate like shared secrets or passwords — learn the secret and you're in! But there are some very important difference between biometrics and passwords: you cannot change them and have no choice but to keep them for life. Lose control of your lifetime password and you will have some explaining to do! This, regardless of the fact that security experts roundly condemn using unchangeable passwords as shared secrets (e.g. birthdates and SSNs).

4. Security Vulnerabilities of a Biometric System

Biometric systems may become vulnerable to potential attacks.

Some of those security vulnerabilities include the following:

- Spoofing: It has been demonstrated that a biometric system sometimes can be fooled by applying fake fingerprints, face or iris image, etc.
- Replay attacks: Example, circumventing the sensor by injecting a recorded image in the system input — much easier than attacking the sensor.
- Substitution attack: The biometric template must be stored to allow user verification. If an attacker gets an access to the storage, either local or remote, he can overwrite the legitimate users template with his/her own — in essence, stealing their identity.
- Tampering: Feature sets on verification or in the templates can be modified in order to obtain a high verification score, no matter which image is presented to the system.
- Quality of biometric data: poor quality may lead to higher FRR and FAR. While FAR increases the security risks for the system, a false rejection often causes some follow-up procedures which can be privacy-invasive to the individual.

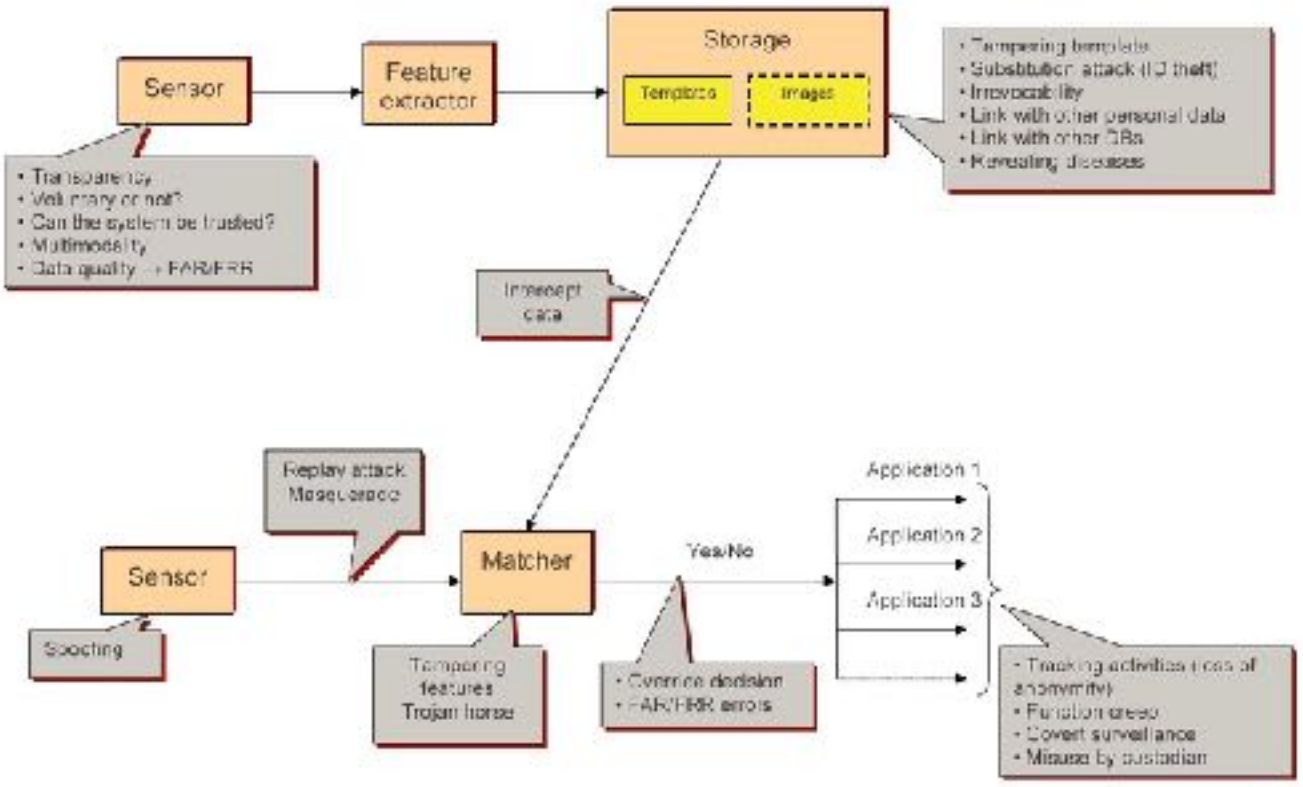

Figure 1.1: Privacy and Security issues involving Biometric System

Biometric Encryption

1. Biometrics and Cryptography

Conventional cryptography uses encryption keys, which are just bit strings long enough, usually 128 bit or more. These keys, either "symmetric", "public", or "private" are an essential part of any cryptosystem. A person cannot memorize such a long random key, so that the key is generated, after several steps, from a password or a PIN that can be memorized. The password management is the weakest point of any cryptosystem, as the password can be guessed, found with a brute force search, or stolen by an attacker.

On the other hand, biometrics provide a person with unique characteristics which are always there. Can they be used as a cryptographic key? Unfortunately, the answer is negative: biometric images or templates are variable by nature, i.e., each new biometric sample is always different. Needless to remind that conventional cryptography does not tolerate a single bit error.

2. What is Biometric Encryption?

Because of its variability, the biometric image or template itself cannot serve as a cryptographic key. However, the amount of information contained in a biometric image is quite large: for example, a typical image of 300x400 pixel size, encoded with eight bits per pixel has 300x400x8 = 960,000 bits of information. Of course, this information is highly redundant.

Biometric Encryption is a process that securely binds a PIN or a cryptographic key to a biometric, so that neither the key nor the biometric can be retrieved from the stored template. The key is re-created only if the correct live biometric sample is presented on verification.

The digital key (password, PIN, etc.) is randomly generated on enrolment, so that the user (or anybody else) does not even know it.

The key itself is completely independent of biometrics and, therefore, can always be changed or updated. After a biometric sample is acquired, the BE algorithm securely and consistently binds the key to the biometric to create a protected BE template, also called "private template". In essence, the key is encrypted with the biometric. The BE template provides an excellent privacy protection and can be stored either in a database or locally (smart card, token, laptop, cell phone, etc.). At the end of the enrolment, both the key and the biometric are discarded.

On verification, the user presents her fresh biometric sample, which, when applied to the legitimate BE template, will let the BE algorithm retrieve the same key/password. In other words, the biometric serves as a decryption key. At the end of verification, the biometric sample is discarded once again. The BE algorithm is designed to account for acceptable variations in the input biometric. On the other hand, an attacker, whose biometric sample is different enough, will not be able to retrieve the password. This encryption/decryption scheme is fuzzy, as the biometric sample is different each time, unlike an encryption key in conventional cryptography. Of course, it is a big technological challenge to make the system work.

After the digital key, password, PIN, etc., is retrieved, it can be used as the basis for any physical or logical application. The most obvious way lies in the conventional cryptosystem, such as a PKI, where

the password will generate a pair of Public and Private keys.

Thus, Biometric Encryption is an effective, secure, and privacy friendly tool for biometric password management, since the biometric and the password are bound on a fundamental level.

Methods and Algorithms used in Encryption

Cryptographically Secure Pseudorandom Number Generators

A cryptographically secure pseudo-random number generator is a pseudo-random number generator with properties that make it suitable for use in cryptography.

Many aspects of cryptography require random numbers, for example:

– key generation

– nonce

– one-time pads

There are two basic algorithms: ***asymmetric*** and ***symmetric***

Symmetric Encryption

WHAT IS IT?

Symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key), whereas asymmetric algorithms use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key.

WHAT KIND OF TYPES DOES IT EXIST?

Symmetric algorithms can be divided into two types - stream ciphers and block ciphers. Stream ciphers encrypt a single bit of plaintext at a time, whereas block ciphers take a number of bits (typically 64 bits in modern ciphers), and encrypt them as a single unit.

EXAMPLES OF SYMMETRIC ALGORITHMS

1. *AES (Advanced Encryption Standard)*
2. *Serpent*
3. *Blowfish*
4. *IDEA*
5. *RC2*
6. *Twofish*

Let's see an example:
There are Alice and Bob. Alice generates key and encrypt her message with it for Bob before send it. However, Bob cannot read that message, because he doesn't know a key to decrypt it. The problem is how Alice can share a key to Bob securely.
This is why asymmetric algorithms was invented, that is supposed to solve this problem.

Asymmetric Encryption

WHAT IS IT?

Asymmetric algorithms (public key algorithms) use different keys for encryption and decryption, and the decryption key cannot (practically) be derived from the encryption key. Asymmetric algorithms are important because they can be used for transmitting encryption keys or other data securely even when the parties have no opportunity to agree on a secret key in private.

EXAMPLES OF SYMMETRIC ALGORITHMS

1. *RSA*
2. *Diffie-Hellman*
3. *SSH*
4. *Bitcoin*
5. *HTTPS websites*

Let's see an example:

There are Alice and Bob.
Alice and Bob generate two keys (public and private).
They swapped their public keys.
To send a message to Bob, Alice encrypts message with Bob's public key and send it to Bob. Consequently, Bob decrypted this message with his private key.

And can do that the same way regarding to send it to Alice.
Both they can keep private key securely. Even if public key can be stolen by others.

Encryption biometrics

Enrolment and certification

1. Case Study #1: Small-scale use of Biometric Encryption

1. Alice creates a Biometric Encryption template from her biometric and a randomly selected PIN. Neither the biometric nor the PIN can be recovered from the template;
2. The PIN is used to generate a pair of keys called public and private keys;
3. The biometric, the PIN, and the private key are discarded;
4. If secure officer is satisfied that Alice has executed the steps honestly, he certifies the binding between Alice's name and the public key, i.e., he digitally signs the pair [Alice, public key]. At this point, Alice may send the public key to Bob, or even publish it for all to see.

Verification (A challenge/response scheme is used to verify Alice):

1. At any time when appropriate (e.g. whenever Alice desires to authenticate herself to Bob), Bob sends Alice a fresh random challenge;
2. By obtaining her new biometric sample and applying it to her Biometric Encryption template, Alice recovers on-the-fly her PIN, which, in turn, regenerates her private key;
3. Alice signs the challenge with her private key and gives Bob the signature;
4. Bob authenticates Alice by checking the validity of the signature under her authentic public key.

In summary, Alice has in her possession and under her control as many BE templates as necessary. She can use them to digitally sign in, either for remote authentication or for logical or physical access. The authentication is done simply by checking the validity of her digital signature using standard cryptographic means. Neither Alices biometric nor her PIN are stored or revealed. As a result, the system is both secure and highly privacy protective.

2. Case Study #2: Anonymous database; large or medium-scale applications

The authentication procedure using challenge/response scheme is similar to that in case study 1:

1. If Alice does not have her smart card with her (e.g. in the case of an emergency), Bob sends Alice's BE template to the doctor's office;
2. Alice applies her new biometric sample to the BE template and recovers on-the-fly her PIN;
3. The PIN is used to regenerate her private key, the pointer to her medical record, and the crypto-key;
4. Bob sends Alice a fresh random challenge;
5. Alice signs the challenge with her private key and gives Bob the signature;
6. Bob authenticates Alice by checking the validity of the signature under her public key;
7. Alice securely sends Bob the pointer to her medical record;

8. Bob recovers Alices encrypted medical record (or a part of it, also encrypted) and sends it to Alice;
9. Using her crypto-key, which was regenerated from her PIN, Alice decrypts her medical record for the doctor;
10. Alices biometric, the PIN, the private key, the pointer, and the crypto-key, are discarded.

In summary, Bob (the database administrator) has an assurance that Alice is, in fact, who she claims to be (she was able to unlock her BE template in the doctor's office); he is also assured that her medical record was sent to the right person. On the other hand, Alice retains full control over her medical record, so that even Bob (the database administrator) has no access to it, since he does not have the crypto-key to decrypt it. The privacy protection is embedded into the system at a very basic technological level.

3. Case Study #3: Travel documents; large-scale database applications

Border passage now involves the following steps:

1. At a kiosk, a user claims his identity (ID), and presents his biometric (e.g. facial image, fingerprint or iris) for measurements;
2. The ID is sent to the third-party database to extract the corresponding BE template;
3. The BE template is transmitted to the kiosk;
4. The BE template and the biometric measurement are combined to derive a cryptographic key, or rather a hashed version of it;
5. The image of the iris, face or fingerprint is extracted from the ePassport and used together with the BE template to derive another hashed version of the cryptographic key. This will validate the biometric stored on the ePassport;
6. Both hashed versions of the key derived on Steps 4 and 5 are transmitted to the border- control authority and verified against the database version. A positive authentication is achieved when all three versions are exactly the same.

In summary, the user's privacy is protected since the biometric image or template is not stored in a central database; instead, a secure BE template is stored. The database is inherently secure, meaning there is no need for complicated encryption and key management protocols. The ePassport is protected against tampering, since a potential attacker or any unauthorized user will not know the cryptographic key that was used to create the BE template.

Conclusion

Biometric Encryption technology is a fruitful area for research and has become sufficiently mature for broader public policy consideration, prototype development, and consideration of applications.

While introducing biometrics into information systems may result in considerable benefits, it can also introduce many new security and privacy vulnerabilities, risks, and concerns, as discussed above. However, novel Biometric Encryption techniques have been developed that can overcome many, if not most, of those risks and vulnerabilities, resulting in a win-win, positive-sum scenario. One can only hope that the biometric portion of such systems is done well, and preferably not modelled on a zero-sum paradigm, where there must always be a winner and a loser. A positive- sum model, in the form of Biometric Encryption, presents distinct advantages to both security AND privacy.

References

[1] *A Survey on Biometrics based Cryptographic Key Generation Schemes*; Mr.P.Balakumar and Dr.R.Venkatesan, IRACST — International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555, Vol. 2, No. 1, 2012.

[2] *Combining Cryptography with Biometrics for Enhanced Security*; S.P. Venkatachalam, P.M. Kannan and V. Palanisamy, IEEE International Conference on Control, Automation, Communication and Energy Conservation, 2009.

[3] *Biometric Cryptosystems: Issues and Challenges.*; U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain., Proceedings of the IEEE, v. 92, no. 6, June 2004.

[4] *"Biometric Encryption"*; C. Soutar, D. Roberge, A. Stoianov, R. Gilroy and B.V.K. Vijaya Kumar,ICSA Guide to Cryptography, McGrow-Hill, 1999, also available at *http://www.bioscrypt.com/assets/Biometric Encryption.pdf*.