Enhancing Digital Signature Schema Using Fingerprint Minutiae Point and RSA Algorithm

Rima DJELLAB, Aicha ABDENNABI
Departement of Computer Science
University of Batna
Algeria
{rima.djellab, rachidasamia15}@gmail.com

ABSTRACT: *Digital signature method is inspired from the handwriting signature, which must be unique and representative of an individual. The digital signature is a technique that allows identification of a user by relating one entity to one identity. Digital signature has many other applications in security field; including authentication, data integrity, and non-repudiation. The digital signature can be performed using asymmetric algorithm RSA, which is time-consuming. Hence, instead of ciphering all data, a representative data of the initial one is used. The minutiae point is an important feature of a fingerprint image due to the uniqueness characteristic of this descriptive set.*

The intent of this paper is to present an enhanced method for digital signature identification based one RSA and using minutiae point features of fingerprint image.

Keywords: Digital Signature, Fingerprint, Minutiae Point, Authentication, Biometrics

Received: 09 June 2012, Revised 24 July 2012, Accepted 1 August 2012

1. Introduction

Nowadays, Biometric is an important technique used to enhance security of systems where identification and authentication are need. In [7] Biometric refers to the use of distinctive anatomical and behavioral characteristics called biometric identifiers or traits or characteristics for automatically recognizing individuals.

The main advantage of biometric is that every individual has its own physical characteristics that can't be changed, stolen or lost. In fact, the biometrics (physical characteristic) must be:

Universal (every individual has this biometrics); Unique (allowing differentiating an individual from another one); Permanent (that do not change); recordable (with authorization of the individual) and measurable (for further comparison) [6].

Different biometrics can be used to enhance security, such as face; hand geometry; hand/finger vein; iris; signature; voice and fingerprint. This latter is justly a biometric that corresponds to all the previous characteristics, and that was largely used.

Fingerprinting is the oldest biometric technique that has been successfully used in various security applications. It is based on the minutiae points that offer the uniqueness property to a fingerprint and identify an individual. Minutiae points are local ridges characteristics that occur at either a ridge bifurcation or ridge ending [2].

Furthermore, the asymmetric algorithm RSA, known to be a standard, is used to perform signature schema by inverting the role of the public and private keys.

The main idea of the paper is to combine these two techniques to enhance a security system.

The paper is organized as follow: in the section 2 we review the fingerprint technique, and then we introduce the digital signature scheme; followed by an outline of a standard asymmetric algorithm, namely the RSA, used for purpose of signature. In the next section we review the fingerprinting method and its use and finally we present our enhanced schema of digital signature using fingerprint minutiae points and RSA.

2. The Fingerprint

A fingerprint is a set of ridges and valleys of a finger of an individual, where a ridge is a curved segment and the valley is the region limited by two adjacent ridges (see figure 1).

In [5] a fingerprint is defined as a unique pattern of ridges and valleys on the surface of a finger of an individual. Because of the uniqueness and immutability features of this physiological characteristic, the fingerprint is the most biometric parameter used for personnel identification among all the biometrics.

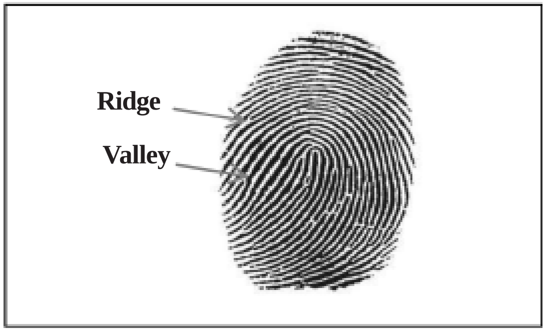


Figure 1. Fingerprint

According to the orientation, and shape of the ridges, we can distinguish five classes of fingerprints, namely: whorl, right loop, left loop, arch, and tender arch (see figure 2).

The local ridge characteristics that occur at either a ridge bifurcation or a ridge ending are the *minutiae* [2]. Francis *Galton* (1822-1922) was the one who observed the structures and permanence of minutiae, therefore, the minutiae points are also called "*Galton details*" [5]. In Table 1 six common types of minutiae points are listed, but there are 150 types of minutiae points that can be seen as combinations of ridge- ending and ridge-bifurcation. Each fingerprint has its set of minutiae points that is determining its uniqueness, and a good quality image has around 40 to 100 minutiae [5].

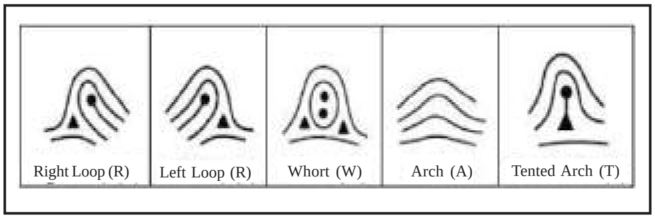


Figure 2. Fingerprint's classification [5]

Nowadays, fingerprint technique is known to be automatic approach named AFRS (**A**utomatic **F**ingerprint **R**ecognition **S**ystem). A fingerprint technique consists of three operations: fingerprint enrollment, verification and identification. In [6] the enrollment is defined as the process that is responsible for registering individuals in biometric system storage. The aim of verification step is to make a one-to-one comparison in order to verify the authenticity of individual. Nevertheless, in the identification step, it is a one-to-many comparison that is performed in order to determine the individual identity.

In both cases, verification and identification, matching techniques are used. The correlation-based, pattern-based and minutiae-based one are the classes of the matching techniques used in most AFRS [5] [7].

The correlation-based matching technique is the one where two fingerprints are superposed and the correlation between corresponding pixels is computed for different alignments [7]. The shortcoming of this technique is that it requires a precise location of a registration point and is affected by image translation and rotation [1].

In the pattern-based, also called Ridge Feature based matching technique; the fingerprint ridge pattern may be extracted more reliably than minutiae whereas this latter can be affected by external factors.

In the minutiae-based technique, first the minutiae points are find, and placed in a two dimensioned plan this constitutes a template. The template will be mapped on fingerprint image in order to find an alignment between them.

The minutiae-based technique is largely used. Two fingerprints match if their minutiae points match. This is verified after extraction phase, the relative placements are then mapped on the finger for matching. The difficulty in this case is the minutiae extraction phase because it is not easy to extract accurately the minutiae point of which the quality depends on the quality of the input fingerprint. Different external factors like scars, sweat, or dirt can alter the minutiae quality.

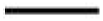
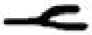
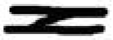
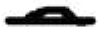
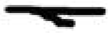
		
Ending	**Bifurcation**	**Crossover**
		
Island	**Lake**	**Spur**

Table 1. Common Types of Minutiae Point

Using fingerprint in automatic way means that the fingerprint image must be treated before extraction of minutiae point. First step is the *binarisation* of the image, then comes *skeletonization*, where the thickness of the ridges is reduced to one pixel, and finally, the extraction of minutiae points, which are either an ending point or a bifurcation (that can form a delta, spur…).

2.1 Characteristics of fingerprint application

In [7] it is précised that it is possible to understand the context of biometrics application by examining a set of characteristics presented as seven dichotomies as follow:

1. Cooperative versus non-cooperative: This characteristic refers to the behavior of the fraud, where in the first case, it is in the interest of the fraud to cooperate with the system to be accepted as valid user, whereas in the second case it is in the interest on the impostor to not cooperate with the system so that this one do not find any matching of the individual in a watch list.

2. Habituated versus non-habituated: This refers to user's interaction frequency with the biometric system.

3. Attended versus non-attended: refers to the human intervention to guide, observe, or supervise the biometric data acquisition.

4. Standard versus non-standard operating environment: refers to whether or not the application is operated in controlled environment (exp: temperature, pressure, moisture, lighting condition…) Night surveillance using biometric system is an example of a controlled environment where lighting conditions are important and must be taken into account.

5. Public versus private: This dichotomy distinguishes between two kinds of users namely customers and employees. Using biometric like fingerprint in conjunction with electronic identity card is an example of public application [7].

6. Open versus closed: refers to whether or not the biometric template is used for a single or multiple application.

7. Overt versus covert: This is in relation with the user's awareness of being or not recognized. Some government and law enforcement applications are covert [7].

2.2 Fingerprint application caterogies

The fingerprint application is increasingly used in many sectors. Three of the most important ones are namely: Forensic; Government (Civil) and Commercial. These three sectors are a part of vertical categorization of the fingerprint applications. Each of these sectors needs a combination of applications to attend their goal. These applications are aggregated according to the required fingerprint features and constitute a horizontal categorization.

Following table resumes these taxonomies.

Forensic	Government (Civil)	Commercial
Corpse identification Crminal investigation Missing children	Social security Welfare disbursement Border control Passport control National ID card Driver license Credentialing	Computer network logon Electronic security E-Commerce Internet access ATM Credit card Physical access control Cellual Phones Personal digital assistant Medical records management Distance learning

Table 2. Vertical and Horizental of Fingerprint Application [7]

3. Digiatl Signature Scheme

Confidentiality, authentication, integrity and non-repudiation, are the main goals in data security context. The encryption process assumes the confidentiality of data so that only authorized entities decipher the data using secured keys. Nevertheless, issues like personification, that could not be avoid only by confidentiality, have to be prevented.

Digital signature is a technique that the aim is to guarantee that an entity can verify the source of a send data and bind an identity to the received data. Hence, the digital signature has to be tied to the data to sign.

The digital signature is inspired from the concept of the handwritten signature. Like the handwritten signature, that is unique and representative of an individual. The digital one is used to identify a unique entity. For K.Sako in [3] "*digital signature schemes are techniques to assure an entity's acknowledgement of having sent a certain message.*" in [1] "*digital signature is defined as data string which associates a message (in digital form) with some originating entity*".

In fact, digital signature scheme consists of a mechanism of generating and integrating a signature, and a verification one. More formally, it is defined in [1] as follows:

- **M** is a set of messages that signer can affix a digital signature;
- **S** is a set of signature;
- $\mathbf{S}_{\mathbf{A}}$ is a signature transformation of the entity **A**. It is a transformation from the set **M** to **S**. $\mathbf{S}_{\mathbf{A}}$ is private to **A**;
- $\mathbf{V}_{\mathbf{A}}$ is a verification transformation of the entity **A** from **M**x**S** to the binary set {true, false}. $\mathbf{V}_{\mathbf{A}}$ is a public transformation;
- $\mathbf{S}_{\mathbf{A}}$ and $\mathbf{V}_{\mathbf{A}}$ form a digital signature scheme for the entity **A**.

Practically, the main idea of digital signature can be performed using a public key cryptography (exp: RSA), where only Alice can signed the message using her private key, and all the other protagonists can verify Alice's signature, since every one of them have access to her public key.

In fact, signature category depends on whether or not the original message is used during the verification step. If the original message is appended to the signature before transmission, the scheme is called signature with appendix (see figure 3). Whereas when the message output by the signature verification, the scheme is called signature with message recovery (see figure 4).

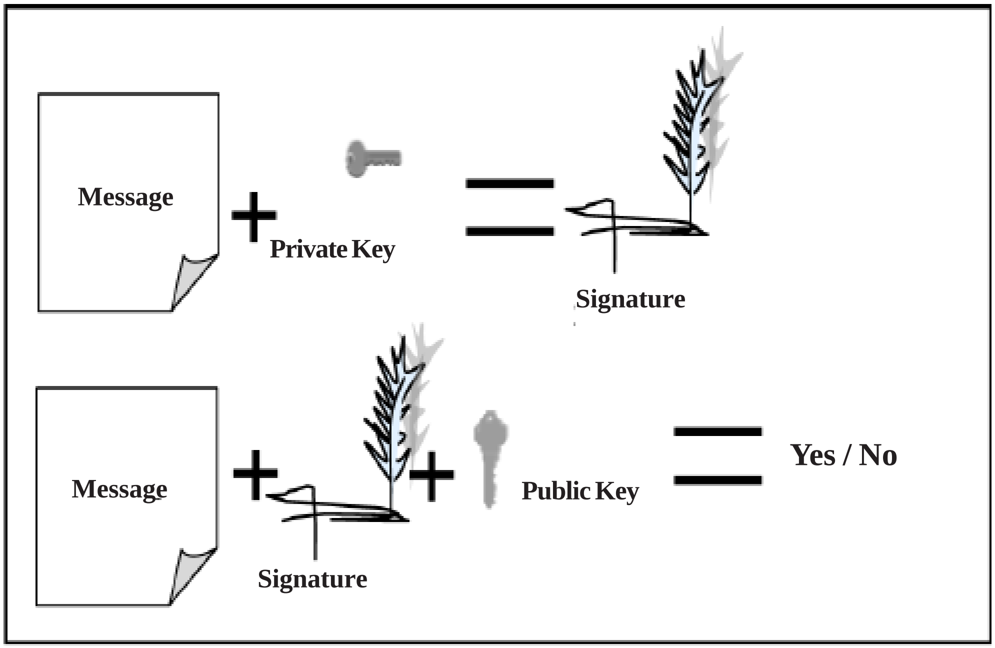


Figure 3. Signature scheme using public key whith Appendix

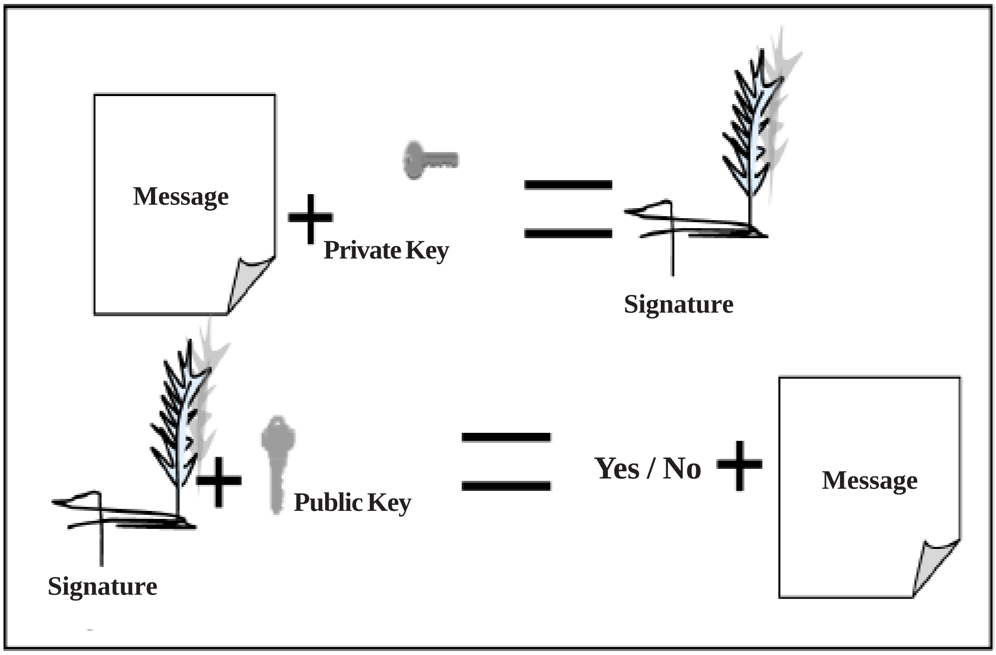


Figure 4. Signature scheme using public key with message recovery

4. Overview of the RSA

Taxonomy, based on cipher's keys, classifies ciphering algorithms into two categories, namely the symmetric and the asymmetric one. When using symmetric algorithm, sender and receiver must share securely same and unique key. The shared key is used either for ciphering and deciphering. When using asymmetric algorithm, a pair of keys is used (public and private keys). Generally, the public key is used for ciphering, and the private one for deciphering.

RSA is known to be a standard asymmetric algorithm. RSA stands for Ron Rivest Adi Shamir and Leonard Adleman, who described in 1978 at the MIT the principle of this asymmetric algorithm.

RSA is based on factorization problem, hence it is based on the difficulty of finding the prime factors of large integers, it is possible to generate a pair of keys to be used for ciphering/deciphering.

The generation of the pair of public and private keys in RSA is as following:

1- Choose randomly two distinct prime numbers and.

2- Compute = 1

3- Compute $\varphi(n) = (p - 1)(q - 1)$ where is Euleur's totient function.

4- Choose e an integer such that $1 < e < \varphi$ and GCD $(e, \varphi) = 1$ where GCD is the Greatest Common Denominator.

5- Determine $d = e^{-1}$ *mod* φ i.e d is the multiplicative inverse of *e mod* φ*.*

The public key is then the modulus n and the *public* exponent e, where the *private* one consists of the modulus ***n*** and the private exponent ***d***. The couple (***n, e***) is diffused to all the correspondents, but the couple (***n, d***) must be kept secret.

Let Alice and Bob be the traditional protagonists who want to exchange secured message ***M***. Alice generates ($\boldsymbol{n, e_{Alice}}$) and ($\boldsymbol{n, d_{Alice}}$) , respectively, the public and the private keys.

Once the keys are generated, the encryption process is as follows:

1- Bob computes $\boldsymbol{C = M^{e}{}_{Alice}}$ ***mo***. ***C*** is the ciphered message;

2- Bob sends C to Alice;

3- Alice computes $M :: C$. Hence she retrieves the message ***M*** from ***C*** using her public key.

Using asymmetric cryptosystem, a signature scheme can be performed by inverting the use of the key the way it was proposed in previous section. However, because the asymmetric cryptosystem are time-consuming, it is possible to use a representative data instead of the entire message. The representative data can be generated using a one way hash function.

A digital signature scheme using asymmetric algorithm and hash function can be performed as follows (see figure 5):

1- Alice calculates the representative data, let's say ***s***, using one way hash function;

2- Alice encrypts s with her private key, let's say that ***s'*** is the result of the encryption process;

3- Alice sends the original message and ***s'*** to Bob;

When receiving the message, Bob calculates the representative data of the original message using the same one way hash function. Let's ***s''*** be the result. Then, Bob compares ***s''*** and ***s'*** that he retrieves using Alice public key. The signature is a valid one, if ***s'*** and ***s''*** are equals.

Indeed, when the private key is used for ciphering, all receivers, by deciphering the data using the copies of the sender's public key that they own, verify that the corresponding private key was used. Hence, the receivers verify the identity of the sender.

This scheme does not assure the confidentiality, but gives a considerable gain in time. Moreover, using asymmetric encryption algorithm, important characteristics are assured [4]:

1- Signature is authentic: when Bob decrypts the received message using the public key of Alice, he verifies that it was Alice who signed it;

2- The signature is unfalsifiable : Because only Alice has the private key;

3- Signature cannot be reused: using encryption algorithm to sign, a message gives a result bind to this message. The signature is a function of the message;

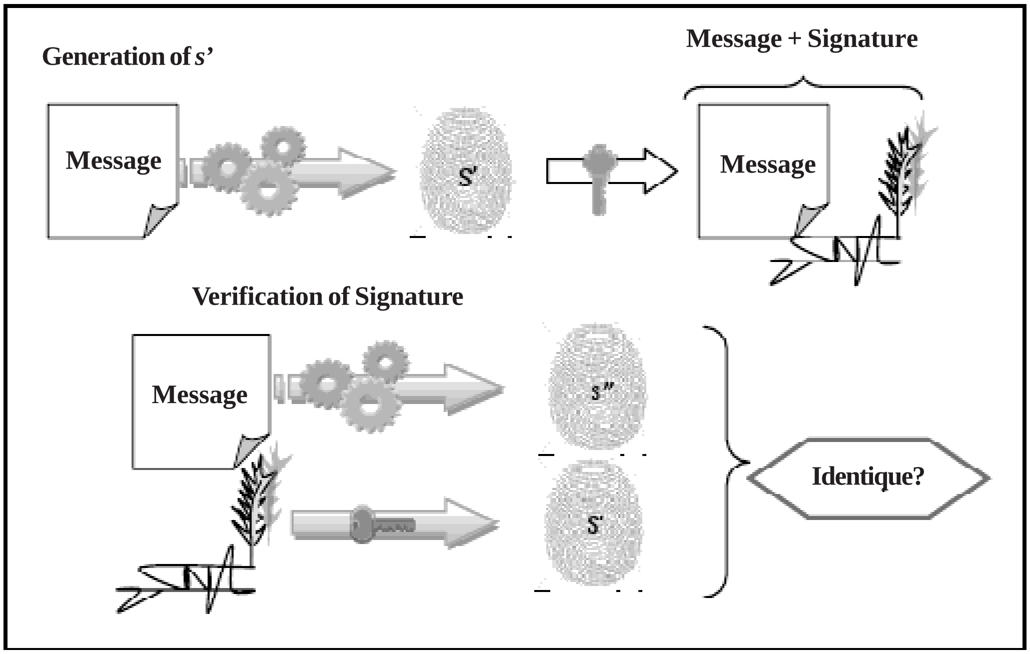


Figure 5. Signature scheme using Hash function and Public key

4- The signed message cannot be distorted. When verify the signature, using the Alice public key, Bob can detect any eventual change.

5- Alice cannot deny her signature.

In order to guarantee the confidentiality, it is possible to enhance the previous scheme. So, instead of encrypting only the representative data ***s'***, the original message and the representative data are encrypted using Alice private key. When receiving the message, Bob will decipher the message using Alice public key, then he proceed to the verification of ***s'*** after calculating ***s''*** using the same one way hash function, in the same way shown previously.

5. Proposed Scheme

We proposed, here, a digital signature scheme with appendix where we introduce the idea of signing message (fingerprint image) using the asymmetric algorithm RSA, and maintaining the idea of using a representative data s. The representative data, s, is the set of minutiae point extracted from the fingerprint image rather than result of one way hash function.

The verification step of the scheme needs the original image of the fingerprint to extract the set of the minutiae points that is why the scheme is considered as a signature scheme with appendix.

Let **A** and **B**, be two legitimates entities which have to exchange a fingerprint, but **B** needs to be sure that the fingerprint comes from **A**. **B** requires an authenticated message from **A**.

Let ***F*** be the fingerprint image, and ***MA*** the minutiae points array.

We assume that the fingerprint image already passes through the *binarisation* and *skeletonization* phases.

The scheme's steps are as follows (see figure 6):

1- **A** and **B** generate and distributed pairs of keys using RSA algorithm, so that K_{prA} **,** K_{pbA} are respectively the private and the public keys of the entity **A** and K_{prB} , K_{pbB} are respectively the private and the public keys of the entity **B**.

2- **A** submits the fingerprint to minutiae point extraction algorithm. The result constitutes the representative data noted ***MA***.

3- **{MA}** K_{prA} **: A** enciphers ***MA*** using its private key K_{prA}.

4- The message {F+{MA} K_{prA} } is then enciphered using the public key of **B**, K_{pbB}

When receiving the message { F + {MA} K_{prA} } K_{pbB} the entity **B** deciphers the message using its private key K_{prB}. **B** is the only one to decipher the message, because it is the only one to have the corresponding private key.

B submits **F** to the same minutiae point extraction algorithm used by **A** and extracts **MA'** a minutiae point set that will be compared to **MA** after its extraction from the message received from **A** using K_{pbA}.

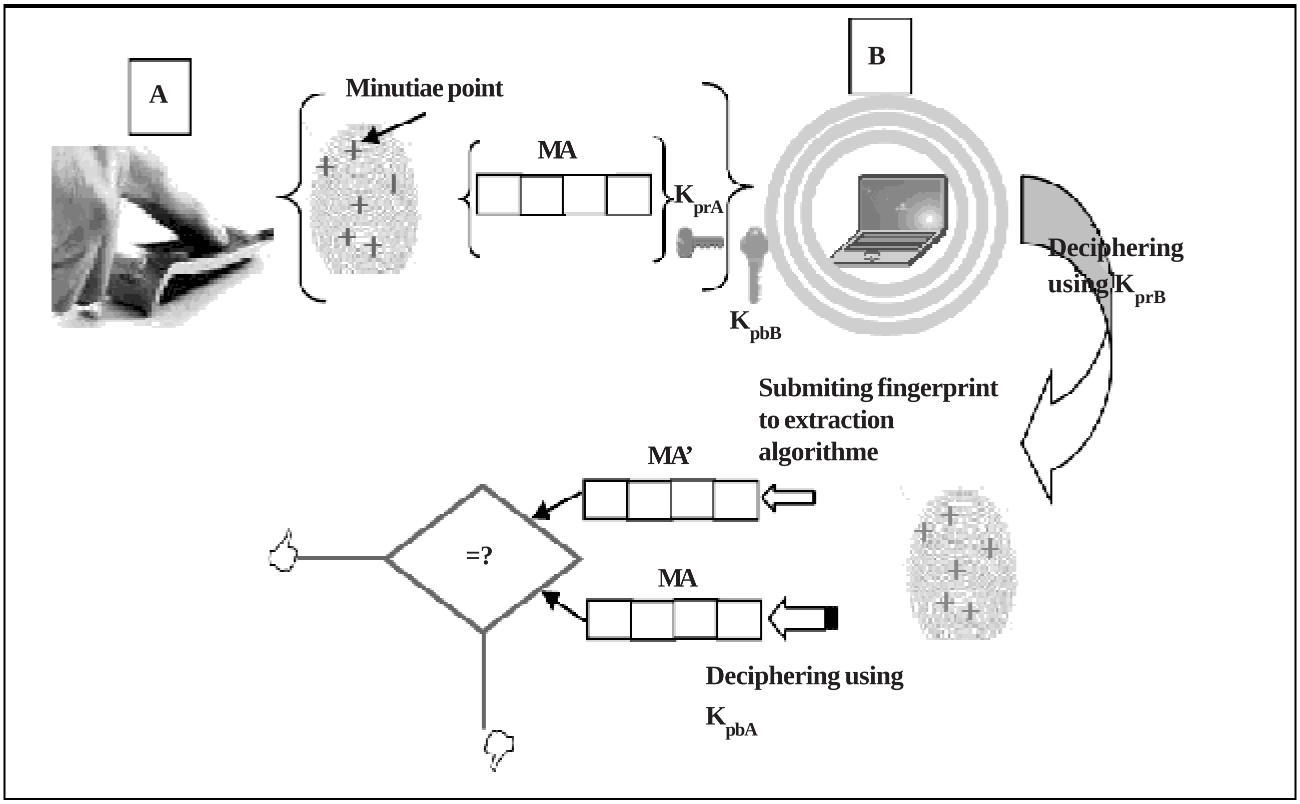

A
Minutiae point
MA
K_{prA}
B
Deciphering using K_{prB}
K_{pbB}
Submiting fingerprint to extraction algorithme
MA'
=?
MA
Deciphering using K_{pbA}

Figure 6. Proposed Schema

5.1 Scheme Analysis

The main idea proposed in this paper is to introduce the use of the minutiae points to perform a digital signature of a fingerprint image. The use of minutiae points is justified by the fact that fingerprint is unique for each person and each fingerprint has its characterized set of minutiae that makes it different from another fingerprint. Hence, the set of minutiae is considered as representative data of fingerprint image.

The scheme is also based on the use of the RSA to perform a signature by inverting the use of public and private keys in step 3 of the proposed scheme, so that the set of the minutiae cannot be retrieved if it is not K_{pbA} which is used to decipher the received message at **B**.

Therefore, the proposed digital signature scheme is an enhancement of the known one using RSA, which is time- consuming if usually used. The use of minutiae improves the traditional scheme by its uniqueness. Indeed, when using a representative and unique data as signature, an adversary can't personify an entity, because he do not ever has the initial image (fingerprint) to extract the features that is used as signature. Moreover, he do not have the private key used to encipher the fingerprint image and its corresponding minutiae set which is already encrypted by another private key that the eavesdropper do not ever have.

Characteristics			
Cooperative	x	Non-cooperative	
Habituated	x	Non-habituated	
Attended	x	Non-attended	
Standard enviroment	x	Non-standard	
Public		Private	x
Open		Closed	x
Overt	x	Covert	

Table 3. Characteristic of Corresponding Application Matching Which the Proposed Schema

According to the characteristics defined previously, the proposed scheme can be used in an application matching to the following context's characteristic:

Consequently, the proposed scheme draws its strength from combining two important techniques, namely the signature using asymmetric algorithm, precisely the RSA, and the fingerprint minutiae point.

6. Conclusion

Our society becomes more and more electronic; many daily used applications need a height level security. Security is starting by authentication of the individual and identification, to preserve privacy and confidentiality of corresponding data.

Consequently, data security is not only based on confidentiality using ciphering algorithm,other issues must be taken into account. Digital signature algorithm assures the authentication which is an important goal of security. In this paper we overviewed the traditional signature scheme using RSA algorithm, as well as one of the most important biometric technique used for identification; namely the fingerprinting. This latter covered a large scale of applications ranging from forensics to mobile phones.

We present, here, an enhanced signature scheme based on the fusion of the RSA and the minutiae points extracted from the fingerprint image.

The strength of the proposed scheme is based on the uniqueness of the set of the minutiae points extracted from the fingerprint image, and which constitute the signature. The signature is ciphered using RSA which is one of the most important and powerful asymmetric algorithm.

Referenses

[1] Vacca, J. (2007). Biometric technologies and verification systems, Elsevier.

[2] Henk, C. A., Tilborg, V. (1996). Encyclopedia of cryptography and security, Springer.

[3] Menzer, A. J., Van Oorschot, P. C., Vanstone, S. A. (1996). Handbook of Applied Cryptography, CRC Press, August.

[4] Schnieder, B. (1996). La cryptographie Appliquée, International Thomson publishing, NY.

[5] Bansal, R., Sehgal, P., Bedi, P. (2011). Minutiae extraction from fingerprint images - a Review, *International Journal of Computer Science*., 8 (5) 74–85, September.

[6] Bao, LE Duc. (2011). Authentification des empreintes digitales dans un système BioPKI, Institut de la Francophonie pour l'Informatique, Janvier.

[7] Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S. (2009). Handbook of fingerprint recognition, Springer-Verlag, London.

[8] Smart, N. Cryptography: An introduction, 3rd Edition, available on: http://www.cs.bris.ac.uk/~nigel/Crypto_Book/