2011 International Conference on Information and Network Technology
IPCSIT vol.4 (2011) © (2011)IACSIT Press, Singapore

Stegano-CryptoSystem for Enhancing Biometric-Feature Security with RSA

Pravin M.Sonsare[1], Shubhangi Sapkal[2]

[1,2]Department of Computer Science, Government College Of Engineering, Aurangabad

Abstract. Biometric is method of identifying a person or verifying the identity of a person based on physiological or behavioral characteristics.RSA is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. Biometric template may be modified by attacker. To deal with this issue RSA cryptography can be used to secure Biometric Template. Cryptography and steganography provides great means for helping such security needs as well as extra layer of authentication.

Keyword: Biometric, Cryptography, RSA, Steganography, public-key cryptography.

1. Introduction

Biometrics is the science of establishing or determining an identity based on the physiological or behavioral traits of an individual. These traits include fingerprints, facial features, iris, hand geometry, voice, signature, etc. In conjunction with traditional authentication schemes, biometrics is a potent tool for establishing identity [1].

Traditional token-based or knowledge-based personal identification techniques are unable to differentiate between an authorized person and an impostor who fraudulently acquires the access privilege of an authorized person. Biometrics technology is based on using physiological or behavioral characteristics in personal identification, and can easily differentiate between an authorized person and a fraudulent impostor .While the biometrics techniques offer a reliable method for personal identification, the problem of security and integrity of the biometrics data poses new issues. For example, if a person's biometric data (e.g., his/her fingerprint image or fingerprint features) is stolen, it is not possible to replace it as compared to replacing a stolen credit card, ID or password [2].

To increase security of the biometric data, technique such as encryption, steganography and watermarking are used. Cryptographic approach attempts to make the biometric information meaningless to attackers. Steganography pertain to the area of data hiding, which aims at private information protection by hiding critical information in unsuspected carrier signal. Steganography is a useful tool that allows covert transmission of information over an overt communications channel. The hidden data is both difficult to detect and when combined with known encryption algorithms, equally difficult to decipher.

In this paper, we discuss biometric module, various attacks and related work regarding security of biometric data. Section 1 briefly introduces biometrics, steganography and cryptography. Section 2 presents biometric module, various attack and related work. RSA and steganography reported in Section 3.Proposed system presents in Section 4 and concluding remarks is given in the Section 5.

[+]Corresponding author. Tel.: + (91-9970083800)
E-mail address: (sonsare@gmail.com)

2. Biometric Modules and Related Work

A typical biometric system comprises of several modules. The sensor module acquires the raw biometric data of an individual in the form of an image, video, audio or some other signal. The feature extraction module operates on the biometric signal and extracts a salient set of features to represent the signal; during user enrolment the extracted feature set, labeled with the user's identity, is stored in the biometric system and is known as a template. The matching module compares the feature set extracted during authentication with the enrolled template(s) and generates match scores. The decision module processes these match scores in order to either determine or verify the identity of an individual. Thus, a biometric system may be viewed as a pattern recognition system whose function is to classify a biometric signal into one of several identities (viz., identification) or into one of two classes - genuine and impostor users (viz., verification)[1].While a biometric system can enhance user convenience and bolster security, it is also susceptible to various types of threats as discussed below [3,4].

1. Circumvention: An intruder may gain access to the system protected by biometrics and peruse sensitive data such as medical records pertaining to a legitimately enrolled user. Besides violating the privacy of the enrolled user, the impostor can also modify sensitive data.

2. Repudiation: A legitimate user may access the facilities offered by an application and then claim that an intruder had circumvented the system. A bank clerk, for example, may modify the financial records of a customer and then deny responsibility by claiming that an intruder could have possibly stolen her biometric data.

3. Covert acquisition: An intruder may surreptitiously obtain the raw biometric data of a user to access the system. For example, the latent fingerprints of a user may be lifted from an object by an intruder and later used to construct a digital or physical artifact of that user's finger.

4. Collusion: An individual with wide super-user privileges (such as an administrator) may deliberately modify system parameters to permit incursions by an intruder.

5. Coercion: An impostor may force a legitimate user (e.g., at gunpoint) to grant him access to the system.

6. Denial of Service (DoS): An attacker may overwhelm the system resources to the point where legitimate users desiring access will be refused service. For example, a server that processes access requests can be flooded with a large number of bogus requests, thereby overloading its computational resources and preventing valid requests from being processed.

In the first type of attack, a fake biometric (such as a fake finger) is presented at the sensor. Resubmission of digitally stored biometric data constitutes the second type of attack. In the third type of attack, the feature detector could be forced to produce feature values chosen by the attacker, instead of the actual values generated from the data obtained from the sensor. In the fourth type of attack, the features extracted using the data obtained from the sensor is replaced with a synthetic feature set. In the fifth type of attack, the matcher component could be attacked to produce high or low matching scores, regardless of the input feature set. Attack on the templates stored in databases is the sixth type of attack. In the seventh type of attack, the channel between the database and matcher could be compromised to alter transferred template information. The final type of attack includes altering the matching result itself. All of these attacks have the possibility to decrease the credibility of a biometric system [5][6].

In the past few years, several researchers have made attempts on biometric data protection with the help of data hiding techniques and cryptography technique. Digital Watermarking provide Embedding information of multimedia data (e.g., image, video, audio, etc.) in the host data. Fragile Watermarking provide fingerprint image tampering detection. .Chaotic Watermarking is done by mixing the watermark to a random-textured pattern. Amplitude Modulation base Watermarking Include image adaptively, minutiae analysis, watermark strength controller along with basic method. Wavelet-based Watermarking method embeds the watermark in the coefficients of the discrete wavelet transform (DWT) using quantization-based watermarking. DWT and SVM

Watermarking enhance the quality of extracted face image. Steganography hide critical information in unsuspected carrier data.

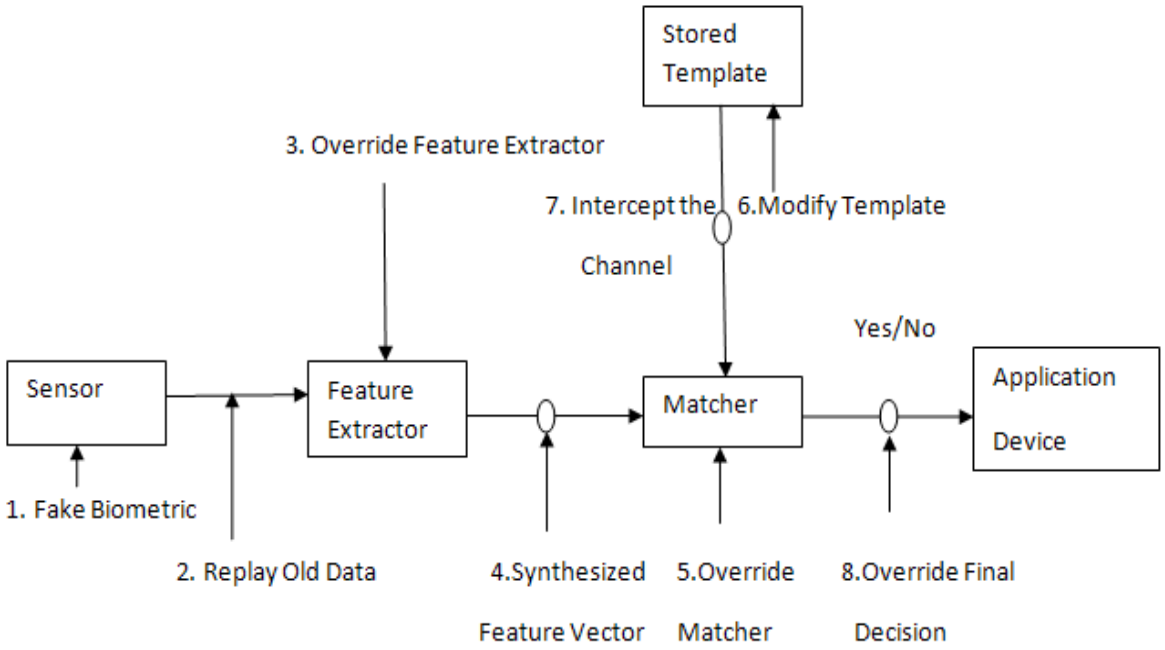

Fig1: Biometric System With attacks (adapted from [1])

3. Approaches

3.1. RSA

RSA is public key algorithm invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman (RSA) which supports Encryption and Digital Signatures.It is most widely used public key algorithm and gets its security from integer factorization problem. It is relatively easy to understand and implement. RSA is used in security protocols such as IP data security, transport data security, email security, terminal connection security and many more. RSA use two different keys with a mathematical relationship to each other. Their protection relies on the premise that knowing one key will not help you figure out the other. The RSA algorithm uses the fact that it's easy to multiply two large prime numbers together and get a product. But you can't take that product and reasonably guess the two original numbers, or guess one of the original primes if only the other is known. The public key and private keys are carefully generated using the RSA algorithm; they can be used to encrypt information.

3.2. Steganography

Steganography is art of hiding information inside information. It is used for hiding the fact that you are sending, hiding several messages inside data, digital watermarking. It considers security with knowledge of the system and message can only be read with secret key. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden.

4. Proposed Model

To solve the issue of biometric security we proposed following system consist of six module that is RSA encryption, hiding module, detection module, extraction module,RSA decrytion,decision module. Biometric image is captured from the sensor and image processing algorithms are performed to extract the features. These data are unique for different person and converted into a binary stream to generate the biometric code [7].

4.1. RSA Encryption

In this module we encode biometric code by making a public key, and use that key to send a message. For that one person selects two prime number say p and q.One person multiplies two numbers and get pq which is the public key. Person also chooses another number e which must be relatively prime to (p −1) (q – 1). e is also part of the public key, so another person also is told the value of e. Now another person knows enough to encode a message, suppose the message is the number M. Another person calculates the value of $C = M^e \pmod N$ where N=pq which is the encoding number that is to be send.

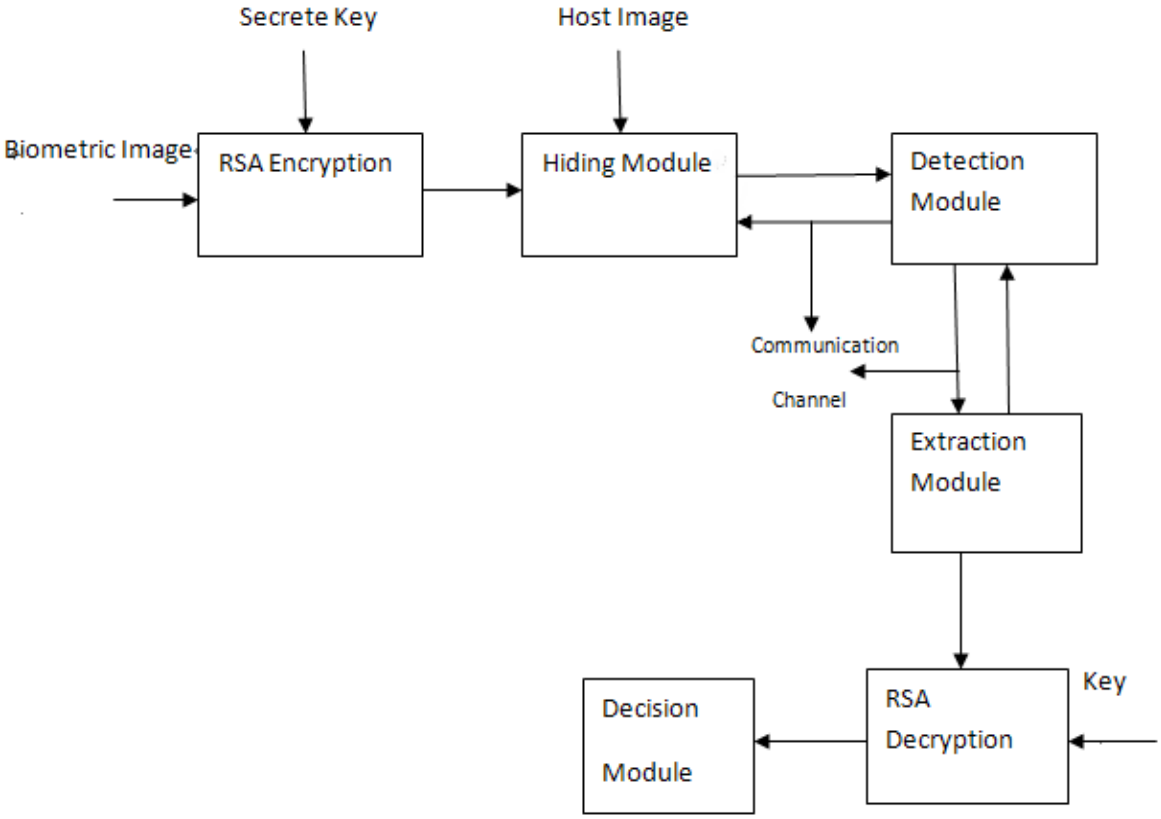

Fig2: Stegano-Crypto system

4.2. Hiding Module

In this module, to hide the biometric code we use discrete cosine transformations (DCT) and transform pixel blocks to DCT coefficients. To identify redundant data get least significant bit of each DCT coefficient. Replace LSB with secret message bit and insert modified DCT into output image.JPEG stegencryption operates in transformation space and subject to no visual changes.GIF and BMP stegencryption operates in low bit planes subject to visual attacks.

4.3. Detection Module

In this module, verify whether secrete information properly hidden or not. It is verified by examining color palette and size of the image. Hidden information is detected by analyzing frequency of DCT coefficient. Hidden content has higher entropy.

4.4. Extraction Module

In this module, for visible representation of statistical data filters are applied to steganograms. To prevent loss of generality, we consider modified 2D Gabor filter. There are many algorithms to extract biometric feature in literature [8].

4.5. RSA Decryption

Now in this module we want to decode biometric code. To do so, we needs to find a number d such that $ed = 1\ mod((p-1)(q-1))$ .Calculate C^d (mod N) where N=pq such that calculated value is original biometric code.

4.6. Decision Module

The decision module processes decrypted biometric code in order to either determine or verify the identity of an individual. Thus, a biometric system may be viewed as a pattern recognition system whose function is to classify a biometric signal into identification or into verification [1].

5. Conclusion

This paper presented crypto graphical approach with steganography to protect biometric template from different attack. In this approach we use same key for encryption and decryption. This approach provide digital signature that cannot be repudiated. This approach not protects the biometric message but also protect the communication parties.

6. References

[1] A. K. Jain, A. Ross, and U. Uludag, "Biometric template security: challenges and solutions," Proc. of the European Signal Processing Conference (EUSIPCO '05), Sep.2005

[2] A.K.Jain, U.Uludag, and R.K.Hsu, “Hiding a face in a fingerprint image,” Proc. of Intl Conf. on Pattern Recognition, vol.3, pp. 756-759,Aug. 2002.

[3] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. Springer-Verlag, 2003

[4] U. Uludag and A. K. Jain, “Attacks on biometric systems: a case study in fingerprints,” in Proc. SPIE, Security, Steganography and Watermarking of Multimedia Contents VI, vol. 5306, pp. 622–633, (San Jose, CA), January 2004.

[5] A.K.Jain and U.Uludag, “Hiding biometric data,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 25, no. 11, pp. 1494-1498, Nov.2003

[6] N.K. Ratha, J.H. Connell, and R.M. Bolle, “An Analysis of Minutiae Matching Strength,” Proc. Third Int’l. Conf. Audio- and Video-Based Biometric Person Authentication, pp. 223-228, June 2001

[7] Wang Na, Zhang Chiya, Li Xia, Wang Yunjin,”Enhancing Iris-feature Security with steganography”, 2010

[8] J. Daugman. “High Confidence Visual Recognition of Persons by a Test of Statistical Independence”, IEEE Tans. Pattern Analysis and Machine Intelligence, vol.15, pp.1148-1161, 1993.