A New Special Biometric Identity Based Signature Scheme

Xiaodong Liu, Quan Miao, Daxing Li
Institute of Network Security, Shandong University,
Jinan 250100 Shandong, China
liuxiaodong@sdu.edu.cn

Abstract

We propose a new special identity based signature scheme that make uses of fractal transform and entropy arrangement algorithm to generate the public key string from a biometric measurement of signer. A biometric reading provided by the alleged signer would be enough to verify the signature. The characteristic of this scheme is that When verifier finished the verification on the signature, he can compare the biometric information reconstructed by public key with that provided by signer to ensure the relationship between the public key and signer. So, this makes the verification more convenient and intuitionistic. Finally, we describe two possible attacks on this system and suggest ways to combat it.

1. Introduction

Identity based signature scheme [1] is based on a public key cryptosystem with extra twist: Instead of generating a random pair of public/private keys, the user chooses his name and network address as his public key. Any combination of name, social security number, telephone number and street address can be used provided that it uniquely identifies the user in a way he cannot later deny, and that it is readily available to the other party. The corresponding private key is computed by a key generation center (KGC) and issued to the user in a secure way.

Recently, a biometric identity based signature scheme (BIO-IBS) [2] is proposed by Burnett, Duffy and Dowling. In scheme [2], they have used a biometric measurement of an individual instead of very long integers, typically 2048 bits, to construct the public key. They have shown us how to use a hash function to make the biometric embedded onto a point on the elliptic curve and how to make the point as part of the key pair generation for a signature scheme.

Obviously, in scheme [2], the public key generation is a one way procedure, that is, the biometric data cannot be reconstructed from the public key data. Consider the following situation: the signer comes to see the verifier with the contract he signed. The verifier has verified the signature of the contract using public key of signer successfully. But how to confirm the signer is the very one who has signed the contract if the verifier had never known the signer. So, if the verifier can reconstruct the biometric such as fingerprints from the public key, he would ask the signer to provide his fingerprints on the spot and make a matching easily and conveniently.

In this paper we present a biometric identity based signature scheme and the scheme is particularly useful in this area as biometric measurements such as fingerprints are long established evidential tools [3]. In our case, we use a biometric measurement of an individual to construct the public key. Using biometrics does however create a problem that how to turn biometrics data into public key strings. We present two steps to overcome this problem. Step 1, compress the biometrics data such as fingerprints image using fractal transform. Step 2,

turn the biometrics data compressed into public key strings using entropy arrangement algorithm.

The paper is organized as follows. In section 2 we briefly outline the basics of fractal transform and entropy concept. In section 3, we describe the coding process of turning biometric data into key strings making use of fractal transform and entropy arrangement algorithm. Section 4 will give an overview of Shamir scheme [1] using the key pair generated from the biometric data. Section 5 outlines two possible attacks on the system and suggests countermeasures. Finally, we will discuss conclusions.

2. Basics of fractal transform and entropy concept

Some special fractal can be raised from both Computer Graphics and Maths Construction. The simplest one is called as self-similarity set. In 1981, J. E. Hutchinson introduced the theory of the Iterated Function Systems, abbreviated as IFS in [4]. He used the compression transform in metric space as model of dynamical system and applied the idea of IFS to image compression. IFS plays the leading role during the development of fractal image compression. Most of the fractal image compression jobs are based on IFS or its extension.

For some images, fractal compression arithmetic has more tremendous compression ratio than other traditional image compression algorithms, such as DCT, Wavelet and so on. And such images (such as fingerprint image) have the following features, i.e. they contain a lot of regular veins information.

The theory basis of fractal image compression coding consists of the following four parts: the iterated function system, the fixed-points theorem, the college theorem and affine transform, while the iterated function system forms the basic theory .of fractal image compression coding. See [4,5,10] for more details.

The entropy concept was proposed by Shannon [6]. He used H(X) to present the entropy of a gray image:

$$H(X) = -\sum_{i=0}^{255} p(i) \log_2 p(i), \qquad (1)$$

where

- i is the grey level of pixel, which a value is between 0 and 255
- $p(i)$ is the relative frequency of grey level i that occurs in the image

It's easy to know the entropy of a image is 0 if the image consists of a single grey level, i.e. it is an invariant image. That is, the more "orderly" the content of a group information (image) is, the less the amount of information it contains.

3. Generating public key data from biometrics

First, we define f is the fingerprint image, R_k is the sub block, typically 4×4pixels, D_j is the parent block, typically 8×8pixels and w_i is the fractal compression transform.

The below is the coding procedure: Divide f into sub block set $R_1, R_2, ..., R_n$. For each sub block R_k, find the parent block $D_j \in f$, and transform w_i to make certain sub block R_k can be equal or close to certain parent block D_j extremely under the transform w_i. Then this parent block D_j can be replaced by the sub block R_k after transform w_i. It must be ensured that Transform w_i is compressed. Thus the coding is finished. Because we only need store the

factor of w_i, the position of D_j and the transform information from D_j to R_k, this information is less than information of original image greatly, thus we reach the purpose of compression.

With a large amount of experiments, we find that the lower the entropy [6] of a sub block R_k is, the easier it is to find a match parent block D_j for the sub block as the percentage of this section is larger in the image. This supplies us the evidence for improving compression algorithm further.

Here is the coding procedure improved with entropy arrangement algorithm: First, we calculate the entropy $Entropy_k$ of every sub block R_k and sort them. Next, use it to match parent block D_j by the entropy from low to high. According to the structure features of images, it's easy to know if a sub block R_k with a lower entropy $Entropy_k$, there are more parent block D_j matched with it, and the number of the parent blocks D_j matched will reduce with the entropy $Entropy_k$ of the sub block R_k is larger and larger.

It is obvious that, the coding speed of fractal transform can be raised remarkably by improvement of entropy arrangement algorithm. And we can set a threshold *K*, make $n \le K$, *n* is the number of sub block need to match parent blocks. Thus, with a certain threshold *K* we have chosen, it was easy to make the size of the compressed image to adapt to the public key's size that required by KGC.

A typical fingerprint image, in black-white, 128×128 pixels, is about 2.3K bytes in size. Experiments have shown, with the improved algorithm above, the coding time is about twenty times faster than traditional fractal transform and image compression ratio is about 21.0 with almost the same PSNR [5].

So, according to the coding procedure, we can generate a public key from biometrics and obviously, it is easy to reconstruct the biometrics from the public key.

4. Incorporating into an identity based signature scheme

An overview of an identity based signature scheme is given in this section. This scheme was proposed by Shamir [1] and consists of three stages.

The first stage is the System Parameter Generation stage. *n* is the product of two large primes, *e* is a integer and $\gcd(e, \varphi(n)) = 1$, *d* is a integer and $ed = 1 (\mathrm{mod}\, \varphi(n))$, $h : \{0,1\}^* \to Z_{\varphi(n)}$ is a Hash function. And *d* is the secret key of KGC. The parameters *n*, *e* and the function *h* are chosen by KGC and they can be made public. Assume *ID*, that is the biometrics such as fingerprints, is the unique identity of a user, and the corresponding private key *g* generated by KGC is

$$g = ID^d (\mathrm{mod}\, n) \qquad (2)$$

The second stage is the signing stage. To sign message $m \in \{0,1\}^*$, the signer chooses a random number *r* and computes

$$t = r^e (\mathrm{mod}\, n) \qquad (3)$$

$$s = g r^{h(t\|m)} (\mathrm{mod}\, n) \qquad (4)$$

And (*t, s*) is the signature.

The third stage is the verification stage. The signature scheme is based on the verification condition:

$$S^e = ID \cdot t^{h(t\|m)} (\mathrm{mod}\, n) \qquad (5)$$

Where

- m is the message
- t, s is the signature
- ID is the user's identity
- n is the product of two large primes
- e is a large prime which is relatively prime to $\varphi(n)$.

f is a Hash function.

5. Two possible attacks

Here we describe two possible attacks to the scheme and identify ways of preventing it.

A. it is possible for an attacker to obtain a copy of the signer's biometric data. Then he can send the data as his own to KGC and acquire the corresponding private key as the same as the signer's. That is, the attacker has obtained the private key of the signer and could imitated signer to sign some contracts or documents.

To prevent this attack, we suggest that in key generating stage, user must have provided his biometric data on the spot in KGC with a trusted witness in presence. Then KGC turns the biometric data into public key string using compression algorithm proposed in this scheme, assures that the public key is unique in the system and issues the public/private key pairs to user in a secure way.

B. If biometric data such as fingerprints of an attacker is extremely similar with the signer's, attacker could come to see the verifier with a contract signed by signer and claim that he is the very one who had signed the contract. To prove it, he could provide his fingerprints data on the spot. It is very difficult for verifier to distinguish the two extremely similar fingerprints image. So, the verifier maybe has trusted the attacker.

To prevent this attack, contract can be signed in the presence of a trusted witness. If there is a legal dispute over whether a contract had been signed or not by a user later, the witness could come to assert which one is the genuine signer. Alternatively, signers also can utilize a digital certificate obtained from a trusted certificate authority. The digital certificate will contain the public key and some other information such as social security number about the signer.

6. Conclusion

We have presented a biometric identity based signature scheme and described how to turn the biometric data of an individual into the public key string. We have suggested countermeasures for two possible attacks on the system. Contrasted with Burnett Scheme [2], our scheme has an advantage that the biometric data could be reconstructed from the public key. Thus in our scheme, it is more visible and convenient for the verifier to finish a verification. And amounts of experiments have shown us, our scheme could satisfy the practical applies.

7. References

[1] A. Shamir, “Identity-based Cryptosystems and Signature Schemes”, Advances in Cryptology-Crypto'84, LNCS 196, Springer-Verlag, 1985, pp. 47-53.

[2] Burnett A, Duffy A, Dowling T, “A biometric identity based signature scheme”. http://eprint.iacr.org/2004/176

[3] D. Maltoni, D.Maio, A.Jain, and S. Prabhakar, “Handbook of Fingerprint Recognition”. Springer, 2003

[4] J.Huchinson, “Fractals and Self Similarity, indiana Univ”. Math.J.30.1980

[5] M. F. Barnsley, A. D. Sloan, “A Better Way to Compress Image Byte”, Jan, 1988

[6] Shannon, C. E., “A Mathematical Theory of Communication”, Bell Syst. Tech. J., 27, 1948

[7] K.G. Paterson, “ID-based Signatures from Pairings on Elliptic Curves”, IEEE Communications Letters, Vol.38, No.18, 2002, pp. 1025-1026.

[8] Paterson. K. G “ID-based signatures from pairings on elliptic curves”, Electronic Letters, 2002, 38(12): 1025-1026

[9] Zhang F, Safavi-Naini R, Susilo W. “Attack on Han et al.’s ID-based confirmer(undeniable) signature” at ACM-EC’03, 2003,http://eprint.iacr.org/- 2003/129

[10] I. H. Witten, R. Neal, J. G. Cleary, “Arithmetic coding for data compression”, Comm, ACM, Vol 30, pp 520-540, June 1987.

[11] Chow. S, Hui L, Yiu. S et al. “A secure modified id-based undeniable signature scheme based on Han et al.’s Scheme againse Zhang et al.’s Attacks”. http://eprint.iacr.org/2003/262

[12] Harn. L, Yang. S. “ID-based cryptographic scheme for user identification, digital signature, and key distribution” , IEEE Journal on selected areas in communications, 1993, 11(5): 757-760

[13] Laih. C, Lee. J, Harn. L et al. “A new scheme for ID-based cryptosystemand signature”. //INFOCOM’89. Proceedings of the Eighth Annual Joint Conference of the IEEE Computer and Communications Societies. Technology: Emerging or Converging IEEE 23-27, Apr 1989, 3:998-1002

[14] Fiat. A, Shamir. A. “How to prove yourself: Practical solutions to identifiCation and signature problems”, // Advances in Cryptology-CRYPTO’86, LNCS 263. Berlin: Springer-Verlag, 1986.

[15] Ohta. K, Okamoto. E, “Practical extension of Fiat-Shamir scheme”. Electr. Lett. 1988, 24(15): 955-956

Authors

Xiaodong Liu received the M.E. degree in Computer Science, Shandong University in 2001. He is currently D.S. in Network Security form Shandong University, Jinan, Shandong, China. His main research work include computer system security, network security, and cryptography.

Quan Miao received the M.E. degree in Computer Science, Xian Institute of Post and Telecommunications in 1998. He is currently D.S. in Network Security form Shandong University, Jinan, Shandong, China. His main research work include computer system security, network security, and cryptography.

Daxing Li received the D.E. degree in mathematics, Shandong University in 1989. He works as professor, and currently the leader in Network Security institute of Shandong University, Jinan, Shandong, China. His main research work include computer system security, network security, and cryptography.