A PUBLIC KEY SIGNATURE FOR AUTHENTICATION IN TELEPHONE CONVERSATION

Suhono H. Sugangkat1, Theodorus Eric2, and Agus S. Fannuji3

ABSTRACT

This paper presents an authentication method for telephone signal using public key signature. Analog telephone signal needs special signature which is robust to noise and other disturbances in telephone line. The signature is generated from some part of telephone signal using robust Hash function. The Hash function works by projecting some parts of the telephone signal to N patterns of pseudo noise to produce hash bit. The output of the Hash function is encrypted using RSA as the signature and then inserted into some other part of telephone signal as watermark using spread spectrum modulation without disturbing the conversation. This paper also discusses the possibility of producing false telephone conversation and the robustness of the signature.

INTRODUCTION

Authentication in the telephone can be performed using caller ID system. This system sends additional information such as the name of the addressee of the caller before the conversation begins [1]. This method is not secure because telephone lines are easy to be tapped and it's possible for someone to change the caller ID information. In order to be more secure, it’s better to send content based signature that is related to the message, in this case the telephone signal, as in the digital signature technique[2].

Digital signature technique using Hash function can be applied directly to the telephone signal due to the nature of the analog telephone signal which sometimes has some disturbances. Standard Hash function such as MD5 and SHA-1 can not be applied to telephone signal because the output changes dramatically with little change in input [3]. The Hash function for telephone signal needs to produce the same output for the signal with some disturbances, but produces different output for different signal. It is necessary to find an appropriate Hash function to generate signature for telephone signal.

In this paper, a method to calculate robust Hash function and insert robust signature into telephone signal is presented for authentication using public key system.

SYSTEM OVERVIEW

The signature for the authentication is generated from some part of telephone signal using special Hash function and then encrypted using public key system (RSA) as the signature. The signature is then inserted into another part of telephone signal using watermarking technique.

This authentication process works similar to digital signature method using Hash function but has some differences especially in calculating the Hash function and sending the signature.

In the digital signature using Hash function (example for email), the whole message will be used to generate the signature. In the application for telephone, the user wants that the authentication can be performed soon without having to wait until the conversation ends. For this purpose, the telephone signal is divided into several blocks and the signatures are inserted for each block using watermarking technique without disturbing the conversation.

Figure 1 shows a situation in which a person A sends signature to person B. Later person B will extract the signature and verify whether the call comes from person A. If person A wants to be sure that the person speaking is really person B, then person B can also send her signature.

Figure 1. Authentication system for telephone

SIGNATURE FOR TELEPHONE SIGNAL

The process is the sender consists of three steps, calculating the Hash function, encrypting the output from the Hash function, and then inserting the

1 Suhono H. Sugangkat, Department of Electrical Engineering, Bandung Institute of Technology, Jl. Ganesha 10 Bandung, Indonesia 40174 Phone: +62-22-2534282, Fax: +62-22-2500855; Email: suhono@iai-bkt.ac.id
2 Theodorus Eric, Department of Electrical Engineering, Bandung Institute of Technology, Jl. Ganesha 10 Bandung, Indonesia 40174 Phone: +62-22-2534238, Fax: +62-22-2500855; Email: eric@ielkemen.com
3 Agus S. Fannuji, Department of Electrical Engineering, Bandung Institute of Technology, Jl. Ganesha 10 Bandung, Indonesia 40174 Phone: +62-22-2534238, Fax: +62-22-2500855; Email: agusf@ielkemen.net

MEDIA TEKNIK No.2 Tahun XXVIII Edisi Mei 2006 No.ISBN 0216-3012 19
signature as watermark into the telephone signal. The analog telephone signal is converted to digital using ADC (Analog to Digital Converter) before the process. Figure 2 shows the process that occurs in this system when a person A sends signature.

![Figure 2. Signature generation and insertion](image)

As shown in the figure above, the telephone signal is divided into several blocks: block 1, block 2, block 3, and so on. Every block of signal is divided into two parts, left part BL and right part BR. The right part BR is used as the input to the Hash function to generate the signature. The signature will be inserted to the left part BL as watermark.

**Robust Hash Function for Telephone Signal**

The Hash function works by projecting telephone signal to N pseudo noise patterns $PH_i$, $1 \leq i \leq N$. This technique was originally used to calculate Hash function for digital image [4], but with some modifications, it can also be applied for telephone signal. This method is well suited for the telephone signal because it is robust to some disturbances such as noise, scaling, or random deletion.

Pseudo noise generator (PNG) uses time as the key to generate $N$ pseudo noise patterns. The pseudo noise pattern is random numbers with uniform distribution in the interval $[0,1]$. Low pass filtering is applied to the pseudo noise patterns to obtain smooth pattern and then the DC component is eliminated.

Consider part of a block $BR$ and pseudo noise pattern, both with the length of $L$, as vectors. The part $BR$ is projected to every pseudo noise pattern $PH_i$, i.e. $i \leq N$. The value is compared to the average of all the projections of $BR$ to the $N$ pseudo noise patterns to obtain $N$ Hash bits $b_i$ (see equation 1).

\[
\text{if } \sum_{j=1}^{L} |BR_j - PH_j| \leq \text{average } b_i = 0
\]

\[
\text{if } \sum_{j=1}^{L} |BR_j - PH_j| > \text{average } b_i = 1
\]

(1)

The average value is calculated after $BR$ is projected to all $N$ pseudo noise patterns. The average value is used as threshold to determine the output of the Hash function. Normally, half of the bits are 0 and half of the bits are 1 which results the highest information content in extracting the Hash bits [4].

Figure 3 shows an example of some patterns of pseudo noise and their projection values to some part of telephone signal $BR$. From the projection of 15 patterns of pseudo noise, the average is 393.89. The projection of each pattern is compared to the average projection value and then the Hash output $b_i$ is obtained using equation (1).

![Figure 3. Some pseudo noise patterns and their projection values](image)

The output of the Hash function consisting stream of bits 0 or 1 is assumed as binary number. The binary number is converted into decimal and then encrypted. In this project, the Hash output is encrypted using RSA [2] with the length of the key is 20 bits. The result is then converted again into binary number to be inserted to the other part of telephone signal $BL$ as watermark.

Scaling operation doesn’t change the output of the Hash function since the DC component of the pseudo noise signal has been eliminated and the

---

20 MEDIA TEKNIK No.2 Tahun XXVIII Edisi Mei 2006 No.ISSN 0216-3012
projection only depends on the variations of the signal. The pseudo noise patterns are generated by using time as the key to add time information to prevent someone from making a false conversation by concatenating from previously recorded conversation.

**Signature Insertion as Watermark**

The signature that is inserted as watermark must be robust against some disturbances and doesn't need the original signal for the detection. The watermark technique for this system uses spread spectrum modulation using pseudo noise signal for the insertion and detection [6].

The pseudo noise signal for watermark is generated using pseudo noise generator with the time as the key. The idea is modulating the pseudo noise signal with the watermark bits [5] to be inserted into some part of telephone signal. Therefore, in this method there are two kinds of pseudo noise according to the functionality, the first one is pseudo noise pattern $PW$ that is used in calculating the Hash function, and the second one is pseudo noise signal $PW$ to insert the signature as watermark. The pseudo noise signal which is used for watermarking is also random numbers in interval $[0,1]$ with uniform distribution. Pseudo noise signal has energy to all frequency components. We can choose in which frequency the watermark will be inserted by applying proper filtering. In this experiment, the watermark is inserted in mid frequency somewhere between 2000 until 3000 Hz.

The encrypted Hash output is stream of bits 0 or 1. In the signature insertion, signature bit 0 is converted into $-1$. For example $a_i$ is the sequence of watermark bits (1 or $-1$) with the length of $m$ bits to be inserted into the telephone signal. Part of the telephone signal $BL$ which will be used to insert the watermark is divided into $m$ blocks $BL_1, BL_2, ..., BLm$. Each signature bit will be spread into one of those blocks. The pseudo noise signal is modulated with the signature bit, amplified with $\alpha$, and then added to the telephone signal yielding a signal with signature:

$$BL_i = BL_i + \alpha \cdot a_i \cdot PW$$

$1 \leq i \leq m$  

(2)

Figure 4. shows the watermark insertion process to insert watermark bits [10].

Other methods for watermarking can also be applied to insert the signature, but for the telephone application the detection process should not need the original signal.

**AUTHENTICATION OF TELEPHONE SIGNAL**

Authentication is intended to check whether the signature which is detected corresponds to the telephone signal being received. Signature detection is performed by filtering the received signal on the frequency where the watermark was inserted in the part of the telephone signal $BR^*$ (see Figure 5).

For example, $PW$ is the pseudo noise signal which is used to insert the watermark and $BR_i$ is the filtered block signal to be detected with the length $K$. For every block $BL_i$ which contains one watermark bit, multiply every component $PW$ with $BR_i$ and then sum:

$$x_i = \sum_{j=1}^{K} BR_i \cdot PW_j$$

(3)

The formula above is the approximation to detect the signature bit [5]. The watermark bit $b_i$ can be obtained by thresholding:

$$b_i = sign(x_i)$$

(4)

If $y_i$ is positive, then watermark bit 1 is detected, otherwise watermark bit 0 is detected. The output of the watermark detection is then decrypted using the public key of the sender. The result will be compared with output of the Hash function which is calculated for the received signal $BR^*$. If they are the same, it means the signature was generated by the authentic source (see Figure 6).

**Figure 5. Signature detection**
EXPERIMENTAL RESULTS

This system has been implemented using DSK TMS 5402. Some disturbances are simulated using Matlab. From the experiment, the signature was robust against several operations:

- Scaling form 0.1 up to 100
- Random deletion up to 5% of the signal
- Noise addition with the amplitude lower than 1% of the average signal
- Low pass filtering using Butterworth filter with the cut off frequency 3750 Hz.

The signal can still be authenticated even with some disturbances as mentioned above. The signature insertion results a signal with SNR of 15 dB.

DISCUSSION

A cryptanalyst might try to generate signature for false speech signal or produce collision signature by modifying false signal in order to obtain the same Hash output as the authenticating signal (property of being collision). Generating signatures for false speech signals means that he needs to crack the RSA system because only the authorized person who has the secret key to generate the signature.

Modifying the false speech signal to produce a desired signature means the signal needs to have the right projections for all the N of pseudo noise patterns. Someone might be able to make some modifications to change the projection for the first pseudo noise pattern, but how about the other patterns. Changing the signal again to change it’s projection for the second pattern might result in a change in the projection for the first pattern. Many changes in the signal will cause degradation in the quality of the signal.

The problem is how many projections can be changed simultaneously, not one by one. The security can be increased by using more pseudo noise patterns in the Hash function to produce more bit output for longer signature.

CONCLUSIONS

The performance of this system mainly depends on the noise in telephonic line. The experimental results show that the signal can still be authenticated although there are some disturbances which sometimes occur in telephonic line. The insertion of signature will certainly degrade the signal quality, but still in acceptable degree without disturbing the conversation. To preserve the signal quality, the signature can be inserted only in some part of signal. The signal quality and the signature robustness will become trade off to determine the optimum parameter for this system.

REFERENCES


