2012 International Conference on Computer Technology and Science (ICCTS 2012)
IPCSIT vol. 47 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V47.7

A Dynamic Fuzzy Commitment Scheme

Nol Premasathian[1+] and Wacharee Tantikittipisut [2]

[1] Faculty of Information Technology, King Mongkut's Institute of Technology
Ladkrabang, Bangkok, Thailand
[2] Independent Researcher
Ladkrabang, Bangkok, Thailand

Abstract. Fuzzy commitment scheme allows commitment where inputs can be altered by some certain number of bits. This paper presents a dynamic fuzzy commitment scheme where the commitment can gradually change by the time and retain the fuzzy authentication capability. When an entry passes the authentication, its value is taken to adjust the commitment. To achieve this, the exponential averaging method is used to generate the next commitment from a successful input along with the existing commitment. The optimal smoothing factor is recommended to achieve the highest successful authentication rate.

Keywords: fuzzy commitment, biometric commitment, fuzzy matching

1. Introduction

Commitment schemes are important components of a number of cryptographic protocols. In a commitment scheme [1], a user commits to a value while keeping it a secret. Later, an attempt is made to guess the value or to prove the possession of it. Then committed value is revealed and compared with the attempted one. The attempt is successful if and only if both values are exactly the same. A string with a single bit change will fail the verification. The committed value cannot be changed after the commitment is made. The original commitment scheme is not suitable for a biometric secrecy system due to the random noise in the data. The fuzzy commitment scheme introduced by Juels and Wattenberg allows the commitment to be made in a fuzzy manner [2]. That means the attempt is successful when the attempted input is the same as or is slightly different from the committed value. Some biometric information such as voice or speech gradually changes as time passes by. Therefore the fuzzy commitment scheme where the commitment is anchored as a particular value cannot be used in verifying the biometric information, especially when the usage spans a long period of time. This paper introduces a fuzzy commitment scheme that allows the commitment to changes gradually by updating the commitment information with the recently obtained biometric data. The paper is organized as follows. The second part describes related works. The third part explains a proposed scheme using exponential averaging technique and its testing. The last part is the conclusions and the future work.

2. Related Works

2.1. Fuzzy Commitment Scheme

The fuzzy commitment scheme introduced by Juels and Wattenberg makes use of error correction to correct the attempted input to the committed value if the attempted input is close enough to the committed value. If the attempted input is not close enough to the committed value, the correction will transform it to a value completely different to the committed one. The scheme works as follows.

[+] Corresponding author.
E-mail address: nol.pre@gmail.com

1. A codeword *w* is randomly chosen from a set of error correcting code *C,* which contains codes capable of correcting up to *t* bits of error.

2. The committed value *s* is added with the codeword *w* using exclusive-or operation. The result is $s \oplus w$.

3. Hash the code word *w* to get H(*w*). Destroy *w* and keep only $s \oplus w$ and H(*w*).

4. An attempting user enters s' to the scheme, which calculates $s' \oplus s \oplus w$. If s' does not differ from *s* by more than *t* bits, then it is possible to correct $s' \oplus s \oplus w$ back to w. This can be verified by computing the digest of corrected $s' \oplus s \oplus w$ and compared it with the stored H(*w*).

The first three steps belong to the enrolment part of the protocol while the last step is the authentication part. There are some other fuzzy matching techniques proposed such as the one by Al-saggaf and Acharya [3], which employs a technique similar to the one proposed by Juels and Wattenberg. Ojha and Sharm proposed a fuzzy commitment scheme with McEliece's cipher, an asymmetric encryption based on error correction [4].

2.2. Exponential Averaging

Exponential averaging or exponential smoothing introduced by Charles C. Holt in 1957 [5] is a technique to average or smooth time series data. It is often applied to financial or economic data for forecasting purposes [6][7]. The raw data sequences x_t and the exponential smoothing s_t is expressed in the following formula.

$$s_1 = x_0 \quad (1)$$

$$s_t = \alpha.\ x_{t-1} + (1-\alpha).\ s_{t-1} \quad (2)$$

In contrast to the moving average technique, which is the average of certain number of latest measurements, exponential averaging does not require a minimum of data to be collected before commencing the smoothing process. It also reduces the amount of calculation as well as the space requirement as it uses just the previous average value, not a set of preceding values.

3. The Proposed Scheme

3.1. Formulation

In contrast to the original fuzzy commitment scheme, which maintains a static commitment, the proposed scheme makes adjustment to the commitment when an authentication attempt succeeds. In order to adjust the commitment, we must predict or estimate the next incoming value using the previous ones. Only the values that were successfully matched in the authentication process account for the adjustment or the estimation process. We use the exponential averaging method to adjust the value as shown in equations 3 and 4.

$$\text{Commitment}_0 = \text{The Enrolled Data} \quad (3)$$

$$\text{Commitment}_t = \alpha.\text{Commitment}_{t-1} + (1-\alpha).\text{current input} \quad (4)$$

The smoothing factor (α) is between 0 and 1. When α is 0, the commitment is replaced with the new successful input. When α is 1, the commitment never changes, and is the same as the original fuzzy commitment scheme. As the fuzzy commitment scheme operates by bit but the exponential averaging is performed by value, randomly chosen (α x Commitment Length) bits from the existing commitment together with the remaining (1-α) x Commitment Length from the current input forms the new commitment. Alternatively the fuzzy matching scheme [8], which breaks the commitment into parts in unary representation and recovers the original commitment using Chinese Remainder Theorem, is a fuzzy commitment scheme that the authentication is operated by value and can be applied in this problem.

3.2. Testing

The proposed scheme is tested to find the optimal value of α, which gives the highest rate of successful authentication. We define two types of rates. The "pass rate" is the rate of input passing the authentication test. That means an input is count toward the pass rate even if, in reality, it should not be authenticated. Another rate is called "successful authentication rate" is the rate of an input passing the authentication test when it is supposed to be so. For example, a commitment value c_1 is set and a valid input i_1 is entered. Algorithm One, after processing i_1, changes the commitment to c_{ONE} while algorithm Two, after processing i_1,changes the commitment to c_{TWO}. When the next input i_2 is entered, it is not supposed to pass the authentication test. If it passes the test when the commitment c_{ONE} is used and fails with the other c_{TWO}, it is counted toward the pass rate for c_{ONE} but the successful authentication rate for none of the algorithms. In the experiment, we adjust the commitment when the input passes the authentication test but for the measurement of how suitable a smoothing factor is, we count the number of successful authentication.

Our test uses the commitment value of 1000 and the value is incremented in 1000 steps. The acceptable error is 0.5. An input is a random number (normal distribution, average being the commitment value and SD =1). In each step, the commitment is incremented by 0.1, 0.2, …, 0.9, 1.0 and 1.5. We found that increments larger than the standard deviation give low successful authentication rates. The smoothing factor α increases from 0 to 0.1 by a step of 0.001. The actual stored commitment that is used to test the passing is calculated each time that an input passes the authentication. The successful authentication is counted only when the authentication is approved (by the stored commitment value) as well as it does not differ from the real commitment value by the specified error. For a combination of each increment and commitment value, a number of 1000 values are randomly generated. The result of the test is shown in figure 1.

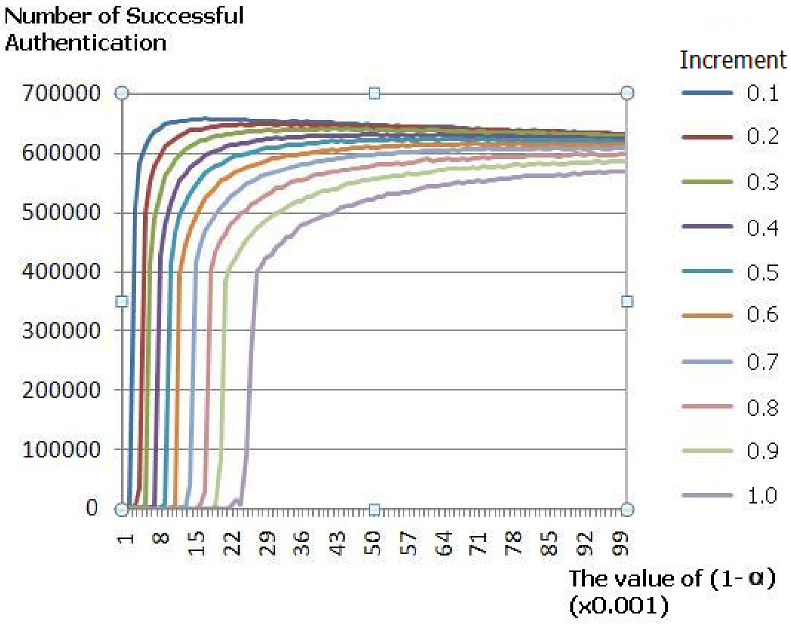

Fig. 1: The number of successful authentication for each increment, α = 0.000 - 0.100

From the figure, there are 10^6 tests for a combination of each increment (1000 commitment values x1000 random inputs). In the original fuzzy commitment scheme, we found that the successful authentication rate for SD=1 and the error is less than or equal to 0.5 is about 68.26%. It can be seen that the proposed scheme suffers a small drop in successful authentication rate compared to the original fuzzy commitment scheme but it improves the successful authentication rate when it is used in a situation where the commitment value can change. The result of the original fuzzy commitment scheme is shown in the figure where α=1 (or 1- α = 0). The successful authentication rate of the original fuzzy commitment scheme is naturally low due to its static commitment. When the increment increases, the number successful authentication decreases almost linearly. For each increment, there exists a smoothing factor (α) that gives the highest successful authentication rate. We conduct a similar experiment using a coarser smoothing factor increment of 0.01, with α ranging from 0 to 1. The result is shown in figure 2.

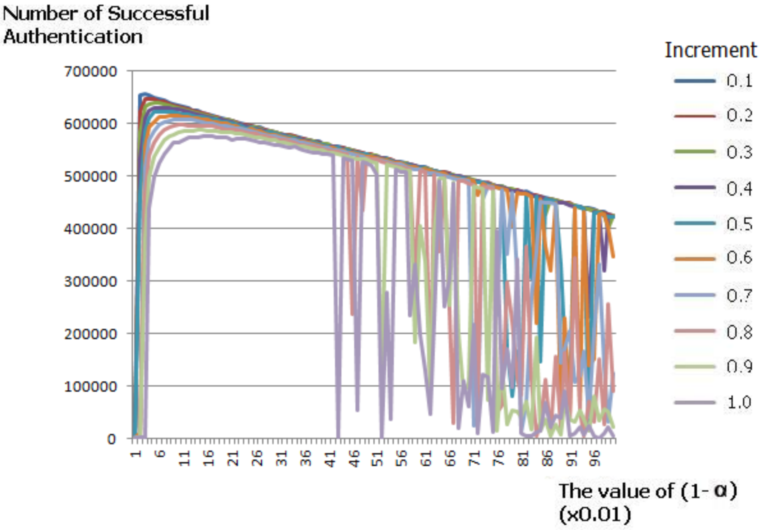

Fig. 2: The number of successful authentication for each increment, α = 0.00 – 1.00

We can see that the successful authentication rate is unpredictable when the smoothing factor (α) is too high. The smoothing factor that gives highest number of successful authentication for each increment is shown in table 1.

Table 1: The optimal smoothing factor for each increment

Increment	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
The optimal smoothing factor	0.03	0.04	0.05	0.07	0.09	0.11	0.14	0.12	0.16	0.17

From the table, we found that the increment/optimal smoothing factor ratio for SD=1 is about 3-6 to 1. For any other sample where SD has a different value, the optimal smoothing factor can be chosen in the same way and multiply it with the SD. That means if we know or can predict the increment, we can choose an appropriate smoothing factor for the scheme.

4. Conclusions and Future Works

We have presented an approach of fuzzy matching that the commitment is dynamically changed. This can be useful for biometric authentication where the biometric data can gradually be altered. We found that there is a particular smoothing value for each increment that can be used to obtain the highest successful authentication rate.

Our future works will address the problem of the dynamic fuzzy commitment that checks the commitment by bit not by value. Also we plan to construct a dynamic fuzzy commitment scheme that keeps some previous information for prediction purposes. By using this, we will not need the exponential smoothing in the scheme.

5. Acknowledgment

We would like to express gratitude to the Faculty of Information Technology, King Mongkut's Institute of Technology Ladkrabang for the continual support.

6. References

[1] G. Brassard, D. Chaum, and C. Crepeau. Minimum Disclosure Proofs of Knowledge. In: *Journal of Computer and System Sciences*. 1988, **37**: 156-189.

[2] A. Juels and M. Wattenberg. A Fuzzy Commitment Scheme. In: *Proceedings of the 6th ACM Conference on*

Computer and Communications Security (ACM CCS '99), pp. 28-36. November 1-4 1999, Singapore.

[3] A. A. Al-saggaf and H. S. Acharya. A Fuzzy Commitment Scheme. In: *Proc. of IEEE International conference on Advances in Computer Vision and Information Technology (ACVIT)*. November 28-30, 2007, Aurangabad, India.

[4] D. B. Ojha and A. Sharm. A Fuzzy Commitment Scheme with McEliece's Cipher. In: Surveys in Mathematics and its Applications. 2010, **5**: 73–82.

[5] C. C. Holt. Forecasting Trends and Seasonal by Exponentially Weighted Averages. In: *Office of Naval Research Memorandum*. 1957, **52**.

[6] J. J. Wang, J. Z. Wang, Z. G. Zhang, and S. P. Guo. Stock index forecasting based on a hybrid model. *Omega*. 2012, **40**(6): 758-766.

[7] J. W. Taylor, and R. D. Snyder. Forecasting intraday time series with multiple seasonal cycles using parsimonious seasonal exponential smoothing. *Omega*. 2012, **40**(6): 748-757.

[8] A. Satienjarurat and N. Premasathian. Fuzzy Matching of Object using Fuzzy Commitment Scheme. In: *Proc. of 6th International Conference on Electrical Engineering, Electronics, Computer, Telecommunications, and Information Technology (ECTI-CON)*. May 6-9 2009, Chonburi, Thailand.