数理解析研究所講究録 1268 巻 2002 年 40-46

Formal Language Theoretical Approach to Secret Sharing Schemes

Akihiro Yamamura (山村明弘) and Osamu Takizawa (滝澤修)

Communications Research Laboratory (通信総合研究所),
4-2-1, Nukui-Kitamachi, Koganei, Tokyo, 184-8795 Japan
{aki, taki}@crl.go.jp

1 Introduction

Secret sharing scheme was proposed by Shamir [10] and Blakley [2] independently. The basic idea is to share (or distribute) a secret, usually random bit string, among multiple shareholders, and if enough number of the share holders agree that they want to retrieve the secret then they offer their own shares and obtain the secret. None of the share holders knows the secret, and essentially there is no way to find it by any combination of shareholders with less number participants. Shamir and Blakley used polynomial interpolation to construct a secret sharing scheme.

Naor and Shamir [9] introduced the *visual cryptography*, which is a secret sharing scheme using a physical device such as transparency sheets (or OHP sheets). Their scheme has advantage that secret can be retrieved without computation. This implies that we do not have to appeal to a computer. In this scheme, the dealer makes transparency sheets or any physical mean as shares and distribute to the shareholders. Shareholders can collect shares and obtain the secret. In this situation, the secret is a graphical image, and the shareholders can recognize the secret via human eyes.

Information security supplies methods of manipulating digital data for our secure and reliable communication environment. The visual cryptography tries to give us techniques in the context of physical device not in the digital data. In this paper, we discuss another attempt to attain information security basically based on non-digital data, that is, natural language texts. Our attention is in secret sharing schemes, however, other proposals on natural language steganography are also presented [1]. This paper is an extended abstract and the detailed version will be published elsewhere

2 Secret Sharing Schemes

We recall the threshold scheme and the visual cryptography in this section. A definition of threshold secret sharing scheme is given as follows.

Definition Let w, t be natural numbers with $t \leq w$. A (t, w) threshold scheme provides a method to share a random bit string K (called a *key*) among the set of w participants (denoted by $\mathcal{P}$) so that any t participants can find K but no group of less than t participants

can obtain K.

We note that no group of less than t participants has any clue for K. This means that any computation cannot specify K.

2.1 Threshold Secret Sharing

We describe Shamir's threshold scheme [10] using polynomial interpolation. Let $\mathbb{F}$ be a finite field. The set $\{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \ldots, \mathcal{P}_w\}$ is denoted by $\mathcal{P}$.

2.1.1 Initialization

The dealer (denoted $\mathcal{D}$) chooses randomly w distinct elements from $\mathbb{F}$, where the cardinality of $\mathbb{F}$ is bigger than w. These are denoted by x_i $(1 \leq i \leq w)$. $\mathcal{D}$ gives x_i to $\mathcal{P}_i$ for each $1 \leq i \leq w$.

2.1.2 Share Distribution

Let K be the key chosen from $\mathbb{F}$. $\mathcal{D}$ chooses randomly and independently $t-1$ elements $a_1, a_2, a_3, \ldots, a_{t-1}$ of $\mathbb{F}$. Set $a_0 = K$. $\mathcal{D}$ computes $y_i = a(x_i)$ for each $1 \leq i \leq w$, where

$$a(x) = a_0 + \sum_{j=1}^{t-1} a_j x^j.$$

$\mathcal{D}$ gives y_i to $\mathcal{P}_i$ for each $1 \leq i \leq w$.

We now observe how a group of t participants reconstruct the key K.

2.1.3 Key Reconstruction

Suppose that $\mathcal{P}_{i_1}, \mathcal{P}_{i_2}, \mathcal{P}_{i_3}, \ldots, \mathcal{P}_{i_t}$ want to find K. Each of $\mathcal{P}_{i_j}$ provides $y_{i_j} = a(x_{i_j})$ Recall that $a(x) = a_0 + \sum_{j=1}^{t-1} a_j x^j$ and so $a(x)$ has the degree at most $t-1$. We also note that the constant coefficient a_0 is the key K. Thus the group $\{\mathcal{P}_{i_1}, \mathcal{P}_{i_2}, \mathcal{P}_{i_3}, \ldots, \mathcal{P}_{i_t}\}$ obtains t linear equations in the t unknowns $a_0, a_1, a_2, \ldots, a_{t-1}$, and thus they can reconstruct $a_0 = K$.

It is easy to see that no group of less than t participants can reconstruct K. Secret sharing scheme is generalized to a great extent. The reader is referred to [11].

2.2 Access Structures

In the threshold secret sharing schemes, any t out of w participants can obtain find the secret key. It may be plausible that more general subset structure is required. For example, some participants are given higher priority and the others are not.

The set Γ of subsets of $\mathcal{P}$ is called an *access structure* of a secret sharing scheme if (i) the participants of any subset in Γ pool their shares and obtain the secret key, and (ii) the participants forming of a subset containing no subset in Γ can obtain (basically) no information on the secret key. We should note that an access structure should be monotone, that is, if a subset $\mathcal{A}$ includes a subset $\mathcal{B}$ in $\mathcal{P}$ should lie in $\mathcal{P}$, then $\mathcal{A}$ must lie in $\mathcal{P}$. In the (t, w) threshold scheme, the access structure is provided by

$$\{\mathcal{B} \subset \mathcal{P} \,|\, t \leq |\mathcal{B}|\}.$$

In the text secret sharing scheme, we often need not only subset structure but the *order structure* of the set of participants. It is quite difficult to manage access structure in text secret sharing schemes.

2.3 Visual Cryptography

The visual cryptography scheme, introduced by Naor and Shamir [9], is a method encryption of printed text, handwritten notes, pictures or so in a perfectly secure way that the hidden information can be decoded by the human eyes. This system is considered as a secret sharing scheme without computation. The basic idea is that the hidden information is embedded into a transparency with noise. The transparency is just a noise data for anybody who do not have a secret decoding transparency. The system can be seen as a physical version of the one time pad. Our text secret sharing scheme can be seen as a text version of one time pad. The data is just replaced by text in our situation.

3 Formal Language Theory

Although our ultimate goal is an application to natural language based information security, it may be reasonable to start our research from formal language theory. As Chomsky [3, 4, 5, 6] defined several classes of a formal language as models of natural language, we consider formal language as models of natural language. A mathematical model of a language is a set of sentences, that is, finite strings of fixed alphabet. The aim of formal language theory is to give a concise specification of a language. Thus we need a finite description device to represent an infinite language. Traditionally, there are two ways: generative devices and recognition devices. A *grammar* is a generative method and an *automaton* is a recognition method. In applying to information security, we use both of them because both generation and recognition of language are equally significant. In initializing the system and distribute shares to the participants, sentence generation device is required. In finding the secret key, the recognition device is an ideal tool.

3.1 Language recognizers

A *finite deterministic automaton* is a simple device to recognize a string on a fixed alphabet as a sentence in a language [7, 8]. Let Σ be an alphabet. A finite state automaton over Σ is a quintuple $M = (Q, \Sigma, \delta, q_0, F)$, where Q is the set of states, q_0 belongs to Q and called the *initial state*, F is a subset of Q and called the *set of final states*, and δ is the *transition function* mapping $Q \times \Sigma$ to Q. We denote the image of (q, a) in $Q \times \Sigma$ under δ by $\sigma(q, a)$. We now define the function $\widehat{\delta}$ of $Q \times \Sigma^*$ to Q recursively.

(i) $\widehat{\delta}(q, \lambda) = q$, where $q \in Q$ and λ is the empty string.

(ii) $\widehat{\delta}(q, wa) = \delta(\widehat{\delta}(q, w), a)$ for $w \in \Sigma^*$ and $a \in \Sigma$.

The language $L(M)$ accepted by the automaton M is the set of string w such that $\widehat{\delta}(q_0, w)$ belongs to F.

There are variants of an automaton with additional computation power. We note that recognition of a sentence is done during the time of reading the string. This means that an automaton is very effective device to recognize a language. On the other hand, more intricate machine like a Turing machine takes more time to recognize. We also note that

an automaton has very simple description, and so it is an ideal tool to simulate language theoretical information systems.

In constructing text based secret sharing schemes, we need manage not only sentences but a block of sentences or arrays consisting of sentences. In the situation, automata are still basic tool to recognize such an object but we have questions whether automata are ideal tool for recognition. It may be possible to invent more effective recognition. We pose several questions concerning text based secret sharing schemes in Section 5.

3.2 Language generators

A mathematical model for a generative device for sentences is a *grammar*. Corresponding to the hierarchies of automata, there are hierarchies of grammars. We discuss only a *regular grammar* corresponding to finite deterministic automata.

A grammar G is a quadruple (V, T, P, S), where V and T are finite sets of variables and terminals. P is a finite set of productions of the form $A \to \alpha$, where α belongs to $(V \cup T)^*$. S is a special variable called the start symbol. Such G is called a *context free grammar*. If each production is of the form $A \to wB$ or $A \to w$, then G is called *regular grammar*. We define binary relations $\Rightarrow$ and $\overset{*}{\Rightarrow}$. If $A \to B$ is a production in P, then $\alpha A\beta \Rightarrow \alpha B\beta$ for any α and β in $(V \cup T)^*$. If β is obtained from α by applying $\Rightarrow$ several times, then we have $\alpha \overset{*}{\Rightarrow} \beta$. Then the language generated by G is the set $\{w \mid w \in T^*,\ S \overset{*}{\Rightarrow} w\}$. The language generated by a regular grammar is a regular set and so recognized by a finite deterministic automaton.

A grammar is a useful device to generate a sentence, however, it may not be enough to generate a number of sentences. It is extremely important to generate a set of sentences which are consistent, that is, the set of sentences has real life meaning, and so, one does not doubt the existence of the secret information. This type of information security technique is called steganography and discussed in the next section.

4 Steganography

Steganography is the method to conceal the existence of messages, and it is different from cryptography. It offers us the technology to embed hidden message or any secret information in images, videos, and audio files. The most successful methods is based on the discrete Cosines transform or the discrete Fourier transform. Natural language steganography should enable us to embed secret text data into natural language text, however, the discrete Fourier transform does not work on text. Natural language watermarking is proposed in [1], and several plausible methods to put the hidden watermark into meaning natural sentences are presented. In general, text steganography aims at embedding hidden information into natural language sentences.

We discussed only syntactic aspect of language, that is, the grammar. On the other hand, the semantic aspect of natural languages is important for our research on text secret sharing schemes because such scheme can have advantage to embed each share in a meaningful natural language text, which is not accomplished by any existing secret sharing scheme.

Since the steganography is the study of systems to hide a secret in digital media or physical devices, we want to apply natural language steganography to embed each share in a natural language text. In such a situation, texts should not be artifact, because language is a mean to transmit information from one person to another. So sentences must contain some meaning.

Our approach to secrete sharing schemes can be considered from the standpoint of natural language steganography. In Section 6, we slightly mention our experimental approach.

5 Discussion on Text Secret Sharing Schemes

A text secret sharing scheme is a system to embed a hidden text in several text in a way that nobody who do not have access to the information can obtain the information. Our aim is to construct such a system in both formal language context and natural language context. We have done some experiments to construct such systems in ad hoc manner, however, we have no general tactics for it.

There are three goals for text secret sharing scheme: constructing a new secret sharing scheme, steganography in natural language and development in formal language theory. Our secret sharing scheme can be integrated into a matrix representation of symbols in the alphabet. Our data is a matrix

$$\begin{array}{cccc} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{array}$$

where each entry is from the alphabet A. We suppose that each share corresponds to each row, and so they should be sentences belonging to a fixed language $L(M)$ for some machine M, on the other hand, each column does not belong to the language. This is similar to the idea in the visual cryptography in Section 2.3. In the case of the visual cryptography, the tile data is transparency.

As we mentioned before, a grammar is a useful device to generate a sentence. But it may not be enough to generate a set of sentences which are consistent and have real life meaning, for example, a story. We want to include semantics in the set of sentences to achieve the practical way to hide secret information. The starting point is how to generate a set of sentences in a consistent manner. We would like to pursue the study of this question in formal language theory. Technical issues are the following.

- Generating efficiently consistent sentences
- Access structure
- Recognizing efficiently sentences
- Use of natural language database
- Storage method of sentences

The first issue is related to the need for a generalized idea for a grammar. A grammar gives us the way to generate a sentence, however, we need to generate a set of sentences in a way that the generated sentences are consistent and have a real meaning. Suppose that the order of pile of the strings (shares) is correct, then only one column belongs to the language and we can recognize the sentence, and it is the hidden secret. The dealer $\mathcal{D}$ makes up such matrix and the order structure of the participants, and then distribute to the participants. It does not seem an easy task to construct such a matrix. We also note that we need take into consideration of a variation of natural languages. Possibly English is the most reasonable target, but we may want to consider Japanese language as well.

The second issue is that we need give more structure on the set of participants. In Shamir's threshold scheme, the set of participants is a set. On the other hand, in the natural text secret sharing scheme, we possibly require the order structure and need consider an ordered set instead of just a set.

The third is the effective way of recognizing sentences. Each row belongs to the language $L(M)$. On the other hand, only one column belongs to $L(M)$. To find the column, the participants may need change their order unless the order structure has previously determined.

The issue is related to the systems using the natural languages. We have made up an experimental system which works on Japanese text 6. In the system we use a text database to construct shares.

The last issue is related to steganography. The shares are embedded into texts. If we use the natural language oriented system, the share should be embedded into natural language texts having real life meaning. Then the texts should be stored in the form of a diary, a book, a note or so. It means the share should be physically protected.

6 Experiments

We constructed a natural language text secret sharing scheme by setting a threshold value in Japanese language. We here omit the details on the computation experiments in Japanese language systems. Instead, we just outline our system. In our system, the shares are made up using the texts database. We search the database and pick up sentences. The we construct share in an ad hoc manner. The recognition of the secret information is done by checking the plausibility that the string is a natural language sentence. We check the frequency of the consecutive characters which form basic vocaburary in a Japanese dictionary. If the string contains more than a certain number of characters forming vocaburaries, then we recognize it as a natural language sentence. The method is pretty effective to recognize a natural language sentences. There are no theory for the recognition of natural language sentences, however, the theory of formal language is based on firm mathematical ground and so gives us inspiration.

Every natural language has characteristics, and so we cannot develop a similar system for English or other European languages just by modifying our system in Japanese language. We are planning to show our experiments in English in the future, and we shall report on it.

References

[1] M.J.Atallah, V.Raskin, M.Crogan, C.Hempelmann, F.Kerschbaum, D.Mohamed, and S.Naik, "Natural language watermarking: Design, analysis, and a proof-of-concept implementation", Information Hiding (IH 2001) LNCS 2137, Springer-Verlag 185–199, 2001.

[2] G.Blakley, "Safeguading cryptographic keys", Proceedings of AFIPS National Computer Conference, 313–317, 1979.

[3] N.Chomsky, "Three models for the description of language", IRE Trans. on Information Theory **2**, 113–124, 1956.

[4] N.Chomsky, *Syntactis Structures*, Mouton Gravenhage, 1957.

[5] N.Chomsky, "On certain properties of grammers", Information and Control **2**, 137–167, 1959.

[6] N.Chomsky, "Formal properties of grammers", Handbook of Math. Psych. Vol 2, 323–418, 1963.

[7] J.Hopcroft and J.Ullman, *Introduction to automata theory, languages, and computation*, Addison Wesley, 1979.

[8] H.Lewis and C.Papadimitriou, *Elements of the Theory of Computation* 1998

[9] M.Naor and A.Shamir, "Visual Cryptography", Advances in Crypt CRYPT'94), LNCS 950, Springer-Verlag 1–12, 1994.

[10] A.Shamir, "How to share a secret", Communications of the ACM, **22**, 61

[11] D.Stinson, *Cryptography*, CRC Press, 1995.