Chapter 45
Security in Management of Distributed Information

Marek R. Ogiela, Lidia Ogiela and Urszula Ogiela

Abstract In the chapter will be shortly presented some advances in the area of computer methods used for encryption and division of confidential data, as well as modern approaches for management of shared information. Cryptographic techniques for secret information distribution allow to secure strategic data against disclosure to unauthorized persons. The chapter will shortly describe algorithms for information sharing on the basis of personal biometric features. The development of computer techniques for classified information sharing should also be useful in the process of shared information distribution and management.

Keywords Cryptographic protocols · Secret sharing · Secure information management

45.1 Introduction

One of the fastest developing subjects associated with application of modern and advanced information technologies to manage information in commercial organizations, comprises the acquisition, flow and intelligent analysis of the information management process. During several recent years there were developed many different cryptographic procedures for secure information splitting or sharing, which may be applied for secure information distribution in particular organization. Among such algorithms it is possible to find some special examples of splitting

M.R. Ogiela (✉) · L. Ogiela · U. Ogiela
Cryptography and Cognitive Informatics Research Group, AGH University of Science and Technology, Al. Mickiewicza 30, 30-059 Krakow, Poland
e-mail: mogiela@agh.edu.pl

L. Ogiela
e-mail: logiela@agh.edu.pl

U. Ogiela
e-mail: ogiela@agh.edu.pl

J.J. (Jong Hyuk) Park et al. (eds.), *Ubiquitous Computing Application and Wireless Sensor*, Lecture Notes in Electrical Engineering 331,
DOI 10.1007/978-94-017-9618-7_45

procedures, which are based on using personal data in the sharing algorithm. From strategic point of view it may be very interesting, when as input values we can also put biometric or personal information for generation of particular shares. In the next section we'll try to describe some important features of crypto-biometric techniques, which may be used for secret sharing tasks [8, 9].

45.2 Security of Threshold Schemes

Secure information management procedures may be oriented towards developing cryptographic threshold schemes for sharing and secure distribution of information. The ideas of such schemes are hide information and guarantee its confidentiality, but in our research we also made attempts to use such techniques to create new models for intelligent management of strategic information [10, 11]. Especially challenging problem is to perform hierarchical secret splitting and shares management. What characterizes such a split is the possibility of reconstructing information from sets containing various numbers of shares of split secret. For this purpose we proposed a special threshold schemes called linguistic threshold schemes [9] dedicated for information sharing and using them to manage secret data in various hierarchical organisational structures [7].

Such algorithms allow effectively use threshold techniques of information sharing for multilevel management of data in digital form. The proposed general model for sharing information was additionally based on mathematical linguistic formalisms including protocols for information retrieval, and the range of application of such techniques is very broad for various organizational structures.

Linguistic threshold schemes allow to move from purely mathematical models of information sharing, or from using them only in dedicated, specialized information sharing problems, to a broader application of such techniques to manage secret data, designed for broader user groups. Such information can be stored by any commercial organization or state institution, and its meaning can be used only if it is accessed as authorized by appointed, entitled groups of users or employees. This is why we will attempt to define a model structure of the flow and assignment of information shares to individual groups of stakeholders. The proposed model could then be rolled out for its practical use in any commercial organization or state institution based on its legacy information system [1].

The new method of information splitting is called linguistic threshold schemes [8]. Mathematical linguistic techniques have not yet been used in information splitting, so building a new protocol for splitting secret data using these techniques represents a new research element in this field.

45.3 Crypto-Biometric Sharing Schemes

A great number of cryptographic threshold procedures were developed. Some of them may also use individual human information or biometric patterns [2–4]. Nowadays, information frequently needs to be kept back from unauthorized persons, so it is not always enough to just encrypt it with various types of algorithms.

For better supporting the authentication and authorization process, we can also verify biometric features, like fingerprints, voice characteristics or the retina. DNA molecules are also playing an increasing role in cryptography, but it was only in the 21st century that science offered opportunities of using them as information media, and the replication processes taking place in them as information coding techniques. Recent years have seen increasingly frequent reports of further discoveries, while the results of DNA research are becoming significant not just in biology or genetics, but also in the field of cryptography and steganography [11].

People have not realises the computational potential associated with molecules for many years. The first ideas of combining computers with DNA chains appeared in 1973, when Charles Bennett published a paper in which he proposed a model of a programmable molecular computer capable of executing any algorithm [11]. Since then, many new proposals for using DNA sequences as an information medium, have been made. Practically every such method of classifying data boils down, at least at one stage, to storing this data in the appropriate DNA molecules. At this level there are several available possibilities of using these acids as the medium for coded information.

The most obvious one is using the structure of particular nucleotides. As four types of them can be distinguished, one base can store 2 bits of information. We can thus assume that the coding will, for example, be executed as presented in Fig. 45.1. One can also start from the assumption that one pair of nucleotides (a single hydrogen bond irrespective of its polarisation) corresponds to one bit of information (Fig. 45.1).

Such information coding methods are used in biological solutions which have inspired us to development of a new class of algorithms for secret splitting [11]. However, linguistic threshold scheme operates in a more general way and supports coding secret information (to be split) in longer sequences, i.e. containing more than 2 bits of information [9]. The purpose of this algorithm is a threshold split of strategic data managed within hierarchical structures, with varied access capabilities dependent on the rights granted [11].

45.4 Security Features for Strategic Information Management

In presentation of strategic data splitting and sharing algorithms it has become necessary to describe security features of linguistic algorithms used for information splitting and data reconstruction. The essence of this approach, representing an

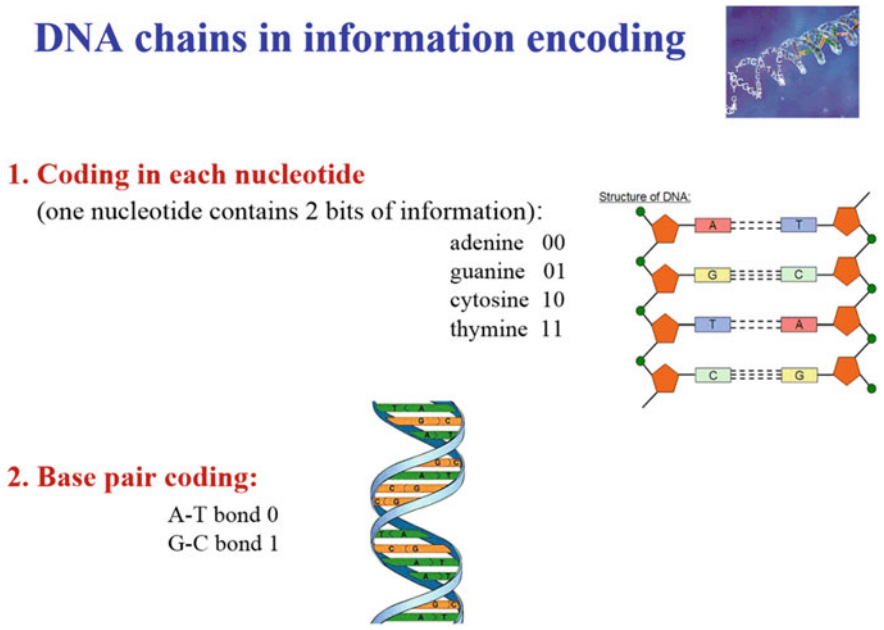

Fig. 45.1 Possible methods of coding information using DNA molecules

interdisciplinary topic straddling the border between the subjects of commercial organisation management and of information theory, is an attempt to use cryptographic methods more commonly applied in engineering and technical fields for purposes for which such solutions have not yet been proposed like economy and management sciences.

The proposed algorithmic solutions for data splitting and sharing have the following important properties and characteristic security features:

- Linguistic cryptographic threshold algorithms are suitable for dividing important strategic data and assigning shares to members from the authorized group;
- The algorithms are based on digital data (texts, images, voice recordings) which needs to be intelligently split among authorized persons, and then its secret reconstruction must be possible;
- There are wide opportunities to combine traditional methods of cryptographic information splitting ((m, n)-threshold schemes) with the presented protocols;
- The ability to present information in the form of its bit recording or sequences of blocks containing n bits;
- Introducing additional safeguards against the unauthorized reconstruction of the information and the possibility of implementing two independent versions of protocols for assigning the created shadows to individual protocol participants: the option with a trusted arbitrator intermediating in assigning and reconstructing the information and the option without an arbitrator (an additional

trusted party), but only with assigning the introduced grammar as an additional part of the secret;
- The ability to introduce restrictions of the length of coded bit blocks in the proposed scheme, as a result of which the defined grammar will not contain a large number of derivation rules;
- The computational complexity of the proposed schemes is polynomial.

The above characteristics of the linguistic algorithms of information division constitute their advantages and show how universal these proposed methods for splitting and sharing secret or strategic information in commercial organisation are.

45.5 Conclusions

In this chapter were described some advances in using biometric information to develop new procedures for secret information sharing called linguistic thresholds schemes. Processes of splitting strategic data are currently used in many fields of life, science and economy. Application of linguistic coding methods in the concealment and analysis processes, offers the full capability of using personal information for such purposes. Concealing biometric or personal data constitutes a very important problem because it is highly probable that personal data will be taken over by unauthorized persons. The individual DNA code and many other standard or non-standard biometrics may be used during sharing procedure [5, 6].

Acknowledgments This work has been supported by the National Science Centre, Republic of Poland, under project number DEC-2013/09/B/HS4/00501.

References

1. Cohen H, Lefebvre C (eds) (2005) Handbook of categorization in cognitive science. Elsevier, Amsterdam
2. Hachaj T, Ogiela MR (2012) Framework for cognitive analysis of dynamic perfusion computed tomography with visualization of large volumetric data. J Electron Imaging 21 (4):043017
3. Ogiela L (2008) Syntactic approach to cognitive interpretation of medical patterns. Lect Notes Artif Intell 5314:456–462
4. Ogiela L (2008) Cognitive systems for medical pattern understanding and diagnosis. Lect Notes Artif Intell 5177:394–400
5. Ogiela L (2009) UBIAS systems for cognitive interpretation and analysis of medical images. Opto-Electron Rev 17(2):166–179
6. Ogiela L (2010) Cognitive informatics in automatic pattern understanding and cognitive information systems. Studies in computational intelligence, vol 323. Springer, Berlin, pp 209–226
7. Ogiela L, Ogiela MR (2009) Cognitive techniques in visual data interpretation. studies in computational intelligence, vol 228. Springer, Berlin

8. Ogiela MR, Ogiela U (2009) Security of linguistic threshold schemes in multimedia systems. In: 2nd international symposium on intelligent interactive multimedia systems and services, Mogliano Veneto, Italy, 16–17 July 2009. New directions in intelligent interactive multimedia systems and services—2, Studies in computational intelligence, vol 226, pp 13–20
9. Ogiela MR, Ogiela U (2010) The use of mathematical linguistic methods in creating secret sharing threshold algorithms. Comput Math Appl 60(2):267–271
10. Ogiela MR, Ogiela U (2012) DNA-like linguistic secret sharing for strategic information systems. Int J Inf Manage 32(2):175–181
11. Ogiela MR, Ogiela U (2014) Secure information management using linguistic threshold approach. Advanced information and knowledge processing. Springer, London