Crypto-Biometric Models for Information Secrecy

Marek Ogiela, Lidia Ogiela, Urszula Ogiela

Crypto-biometric Models for Information Secrecy

Marek R. Ogiela, Lidia Ogiela, Urszula Ogiela

AGH University of Science and Technology
Cryptography and Cognitive Informatics Research Group
30 Mickiewicza Ave., PL-30-059 Krakow, Poland
{mogiela, logiela, ogiela}@agh.edu.pl

Abstract. In this paper will be presented some advances in crypto-biometric procedures used for encryption and division of secret data, as well as modern approaches for strategic management of divided information. Computer techniques for secret information sharing aim to secure information against disclosure to unauthorized persons. The paper will present algorithms dedicated for information division and sharing on the basis of biometric or personal features. Computer techniques for classified information sharing should also be useful in the process of shared information generation and distribution. For this purpose there will be presented a new approach for information management based on cognitive systems.

Keywords: cryptographic protocols; bio-inspired cryptography; secret sharing algorithms

1 Introduction

The important and vital information is very often secret. These information need to be protected using modern cryptographic procedures and techniques. To guarantee the highest level of protection needed to be applied special kinds of security. Sometimes it may be a personalized cryptography, which use some personal o biometric pattern for security purposes.

Many methods of information secrecy include secret splitting techniques, secret sharing, secure information, individual human biometrics analysis [7-11]. The last one – the biometrics analysis include personal features, which are different for each person. The most important in such type of analysis is the ability to take into account the individual characteristics, for example personal biometrical features. Of course we can consider for such purpose both standard as well as non-standard biometric patterns.

The most important personal biometrics are following [11]:

- the DNA code,
- face/hand/foot geometry,
- the shape of fingerprints, of hand/foot bones,
- anatomical features of the face, hand, foot, iris,
- anatomical feature of the body,

- the structure of blood vessels.

The personal features are used to create crypto-biometrics secrecy. These type of secrecy is most important in many different kinds of IT systems [5, 6], but the particularly important in cognitive information systems, which may be applied for following tasks [11]:

- to sharing the secret information in enterprise,
- to splitting the strategic information in organization,
- to protection of confidential information.

The basic components of biometric analyses adopted in this paper are crypto-biometrics for the secrecy of information. The main content of this aspects can be a component for analysis, interpreting and mining managing processes [3, 4].

2 Data Security in Crypto-biometrics Model

Data security in crypto-biometrics models may be achieved using of one of the following algorithm [4, 9, 13, 14] :

- Lagrange'a algorithm,
- vector algorithm,
- Asmuth-Bloom algorithm,
- Karnin-Greene-Hellman algorithm,
- Ong-Schnorr-Shamir algorithm,
- ElGamal algorithm,
- Fiat-Shamir algorithm.

These cryptographic algorithms are used for information sharing and information splitting, and also to secure data by asymmetric encryption [2]. Among these procedures in particular information sharing protocols may be divided into the following groups [9, 14]:

- information sharing without the involvement of a trusted person,
- message sharing without disclosing one's parts,
- message sharing with disclosure prevention,
- message sharing with cheaters,
- message sharing with testing,
- message sharing with a share withdrawal.

Cryptographic algorithms of data sharing and splitting are used to construct the data security model. Such models are used to secure of encrypted or divided data.
The essence of this kind of models is application of biometric features to sharing and reconstruction of information [9, 12]. Some of the data security algorithms are based on the use of linguistics algorithms for data interpretation, analysis, and understanding, before its encryption and distribution. Information sharing and information split-

ting approaches may use mathematical linguistics formalisms especially during coding processes. The main idea of this approach is used to linguistics formalism to process of data encryption [1, 7], especially sequence, tree and grammatical formalisms. Such formalism are used to record and interpret the meaning of the analyzed biometric data.

Individual biometric features are used for example in DNA cryptography. DNA cryptography may be used to generate keys based on DNA codes and personal information. It should be noted that DNA molecules, which have existed in nature as long as known life forms, are beginning to play 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 steganography.

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 Benett published a paper in which he proposed a model of a programmable molecular computer capable of executing any algorithm. However, the first successful attempts were made 20 years after this idea publication. In 1993, Leonard Adleman became the first to execute calculations using a DNA computer and solved the Hamilton path problem for several cities [1].

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 1. One can also start from the assumption that one pair of nucleotides (a single bond) corresponds to one bit of information.

Such information coding methods are used in biological solutions which have inspired us to development of a new class of algorithms for secret splitting described in [10]. However, presented algorithm, called a 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. 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 [9, 10, 11].

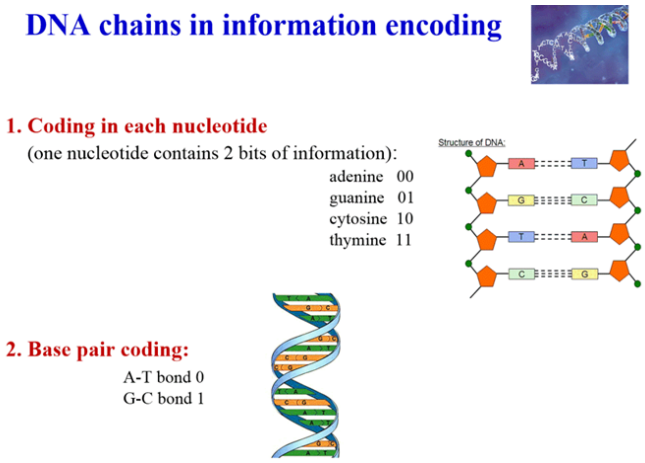

Fig. 1. Possible methods of coding information using DNA molecules

Thus, crypto-biometrics models based on DNA encoding and others biometric patterns are used to:

- secret sharing and secret splitting,
- secure information,
- encoding of information by individual biometrics feature,
- decoding information by personal biometrics feature,
- secure information prior to the disclosure to others person.

The secret and confidential information is analyzed and interpreted by way of cryptographic information analyses. The authors of this paper proposed to use the crypto-biometrics analysis to strategic information management in enterprises.

3 Crypto-biometrics Model for Strategic Information Management

Strategic business data require special protection, therefore they must be protected from disclosure. The methods of strategic data sharing in the enterprise presents Fig.2. Strategic data are splitting by used one of the cryptographic algorithms used to splitting processes. Consequently in this process information is divided into a number of parts of this information. Each of them is assigned to another holder. And no other person knows the other parts of strategic data. Therefore data are protected. To reproduce the strategic information is necessary to submit a certain number of them. Not necessarily all parts of divided strategic information. The number of necessary parts of strategic information needed to reproduced specifies the algorithm that was used to divide strategic information.

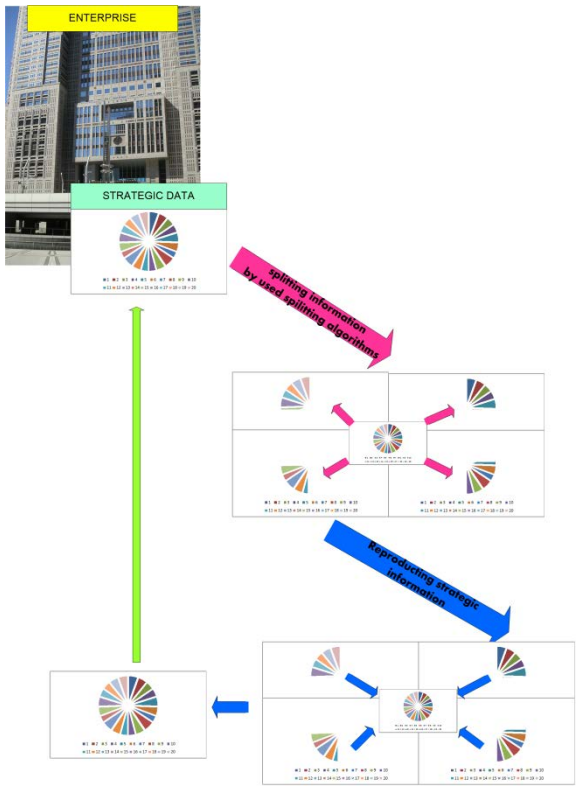

Fig. 2. The process of sharing strategic information in enterprise

The strategic information management in enterprise present Fig. 3.

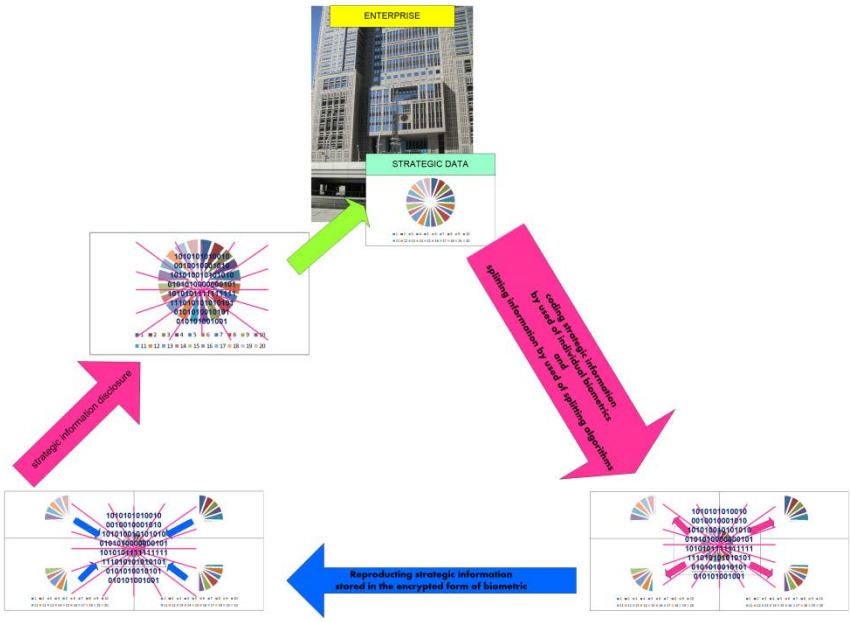

Fig. 3. The process of crypto-biometrics model for strategic information management in enterprise

In this process the most important is stage of coding strategic information using personal biometrics feature. The biometrics features are different for different persons or kinds of biometrics. The encoded strategic information by one of the personal biometric is shared between the participants of procedure. In this way the information is not only divided, but also encoded. Reproduction of information therefore requires:

- submit an appropriate amount of parts shared information,
- disclosure of key biometric that was used to encode information.

Crypto-biometrics models therefore protected by algorithms of secret sharing and biometrics keys.

4 Conclusions

Crypto-biometrics models are currently used to ensure security of different kinds of information, especially strategic information in organization. Strategic information management is often understood as management secret information. Ensure secrecy of strategic information is the responsibility of crypto-biometrics systems. The advantages of the proposed systems is:

- guarantee the security of strategic information,
- safety features during performing secret distribution,

- dividing important strategic data and assigning its shares to members of the authorized group,
- handle any digital data which needs to be intelligently divided among authorized persons and then possible to secretly reconstruct,
- used in different economical management structures e.g. hierarchical, divisional, functional etc.

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. Adleman LM, Rothemund PWK, Roweiss S, et al. (1999) On applying molecular computation to the Data Encryption Standard, Journal of Computational Biology, 6(1):53－63
2. Blakley GR (1979) Safeguarding Cryptographic Keys, Proceedings of the National Computer Conference:313–317
3. Chomsky N (1957) Syntactic Structures, London Mouton
4. Menezes A, van Oorschot P, Vanstone S (2001) Handbook of Applied Cryptography, Waterloo, CRC Press
5. Ogiela L (2010) Cognitive Informatics in Automatic Pattern Understanding and Cognitive Information Systems, in: Wang YX, Zhang D, Kinsner W (Eds.), Advances in Cognitive Informatics and Cognitive Computing, Studies in Computational Intelligence 323:209-226
6. Ogiela L, Ogiela MR (2012) Advences in Cognitive Information Systems, COSMOS 17, Springer-Verlag, Berlin-Heidelberg
7. Ogiela MR, Ogiela U (2009) Security of Linguistic Threshold Schemes in Multimedia Systems, in: Damiani E, Jeong J, Howlett RJ, Jain LC (Eds.), New Directions in Intelligent Interactive Multimedia Systems and Services 2, Studies in Computational Intelligence 226, Berlin Heidelberg, Springer Verlag:13–20
8. Ogiela MR, Ogiela U (2009) Shadow Generation Protocol in Linguistic Threshold Schemes, in: D. Ślęzak, T.-h. Kim, W.-C. Fang, K. P. Arnett (Eds.), Security Technology: Communication in Computer and Information Science 58, Berlin Heidelberg, Springer Verlag:35-42
9. Ogiela MR, Ogiela U (2010) The use of mathematical linguistic methods in creating secret sharing threshold algorithms, Computers and Mathematics with Applications 60(2):267-271
10. Ogiela MR, Ogiela U (2012) DNA-like linguistic secret sharing for strategic information systems, International Journal of Information Management 32:175–181
11. Ogiela MR, Ogiela U (2012) Linguistic Protocols for Secure Information Management and Sharing, Computers and Mathematics with Applications 63(2):564-572
12. Peters W (2011) Representing Humans in System Security Models: An Actor-Network Approach. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 2(1):75-92
13. Shamir A (1979) How to Share a Secret, Communications of the ACM:612–613
14. Tang S (2004) Simple Secret Sharing and Threshold RSA Signature Schemes, Journal of Information and Computational Science 1:259–262