Secure Information Sharing Using Personal Biometric Characteristics

Marek R. Ogiela, Urszula Ogiela, and Lidia Ogiela

AGH University of Science and Technology
Al. Mickiewicza 30, PL-30-059 Krakow, Poland
{mogiela,ogiela,logiela}@agh.edu.pl

Abstract. In this publication will be proposed a new algorithm for secure information sharing using personal or biometric information. In classic cryptographic threshold schemes used for secret splitting or sharing there aren't any connection between generated shares and particular participants of communication protocol. Sometimes it may be worth to generate personalized shadows, which allow not only recovery the original information or secret data, but also to identify who exactly took part in the secret reconstruction procedure. In the paper will be described the way of extraction some personal or biometric characteristics using cognitive information systems, as well as the algorithm of application such personal information for shadow generation in threshold schemes. Such new approach may play a great role in intelligent distributed computing or secure urban life.

Keywords: security of distributed information, cryptography, Urban Life, personal identification processes, information sharing.

1 Introduction

There are various methods of concealing (classifying) information and protecting it from being accessed by persons not authorised to learn it. They include secret splitting techniques. In this paper, the secret will consist of individual human biometrics, which include physical features. The most important physical features used for the biometric/identification analysis are the features of the iris, the shape of fingerprints, of hand/foot bones [6, 7], anatomical features of the face, the structure of blood vessels (including coronary ones) [5] and the DNA code [11].

The basic components of biometric analyses adopted in this paper are the features of the iris, which also determine the eye colour which is material for the verification analysis in biometric systems. The following factors determine the eye colour:

- the melanin content of pigments in the iris epithelium,
- the melanin content of the stroma of the iris,
- the density of cells in the stroma of the iris.

The melanin content of the iris can be a component for recognition processes executed as part of processes of information concealment (by splitting information into parts of the secret) after the stage of the proper personal verification.

T.-h. Kim et al. (Eds.): MulGraB/BSBT/IUrC 2012, CCIS 353, pp. 369–373, 2012.

2 Information Splitting and Sharing

In their research, the authors of this paper have assumed that the information sharing methods are based on the use of one of the following three algorithm types [1-4, 8-13]:

- vector algorithm,
- Asmuth-Bloom algorithm,
- Karnin-Greene-Hellman algorithm.

Information sharing protocols, in turn, are split into the following groups [4, 8-11]:

- 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.

Information splitting algorithms dealing with concealing biometric information contained in the iris can be executed by two mutually independent ways of data splitting – both by a layer split and by a hierarchical split. The former means splitting the information between n secret holders and its reproduction by n-m trustees of the secret (from the same group). The latter case means that the secret is split between n holders of the secret, but the information can be reproduced by superior groups of secret holders within which the specific secret has been split into k parts (k < n). Thus the splitting methods depend on the purpose for which the information is split and concealed. In the case of personal identification systems or recognition systems, the methods of biometric data splitting most frequently used are layer splits (Fig. 1).

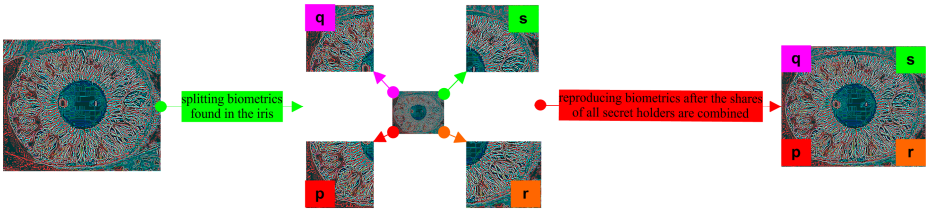

Fig. 1. Biometric information splitting

The presented information splitting and sharing methods and algorithms are based on the use of mathematical algorithms for data analysis and transmission. The information constituting the secret and the confidential information is analysed and interpreted by way of cryptographic information analyses.

3 Linguistic Coding in DNA Cryptography

Linguistic coding processes are based on the use of mathematical linguistic formalisms, particularly grammatical formalisms to record and interpret the meaning of the analysed biometric data. Linguistic coding processes are used because of the ability to execute generalised information coding as in DNA cryptography. In the traditional DNA coding model, one- or two-bit coding is used (utilising one of the four nitrogen bases, i.e. A, C, G, T or of the A-T and G-C bridges). DNA cryptography used to generate keys based on DNA codes and genetic/personal information can be combined with biometric features. The nucleotide polymer (DNA) is made up of purine bases are bonded in pairs [5]:

A-T, G-C, T-A, C-G

The bonding between purine and pyrimidine basses allows the DNA code to be written in an unanimous form, and the DNA code itself can be used for personal biometric characteristics.

In linguistic coding, it is possible to code longer bit sequences containing more than 2 bits of information. This coding is done using terminal symbols introduced in this grammar, and lengthening the coded blocks directly proportionally contributes to accelerating information splitting and reproduction, as well as to increasing the secret component containing information on the grammar used. The formal notation of a sequential grammar used to split information about the iris biometrics is as follows [11]:

$$G_{bi} = (N_{bi}, T_{bi}, P_{bi}, ST)$$

where:
N_{bi} = {IRIS, BIT, 1B, 2B, 3B, 4B, 5B, 6B, …, NB} – non-terminal symbols,
T_{bi} = {1b, 2b, 3b, 4b, 5b, 6b, …, nb, Ø} – terminal symbols containing defined *n*-bit blocks,
{Ø} – an empty symbol,
ST = IRIS – the start symbol,
P_{bi} – the production set:

1.IRIS → BIT BIT
2.BIT → 1B | 2B | 3B | 4B | 5B | 6B, … | NB
3.BIT → Ø
4.1B → 1b {0, 1}
5.2B → 2b {00, 01, 10, 11}
6.3B → 3b {000, 001, 010, 011, 100, 101, 110, 111}
7.4B → 4b
8. ……
9.NB → nb
10. b → {0, 1}

Linguistic information splitting and coding methods are presented in Fig. 2.

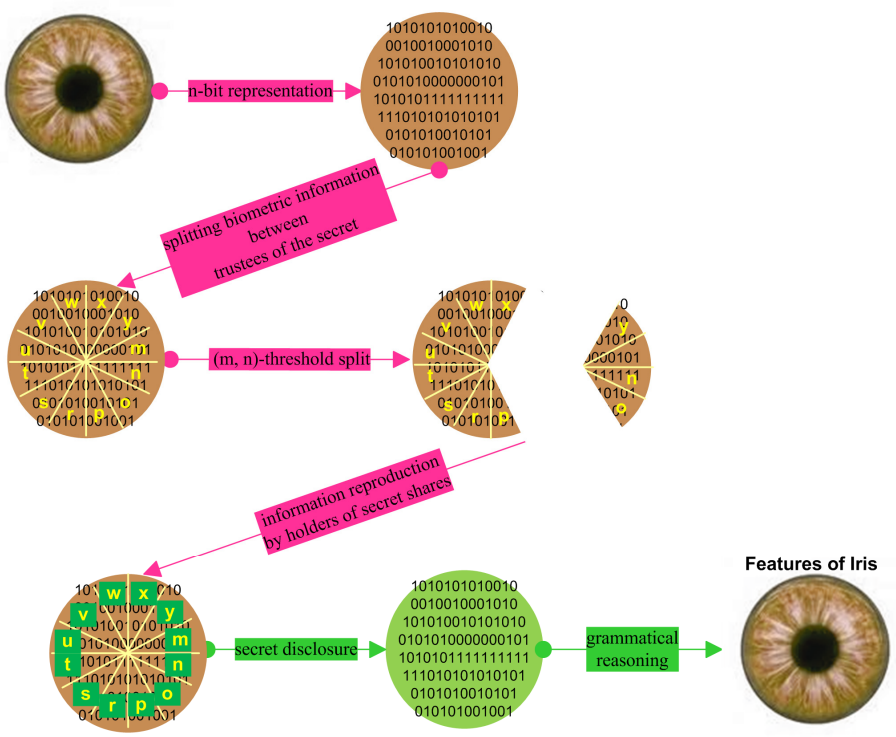

Fig. 2. Linguistic coding in the process of biometric information splitting

The coded biometric information recorded in the form of an n-bit representation is split using a selected information splitting algorithm. The (m, n)-threshold split allows this information to be reproduced by combining at least *m* of all *n* shares of the secret. Combining m shares of the secret causes the information to be reproduced in a coded version which can be fully understood only after executing its semantic analysis consisting in a grammatical reasoning carried out for the coded data set.

4 Conclusion

Processes of concealing (classifying) data are currently used in many fields of life, science and research. Employing linguistic coding methods in the concealment processes offers the full capability of using semantic processes for the identification and grammatical reasoning. Concealing biometric data (specific for every person) constitutes a very important problem because it is highly probable that personal data will be taken over by unauthorised persons. The individual DNA code, fingerprints, iris features and many other biometrics represent protected data and as such a valuable source of information not just about the specific person, but also their origin (genetic information), environment, interests, habits etc. Methods of concealing biometric information concerning the iris can also

be used to split and conceal other sets of personal/biometric data due to the universal nature of linguistic methods.

Acknowledgement. This work has been supported by AGH University of Science and Technology research Grant No. 11.11.120.612.

References

1. Adleman, L.M., Rothemund, P.W.K., Roweiss, S., et al.: On applying molecular computation to the Data Encryption Standard. Journal of Computational Biology 6(1), 53–63 (1999)
2. Blakley, G.R.: Safeguarding Cryptographic Keys. In: Proceedings of the National Computer Conference, pp. 313–317 (1979)
3. Chomsky, N.: Syntactic Structures, London Mouton (1957)
4. Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. CRC Press, Waterloo (2001)
5. Ogiela L.: Semantic Analysis and Biological Modelling in Cognitive Categorization Systems. Mathematical and Computer Modelling (in press, 2013)
6. Ogiela, L., Ogiela, M.R.: Cognitive Techniques in Visual Data Interpretation. SCI, vol. 228. Springer, Heidelberg (2009)
7. Ogiela, L., Ogiela, M.R.: Advences in Cognitive Information Systems. COSMOS, vol. 17. Springer, Heidelberg (2012)
8. Ogiela, M.R., Ogiela, U.: Security of Linguistic Threshold Schemes in Multimedia Systems. In: Damiani, E., Jeong, J., Howlett, R.J., Jain, L.C. (eds.) New Directions in Intelligent Interactive Multimedia Systems and Services - 2. SCI, vol. 226, pp. 13–20. Springer, Heidelberg (2009)
9. Ogiela, M.R., Ogiela, U.: Shadow Generation Protocol in Linguistic Threshold Schemes. In: Ślęzak, D., Kim, T.-H., Fang, W.-C., Arnett, K.P. (eds.) SecTech 2009. CCIS, vol. 58, pp. 35–42. Springer, Heidelberg (2009)
10. Ogiela, M.R., Ogiela, U.: The use of mathematical linguistic methods in creating secret sharing threshold algorithms. Computers and Mathematics with Applications 60(2), 267–271 (2010)
11. Ogiela, M.R., Ogiela, U.: DNA-like linguistic secret sharing for strategic information systems. International Journal of Information Management 32, 175–181 (2012)
12. Ogiela, M.R., Ogiela, U.: Linguistic Protocols for Secure Information Management and Sharing. Computers and Mathematics with Applications 63(2), 564–572 (2012)
13. Shamir, A.: How to Share a Secret. Communications of the ACM, 612–613 (1979)
14. Tang, S.: Simple Secret Sharing and Threshold RSA Signature Schemes. Journal of Information and Computational Science 1, 259–262 (2004)