Strategic Information Splitting Using Biometric Patterns

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

Abstract

In this paper will be proposed a new algorithm for secure strategic information sharing using biometric information. In classic cryptographic threshold schemes used for secret splitting and sharing there aren't any connection between generated shares and particular participants of threshold protocol. In fact sometimes it may be useful to generate a special personalized shadows, which allow not only reveal the original secret information, but also to identify who is the owner of particular shares or information shadow.

Keywords: bio-cryptography, security of distributed information, personal identification processes, information sharing.

1 Introduction

There are many types of methods for classifying information and protecting it from being accessed by no authorized persons. They include threshold schemes sharing techniques [2] [4] [7] [1]. In this paper, the secret will consist of individual human biometrics or personal features. The most important features used for the biometric identification are the features of the iris, fingerprints, hand/foot bones [9], anatomical features of the face, the structure of blood vessels (including coronary ones) [5].
The basic components of biometric analyses adopted in this paper are the features of the iris as well as coronary arteries layouts, which is material for the verification analysis while revealing secret information [10].
Using such personal templates 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. The same role may play the information record containing some personal information about coronary vessels conditions and spatial topology. Such information may be extracted during medical examination for particular person [6].

2 Information Sharing Using Iris Features

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 (Figure 1).

Journal of Internet Services and Information Security (JISIS), volume: 2, number: 3/4, pp. 129-133
*Corresponding author: Tel: +48-12-617-38-54, Web: http://home.agh.edu.pl/~mogiela/

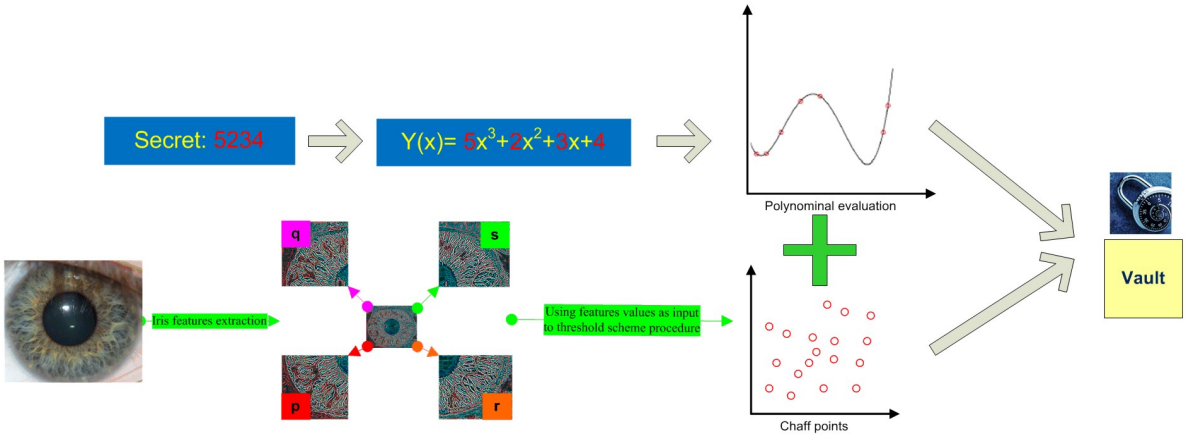

Figure 1: Biometric information splitting using fuzzy vaults approach

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 Information Sharing using Coronary Arteries Spatial Features

When coronary arteries visualisations are used for personal data extraction for secret sharing algorithm, the methodology of extracting individual features which may be used for information shares generation is as follows:

(1) 3D reconstructions of coronary vascularisation must be pre-processed as described in [3]. After a projection is obtained of the image showing all the characteristics of the coronary vascularisation, arteries are thinned to produce a skeleton of particular parts of heart vessels.

(2) A graph is then spanned on a skeleton thus obtained in the image, for which graph a graph grammar is defined. All points of skeleton ramification are represented by graph peaks, while the sections of arteries connecting them are approximated by graph edges. Introducing this representation allows a unique graph to be created for every visualisation, which graph describes the individual features using particular peaks, their number, relative location (directions and distances etc.)[3]. An example graph representation of the coronary vascularisation is presented in Figure 2. The graph structure created in this way will describe the spatial topology of the heart muscle vascularisation including its possible morphological changes.

(3) Each coronary vascularisation artery defined by graph edges is analysed to determine the morphometric parameters of these selected sections and assess the possible reduction of the inside diameter of these arteries. In addition, it is possible to calculate the value of selected shape ratios describing the directions or curves of the analysed arteries.

The obtained vector of features describing all structures of coronary vessels can then be recoded into a personal information vector, which may used for secret sharing.

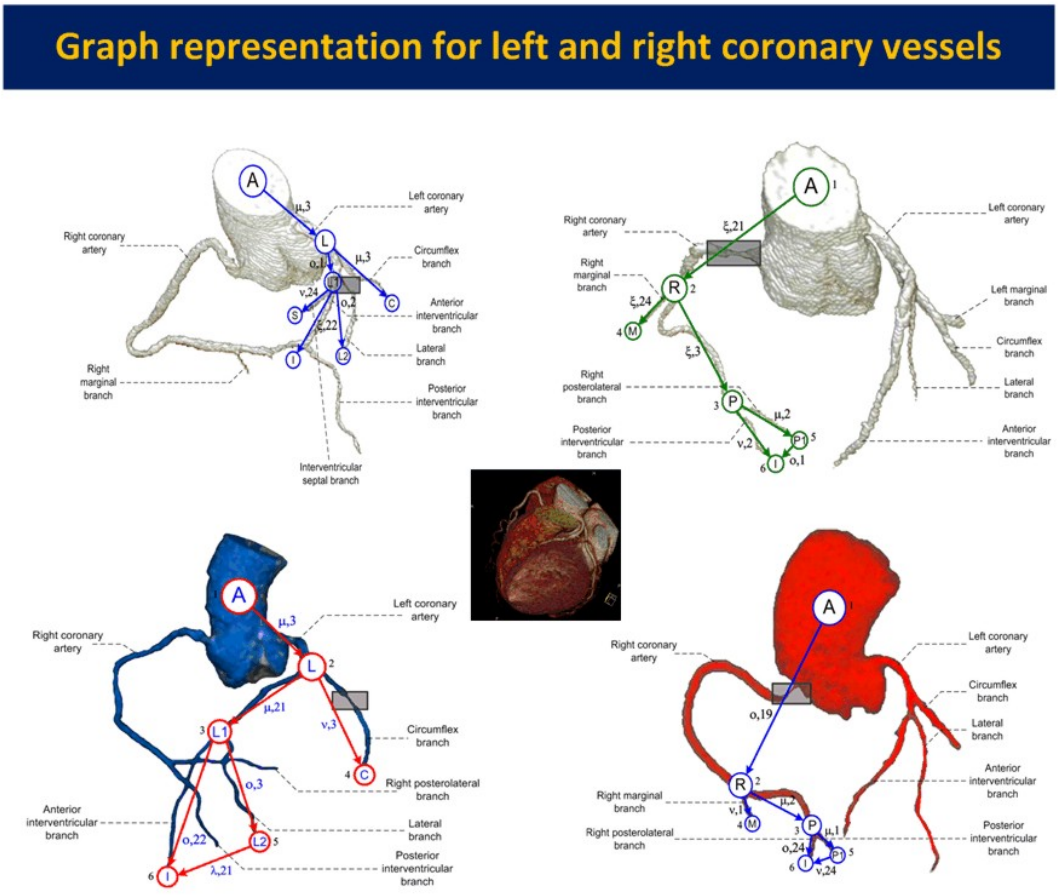

Figure 2: The graph representations of the right and the left coronary arteries

4 Conclusion

Secret splitting and sharing techniques are currently used in many areas of life, science and research. Employing biometric or personal information coding methods in the shadow generation processes offers the full capability of using personal unique features for the identification of participants of secure communication protocol.

Using biometric data or information specific for every person, constitutes a very important problem because it is highly probable that personal data will be taken over by unauthorised persons. Techniques of concealing biometric information concerning the iris templates as well as coronary arteries features can also be used to split and conceal other sets of personal/biometric data due to the universal nature of secret sharing threshold schemes [8].

Acknowledgement

This work has been supported by the National Science Centre, Republic of Poland, under project number N N516 478940.

References

[1] S. A. How to share a secret. *Communications of the ACM*, 22(11):612–613, November 1979.

[2] B. G.R. Safeguarding cryptographic keys. In *Proc. of the National Computer Conference, New York, USA*, pages 313–317, June 1979.

[3] T. M. Graph image language techniques supporting advanced classification and cognitive interpretation of CT coronary vessel visualizations. *Computational Intelligence Paradigms in Advanced Pattern Classification*, 386(1):89–111, 2012.

[4] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[5] L. Ogiela and M. Ogiela. *Cognitive Techniques in Visual Data Interpretation*. Springer, 2009.

[6] L. Ogiela and M. Ogiela. *Advences in Cognitive Information Systems*. Springer, 2012.

[7] M. Ogiela and U. Ogiela. Security of linguistic threshold schemes in multimedia systems. *New Directions in Intelligent Interactive Multimedia Systems and Services - 2*, 226(1):13–20, 2009.

[8] M. Ogiela and U. Ogiela. The use of mathematical linguistic methods in creating secret sharing threshold algorithms. *Advances in Cryptography, Security and Applications for Future Computer Science*, 60(2):267–271, July 2010.

[9] M. Ogiela and U. Ogiela. DNA-like linguistic secret sharing for strategic information systems. *International Journal of Information Management*, 32(2):175–181, April 2012.

[10] M. Ogiela and U. Ogiela. Linguistic protocols for secure information management and sharing. *Computers & Mathematics with Applications*, 63(2):564–572, January 2012.

Marek R. Ogiela works at the AGH University of Science and Technology in Krakow. In 1992 graduated from the Mathematics and Physics Department at the Jagiellonian University. In 1996 for his honours doctoral thesis on syntactic methods of analysis and image recognition he was awarded the title of Doctor of Control Engineering and Robotics at the Faculty of Electrical, Automatic Control, Computer Science and Electronic Engineering of the AGH University of Science and Technology. In 2001 he was awarded the title of Doctor Habilitated in Computer Science for his research on medical image automatic analysis and understanding. In 2005 he received a professor title in technical sciences. Member of numerous world scientific associations (IEEE-Senior Member, SPIE-Senior Member, SIIM etc.) as well as of the Forecast Committee 'Poland 2000 Plus' of the Polish Academy of Science and member of Interdisciplinary Scientific Committee of the Polish Academy of Arts and Sciences (Bio cybernetics and Biomedical Engineering Section in years 2003-2011). Author of more than 220 scientific international publications on pattern recognition and image understanding, artificial intelligence, IT systems and biocybernetics. Author of recognised monographs in the field of cryptography and IT techniques; author of an innovative approach to cognitive medical image analysis. For his achievements in these fields he was awarded many prestigious scientific honors, including Prof. Takliński's award (twice) and the first winner of Prof. Engel's award.

Lidia Ogiela received Master of Science in mathematics from the Pedagogical University in Krakow, and Master of Business Administration in management and marketing from AGH University of Science and Technology in Krakow, both in 2000. In 2005 she was awarded the title of Doctor of Computer Science and Engineering at the Faculty of Electrical, Automatic Control, Computer Science and Electronic Engineering of the AGH University of Science and Technology, for her thesis and research on cognitive analysis techniques and its application in intelligent information systems. She is an author a few dozen of scientific international publications on information systems, cognitive analysis techniques, biomedical engineering, and computational intelligence methods. She is a member

of few prestigious international scientific societies as: SIAM – Society for Industrial and Applied Mathematics, as well as SPIE – The International Society for Optical Engineering, CSS – Cognitive Science Society. Currently she is at the associate professor position, and works in Faculty of Management at the AGH University of Science and Technology.

Urszula Ogiela received Master of Science degree and Master of Business Administration in Information Management from AGH University of Science and Technology in Krakow in 2002. Currently she is a Ph.D. student at Krakow University of Economics, and works at the AGH University of Science and Technology, leading her research on linguistic aspect of information data sharing, as well as grammar extensions for secret splitting threshold protocols.