Personal Information in Strategic Data Sharing and Communication Protocols

Lidia Ogiela and Marek R. Ogiela
Cryptography and Cognitive Informatics Research Group, AGH University of Science and Technology, 30 Mickiewicza Ave., 30-059 Krakow, Poland
Email: {logiela, mogiela}@agh.edu.pl

***Abstract*—One of the most important areas of application of biometric patterns or personal information is security purposes. Personal information or individual characteristics may be applied not only for authentication purposed, but also in advanced protocols dedicated for strategic information sharing and distribution. Such techniques allow joining unique personal data with encryption and secret data management processes. In this paper will be described such protocols, which enable reconstruction of secured information exclusively by authorized parties, which received accessing grants for secret information reconstruction.**

***Index Terms*—biometric patterns in cryptography, cryptographic protocols, secret splitting and sharing, strategic data**

I. Introduction

Application of personal information/data in secret sharing algorithms is very important among cryptographic protocols and secure data techniques. The cryptographic algorithms for securing information generally focus around two kinds of algorithms: data splitting and data sharing protocols. Data splitting protocols is always connected with distribution of generated information parts between selected groups of persons called secret trustees. Data splitting and sharing protocols usually divide secure information, data sets or strategic data, communication protocols into *n* parts or secure shares. The secret splitting algorithms were discussed in [1]-[5]. Secret sharing algorithms were discussed in [6]-[8]. The sharing protocols were dedicated to many kind of digital information [4], [5], [8]-[10]. The sharing protocols dedicated to data secret was described in [10], to manage information in business protocols or management processes [2], [3], [11], to distribute strategic information [7], and also for homeland security purposes [1].

A new aspect of information sharing protocols is a personal and biometric marking of shared strategic data, authorized parties, communication protocols. Such biometric tagging allows assigning particular data to the selected person. The one of the personal and biometric analysis is the hand analysis. In this kind of analysis are two different aspects:

- The hand geometry analysis – the analysis of the shape of the hand,
- The hand biometric analysis,
- The analysis of the characteristics of writings.

The different kinds of analysis of hand characteristics are very important in cryptography.

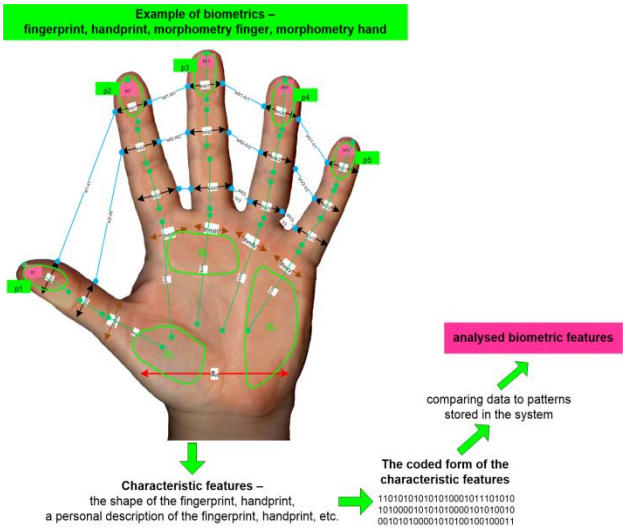

Figure 1. The biometric verification process.

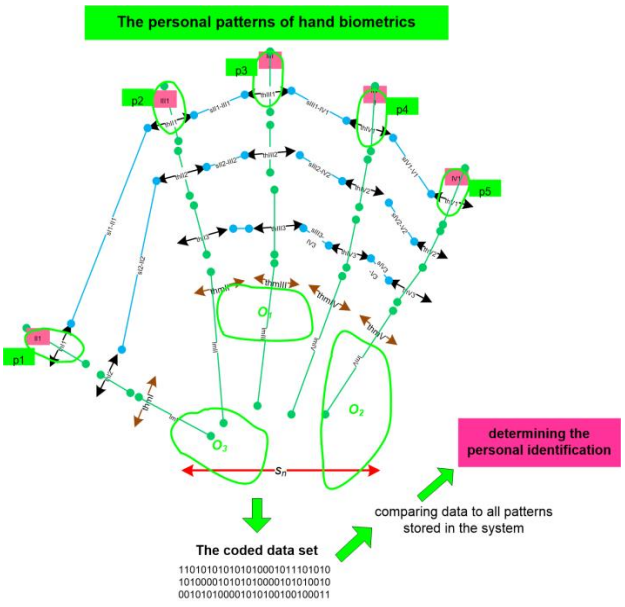

Figure 2. The personal identification scheme.

Manuscript received July 12, 2015; revised November 26, 2015.

doi: 10.18178/lnit.3.2.75-80

For biometric and personal verification and identification processes may be use different types of biometric patterns. Each biometrics is dependent on the type of biometrics features and is unique for each person. The analysis of personal characteristics is very important in personal authentication processes. Such analysis is the kind of verification processes (Fig. 1) or identification processes (Fig. 2).

The personal verification system may analyze selected biometrics and evaluate characteristic features. Such characteristic features or personal biometrics may be also coded, and compared to patterns stored in the system or database. During the verification analysis system should evaluate and compared the most important features which belong to the particular person.

The identification procedure also analyzes the coded patterns which may contain personal biometric. The coded biometrics data may be compared to the all patterns stored in the identification system. The result of such analysis is information who the person is.

The personal analysis is based on using biometric features characteristic for:

- The hand features,
- The face [12],
- The voice.

In this publication authors describe the first example of using personal features – the hand geometrics and biometrics. The characteristic features of the human hand are dedicated to describe and interpret individual parameters in personal data evaluation processes [13]. In this process we describe human hand components (Fig. 3).

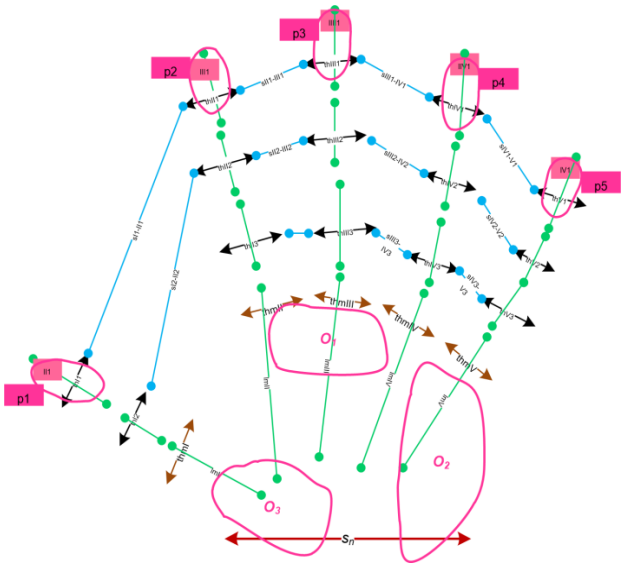

Figure 3. The typical hand biometrics. Source: [13].

We defined the set with the human hand parameters [13]:

$$B\text{-}L_h = \{th_{ij}, l_{ij}, s_{ij\text{-}ij}, th_{mi}, l_{mi}, s_n, p_i, o_j\}$$

where:

th_{ij} – is the thickness of the bones of the i^{th} finger and the j^{th} phalanx,

l_{ij} – is the length of the bones of the i^{th} finger and the j^{th} phalanx,

$s_{ij\text{-}ij}$ – denotes the size of areas between individual hand bones,

th_{mi} – denotes the thickness of the i^{th} metacarpus bone,

l_{mi} – denotes the length of the i^{th} metacarpus bone,

s_n – denotes the size of wrist bones,

p_i – is the print of the i^{th} finger of the hand,

o_j – is the shape of one of the three biometric prints of the palm,

for the $B\text{-}L_h$ set:

i = {I, II, III, IV, V},

j = {1, 2, 3}.

The personal analysis of the hand assesses:

- The hand geometrical features:
  - The length of the fingers,
  - The thickness of the fingers,
  - The number of fingers,
  - The spacing of the fingers,
- The hand biometrics features:
  - The shape of the fingerprint,
  - The shape of the handprint,
  - The biometrics features of the fingers,
  - The biometrics features of the hand.

This type of personal analysis is used to secure of strategic data.

The most important kind of personal analysis is also the handwriting analysis. The personal features are also characteristic and included in the process of writing. The personal kinds of writing allow identifying the person who wrote the text. In the process of analysis is determined the characteristic features of the individual (personal) signature. The characteristics features are defined as characteristics points of the signature (Fig. 4).

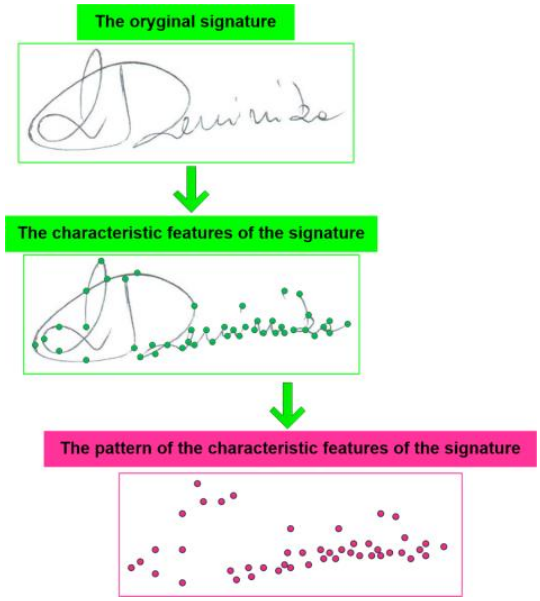

Figure 4. The characteristic features of the personal signature.

Characteristic features of the signature (writing) form the basis for executing individual analysis, personal identification and verification, the correct personal recognition.

The personal hand analysis, the individual fingerprint and the signature analysis are the kinds of personal

analysis. These kinds of analysis are very important for the verification and identification processes. The verification and identification processes are used in cryptographic protocols reproducing the secret data. As example of secret data are the strategic data (in enterprises, in organizations, etc.). Strategic data management it requires the use cryptographic protocols for secure information.

II. Secret Sharing Protocols for Secure Strategic Information

Secret sharing protocols are dedicated to divided important information. One of the types of secret data is the strategic data. This kind of data is very important in enterprises or organizations. In cryptographic protocols the strategic information is divided between a fixed number of participants of protocols.

The strategic information I is divided between n secret shares. Each of participants may receive one of generated parts of divided secret. Thus disclosing a single fragment of the divided information poses no threat to the security of the entire data set. Trustees of the divided secret store the information until it becomes necessary to reproduce and disclose it. This process differs for data splitting and sharing algorithms.

Data splitting algorithms require combining all existed shares to reproduce the original information. If a less number of shares are combined, secret I will not be discovered. On the other side data sharing algorithms require combining only particular number of shares to reproduce original information. Of course the number of secret shares required to reproduce information I depends on what information sharing scheme is selected. Solutions of this type are known as (m, n)-threshold schemes, where the number n denotes the number of shares into which information I will be divided, while the number m represents the number of shares absolutely required to reproduce information I [1], [8], [11], [14].

Fig. 5 shows the information splitting and sharing method.

To restore original information, splitting algorithms require that all shares of the split secret be combined, while data sharing algorithms only require a selected number of them. From the point of view of information management, data sharing algorithms are more convenient and universal to perform efficient information management [7], [15]. They make it possible to reproduce the information without all trustees of the secret having to participate. Even if some secret parts are excluded from the protocol, the shared message can still be restored, which would be impossible in a data splitting algorithm. If a selected share of the secret is accidentally or intentionally obtained in data splitting algorithms and thus poses the threat that the secret information will be revealed to unauthorized individuals, there is the danger that the information may be revealed in an uncertain situation. In the case of information sharing algorithms, it is possible to exclude a suspected or just unreliable person whose loyalty is in any doubt [15].

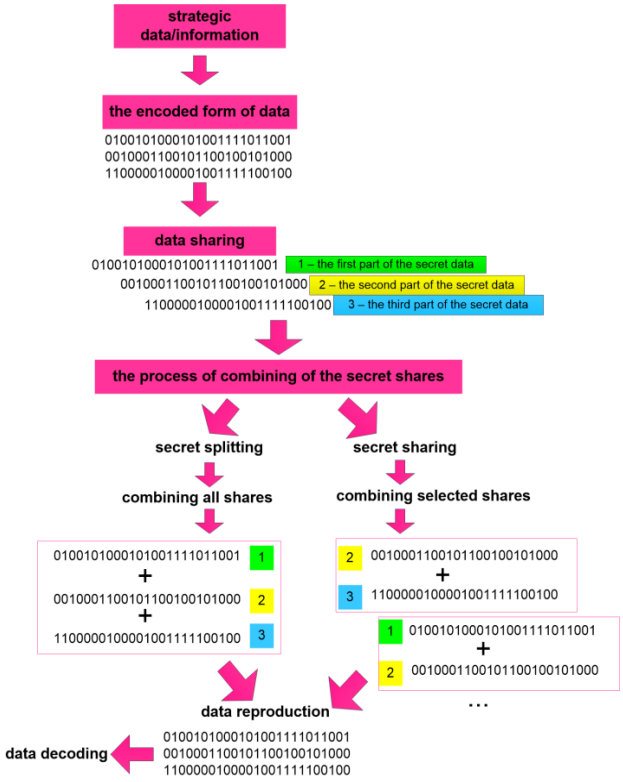

Figure 5. The secret data splitting and sharing scheme.

The most important and useful cryptographic algorithms for secure secret information are the Shamir's and Tang's algorithms [4], [5].

Shamir's algorithm presents the operation of a threshold scheme based on Lagrange's interpolating polynomial [4], [8]. This algorithm allows generating particular number of secret parts with equal accessing grants.

Tang's algorithm [5] allows generating shares with different accessing grants. This method has the extremely interesting property that if there is a certain number smaller than requested threshold k, some of the sets of obtained shadows are enough to reconstruct the secret, whereas other ones are insufficient. Thus we have a situation in which certain parts are more privileged and by themselves allow you to reconstruct the information even though they are less numerous than the required number of standard parts.

Due to such feature this algorithm can be used to construct much more complex schemes, e.g. hierarchical ones.

III. Personal Verification in Strategic Secret Sharing Protocols

In this section we present a new scheme of signature tagging in data sharing protocols. The secret information divided using sharing algorithms may be marked at two levels:

- Level of splitting secret strategic information,
- Level of combining all shares of data splitting,
- Level of combining selected shares of data sharing.

This situation presents Fig. 6.

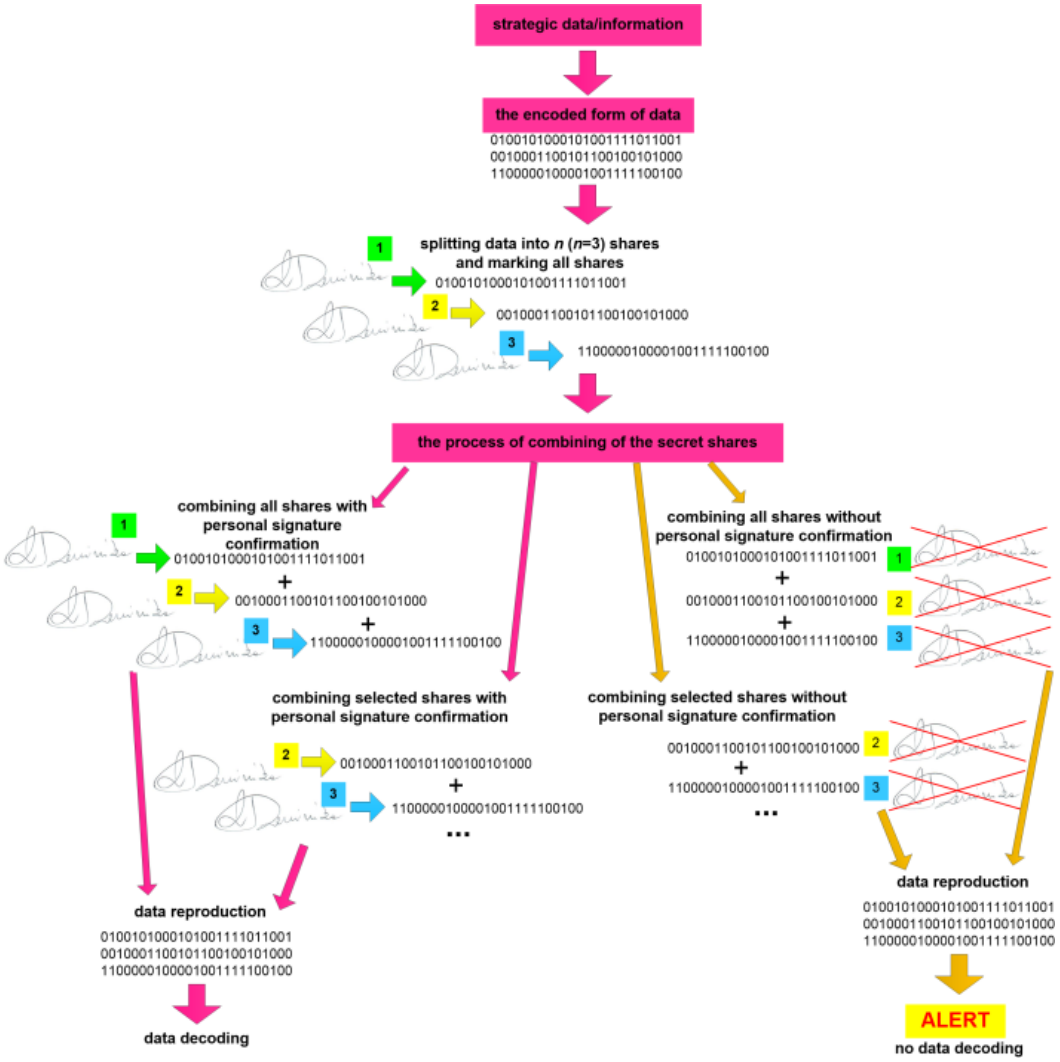

Figure 6. The personal signature verification in strategic data sharing and communication protocols.

The personal signature as a one of kind of the human characteristics, may be applied in strategic secret sharing protocols, and determine the secure of strategic information. Secret data (strategic information) divining into *n* shares, and combining process from shares with personal authentication. The strategic data sharing is very useful for information management processes and communication between each of users of protocols.

The second kind of personal verification processes is the personal hand or palm characteristics verification. In the splitting data processes each shares are marking by the individual hand characteristics. Also in the combining processes with all or selected shares, it's a very important to confirm authentication of person (Fig. 7).

The personal verification protocols are possible to reproduce the divided strategic secrets, and decoding them. When in process of combing shares no signature confirmation was included, then it isn't possible to perform strategic information decoding. The signature confirmation process may be used in strategic secret splitting and sharing in hierarchical, divisional or mixed structure. The personal confirmation of data sharing can be also use in strategic data management processes and communication protocols.

The communication protocols in management processes are for example:

- The interpersonal communication protocols,
- The cryptographic secret protocols,
- The secret data transfer protocols.

Each of secret strategic data can be marking in sharing processes. Such marking serves to [12]:

- Protect secret information,
- Efficient management of secure information.

IV. Conclusions

In this paper we have presented new solutions for application some selected biometric patterns in creation of secret sharing cryptographic protocols. This solution is especially dedicated for sharing strategic information and distribution of secret parts [16]. Such methods allow protecting confidential data, as well as performing intelligent and hierarchical information management in different decision structures. Development of such algorithms will enable reconstruction of shared data exclusively by authorized parties, which received accessing grants for secret information reconstruction.

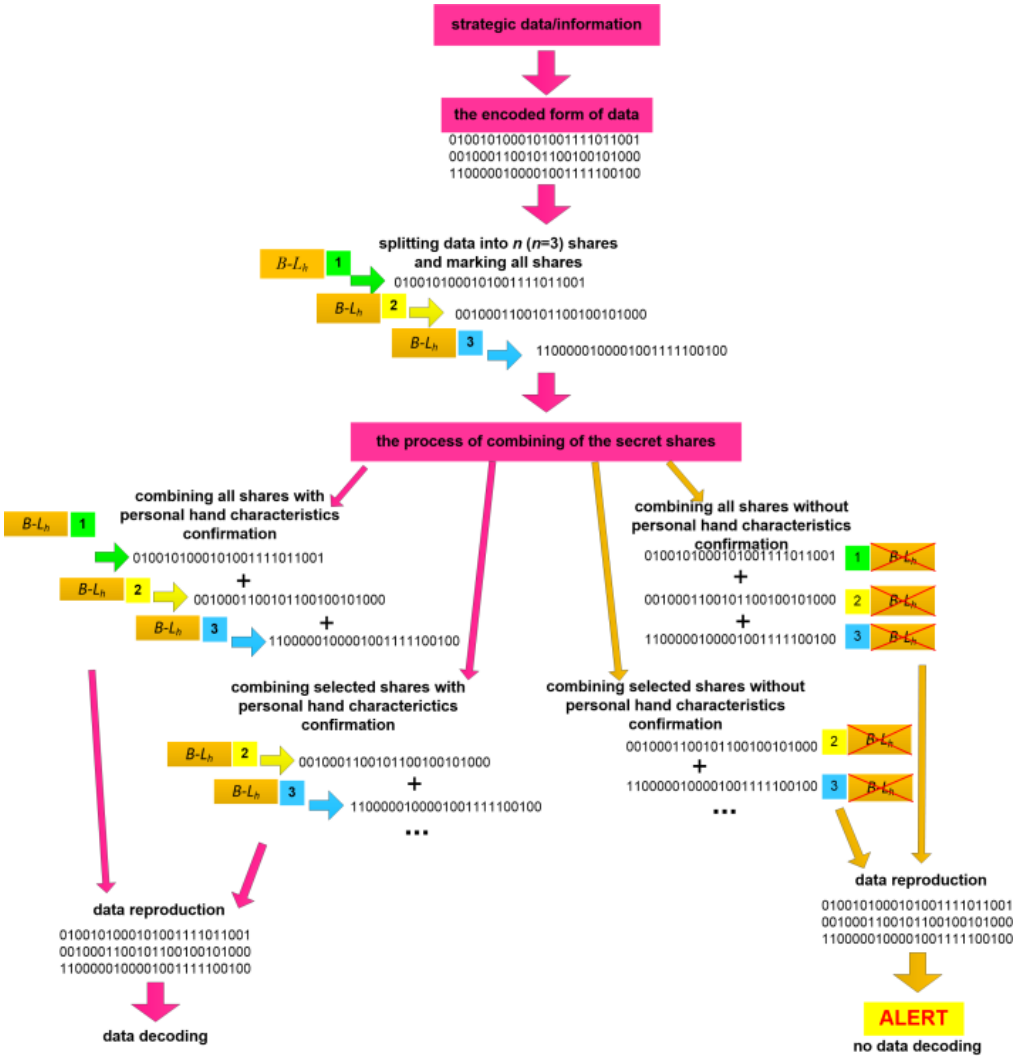

Figure 7. The personal hand characteristics verification in strategic data sharing and communication protocols.

ACKNOWLEDGMENT

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

REFERENCES

[1] L Ogiela and M. R. Ogiela, "Cognitive systems and bio-inspired computing in homeland security," *Journal of Network and Computer Applications*, vol. 38, pp. 34-42, 2014.

[2] M. R. Ogiela, L. Ogiela, and U. Ogiela, "Cryptographic techniques in advanced information management," in *Proc. Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Birmingham, UK, 2014, pp. 254-257.

[3] M. R. Ogiela, L. Ogiela, and U. Ogiela, "Security and privacy in distributed information management," in *Proc. 6th International Conference on Intelligent Networking and Collaborative Systems*, Salerno, Italy, September 10-12, 2014, pp. 73-78.

[4] A. Shamir, "How to share a secret," *Communications of the ACM*, pp. 612-613, 1979.

[5] S. Tang, "Simple secret sharing and threshold RSA signature schemes," *Journal of Information and Computational Science*, vol. 1, pp. 259-262, 2004.

[6] M. R. Ogiela and U. Ogiela, "The use of mathematical linguistic methods in creating secret sharing threshold algorithms," *Computers & Mathematics with Applications*, vol. 60, no. 2, pp. 267-271, 2010.

[7] M. R. Ogiela and U. Ogiela, "DNA-Like linguistic secret sharing for strategic information systems," *International Journal of Information Management*, vol. 32, no. 2, pp. 175-181, 2012.

[8] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley, 1996.

[9] T. Hachaj and M. R. Ogiela, "A system for detecting and describing pathological changes using dynamic perfusion computer tomography brain maps," *Computers in Biology and Medicine*, vo. 41, no. 6, pp. 402-410, 2011.

[10] L. Ogiela and M. R. Ogiela, "Semantic analysis processes in advanced pattern understanding systems," in *Advanced Computer Science and Information Technology*, T. Kim, H. Adeli, R. J. Robles, and M. Balitanas, Eds., Heidelberg: Springer-Verlag, 2011, pp. 26-30.

[11] M. R. Ogiela and U. Ogiela, "Linguistic protocols for secure information management and sharing," *Computers & Mathematics with Applications*, vol. 63, no. 2, pp. 564-572, 2012.

[12] M. R. Ogiela, L. Ogiela, and U. Ogiela, "Biometric methods for advanced strategic data sharing protocols," in *Proc. 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Blumenau, Santa Catarina, Brazil, July 2015, pp. 179-183.

[13] L. Ogiela, "Semantic analysis and biological modeling in selected classes of cognitive information systems," *Mathematical and Computer Modelling*, vol. 58, pp. 1405-1414, 2013.

[14] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. National Computer Conference*, 1979, pp. 313-317.

[15] M. R. Ogiela and U. Ogiela, "Secure information management using linguistic threshold approach," in *Advanced Information and Knowledge Processing*, London: Springer-Verlag, 2014.

[16] A. Beimel and B. Chor, "Universally ideal secret sharing schemes," *IEEE Transactions on Information Theory*, vol. 40, pp. 786-794, 1994.

Dr. Lidia Ogiela is computer scientist, mathematician, and economist. She 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 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 author of a few dozen of scientific international publications on information systems, cognitive analysis techniques, biomedical engineering, and computational intelligence methods. She is member of few prestigious international scientific societies as: SIAM, SPIE, and 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.

Prof. Marek R. Ogiela is professor of Computer Science, cognitive scientist and cryptographer, head of Cryptography and Cognitive Informatics Laboratory. He works at the AGH University of Science and Technology and Pedagogical University in Krakow. In 1992 he 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.

He is member of numerous world scientific associations (IEEE-Senior Member, SPIE-Senior Member, etc.). He is author of more than 300 scientific international publications on pattern recognition and image understanding, artificial intelligence, IT systems and biocybernetics.

He is author of recognized monographs in the field of cryptography and IT techniques; author of an innovative approach to cognitive medical image analysis, and linguistic threshold schemes. 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. He is Associate Editor in Electronic Commerce Research and Applications Journal, Soft Computing, and Security and Communication Network.