Soft Comput (2017) 21:2451–2464
DOI 10.1007/s00500-017-2546-2

METHODOLOGIES AND APPLICATION

Personalized cryptography in cognitive management

Lidia Ogiela[1] · Makoto Takizawa[2]

Published online: 21 March 2017

Abstract One of the existing problems of information management is an information security. In this aspects one of possible solution is divide information between a group of persons authorized to manage this information. Information sharing processes allow to protect the information from disclosure. In this paper, the process of division of the information has been enhanced by biometric identification stage. Secure information processes with biometric identification are used to manage very important and strategic data. This paper presents the questions of personal cryptography understood as a combination of the tasks of classifying information and biometric techniques used for this kind of tasks. The techniques of biometric data marking are present on the examples of data division and sharing protocols, expanded by the stages of personal identification and verification. This kind of solutions is presented for the tasks of dividing appropriately the shared secret information. Moreover, we shall present the management process of shadow sets, i.e., of parts of the divided, secret information. The processes of secret data management are refer to tasks of cognitive management, understood as management executed on the basis of understanding the meaning of the processed data.

Communicated by V. Loia.

✉ Lidia Ogiela
logiela@agh.edu.pl

Makoto Takizawa
makoto.takizawa@computer.org

[1] Cryptography and Cognitive Informatics Research Group, AGH University of Science and Technology, Al. Mickiewicza 30, 30-059 Kraków, Poland

[2] Department of Advanced Sciences, Hosei University, 3-7-2, Kajino-cho, Koganei-shi, Tokyo 184-8584, Japan

Keywords Personalized cryptography · Biometrics in data sharing protocols · Cognitive systems

1 Introduction

Cryptographic techniques of securing information refer to algorithms of classifying data (Menezes et al. 2001). The techniques of data classification serve the processes of protecting information from disclosure to persons unauthorized or persons who have no access to this type of information (Ogiela and Ogiela 2008; Schneier 1996). Securing data are therefore the most important stage of protecting information against disclosure, against making it public or declassification. This is an prime process in the whole process of guaranteeing the security of information (Castiglione et al. 2010; Enokido and Takizawa 2011; Ogiela and Ogiela 2009a, b).

In the group of protocols used to classify information, we differentiate between various data division protocols. It is on their basis that it is possible to divide information among a group of specified secret holders in order to protect the divided information from disclosure (Nakamura et al. 2015b, 2016). In the group of information division protocols, there are the following ones (Schneier 1996):

- information division,
- information sharing.

The process of data division depends on the type of the division protocol applied. In this group we can differentiate an independent group of protocols, the so-called information sharing protocols.

The protocols of data division specify how will the data be split between all protocol participants. Every protocol participant will receive a part of the divided secret, which can be re-created only after putting together all its constituting elements. In a situation when information sharing protocols are used, the number of parts of the divided secret necessary to reproduce it depends on the applied information sharing protocol.

In the case of information division protocols, to reproduce the split information it is necessary to put together all the parts of the divided secret.

For data sharing protocols, to reproduce the shared secret it is necessary to put together a certain number of parts of the divided secret. The number of parts required to reproduce the whole secret is specified in the sharing protocol at the stage of its development.

Classic data sharing protocols ensure:

- security of the divided information—no possibility to disclose the secret data by any shadow holder (parts of the divided secret) without the other shadow holders taking part in the process of secret reproduction,
- security of the shared parts of data (shadows)—disclosure of any part of the secret does not disclose the content of the whole secret because every part of the secret taken separately has no meaning of its own,
- no possibility to reproduce the shared information without the participation of a specified number of shadow holders,
- no possibility to intercept by unauthorized persons such part of the secret, which is necessary to reproduce it.

All the features of information sharing protocols result in that this type of protocols are an effective tool to classify data of various importance and destination, collected by various entities and for various purposes (Nakamura et al. 2015a, c). The lead topic of this paper is the information sharing protocols. This is due to the fact that this type of algorithms are more useful in the process of classifying data.

2 Data sharing protocols

The protocols of data sharing divide the secret among a selected group of secret holders (Shamir 1979; Tang 2004). The number of protocol participants is specified at the stage of defining the proper protocol of information sharing. The secret is split among a group of k protocol participants, of whom every one obtains part of the information shared. The allocation of parts of the shared secret can differ:

- equal division with an allocation of one part—every protocol participant obtains only one part of the shared secret—he or she receives one shadow (Fig. 1),
- equal division with an allocation of more than one secret parts—every secret holder receives the same number of parts of the co-shared secret (Fig. 2),
- privileged division—every protocol participant receives parts of the co-shared secret, plus:
  - a selected group of secret holders receives a higher number of shades than the remaining secret holders (Fig. 3),
  - every protocol holder receives a different number of shadows (Fig. 4),
  - one group of secret holders receives a smaller number of shadows, while another group of secret holders receives a higher number of shadows (Fig. 5).

Figure 1 presents the situation where the secret is split among a group of k protocol participants, in this example k is equal 9 participants. In this solution, every one of participants obtains part of the information shared. In Fig. 1, we see example of equal division with an allocation of one part. In this solution every protocol participant obtains only one part of the shared secret—each participant receives only one shadow.

Figure 2 presents the situation where the secret is split among a group of k protocol participants, in this example k is equal 3 participants. In this solution every one of participants obtains part of the information. In Fig. 2, we see example of equal division with an allocation of more than one secret parts. In this solution, every protocol participant receives the same number of parts of the co-shared secret—each participant receives three shadows.

Figure 3 presents the situation where the secret is split among a group of k protocol participants, in this example k is equal 6 participants. In this solution every one of participants obtains part of the information. In Fig. 3, we see example of privileged division of information. In this solution, every protocol participant receives parts of the co-shared secret, but the selected group of secret holders (three participants) received a higher number of shadows (two shadows) than the remaining secret holders (three participants receive one shadow).

Figure 4 presents the situation where the secret is split among a group of k protocol participants, in this example k is equal 3 participants. In this solution every one of participants obtains part of the information. In Fig. 4, we see example of privileged division of information. In this solution, every protocol participant receives a different number of shadows. The first participant receives three shadows, the second participant receives four shadows, and the last one receives only two shadows.

Figure 5 presents the situation where the secret is split among a two group of participants. The first group assigned four shadows, and the second group five shadows. In this

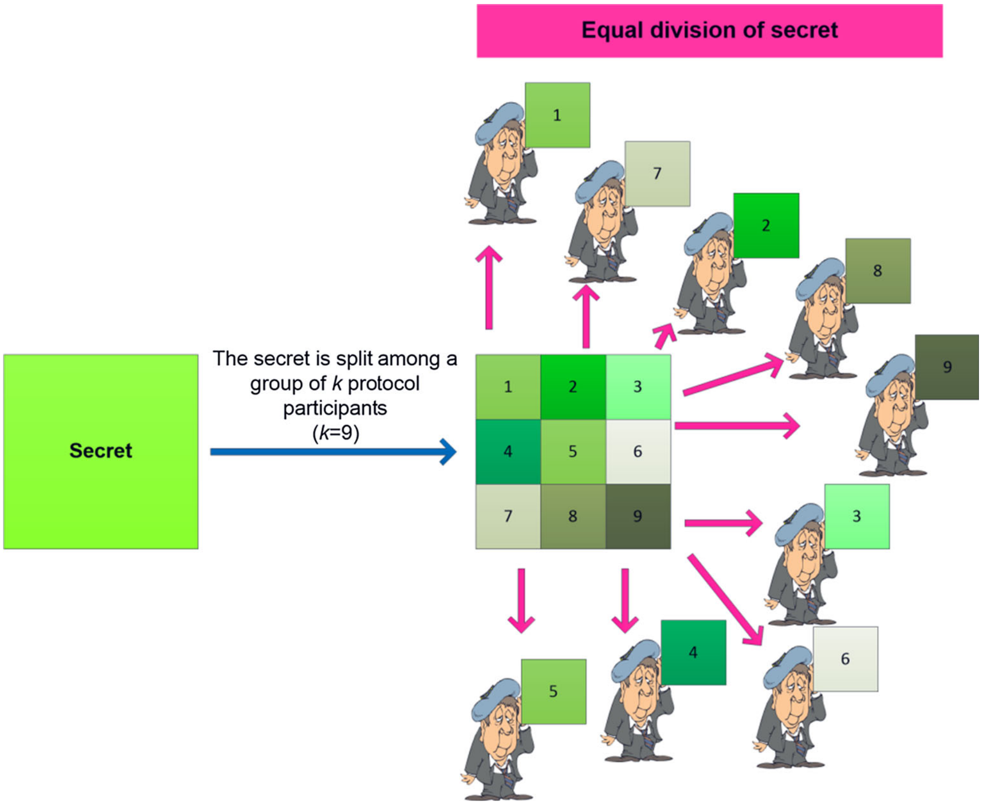
Equal division of secret
Secret
The secret is split among a group of *k* protocol participants (*k*=9)
1
2
3
4
5
6
7
8
9

Fig. 1 Equal division with an allocation of one part of secret—the secret is split among a group of $k = 9$ participants of protocol

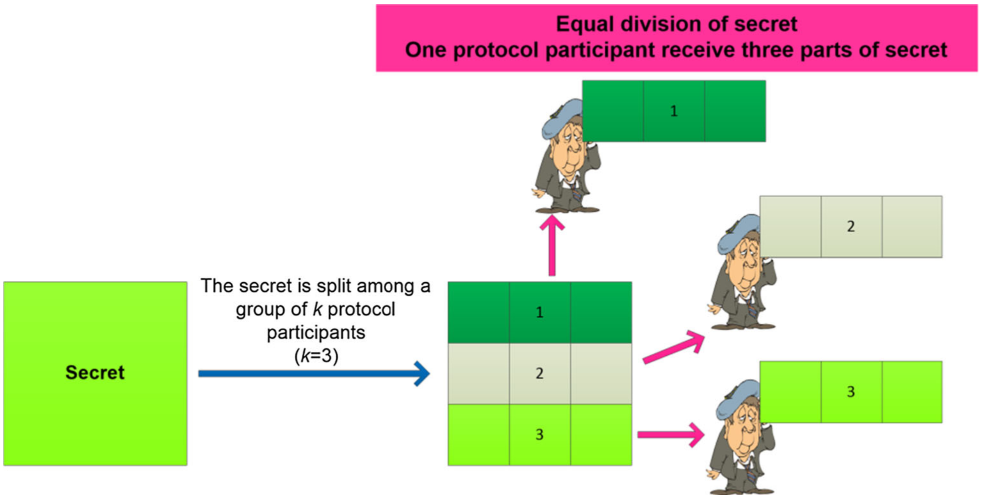
Equal division of secret
One protocol participant receive three parts of secret
Secret
The secret is split among a group of *k* protocol participants (*k*=3)
1
2
3

Fig. 2 Equal division with an allocation of more than one part of secret—the secret is split among a group of $k = 3$ participants of protocol which everyone receive three parts of secret

example we see the split information between k protocol participants, in this example k is equal 7 participants. In this solution every one of participants obtains part of the information. In Fig. 5, we see example of privileged division of information. In this solution one group of secret holders receives a smaller number of shadows (only four shadows), while the second group of secret holders receiver a higher number of shadows (five shadows). In the first group, each of participants (two participants) receives two shadows. In the second group each of participant (five participants) receives one shadow. In each of the groups, shadow division is equal.

What is important in information sharing protocols—apart from the process of data division among the selected group of secret holders—is the reproduction of the shared data. In this

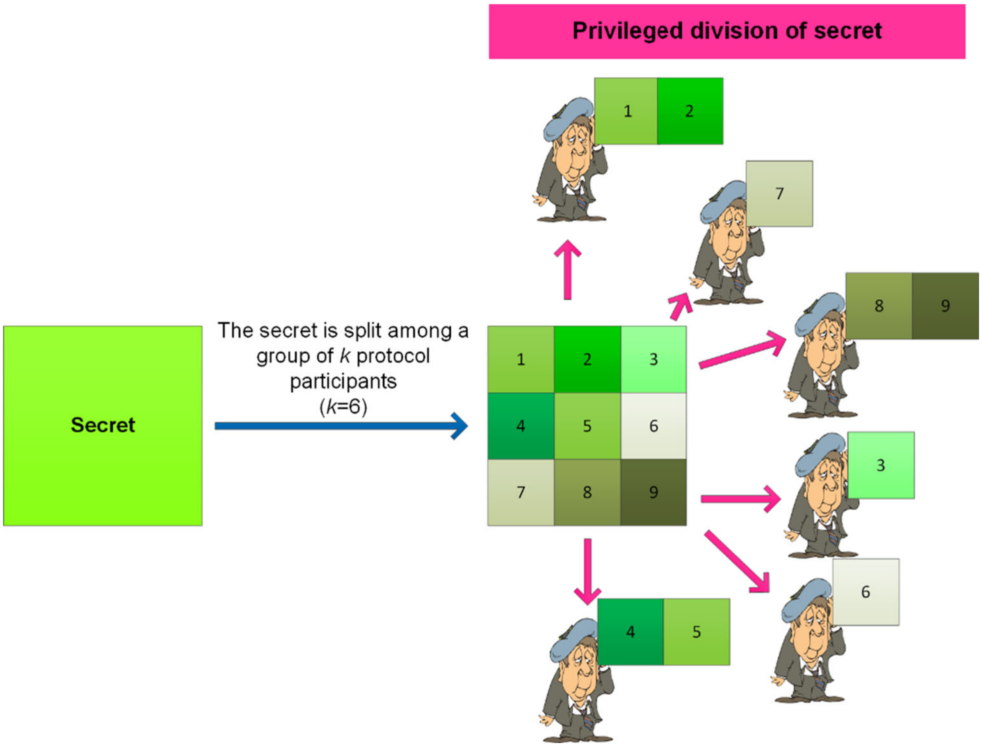
Privileged division of secret
Secret
The secret is split among a group of k protocol participants (k=6)
1
2
3
4
5
6
7
8
9

Fig. 3 Example of privileged division of secret—a selected group of secret holders receives a higher number of shades than the remaining secret holders

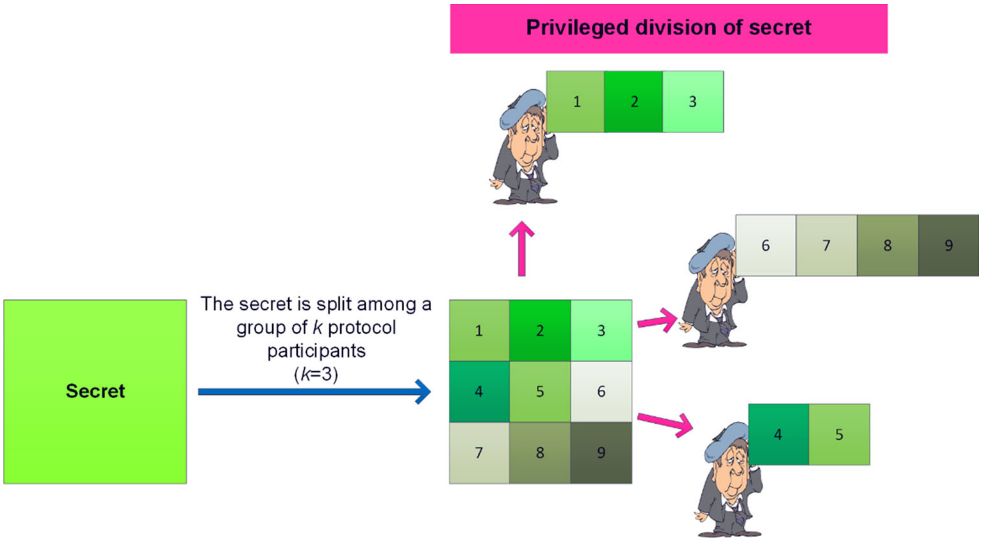
Privileged division of secret
Secret
The secret is split among a group of k protocol participants (k=3)
1
2
3
4
5
6
7
8
9

Fig. 4 Example of privileged division of secret—every protocol holders receives a different number of shadows

process to re-create the secret, it is necessary to put together a specified number of the shared secret parts (m). This number is specified at the stage of the information sharing protocol development. In the protocols of data sharing, this number is smaller or equal to the number of the shared secret parts (n). Should $m = n$, we are dealing with data sharing protocols.

To reproduce the shared secret, it is therefore necessary to put together m out of n parts of the shared secret. These are (m, n)-threshold schemes, described in the following papers (Menezes et al. 2001; Ogiela and Ogiela 2008, 2009a, b, 2015a).

Should equal division be applied, one in which every protocol participant has one part of the shared secret, the number of all parts of the shared secret (n) equals the number of protocol participants (k_1).

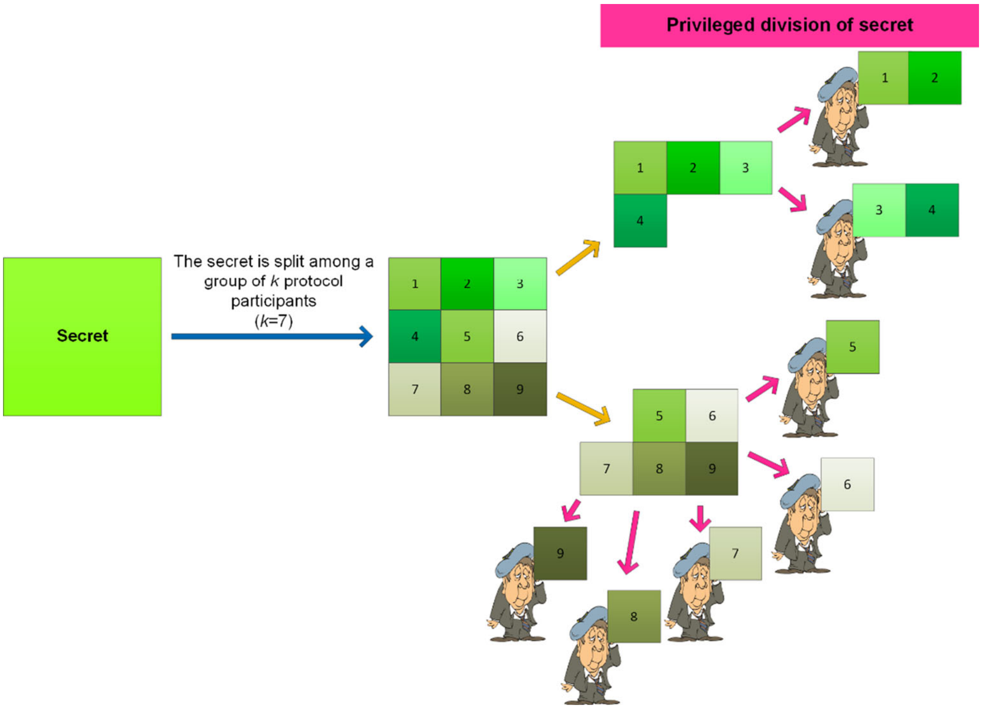
Privileged division of secret
Secret
The secret is split among a group of *k* protocol participants (*k*=7)
1
2
3
4
5
6
7
8
9

Fig. 5 Example of privileged division of secret—one group of secret holders receives a smaller number of shadows while another group of secret holders receives a higher number of shadows

Therefore there is an equality:

$$n = k_1$$

From the k_1 set of participants, any m of participants, having put together the secret parts they have, can reproduce the shared information (Fig. 6).

Figure 6 presents the example of reproduce the secret information. In this figure we see the situation where the secret is split among a group of $k_1 = 9$ protocol participants. In this solution, every participant obtains part of the information shared. In this example each participant receives only one shadow. To reproduce the original information any m (in this example $m = 5$) of participants can reproduce the information. Each 5 of 9 participants can reproduce the original information by the put together them parts.

Should an equal division be applied, one in which every protocol participant has the same number of parts of the shared secret, the number of all parts of the shared secret (n) equals the product of i_1 and the number of protocol participants (k_2).

Therefore there is an equality:

$$n = i_1 * k_2$$

where $i_1 \in N, i_1 > 1$.

From the k_2 set of participants, any m of participants, having put together the secret parts they have, can reproduce the shared information (Fig. 7).

Figure 7 presents the example of reproduce the secret information. In this figure we see the situation where the secret is split among a group of $k_2 = 3$ protocol participants. In this solution every participant obtains part of the information shared. In this example each participant receives three shadows—the same number of shadows. To reproduce the original information any m (in this example $m = 2$) of participants can reproduce the information. Each 2 of 3 participants can reproduce the original information by the put together them parts. Also, each 6 of 9 secret shadows is enough to reproduce the original information.

Should a privileged division be applied, in which a selected group of secret holders receives a higher number of parts of the shared secret than the remaining secret holders, the number of all parts of the shared secret (n) is equal to the sum of the products of i_2 and the number of those protocol participants who receive a higher number of secret parts (k_3) and i_3 as well as the number of those protocol participants who receive a smaller number of shadows (k_4).

Therefore there is an equality:

$$n = i_2 * k_3 + i_3 * k_4$$

where $i_2, i_3 \in N, i_2, i_3 \geq 1$.

From the $k_3 \cup k_4$ set of shadow owners, any m of participants, having put together the secret parts they have, can reproduce the shared information (Fig. 8).

Figure 8 presents the example of reproduce the secret information. In this figure we see the situation where the

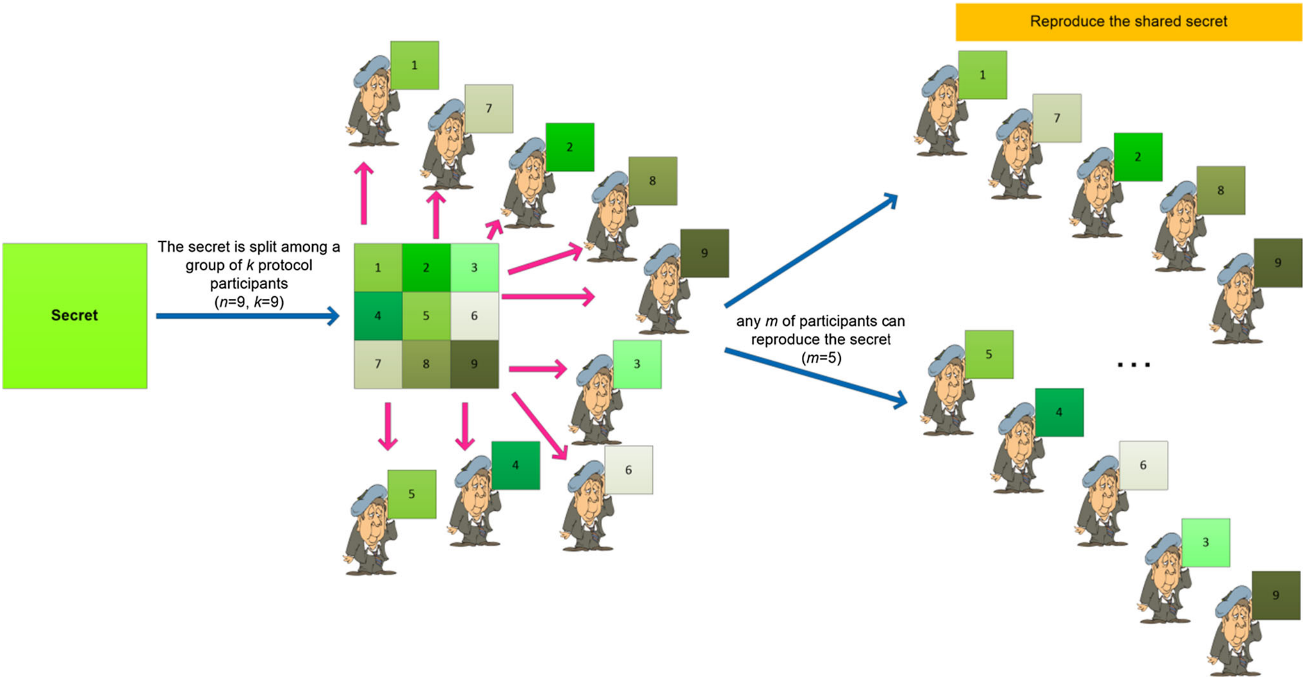
Reproduce the shared secret
Secret
The secret is split among a group of *k* protocol participants (*n*=9, *k*=9)
1 2 3 4 5 6 7 8 9
any *m* of participants can reproduce the secret (*m*=5)
1 7 2 8 9
5 4 6 3 9
. . .

Fig. 6 Example of reproduce the shared secret process—any m ($m = 5$) of participants can reproduce the secret

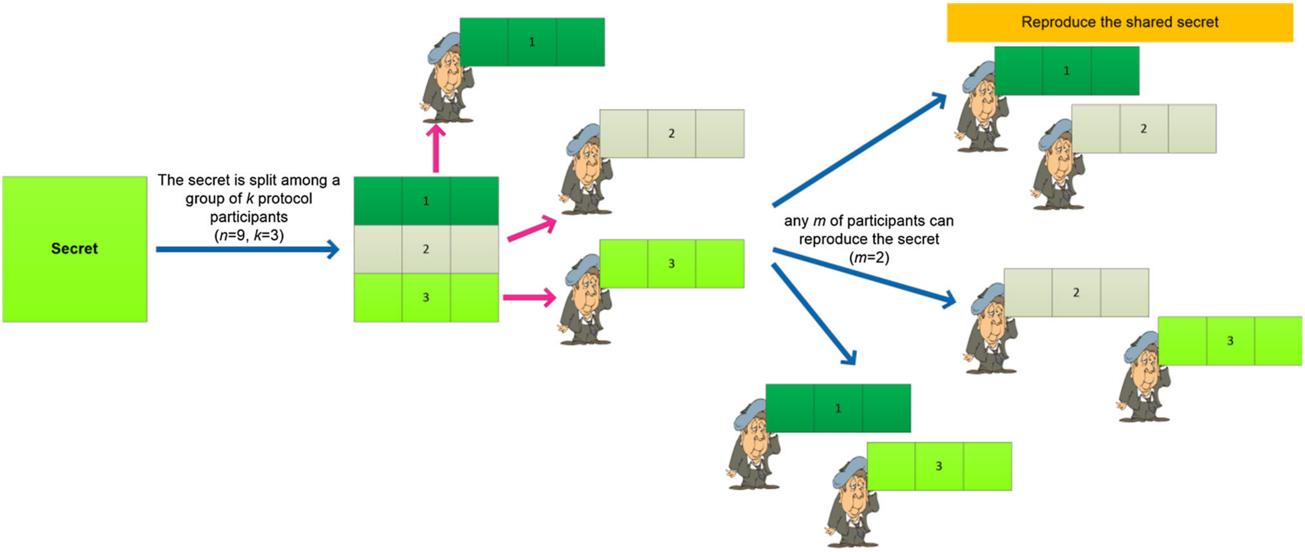
Reproduce the shared secret
Secret
The secret is split among a group of *k* protocol participants (*n*=9, *k*=3)
1 2 3
any *m* of participants can reproduce the secret (*m*=2)
1 2
2 3
1 3

Fig. 7 Example of reproduce the shared secret process—any m ($m = 2$) of participants (every one of them receive three secret parts) can reproduce the secret

secret is split among a group of $k_3 = 6$ protocol participants. In this solution every participant obtains part of the information shared. In this example each participant receives parts of the co-shared secret. The selected group of secret holders—three participants—received a higher number of shadows—two shadows, than the remaining secret holders—three participants receive one shadow. To reproduce the original information any m of participants can reproduce the information. Each 6 of 9 secret shadows is enough to reproduce the original information. Participants who take six parts of secret can reproduce the original information. If participants take two parts of secret, than combining three of them is enough to reproduce the information. If participants take a different number of shadows, than combining six different shadows is enough to secret reproduction.

Should an equal division be applied, one in which every protocol participant has the same number of shadows, the number of all parts of the shared secret (n) equals the product

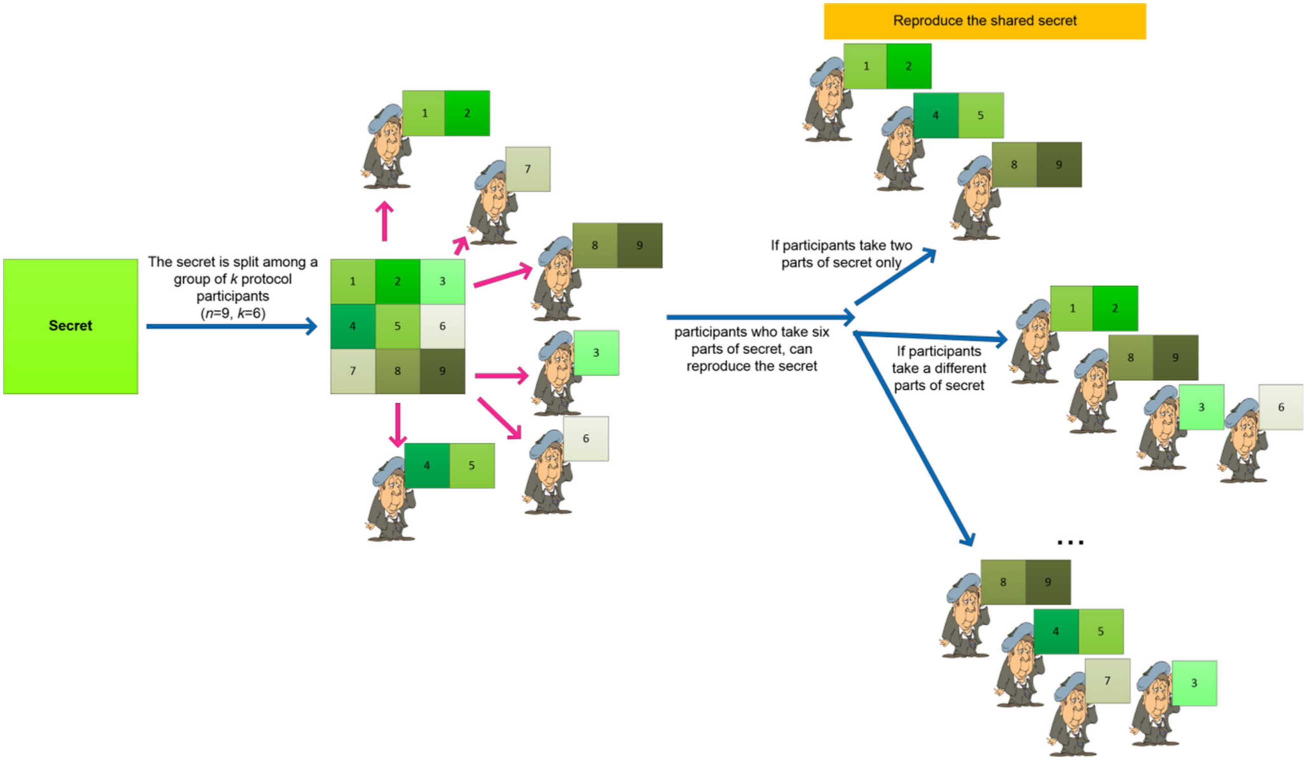
Reproduce the shared secret
Secret
The secret is split among a group of k protocol participants (n=9, k=6)
1 2 3
4 5 6
7 8 9
If participants take two parts of secret only
participants who take six parts of secret, can reproduce the secret
If participants take a different parts of secret
...

Fig. 8 Example of reproduce the secret sharing process—any six secret parts reproduce the secret

of i_j and (k_j), i.e., the number of protocol participants who receive parts of the secret.

Therefore there is an equality:

$$n = \sum_{j=1}^{k} i_j * k_j$$

where $i_j \in N, i_j \geq 1, 1 \leq j \leq k$.

From the k_j set of protocol participants, any m of participants, having put together the shadows they have, can reproduce the shared information (Fig. 9).

Figure 9 presents the example of reproduce the secret information. In this figure we see the situation where the secret is split among a group of $k_4 = 3$ protocol participants. In this solution every participant obtains part of the information shared. In this example each participant receives a different number of shadows. The first participant receives three shadows, the second participant receives four shadows, and the last one receives only two shadows. To reproduce the original information any m (in this example $m = 2$) of participants can reproduce the original information. Each 2 of 3 participants take together five parts of secret. Participants who take minimum five parts of secret can reproduce the original information.

Should a privileged division be applied, in which a selected group of secret holders receives a smaller number of parts of the shared secret, while the remaining secret holders receive a higher number of shadows, the number of all parts of the shared secret (n) is equal to the sum of the products of i_4 and the number of protocol participants who receive the smaller number of secret parts (k_5) and i_5 as well as the number of those protocol participants who receive a greater number of shadows (k_6).

Therefore there is an equality:

$$n = i_4 * k_5 + i_5 * k_6$$

where $i_4, i_5 \in N$, i$_4$, $i_5 \geq 1, i_4 \neq i_5$.

From the $k_5 \cup k_6$ set of shadow owners, any m of protocol participants, having put together the secret parts they have, can reproduce the shared information (Fig. 10).

Figure 10 presents the example of reproduce the original information. In this figure we see the situation where the secret is split among a two group of participants. One group of secret holders receives a smaller number of shadows—four shadows. The second group of secret holders receiver a higher number of shadows—five shadows. In the first group, each of two participants receives two shadows. In the second group, each of five participant receives one shadow. In each of the groups, shadow division is equal. To reproduce the original information any five parts of secret can reproduce the original information. For example combining any two parts from the first group and three parts from the second group can reproduce the original information. Thus, one participant from the first group and three participants from the second group can reproduce the secret.

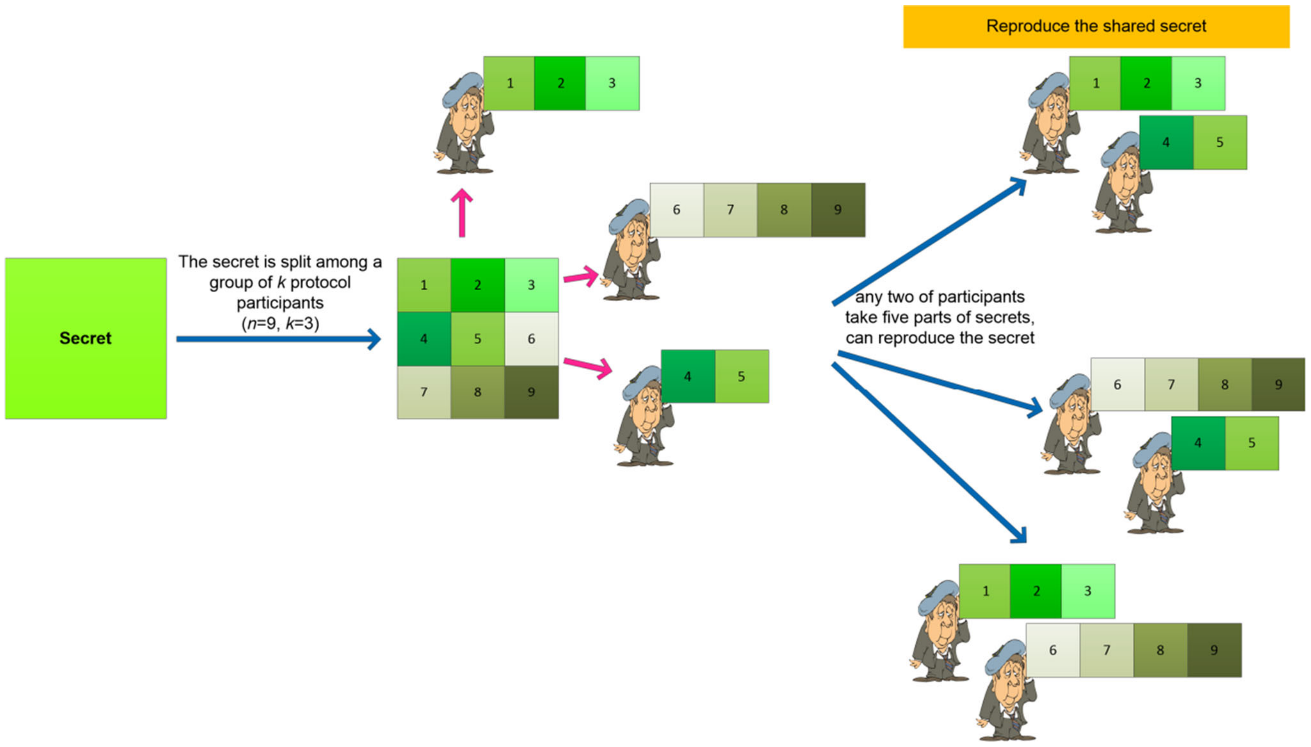
Reproduce the shared secret
Secret
The secret is split among a group of *k* protocol participants (*n*=9, *k*=3)
1 2 3
4 5 6
7 8 9
6 7 8 9
4 5
any two of participants take five parts of secrets, can reproduce the secret

Fig. 9 Example of reproduce the secret sharing process—any two of participants take together five parts of secrets, reproduce the shared secret

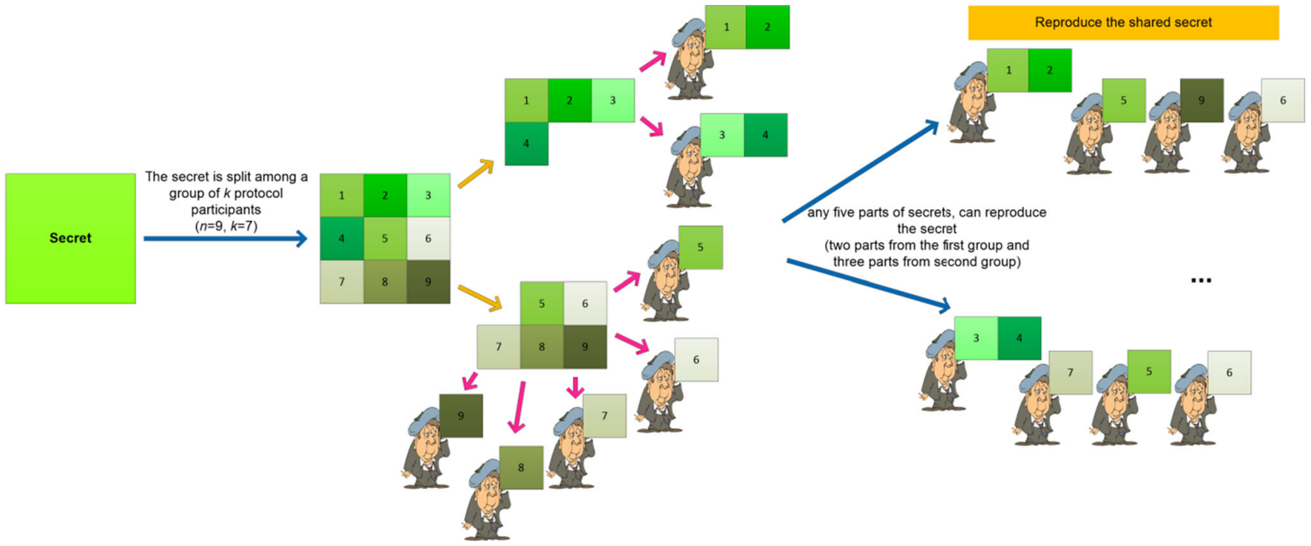
Reproduce the shared secret
Secret
The secret is split among a group of *k* protocol participants (*n*=9, *k*=7)
1 2 3
4 5 6
7 8 9
any five parts of secrets, can reproduce the secret (two parts from the first group and three parts from second group)
...

Fig. 10 Example of reproduce the secret—any five parts of secrets reproduce the shared secret (two parts from group 1 and three parts from group 2 = one participants from group 1 and three participants from group 2)

Every above-presented method of information sharing can be applied in order to divide the secret among any group of secret holders. At the same time, everyone will be used to reproduce the shared information by a specified group of shadow holders. The selection of the optimum solution depends on the type of the shared information, the specification of how confidential it is and the method of reproduction of the secret data.

3 Personalized cryptography

Personal cryptography refers to classifying information in the protocols of data sharing by means of labelling information conducted pursuant to the personal features of secret holders. In the case of data sharing protocols, every part of the divided information is subject to:

- the labelling process executed at the stage of shadow allocation,
- the identification process conducted at the stage of information reproduction.

The process of information labelling is run based on the use of individual features of every protocol participant (shadow holder) (Ogiela 2016; Ogiela and Ogiela 2015a).

An individual personal code is contained in bio-labels (biometric information). Based on biometric features contained in personal information sets it is possible to specify unambiguously who is the person whose biometrics we have or to allocate personal features to the right person.

Individual biometric features are specified based on the analysis of (Ogiela and Ogiela 2015a):

- DNA code—deoxyribonucleic acid, the genetic information contained in the nucleotide sequence of the nucleic acid (DNA or RNA) in cells of all organisms—this information showing the sequence of amino acid sequence in the protein in the protein biosynthesis,
- fingerprints—one of the most popular biometric features, shows the fingerprint imprinted in order to identify the person, also used in cryptography as a short sequence of characters that identifies a greater number of personal, individual data,
- facial features—the characteristic facial features indicative of a person, as an eyes system, the system faces, spacing ears, eyes, the size of the mouth, nose, eyes, etc.
- eye features—colour, position, spacing, size of eyes,
- palm features—the layout, size, range, deformations, pathologies of the hand,
- speech—voice and speech characteristics, volume, colour, accent, frequency of repetition,
- handwriting—characteristics of handwriting, the slope of writing, incline letter, accent, repetition frequency, size of letters, combination of letters,
- walking manner—the characteristics of walking, walking speed, volume, tilt the figure, the size and frequency of steps,
- characteristic features of human body organs—the important features of body organs like a deformation, pathologies, anomalies, and the construction of various human organs.

The individual biometric features are the basis for the creation of database systems, included all of important, characteristic and useful personal features. Each biometrics can be used to identify a person in different situations. One of the most important of them is identification process in personal cryptography dedicated to management processes. Individual characteristic features and personal information are included in knowledge base, and processed by the information system.

Individual personal features specified by a selected type of biometrics serve the purpose of personal identification and verification. In the processes of personal identification the selection of the appropriate analysis method depends on a variety of factors, of which the most important refers to the technical capacity related to personal data collection. Moreover, the selection of the appropriate biometric method for personal identification and personal verification depends on:

- the availability of special equipment and software to record and process biometric data,
- the quantity of information/personal data obtained,
- specification of personal patterns for various biometric techniques,
- the degree of difficulty of the performed identification and verification tasks,
- the number of identification and verification tasks executed.

The selection of the appropriate biometric method for personal verification and identification depends on the quantity of information that can be stored in the IT system. The volume of information refers to the biometric information/data, which will be processed with a view to clear personal verification.

The processes of identification and verification based on the use of biometric data belong to the personal cryptography area.

Personal cryptography serves therefore to classify data using various information classification techniques enriched by personal information. An example of such solutions are cryptographic protocols for information division and sharing. They serve the tasks of protecting information against disclosure to unauthorized persons. In the protocols of this group, securing the information takes place by means dividing it and distributing shadows among a group of protocol participants, so that the information is not in the hands of one holder only. The very method of dividing information and allocating it to the secret holders is specified by cryptographic protocols, which include:

- information splitting protocols,
- information sharing protocols.

Cryptographic data classification protocols assume various forms. In this paper we discuss solutions aimed to classify information by dividing it. In this respect we can differentiate between the information splitting protocols and sharing protocols. The most important cryptographic algorithms to secure and classify data are (Menezes et al. 2001; Ogiela and Ogiela 2008, 2009a, b; Schneier 1996):

- the Shamir, the Schnorr, the Ong–Schnorr–Shamir protocols,
- the ElGamal algorithm,
- the Tang algorithm,
- the Diffi–Hellman, Pohling–Hellman algorithms,
- the Rabin algorithm, etc.

A novelty among the presented solutions is the introduction—at the stage of splitting information and allocating parts of the divided information to protocol participants—the biometric process of shadow labelling, which have appeared at the stage of information division.

The process of biometric labelling of parts of the divided information (shadows) refers to the use of individual personal features contained in the biometric sets. This offers a possibility to allocate clearly shadows to holders of the divided information parts. Moreover, this process allows for an appropriate reproduction of the divided information by means of verification of the ownership of shadows by their holders.

The application of cryptographic protocols of data classification by means of dividing it, with simultaneous use of biometric solutions to label parts of the split information is a new solution. It ensures an appropriate allocation of parts of the shared secret to their holders.

We can use any type of biometrics to label the divided secret biometrically. We should remember that the biometric labelling process referring to information division must be the same for all protocol participants. There is no possibility to apply different bio-labels to the participants of the same process of dividing a secret.

The choice of the applied biometrics should respect the rule of best financial and time results (savings). The first rule determines the selection of biometrics with regards to allocating the same amount of financial means for the execution of this task, so as not to outweigh the prospective advantages resulting from such solution.

The second rule stands for the selection of such a solution, which will be feasible in real time. The results obtained cannot reach recipients after an excessively long waiting time.

The choice of biometric labelling of the divided secret depends on:

- the size of secret data sets,
- the type of labelled data,
- the size of data bases, which would store biometric information,
- access to data sets for personal identification,
- capacity to store and secure personal information (biometrics) from disclosure,
- the amount of financial means allocated to the execution of biometric analysis tasks,
- capacity to process biometric data and update data bases by new elements.

Labelling the divided information with the use of biometrics can occur at various stages of information management. The process of information management with the use of biometric labelling techniques of parts of the shared secret shall be discussed in reference to the processes of cognitive data management.

4 Cognitive management

The processes of data cognitive management refer to information management processes enriched by the stages of data interpretation based on the meaning of the data. Such solutions were described in the papers (Hachaj and Ogiela 2010; Ogiela 2010, 2012, 2013; Ogiela and Ogiela 2014, 2015b). Here an important element of the analysis process was to obtain, from the analysed information sets, their semantic layers, i.e., the meaning of the information contained in these sets (Grossberg 2012; Ning et al. 2012; TalebiFard and Leung 2011).

Extracting semantic information from data sets is possible due to the application of linguistic techniques of data description. Linguistic techniques are there to present data based on its meaning. The meaning contained in information sets offers a possibility to interpret data with regards to how important it is for the entire analysis process.

The process of cognitive data interpretation is used also for the process of cognitive management. The paradigm of cognitive management has been proposed in the paper (Ogiela 2014).

This paradigm allows to define cognitive management as a process of the execution of a meaning task aimed to achieve a specified objective, by using appropriate means as well as an evaluation of the meaning of the analysed data for the basic management processes, i.e., obtaining, developing, analysing, storing and making data available.

Cognitive management refers therefore to various objects, states and situations.

In this paper, we have focused on the issues of personal cryptography dedicated to the processes of cognitive management. The processes of cognitive management have been directed at the management tasks belonging to the application range of personal cryptography.

The process of cognitive management refers therefore to the management of secret information. Every secret information is:

- divided among protocol participants,
- shadows are biometrically labelled,
- shadows are split among secret holders,

- shadows are stored by secret holders,
- shadows are put together to reproduce the secret,
- the parts put together are verified for their compliance of biometric information contained in the shadow labelling and in the data base which contains biometric data of secret holders.

The process of management of biometrically labelled shadows (parts of the secret) refers to the following stages:

- data collection—obtaining secret data subject to the process of their classification by means of dividing them, additionally they are biometric labelled,
- data processing—processing the secret in order to divide the classified information among protocol participants and shadow allocation in order to run the process of biometric labelling,
- data description and identification—the process of biometric labelling of parts of the divided information,
- storing data—the process of storing the secret parts (shadows) by their holders (participants of the data division protocol),
- data transfer—the process of transferring shadows with a view to reproduce the secret,
- making data available—the process of disclosing the secret based on verification of access to confidential information by means of personal verification of those protocol participants who are authorized to learn about secret parts.

The principal role of the here-proposed solutions is therefore to classify secret data. Its meaning is determined based on the secret's cognitive analysis by persons authorized to do that—and—to allocate the shared secret to a group of secret holders in order to classify the secret content and its meaning. This process is executed on the basis of biometric labelling of parts of the divided secret.

The process of biometric identification in cognitive management is presented by Fig. 11.

The processes of biometric identification refer to stage of:

- mark shared secret parts, which are divided to all secret participants,
- reproduce the secret information/data, based on verification processes of biometrics.

In each of these stages the biometric data/information create a new data/information sets containing the individual, personal, biometric data. These data are used to support management processes by using only selected and important information. The validity of the information/data is determined on the basis by cognitive and semantic analysis of data. The cognitive aspects of data analysis are very useful in selected only important information and understanding the analysed information.

Cognitive management refers to aspects of meaning assessment and the interpretation of data subject to the management processes. The assessment of the content and meaning of data subject to the processes of cognitive data management makes it possible to enhance the information management process by means of:

- determining the degree of importance of the data managed,
- eliminating from the data management processes such data that is not important for the whole process,
- giving the overriding status to the management process of the most important data,
- determining the degree to which some data impact other data,
- eliminating the causes of occurrence of negative phenomena determined by means of meaning analysis,
- foreseeing the future state on the basis of determining the importance of the managed data sets in order to bring about a specified future state.

The processes of cognitive management in the above-presented scope enhance considerably the processes of data management.

Cognitive management processes refer to the:

- management processes by the data analysis and interpretation based on the meaning and semantic description of the data or information,
- processes of the execution of a meaning evaluation task by using appropriate means dedicated to all management processes,
- understanding the semantic meaning of data in management processes.

5 Related works

In this paper was proposed a new solution, in which the most important are:

- used of personalized cryptography dedicated to:
    - data watermarking,
    - processes of data security,
    - data management processes,
- description of protocols of data security and data splitting and sharing methods, dedicated to management processes,
- extended data security algorithms, by the processes of biometric identification and verification,

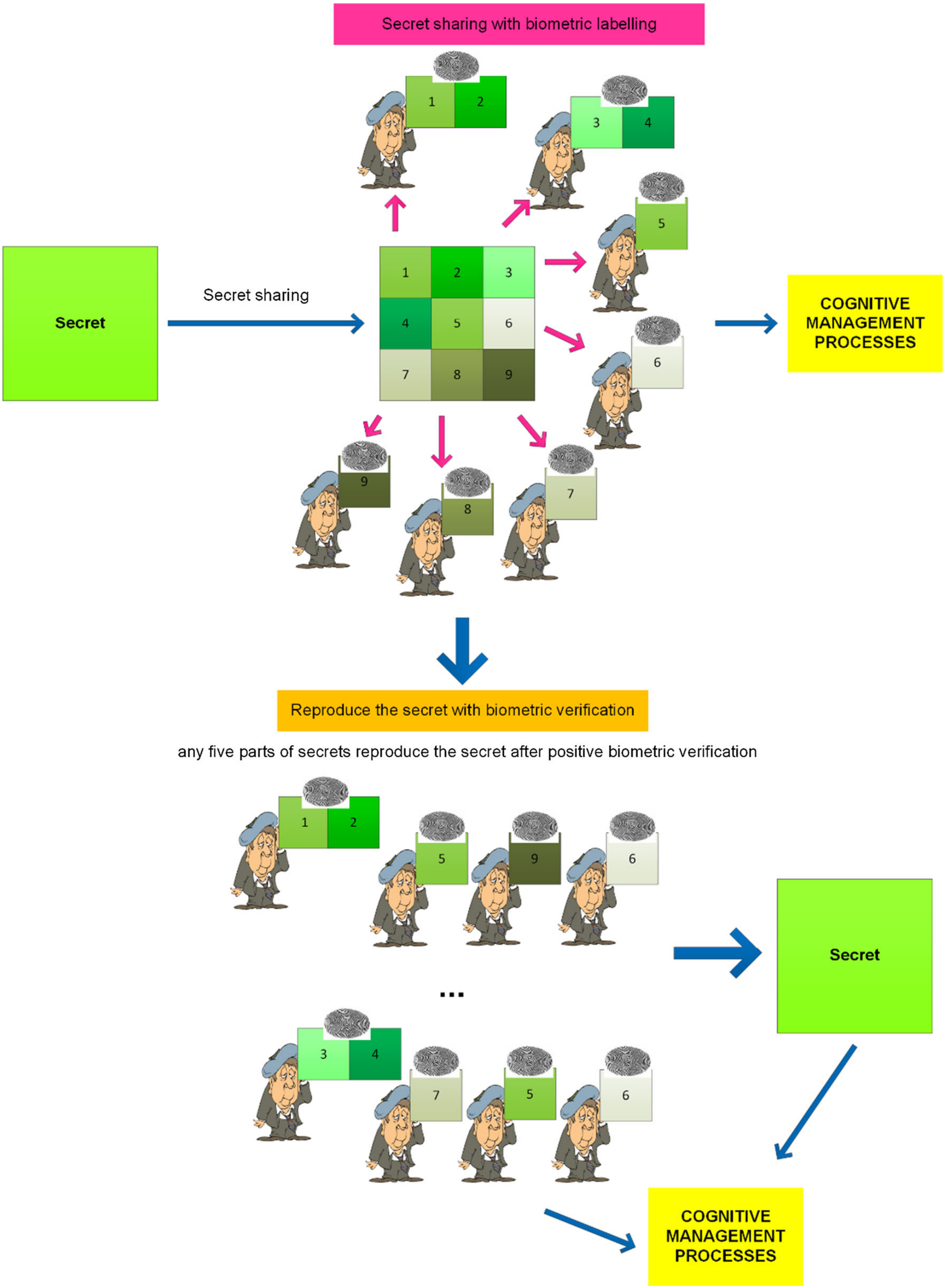
Secret sharing with biometric labelling
Secret
Secret sharing
1 2 3
4 5 6
7 8 9
COGNITIVE MANAGEMENT PROCESSES
Reproduce the secret with biometric verification
any five parts of secrets reproduce the secret after positive biometric verification
...
Secret
COGNITIVE MANAGEMENT PROCESSES

Fig. 11 The process of biometric identification in cognitive management

- dedicated new algorithms of data security, to secure and manage strategic data in cognitive management processes.

6 Conclusions

Personal cryptography is dedicated to the tasks of information storage, classification and protecting data (from access to it by unauthorized persons) with the use of biometric information in order to allocate appropriately a piece of information to a holder. The very allocation of information to a holder based on personal verification in reference to confirming the biometric compliance is a process of personal cryptography. Nevertheless, in this paper the process has been enriched by the stage of splitting parts of the secret among a group of its holders in order to avoid such a situation, in which the secret is held by one secret holder only. The process of secret data division and allocation to a group of secret holders guarantees that the data is safe from being disclosed by one person. The decision to reproduce classified data must be taken by a specified group of shadow holders. In this way the data is protected against unauthorized disclosure, should a decision be taken single-handedly.

Moreover, the process of dividing data among a group of secret holders has been enriched by the stage of biometric labelling of the information held. This process prevents handing over shadows to persons unauthorized to hold them, it prevents cyber-thefts as a result of which shadows could end up with unauthorized holders. The process of biometric shadow verification at the stage of information reproduction eliminates actions aimed to sell shadows and hand them over to persons who are not the protocol rightful participants.

The process of secret division, shadow storage and reproduction of the shared information is subject to information management processes. This paper has presented how these processes could be enhanced by stages of cognitive management of secret information. The management process of biometrically labelled shadows is also subject to management. Therefore the proposed solutions belonging to personal cryptography in the tasks of cognitive secret management seem to be original solutions. In the future they could have their application solutions dedicated to the tasks of strategic information classification.

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

Compliance with ethical standards

Conflict of interest The authors declare that they has no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

Castiglione A, Cepparulo M, De Santis A, Palmieri F (2010) Towards a lawfully secure and privacy preserving video surveillance system. In: Buccafurri F, Semeraro G (eds) E-commerce and web technologies. 11th international conference, EC-Web 2010, Bilbao, Spain, September 1–3, 2010 (Lecture notes in business information processing), vol 61. pp 73–84

Enokido T, Takizawa M (2011) Purpose-based information flow control for cyber engineering. IEEE Trans Ind Electron (TIE) 58(6):2216–2225

Grossberg S (2012) Adaptive resonance theory: how a brain learns to consciously attend, learn, and recognize a changing world. Neural Netw 37:1–47

Hachaj T, Ogiela MR (2010) Automatic detection and lesion description in cerebral blood flow and cerebral blood volume perfusion maps. J Signal Process Syst Signal Image Video Technol 61(3):317–328

Menezes A, van Oorschot P, Vanstone S (2001) Handbook of applied cryptography. CRC Press, Waterloo

Nakamura S, Duolikun D, Takizawa M (2015a) Read-abortion (RA) based synchronization protocols to prevent illegal information flow. J Comput Syst Sci 81(8):1441–1451

Nakamura S, Duolikun D, Enokido T, Takizawa M (2015b) A write abortion-based protocol in role-based access control systems. Int J Adapt Innov Syst 2(2):142–160

Nakamura S, Duolikun D, Enokido T, Takizawa M (2015c) A flexible read-write abortion protocol to prevent illegal information flow among objects. J Mobile Multimedia 11(3&4):263–280

Nakamura S, Duolikun D, Enokido T, Takizawa M (2016) A read-write abortion (RWA) protocol to prevent illegal information flow in role-based access control systems. Int J Space-Based Situat Comput 6(1):43–53

Ning Y, Liu J, Yan L (2012) Uncertain aggregate production planning. Soft Comput 17:617–624

Ogiela L (2010) Computational intelligence in cognitive healthcare information systems. In: Bichindaritz I, Vaidya S, Jain A et al (eds) Computational intelligence in healthcare 4: advanced methodologies, studies in computational intelligence, vol 309. Springer-Verlag, Berlin, Germany, pp 347–369

Ogiela L (2012) Semantic analysis in cognitive UBIAS & E-UBIAS systems. Comput Math Appl 63(2):378–390

Ogiela L (2013) Cognitive informatics in image semantics description, identification and automatic pattern understanding. Neurocomputing 122:58–69

Ogiela L (2014) Towards cognitive economy. Soft Comput 18(9):1675–1683

Ogiela L (2016) Cryptographic techniques of strategic data splitting and secure information management. Pervasive Mob Comput 29:130–141

Ogiela MR, Ogiela U (2008) Linguistic approach to cryptographic data sharing. In: 2nd international conference on future generation communication and networking, Hainan, Peoples Republic of China, 13–15 December 2008, IEEE FGCN: Proceedings of the 2008 second international conference on future generation communication and networking, vol 1, 2. IEEE Computer Soc, LOS ALAMITOS, CA, USA, pp 377–380

Ogiela MR, Ogiela U (2009a) Security of linguistic threshold schemes in multimedia systems. In: Damiani E, Jeong J, Howlett RJ et al (eds) New directions in intelligent interactive multimedia systems and services 2, Studies in computational intelligence, vol 226. Springer-Verlag, Berlin, pp 13–20

Ogiela MR, Ogiela U (2009b) Shadow generation protocol in linguistic threshold schemes. In: Slezak D, Kim TH, Tang WC et al (eds) Security technology, communications in computer and information science, vol 58. Springer-Verlag, Berlin, Germany, pp 35–42

Ogiela L, Ogiela MR (2014) Cognitive systems for intelligent business information management in cognitive economy. Int J Inf Manag 34(6):751–760

Ogiela L, Ogiela MR (2015a) Efficiency of cognitive information systems supporting enterprise management tasks. In: Barolli L et al (eds) 9th international conference on innovative mobile and internet services in ubiquitous computing (IMIS), Blumenau, Brazil, 08–10 July 2015, pp 166–170

Ogiela L, Ogiela MR (2015b) Management information systems. In: Park JJ, Pan Y, Chao HC et al (eds) Ubiquitous computing application and wireless sensor. 2nd FTRA international conference on ubiquitous computing application and wireless sensor network (UCAWSN), South Korea, 07–10 July 2014 (Lecture notes in electrical engineering), vol 331, pp 449–456

Schneier B (1996) Applied cryptography: protocols, algorithms and source code in C. Wiley, London

Shamir A (1979) How to share a secret. Commun ACM 22(11):612–613

TalebiFard P, Leung VCM (2011) Context-aware mobility management in heterogeneous network environments. J Wireless Mobile Netw Ubiquitous Comput Dependable Appl 2(2):19–32

Tang S (2004) Simple secret sharing and threshold RSA signature schemes. J Inf Comput Sci 1:259–262