International Journal of Information Management 35 (2015) 154–159

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Advanced techniques for knowledge management and access to strategic information

Lidia Ogiela*

AGH University of Science and Technology, Al. Mickiewicza 30, PL-30-059 Krakow, Poland

ARTICLE INFO

Article history:

Keywords:
Knowledge management
Strategic information
Cryptographic algorithms
Secret sharing

ABSTRACT

This publication discusses advanced knowledge management techniques based on information splitting and sharing algorithms for secret, strategic information. Information splitting techniques will be dedicated to problems of secure information storage and managing sets of strategic data. The management of strategic corporate/organisational data will provide the illustration of the discussion of knowledge management which constitutes the starting point for advanced information management processes. Advanced knowledge management techniques will be discussed using the example of applying cryptographic algorithms in processes of managing information and access to it. Restricted access to strategic corporate information means that this type of data must be stored securely and must not be disclosed to unauthorised individuals. The use of cryptographic algorithms for strategic information sharing keeps this data completely confidential and ensures no access of unauthorised people to the knowledge possessed.

1. Introduction

Knowledge management is a very difficult task in the contemporary world. This is because it poses challenges concerning the correct management and is considered to be one of the most difficult of all currently known management problems (Laudon & Laudon, 2002; Ogiela, 2013a). What is this difficulty about? Firstly, it relates to defining what knowledge really is, in precise terms. In addition difficulties as seen in the way of using knowledge as well as the intentions and methods of using it. When knowledge is used for cognitive, scientific, interpretation purposes, it is easy to define and identify (Bodzioch & Ogiela, 2009; Hachaj & Ogiela, 2011; Ogiela & Ogiela, 2012a; Ogiela, 2008a, 2008b, 2008c). However, when it is used for unethical purposes, it becomes difficult to define and it is difficult to confirm that this or that layer of knowledge was used. In this case, an ethical contradiction arises: knowledge which is perceived as an element of the ethical world can be used for unethical purposes. It is, therefore, important what purpose information, data and messages constituting elements of the knowledge are used for, who uses the collected knowledge and what for, whom the results of the use knowledge concern, etc.

It is very similar with regard to identifying, defining, and sourcing knowledge in an organization (Buchanan & McMenemy, 2012; Ogiela, 2013a; TalebiFard & Leung, 2011). How to collect knowledge, how to use the collected knowledge, in what case to use it, etc.: decision-makers are constantly struggling with these and similar questions. However, answering these questions does not yet guarantee that the organisation will operate correctly. It is only the efficient management of knowledge collected within the organisation that guarantees the correct growth of the company. In management processes, knowledge is understood as the correct use of all reliable information about the past, present and future situation of the company, its environment, the reasons for the current situation and also the ability to project the future state. Knowledge accumulated at various levels allows management processes to be improved, but only that collected at the highest level, i.e. the strategic decision-making one, allows the organisation to be managed effectively because it enables the intellectual capital of the organisation to be consolidated. Just collecting knowledge is obviously insufficient, what is important in knowledge management processes is using it properly. IT systems for knowledge management which improve management processes differ depending on whether the knowledge is centralised or decentralised. In every system, however, it is important that information should be transferred efficiently and reliably. If information is distorted or omitted, the entire knowledge management process becomes useless (Bernstein & Wild, 1999; Ogiela & Ogiela, 2011; Ogiela, 2013b, 2013c).

In traditional knowledge management systems, layers of information form an element supporting corporate management. This situation is presented in Fig. 1.

* Tel.: +48 12 617 45 07.
E-mail address: logiela@agh.edu.pl

http://dx.doi.org/10.1016/j.ijinfomgt.2014.11.006
0268-4012/

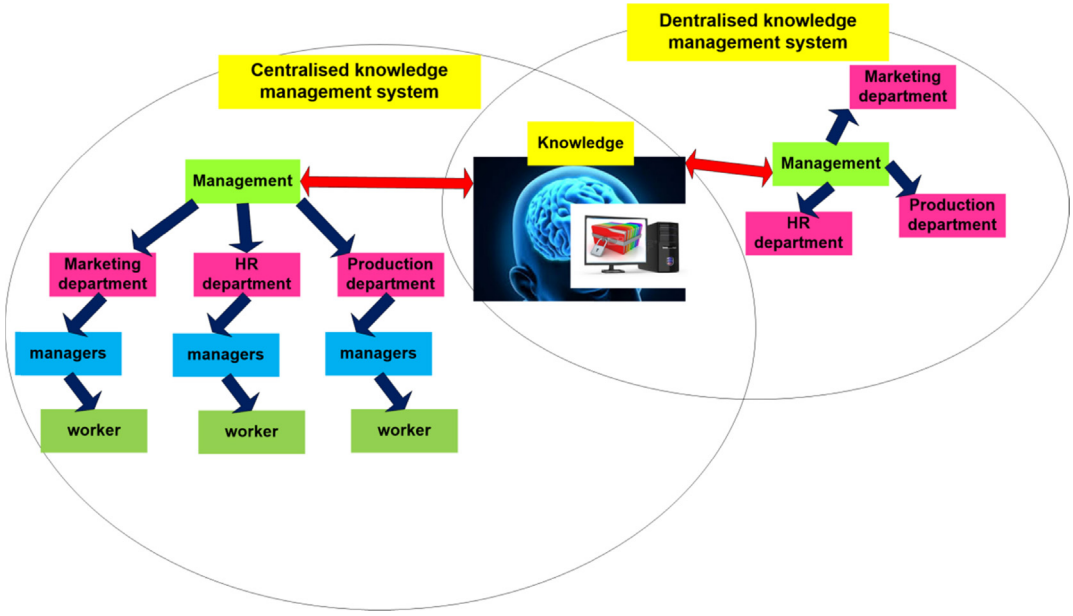

Fig. 1. Knowledge layers in knowledge management systems.

In both cases, managers gain the most accurate knowledge possible in order to collect the complete information about the company situation, its environment, competitive conditions, the drivers of the current and future company success, the reasons for its failure, etc. There are, however, differences in how knowledge is transferred between the remaining elements of the entire system. These differences are mainly due to the design and type of organisational structures to which they are dedicated.

In a centralised system, knowledge forms one of many elements of the entire management process, whereas in a decentralised one, it constitutes one of few elements of the entire system. Consequently, in knowledge transferring processes, it is better to use decentralised systems as they pose a lower risk of possible distortions or errors at each stage of knowledge transfer.

Knowledge management processes do not apply solely to the methods of collecting knowledge, processing it and using it to improve the operational processes of the organization. Obtaining knowledge from generally accessible information resources implies the use of information management processes including the following topics (Ogiela & Ogiela, 2014):

- planning, designing and implementing an information strategy;
- the information flow in external communication;
- the information flow in internal communication;
- ensuring investment funds for developing and implementing new IT solutions;
- the correct use of available IT solutions;
- information quality management;
- ensuring data security;
- ensuring training and development of the IT staff and system users;
- the ability of the company to effectively interact with the information market;
- integrating information systems used at various levels.

Information management processes precisely indicate directions in which knowledge management process support will be used to secure strategic information. The analysis of this subject forms the basis of this work, and the related methods will be discussed in subsequent chapters.

2. Cryptographic algorithms for strategic data division

The correct, i.e., secure, process of managing knowledge within a business organisation/enterprise/company can be ensured by using cryptographic information division algorithms in such a way that company security is entrusted not to one person but to a certain trusted group. Such capabilities are offered by cryptographic algorithms which divide information. These protocols are used to divide information within a given group of secret trustees. The secret consists in secret, strategic information which must not be disclosed publicly. The trustee can be either a person or a computer. The data division algorithm is used to divide this data (depending on the cryptographic algorithm applied) within a selected group of secrets trustees. In the information division process, security must be ensured:

- during the allocation of shares of the secret to each of their holders;
- at the stage when these holders store their shares; and
- at the stage when these shares are combined to recreate the split information.

Data division techniques are classified into two basic groups.

The first comprises information splitting algorithms, designed for splitting information into shares, which are distributed to all secrets trustees. Each trustee receives their share of the split secret, and all shares must be combined to recreate the split information. The lack of even only one share makes it impossible to recreate the original information.

The second group comprises data sharing algorithms. This type of algorithm is used to divide information within a selected group of secret trustees, each of whom receives their share of the divided secret. However, to recreate the divided information, it is necessary to combine a number of secret shares (which number is selected when the algorithm is defined).

Information sharing protocols enable any data division between n protocol participants. Theoretical foundations of data sharing algorithms are described, among others, by (Menezes, van Oorschot, & Vanstone, 2001; Ogiela & Ogiela, 2014; Schneier, 1996; Shamir, 1979; Tang, 2004):

- Shamir's algorithm;
- Tang's algorithms;
- Lagrange's interpolation polynomial algorithm;
- Blake's vector algorithm;
- Karnin–Greene–Hellman algorithm;
- Asmuth–Bloom algorithm.

For the knowledge management tasks supporting strategic information management processes which the Author researches, she has selected information sharing algorithms because of the divided information is reconstructed by combining only a selected number of shares of the split information. The author of this publication has used the so-called (m, n)-thresholding schemes for sharing strategic information. In this type of algorithms, the information is shared between any number n of protocol participants, and to reconstruct it, it is necessary to combine at least m shares of the divided secret $(m < n)$. Examples of this type of algorithms were proposed, among others, by Shamir (1979) and Tang (2004).

2.1. Shamir's algorithm for strategic information sharing

Strategic information I is coded into the form of an integer, and then divided among any number n representing the number of people who will receive their shares of the secret. Any subgroup of this group made up of any m individuals $(m < n)$ can recreate the divided information I.

The first prime number p greater than the number of possible shadows of information I which will be shared is chosen. The number p fulfils the condition $p > \max(I, n)$. Then, $m-1$ is randomly chosen as the number of independent factors of the polynomial $a_1, \ldots, a_{m-1}$ which fulfil the condition $0 \le a_j \le p-1$ and which randomly define the polynomial of the $m-1$ degree over a field of integers in a modulo p arithmetic, of the following form (Shamir, 1979):

$$F(x) = \sum_{j=0}^{m-1} a_j x^j \bmod p$$

Factors of the polynomial $F(x)$ are selected randomly and constitute the secret. After the shadows have been distributed, these factors are rejected. Shadows are produced by calculating the value of the polynomial at n different points, $k_i = F(x_i) \bmod p$ where $1 \le x_i \le p-1$.

The last stage of the information sharing protocol is to allocate shadows k_i to individual persons together with the values of arguments x_i.

A polynomial of the $m-1$ degree has m independent factors $a_0 = I, a_1, \ldots, a_{m-1}$, where to reconstruct information I any m of the distributed shadows is sufficient. These define m equations with m unknowns, whose solution determines the values of all m factors of the polynomial including $a_0 = I$, i.e., the secret I.

Factors of the polynomial $F(x)$ of a degree lower than m, defined by m points (x_i, k_i), $1 \le i \le m$, can be expressed by Lagrange's interpolation formula (Schneier, 1996):

$$F(x) = \sum_{i=1}^{m} k_i \prod_{1 \le j \le m, j \ne i} \frac{x - x_j}{x_i - x_j}$$

As $F(0) = a_0 = I$, the shared secret can be represented by the following formula:

$$I = \sum_{i=1}^{m} c_i k_i$$

where:

$$c_i = \prod_{i \le j \le m, j \ne i} \frac{x_j}{x_j - x_i}$$

When m shadows are known, the value of secret I is calculated as the linear combination of the shadows.

2.2. Tang's algorithm for strategic information sharing

Let F be the message domain, k and n – positive integer such that $k \le n$, and d be the secret belonging to set F. The protocol distributes the shared information between n participants of the scheme, allocating exactly one share to each. Combining k or more shadows is sufficient to reconstruct the original message. At the same time, $m-1$ or fewer shares are not enough to reconstruct the shared secret where $m = [n/(n-k+1)]$, and $\lceil x \rceil$ represent the smallest integer greater than or equal to x (Tang, 2004; Menezes, van Oorschot, & Vanstone, 2001).

In order to generate the shadows for scheme participants, numbers $d_0, d_1, \ldots, d_{n-2}$ belonging to the domain F are randomly selected and the value of d_{n-1} is computed (Tang, 2004):

$$d_{n-1} = d - \sum_{i=0}^{n-2} d_i$$

Let us use A_j to represent the following set:

$$A_j = \{(i \bmod n, d_{i \bmod n}) : j \le i \le n-k+j\}$$

where: $j = 0, 1, \ldots, n-1$.

After all sets A_j have been determined, they are distributed among scheme participants as follows: The j_{th} participant receives the set A_j.

In this algorithm, combining any k shares is sufficient to reconstruct the shared message. For this purpose, one has to calculate the number $d = \sum_{i=0}^{n-1} d_i$, which constitutes the solution. Combining $m-1$ or fewer shares is not enough to reconstruct the secret.

Information sharing protocols allow the shared information to be recreated by any subgroup of secrets trustees. The number of shares of the divided secret required to recreate the complete information is determined when the information sharing scheme is defined. The operating principle of information sharing protocols is presented in Fig. 2.

3. Example of access knowledge management for strategic information

Managing strategic information by using cryptographic data sharing algorithms allows the information constituting company/corporate/organisational secrets to be secured from being disclosed to unauthorised individuals. In addition, it significantly contributes to improving processes of corporate strategic information management by taking this information out of circulation between units and individuals not authorised to learn and process it. The requirement to split strategic information within a selected group of individuals allows this information to remain secret even if one of the secret trustees decides to disclose it. This is because such disclosure is impossible because all trustees of shares of the divided information only hold shares of information which are useless on their own. In contrast, to recreate the shared information it is necessary to combine a selected number of secrets shares which solves the problem that a single member of the entire group of trustees of secret information shares could veto the disclosure of this information.

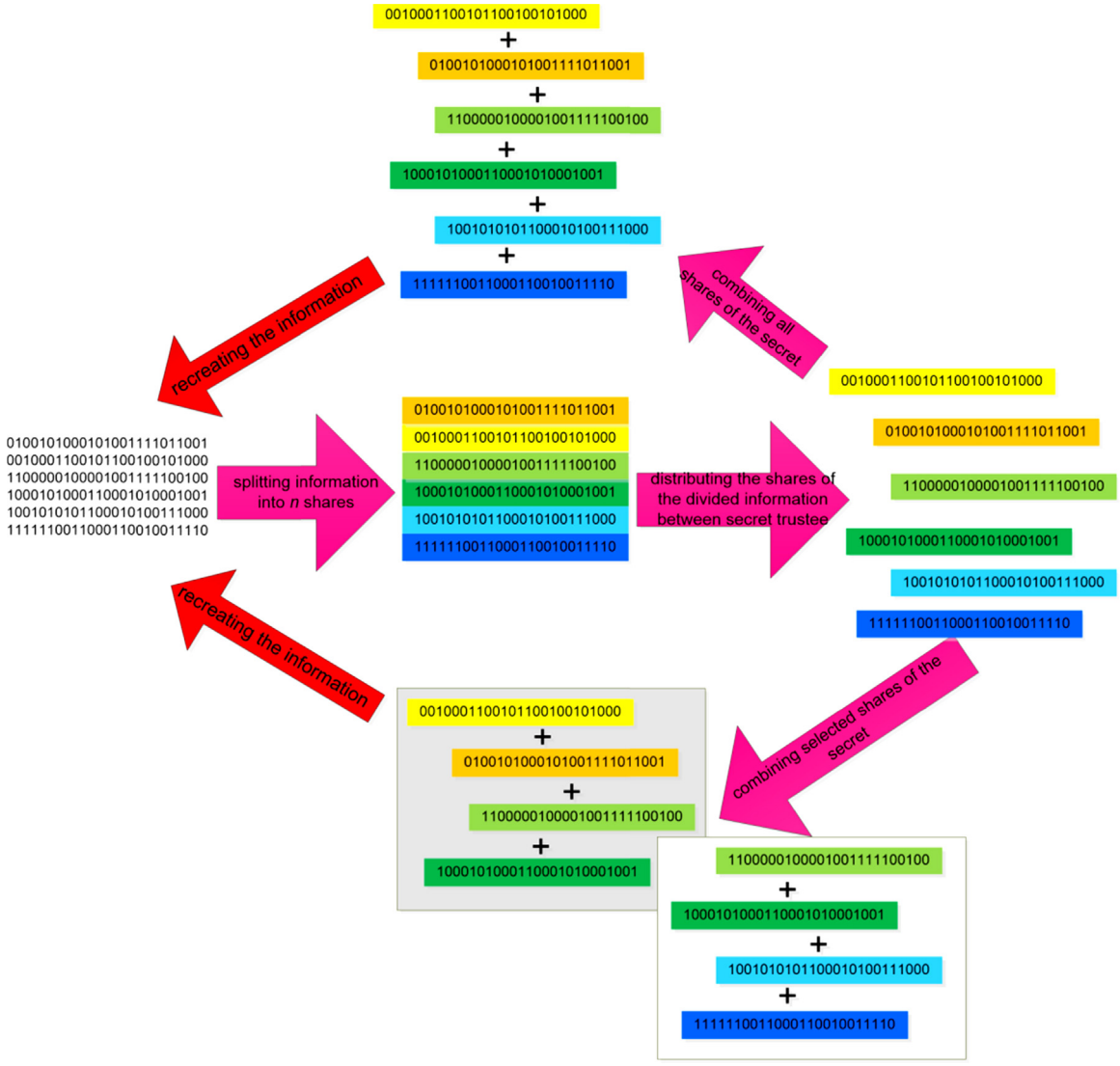

Fig. 2. General operating principle of information sharing schemes.

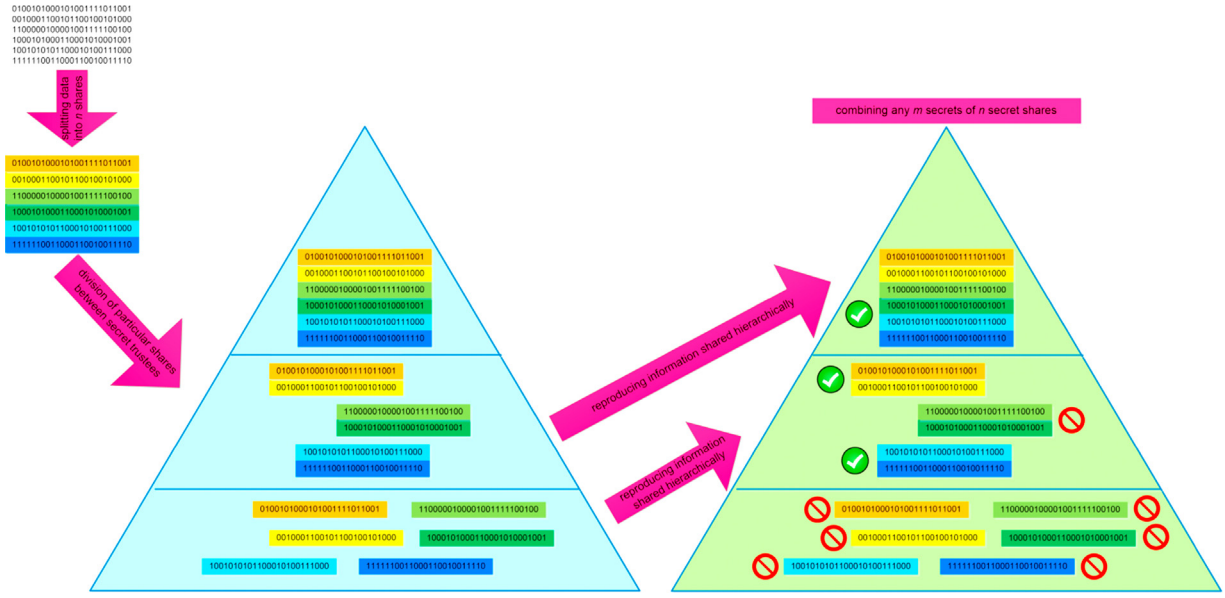

Fig. 3. Information sharing and recreation in hierarchical structures.

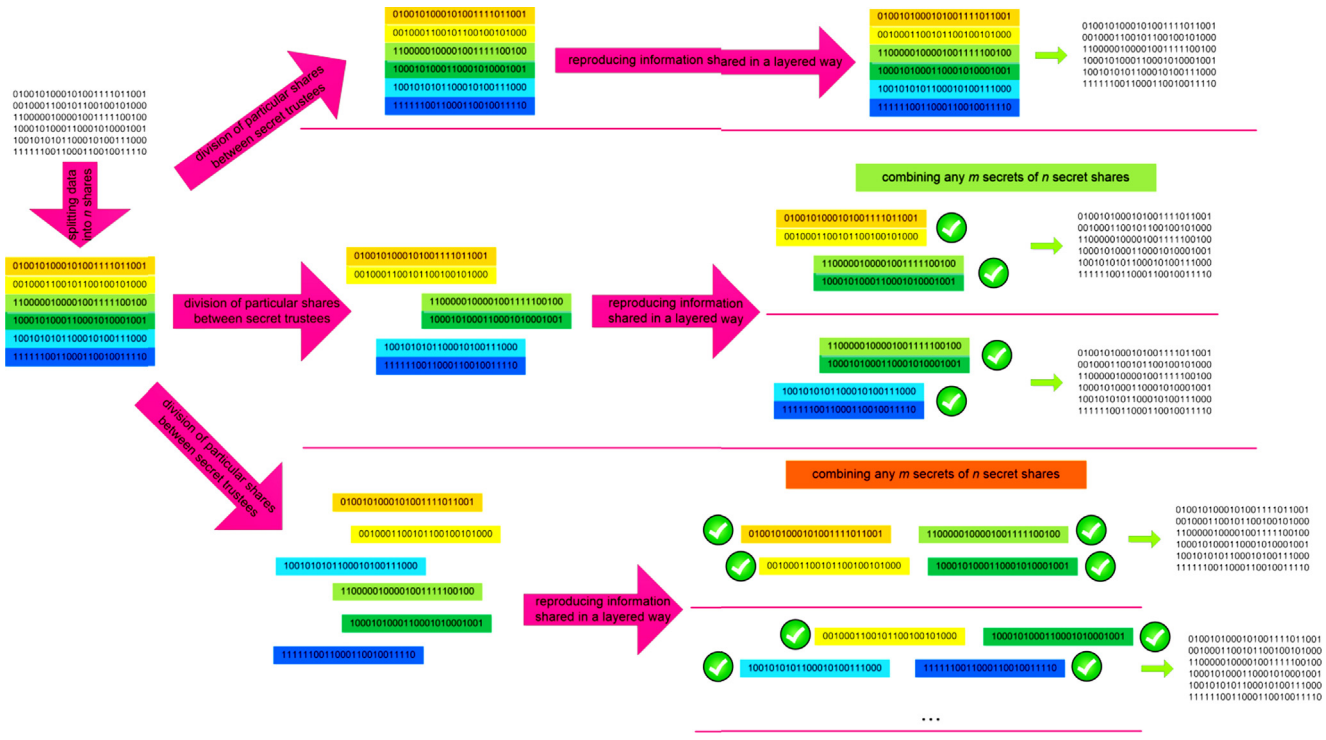

Fig. 4. Information sharing and recreation in layered structures.

The security of this type of solutions is also ensured by the ability of members of superior structures to recreate the information (Ogiela & Ogiela, 2010; Ogiela & Ogiela, 2012b). This is because if information is shared in hierarchical structures, it can only be recreated by the higher level structure (Fig. 3).

If shared information is held in layered structures, it will only be recreated by authorised members of a given layer (Fig. 4).

If what is divided is strategic information, it is possible to share this information using thresholding schemes. Information is then recorded in the binary form with the selected length of information blocks. The next to be defined are the number of shadows, also determining the number of trustees of the shared information, and the minimum number of trustees who can correctly recreate the shared information. This information is divided among the selected number of secret trustees, and can be recreated using any shares, as long as their number is the same as the number determined at the algorithm definition stage as required for recreating the information. This situation is illustrated in Fig. 5.

Actual information with the contents "*solvency problems*" has been presented in the form of bits with the length of 2. Then, after a long prime number has been generated, the strategic information was divided into four shadows and it was specified that any two of them will be sufficient to recreate the strategic information. Shadows two and three were chosen for recreating the information. As a result of their combination, the original information was recreated. To recreate information, one can combine any two of the four generated shadows, but if any number of shadows greater than two is combined, the strategic information will also be recreated.

This method can be used to hide any important information whose possession is crucial for company growth. Information sharing algorithms ensure that this kind of data is not accessible to unauthorised individuals. Their use means that information storage is delegated to system users, and the recreation of this information requires the consent of a selected portion of its holders.

As a result of using strategic information sharing algorithms, the stewardship of knowledge collected within the organisation

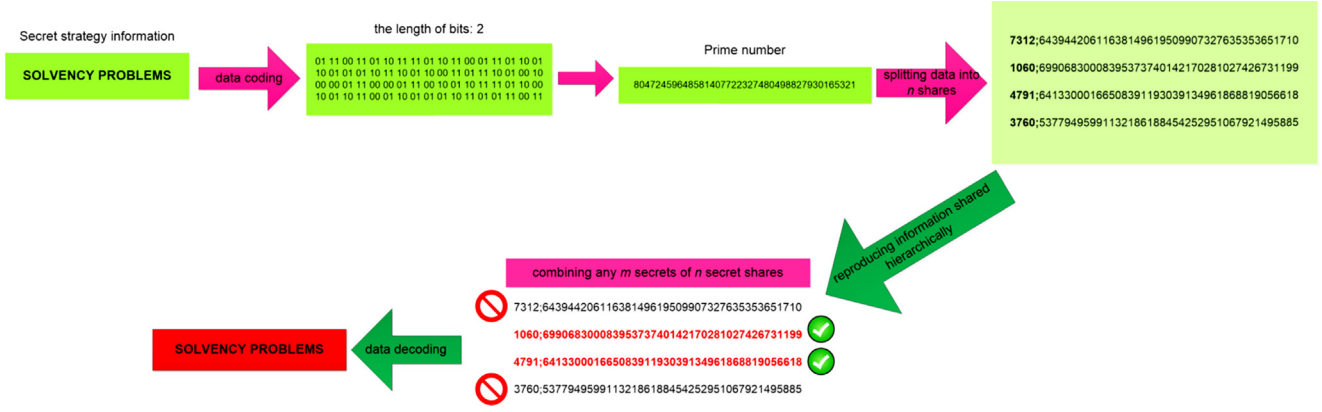

Fig. 5. Strategic information sharing and recreation using an (m, n)-thresholding scheme.

significantly improves management processes. These improvements apply to the following areas:

- corporate financial management;
- HR information management;
- development strategy definition;
- managing information as part of information circulation process within the enterprise;
- company growth;
- competitive market;
- competitive strategy development.

4. Conclusions

Advanced knowledge management techniques focus on processes of knowledge collection, selecting knowledge currently useful for developing the company/organisation and also knowledge which is not necessary for the proper development of the organisation now, but can be used later depending on the development of the organisation and its environment.

Knowledge management techniques now focus not only on the use of IT systems to effectively manage knowledge or information, but primarily on the use of techniques for information sharing within the appropriate authorities and its storage until it becomes significant for the development of the organisation/enterprise. Information splitting techniques, the correct information storage and its use in the necessary situations imply the application of cryptographic problems which ensure the security of the solutions used.

Information can be divided within a given organisation in various ways. The method of secure information recreation, without disclosing contents of this information to an authorised individuals, forms an important element of the entire information division process. This is why information sharing protocols are better in strategic information management processes. Access to strategic information is restricted and dedicated to a selected group of individuals. Consequently this method of hiding important, strategic information that cannot be disclosed to the public employs information sharing and guarantees the highest security as unauthorised individuals cannot access knowledge bases containing strategic information.

Acknowledgment

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

References

Bernstein, L., & Wild, J. (1999). *Analysis of financial statements* (5th ed.). New York: Amazon.

Bodzioch, S., & Ogiela, M. R. (2009). New approach to gallbladder ultrasonic images analysis and lesions recognition. *Computerized Medical Imaging and Graphics*, *33*(2), 154–170.

Buchanan, S., & McMenemy, D. (2012). Digital service analysis and design: The role of process modelling. *International Journal of Information Management*, *32*(3), 251–256.

Hachaj, T., & Ogiela, M. R. (2011). A system for detecting and describing pathological changes using dynamic perfusion computer tomography brain maps. *Computers in Biology and Medicine*, *41*(6), 402–410.

Laudon, K. C., & Laudon, J. P. (2002). *Management information systems – Managing the digital firm* (7th ed.). New Jersey: Prentice-Hall International: Inc.

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

Ogiela, L. (2008a). Cognitive systems for medical pattern understanding and diagnosis. In I. Lovrek, R. J. Howlett, & L. C. Jain (Eds.), *Knowledge-based intelligent information and engineering systems* (pp. 394–400). Berlin, Heidelberg: Springer-Verlag.

Ogiela, L. (2008b). Modelling of cognitive processes for computer image interpretation. In D. Al-Dabass, A. Nagar, H. Tawfik, A. Abraham, & R. Zobel (Eds.), *EMS 2008 European Modelling Symposium, Second UKSIM European Symposium on Computer Modeling and Simulation* (pp. 209–213). United Kingdom: Liverpool, 8–10 September.

Ogiela, L. (2008c). *Syntactic approach to cognitive interpretation of medical patterns. Intelligent robotics and applications, book series* Lecture Notes in Artificial Interlligence 5314. Berlin, Heidelberg: Springer-Verlag.

Ogiela, L. (2013a). Data management in cognitive financial systems. *International Journal of Information Management*, *33*, 263–270.

Ogiela, L. (2013b). Semantic analysis and biological modeling in selected classes of cognitive information systems. *Mathematical and Computer Modelling*, *58*, 1405–1414.

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

Ogiela, L., & Ogiela, M. R. (2011). Semantic analysis processes in advanced pattern understanding systems. In T-h. Kim, H. Adeli, R. J. Robles, & M. Balitanas (Eds.), *Advanced computer science and information technology. Comunications in computer and information science 195* (pp. 26–30). Berlin Heidelberg: Springer-Verlag.

Ogiela, L., & Ogiela, M. R. (2012). *Advances in cognitive information systems. COSMOS 17*. Berlin Heidelberg: Springer-Verlag.

Ogiela, M. R., & Ogiela, U. (2010). The use of mathematical linguistic methods in creating secret sharing threshold algorithms. *Computers & Mathematics with Applications*, *60*(2), 267–271.

Ogiela, M. R., & Ogiela, U. (2012). DNA-like linguistic secret sharing for strategic information systems. *International Journal of Information Management*, *32*(2), 175–181.

Ogiela, M. R., & Ogiela, U. (2014). *Secure information management using linguistic threshold approach*. London: Springer-Verlag.

Schneier, B. (1996). *Applied cryptography: Protocols, algorithms, and source code in C*. New York: Wiley.

Shamir, A. (1979). How to share a secret. In *Communications of the ACM* (pp. 612–613).

TalebiFard, P., & Leung, V. C. M. (2011). Context-aware mobility management in heterogeneous network environments. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *2*(2), 19–32.

Tang, S. (2004). Simple secret sharing and threshold RSA signature schemes. *Journal of Information and Computational Science*, *1*, 259–262.

Dr Lidia Ogiela Computer scientist, mathematician, 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 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 of more than 100 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, and Cognitive Science Society. Currently she is at the associate professor position, and works in Management Faculty at the AGH University of Science and Technology.