Intelligent UBMSS Systems for Strategic Information Management

Lidia Ogiela, Marek R. Ogiela

HAL Id: hal-01506573

https://inria.hal.science/hal-01506573

Submitted on 12 Apr 2017

Intelligent UBMSS Systems for Strategic Information Management

Lidia Ogiela, Marek R. Ogiela

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

Abstract. In this publication will be described the most important features of UBMSS cognitive information systems, as well as security issues connected with these new generation information systems. Such systems are mainly designed to perform an intelligent information management based on semantic analysis of data merit content. In paper will be also presented some possibilities to develop such systems for strategic information management in state or government institution. The paper will describe both UMBSS internal safety features, and external possible application of authentication procedures along with intelligent information management.

Keywords: Strategic information management, security of information systems, cognitive systems in homeland security

1   Introduction

Intelligent UBMSS (Understanding Based Management Support Systems) systems are one of the modern classes of cognitive information systems. Cognitive analysis processes are characteristic of the intellectual processes running in the human brain, particularly those of analyzing, interpreting, reasoning, and forecasting about specific situations, meanings and the significance of information.

Cognitive reasoning consists in analyzing and understanding the contents and the semantics of the data examined. Such examination may be very important during strategic information management in different companies or institution.

In such systems the semantic analysis is based on a lexical analysis in which the structure of a given word is used to describe it, and to find the meaning of the content of the word. The basis for this analysis is a specific language to which the above element belongs, and the process of understanding results from comparing the previously recorded expectations concerning specific features of data with the features from the input information. The set of expectations concerning the anticipated features of the analyzed elements is produced by analyzing the knowledge of experts whose expectations of the meanings of particular situations are presented in the system database. This set of semantic hypotheses is compared with the stream of input data, and this leads to cognitive resonance [2, 3, 4,5]. This process produces a list of selected inter-

pretations which were found to correspond to the analyzed input data – this leads to the stage of understanding the analyzed data.

Presented cognitive resonance functions may be used to guarantee the security and safety features during management of strategic or secret information, both in layered and hierarchical management structures.

2 An Idea of UBMSS Cognitive Systems

The general goal of UBMSS is to support enterprise management and handling in secure manner of strategic information, as well as its distribution for authorized persons or participants of communication protocols. Such systems may also be used for another procedures mostly connected with economical task like focus on the correct choice of the right economic ratios and theirs prediction for near future. These ratios precisely reflect the business activity of a given enterprise, its standing, its financial result, and are also an expression of the record and the generalization of specific economic events.

During our research we could also analyze some security features of such systems and theirs possibility of theirs application for strategic information management in the form of secret information sharing for layered and hierarchical structures.

3 UBMSS Systems for Strategic Information Management

Using UBMSS systems, an information is divided within institutions or organizations regardless of its type or the purpose for which the organization collects it. The significance of information splitting may depend on the method of its splitting, the purpose of splitting it, and the type of information. The significance of information sharing, on the other hand, may depend on its importance and the meaning it contains for the specific organization. If information is important and of great materiality for the organization or for e.g. external organizations, then it makes sense to attempt sharing this information to protect it and secure it from disclosure to unauthorized persons (or organizations). When defining the type of information to undergo the splitting or sharing process, we should consider its 'character' determined by its confidentiality, significance and importance, because only important information justifies applying the method of its division and the effort to do so.

Multi-level information division algorithms are named after the type of division applied. This division can be hierarchical or by layers. The principal difference between the presented types of divisions concerns the method of introducing the division itself. When a division is made within homogenous, uniform groups of layers, then it is a layer division, whereas if the division is made regardless of the homogeneity of the group or layer but by reference to several groups ordered hierarchically, it is a hierarchical division [8].

A layer division is thus a division made relative to a given layer, while a hierarchical division accounts for the hierarchy (dependency) of the structure or more structures relative to one another.

Information can be divided both within the entire structure in which some hierarchical dependency is identified, within a given group, or within any homogenous layer. This is why, depending on the type of information divided, it makes sense to identify correctly selected information dividing algorithms.

The division of information between the members of a given group in which everyone has the same privileges is a layer division.

A hierarchical division is characterized by the ability to make any division of secret information in the way determined by the access rights at individual levels of a hierarchical structure.

4   Types of UBMSS Systems

There are various methods of information protecting from being accessed by persons not authorized to learn it. Based on such different approaches we can define two types of UBMSS systems. The first class may contain the procedures in which the secret information will be secured using some individual personal biometrics, and the second one based on mathematical linguistic formalisms [7].

The first class of UBMSS systems are connected with biometric threshold schemes [10, 11], which particularly use some most important physical and biometric features like the iris, the shape of fingerprints, hand bones or veins [9], anatomical features [1], face, the structure of blood vessels [6] and also the DNA code [10].

The second class of UBMSS systems uses linguistic coding processes, which are based on the use of mathematical linguistic formalisms, particularly grammatical formalisms to record and interpret the meaning of the secured data. Linguistic coding processes are used because of the ability to execute generalised information coding similar to DNA cryptography [10], but in UBMSS systems it is also possible to code longer bit sequences containing more than 2 bits of information. This coding is done using terminal symbols introduced in special grammar.

5   Example of Application UBMSS System for Strategic Information Management

This section presents an example of information splitting using UBMSS system and the distribution of secret parts with the use of the linguistic or biometric threshold schemes. This example represents a simplified model aimed at demonstrating the opportunities offered by UBMSS systems to create and distribute secret information between persons at various management levels or employees at various organisational levels. The UBMSS schemes for information distribution enable generating and distributing parts of the shared information both in layered and hierarchical structures. For this reason, the discussion of the example shown in Fig. 1 will apply to executing precisely these sharing types.
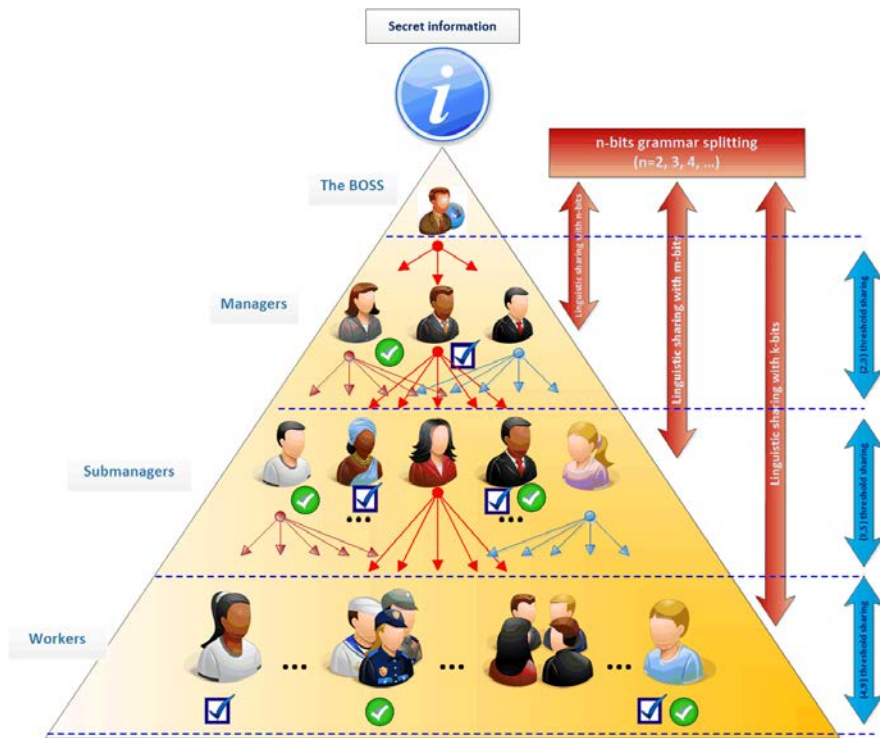
Fig. 1 An example of splitting a secret in the layered and hierarchical way

The first case presented in the example diagram in Fig. 1 concerns the method of sharing and distributing a secret for individual layers in a management pyramid.

These layers may be treated as completely independent, and then the highest authorities will share the secret in various layers independently, but the sharing will be done in various ways using linguistic threshold schemes based on various grammars, i.e. coding the shared input data with bit blocks of different lengths. In Fig. 1 this is marked with vertical red arrows of various lengths. In such layered sharing, employees at a given level are equal and have the same rights to access the secret data, but individual layers stay completely independent, so staff from a given management level cannot cooperate with individuals from other management layers when restoring the secret.

However, as the highest authorities of the enterprise or the arbitrator performing the sharing may also provide lower levels with information about the grammar used (or biometric information) for this sharing, an additional opportunity arises for information to flow between individual management layers, causing a transition from a layered structure to a hierarchical one.

Fig. 1 also demonstrates that hierarchical sharing can be executed in such a way that the secret shares obtained at various levels of the management hierarchy can be shared again using a selected threshold scheme and information about the chosen formal grammar (blue arrows of equal lengths joining individual layers of the man-

agement pyramid). In this protocol, every share of the secret generated for a selected employee may be shared at the lower level between a greater number of staff of that lower level.

When we analyse the information sharing procedure in hierarchical structures, the Boss holds important information which can be shared between his/her subordinates observing layer relationships, i.e. employees of a given level are equal and have equal rights to access the secret data under consideration. However, individual layers are not completely separated from one another in information terms and in this regard to not retain their independence, as secret shares at a given management layer can, at subsequent steps, be shared between selected employees of a lower level. This procedure can be repeated for further, still lower layers.

Within such a structure, the original information can be reconstructed in any layer by combining the required number of shadows or using shares coming from different layers. In the second case, a greater number of shares from lower levels is required to reconstruct selected shares from higher layers.

6 Security Features of UBMSS Systems

As was noted before the UBMSS systems could guarantee the security of strategic information and also some safety features during performing secret distribution. The most important features of such systems are following:

- UBMSS systems are suitable for dividing important strategic data and assigning its shares to members of the authorized group;
- UBMSS systems can handle any digital data (text or image) which needs to be intelligently divided among authorized persons and then possible to secretly reconstruct;
- UBMSS systems may be used in different economical management structures e.g. hierarchical, divisional, functional etc.

7 Conclusions

In this paper were presented the cognitive UBMSS systems designed for the secure information management in various management structures. Such systems have the ability to perform a semantic analysis of information which allow to classify it for different semantic categories. Such semantic analysis may further supporting decision-making processes in particular institution or company. Such systems allow also to perform an intelligent information management especially for important, and strategic data. In this paper there were described such possibilities, and also defined two different classes of secure information sharing, especially based on linguistic approach as well as based on some personal biometric features [12]. It seems that in near future such systems will play an increasing role in developing new solutions in areas of very special and strategic information management, especially for government use or homeland security areas.

References

1. Bodzioch S, Ogiela MR (2009) New approach to gallbladder ultrasonic images analysis and lesions recognition. Comput. Med. Imaging Graph. 33:154–170
2. Cohen H, Lefebvre C. (Eds.) (2005): Handbook of Categorization in Cognitive Science. Elsevier, The Netherlands
3. Meystel AM, Albus JS (2002) Intelligent Systems – Architecture, Design, and Control. Wiley & Sons, Inc., Canada
4. Ogiela L (2008) Syntactic Approach to Cognitive Interpretation of Medical Patterns, 1st International Conference Intelligent Robotics and Applications, Wuhan, China, Oct 15-17, 2008, Lecture Notes in Artificial Intelligence, Vol. 5314, pp. 456-462
5. Ogiela L (2008) Cognitive systems for medical pattern understanding and diagnosis, 12th International Conference on Knowledge-Based Intelligent Information and Engineering Systems, Zagreb, Croatia, Sep 03-05, 2008, Lecture Notes in Artificial Intelligence, Vol. 5177, pp 394-400
6. Ogiela L (2009) UBIAS Systems for Cognitive Interpretation and Analysis of Medical Images. Opto-Electronics Review 17(2):166-179
7. Ogiela L, Ogiela MR (2009) Cognitive Techniques in Visual Data Interpretation, Studies in Computational Intelligence 228, Springer-Verlag Berlin Heidelberg
8. Ogiela MR, Ogiela U (2010) The use of mathematical linguistic methods in creating secret sharing threshold algorithms. Computers and Mathematics with Applications, 60(2):267-271
9. Ogiela L, Ogiela MR (2012) Advances in Cognitive Information Systems, COSMOS 17, Springer-Verlag, Berlin-Heidelberg
10. Ogiela MR, Ogiela U (2012) DNA-like linguistic secret sharing for strategic information systems. International Journal of Information Management 32:175–181
11. Ogiela MR, Ogiela U (2012) Linguistic Protocols for Secure Information Management and Sharing. Computers and Mathematics with Applications, 63(2):564-572
12. Peters W (2011) Representing Humans in System Security Models: An Actor-Network Approach. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2(1):75-92