Advanced Techniques for Computer Sharing and Management of Strategic Data

Marek R. Ogiela, Lidia Ogiela, Urszula Ogiela

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

Abstract. In the paper will be presented some advances in the area of computer methods used for encryption and division of confidential data, as well as modern approaches for management of splitted information. Computer techniques for secret information sharing aim to secure information against disclosure to unauthorized persons. The paper will present algorithms allowing for information division and sharing on the basis of biometric or personal features. The development of computer techniques for classified information sharing should also be useful in the process of shared information distribution and management. For this purpose there will be presented a new approach for information management based on cognitive information systems.

Keywords: cryptographic protocols, bio-inspired cryptography, secret sharing algorithms

1 Introduction

In the recent years there were developed many advanced cryptographic procedures for secure information splitting or sharing. Some of them are very intuitive and simple, but some others are more advanced and often dedicated for sharing of particular typed of data e.g. visual information. Among such procedures we can also find some interesting examples of splitting procedures, which are based on using some special input data to the splitting algorithm. Such universal approach for information sharing may be very interesting, when as input values we can also put biometric or personal information for generation of particular shares or information shadows. In the next section we'll try to describe some important features of such crypto-biometric techniques, which may be used for secret sharing tasks. Additionally we'll also try to present some others procedures, especially oriented for performing management task, and allowing for intelligent information shares distribution using a new classes of cognitive information systems. Such systems may play a great role in future, developing the new areas of cognitive cryptography [12].

2 Crypto-biometrics Approach

A lot number of cryptographic methods for secret splitting or sharing are developed. Some of them may also use individual human information or biometrics during generation particular number of secret shares. For such purposes may be used different personal information, starting from the physical personal features, as well as standard biometrics or non-standard biometric features [13]. The most popular physical and biometric features are: iris features, fingerprints patterns, facial features, blood vessels layout or even DNA code. Among non-standard biometric we can find some personal information connected with any pathological changes observed on medical diagnostic visualization [1], obtained during medical examination of particular human body parts or internal organs. Examples of such non-standard personal biometrics can be found in [13], and it may be connected with coronary arteries structures, brain perfusion parameters or other similar values [3, 4].

The process of information splitting with using biometrics or personal information can be executed by two different ways i.e. by a layer split and by a hierarchical split. The former means splitting the information between n secret holders and its reconstruction by n-m trustees of the secret. The latter case means that the secret is split between n holders of the secret, but the information can be reproduced by superior groups of secret holders within which the specific secret has been split into k parts ($k < n$). Thus the splitting methods depend on the purpose for which the information is split and concealed.

Using biometrics during sharing procedure is possible thanks to application of linguistic coding processes [14, 15, 16]. Those procedures are based on the mathematical linguistic formalisms, particularly sequence, tree and grammatical formalisms to record and interpret the meaning of the analysed biometric data. Linguistic coding processes are used because of the ability to execute generalized information coding as in DNA cryptography. In the traditional DNA coding model, one- or two-bit coding is used (utilizing one of the four nitrogen bases or nitrogen bonds). In DNA cryptography any personal information can be combined with biometric features. In linguistic coding, it is possible to code longer bit sequences containing more than two bits of information [17, 18, 19]. This coding is done using terminal symbols introduced in this grammar, and lengthening the coded blocks directly proportionally contributes to accelerating information splitting and reproduction, as well as to increasing the secret component containing information on the grammar used.

The coded biometric information recorded in the form of an n-bit representation is split using a selected information splitting algorithm. The (m, n)-threshold algorithm allows this information to be reproduced by combining at least m of all n shares of the secret. Combining m shares of the secret causes the information to be reproduced in a coded version which can be fully understood only after executing its semantic analysis consisting in a grammatical reasoning carried out for the coded data set.

3 Cognitive Systems for Strategic Information Management

Application of cryptographic procedures for secret sharing allow us to obtain particular number of secret shares. Having splitted information the main problem remains in distribution and intelligent management of generated information shares. In our research we've tried to introduce a new approach based on using cognitive information systems. Cognitive systems allow understanding the contents and the semantics of the data examined [2, 5, 6, 7, 8]. Such examination may be very important for secure information management. Cognitive systems during application performs cognitive resonance functions, which may be used to guarantee the security and safety features during management of strategic data, both in various management structures.

During application of cognitive systems an information may be divided within particular group of persons or institutions regardless of its type or the purpose. The significance of information splitting may depend on the method of its splitting, the purpose of splitting it, and the type of information. Regarding the accessing privileges for particular persons division of information can be hierarchical (for different accessing grants) or layered (similar privileges). The principal difference between these types of divisions concerns the method of introducing the division itself. When a division is made within homogenous, uniform groups of participants with similar privileges, then it is a layer division, whereas if the division is made regardless of the homogeneity of the group but by reference to several different groups it is a hierarchical division [12]. Hierarchical division presents some dependencies between several different structures.

Finally 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.

There are various methods of information protecting in layered or hierarchical structures, from being accessed by persons not authorized to learn it. Based on such different approaches we can define two types of UBMSS (Understanding Based Management Support Systems) systems [9, 10, 11]. The first class may contain the procedures in which the secret information will be secured using some individual standard or non-standard biometrics, and the second one based on mathematical linguistic formalisms [6]. The first class of such systems are connected with biometric threshold schemes [13], which may use some important physical and biometric features like the iris, fingerprints, hand veins, face etc. [12].

The second class uses linguistic coding processes, which are based on mathematical linguistic formalisms, particularly grammatical formalisms to encode the meaning of the secured data. Linguistic coding processes are very efficient because they have ability to execute generalised information coding similar to DNA cryptography mentioned in previous section [17].

An illustrative example of application of cognitive information systems UBMSS for information sharing and management may be found in [12], but from security point of view we can note that such systems could guarantee the security and integrity of shared information, and also guarantee safety features during distribution of secret

parts. Among many important features we can point out following the most important. Cognitive systems are enough suitable for dividing strategic data and assigning its shares to members of the authorized group. Such systems can handle any digital data (both in visual or text form) which needs to be intelligently distributed among authorized persons and then secretly reconstruct. Such systems may be used in different management structures i.e. hierarchical or divisional.

4 Conclusions

In this paper we have presented some advances in using biometric information and personal characteristics to develop new procedures for secret information sharing and spiltting. Processes of splitting or hiding data are currently used in many fields of life, science and research. Employing linguistic coding methods in the concealment and analysis processes offers the full capability of using personal information for such purposes. Concealing biometric or personal data constitutes a very important problem because it is highly probable that personal data will be taken over by unauthorised persons. The individual DNA code, fingerprints, iris features and many other biometrics may be used during sharing procedure.

Additionally we presented the cognitive 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 systems allow also to perform an intelligent information management for strategic data. There were defined two different classes of secure information sharing, especially based on linguistic approach as well as based on some personal biometric features. 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 [20].

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

References

1. Bodzioch, S., Ogiela, M.R.: New approach to gallbladder ultrasonic images analysis and lesions recognition. Comput. Med. Imaging Graph. 33, 154–170 (2009)
2. Cohen, H., Lefebvre, C. (Eds.): Handbook of Categorization in Cognitive Science. Elsevier, The Netherlands (2005)
3. Hachaj, T., Ogiela, M.R.: A system for detecting and describing pathological changes using dynamic perfusion computer tomography brain maps. Computers in Biology and Medicine. 41(6), 402-410 (2011)
4. Hachaj, T., Ogiela, M.R.: Framework for cognitive analysis of dynamic perfusion computed tomography with visualization of large volumetric data. Journal of Electronic Imaging. 21(4), Article Number: 043017 (2012)
5. Meystel, A.M., Albus, J.S.: Intelligent Systems – Architecture, Design, and Control. Wiley & Sons, Inc., Canada (2002)

6. Ogiela, L.: Syntactic Approach to Cognitive Interpretation of Medical Patterns. Lecture Notes in Artificial Intelligence. 5314, 456-462 (2008)
7. Ogiela, L.: Cognitive systems for medical pattern understanding and diagnosis. Lecture Notes in Artificial Intelligence. 5177, 394-400 (2008)
8. Ogiela, L.: UBIAS Systems for Cognitive Interpretation and Analysis of Medical Images. Opto-Electronics Review. 17(2), 166-179 (2009)
9. Ogiela, L.: Cognitive Informatics in Automatic Pattern Understanding and Cognitive Information Systems. Studies in Computational Intelligence, vol. 323, 209-226, Springer-Verlag Berlin Heidelberg (2010)
10. Ogiela, L., Ogiela, M.R.: Cognitive Techniques in Visual Data Interpretation, Studies in Computational Intelligence, vol. 228, Springer-Verlag Berlin Heidelberg (2009)
11. Ogiela, L., Ogiela, M.R.: Advances in Cognitive Information Systems, COSMOS 17, Springer-Verlag, Berlin-Heidelberg (2012)
12. Ogiela, L., Ogiela, M.R.: Towards Cognitive Cryptography. Journal of Internet Services and Information Security. 4(1), 58-63 (2014)
13. Ogiela, M.R., Ogiela, L., Ogiela, U.: Strategic Information Splitting Using Biometric Patterns. Journal of Internet Services and Information Security. 2(3/4), 129-133 (2012)
14. Ogiela, M.R., Ogiela, U.: Linguistic Extension for Secret Sharing (m, n)-threshold Schemes. SECTECH 2008 – International Conference on Security Technology, China, Dec 13-15, 2008, Proceedings, pp. 125-128 (2008)
15. Ogiela, M.R., Ogiela, U.: Security of Linguistic Threshold Schemes in Multimedia Systems, 2nd International Symposium on Intelligent Interactive Multimedia Systems and Services, Mogliano Veneto, Italy, Jul 16-17, 2009, New Directions in Intelligent Interactive Multimedia Systems and Services – 2, Studies in Computational Intelligence, vol. 226, 13-20 (2009)
16. Ogiela, M.R., Ogiela, U.: The use of mathematical linguistic methods in creating secret sharing threshold algorithms. Computers and Mathematics with Applications. 60(2), 267-271 (2010)
17. Ogiela, M.R., Ogiela, U.: DNA-like linguistic secret sharing for strategic information systems. International Journal of Information Management. 32, 175–181 (2012)
18. Ogiela, M.R., Ogiela, U.: Linguistic Protocols for Secure Information Management and Sharing. Computers and Mathematics with Applications. 63(2), 564-572 (2012)
19. Ogiela, M.R., Ogiela, U.: Secure Information Management using Linguistic Threshold Approach. Advanced Information and Knowledge Processing, Springer-Verlag, London (2014)
20. Peters, W.: Representing Humans in System Security Models: An Actor-Network Approach. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2(1), 75-92 (2011)