Towards Cognitive Cryptography

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

Abstract

This publication describes the new paradigm of cognitive cryptography. This new scientific area is marked by a new generation of information systems, focused on developing intelligent cryptographic protocols and procedures utilising cognitive information processing approaches. Such systems are mainly designed to use the semantic analysis of encrypted data to select the most appropriate method of its encryption. Our paper presents a possible application of such techniques in intelligent information sharing or visual cryptography. Additionally, some cryptographic solutions inspired by biological models are presented.

Keywords: cryptographic protocols, cognitive systems, bio-inspired cryptography

1 Introduction

Cognitive sciences have been developing for several decades and deal with such areas as neurobiology, psychology, linguistics, and recently technology as well [3]. New computational paradigms proposed in recent years as part of informatics have mainly consisted in the development of neural networks which imitate the operation of biological structures: the neuron and the central nervous system. They also included new techniques for the semantic interpretation of complex patterns in the form of images, scenes or huge volumes of data associated with economic development, smart information management as well as the supervision of multi-media transmissions [1] [4]. One can easily see that recently there has been more research in the areas of cognitive science and cognitive informatics. This is mainly due to major technological progress in contemporary computers and the attempt to use them to discover further secrets about the way the brain operates, understand the cognitive processes taking place in it, and use this knowledge to build modern technical solutions, e.g. cognitive humanoid robots [3]. An analysis of the progress in many areas of contemporary cognitive science and cognitive informatics also suggests that they may contribute to the development of contemporary cryptography or even create its new fields by combining techniques which guarantee data confidentiality and integrity with personal information, e.g. biometrics, or with semantic information extracted from analysed patterns (e.g. images or scenes). Such a combination of cryptography with cognitive informatics can give birth to a new branch of science, the so-called cognitive cryptography.

2 The Idea of Cognitive Cryptography

Traditional cryptography is the science of hiding information using symmetrical or asymmetrical techniques, or if executing various protocols which ensure the confidentiality and integrity of data as well as the authentication or the authorisation of the parties [2]. Practically every algorithm for the above tasks

Journal of Internet Services and Information Security (JISIS), volume: 4, number: 1, pp. 58-63
*Corresponding author: Tel: +48-126173854

makes use of a sequence of bits (keys) of a specific length which ensure the computational security of the algorithm or cryptographic procedure used. In the traditional approach based on Shannon's information theory, the best keys for data encryption are random keys (or one-time pads) which contain no superfluous information measured quantitatively by the redundancy. Such algorithms are very secure, but they do not allow the whole encryption process to be personalised and made dependent on individual information associated with a specific person. Such a need arises in the so-called personalised cryptography, i.e. when we want to e.g. generate encryption keys which are not purely random sequences of bits, but in which some personal information is encoded. Such keys not only allow data to be hidden, but in special cases could also enable identifying the owner of a specific key which has been used to perform the relevant task. Such characteristics may be very useful when:

- authenticating the parties,
- sharing secret information,
- or encrypting with Fuzzy Vault methods.

Obviously, we can imagine a situation in which we would like to use not just the biometric data of a specific person, but also completely different information extracted from some pattern, e.g. an image or Big Data, and used to make this pattern or selected data repositories secret. To do this, we need to have a system which will semantically analyse selected patterns (images, sounds, multimedia data etc.) and extract certain unique characteristics or information from them, which characteristics/information can then be used to perform the appropriate cryptographic procedure.
It is thus clear that the area of cognitive cryptography represents more than just personalised cryptography concerning crypto-biometric techniques and methods. It also enables the use of cognitive information systems to semantically analyse any data, thus producing a semantic description of the examined information, and then use this description to apply a specific cryptographic procedure aimed at encrypting this information, secretly sharing it or hiding it. The main differences between traditional cryptographic techniques and cognitive cryptography are presented in Figure 1.

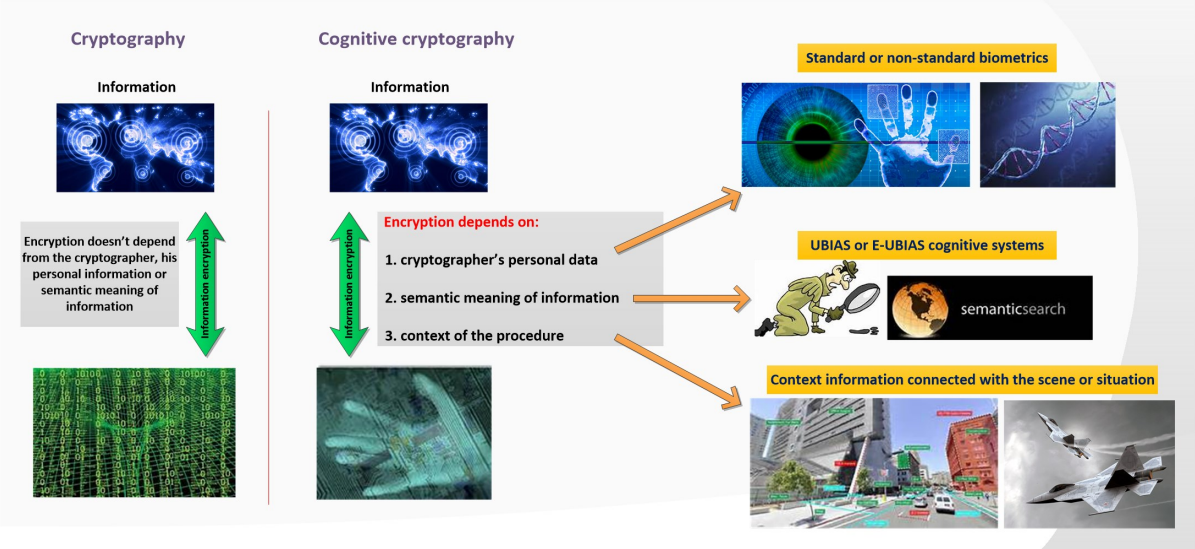

Figure 1: Differences between traditional and cognitive cryptography.

3 Application Areas of Cognitive Cryptography

In the light of the rapid development of cognitive information systems and the ability to use them for many diverse tasks of semantic data analysis, several leading areas and applications of cognitive cryptography can be defined.

The most important of them include:

1. Threshold algorithms for sharing secrets depending on the contents of the shared information;
2. Visual cryptography with a visual perception threshold set for a given person;
3. Image steganography, watermarks and schemes depending on image contents;
4. Other applications based on the use of biological models in cryptography.

The first of the listed applications concerns methods of information splitting or sharing with the use of cryptographic threshold schemes. Publication [5] [6] proves that it is possible to develop so-called biometric threshold schemes or schemes which allow certain additional information (in this case the meaning of the shared secret) to be used in the process of generating and distributing shares of secret data. Of course, depending on the type of information shared, it seems necessary to use certain types of cognitive information systems which will determine the meaning of the shared data which consists in text (UBMSS systems) or images (E-UBIAS systems) [3].
The second listed area of application is visual cryptography. It is known that this type of cryptography concerns mainly image data and makes it possible to hide or share the image by the threshold method or using special image masks, without requiring a lot of computing capacity. In this case, the opportunities to use cognitive cryptography could consist in individually setting visual perception thresholds which, if threshold schemes are applied, would allow the visual information to be reconstructed in various ways for different individuals. Such a scheme would thus allow creating secret image shares whose combination would enable recombining the image into a visible form in certain cases (for specific persons), but not in other cases.
The third area of application is image steganography and watermarks (particularly invisible ones) [7]. Many watermarking and steganography algorithms allow any information in a textual or image form to be inserted into the marked object. In cognitive cryptography, this inserted information may consist of personal data obtained from biometrics, but it could also be a type of security code reflecting the original contents of the marked data. Such a watermark would make it possible to detect geometric changes and modifications of the contents of marked images. Obviously, to extract data unambiguously identifying the marked image, this image must be analysed using E-UBIAS cognitive systems which can cognitively, semantically analyse the image.
The last of the above areas of cognitive cryptography application is associated with using various biologically-inspired models for cryptographic purposes. The most important examples of such solutions include DNA cryptography and also linguistic threshold schemes allowing a secret to be threshold-shared with the use of mathematical linguistic formalisms. More information on this subject is available in previous publications of the authors [5] [6].

4 Cognitive Cryptography in Preventing Insider Threats

Looking on the above mentioned areas of application of cognitive cryptography techniques, we can easily realize that such techniques may also play important role for preventing insider threats and information

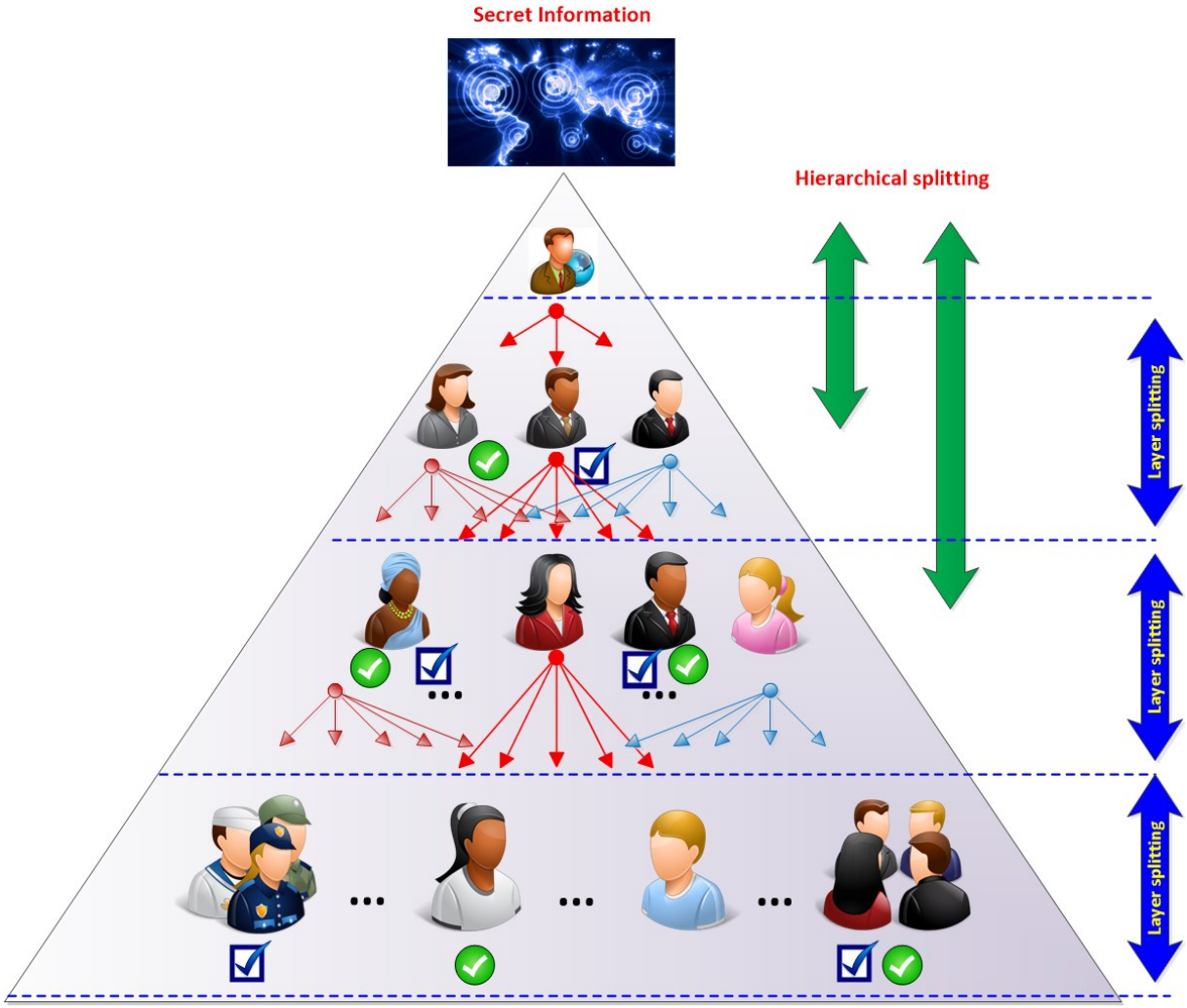

Figure 2: Different types of secure information splitting and distribution using linguistic threshold schemes.

leakage from the secured system. There are two main reasons, which make these methods very useful for such purposed.

The first one is connected with application of linguistic threshold schemes. As has been noted, such procedures may be used for hierarchical information sharing and performing intelligent management of splitted information, on different levels in hierarchical structures. Linguistic threshold schemes allow to share and distribute particular secret information in various manners for different participants groups, depending on theirs accessing grants for information retrieval. Different approaches for information splitting and distribution is presented in Figure 2. Depending on the types of information structure (layered or hierarchical) we can apply different models for secret information distribution. Application of such different models allow to prevent the information leakage while performing the whole distribution

protocol [6].
The second possible application of cognitive cryptography for preventing information leakage is connected with personalized cryptography, and application of biological models, or biometrics information for various security tasks. The most important example showing such possibilities is connected with generation of personalized cryptographic keys for symmetric or asymmetric encryption. For this purpose were proposed bio-inspired techniques which allow to encode some personal features or characteristics into long and enough strong encryption keys [5]. Such keys allow to identify who is the owner, and in case of secured information leakage also point out for the untrusted participants or communication unit.

5 Conclusion

This article presents new development directions of contemporary cryptography and a new area of research on cognitive cryptography. In the future, modern cryptographic systems may develop towards personalised cryptography, in which a significant role will be played by personal information allowing a specific person to be identified, but which also aims at creating encryption methods taking into account the meaning of the hidden or shared data and applying various encryption methods depending on this meaning. The development of such methods will allow abandoning traditional techniques which use a lot of computing power to guarantee data confidentiality and instead applying cognitive algorithms which guarantee the security of information depending on the context in which this information appears or on its meaning. The creation of cognitive cryptographic algorithms is becoming possible thanks to the development of many classes of intelligent cognitive systems described in publication [3] [6].

Acknowledgement. This work has been supported by the AGH University of Science and Technology research Grant No 11.11.120.329

References

[1] T. Hachaj and M. R. Ogiela. Nowadays and future computer application in medicine. *IT CoNvergence PRActice (INPRA)*, 1(1):13–27, 2013.

[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. Waterloo, CRC Press, 2001.

[3] L. Ogiela and M. R. Ogiela. *Advences in Cognitive Information Systems*. COSMOS 17, Springer-Verlag, Berlin-Heidelberg, 2012.

[4] M. R. Ogiela and T. Hachaj. Automatic segmentation of the carotid artery bifurcation region with a region-growing approach. *Journal of Electronic Imaging*, 22(3), 2013.

[5] M. R. Ogiela and U. Ogiela. Dna-like linguistic secret sharing for strategic information systems. *International Journal of Information Management*, 32:175–181, 2012.

[6] M. R. Ogiela and U. Ogiela. *Secure Information Management using Linguistic Threshold Approach*. Advanced Information and Knowledge Processing, Springer-Verlag, London, 2014.

[7] W. Wójtowicz and M. R. Ogiela. Security issues on digital watermarking algorithms. *Annales UMCS Informatica AI XII*, 4:123–139, 2012.

Author Biography

Lidia Ogiela 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 a few dozen of 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, CSS – Cognitive Science Society. Currently she is at the associate professor position, and works in Faculty of Management at the AGH University of Science and Technology.

Marek R. Ogiela works at the AGH University of Science and Technology in Krakow. In 1992 graduated from the Mathematics and Physics Department at the Jagiellonian University. In 1996 for his honours doctoral thesis on syntactic methods of analysis and image recognition he was awarded the title of Doctor of Control Engineering and Robotics at the Faculty of Electrical, Automatic Control, Computer Science and Electronic Engineering of the AGH University of Science and Technology. In 2001 he was awarded the title of Doctor Habilitated in Computer Science for his research on medical image automatic analysis and understanding. In 2005 he received a professor title in technical sciences. Member of numerous world scientific associations (IEEE-Senior Member, SPIE-Senior Member, SIIM etc.) as well as of the Forecast Committee 'Poland 2000 Plus' of the Polish Academy of Science and member of Interdisciplinary Scientific Committee of the Polish Academy of Arts and Sciences (Bio cybernetics and Biomedical Engineering Section in years 2003-2011). Author of more than 250 scientific international publications on pattern recognition and image understanding, artificial intelligence, IT systems and biocybernetics. Author of recognised monographs in the field of cryptography and IT techniques; author of an innovative approach to cognitive medical image analysis, and linguistic threshold schemes. For his achievements in these fields he was awarded many prestigious scientific honors, including Prof. Taklińskis award (twice) and the first winner of Prof. Engel's award.