International Journal of Information Management 40 (2018) 21–27

Contents lists available at ScienceDirect

International Journal of Information Management

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

Cognitive cryptography techniques for intelligent information management

Marek R. Ogiela*, Lidia Ogiela

AGH University of Science and Technology, Cryptography and Cognitive Informatics Research Group, Al. Mickiewicza 30, 30-059, Krakow, Poland

ARTICLE INFO

Keywords:
Intelligent information management
Cognitive cryptography
Semantic and personal information
Data sharing

ABSTRACT

This paper discusses the foundations of cognitive cryptography used to secure information by splitting it and distributing the split parts among selected groups of secret trustees. The process of concealing data by its splitting and distributing secret parts (shadows) with the use of cognitive techniques will be discussed. Cognitive cryptography describes the possibilities of using personal information contained in individual biometric traits. At the same time, it will be presented as an innovative solution allowing the holder of a secret shadow to be identified based on their characteristic biometrics and their semantic features. Cognitive cryptography is used to manage strategic information. By using techniques for splitting and sharing this type of data as well as utilising individual biometric traits in the entire process of distributing all shadows of the concealed and split information makes the proposed cognitive cryptography techniques an innovative, extremely useful tool for securing data of major importance.

1. Introduction

Cryptographic techniques are used to secure information and restrict access to it. Securing the information is mainly aimed at protecting it from theft. This theft is understood as the ability of unauthorised individuals (systems) to access information and use it (Menezes, van Oorschot, & Vanstone, 2001; Ogiela, 2016; Schneier, 1996). Every piece of information is thus subject to protection whose level depends on the important message (data) contained in this information. It is, however, worth noting that in the case of information which is in public domain, this information is not subject to any special security, but if it has to be protected, cryptographic protocols can be used for this purpose. In the case of data that is confidential, secret or strategic, it is necessary to use data protection algorithms to verify the individuals having access to this data. Cryptographic algorithms are among those that are to ensure the appropriate security and protection of information (Beimel et al. 2016; Ogiela, 2015b; Ogiela & Ogiela, 2008, 2011, 2014; Tang, 2004). They are considered secure if their use ensures the complete protection of data. Data security is a necessary element in the operation of various information exchange processes. These processes can include, for instance, the exchange of information between:

- parties to or participants of a process – the exchange of information between various individuals who participate in the data/information exchange process,
- sites where process participants are located – the exchange of information between different places in which parties to the process are situated, such as company branches, representative offices, remote sites,
- process participants, but at different points in time – creating copies of information which will be reproduced after a certain period of time has expired.

In all the above situations, the complexity of the process of exchanging information between parties to the protocol should be accounted for as well (Shamir, 1979; TalebiFard & Leung, 2011). This is because there are single, simple information exchange protocols, and protocols dedicated to complex ranges of users, such as information splitting and sharing. These kinds of solutions are designed for securing data by splitting it and distributing parts of this split information (the so-called shadows) among a selected group of secrets trustees. This information is not stored by one protocol participant whose action would depend only on their own decisions, but is distributed among a specific group of participants (individuals, computers), who should act rationally as a group. This means that if a decision needs to be taken, a group of secret trustees must work in concert, and in addition:

- intent to disclose the secret in a situation in which its contents need to be disclosed,
- guard the secret if its security is threatened.

Any action aimed at operating contrary to the other participants may cause:

* Corresponding author.
E-mail addresses: mogiela@agh.edu.pl (M.R. Ogiela), logiela@agh.edu.pl (L. Ogiela).

https://doi.org/10.1016/j.ijinfomgt.2018.01.011
Received 12 December 2017; Accepted 24 January 2018

- disclosing secret information in a situation in which it should not have been,
- no access to the information when its disclosure has a priority, overriding nature.

In every instance, the assessment of the situation and the need to take appropriate decisions rests with the protocol participants (holders of parts of the split secret) who should ensure the complete protection of information against its unauthorised disclosure and seizure. Consequently, the choice of the appropriate data security protocol represents the main step in securing data from its unauthorised disclosure. Cryptographic protocols used for data security are divided into two classes (Beimel, Farras, & Mintz, 2016; Ogiela, 2015a, 2015b; Ogiela & Ogiela, 2008, 2011, 2014, 2016b):

- Data splitting protocols – this class includes cryptographic protocols allowing the secret information to be split between a group of n participants, of whom every participant receives one part of the secret (shadow). Each separate shadow is useless on its own, because it contains no complete information. To reconstruct the split secret, all parts of the secret have to be combined. Hence, to retrieve the secret information, all protocol participants must be in full agreement.
- Data sharing protocols – this group includes cryptographic protocols which allow the secret to be split between a group of n participants, and to retrieve the secret m ($m < n$) parts of all n must be combined. Just as in the case of data splitting protocols, each shadow does not contain any complete information, but once the required number of shadows is combined, the complete content of the secret can be retrieved. In this case, to retrieve the concealed information, it is necessary for a specific group of secret trustees $-$ m of n participants – to agree.

Cryptographic techniques aimed at securing information by splitting it have been described, among others, in publications (Beimel et al., 2016; Ogiela, 2015a, 2015b; Ogiela & Ogiela, 2008, 2011, 2014, 2016b; Schneier, 1996; Shamir, 1979; Tang, 2004)), which present the characteristic features and the method of selecting optimal solutions and cryptographic techniques dedicated to secret information sharing. The method of concealing information by splitting it and distributing individual parts of the secret (shadows) to protocol participants allows the data to be protected by restricting access to it. This is because no protocol participant owns all parts of the split secret, and therefore they cannot take an individual decision to disclose or refuse to disclose the information.

However, these types of solutions also have drawbacks, such as the ability to generate empty shadows and assign them to protocol participants without their knowledge of the contents of the shadows they receive. In the case of data sharing protocols, a kind of collusion between a selected group of secret trustees is also possible, resulting in them deciding about the fate of the data that they have been entrusted with without the knowledge and agreement of the remaining participants.

In order to eliminate this type of threat, it is necessary to introduce the ability to randomly select protocol participants who can reconstruct the secret information. Then, no participants will know whether, in the given protocol, they are appointed as a trustee deciding about the fate of the data or not.

An innovative solution eliminating the above threats is offered by cognitive cryptography, which is the main subject of this publication.

2. Cognitive cryptography

Cognitive cryptography is to improve personal identification processes using personal information (Haynes, Bawden, & Robinson, 2016; Ogiela, 2010, 2014; Ogiela & Ogiela, 2016a) characteristic for each protocol participant. This personal information is contained in individual biometrics sets describing the biometric features of each protocol participant (Ogiela, 2016a, 2016b;). Because of the nature of biometrics, they constitute individual, unique information that unambiguously characterises their owner. Because of this individual and unique nature of biometric features, it is a very significant both from the scientific and the practical perspective to use biometrics for the personal identification and verification. The ability to combine solutions that secure information with an unambiguous way of verifying its owner by identifying their characteristic biometrics has allowed the authors of this publication to develop an innovative solution called cognitive cryptography.

Cognitive cryptography is thus a novel approach to securing data using the individual personal features of each protocol participant.

Definition 1. Cognitive cryptography is a division of cryptography within which any information set can be secured using personal information contained in the biometric sets of information and semantic information unambiguously identifying individual features of protocol participants.

Personal information contained in individual biometrics is used during personal identification to correctly assign biometric traits to the right person, and then, during personal verification it is used to assess whether the biometric traits characterise the right person or whether

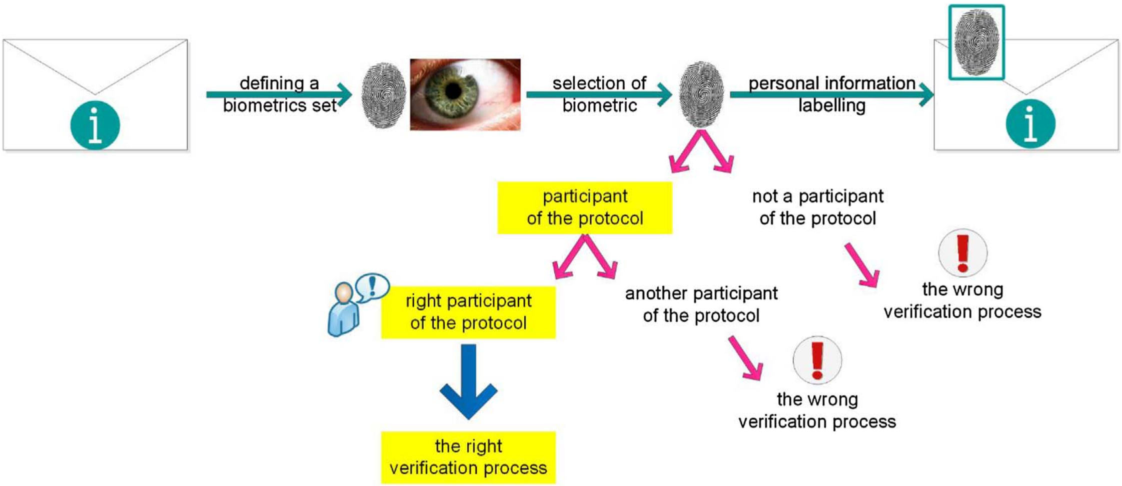

Fig. 1. The scheme of personal veryfication.