Security of Selected Secret Sharing Schemes

Urszula Ogiela[1], Makoto Takizawa[2], and Lidia Ogiela[1](✉)

[1] Cryptography and Cognitive Informatics Research Group,
AGH University of Science and Technology, 30 Mickiewicza Ave., 30-059 Krakow, Poland
{ogiela,logiela}@agh.edu.pl

[2] Department of Advanced Sciences, Hosei University,
3-7-2, Kajino-Cho, Koganei-Shi, Tokyo 184-8584, Japan
makoto.takizawa@computer.org

Abstract. In the paper will be described a few most important aspects connected with innovative secret sharing procedures, and also an idea of linguistic cryptography in processes of data encryption. The most important aspects are using parts of divided data to finally reconstruction them. Linguistic algorithms dedicated to securing data as well as secret sharing techniques, are also very useful to guarantee data security. Secret sharing algorithms allow to distribute information within a separate group of secret trustees. In this paper authors describe techniques of using that methods for linguistic data sharing techniques. Authors propose also captcha analysis for linguistic threshold schemes. All secret parts of data can be written by used any parts of selected captcha.

Keywords: Secret sharing · Threshold algorithms · Linguistic techniques · Data security

1 Introduction

Many kinds of cryptographic techniques dedicated to securing data create secret parts, which may be distributed between different numbers of secret trustees. One of those algorithms is data division techniques dedicated to data splitting processes. In group of information splitting techniques we can find many others solutions as well as data splitting algorithms and data sharing techniques [1–3]. In this group was proposed new techniques dedicated to information security and used linguistic methods [4–7]. Linguistic techniques are very useful for supporting the semantic meaning analysis [8–10] of data security aspects [11–13].

The main idea of securing data by using linguistic algorithms, proposed used semantic methods of describe information for divided data [6, 14].

In this paper, the authors propose the main idea of application linguistic techniques for information/data sharing procedure by used captcha secrets.

The essence of linguistic cryptographic algorithms consists in generating an additional part of divided secret, as shadow which including linguistic information – names "linguistic shadow". In that shadow are include only linguistic information [8]. In

L. Barolli and T. Enokido (eds.), *Innovative Mobile and Internet Services in Ubiquitous Computing*, Advances in Intelligent Systems and Computing 612,
DOI 10.1007/978-3-319-61542-4_37

linguistic shadow there were all data/information about semantic contents of analyzed data.

2 Linguistic Shadows in Secret Sharing Schemes

Linguistic shadows dedicated to secret sharing procedures can be distributed in different ways. The first one is selected participants of secret trustees, and the second is a groups of participants of secret trustees.

The meaning aspects of data, means impact of analyzed and interpreted data for other information. Process of extraction the meaning aspects of sharing data is very important for secure processes. For this kinds of analysis is possible used linguistic shadows, which are used for division processes. The threshold schemes which include linguistic shadow names linguistic threshold schemes [1, 6]. In this group of secret sharing techniques, were proposed different class of data splitting [14]:

- linguistic threshold schemes without splitting linguistic shadow,
- linguistic threshold schemes with included linguistic information splitting.

Linguistic threshold schemes without linguistic information splitting means that semantic information is included in one part of secret. Linguistic shadow is contain to one secret holder. To reconstruct original information is necessary combining selected group of secret parts included also linguistic shadow.

The second example of linguistic threshold schemes included with linguistic information splitting procedure, means that linguistic is divided into a group of secret holder. To reconstruct original data, is necessary combining selected group of secret included linguistic shadow, which can restore by group of linguistic shadow holders.

Linguistic methods create an additional kinds of cryptographic techniques for sharing procedures.

3 Captcha Idea

Idea of captcha verification processes create confirmation the access by mark selected options (images, letters, etc.) at captcha images. This solution confirm that the action are made by human (not by machine). Captchas are used in verification processes, when is possibility to change human by robots. In this process we can verify that operation which is necessary, was done by human. So, it's possible to do simple operations, like mark designated object, letters, images, etc.

Figure 1 presents two different images with many different objects, but for captcha analysis is necessary select and mark only designated object (in this example – fruits). The first captcha picture presents one image selected for nine parts with apricot-tree. Human who analyzed this picture should mark only those parts which presents fruits (in this example – apricots). The second picture presents different objects, trees, fruits, flowers, waterfalls, clouds, sky, and sun. In this picture it's also necessary mark only those images which presents fruits. We see different ways, but the same kinds of analysis by semantic interpretation of analyzed objects.

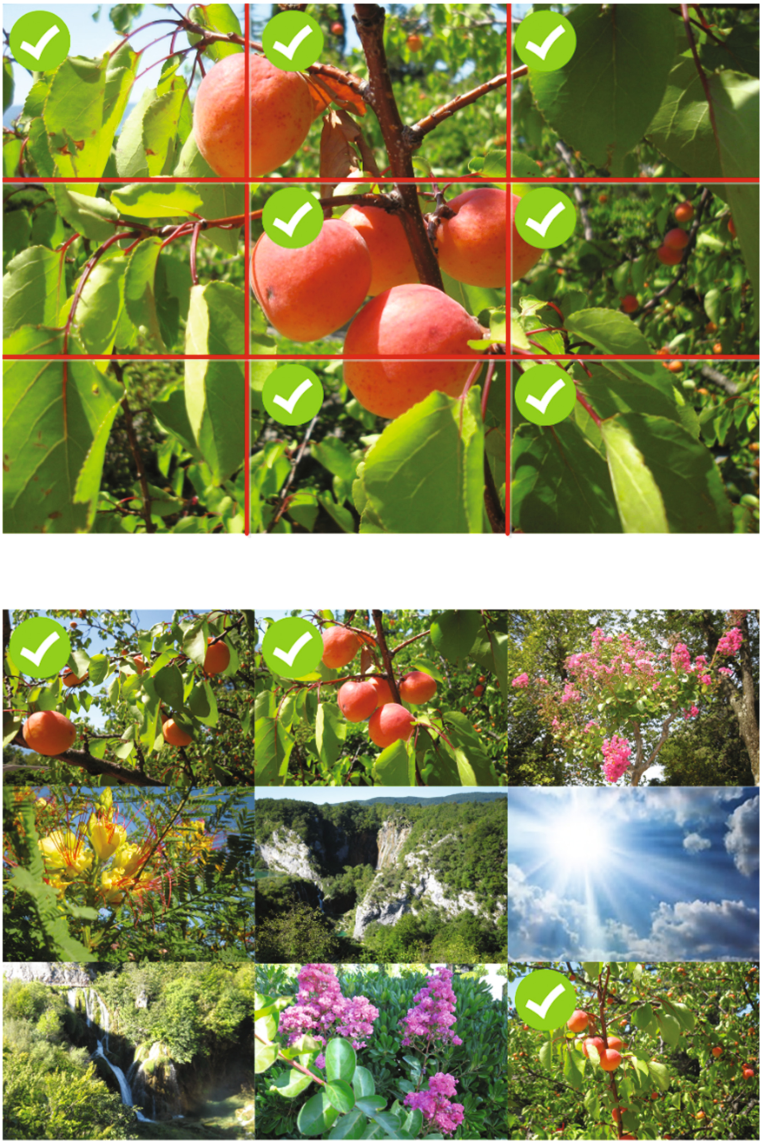

Fig. 1. Examples of captcha pictures. Top: in one image. Bottom: picture with different objects, with mark only those which present fruits.

The main step of captcha analysis is understanding the pictures and meaning of them. At this example is necessary mark the “object” which presents fruits. At the first picture is necessary mark this parts of images, in which we see correct image. At the second picture is necessary to select those pictures, at which we see fruits images. In this processes the main role play the semantic meaning of describe and analyse images/pictures/objects.

This type of meaning interpretation can be used by linguistic threshold schemes to verify participants which have parts of linguistic data.

4 Captcha Analysis for Linguistic Cryptography

In the case of cryptographic linguistic threshold schemes the required number of shadows should be combined to reconstruction the divided data. Also is possible to analyse the contents of the data. The meaning of analyse information, can select the most important data – for example strategic data. In linguistic threshold algorithms we create number of shadows divided for all secret trustees. The number of them depends of defined threshold schemes. The number of parts of divided secret, which is necessary to reconstruct the original data is defined in the data sharing algorithm. The reconstruction processes in linguistic threshold schemes consist [6, 13]:

- classical (m, n)-threshold schemes,
- combining the required number of secret parts which includes the shadow containing linguistic data,
- combining the required number of secret parts which includes only a part of linguistic shadow,
- captcha analysis processes.

Captcha analysis processes in linguistic threshold schemes consist the following stages:

- reconstruction linguistic shadow at the stage of combining the required parts of linguistic part of secret,
- reconstruction secret data at the stage of combining the required parts of all secret parts.

Figure 2 presents the example of process of reconstruction data included the linguistic shadow. That process is realize after captcha verification stage. At the stage of combining the required parts of secret, can restore original data with semantic information (meaning data).

Figure 2 presents the captcha analysis technique in linguistic threshold algorithms. The captcha analysis presents two way. One of them is correct mark captcha used to secret reproduce procedure. The second one is false mark captcha. In this stage is not possible to reproduce original information. In secret reconstruction procedure is after collecting number of necessary secret parts is also add the linguistic shadow. So, the restore secret include linguistic information.

Security of linguistic threshold schemes is guaranteed by used strong cryptographic algorithms. Those classes of secure algorithms are very useful for data security.

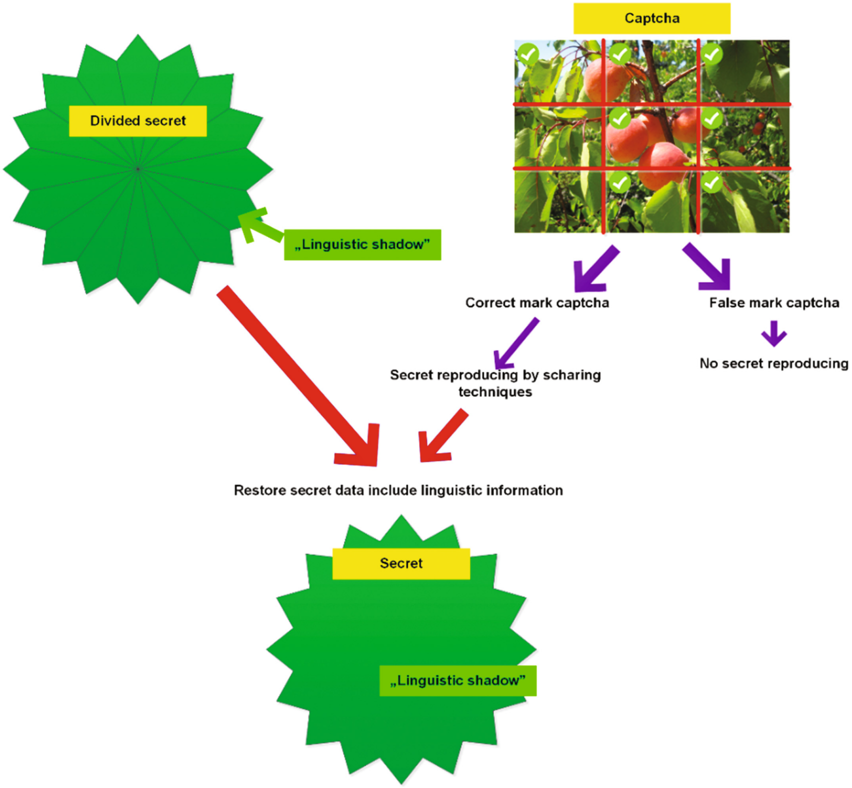

Fig. 2. Linguistic threshold scheme with linguistic shadow including captcha analysis stage.

5 Conclusions

Linguistic algorithms applied for information sharing schemes create a new way of data security. Algorithms including meaning aspects of data division as additional way of secret splitting and sharing methods. Meaning aspects and semantic details included in information security procedures allow to verify all kinds of data and eliminate not significant of them. In this paper was proposed captcha analysis for linguistic threshold schemes. This process was proposed especially for verification person and select robots users. The captcha analysis processes included linguistic algorithms were proposed for data sharing processes. The main idea of proposed solution is to generate an additional shadow containing linguistic information. This shadow with other parts of the shared secret, is split between all shadow holders.

Acknowledgments. This work was partially supported by JSPS KAKENHI grant number 15H0295.

References

1. Ogiela, M.R., Ogiela, U.: Security of linguistic threshold schemes in multimedia systems. Stud. Comput. Intel. **226**, 13–20 (2009)
2. Ogiela, M.R., Ogiela, U.: Grammar encoding in DNA-like secret sharing infrastructure. In: Kim, T., Adeli, H. (eds.) ACN/AST/ISA/UCMA -2010. LNCS, vol. 6059, pp. 175–182. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13577-4_15
3. Yan, S.Y.: Computational Number Theory and Modern Cryptography. Wiley, Hoboken (2013)
4. Ogiela, L.: Computational intelligence in cognitive healthcare information systems. Stud. Comput. Intel. **309**, 347–369 (2010)
5. Ogiela, L., Ogiela, M.R.: Beginnings of cognitive science, in advances in cognitive information systems. Cogn. Syst. Monogr. **17**, 1–18 (2012)
6. Ogiela, M.R., Ogiela, U.: Linguistic approach to cryptographic data sharing. In: The 2nd International Conference on Future Generation Communication and Networking, FGCN 2008, Hainan Island, China, 13–15 December 2008, vol. 1, pp. 377–380 (2008)
7. Ohkawara, T., Aikebaier, A., Enokido, T., Takizawa, M.: Quorum-based synchronization protocols for multimedia replicas. Int. J. Cluster Comput. **16**(4), 979–988 (2013)
8. Ogiela, L.: Cognitive informatics in image semantics description, identification and automatic pattern understanding. Neurocomputing **122**, 58–69 (2013)
9. Ogiela, L., Ogiela, M.R.: Data mining and semantic inference in cognitive systems. In: Xhafa, F., Barolli, L., Palmieri, F., et al. (eds.) 2014 International Conference on Intelligent Networking and Collaborative Systems (IEEE INCoS 2014), Salerno, Italy, 10–12 September 2014, pp. 257–261 (2014)
10. Ogiela, L., Ogiela, M.R.: Management information systems. In: Park, J., Pan, Y., Chao, H.-C., Yi, G. (eds.) Ubiquitous Computing Application and Wireless Sensor. LNEE, vol. 331, pp. 449–456. Springer, Dordrecht (2015). doi:10.1007/978-94-017-9618-7_44
11. Duolikun, D., Aikebaier, A., Enokido, T., Takizawa, M.: Design and evaluation of a quorum-based synchronization protocol of multimedia replicas. Int. J. Ad Hoc Ubiquitous Comput. **17**(2/3), 100–109 (2014)
12. Gregg, M., Schneier, B.: Security Practitioner and Cryptography Handbook and Study Guide Set. Wiley, Hoboken (2014)
13. Ogiela, M.R., Ogiela, U.: Secure information management using linguistic threshold approach. In: Advanced Information and Knowledge Processing. Springer, London (2014)
14. Ogiela, M.R., Ogiela, U.: Shadow generation protocol in linguistic threshold schemes. In: Communication in Computer and Information Science, vol. 58, pp. 35–42 (2009)