Personalized Protocols for Data Hiding in Cloud-to-Things Applications

Marek R. Ogiela
AGH University of Krakow
30 Mickiewicza Ave, 30-059 Kraków, Poland
e-mail: mogiela@agh.edu.pl

Urszula Ogiela
AGH University of Krakow
30 Mickiewicza Ave, 30-059 Kraków, Poland
e-mail: ogiela@agh.edu.pl

***Abstract*— In this article, we will introduce the idea of creating personalized security protocols for hiding and distributing secret information. In particular, a new paradigm combining Cloud Computing with IoT will be considered as an application area for the proposed hiding technologies. Such protocols will take advantage of selected user characteristics in protocols dedicated to secret data transmission.**

Keywords-Cloud-to-Things protocols; data hiding; personalized security protocols.

I. INTRODUCTION

Information hiding algorithms play a huge role in modern computer systems and IT security. Such methods are categorized as steganography, which deals with a variety of techniques for hiding data or creating invisible communication channels. Among the most popular methods are techniques for transmitting secret data placed in image container [1]. The way the information is hidden in the container is the key, which must also be used to reconstruct the data from the media [2].

This paper will describe the idea of using personal data to create a key that allows to distribute secret information in the selected visual container. Since cryptographic keys usually have a fixed length, the proposed method will also use hash functions to encode the personal characteristics of a particular user in the form of hash sequence with particular length.

The rest of the paper is structured as follows. In Section II, we introduce the hash-based personalized hiding protocols. In Section III applications of hiding protocols will be described. Finally, we conclude the work in Section IV.

II. HASH-BASED PERSONALIZED DATA HIDING PROTOCOLS

Information hiding techniques, which exploit users' personal characteristics can use various unique personal biometric or behavioral traits. Popular biometric can be acquired using sensors, or motion capture devices that allow analysis of selected gestures or movements [3]. The resource of individual features acquired in this way makes it possible to select some of them and apply them to an appropriate algorithm for hiding the secret. Selected personal features regardless of their characteristics can be encoded using hash functions. Such an operation allows one to generate a hash of a certain length depending on the selected hash function. Since the resulting hash will be used as a key to place the secret data in the information carrier, it makes sense for it to be as long as possible, which can be achieved by choosing hash functions that generate hashes about 512 bits long.

After generating a personal key for hiding the data in the information carrier, one can proceed to encode the secret so that it is invisible in the container. The key sequence can be used here in various ways. The first is that the key bits can be interpreted as offsets indicating the next pixels of the data where we place the secret information. These offsets can be determined taking into account individual bit values, i.e., 0, 1, or bit blocks containing a larger number of bits and determining larger offset values when determining the next points (pixels) of the carrier to place the secret information in Figure 1.

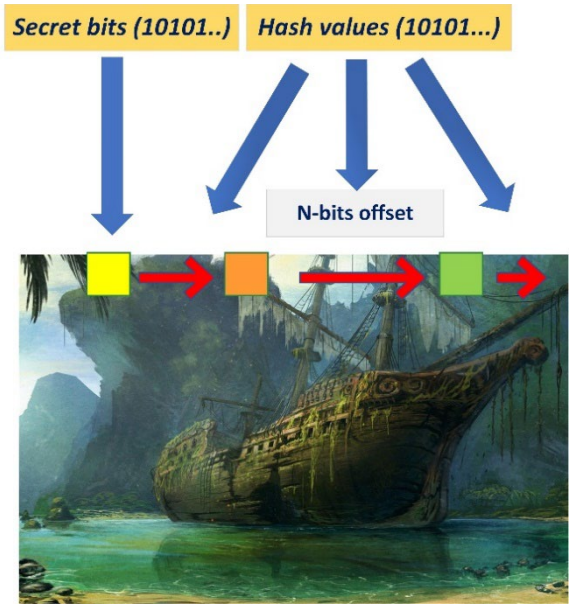

Figure 1. Secret hiding procedure based on offset values.

The second way to use the key can be to use successive bit values to determine the color components of successive image points where part of the secret is to be placed [4]. Thus, in this method, all the points of the container are considered consecutively, and only the bits of the key decide in which color component we place the secret bit of information. The idea of this method is illustrated in Figure 2.

 ISBN: 978-1-68558-036-0

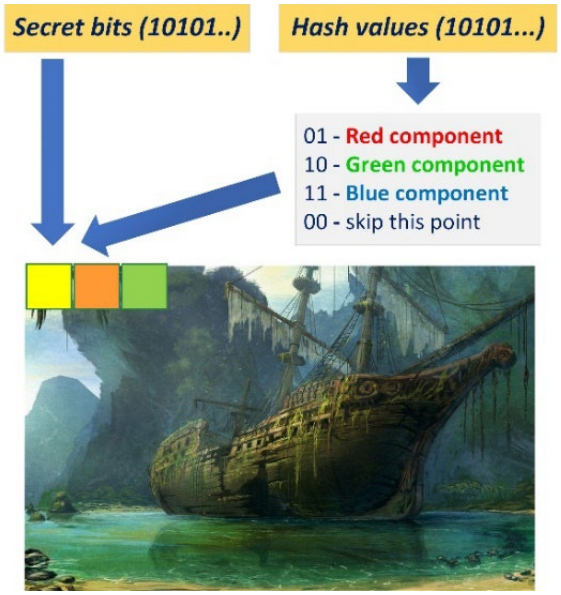

Figure 2. Secret hiding procedure based on color components.

This method can also be modified and place secret information in the color components of consecutive points determined in an irregular way, i.e., not a raster bitmap. Here, it is possible to use a column order of viewing the image and placing the secret instead of a row order, or to use special bit masks of specific sizes (e.g. 3x3, 5x5), which will indicate the neighboring points for the currently considered point, and just in them will allow placing the next bits of secret data.

III. Hiding Protocols in Cloud-to-Things Applications

Methods for hiding secret information in visual containers have a number of practical applications. Among them are guaranteeing copyrights in digital works, transferring strategic information or splitting secrets to create multiple keys.

Such applications are of great importance in Cloud-to-Things computing technologies, where there is a need to use particularly important information processed in the computer cloud in the task of guaranteeing confidentiality in the IoT area [5]. IoT-related protocols and services require the use of personalized cryptographic keys, which can be generated and transmitted using the described secrecy hiding protocols [6]. Personal keys, obtained using hash functions, can also be used for user authentication tasks when accessing remote services and data in distributed systems [7].

The presented protocol for generating personal keys in the form of a hashed string is very versatile and can be used wherever the collected information resources are processed using cloud computing resources, and then transmitted and used in Internet of Things devices.

The main advantage of the described approach is the ability to create personalized cryptographic solutions that are oriented to a specific system user, and at the same time allow only authorized users for whom personalized keys have been generated to run procedures for data transmission, device control, resource access or data analysis.

IV. Conclusions

This paper describes methods of using individual user characteristics and personal features in the creation of personalized cryptographic protocols. In particular, a method for creating personal keys using hash functions has been presented. Such keys are in the form of a hashed bit sequences of a certain length, which was created from encoding selected personal characteristics using a hash function. The resulting keys can then be used in authentication protocols or hiding data procedures. They can also be used in cloud-based services and applications that are dedicated to performing tasks and communicating with devices in IoT.

The techniques presented develop methods categorized as cognitive and personalized cryptography. Future work will attempt to extend them toward creating multiple personalized keys that can be used interchangeably by a single user. Such a solution would provide opportunities for a selected user to simultaneously implement multiple protocols using his personal characteristics. Such protocols would be quite independent and would be implemented using different personal characteristics and the keys produced for them by means of hash functions.

Acknowledgment

This work has been partially supported by the funds of the Polish Ministry of Education and Science assigned to AGH University of Krakow. The research project was supported by the program „Excellence initiative – research university” for the AGH University of Krakow.

References

[1] L. Ogiela, “Transformative computing in advanced data analysis processes in the cloud,” Inf. Process. Manage. Vol. 57(5), paper 102260, 2020.

[2] S. Zapechnikov, “Privacy-Preserving Machine Learning as a Tool for Secure Personalized Information Services,” Procedia Computer Science, Vol. 169, 2020, pp. 393-399, doi: 10.1016/j.procs.2020.02.235.

[3] M. R. Ogiela, L. Ogiela, and U. Ogiela, “Biometric methods for advanced strategic data sharing protocols,”. In: 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing IMIS 2015, pp. 179–183, 2015, doi: 10.1109/IMIS.2015.29.

[4] M. R. Ogiela and U. Ogiela, “Secure information splitting using grammar schemes,” Studies in Computational Intelligence, Vol. 244, pp. 327–336. Springer, 2009, doi: 10.1007/978-3-642-03958-4_28.

[5] C. Guan, J. Mou, and Z. Jiang, “Artificial intelligence innovation in education: a twenty-year data-driven historical analysis,” Int. J. Innov. Stud. 4(4), pp. 134–147, 2020.

[6] N. Ferguson and B. Schneier, “Practical Cryptography,” Wiley, 2003.

[7] S. J. H. Yang, H. Ogata, T. Matsui, and N.-S. Chen, “Human-centered artificial intelligence in education: seeing the invisible through the visible,” Comput. Educ.: Artif. Intell. Vol. 2, paper 100008, 2021.

 ISBN: 978-1-68558-036-0