Security of Linguistic Threshold Schemes in Multimedia Systems

Marek R. Ogiela and Urszula Ogiela

Abstract This publication will present a new approach how to extend well-known algorithms of secret sharing, towards another stage of information encoding with the use of the grammar formalism. Such an algorithm would be based on the appropriate sequential LALR grammars allowing shared bit sequences, and more generally blocks of several bits, to be changed into new representations, namely sequences of production numbers of the introduced grammar. This stage can be executed by a trusted third party or arbiter generating shadows of the secret. Such methods would form an additional stage improving the security of shared data.

1 Introduction

Advanced information management systems use various techniques and methods to manage data, search for it semantically, classify it as secret, make meaning tables etc. They are designed to facilitate the access to and improve the effectiveness of finding important information with specific meaning. Cryptographic algorithms for threshold secret splitting and sharing are among such techniques. They can be used to split important information and to assign its components to people from an authorised group. Such authorised, selective access to information is used when it is necessary to safely manage strategic data. This information may be military, but also economic data or multimedia files. This last type of data is gaining increasing importance due to the fast development various multimedia platforms or modalities. Sometimes such data is classified and inaccessible to ordinary people. Within the structure of the specific organisation there are individuals at the appropriate management levels who have access rights to the data addressed to them. Such rights are exercised in hierarchic structures, usually connected with the office held. In practice,

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

E. Damiani et al. (Eds.): New Direct. in Intel. Interactive Multimedia Sys., SCI 226, pp. 13–20.
springerlink.com

this means that higher-placed individuals have access to more confidential data, and people at lower levels to less information. Consequently, the flow of information within such structures may require implementing hierarchical threshold schemes for secret and data splitting, which schemes assign the appropriate level of rights to individuals who want to receive authorised access to secret data at particular levels. Obviously, when talking of information management, we refer to data stored on digital media or in computer databases. For such data, there is a need to intelligently split it between the authorised individuals and then to reconstruct it in secret. Therefore, it is worth turning our attention to the other significant question related to intelligent information management. It is the question of the capacity to ensure secrecy and selective access to such data for the authorised persons. Such a potential of managing strategic information may be acquired thanks to the use of certain mathematical techniques, originating from the fields of cryptography and steganography. In our case, the task comes down to searching for the formulas that allow intelligent sharing of information in a way that would allow its reconstruction to appropriately authorised people. The only condition here is the possibility of splitting the data and later their reconstruction by a group of appropriately authorised people. In this work we make an attempt to enrich known algorithms for secret sharing, with an additional stage of splitting the linguistic representation, defining the split data in the binary form. To achieve this, a sequential grammar of LALR type is introduced to allow converting a sequence of bits into its linguistic representation. This representation will then be subject to sharing with the use of one of the known threshold schemes.

2 An Idea of Secret Sharing

Secret sharing and splitting algorithms are quite young branch of information technology and cryptography. In the most general case, their objective is to generate such parts for the data in question that could be shared by multiple authorised persons. What arises here is the problem of splitting information in a manner allowing its reconstruction by a certain n-person group interested in the reconstruction of the split information. Algorithm solutions developed to achieve this objective should at the same time make sure that none of the groups of participants in such a protocol, whose number is lesser than the required m persons, could read the split message. The algorithms for dividing information make it possible to split it into chunks known as shadows that are later distributed among the participants of the protocol so that the shares of certain subsets of users, when combined together, are capable of reconstructing the original information. There are two groups of algorithms for dividing information, namely, *secret splitting* and *secret sharing*. In the first technique, information is distributed among the participants of the protocol, and all the participants are required to put together their parts to have it reconstructed. A more universal method of splitting information is the latter method, i.e. *secret sharing*. In this case, the message is also distributed among the participants of the protocol, yet

to have it reconstructed it is enough to have a certain number of constituent shares defined while building the scheme. Such algorithms are also known as threshold schemes, and were proposed independently by A. Shamir [13] and G. Blakley [5] [6], and were thoroughly analysed by G. Simmons [14]. The next section describes a method of extending classical threshold schemes for secret sharing to include an additional linguistic stage at which binary representations of the shared secret are coded into new sequences representing the rules of a formal grammar introduced. Such stage will introduce additional security against the unauthorised reconstruction of the information and can be executed in two independent versions of protocols for assigning created shadows to protocol participants. The first one is the version involving a trusted arbiter to mediate in the assignment and reconstruction of information. The second is the version without the arbiter, but with the assignment of the introduced grammar as a new, additional part of the secret.

3 Protocol for Linguistic Threshold Schemes

Executing the secret sharing protocol with the use of sequential grammars will lead to generating one additional shadow for the shared information. As already mentioned above, depending on the function of this information element, you can execute an arbitration protocol with a trusted arbiter holding the linguistic component necessary to reconstruct the secret, or a simple protocol without an arbiter. However, in the second case, the person holding the linguistic information (the grammar rule set) will be privileged, as his/her information will always be necessary to reconstruct the original secret. This situation will depend on the scheme executed and will be independent of the selected threshold secret sharing algorithm. This version can be beneficial when executing hierarchical threshold schemes, i.e. schemes with privileged shares. However, if it is necessary to create a fair, equal threshold scheme, the generation rule set of the grammar can be made public and then all shadows will have exactly equal rights. Further, this work proposes an algorithm for expanding the operation of such schemes and generation of a single additional shadow in the form of linguistic information necessary for the reconstruction of the entirely secret. Main steps of using the grammatical approach to the expansion of threshold systems are presented in Fig. 1.

4 Grammar for Coding Bit Positions

Expansion of the threshold scheme by an additional stage of converting the secret recorded in the form of a bit sequence is performed thanks to the application of context-free grammar in the following formula:

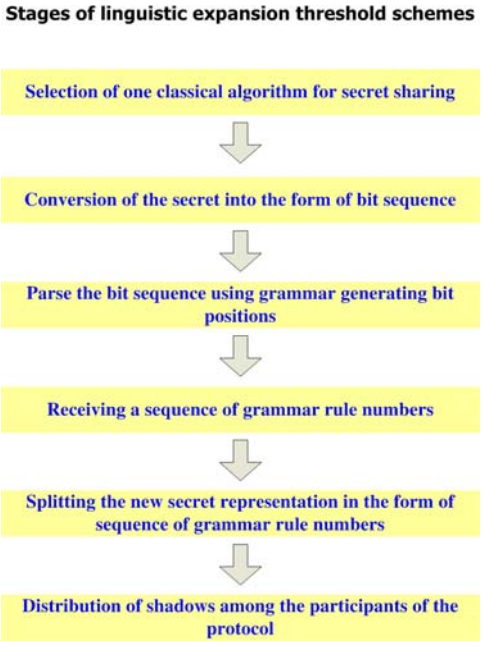

Fig. 1: Methodology of linguistic expansion threshold schemes.

$$G_{SECRET} = (N, T, P, STS), \tag{1}$$

where:

$N-$ non-terminal symbols, $T-$ terminal symbols, $\varepsilon-$ an empty symbol, $STS-$ grammar start symbol, $P-$ is a production set. Depending on the production set such grammar can change the bit sequences in the form of zeros and ones into a sequence of grammar production numbers that allow the generation of the original bit sequence.

The conversion of representation is ensured through syntax analyser that changes the bit sequence into numbers of linguistic rules of the grammar in square time. The graphic representation of using the grammar expansion in classical threshold schemes is presented in Fig. 2.

After performing such a transformation, any scheme of secret sharing can be applied to distribute the constituents among any number of n participants of the protocol. This means that at this stage, any classical (m, n)-threshold algorithm for secret sharing can be run. However, the secret being split is not a pure bit sequence, but a sequence composed of numbers of syntactic rules of the introduced grammar. Depending on its structure and type, it can contain values of two or more bits. So you can imagine a situation in which the grammar conversion will not consist in transforming single bits but also transforming pairs or greater numbers of bits at the same time (i.e. values of two, three, four and more bits will be considered). In that case,

the structure of the grammar will be similar, but the sequence of generation rule numbers obtained will have a greater range of values (i.e. the number of generation rules of the grammar defined for the conversion will increase).

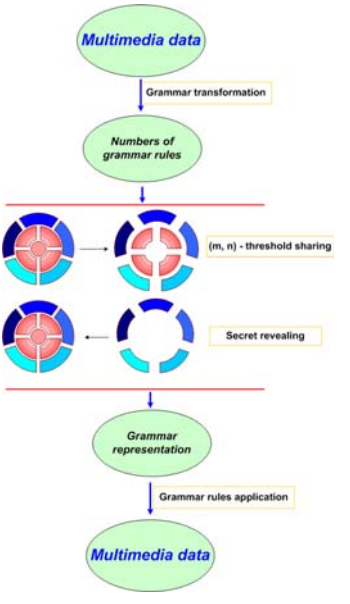

Fig. 2: Shadow generation scheme in the expanded threshold algorithm. The expansion concerns the use of grammar at the stage of converting the bit representation into sequences of numbers of linguistic rules in grammar.

To illustrate the idea of such linguistic coding, an example of a grammar that converts 3-bit clusters is presented. Such a grammar can be defined as follows:

$$G_{3\ BIT} = (N, T, P, STS), \tag{2}$$

where:
$N = \{SECRET, LN, 3B\}-$ non-terminal symbols,
$T = \{000, 001, 010, 011, 100, 101, 110, 111, \varepsilon\}-$ terminal symbols which define each 3-bit value,
$\varepsilon-$ an empty symbol.
$STS =$ SECRET - grammar start symbol.

A production set P is defined in following way:

1. $SECRET \rightarrow LN$

2. $LN \rightarrow 3\text{B LN}$

3. $LN \rightarrow \varepsilon$

4. $3B \rightarrow 000|001|010|011$

5. $3B \rightarrow 100|101|110|111$

A grammar introduced in this way can support a quicker and briefer recoding of the input representation of the secret to be shared. Versions for longer bit blocks can be used in the same way. However, this will require introducing a greater number of linguistic rules. An obvious benefit of grouping bits into larger blocks is that during the following steps of the secret sharing protocol we get shorter representations for the split data. This is particularly visible when executing procedures that use excessive bit representations, i.e. when single-bit or several-bit values are saved and interpreted using codes in 8 or 16-bit representations. As said previously executing the introduced algorithms provides an additional stage for recoding the shared secret into a new representation using grammatical rules. The grammar itself can be kept secret or made available to the participants of the entire protocol. If the allocation of grammatical rules is to remain secret, as mentioned earlier, what we deal with is an arbitration protocol, which - to reconstruct the secret for the authorised group of shadow owners - requires the participation of a trusted arbiter, equipped with information about grammar rules. Should the grammar be disclosed, the reconstruction of the secret is possible without the participation of the trusted person and only on the basis of the constituent parts of the secret kept by the authorised group of participants in the algorithm of information sharing.

5 Conclusion

In this work we present the potential way of expanding clasic threshold secret sharing schemes towards the linguistic descriptions that allow obtaining additional representations that improve the security of the information being split. Linguistic representations were achieved as a result of using sequential grammars that allow conversion of bit representation of the shared secret to the form of a series of numbers of grammatical rules. Such a conversion to the linguistic form is possible thanks to the use of an analyser of polynominal complexity. The possibility of establishing new types of arbitration protocols is the result of introducing linguistic descriptions to the schemes used. The arbitration protocol operates when the rules of the introduced grammar remain secret and are stored with a trusted arbiter. In this case, however, what is necessary to reconstruct the secret is the participation of the arbiter, who will have to disclose his share (being the rules of grammar). Another solution is developing an extended scheme in the case when the grammar defined is public. In such a case, the secret split has the form of a series of grammar production numbers.

Such a presentation is shared by all the participants of the protocol with the same authorisation. The authorised subset of generated shadows allows for the composition of the secret, and the knowledge of the grammatical rules allows for converting this secret into the form of a bit, and later numerical or text, sequence.
The research conducted in this field by the author is focused on the definition of methodology and effective means of using threshold techniques for information sharing for multilevel, intelligent management of strategic or multimedia data stored in digital form. The implementation of the method described allows using mathematical techniques for tasks from the realm of intelligent information management in the case of information assigned to large groups of users or employers of institutions. As application of such methods allows sharing information in any institution, the subsequent step in our research will be an attempt to define the model structure or flow and assignment of constituent information to individual groups of interested and authorised persons. Such a model may later be implemented practically for sharing special multimedia information in the form of multiply digital signatures or multimedia watermarking.

Acknowledgments

This work has been supported by the AGH University of Science and Technology under Grant No. 10.10.120.783

References

1. Asmuth, C.A., Bloom, J.: A modular approach to key safeguarding. IEEE Transactions on Information Theory 29, 208–210 (1983)
2. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Constructions and bounds for visual cryptography. In: Meyer auf der Heide, F., Monien, B. (eds.) ICALP 1996. LNCS, vol. 1099, pp. 416–428. Springer, Heidelberg (1996)
3. Beguin, P., Cresti, A.: General short computational secret sharing schemes. In: Guillou, L.C., Quisquater, J.-J. (eds.) EUROCRYPT 1995. LNCS, vol. 921, pp. 194–208. Springer, Heidelberg (1995)
4. Beimel, A., Chor, B.: Universally ideal secret sharing schemes. IEEE Transactions on Information Theory 40, 786–794 (1994)
5. Blakley, G.R.: Safeguarding Cryptographic Keys. In: Proceedings of the National Computer Conference, pp. 313–317 (1979)
6. Blakley, G.R.: One-time pads are key safeguarding schemes, not cryptosystems: fast key safeguarding schemes (threshold schemes) exist. In: Proceedings of the 1980 Symposium on Security and Privacy, pp. 108–113. IEEE Press, Los Alamitos (1980)
7. Blundo, C., De Santis, A.: Lower bounds for robust secret sharing schemes. Inform. Process. Lett. 63, 317–321 (1997)
8. Charnes, C., Pieprzyk, J.: Generalised cumulative arrays and their application to secret sharing schemes. Australian Computer Science Communications 17, 61–65 (1995)
9. Desmedt, Y., Frankel, Y.: Threshold Cryptosystems. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 307–315. Springer, Heidelberg (1990)

10. Hang, N., Zhao, W.: Privacy-preserving data mining Systems. Computer 40, 52–58 (2007)
11. Jackson, W.-A., Martin, K.M., O'Keefe, C.M.: Ideal secret sharing schemes with multiple secrets. Journal of Cryptology 9, 233–250 (1996)
12. Ogiela, M.R., Ogiela, U.: Linguistic Cryptographic Threshold Schemes. International Journal of Future Generation Communication and Networking 1(2), 33–40 (2009)
13. Shamir, A.: How to Share a Secret. Communications of the ACM, 612–613 (1979)
14. Simmons, G.J.: An Introduction to Shared Secret and/or Shared Control Schemes and Their Application in Contemporary Cryptology. The Science of Information Integrity, pp. 441–497. IEEE Press, Los Alamitos (1992)
15. Tang, S.: Simple Secret Sharing and Threshold RSA Signature Schemes. Journal of Information and Computational Science 1, 259–262 (2004)
16. Wu, T.-C., He, W.-H.: A geometric approach for sharing secrets. Computers and Security 14, 135–146 (1995)