applied sciences

MDPI

Article

Linguistic Methods of Image Division for Visual Data Security

Lidia Ogiela [1,*] and Marek R. Ogiela [2]

[1] Institute of Computer Science, AGH University of Krakow, 30 Mickiewicza Ave., PL-30-059 Kraków, Poland
[2] Cryptography and Cognitive Informatics Laboratory, AGH University of Krakow, 30 Mickiewicza Ave., PL-30-059 Kraków, Poland; mogiela@agh.edu.pl
* Correspondence: logiela@agh.edu.pl

Abstract: This paper defines new classes of algorithms for securing and sharing visual information. Algorithms offering data protection against unauthorised access are cryptographic protocols for data sharing and splitting. These protocols ensure the division of information among a trusted group of secret holders, with every protocol participant being allocated a specified number of shares in the executed algorithm. Proposing and defining new solutions in the field of cryptographic algorithms for data sharing constitutes the main topic of this paper. This paper discusses a new class of algorithms for secret sharing with the use of linguistic formalisms dedicated to the processes of meaning interpretation and linguistic data sharing. Linguistic threshold schemes serve the processes of data protection in distributed systems; they are also used to distribute the shared secret parts in an optimum way, and to perform the meaning analysis and interpretation of various data sets. Semantic analysis as an element of the impact assessment of the meaning of the interpreted and analysed data will make it possible to take into consideration a much wider aspect of description and interpretation of the analysed phenomenon or data set; it will also enable the assessment of the core of the characterised sets in respect to other information with related meaning. The proposed protocols enhance the security of shared data, and allow the generation of any number of secret shares, which is greater than traditional secret sharing methods.

Keywords: information security algorithms; linguistic AI methods; data sharing protocols; information management in distributed systems

Citation: Ogiela, L.; Ogiela, M.R. Linguistic Methods of Image Division for Visual Data Security. *Appl. Sci.* **2023**, *13*, 4847. https://doi.org/10.3390/app13084847

Academic Editors: Jan Egger and Mostafa Fouda

Received: 4 February 2023
Revised: 8 April 2023
Accepted: 10 April 2023
Published: 12 April 2023

1. Introduction

Algorithms used to protect data or strategic information against their disclosure are commonly understood as data concealment algorithms. Data subject to the processes of concealment can cover various degrees of protecting them against the disclosure of their complete content. This is because both individual pieces of information and entire data sets are concealed; this process can also refer to a complete or partial limitation of access to the secured information. Independent of the type of algorithms used for data protection and security, they are examples of cryptographic protocols to conceal information.

Protection and security protocols to protect data against disclosure or access to them are there to completely safeguard information which is secret, confidential or restricted. Such protocols serve the purpose of protecting access to the data by unauthorised data holders. Such processes can be executed at every stage of secret management, both at the stage of obtaining data, processing or storing it, as well as at the stage of data analysis and security [1–3].

Confidential data are subject to protection in the following scope:

- Disclosure both of the very existence of and the content of the secret information,
- Disclosure of secret information holders and persons who have access to the protected information sets,
- Disclosure of the content and meaning of the concealed information sets,
- Making secret information public.

Protocols serving the security of secret information can be used to protect confidential, secret or strategic, defence or other information that is important for further development, etc. They are executed with the use of cryptographic techniques dedicated to the execution of information protection processes. In this group of protocols guaranteeing data protection against disclosure, we can differentiate between the following algorithm classes:

- Information encrypting algorithms,
- Data encoding algorithms,
- Data concealment algorithms,
- Data splitting and sharing algorithms.

The leading topic of this paper is drafting a new class of algorithms for the protection of visual data, with the use of splitting techniques.

Information security protocols ensure that a secret is divided and shared among a specified group of protocol participants and holders of concealed information parts. The participants of secret sharing protocols obtain a specified number of shadows, which on their own do not constitute any information, but when put together with other secret parts, they make it possible to reproduce the concealed information. Every participant of the secret sharing protocol becomes a trustee of the shadows he or she keeps and manages. The execution of data sharing algorithms is possible as a result of the application of both data splitting schemes and information sharing schemes.

The processes of data security with the use of cryptographic data sharing information protocols have been described in previous papers [4–7], where the requirements and individual stages of the processes of data sharing information have been discussed. The selection of an optimum solution depends on the data splitting task executed.

Secret data can be divided among a specified group of secret trustees. Each of them becomes the holder of a part of the split information. Disclosing the content of selected (individual) secret parts does not breach the safety of the entire secret because a single shadow does not contain information that could disclose either a part of the divided secret or its entirety. Moreover, a loss of any shadow has an impact on the possibility to recreate the secret shared.

Cryptographic data sharing protocols cover two types of data concealment algorithms. These are data splitting and data sharing protocols. Data splitting protocols require, in the process of secret re-creation, that all of the constituent elements (shadows) be put back. On the other hand, in data sharing protocols, to reproduce the concealed information it is sufficient to put together a specified number of shadows.

Solutions used thus far have focused on the selection of an optimum protocol for data splitting and sharing as well as methods to generate individual parts of the shared secret, taking into consideration all possible solutions. However, the possibilities of including a process of generating a linguistic shadow containing the characteristics of the concealed data have not been analysed. Generating a linguistic shadow in data sharing protocols would make it possible to take the meaning of the analysed data into consideration, simultaneously bearing in mind the process of splitting (or not) the linguistic shadow. Such an innovative approach to the tasks of concealing data is the leading topic of this paper.

The characteristics of selected solutions are presented in the subsequent chapters of this paper. The structure of this publication is as follows: In chapter two, we discuss secret sharing protocols and their characteristic features. In chapter three, we define a new class of threshold schemes, based on the application of linguistic description formalisms—linguistic threshold schemes. Chapter four contains examples of applications of some defined linguistic threshold schemes. The last chapter presents the summary of this paper and further directions for the development of the solutions proposed here.

2. Secret Sharing Schemes

Data sharing schemes are used to protect and conceal data by means of splitting them into parts, of which, every part (shadow) is allocated to a selected protocol participant. The process of information splitting is executed with the use of a selected data sharing

scheme. Protocols of this class include schemes defined as (m, n)-threshold schemes, where n represents the number of all parts of the split secret, while m represents the number of shadows necessary to reproduce the original message.

The following algorithms belong to the group of data sharing techniques [8–11]:

- (m, n)-threshold schemes,
- Protocols of data sharing with fraudulent (cheating) persons,
- Secret sharing algorithms without the participation of an arbiter,
- Data sharing techniques without disclosure of one's parts,
- Message sharing algorithms with a check,
- Data sharing schemes with measures to prevent disclosure,
- Secret sharing techniques with withdrawal of a shadow.

The data sharing algorithms that are most frequently used are the Lagrange interpolating polynomial, the vector algorithm, the Asmuth–Bloom algorithm, the Karnin–Greene–Hellman algorithm and the Shamir algorithm [8].

Data sharing protocols are used in the process of concealing a secret by means of dividing it and distributing parts of the secret among protocol participants. The information is shared by a specified group of secret trustees, where everyone obtains a specified number of secret parts. A protocol participant does not know the content of the entire secret; he or she only knows the 'content' of the shadow allocated to them, which is of no relevance to the content of the entire secret. Therefore, disclosing the content of the shadow allocated to a given protocol participant, or unauthorised acquisition by third persons, will not put the safety of the entire information at risk. This is because, to disclose the content of the shared secret, it is necessary to have and to put together a given number of shadows, specified as m. The number of shadows, m, necessary to recreate the shared information is defined at the stage of defining the secret sharing protocol.

The data sharing process scheme is shown in Figure 1.

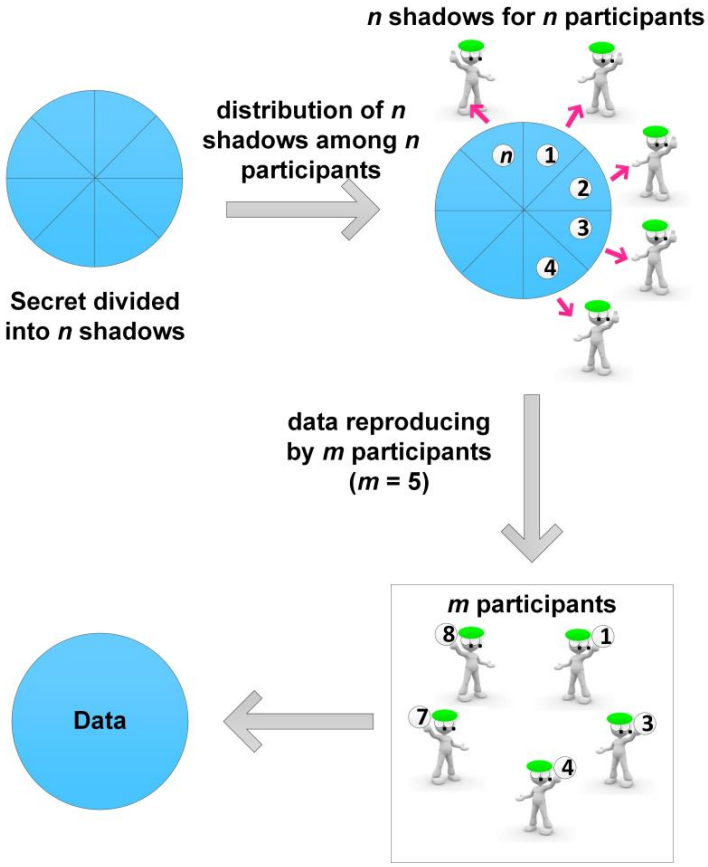

Figure 1. Schematics of the data sharing process.

The threshold data sharing scheme, drafted on the basis of polynomial equation definition in a finite field, has been proposed by Adi Shamir [8]. The main stages of this protocol are as follows:

1. Choosing the number p, which is a prime number, larger than the number of shadows and the largest secret information that is possible to share,
2. Generating any polynomial of m—one degree,
3. Producing shadows $k_i = F(x_i)$ by means of calculating the values of the n polynomial at various points,
4. Distribution of parts of the shared information (shadows) among secret trustees.

In data sharing protocols every protocol participant obtains a specified number of shadows, depending on the number of protocol participants.

The number of participants in the data sharing protocol is determined at the stage of definitions; the secret is divided for a specified (known) number of participants, and each participant obtains the same or different number of shadows. The method of secret shadow distribution among secret holders can be as follows:

- With equal rights:
  - With one shadow allocated—every protocol participant receives only one shadow,
  - With the allocation of more than one shadows—every protocol participant receives the same number of shadows, greater than one,
- Varied:
  - Every secret trustee obtains a different number of shadows,
- Privileged:
  - Every secret trustee in a specified group of shadow holders obtains a larger number of shadows than the remaining protocol participants,
  - A selected group of shadow holders receives a smaller number of shadows, while the remaining protocol participants obtain a larger number.

3. Linguistic Threshold Schemes

The use of threshold schemes in the processes of protection and security of visual data is the most frequent area where these solutions are used. This group also includes a new solution, based on the application of linguistic solutions to the tasks of secret sharing. This task has been discussed in a previous paper [11], where we presented the possibilities of applying linguistic methods for semantic interpretation of data concealment tasks.

The methods of linguistic data description include various linguistic formalisms dedicated to the tasks of meaning description and data interpretation. The most important stage of the entire process of linguistic description is an appropriate selection of linguistic formalism, ensuring an optimum (most appropriate) description of the analysed data. Data meaning analysis has been described by, among others, the authors in [10,12], where it was characterised with an impact assessment of its use in the processes of automatic interpretation of various data sets. In this paper, the authors have focused on the possible applications of linguistic formalisms in the processes of data concealment, particularly in secret sharing schemes.

A new feature of the proposed solution is that it is possible to generate an additional shadow containing linguistic information. This shadow is also subject to the process of allocation among secret trustees; thus, it is also subject to the division process. Depending on the applied division method of the linguistic shadow, we can differentiate between the following solutions:

- The arbiter knows the linguistic information, while the remaining protocol participants do not have such knowledge and the said information:
  - is not subject to the division process—in this case, the shadow containing the semantic information is held by the arbiter as assigning it to any other protocol participant would disclose the content of the information,

- is subject to the division process—in this case, the linguistic shadow is subject to the division process, while its individual parts undergo the process of allocation to protocol participants,

- The arbiter does not have any knowledge concerning the linguistic information and the said information is subject to the division process.

Taking into consideration the options above, we have proposed the following classification of linguistic threshold schemes:

- Linguistic threshold schemes without linguistic shadow division—the semantic information is in a part of the secret that is additionally generated (Figure 2),

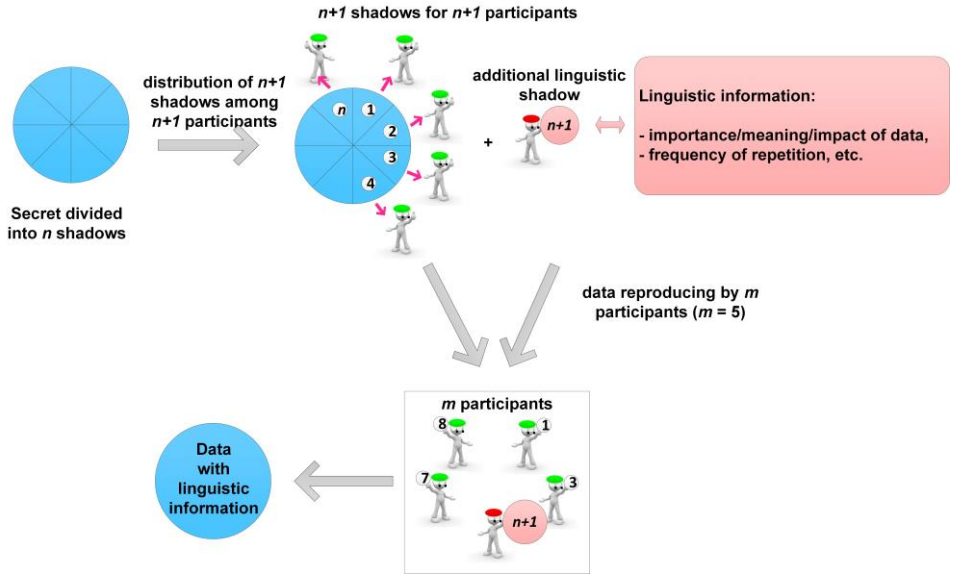

Figure 2. Schematics of linguistic threshold schemes without linguistic shadow division.

- Linguistic threshold schemes with linguistic shadow division—the semantic information is in an additionally generated shadow constituting secret data, subject to the division process (Figure 3).

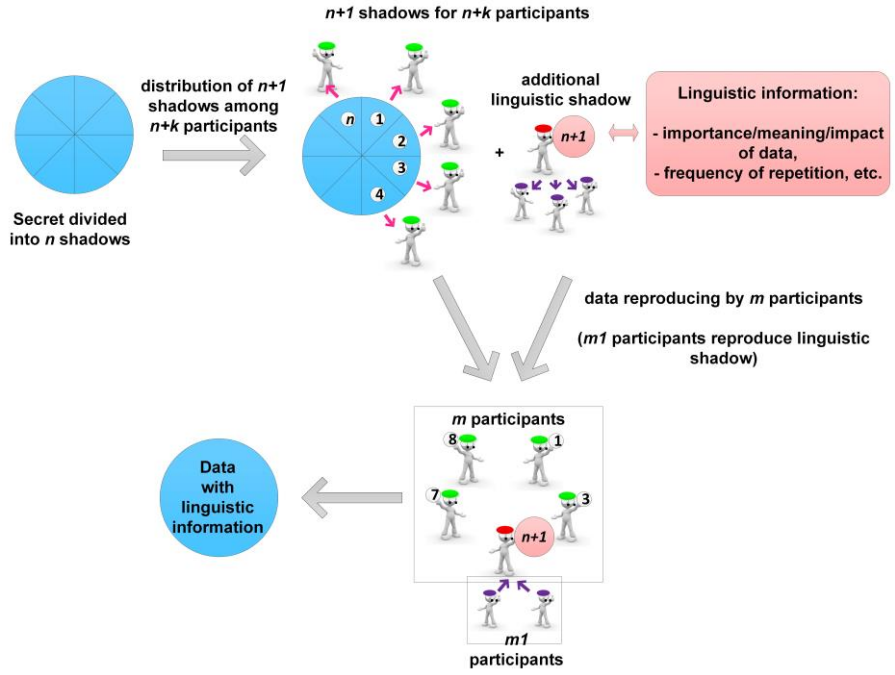

Figure 3. Schematics of linguistic threshold schemes with linguistic shadow division.

Linguistic threshold schemes guarantee information security as a result of the application of not only data sharing protocols and the allocation of individual secret parts to a specified group of secret trustees, but also primarily due to the application of meaning description and interpretation of the shared secret. The application of the meaning techniques of data analysis and interpretation based on the use of grammar formalisms makes it possible to conduct a complete and unambiguous analysis of the shared secret content. The application of linguistic procedures of meaning description of the shared secret makes it possible to enrich the classic solutions with new possibilities in the protected data analysis. This process is important because we can assess the impact of the significance of the protected information on the entire data protection process. The knowledge of the arbiter concerning the role and meaning of the concealed information has an impact on the way he/she selects appropriate data protection protocols.

The application of appropriate (m, n)-threshold schemes generates a clear-cut method of secret division, shadow distribution among protocol participants, as well as the required number of shadows necessary to reproduce the original message. In linguistic threshold schemes, there is a need to determine the number of shadows necessary to recreate the concealed information. In order to reproduce the original message by linguistic threshold schemes, it is necessary to put together:

- The required m number of shadows, without the linguistic shadow; this is an example of a classic (m, n)-threshold scheme,
- The required m number of shadows with the linguistic shadow; this is an example of a linguistic threshold scheme containing semantic information regarding the meaning of the shared data.
- The required m number of shadows, with the required k number of parts of the shared linguistic shadow; this is an example of a linguistic threshold scheme, in which, to reproduce the original information with its linguistic description, it is necessary to reproduce the linguistic shadow by means of k parts of the divided linguistic shadow. The $k < m$ number is the necessary number of parts of the shared linguistic shadows required to reproduce the original message. At the same time, in order to reproduce the entire original message, it is necessary to put together k parts of the linguistic shadow and $m - k$ parts of the remaining shadows.

In linguistic threshold schemes, it is therefore necessary to define the role and significance of the concealed information. The larger their impact, the greater the number of the linguistic shadow parts required in the process of recreating the original message. In this way, it is possible to determine the required k parts of the linguistic shadow as well as the dependence on the m number, i.e., the number of shadows required to reproduce the shared message in linguistic (m, n)-threshold schemes.

By means of application in the linguistic threshold schemes, the rules of grammar description and formalisms of the meaning of data interpretation, these protocols can be used both to guarantee the security of the concealed data and the meaning information contained in the protocols executed. Furthermore, they can also be used to describe the meaning of the protected secret.

Linguistic threshold schemes are a universal data protection tool enhanced by elements of meaning description and interpretation of the shared information; therefore, they can be used by various entities to conceal the meaning of secret (confidential, restricted, strategic) data.

4. Security Analysis

The security of linguistic schemes can be demonstrated based on the properties of classical threshold schemes used to create linguistic protocols. A model for creating new linguistic protocols is based on Shamir's [8] and Tang's [9] schemes. Both of these schemes guarantee absolute security from a cryptographic point of view using appropriately constructed interpolation polynomials [8] or finite field algebra operation [9].

The solutions presented in this work additionally use formal grammars of the appropriate type. These can be regular grammars or context-free grammars of the appropriate class of sequential grammars. Tree or graph grammars, for which syntactic analysis has higher computational complexities, can also be used in the creation of linguistic schemes. Table 1 presents the time complexities for parsing tasks using the appropriate class of grammars that can be used to create image linguistic threshold schemes.

Table 1. Computational complexity for different classes of grammars used in linguistic threshold schemes.

Type of Grammar	Parsing Complexity
Sequential—regular	O(x)—linear
Sequential—context-free	$O(x^k)$—polynomial
Tree grammar, general	$O(2^n)$—exponential
Tree grammar, modified	$O(x^k)$—polynomial
Graph grammar, general	$O(2^n)$—exponential
Graph grammar, modified	$O(x^k)$—polynomial

The use of grammars of the appropriate class fully preserves the security properties of the data sharing protocols created, and additionally allows the generation of linguistic shares. Together with information about the type of grammar used, this constitutes additional secret shares that are necessary for the restoration of the entire secret.

The presented linguistic secret sharing protocol has the properties of cryptographic information sharing procedures. In practice, this means that the secret or image reconstructed after splitting is identical to the data being split. In order to reconstruct the information, such procedures require a particular number of shares that are distributed among users and cannot not be modified in any way. The introduction of modifications to individual shares renders them useless and cannot be used to reconstruct the secret. All information sharing protocols have similar features.

5. Results of the Application of Linguistic Threshold Schemes

The possibilities of applying new classes of cryptographic solutions in the area of data protection, in particular linguistic threshold schemes, are varied. The most important are visual information security and image databases protection. It is also possible to apply such techniques to the strategic development of healthcare institutions and enterprises at a regional and national level, guaranteeing the security of data transmission with information relevant to the patients and institutions and ensuring the security of computer networks and data transmission in IT networks.

An example of the application of linguistic threshold schemes is guaranteeing the security and efficient management of sensitive, secret or personal data. The processes of the safe management of information that is confidential to a significant extent are conducted by governmental or business bodies, corporations and other entities. Linguistic threshold schemes can also be used in the decision-making processes in healthcare institutions, where in order to make an optimal decision, we need a complex analysis of big data and situations, while the actions taken are of strategic or developmental relevance; as such, access to them is limited.

Another area of application of linguistic threshold schemes is in data protection and distribution at various levels of their processing, taking into consideration the level of an entity: the superior level in hierarchical structures or external levels to a given structure (where the level of fog and cloud belong).

Figure 4 presents an example in which we can divide medical visualization towards the generation of a particular number of secret parts. Such generated shares can be distributed over cloud infrastructures, and later reconstructed by the compilation of the required number of visual parts. Depending on the number of compiled shares, we can obtain source data with different quality parameters or simply prevent unauthorised users from revealing source data.

Figure 4. Example of medical visual data sharing. In this example, a selected image was divided into five parts (visible as grey bars) in such a manner that, for restoration, at least three parts are required. Depending on the number of selected parts the original image can be restored with different quality levels.

Figure 5 shows an example of generating language shadows (secret parts) for a very simple input sequence.

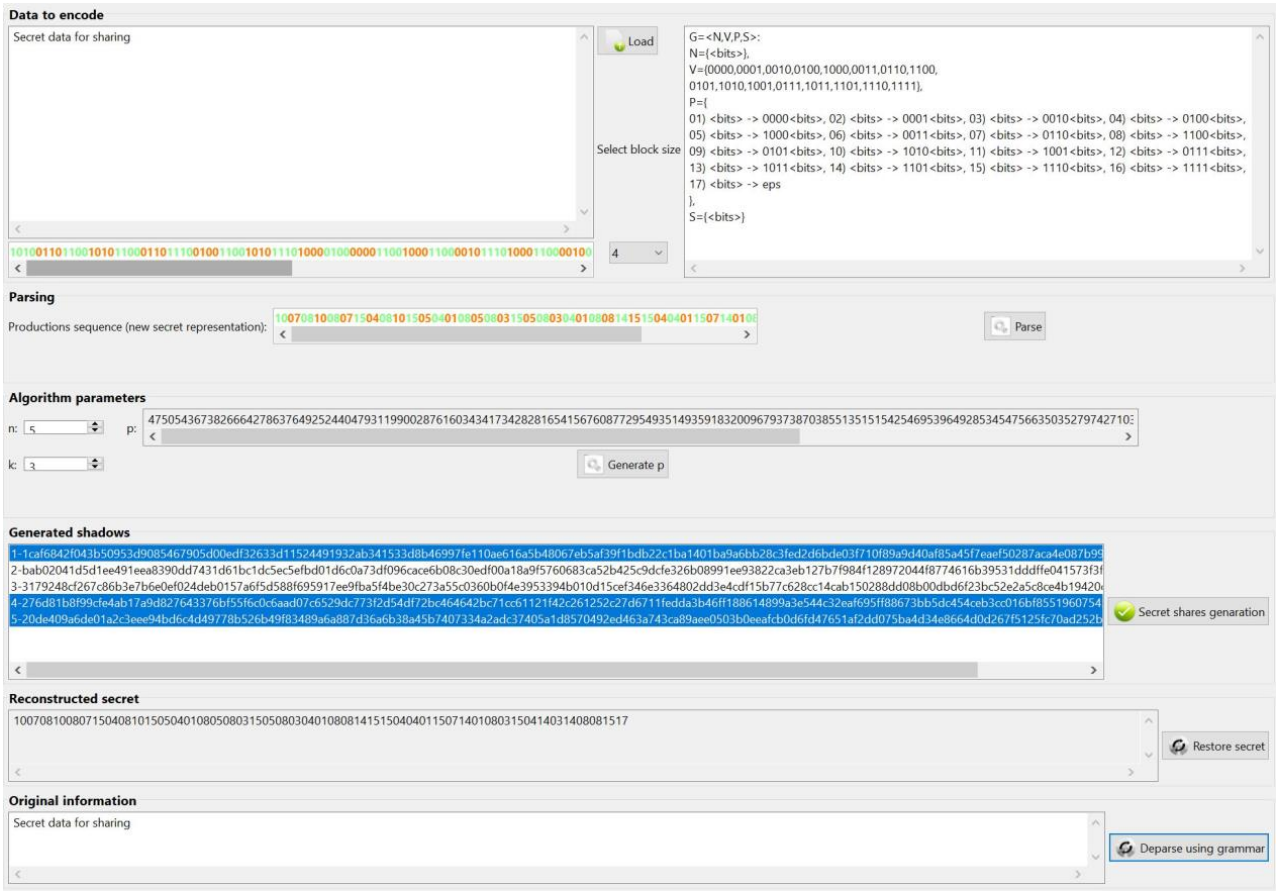

Figure 5. Linguistic shadow generation for an example input sequence. Different colours indicate consecutive 4-bit blocks, and the corresponding rules in the defined grammar.

This example shows how, for a short input sequence and using simple string grammar, a new linguistic representation of the secret can be created and the secret components of the shared data can be generated.

6. Discussion

The meaning description, data interpretation and analysis were dedicated to the processes of cognitive information management. The paradigm of data cognitive management has been defined by the authors in [12,13], where the process of the meaningful execution of tasks to achieve a specified result has been described; with the use of appropriate measures, the meaning of the described data sets in the processes of obtaining, developing, storing and making available the processed information can also be described.

Cognitive management is dedicated to the support of classic data management processes executed in various entities and structures, in reference to various data and information. This can also be used in healthcare applications and systems.

The use of such algorithms in healthcare systems is crucial because, while many hospital data management systems (hospital information systems) allow data to be secured through encryption, such systems make virtually no use of secret sharing algorithms. Simple encryption guarantees the confidentiality of a patient's data, but does not allow the patient to participate in the assignment of rights to reproduce his personal and diagnostic data. Such solutions are instead made possible by using the described linguistic threshold schemes, in which the patient is one of the parties sharing their own diagnostic data.

If we take into consideration the linguistic threshold schemes analysed in this paper, with their application possibilities, we must include in our analysis the possibilities of executing cognitive management processes relating to the discussed data protection protocols [14–17]. The main areas of application of linguistic threshold schemes in the processes of cognitive management are the management and concealment of data with strategic importance as well as the description and interpretation of confidential messages, taking into consideration the reasoning processes relating to possible future changes [18–20].

7. Conclusions

The protocols of data protection and concealment are dedicated to the processes of confidential information protection against disclosure or to prevent access thereto by unauthorised persons. The execution of this task is possible owing to the application of safe cryptographic protocols guaranteeing maximum information protection.

In this paper, we have proposed a new algorithm to divide the secret, taking into consideration the possible meaning of the concealed information. Taking into consideration the opportunity to assess the meaning of the analysed secret data makes it possible both to perform detailed analysis and choose an optimum information sharing protocol. This process includes the division of a secret and distribution of all of its parts among the secret trustees' group. At the same time, the semantic information contained in the protocol referring to the meaning of the concealed information is also subject to the sharing process. The application of data sharing protocols makes it possible to avoid a situation in which secret messages are in the hands of one holder only.

Data sharing protocols ensure information security, which is guaranteed because it is not possible for one single person to disclose the secret. Reproducing the original information is possible only after the number of shadows required by the protocol have been put together.

The innovative solution of this paper is the proposed and discussed linguistic threshold schemes, in which an additional shadow containing linguistic data is generated to describe the meaning of the concealed information and its impact on the entire data protection process. The proposed protocols enhance the security of shared data, and allow the generation of any number of secret shares, which is greater than traditional secret sharing methods.

This paper also presents the possibilities of the application of the discussed solutions as well as further directions for the development of the issues analysed herein.

Author Contributions: L.O.: conceptualization, methodology, software, validation, formal analysis, investigation, writing—original draft, visualization. M.R.O.: conceptualization, methodology, validation, writing—review and editing, supervision. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been partially supported by the funds of the Polish Ministry of Education and Science assigned to the AGH University of Krakow. This research project was supported by the program "Excellence initiative—research university" of the AGH University of Krakow.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analysed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sabir, S.; Guleria, V. Multi-layer security based multiple image encryption technique. *Comput. Electr. Eng.* **2023**, *106*, 108609. [CrossRef]
2. Shan, M.; Guo, J.; Zhong, Z.; Liu, B.; Yu, L.; Liu, L. Security enhanced optical image cryptosystem based on phase encoding by generating a sparse volumetric ciphertext. *Opt. Commun.* **2022**, *516*, 128270. [CrossRef]
3. Ogiela, L. Towards cognitive economy. *Soft Comput.* **2014**, *18*, 1675–1683. [CrossRef]
4. Umapathy, B.; Kalpana, G. A novel symmetric cryptographic method to design block complexity for data security. *Comput. Electr. Eng.* **2022**, *104*, 108467. [CrossRef]
5. Luo, S.; Liu, Y.; Yan, X.; Yu, Y. Secret image sharing scheme with lossless recovery and high efficiency. *Signal Process.* **2023**, *206*, 108931. [CrossRef]
6. Koptyra, K.; Ogiela, M.R. Imagechain—Application of Blockchain Technology for Images. *Sensors* **2021**, *21*, 82. [CrossRef] [PubMed]
7. Ogiela, M.R.; Koptyra, K. Visual Pattern Embedding in Multi-Secret Image Steganography. In Proceedings of the ICIIBMS 2015—International Conference on Intelligent Informatics and BioMedical Sciences, Okinawa, Japan, 28–30 November 2015; pp. 434–437, ISBN 978-1-4799-8562-3/15.
8. Yan, S.Y. *Computational Number Theory and Modern Cryptography*; Wiley: Hoboken, NJ, USA, 2013.
9. Katz, J.; Lindell, Y. *Introduction to Modern Cryptography*; CRC Press: Boca Raton, FL, USA, 2021.
10. Ogiela, M.R.; Ogiela, L.; Ogiela, U. Biometric Methods for Advanced Strategic Data Sharing Protocols. In Proceedings of the 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Blumenau, Brazil, 8–10 July 2015; pp. 179–183. [CrossRef]
11. Ogiela, M.R.; Ogiela, U.; Ogiela, L. Secure Information Sharing Using Personal Biometric Characteristics. In *Computer Applications for Bio-Technology, Multimedia and Ubiquitous City*; CCIS, 353, Kim, T.H., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 369–373.
12. Ogiela, L.; Ogiela, M.R. Cognitive security paradigm for cloud computing applications. *Concurr. Comput. Pr. Exp.* **2020**, *32*, e5316. [CrossRef]
13. Nakamura, S.; Ogiela, L.; Enokido, T.; Takizawa, M. Flexible Synchronization Protocol to Prevent Illegal Information Flow in Peer-to-Peer Publish/Subscribe Systems. Complex, Intelligent, and Software Intensive Systems. *Adv. Intell. Syst. Comput.* **2018**, *611*, 82–93.
14. Gerodimos, A.; Maglaras, L.; Amine Ferrag, M.; Ayres, K.; Kantzavelou, I. IoT: Communication protocols and security threats. *Internet Things Cyber Phys. Syst.* **2023**, *3*, 1–13. [CrossRef]
15. Loukil, F.; Ghedira-Guegan, C.; Benharkat, A.N.; Boukadi, K.; Maamar, Z. Privacy-Aware in the IoT Applications: A Systematic Literature Review. In Proceedings of the International Conference on Cooperative Information Systems (CoopIS), Edinburgh, Scotland, 2–4 September 2017; Springer: Cham, Switzerland, 2017; Volume 10573, pp. 552–569.
16. Bułat, R.; Ogiela, M.R. Comparison of Personal Security Protocols. In *Advanced Information Networking and Applications*; AINA 2021; Springer: Cham, Switzerland, 2021; pp. 672–678.
17. Bojinov, H.; Sanchez, D.; Reber, P.; Boneh, D.; Lincoln, P. Neuroscience meets cryptography. *Commun. ACM* **2014**, *57*, 110–118. [CrossRef]
18. Sfar, A.R.; Natalizio, E.; Challal, Y.; Chtourou, Z. A roadmap for security challenges in the Internet of Things. *Digit. Commun. Netw.* **2018**, *4*, 118–137. [CrossRef]

19. Hadnagy, C. *Social Engineering: The Science of Human Hacking*, 2nd ed.; Wiley Publishing: Hoboken, NJ, USA, 2018.
20. Gutub, A.A.A. Adopting counting-based secret-sharing for e-Video Watermarking allowing Fractional Invalidation. *Multimed. Tools Appl.* **2022**, *81*, 9527–9547. [CrossRef]