

Article

Image Division Using Threshold Schemes with Privileges

Marek R. Ogiela ^{1,*}  and Lidia Ogiela ²

¹ Cryptography and Cognitive Informatics Laboratory, AGH University of Krakow, 30 Mickiewicza Ave., 30-059 Krakow, Poland

² Faculty of Computer Science, AGH University of Krakow, 30 Mickiewicza Ave., 30-059 Krakow, Poland; logiela@agh.edu.pl

* Correspondence: mogiela@agh.edu.pl

Abstract: Threshold schemes are used among cryptographic techniques for splitting visual data. Such methods allow the generation of a number of secret shares, a certain number of which need to be assembled in order to reconstruct the original image. Traditional techniques for partitioning secret information generate equal shares, i.e., each share has the same value when reconstructing the original secret. However, it turns out that it is possible to develop and use partitioning protocols that allow the generation of privileged shares, i.e., those that allow the reconstruction of secret data in even smaller numbers. This paper will therefore describe new information sharing protocols that create privileged shares, which will also use visual authorization codes based on subject knowledge to select privileged shares for secret restoration. For the protocols described, examples of their functioning will be presented, and their complexity and potential for use in practical applications will be determined.

Keywords: cryptographic threshold schemes; threshold schemes with privileged access; image division protocols; perception thresholds



Citation: Ogiela, M.R.; Ogiela, L. Image Division Using Threshold Schemes with Privileges. *Electronics* **2024**, *13*, 931. <https://doi.org/10.3390/electronics13050931>

Academic Editor: Luca Mesin

Received: 22 January 2024

Revised: 22 February 2024

Accepted: 26 February 2024

Published: 29 February 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Issues of data partitioning are closely related to the use of cryptographic partitioning protocols and data sharing protocols. Each of these types of protocols are designed to protect data by dividing them.

Data sharing protocols are characterized by the use of an algorithm that specifies the number of shadows (parts) into which a secret is divided and the number of secret trustees (protocol participants) who will receive each part of the secret. This type of data secrecy algorithm is a fairly simple solution, in which the number of n —i.e., protocol participants who receive individual parts of the secret—is determined. To reconstruct the original message, it is necessary to assemble all parts of the divided secret. It is therefore a solution that requires all shadow holders to unanimously confirm the need to reconstruct the classified information. Without the agreement of at least one participant in the protocol, it is not possible to reconstruct the original message, resulting in the inability to read it [1–3].

Another solution is data sharing protocols. In this class of cryptographic algorithms, there is an important difference that distinguishes this solution from sharing protocols. This is because, in the case of data sharing protocols, the secret is divided into a certain number of n shadows distributed among a selected number of n trustees of the secret, with the difference being that the number of m shadows specified in the protocol is sufficient to reconstruct the original message. Such a solution means that not all participants in the protocol have to take part in the process of reconstructing the secret [4–7]. They do not even need to have knowledge that the secret has been read. To implement the process of data sharing, (m, n) -threshold schemes are used. The number n denotes the number of shadows of the shared secret and the number of trustees of part of the secret. And the number m denotes the number of protocol participants required to reproduce the shared secret.

Examples of cryptographic sharing and data sharing protocols include the following:

- Blackley's algorithm [4];
- Shamir's algorithm [5];
- Tang's algorithm [6];
- Lagrange's interpolation polynomial [7];
- Asmuth–Bloom algorithm;
- Karnin–Greene–Hellman algorithm.

Data splitting and sharing protocols are used as a solution to ensure data security. The process is implemented by dividing the data into parts (referred to as shadows in the protocol). The implementation of data partitioning processes is to restrict access to data only to an authorized group of holders of parts of the secret (referred to in the protocol as secret trustees). In this way, only selected participants in the protocol become part of the protocol due to the fact that they each receive their own shadow.

The distribution of the secret and the distribution of shadows is carried out with the participation of an arbitrator, for whom there are expectations to their impartiality and fairness in the process of generating shadows and determining their allocation. In this process, the arbitrator can generate so-called blank shadows and allocate them to selected protocol participants. In this way, they will be aware of their participation in the process of recreating the secret, but they will not participate in the actual implementation of the process due to the fact that the shadows they have do not contain any information.

In a situation where there is no trust in the arbitrator, protocols without the arbitrator are used, in which case the system itself distributes the various parts of the secret and there is no person supervising the entire process of shadow distribution and secret restoration. This is an unsupervised solution, the implementation of which is fraught with certain risks, and the distribution of shadows should only be supervised due to their privileged allocation.

The methods of shadow distribution are varied and depend on the following factors:

- The type of information/data being protected;
- The group of custodians of the secret among whom the various parts of the secret are distributed;
- Dependencies, such as the type of structure in which the shadow keepers function—their superiority, inferiority, or equality to each other.

Information secrecy protocols which divide information are intended to ensure data security and protection by distributing a portion of the secret among a specific group of secret trustees. Thus, this is an example of a data security protocol that can be used in situations where the secret should not be known to only one holder. An example of this type of data might be strategic data, which, when known to one person, will be used by that person for whatever purpose the holder deems appropriate. If, on the other hand, the data are entrusted to a specific group of trustees of the secret, the analysis and proper use of the data will depend on the joint provisions. Such a situation can occur, for example, in supervisory boards, in the management of companies, in the bodies of state institutions, in military units, in the management of companies, and in local government organizations, universities, boards of institutes, etc. In situations where data are subject to protection and the process of secrecy is recommended, the optimal solution is to use data splitting and sharing protocols.

The difference between data splitting and data sharing protocols is the algorithms used and, at the same time, this difference becomes apparent in the process of reconstructing the secret data. The peculiarity of data sharing protocols is that in order to reconstruct the secret, it is necessary to assemble all the parts into which the secret was divided. Thus, this is an example of a solution in which each participant in the protocol receives its shadow, which is equal to any other shadow. Each participant in the protocol must share their shadow in order for the secret to be pored over.

In data sharing protocols, each trustee of a secret receives a shadow, but not all shadows are required to open the original message. This is because the data sharing algorithm determines the minimum number of shadows required to reconstruct the secret

message. In this way, the other protocol participants, whose shadows will not be used in the process of reconstructing the original message, will not be participants in this stage, even though they are participants in the whole process. They have their shadows, but they do not participate in the process of reconstructing the secret.

A schematic view of the processes of splitting and sharing data and the process of restoring the secret is shown in Figure 1.

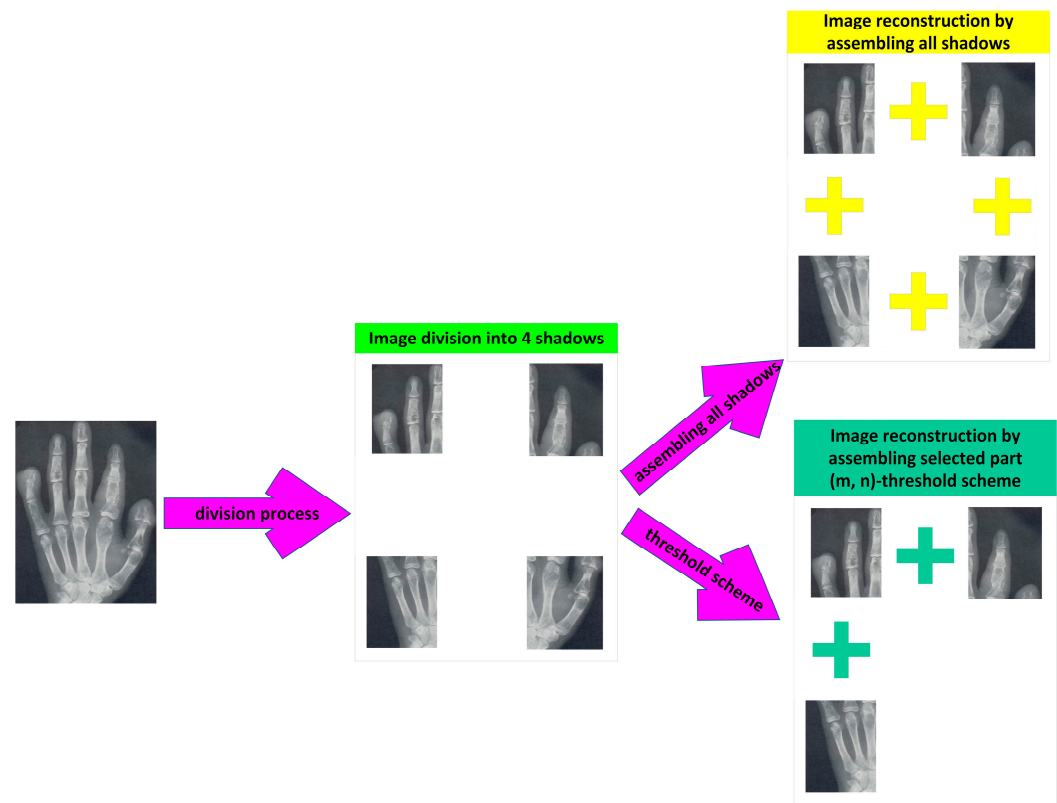


Figure 1. The process of medical image sharing and division along with the process of image restoration. Source: own development.

Figure 1 shows a schematic view of the process of dividing an X-ray image of a hand bone with visible sarcoidosis. The image has been divided into four parts. In the data splitting process, it is necessary to assemble all four parts to reconstruct the original image. In the process of data sharing, it is necessary to assemble a smaller number of parts to reconstruct the image—in this case, the (3, 4)-threshold scheme was used, which means that three of the four parts of the secret are required to be assembled to reconstruct the original image.

In this article, we will propose new protocols for splitting, reconstructing, and sharing data based on information sharing methods that can generate privileged shares. Such techniques will allow the reconstruction of shared information in a threshold manner using the required number of shares, but also using a smaller number of privileged shares. The allocation of privileged shares may consist of linking them for a given user, or allocating them with certain semantic labels in mind [8–11].

These protocols will be used for characteristic data, namely medical image data. The desirability of using such images in data protection protocols is due to the fact that medical images depicting a particular structure often look similar, while different lesions are visible on the image [12].

2. Threshold Schemes with Privileged Access

The main objective of this work is to propose brand new protocols for the sharing of secret or strategic data (including medical images), which will allow the information to be divided into any number of shares which can then be distributed in different locations or assigned to different people or participants of the protocols [13]. The essence of the proposed methods is that some of the created shares or parts of the shared data should be privileged in nature, i.e., the inclusion of privileged parts allows the information to be reconstructed with fewer than the required number of parts. The protocol proposed in the following section will therefore allow the creation of such privileged shares and their transfer to the participants in the secret sharing protocol, who will be able to reconstruct the original information themselves.

We have proposed threshold schemes with privileged distributions as an alternative solution for securing data using privileged access.

The individual steps of the algorithm are as follows:

1. Determination of the method of data distribution and shadow distribution—equal—privileged/privileged distribution;
2. Determination of the number n —the number of participants in the protocol;
3. Determination of the number m —the number of shadows into which the secret will be divided;
4. Determination of the number k —the minimum number of shadows needed to reproduce the shared secret.

In data sharing protocols, it is possible to implement the following image sharing algorithms using a variety of data partitioning and shadow distribution methods:

1. Equal distribution with the allocation of individual shadows to each participant in the protocol. In this solution, the image is divided into n parts, and each part is allocated to one protocol participant. Each participant receives one shadow. The number of participants is equal to the number of shadows. The original image will be reconstructed by assembling any number of m shadows ($m \leq n$).

Symbols relevant to this method are as follows:

n —the number of participants in the protocol and the number of shadows of the shared image;

m —the number of shadows required to reproduce the shared image.

2. Equal division with equal allocation of shadows (greater than 1) to each participant in the protocol. In this solution, the image is divided into n shadows allocated to each participant in the protocol. Each participant receives a certain equal number of shadows. The number of participants is different from the number of shadows. The original image can reproduce a composite of m shadows ($m \leq l$).

Symbols relevant to this method are as follows:

k —the number of shadows allocated to each participant in the protocol ($k > 1$, belongs to natural, $k * l = n$, $k < n$, $k < m$);

n —the number of participants in the protocol;

l —the number of shadows of the shared image;

m —the number of shadows to reproduce the shared image.

3. Privileged division with an equal number of shadows allocated to participants in each group. In this solution, the image is divided into n shadows assigned to individual participants in the protocol. In the protocol, the levels of hierarchy against which the distribution of shadows takes place are defined. Participants of the highest hierarchical level receive the largest number of shadows, and those of the lowest level receive the smallest number of shadows. Each participant of a given hierarchical level receives a certain equal number of shadows. The number of participants in the protocol is different from the number of shadows. The original image can reproduce a composite of m shadows ($m \leq n$).

Symbols relevant to this method are as follows:

n_i —the number of protocol participants at the i -th hierarchical level;

n —the number of shadows of the shared image;

i —the number of hierarchical levels between which the shadows of the shared image will be distributed, $i = 1, 2, \dots, n$;

k_i —the number of shadows allocated to each protocol participant at the i -th hierarchical level

$$\sum (n_i * k_i) = n$$

m —the number of shadows needed to reproduce the shared image.

The above formula determines how to divide the secret in a hierarchical structure consisting of i different layers. The original secret is divided into n different parts altogether, which will be dispersed among participants located in a hierarchical structure containing i different levels. All of the n participants are also at different levels of the hierarchy, and the exact number of participants at each level is determined by the value of n_i . The value of k_i is the number of parts of the secret that has been allocated to the protocol participants located at the i th level of the hierarchical structure.

4. Privileged division with a differentiated number of shadows assigned to participants in each group. In this solution, the image is divided into n shadows assigned to individual participants in the protocol. The protocol specifies the hierarchy levels against which the shadows are distributed. Protocol participants receive varying amounts of shadows, not depending on the group to which they belong. The number of protocol participants is differentiated by the number of shadows. The original image can be reconstructed by assembling m shadows ($m \leq n$).

Symbols relevant to this method are as follows:

n_i —the number of protocol participants at the i -th level;

n —the number of shadows of the shared image;

i —the number of hierarchical levels between which the shadows of the shared image will be distributed, $i = 1, 2, \dots, n$;

k_i —the number of shadows allocated to the protocol participants

$$\sum (n_i * k_i) = n$$

m —the number of shadows needed to reproduce the shared image.

An example of an algorithm that implements the process of image sharing is a solution that divides an image into a specified number of shadows and then assigns privileged shadows to selected protocol participants. In this algorithm, a smaller number of specified shadows can be used to reproduce the original image than would be needed if no privileged shadows are used to reproduce it. The selection of privileged shadows is determined according to the level of expertise dedicated to a specific image (or set of images) that is subject to the sharing process.

A characteristic example of this type of solution can be medical images that highlight lesions in terms of the examined human structure or organ [12]. The process of making these kinds of data secret is to divide the data and distribute the different parts of the medical image, as well as to store individual shadows. The storage of these data can be of importance to those who hold certain positions in public life and to those who seek to keep information about their health secret [14].

In this case, the process of reading the original image will only be possible if all the required parts of the secret are assembled. The assembly of a smaller number of parts, on the other hand, will not reveal the content contained in the image because medical images consist of a group of images whose careful analysis guarantees their correct reading. Any even slight blurring or illegible parts of the image can result in the content of the medical

image being determined in a haphazard manner. In the case of medical imaging, this can result in an overly broad disease spectrum. Even common medical knowledge does not, in the case of medical imaging, provide a clear indication of what can be visualized in a distorted or illegible image. Thus, this is a specific example demonstrating that correct reading/restoration of images is necessary to properly understand the content contained in the image and to fully comprehend it. This is a non-essential process that applies to medical images depicting any of the following:

- Organs of the human body;
- Changes occurring in organs;
- Absence of certain organs or organs with significant deformities, etc.

Other types of images do not carry such ambiguous interpretations. Examples include images of works of art, such as the paintings of a selected master, which, although widely known to a large number of enthusiasts, in the case of lesser-known works of art, knowledge of these paintings will be characterized by a smaller group of people, among whom will be art historians, admirers of the works of a particular painter, museum professionals, and people whose knowledge of works of art is much greater than that of the majority of people.

Similar examples of specialized images can be pointed out, for example, in collections of images of the following categories:

- Satellite images showing:
 - Land deformations;
 - Unusual phenomena;
 - Defense, military, strategic, or secret facilities.
- Geological images showing:
 - The location of geological deposits;
 - Deformations of the terrain;
 - The geological riches of the area, saturation of deposits, etc.

3. Results

The proposed protocols for sharing medical image data are used to implement processes ensuring the security of images representing important medical information. The way to choose an optimal algorithmic solution depends on the information protection procedures adopted. In the case of image data depicting medical information about a specific person, or a selected group of people, it is expedient to use image sharing protocols with a privileged and differentiated distribution of shadows among individual protocol participants. Thus, the distribution of shadows is carried out in a privileged manner, in which a certain number of shadows are held by the person who supervises this protocol (e.g., the person to whom the shared data pertain) and without whose participation it would not be possible to reconstruct the shared medical secret.

The sharing of the data among the other participants in the protocol is intended to ensure the security of the classified information in the event that the data were to be intercepted in an unauthorized manner from the person to whom the data pertain.

Thus, the implementation of an image sharing protocol is a process ensuring secrecy of important information, the disclosure of which may have a negative impact on the diagnostic and therapeutic process of its holder.

An example of the implementation of a medical image data sharing protocol is shown in Figure 2.

Figure 2 shows an example of image data splitting on an X-ray image of a hand bone with visible sarcoidosis. The image was split using the (3, 4)-threshold scheme, which means that the image was divided into four shadows, and the assembly of any three shadows (in this case, they were shadows numbered 1, 3, and 4) allows the image to be reconstructed with the hand bone disease visible. This is an example of equal division, in which the four trustees of the secret are each given one shadow.

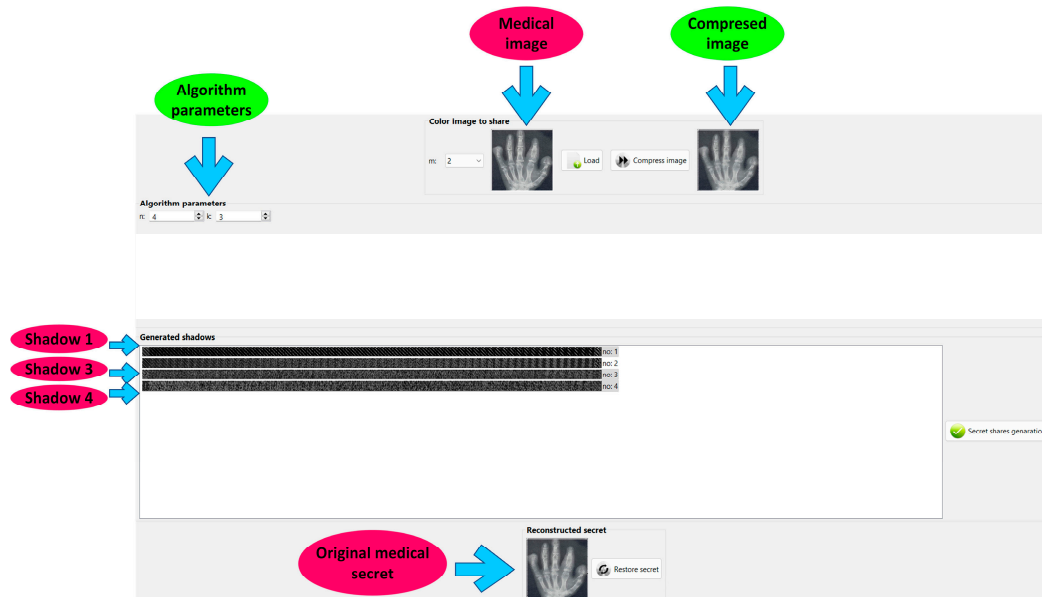


Figure 2. The process of sharing an X-ray image of a hand bone with visible sarcoidosis. Source: own development.

If an unauthorized group of secret trustees attempts to read the image data, the image will not be reconstructed. An example of such an attempt is shown in Figure 3, which highlights an incorrectly reconstructed secret due to the assembly of fewer than the required number of shadows—i.e., an assembly of two out of four shadows when the minimum number of shadows giving a correct reading of the image is three.

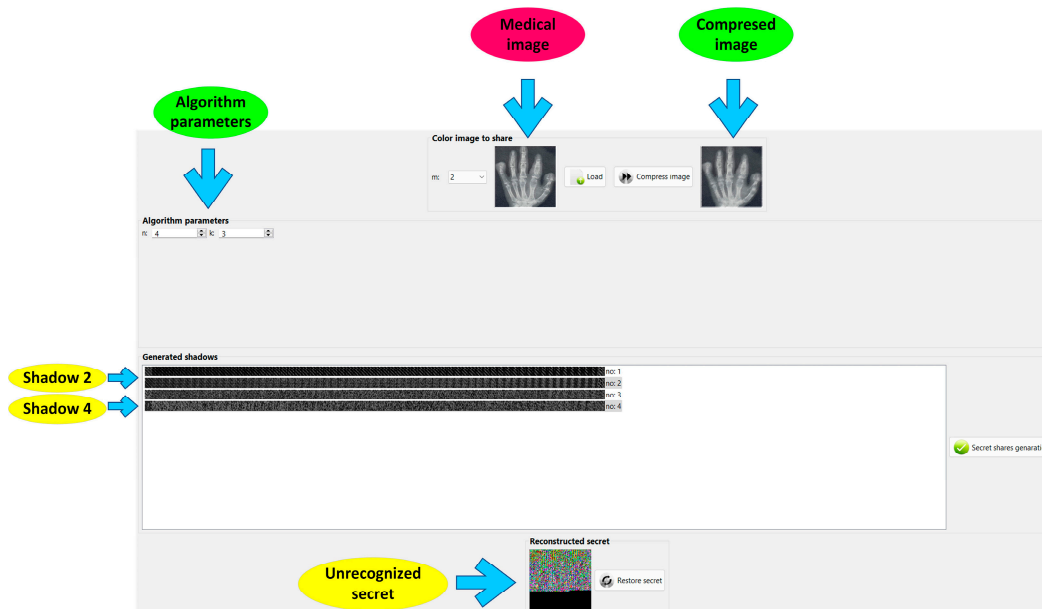


Figure 3. Failure to restore shared X-ray image of a hand bone. Source: own development.

Another example of the use of an image data sharing protocol is shown in Figure 4.

Figure 4 shows the process of reconstructing a shared X-ray image of a hand bone with visible sarcoidosis at different perceptual levels [15,16].

Level one represents the process of reconstructing the secret with the required number of protocol participants. In this case, it is any three of the four protocol participants ((3, 4)-threshold scheme).

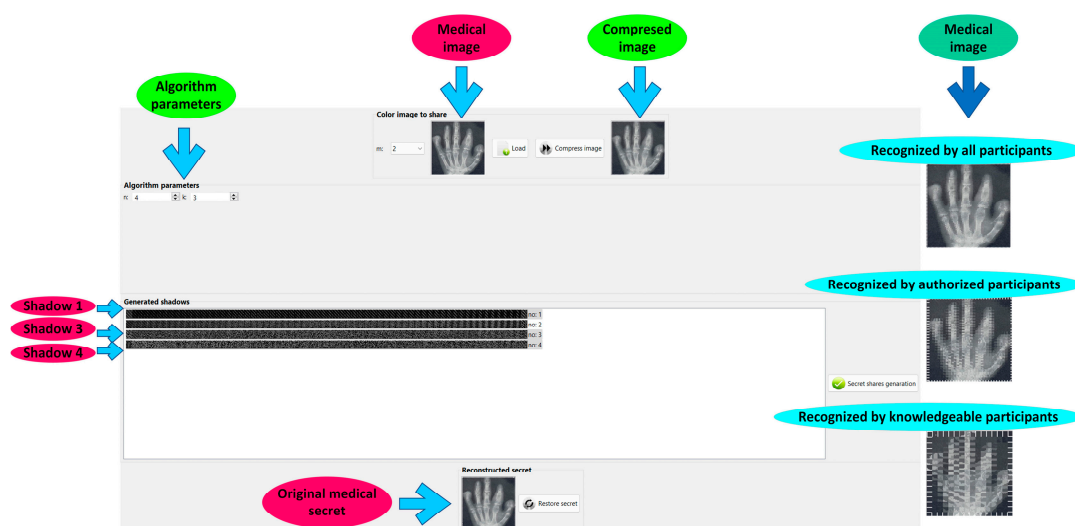


Figure 4. The process of reconstructing a shared X-ray image of a hand bone with different perceptual thresholds. Source: own development.

The second level represents an image that can be correctly reconstructed by authorized participants in the protocol who have factual knowledge of the image being reconstructed. Thus, its correct recognition does not require full restoration because this group may have the knowledge to correctly read the image on the basis of certain features contained in it.

The third level allows the image to be read by protocol participants with specialized knowledge. In this case, although the image is unreadable, certain features of the image combined with the expertise of the specialist will allow the image to be read correctly.

The example shown in Figure 4 showing the possibilities of reading the image at different perceptual levels is characteristic of image sharing protocols with a privileged shadow distribution. In this case, a protocol participant who receives a greater number of shadows than other participants and at the same time has knowledge of the shared secret can successfully reconstruct the shared image. An example of such a solution is shown in Figure 5.

Figure 5 shows the sharing of an X-ray image of a hand bone using the (3, 4)-threshold scheme, in which any three of the four shadows are must be assembled to reconstruct the image, but in which the X-ray image is correctly recognized at a higher perceptual level than the basic level, as the image details at the basic level are unreadable.

Since many threshold sharing schemes for visual data require performing image compression before splitting is performed, therefore, in a situation where the degree of compression somewhat blurs the details of the image, the correct restoration and recognition of the image by the user depends not only on the number of complex shares but also on having the expertise (in this case, medical expertise) to correctly recognize the contents of such an image.

Selecting protocol participants who can reproduce the secret image and who have more than basic knowledge of the shared image allows for proper reading of the image.

In hierarchical structures, such capabilities may be possessed by a decision maker, holding the highest hierarchical position, with specialized knowledge regarding specific lesions present in a particular patient. Thus, as a result of the implementation of a specific cryptographic protocol, this decision maker would be able to read the full content of the shared image.

The effectiveness of the solutions used in the process of image data secrecy is high. This is because of the following aspects:

- The use of cryptographic protocols for sharing image data;
- The proper selection of the shadow distribution process—privileged or peer-to-peer sharing;

- The determination of perceptual levels to facilitate the privileged image reproduction process;
- Any modification of the aforementioned steps.

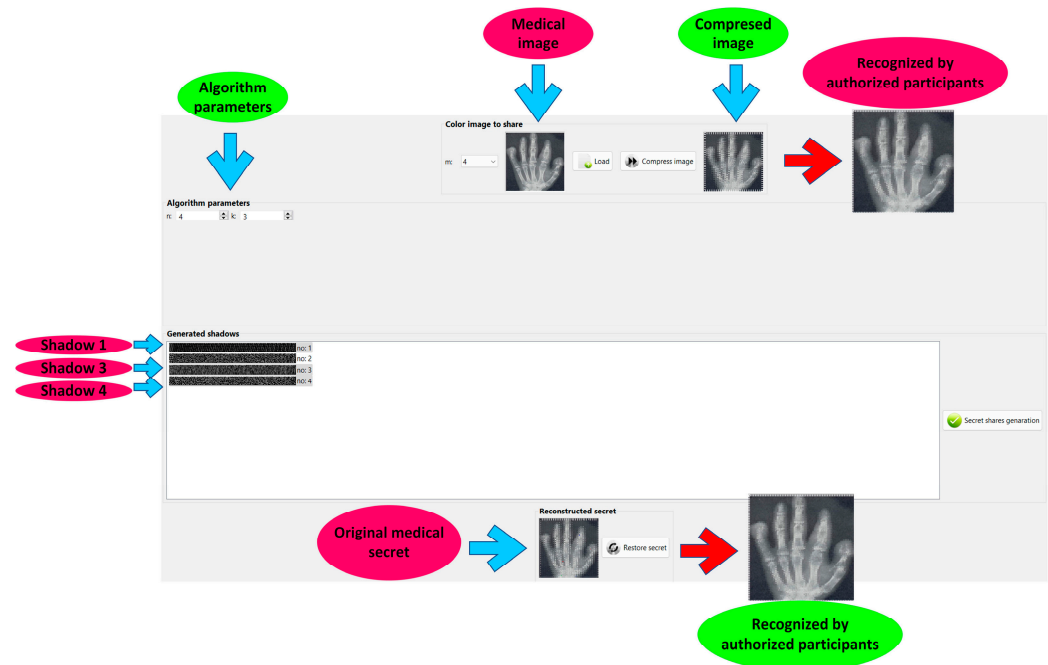


Figure 5. The process of splitting and reconstructing a shared X-ray image of a hand bone with a selected perceptual threshold. Source: own development.

The division of a secret image into privileged shares is implemented using one of the standard threshold division methods, but with the difference being that selected participants (e.g., those with higher priority in accessing the data) will have privileged shares or several independent shares, which will also give them a privileged position.

Evaluating the computational complexity of such a solution must therefore take into account the complexity of the native division algorithm, as well as the procedure for creating and allocating privileged shares, which is placed on polynomial level. Since standard methods of dividing the secret usually also have polynomial complexity, so the additional calculations involved in allocating multiple or preferred shares will also remain at the same level, i.e., polynomial complexity $O(x^n)$, where n denotes the degree of the polynomial. Of course, at this point, we need to take into account the issue of scalability of threshold partitioning algorithms. For example, in the case of Shamir's method based directly on polynomials, large values of (m, n) -threshold division may require calculations on polynomials of the degree $m - 1$. In practice, this may mean that the complexity of the algorithm is polynomial, but that the polynomial is of a high degree.

The described secret division protocols are universal and scalable, and allow any number of secret parts to be easily generated. They can be easily applied in small computing infrastructures, as well as in large distributed systems equipped with many computational or storage nodes. Secret information can also be divided into several thousand parts for security purposes and later revealed by assembling the required number of parts using the presented solutions. These results present solutions that can be implemented for general security purposes, and also for specific cybersecurity solutions.

4. Conclusions

This paper presents a new approach to the issue of image data secrecy by splitting images using image sharing protocols. These protocols have been developed for a variety of shadow distribution types, including peer and privileged separation. These processes

can be effectively implemented in a variety of structures in which image data operate and may be subject to latency. The developed image sharing protocols are discussed on the basis of the division of medical images. The information contained in such images is extremely difficult to interpret unambiguously, which, in the case of image partitioning (i.e., into shadows), results in the fact that a proper image restoration process requires the implementation of a specific cryptographic protocol. In special cases, as shown in this paper, it is possible to correctly reconstruct an image using the generated privileged shares and perceptual thresholds based on the knowledge of the protocol participants so that the image can be understood as a result of having thematic knowledge.

Future research directions on the described issues may concern both the expansion of the application areas of the described methods, as well as their improvement in terms of the use of additional parameters considered in the division of the secret image [17–19]. Among the new application areas, one can point to the division of data stored on the digital cloud, as well as the creation of multiple keys intended for authentication in remote services [20,21]. Such keys can also be used to create personalized cybersecurity locks. Considering additional parameters, on the other hand, can be related to the use of personal characteristics in information division algorithms or behavioral characteristics, which will allow the creation of partitioning procedures aimed at individual protocol participants or groups of people sharing information with each other.

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

Funding: The research project was supported by the program “Excellence initiative—research university” for the AGH University of Krakow.

Data Availability Statement: Data are contained within the article.

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

References

- Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*; Wiley: Hoboken, NJ, USA, 1996.
- Menezes, A.; van Oorschot, P.; Vanstone, S. *Handbook of Applied Cryptography*; CRC Press: Waterloo, Belgium, 2001.
- Gregg, M.; Schneier, B. *Security Practitioner and Cryptography Handbook and Study Guide Set*; Wiley: Hoboken, NJ, USA, 2014.
- Blakley, G. Safeguarding Cryptographic Keys. In Proceedings of the AFIPS 1979 National Computer Conference, New York, NY, USA, 4–7 June 1979; pp. 313–317.
- Shamir, A. How to Share a Secret. *Commun. ACM* **1979**, *22*, 612–613. [[CrossRef](#)]
- Tang, S. Simple Secret Sharing and Threshold RSA Signature Schemes. *J. Inf. Comput. Sci.* **2004**, *1*, 259–262.
- Ogiela, M.R.; Ogiela, U. Secure Information Splitting Using Grammar Schemes. In *Studies in Computational Intelligence*; Springer: Berlin/Heidelberg, Germany, 2009; Volume 244, pp. 327–336.
- Ogiela, L.; Ogiela, M.R. *Advances in Cognitive Information Systems*; Cognitive Systems Monographs, Cosmos 17; Springer: Berlin/Heidelberg, Germany, 2012.
- Perconti, P.; Plebe, A. Deep learning and cognitive science. *Cognition* **2020**, *203*, 104365. [[CrossRef](#)] [[PubMed](#)]
- Zhang, H.; Liu, F.; Li, B.; Zhang, L.; Zhu, Y.; Wang, Z. Deep discriminative image feature learning for cross-modal semantics understanding. *Knowl.-Based Syst.* **2021**, *216*, 106812. [[CrossRef](#)]
- Li, S.; Chen, C.-H.; Lin, Z. Evaluating the impact of wait indicators on user visual imagery and speed perception in mobile application interfaces. *Int. J. Ind. Ergon.* **2022**, *88*, 103280. [[CrossRef](#)]
- Taylor, D.; Quick, S. Students’ perceptions of a near-peer Objective Structured Clinical Examination (OSCE) in medical imaging. *Radiography* **2020**, *26*, 42–48. [[CrossRef](#)] [[PubMed](#)]
- Sardar, M.K.; Adhikari, A. A new lossless secret color image sharing scheme with small shadow size. *J. Vis. Commun. Image Represent.* **2020**, *68*, 102768. [[CrossRef](#)]
- Ogiela, L.; Ogiela, M.R.; Ko, H. Intelligent data management and security in Cloud Computing. *Sensors* **2020**, *20*, 3458. [[CrossRef](#)] [[PubMed](#)]
- Wu, L.; Zhang, X.; Chen, H.; Wang, D.; Deng, J. VP-NIQE: An opinion-unaware visual perception natural image quality evaluator. *Neurocomputing* **2021**, *463*, 17–28. [[CrossRef](#)]
- Yu, S.; Wang, J.; Gu, J.; Jin, M.; Ma, Y.; Yang, L.; Li, J. A hybrid indicator for realistic blurred image quality assessment. *J. Vis. Commun. Image Represent.* **2023**, *94*, 103848. [[CrossRef](#)]

17. Rubio-Solis, A.; Panoutsos, G.; Beltran-Perez, C.; Martinez-Hernandez, U. A Multilayer Interval Type-2 Fuzzy Extreme Learning Machine for the recognition of walking activities and gait events using wearable sensors. *Neurocomputing* **2020**, *389*, 42–55. [[CrossRef](#)]
18. Rastgoo, R.; Kiani, K.; Escalera, S.; Sabokrou, M. Multi-modal zero-shot dynamic hand gesture recognition. *Expert Syst. Appl.* **2024**, *247*, 123349. [[CrossRef](#)]
19. Balaji, P.; Prusty, M.R. Multimodal fusion hierarchical self-attention network for dynamic hand gesture recognition. *J. Vis. Commun. Image Represent.* **2024**, *98*, 104019. [[CrossRef](#)]
20. Wang, Q.; Wu, Z. Structural System Reliability Analysis Based on Improved Explicit Connectivity BNs. *KSCE J. Civ. Eng.* **2018**, *22*, 916–927. [[CrossRef](#)]
21. Wang, Q.A.; Dai, Y.; Ma, Z.G.; Wang, J.F.; Lin, J.F.; Ni, Y.Q.; Ren, W.X.; Jiang, J.; Yang, X.; Yan, J.R. Towards high-precision data modeling of SHM measurements using an improved sparse Bayesian learning scheme with strong generalization ability. *Struct. Health Monit.* **2024**, *23*, 588–604. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.