Journal of New Media

Tech Science Press

DOI: 10.32604/jnm.2023.039962

Review

The Review of Secret Image Sharing

Yao Wan[1,2], Lingzhi Liao[1,2,*], Zhili Zhou[3], Hengfu Yang[4], Fei Peng[3] and Zhilin Huo[5]

[1]Engineering Research Center of Digital Forensics, Ministry of Education, Nanjing University of Information Science and Technology, Nanjing, 210044, China
[2]School of Software, Nanjing University of Information Science and Technology, Nanjing, 210044, China
[3]Institute of Artificial Intelligence and Blockchain, Guangzhou University, Guangzhou, 510006, Guangdong, China
[4]Department of Information Science and Engineering, Hunan First Normal University, Changsha, 410205, China
[5]CSSC Systems Engineering Research Institute, Beijing, China

*Corresponding Author: Lingzhi Liao. Email: lzliao@nuist.edu.cn

Received: 01 February 2023; Accepted: 07 March 2023; Published: 16 June 2023

Abstract: Secret image sharing (SIS) is a significant research topic of image information hiding, which divides the image into multiple shares and distributes them to multiple parties for management and preservation. In order to reconstruct the original image, a subset with predetermined number of shares is needed. And just because it is not necessary to use all of the shares to make a reconstruction, SIS creates a high *fault tolerance* which breaks the limitations of traditional image protection methods, but at the same time, it causes a reduce of safety. Recently, new technologies, such as deep learning and blockchain, have been applied into SIS to improve its *efficiency* and *security*. This paper gives an overall review of SIS, discusses four important approaches for SIS, and makes a comparison analysis among them from the perspectives of pixel expansion, tamper resistance, etc. At the end, this paper indicates the possible research directions of SIS in the future.

Keywords: Secret image sharing; blockchain; deep learning

1 Introduction

Secret image sharing (SIS) [1–3] is a type of information hiding technique that has gained attention in recent years. Unlike the traditional encryption techniques that use a single key to protect the data, SIS divides the secret image into multiple shares and distributes each share to different parties. To reconstruct the original image, a predetermined number of shares must be gathered from some of the parties, as shown in Fig. 1.

The predetermined number is regarded as a threshold value in the SIS scheme. If the number of gathered shares does not approach the threshold, the reconstruction cannot be done. Based on this, the traditional SIS is also called (k, n) threshold scheme [4,5], where k refers to the predetermined minimum threshold number, and n refers to the total number of generated shares $(0 < k \leq n)$.

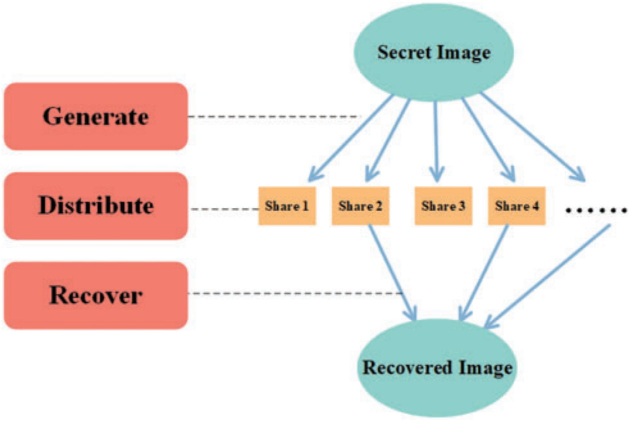

Figure 1: Secret image sharing scheme

The importance of SIS lies in its ability to provide a secure and robust method for image encryption and transmission. By distributing image shares among multiple parties, SIS can protect the secret image against unauthorized access, data loss, and other security threats. Additionally, SIS can be used to facilitate secure communication and collaboration, particularly in situations where sensitive or confidential information must be shared among multiple parties. One of the significant benefits of secret image sharing is its ability to provide fault-tolerance, where the loss or damage of some of the shares does not result in a total loss of the original image [6,7]. This feature makes it highly useful in applications such as remote backup, data storage, and transmission, where there is a high probability of data loss. However, this feature also causes the security issues in SIS. For example, it is possible that the participants who got the shares become as attackers. They can tamper the shares on their own and then make it impossible to reconstruct the original image correctly.

Recently, the development of deep learning and blockchain technology provides more ideas for SIS. Some researches [8–12] based on deep learning take advantage of neural networks to create image shares that are more secure and can get a higher quality of image reconstruction than the traditional SIS techniques. Some researches [13–17] based on blockchain technology store and distribute the image shares in a decentralized and secure manner, ensuring the integrity and confidentiality of the shares. These advancements in SIS have the potential to improve the efficiency and security of the existing techniques and expand the range of applications for SIS in various fields.

The remainder of this paper is organized as follows. Section 2 introduces for important SIS schemes. Section 3 analyzes the security issues of those schemes deeply and shows the recent advances and provides the possible future research directions of SIS. Finally, the conclusions part is presented in Section 4.

2 Variations of Secret Image Sharing

There are many variations of secret sharing. In this section, we review the procedure of various existing secret image sharing schemes including shamir’s secret sharing, visual cryptography, SIS based on deep learning, and SIS based on blockchain, respectively. And the comparison of the existing work is made at the end of this chapter.

2.1 Shamir's Secret Sharing

Shamir's secret sharing [18] is a method for dividing a secret into multiple parts, or shares, such that a certain number of the shares must be combined to reconstruct the secret. Shamir's method is based on polynomial interpolation, where the secret is treated as the constant term of a polynomial, and the shares are generated by computing the polynomial with different values. In order to reconstruct the secret, a predetermined number of shares can be used, but no information can be obtained from the subset which is smaller than the threshold value. Shamir's Secret Sharing is widely used for secret image sharing due to its simplicity, efficiency, and security.

In essence, instead of directly communicating the original secret data on the network, this scheme generates a set of random-like data, called as shares, from the given secret data, and then distributes them to the participants to ensure that each participant has single share. In this scheme, the elements of secret data are hidden into the constant coefficient of a $(k-1)$-degree polynomial $f(x)$. Then, someone can generate n shares by computing $f(x_i)$, where x_i is a real number $x_i \in [0, \mathrm{p}-1]$, and $i \in [1, n]$. After repeating the above process for every k elements of the secret data, n shares are generated and then sent to n corresponding participants on the networks. By Lagrange's interpolation algorithm, any k shares can jointly reconstruct the secret data, but no information of the secret can be revealed by $(k-1)$ or fewer shares. Therefore, this scheme can be deemed as a (k, n) threshold scheme. Thien et al. [1] extended Shamir's scheme for image data, and hided every k secret pixels into all the k coefficients of the polynomial. As a result, the sizes of shadows are decreased to $1/k$ of the original secret image.

Shamir's secret sharing scheme has attracted many researchers' attention. Gupta et al. [19] used the neural encryption protocol combined with the Shamir's scheme for the secure transmission of single image. They claim that their main focus is to share secret information through public channels with less computation power and try to extend this technique for multiple secret images. This combined scheme is suitable for many privacy image protection scenarios, such as medical image management in hospitals.

2.2 Visual Cryptography

Visual Cryptography (VC) [20–24] is a technique that uses the human visual system to reveal a secret image from a set of images that appears to be random noise. It was first developed by Naor et al. in 1995 [21]. Visual cryptography creates shares of an image by dividing it into a set of n shares, such that each share is a binary image with only two possible pixel values (black or white). When any two shares are overlaid, a random noise-like image is produced. However, when all the shares are superimposed, the original image is revealed. This is a simple and safe secret image sharing method for the decoding of secret images. However, since it can cause the problem of pixel expansion, several follow-up studies on VC were making efforts to reduce the pixel expansion and improve the reconstructed image quality [25–29].

Hou et al. [20] proposed an improved extended visual cryptography based on random grid (RG). In this scheme, the meaningful and noise-like shares can be generated. The production of meaningful share images can satisfy the requirements of being easy to carry and easy to manage, and then improve the visual quality of shares and recovered image.

Wu et al. [22] developed a visual secret sharing (VSS) based on RG for general access structures with the ability of cheat preventing. It is the first effort to share a secret with general access structures based on RG. In this scheme, the single secret image can be encrypted into n random grids while qualified sets can reconstruct it visually. This algorithm is more flexible than the other VSS scheme based on RG.

2.3 SIS Based on Deep Learning

Recent advancements in SIS have focused on improving its efficiency and security. One of the significant improvements is based on deep learning. It takes advantage of neural networks with deep learning to create image shares that are more secure and can get a higher quality of image reconstruction than the traditional SIS techniques.

In the deep learning based scheme, neural network is trained to generate shares of an input image such that any subset of shares less than a certain threshold value cannot reveal any information about the original image. The neural network's output is optimized to minimize the perceptual difference between the original image and the reconstructed one, which results in higher quality image reconstruction. Additionally, the application of deep learning can provide better security for SIS against certain types of attacks, such as statistical or machine learning attacks, as the network's parameters can be made secret.

Duan et al. [30] proposed an effective framework to verify in a distributed deep learning environment to reduce the computation and communication cost by following the secret file sharing algorithm. This scheme is an indirect approach to preserve the privacy of training datasets by allowing a participant to locally train and share parameters (gradients) of the locally trained model with a cloud server. Each participant aggregates all received gradients and upload to the cloud server in order to update the global parameters. With the cooperation of SIS, the approach can inject the verifiable data into the input so that the correctness of the returned inference results can be checked.

In 2020, Duan et al. [31] used CNN to embed secret data in image steganography. Before using discrete cosine transform (DCT) embedding, the secret data is preprocessed to improve the anti-detection performance of the steganography algorithm, and elliptic curve cryptography (ECC) is used to encrypt the transformed coefficients to provide additional security. This method has been applied to gray image and color image, and shows better security to the data.

2.4 SIS Based on Blockchain

Another recent development in SIS is the application of blockchain technology. Blockchain technology can be used to store and distribute the shares in a decentralized and secure manner, ensuring the integrity and confidentiality of the shares. The blockchain can also provide an audit trail of the image shares, which can be useful for tracking and monitoring the access to the shares. The combination of secret image sharing and blockchain technology can provide a robust and secure method for image sharing, with potential applications in fields such as healthcare, finance, and government.

Kripa et al. [13] proposed a blockchain framework for storing social media content using Interplanetary File System (IPFS), which is a decentralized file storage system. The secret sharing scheme is applied to the content to be uploaded to IPFS, and combined with the robust hash of the image, it can resist various attacks. However, García et al. [32] believed that this solution does not provide the further details about these smart contracts, nor does it provide a negotiation method for the terms of reuse.

In summary, the integration of blockchain technology can be used for decentralized and secure storage and distribution of the shares. These advancements in secret image sharing have the potential to improve the efficiency and security of the existing techniques and expand the range of applications for secret image sharing in various fields. However, there is still a potential trade-off between how to integrate the consensus mechanism and smart contracts of the blockchain to ensure that image reconstruction can be completed by meeting the pre-set number of participants.

2.5 Comparison of Existing Work

Here we select some of the most interesting features in secret image sharing schemes for comparison, such as the pixel expansion, the need of trusted third-party and codebook, and the tamper resistance.

In the applications of secret image sharing, the pixel expansion is a phenomenon where the size of a pixel exceeds its original size. This is usually caused by a lack of resolution in the image or a misalignment of the pixels. Pixel expansion results in reduced image quality and blurred image details. This may be an important issue when sharing sensitive information because the details of the image may become unrecognizable. In addition, pixel expansion can cause color shifts and destruction in the image, resulting in a destroyed or inaccurate representation of the original image. For the need of trusted third-party and codebook, they are the additional requirements of secret sharing schemes, which will increase the communication and storage costs of the secret sharing system. The tamper resistance has been considered to evaluate the performance of these schemes. Tamper-proof refers to whether these systems provide methods to protect shares, rather than ignoring the security of shares. The results of the comparison among four representative SIS schemes are given in Table 1.

Table 1: Comparison of the different secret image sharing schemes

Schemes	Techniques	Pixel expansion	Trusted third-party needed	Codebook needed	Tamper resistance
Shamir's	Secret sharing	Yes	Yes	Yes	No
Hou's	Visual cryptography	No	No	No	No
SSDDL	Deep learning	No	Yes	Yes	No
Kripa's	Blockchain	No	No	No	Yes

Since the shares generated by the SIS scheme can be used to restore the original image, most existing works generally assume that the shares are stored in a secure environment and that the number of shares in this part is set to less than k , which is the threshold value, even if some of them are leaked. Few existing works consider security analysis in a semi-honest environment. Over-idealized security assumptions do pose a security risk to secret image sharing algorithms in real-world scenarios, because the share is indeed a vulnerable target for attackers throughout the system.

In terms of functional comparison, each existing work has its advantages and disadvantages. Shamir's scheme [18] provides an efficient and fault-tolerant idea in the early stage of research, but the disadvantage is that participants may steal or tamper with the original secret image through collusion. For the traditional visual cryptography scheme that does not require cryptographic computation, this scheme is faster and more effective, but it has the problem of pixel expansion. The SSDDL scheme [30] combined with deep learning can deal with conspiracy attacks in a semi-honest environment, effectively protect the data stored in the cloud server and ensure the security of the data. However, most of the existing schemes do not pay attention to the protection of sharing, which makes these images easy to be tampered with and leads to recovery failure. Fortunately, the secret image sharing scheme combined with blockchain can solve this problem. Kripa et al. [13] have introduced a decentralized secure storage environment, so that the share stored in the interstellar file system will not be maliciously tampered with, because blockchain technology provides audit and tracking for the share. Because of the fault-tolerance of SIS, researchers mostly ignored the security risk of sharing. Protecting these shares can effectively improve the tamper resistance of SIS, as proved in the schemes based on blockchain.

In summary, while secret image sharing provides a secure way to share images, it is important to recognize potential vulnerabilities and take measures to mitigate them. By using the trusted third party, implementing more powerful algorithms and data protection technologies, and using secure communication protocols, the risk of attack can be reduced and the security of shared images can be improved.

3 Analysis of SIS

3.1 Security Issues

The common security issues with secret image sharing mainly focus on three aspects, including conspiracy attacks with unauthorized access, data leakage, and malicious attacks.

One of the major security issues associated with the SIS is unauthorized access to the shares. This may be due to the weak encryption algorithms, poor access control, or other vulnerabilities in the system. Most of the SIS schemes rely on the trusted third parties to control the sharing process. If the access is not strictly controlled, the authorized users can intentionally or unintentionally break the confidentiality of shares. To address this problem, the SIS systems should have strict access control, restricting access to data to individuals who need it. Block chains with the characteristics of decentralization have been shown to be an effective way to resolve this internal attack.

Although secret image sharing technology provides a way to share images securely, there are still some vulnerabilities that can be exploited by attackers. Secret image sharing systems are also prone to data leaks, which can occur when data is transmitted over an insecure network or stored on an insecure device. To address this problem, the secret image sharing systems should use secure networks such as Virtual Private Network (VPN) or other encrypted connections. Devices used to access shared data should also be secure and should have the latest anti-virus and anti-malware installed. In addition to encrypting data, using techniques such as steganography to disguise the data as something less noticeable is also one of the ways to protect the data from disclosure.

The SIS systems are also vulnerable to various types of malicious attacks, such as the statistical attack, the computational attack, and the forgery attacks, which can compromise the confidentiality and authenticity of shares. In order to defend these attacks, researchers have provided many ideas and alternative solutions. Generating shares randomly and evenly so that there is no correlation between shares and the original image is an effective way to avoid being attacked by the statistics attack. The independent shares and unrelated to the original image prevent statistical attacks from obtaining information about confidential images. Another potential vulnerability is the use of computational attacks to guess secrets. This violent attack can be solved by using larger key sizes and more complex algorithms, making it harder for attackers to guess secrets. The purpose of a forgery attack is to create a false share that appears to be a real share, where an attacker can create a false share to deceive participants. To prevent forgery attacks, share should be generated using a secure random process that is not easy to copy, or a technique such as watermarking should be used to make share verifiable. In addition, the firewalls and intrusion detection systems can help prevent and detect attacks.

3.2 Recent Advances

Recently, more and more researchers have paid attention to the potential of secret image sharing in protecting sensitive information, distributing confidential documents and securing multimedia data. In these studies, the multi-level secret image sharing has been widely discussed because of its more efficient, secure and universal characteristics [33–35]. The multi-level SIS scheme can improve the security and efficiency of the sharing process by dividing the secret into multiple levels (each level has different access requirements). For example, the first level may require only one participant to reconstruct the image, while the second level may require three or more participants. This allows a higher level of control over participants who has access to the secret image. Compared with traditional cryptography schemes, multi-level secret sharing does not require additional distribution and storage of keys. At the same time, with the deepening of research, the computational complexity of this scheme is being reduced.

3.3 Future Research Directions

On the other hand, with the continuous development of deep learning, introducing neural network into secret image sharing to learn how to encode and decode images is also one of the recent research advances. The use of neural network allows a high degree of security and robustness, so that the image can resist attacks such as cutting, scaling and rotation. The secret image sharing technology based on deep learning also has the advantage of high hiding capacity, which means that more information can be hidden in the image without reducing the image quality.

Future research on secret image sharing can help solve existing limitations and challenges, including improving security and confidentiality, enhancing the efficiency and flexibility of sharing, and the ability to share large amounts of data safely. With the explosive growth of multimedia data, protecting the security of sensitive personal information and improving efficiency and flexibility are bound to be the main research directions in the future. On the other hand, improving the practicability of the secret image sharing scheme in real scenes, like blockchain, making secret image sharing systems more intuitive and easier to use, is also one of the optimization directions of these systems.

4 Conclusion

In conclusion, the SIS is a promising field that has the potential to enable secure and robust transmission of confidential images. This paper has provided an overview of the different techniques in secret image sharing, including Shamir's secret sharing, visual cryptography, SIS based on deep learning, and SIS based on blockchain. Some of the main security issues in secret image sharing have been discussed, such as conspiracy attacks, the leakage of data, and malicious attacks. Based on these analysis, some potential future research directions in SIS are indicated, including the multi-modal secret image sharing, the secure and robust secret image sharing based on deep learning, and SIS with enhancing efficiency, flexibility and practicality.

Overall, the techniques and approaches discussed in this paper have shown that secret image sharing can be achieved with high levels of security, privacy, and robustness, and can be adapted to different application scenarios. However, the field of secret image sharing is still evolving, and there is a need for further research to address the remaining challenges and explore new possibilities. This paper will serve as a useful reference for researchers and practitioners who are interested in this field, and will contribute to the advancement of secret image sharing and its applications.

Acknowledgement: Thanks to the teacher and students of my team for their guidance in the process of completing this article. We gratefully acknowledge the support of Engineering Research Center of Digital Forensics for providing us the RTX3090 GPU which was used in this research.

Funding Statement: This work is supported in part by the National Natural Science Foundation of China under Grant 61972205, Grant U1936218, in part by the Guangdong Natural Science Funds for Distinguished Young Scholar, in part by CSSC Systems Engineering Research Institute (Grant No. 193-A11-107-01-33), in part by Science and Technology Planning Project of Changsha (No. kq2004004), and in part by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) fund, China.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] C. -C. Thien and J. -C. Lin, "Secret image sharing," *Computers & Graphics*, vol. 26, no. 5, pp. 765–770, 2002.

[2] F. Xing, X. Yan, L. Yu and L. Li, "A novel general (n, n)-threshold multiple secret images sharing scheme based on information hiding in the sharing domain," *Entropy*, vol. 24, no. 3, pp. 318, 2022.

[3] X. Yan, S. Wang, A. A. Abd El-Latif and X. Niu, "New approaches for efficient information hiding-based secret image sharing schemes," *Signal, Image and Video Processing*, vol. 9, no. 3, pp. 499–510, 2015.

[4] O. B. Chanu and A. Neelima, "A survey paper on secret image sharing schemes," *International Journal of Multimedia Information Retrieval*, vol. 8, no. 4, pp. 195–215, 2019.

[5] J. Kurihara, S. Kiyomoto, K. Fukushima and T. Tanaka, "A new (k, n)-threshold secret sharing scheme and its extension," in *Information Security: 11th Int. Conf., ISC 2008*, September 15–18, 2008. Proceedings 11, Taipei, Taiwan, pp. 455–470, 2008.

[6] W. -P. Fang, "Multi-layer progressive secret image sharing," in *Proc. of the 7th WSEAS Int. Conf. on Signal Processing, Computational Geometry & Artificial Vision*, Istanbul, Turkey, pp. 112–116, 2007.

[7] A. Nag, S. Biswas, D. Sarkar and P. P. Sarka, "Secret image sharing scheme based on a boolean operation," *Cybernetics and Information Technologies*, vol. 14, no. 2, pp. 98–113, 2014.

[8] A. F. S. Devaraj, G. Murugaboopathi, M. Elhoseny, K. Shankar, K. Min *et al.,* "An efficient framework for secure image archival and retrieval system using multiple secret share creation scheme," *IEEE Access*, vol. 8, pp. 144310–144320, 2020.

[9] Y. Dong, X. Chen, L. Shen and D. Wang, "Privacy-preserving distributed machine learning based on secret sharing," in *Information and Communications Security: 21st Int. Conf., ICICS 2019*, December 15–17, 2019, Revised Selected Papers 21, Beijing, China, Springer International Publishing, pp. 684–702, 2020.

[10] J. Duan, J. Zhou, Y. Li and C. Huang, "Privacy-preserving and verifiable deep learning inference based on secret sharing," *Neurocomputing*, vol. 483, pp. 221–234, 2022.

[11] X. Wang, H. Shan, X. Yan, L. Yu and Y. Yu, "A neural network model secret-sharing scheme with multiple weights for progressive recovery," *Mathematics*, vol. 10, no. 13, pp. 2231, 2022.

[12] F. Zheng, C. Chen, X. Zheng and M. Zhu, "Towards secure and practical machine learning via secret sharing and random permutation," *Knowledge-Based Systems*, vol. 245, pp. 108609, 2022.

[13] M. Kripa, A. Nidhin Mahesh, R. Ramaguru and P. Amritha, "Blockchain framework for social media DRM based on secret sharing," in *Information and Communication Technology for Intelligent Systems: Proceedings of ICTIS 2020*, vol. 1, Singapore: Springer, pp. 451–458, 2021.

[14] M. P. McBee and C. Wilcox, "Blockchain technology: Principles and applications in medical imaging," *Journal of Digital Imaging*, vol. 33, pp. 726–734, 2020.

[15] R. Nowrozy, A. Kayes, P. A. Watters, M. Alazab, A. Ng *et al.,* "A blockchain-based secure data sharing framework for healthcare," in *Blockchain for Cybersecurity and Privacy*, Boca Raton, Florida, USA: CRC Press, pp. 219–241, 2020.

[16] M. Sultana, A. Hossain, F. Laila, K. A. Taher and M. N. Islam, "Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology," *BMC Medical Informatics and Decision Making*, vol. 20, no. 1, pp. 1–10, 2020.

[17] T. Veeramakali, R. Siva, B. Sivakumar, P. Senthil Mahesh and N. Krishnaraj, "An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model," *The Journal of Supercomputing*, vol. 77, pp. 1–21, 2021.

[18] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[19] M. Gupta, M. Gupta and M. Deshmukh, "Single secret image sharing scheme using neural cryptography," *Multimedia Tools and Applications*, vol. 79, pp. 12183–12204, 2020.

[20] Y. -C. Hou, S. -C. Wei and C. -Y. Lin, "Random-grid-based visual cryptography schemes," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 24, no. 5, pp. 733–744, 2013.

[21] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology—EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques Perugia*, May 9–12, 1994 Proceedings 13, Italy, Berlin Heidelberg, Springer, pp. 1–12, 1995.

[22] X. Wu and W. Sun, "Random grid-based visual secret sharing for general access structures with cheat-preventing ability," *Journal of Systems and Software*, vol. 85, no. 5, pp. 1119–1134, 2012.

[23] X. Jia, D. Wang, D. Nie and C. Zhang, "Collaborative visual cryptography schemes," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 5, pp. 1056–1070, 2016.

[24] K. -S. Lin, C. -H. Lin and T. -H. Chen, "Distortionless visual multi-secret sharing based on random grid," *Information Sciences*, vol. 288, pp. 330–346, 2014.

[25] C. Blundo, S. Cimato and A. De Santis, "Visual cryptography schemes with optimal pixel expansion," *Theoretical Computer Science*, vol. 369, no. 1–3, pp. 169–182, 2006.

[26] D. Jin, W. -Q. Yan and M. S. Kankanhalli, "Progressive color visual cryptography," *Journal of Electronic Imaging*, vol. 14, no. 3, pp. 033019–033019-13, 2005.

[27] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," *Journal of WSCG*, vol. 10, no. 2, pp. 303–310, 2002.

[28] S. J. Shyu and M. C. Chen, "Minimizing pixel expansion in visual cryptographic scheme for general access structures," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 25, no. 9, pp. 1557–1561, 2015.

[29] Z. Wang, G. R. Arce and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 383–396, 2009.

[30] J. Duan, J. Zhou and Y. Li, "Privacy-preserving distributed deep learning based on secret sharing," *Information Sciences*, vol. 527, pp. 108–127, 2020.

[31] X. Duan, D. Guo, N. Liu, B. Li, M. Gou *et al.,* "A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network," *IEEE Access*, vol. 8, pp. 25777–25788, 2020.

[32] R. García, A. Cediel, M. Teixidó and R. Gil, "Semantics and non-fungible tokens for copyright management on the metaverse and beyond," arXiv preprint arXiv:2208.14174, 2022.

[33] S. Beugnon, P. Puteaux and W. Puech, "Privacy protection for social media based on a hierarchical secret image sharing scheme," in *2019 IEEE Int. Conf. on Image Processing (ICIP)*, Taipei, Taiwan, IEEE, pp. 679–683, 2019.

[34] C. -C. Lee, H. -H. Chen, H. -T. Liu, G. -W. Chen and C. -S. Tsai, "A new visual cryptography with multi-level encoding," *Journal of Visual Languages & Computing*, vol. 25, no. 3, pp. 243–250, 2014.

[35] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho and S. W. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," *Multimedia Tools and Applications*, vol. 75, pp. 14867–14893, 2016.