engineering proceedings

MDPI

Proceeding Paper

Polarization-Based (*f*,*k*,*n*)-Threshold Two-Level Visual Secret Sharing Scheme †

Wilson Tsai-Wei Chuang, Justie Su-Tzu Juan * and Wen-Ting Lee

Department of Computer Science & Information Engineering, National Chi Nan University, Nantou 54561, Taiwan; s111321028@mail1.ncnu.edu.tw (W.T.-W.C.); s112321541@ncnu.edu.tw (W.-T.L.)

* Correspondence: jsjuan@ncnu.edu.tw

† Presented at 8th International Conference on Knowledge Innovation and Invention 2025 (ICKII 2025), Fukuoka, Japan, 22–24 August 2025.

Abstract

With the advancement of technology, increasing attention has been focused on the development of encryption techniques. Visual secret sharing (VSS), also known as visual cryptography (VC), is used to encrypt a secret image into multiple share images, which can be stacked together to visually reconstruct the secret without complex computations. Decryption in traditional VSS schemes is equivalent to performing logical OR operations. In 2023, a novel (*k*,*n*)-threshold VSS based on polarization (P-VSS) scheme was proposed. This scheme utilizes the physical property that two orthogonal polarizers block light transmission to simulate a better VSS. A minimum of *k* shares is required to successfully reveal the original secret. In this study, we further propose a (*f*,*k*,*n*) dual-threshold P-VSS scheme. The proposed polarization-based scheme introduces two distinct reconstruction thresholds. When *f* or more shares are stacked, a fake secret image is revealed to mislead potential attackers. Only when *k* or more shares are combined can the true secret image be successfully recovered. This dual-threshold design significantly enhances the security of visual secret sharing by increasing the confusion for potential attackers and improving resistance against information leakage.

Keywords: visual secret sharing; visual cryptography; polarization-based; dual-threshold scheme; fake secret

check for updates

Academic Editors: Teen-Hang Meen, Chun-Yen Chang and Cheng-Fu Yang

Published: 11 February 2026

Citation: Chuang, W.T.-W.; Juan, J.S.-T.; Lee, W.-T. Polarization-Based (*f*,*k*,*n*)-Threshold Two-Level Visual Secret Sharing Scheme. *Eng. Proc.* **2025**, *120*, 60. https://doi.org/10.3390/engproc2025120060

Copyright: © 2026 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

Visual secret sharing (VSS), first introduced by Naor and Shamir [1], is a cryptographic primitive that enables secret image reconstruction without complex computation by encoding the secret into multiple shares. When stacked, these shares visually reveal the secret. The traditional (*k*,*n*)-threshold VSS requires any *k* out of *n* shares to reconstruct the secret, while fewer than *k* shares reveal nothing. Early VSS schemes suffered from pixel expansion, which was later addressed through methods such as random grids (RG-based) [2]. To address practical limitations, research has explored alternative physical properties for encoding secrets. Notably, Biham and Itzkovitz [3] proposed a polarization-based VSS leveraging light polarization, where aligned polarizers transmit light (white) and orthogonal polarizers block it (black), analogous to a logical XOR for two shares. However, this model fails for more than two stacked polarizers, as physical results deviate from XOR predictions. Huang and Juan [4] addressed this by introducing polarization-based VSS (P-VSS), modeling each polarizer as an ordered binary pair (*a*,*b*), where (1,1) blocks

light (black) and other combinations allow light (white). Stacking corresponds to a logical OR operation on the pairs, while light transmission follows logical AND on the resulting pair. This model aligns better with physical behavior, supports a (t,n)-threshold VSS scheme without pixel expansion, and improves image visibility and contrast, particularly in (2,n) schemes.

Inspired by these advances, this paper gives a new (k,n)-threshold P-VSS (named new (k,n) P-VSS), which improves the result of [4]. In addition, a polarization-based (f,k,n) interval threshold visual secret sharing (named (f,k,n) P-IVSS) scheme has been presented, in which the secret image can only be revealed when staking at least f, but no more than $k-1$ shares. Then, we propose a novel polarization-based (f,k,n)-threshold two-level visual secret sharing scheme (named (f,k,n) P-2VSS) using these two new P-VSSs. On the other hand, it can also be considered as a VSS that can restore two different images. When fewer shares are collected, one of the less important secret images can be restored, and when more shares are collected, the other, more important, secret image can be restored. Therefore, this method increases the practicality and applicability of VSS.

2. Preliminaries

The essential tools that are used to evaluate the visual quality of outputs generated by visual cryptography algorithms are introduced in Section 2.1. Next, we introduce the (k,n) P-VSS scheme proposed by Huang and Juan [4]. This method designs four types of polarizers and, by leveraging the concept from Ref. [1], presents a visual secret sharing scheme with significantly improved contrast compared to traditional approaches.

2.1. Definition

Traditionally, *contrast* (α) is commonly used to assess the visibility of reconstructed images and to evaluate the effectiveness of VSS schemes in revealing secret information [5]. The calculation of contrast is based on the difference in optical transmittance between reconstructed white and black regions. For a given image C, the *light transmission* $T(C)$ is defined as the ratio of the number of transparent (white) pixels to the total number of pixels in C. Specifically, let $T_1 = T(C(S(1)))$ denote the light transmission of the regions in image C that correspond to black areas in the original secret image S, and let $T_0 = T(C(S(0)))$ denote the light transmission of the regions in C corresponding to white areas in S. The definition of the contrast (α) of a reconstructed image C is as follows.

$$\alpha = (T_0 - T_1)/(1 + T_1) \tag{1}$$

The theoretical value of contrast ranges between -1 and 1. A value approaching 1 suggests a high-quality reconstruction in which the secret can be easily recognized, whereas a value of 0 indicates a completely disordered image with no discernible information. In traditional RG-based VSS schemes, shares are generated and stacked using random patterns, resulting in a maximum reconstructed image brightness of only one-fourth of the original image. This limitation adversely affects the visual clarity of the recovered secret.

To address this issue, Huang and Juan [4] proposed a novel interpretation for visual secret sharing based on light polarization, named P-VSS, that increases the reconstructed image brightness to seven-sixteenths. This approach adopts ordered binary pairs to represent polarizer directions, allowing stacking operations to better simulate the behavior of light transmission. There are four types of pixel polarizers: (0, 0), (0, 1), (1, 0), and (1, 1). The (1, 0) type corresponds to a horizontal polarizer, the (0, 1) type corresponds to a vertical polarizer, and the (1, 1) type completely blocks light, resulting in a black output. The remaining types allow light to pass through, appearing white. Figure 1 is a schematic diagram of the four styles. The light transmission through a single polarizer

can be represented by the logical AND operation on its binary components. When two polarizers are stacked, the resulting configuration is obtained by applying a logical OR operation component-wise to the individual polarizers.

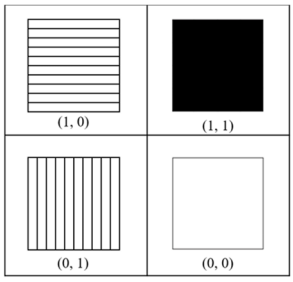


Figure 1. Four types of pixel polarizers [4]. The (1, 0) type: a horizontal polarizer, (0, 1) type: a vertical polarizer, the (1, 1) type: a black glass, and (0, 0) type: a transparent glass.

In this study, we adopt the (0, 1) and (1, 0) polarizer types, which effectively improve the contrast of the reconstructed image to approximately 1/2.

2.2. Related Algorithms

Huang and Juan [4] proposed a (k,n)-threshold P-VSS in 2023. This approach uses ordered binary pairs to represent polarizer directions. When light passes through a stack of two polarizers—one of type (a, b) and the other of type (c, d)—the effect is equivalent to light passing through a single polarizer of type $(a \otimes c, b \otimes d)$, where $\otimes$ denotes the logical OR operation. In the following, $\oplus$ denotes the logical XOR operation, and $(a, b) \oplus (c, d) = (a \oplus c, b \oplus d)$. Algorithm 1 shows the (k,n) P-VSS [4].

Algorithm 1. (k,n) P-VSS [4]

Input:	A $w \times h$ binary secret image S, the threshold parameters (k,n).
Output:	n shares $G_1, \ldots, G_n$.
Step 1.	For each position $(i, j) \in \{(i, j) \mid 1 \leq i \leq w, 1 \leq j \leq h\}$, repeat Steps 2–7.
Step 2.	If $S[i, j] = 0$, then $s = (0, 0)$; else $s = (1, 1)$.
Step 3.	Randomly generate g_1 as (0, 1) or (1, 0)
Step 4.	Randomly generate $g_2, g_3, \ldots, g_{k-1}$ as (0, 0), (1, 0), (0, 1), (1, 1).
Step 5.	$g_k = s \oplus g_1 \oplus g_2 \cdots \oplus g_{k-1}$.
Step 6.	$g_{k+1} = g_1, g_{k+2} = g_2, \ldots, g_{2k} = g_k, g_{2k+1} = g_1, \ldots$, if $n \bmod k = 0$, $g_n = g_k$; else $g_n = g_{(n \bmod k)}$.
Step 7.	Randomly rearrange $g_1, g_2, \ldots, g_n$ to $G_1[i, j], G_2[i, j], \ldots, G_n[i, j]$.
Step 8.	Output the n shares $G_1, G_2, \ldots, G_n$.

3. Result and Discussion

This section outlines the share generation procedure of the proposed P-2VSS scheme. Section 3.1 introduces the basic idea of the three core algorithms. Section 3.2 details the construction steps of these three algorithms, including polarizer initialization, logical operations, and share rearrangement. Section 3.3 presents the experimental results and quantitative analysis, highlighting the visual effects and performance of the scheme under different stacking scenarios.

3.1. Algorithm Functions

The proposed P-2VSS scheme integrates three key algorithms that collectively support its dual-threshold design and visual security properties.

1. The first algorithm is designed to generate share patterns corresponding to a fake secret. When $f \leq t < k$ shares are stacked, the reconstruction reveals a misleading image to unauthorized users. When stacking more than $k - 1$ shares, it becomes a completely black image. This scheme is the (f,k,n) interval threshold P-VSS ((f,k,n) P-IVSS for short)

scheme. This mechanism provides a decoy effect to enhance information hiding and defense against partial collusion attacks.

2. The second algorithm is an enhanced version of Algorithm 1 [4], which improves the contrast of the restored image. This algorithm constructs a sharing mode that supports reconstruction of the true secret only when $t \geq k$. It ensures that no meaningful information about the true secret can be derived from fewer than k shares.
3. The third algorithm introduces a pixel-wise randomization strategy. For each pixel, the algorithm randomly decides whether to apply the first or second algorithm during encoding. This random selection increases the unpredictability of the share generation process and strengthens the scheme's resistance to reverse engineering or statistical analysis.

The three algorithms form the computational foundation of the P-2VSS scheme, enabling it to satisfy the (f,k,n)-threshold requirement while embedding both fake and true secrets in a secure and visually meaningful way.

3.2. Share Construction Procedure

As explained in the previous subsection, Algorithm 2 generates a fake secret to mislead unauthorized users, Algorithm 3 is a new (k,n)-threshold P-VSS scheme, which reconstructs the true secret when the threshold is met, and Algorithm 4 randomly selects between the two on a per-pixel basis to enhance security. Each share generation method includes random initialization of polarizers, calculation of logical operations, and random rearrangement of shared pixels to securely encode the dual-threshold secrets.

Algorithm 2. (f,k,n) P-IVSS

Input: A $w \times h$ binary secret image S, the threshold parameters (f,k,n) for $1 < f < k \leq n$.
Output: n shares $G_1, \ldots, G_n$.
Step 1. For each position $(i, j) \in \{(i, j) \mid 1 \leq i \leq w, 1 \leq j \leq h\}$, repeat Steps 2–7.
Step 2. If $S[i, j] = 0$, then $s = (0, 0)$; else $s = (1, 1)$.
Step 3. Randomly generate $g_1, g_2, \ldots, g_{f-1}$ as (0, 1), (1, 0).
Step 4. $g_f = s \oplus g_1 \oplus g_2 \ldots \oplus g_{f-1}$.
Step 5. $g_{f+1} = g_1$, $g_{f+2} = g_2, \ldots, g_{2f} = g_f, g_{2f+1} = g_1, \ldots$, if $(k-1) \bmod f = 0$, $g_{k-1} = g_f$; else $g_{k-1} = g_{(k-1 \bmod f)}$.
Step 6. For i from k to n, $g_i = (1, 1)$.
Step 7. Randomly rearrange $g_1, g_2, \ldots, g_n$ to $G_1[i, j], G_2[i, j], \ldots, G_n[i, j]$.
Step 8. Output the n shares $G_1, G_2, \ldots, G_n$.

Algorithm 3. New (k,n) P-VSS for $k > 2$

Input: A $w \times h$ binary secret image S, the threshold parameters (k,n) for $1 < k \leq n$.
Output: n shares $G_1, \ldots, G_n$.
Step 1. For each position $(i, j) \in \{(i, j) \mid 1 \leq i \leq w, 1 \leq j \leq h\}$, repeat Steps 2–6.
Step 2. If $S[i, j] = 0$, then $s = (0, 0)$; else $s = (1, 1)$.
Step 3. Randomly generate $g_1, g_2, \ldots, g_{k-1}$ as (0, 1), (1, 0).
Step 4. $g_k = s \oplus g_1 \oplus g_2 \ldots \oplus g_{k-1}$.
Step 5. $g_{k+1} = g_1, g_{k+2} = g_2, \ldots, g_{2k} = g_k, g_{2k+1} = g_1, \ldots$, if $(n \bmod k) = 0$, $g_n = g_k$; else $g_n = g_{(n \bmod k)}$.
Step 6. Randomly rearrange $g_1, g_2, \ldots, g_n$ to $G_1[i, j], G_2[i, j], \ldots, G_n[i, j]$.
Step 7. Output the n shares $G_1, G_2, \ldots, G_n$.

Algorithm 4. (f,k,n) P-2VSS

Input: A $w \times h$ binary secret image S, the threshold parameters (f,k,n) for $1 < f < k \leq n$.
Output: n shares $G_1, \ldots, G_n$.
Step 1. For each position $(i, j) \in \{(i, j) \mid 1 \leq i \leq w, 1 \leq j \leq h\}$, repeat Step 2–3.
Step 2. Randomly select a value num $\in \{0, 1\}$.
Step 3. If (num = 0), generate the corresponding share pixels according to Steps 2–7 of Algorithm 2; else (num = 1), generate them according to Steps 2–6 of Algorithm 3.
Step 4. Output the n shares $G_1, G_2, \ldots, G_n$.

3.3. Visual Results and Data Analysis

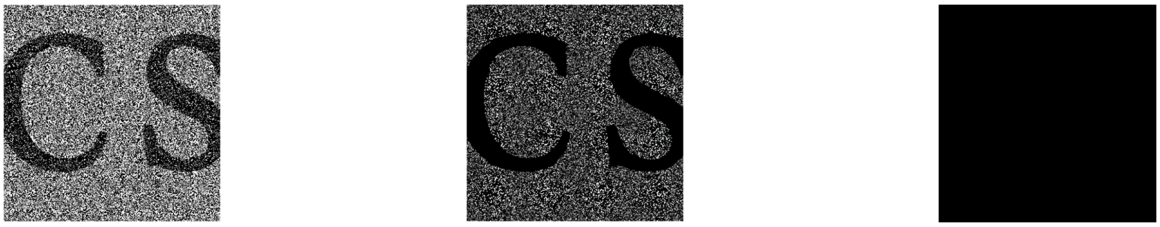
This subsection presents the experimental results of the proposed P-2VSS scheme obtained by stacking shares and provides quantitative analysis using metrics such as light transmission and contrast. The evaluation assesses the scheme's performance in distinguishing fake and true secrets under varying stacking conditions.

3.3.1. Experimental Results of (2, 4, 4) P-IVSS

The secret image used in this experiment, shown in Figure 2, has a resolution of 1000 × 1000 pixels. Figure 3 presents the results of stacking different numbers of shares under the (2, 4, 4) P-IVSS scheme, while Table 1 summarizes the corresponding light transmission and contrast values. As the number of stacked shares increases, the visual quality of the recovered image improves. The secret is completely revealed when three shares are stacked. However, stacking four shares results in a fully black image, demonstrating the threshold behavior and information protection capability of the proposed scheme.



Figure 2. Secret image 1.



(**a**) (**b**) (**c**)

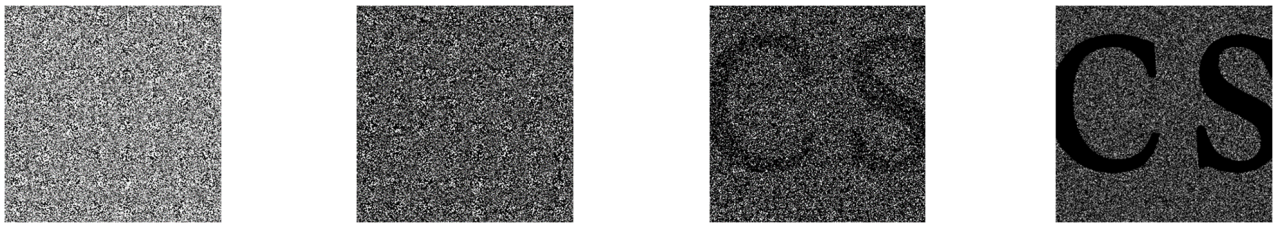
Figure 3. Experimental results of (2, 4, 4) P-IVSS: (**a**) stacking two shares; (**b**) stacking three shares; (**c**) stacking four shares.

Table 1. Experimental results of (2, 4, 4) P-IVSS. Number of stacked shares is t.

	$t = 1$	$t = 2$	$t = 3$	$t = 4$
α	0.0000	0.2857	0.2500	0.0000
T_0	0.7500	0.5000	0.2500	0.0000
T_1	0.7500	0.1667	0.0000	0.0000

3.3.2. Experimental Results of New (4, 5) P-VSS

Figure 4 illustrates the reconstruction results under the (4, 5)-threshold, also using Figure 2 as the secret image. Table 2 provides the corresponding light transmission and contrast values. As the number of stacked shares increases, the clarity of the recovered image gradually improves, and when four shares are merged, the black part is completely reconstructed. Since only (1, 0) and (0, 1) types of polarizers are used (when k is even), all individual shares appear completely white, with no black pixels.



(**a**) (**b**) (**c**) (**d**)

Figure 4. Experimental results of new (4, 5) P-VSS: (**a**) stacking two shares; (**b**) stacking three shares; (**c**) stacking four shares; (**d**) stacking five shares.

Table 2. Experimental results of new (4, 5) P-VSS. Number of stacked shares is t.

	$t = 1$	$t = 2$	$t = 3$	$t = 4$	$t = 5$
α	0	−0.0001	0.0002	0.0867	0.2495
T_0	1	0.5497	0.5000	0.2495	0.2495
T_1	1	0.5499	0.1667	0.2495	0.0000

3.3.3. Experimental Results of (2, 3, 4) P-2VSS

In this experiment, Figure 2 serves as the fake (decoy) secret and Figure 5 as the true secret. Figure 6 illustrates the reconstruction results of the experiment for (2, 3, 4) P-2VSS. When f or more shares are stacked, only the decoy is revealed; when k or more shares are combined ($k > f$), the true secret is recovered while the fake image becomes hidden. This confirms the dual-threshold property of the proposed scheme.

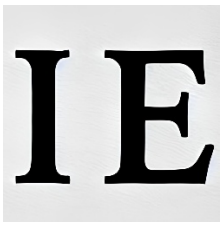
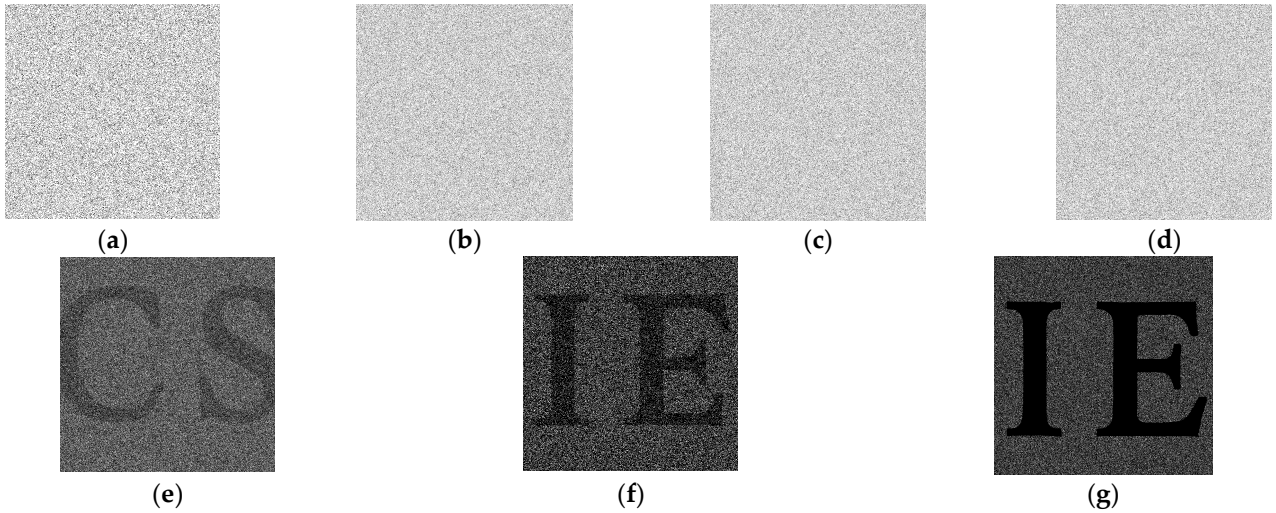


Figure 5. Secret image 2.



(**a**) (**b**) (**c**) (**d**)

(**e**) (**f**) (**g**)

Figure 6. Experimental results of (2, 3, 4) P-2VSS: (**a**–**d**) shares; (**e**) stacking two shares; (**f**) stacking three shares; (**g**) stacking four shares.

Table 3 shows the contrast values for the true and fake secret.

Table 3. Experimental results of (2, 3, 4) P-2VSS. Number of stacked shares is t.

		$t = 1$	$t = 2$	$t = 3$	$t = 4$
α	(Fake)	0.0002	0.0652	−0.0084	−0.0178
	(True)	0.0001	−0.0054	0.1109	0.2496

4. Conclusions

We propose an innovative (f,k,n) dual-threshold polarization-based visual secret sharing scheme (P-2VSS), which integrates the physical properties of light polarization with a logical binary pair representation. The proposed scheme reveals secret images at different levels according to the number of stacked shares. Experimental results demonstrate that when f or more shares are stacked, only a fake secret image is revealed, effectively misleading unauthorized observers. When k or more shares are stacked, the true secret image can be accurately reconstructed, thereby ensuring information security and enhancing the level of confidentiality. Compared to traditional single-threshold schemes, this dual-threshold approach exhibits superior resistance to attacks and provides a stronger misleading capability.

However, the proposed scheme still faces certain challenges. Specifically, as the number of stacked shares increases, the reconstructed fake image tends to become excessively dark, which may reduce the visibility of the fake secret and consequently diminish its ability to confuse potential attackers. Future research may focus on addressing these issues by improving the contrast of the reconstructed images, reducing storage requirements. These enhancements would further broaden the applicability of the proposed scheme in practical domains such as medical image protection, communication, and confidential document sharing.

Author Contributions: Conceptualization, W.T.-W.C.; methodology, W.T.-W.C. and J.S.-T.J.; software, W.T.-W.C.; validation, J.S.-T.J. and W.-T.L.; formal analysis, W.T.-W.C. and J.S.-T.J.; investigation, J.S.-T.J.; resources, W.T.-W.C.; data curation, W.T.-W.C.; writing—original draft preparation, W.T.-W.C.; writing—review and editing, J.S.-T.J. and W.-T.L.; visualization, W.T.-W.C.; supervision, J.S.-T.J.; project administration, J.S.-T.J.; funding acquisition, J.S.-T.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research and the APC were funded by Ministry of Science and Technology of the Republic of China, grant numbers NSTC 112-2115-M-260-001-MY2.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

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

References

1. Naor, M.; Shamir, A. Visual cryptography. In *Advances in Cryptology—EUROCRYPT'94, Proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques, Perugia, Italy, 9–12 May 1994*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1995; Volume 950, pp. 1–12.
2. Kafri, O.; Keren, E. Encryption of pictures and shapes by random grids. *Opt. Lett.* **1987**, *12*, 377–379. [CrossRef] [PubMed]
3. Biham, E.; Itzkovitz, A. Visual Cryptography with Polarization. In the Dagstuhl Seminar on Cryptography, September 1997, and in the RUMP Session of CRYPTO'98, 1997. Available online: https://core.ac.uk/outputs/24679780/ (accessed on 25 January 2026).

4. Huang, C.W.; Juan, J.S. A (t, n)-threshold visual secret sharing scheme based on polarization. In Proceedings of the 2023 IEEE 6th International Conference on Knowledge Innovation and Invention (ICKII), Hokkaido, Japan, 11–13 August 2023; pp. 172–176. [CrossRef]
5. Chen, T.-H.; Tsao, K.-H. Threshold visual secret sharing by random grids. *J. Syst. Softw.* **2011**, *84*, 1197–1208. [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.