Optical and Quantum Electronics (2024) 56:107
https://doi.org/10.1007/s11082-023-05639-2

Optical essential secret image sharing using unequal modulus decomposition and gyrator transform

Mohamed G. Abdelfattah[1,3] · Salem F. Hegazy[2] · Salah S. A. Obayya[1,3]

Received: 12 September 2023 / Accepted: 24 October 2023 / Published online: 13 December 2023

Abstract
Essential Secret Image Sharing (ESIS) decomposes a secret image into a set of shares that are distributed among categorized participants, and ensures that only authorized subsets of these participants can restore the image. All ESIS schemes to date have been based *merely* on computational techniques. In this paper, an optical ESIS system is introduced which uses unequal modulus decomposition (UMD) and optical gyrator transform (GT), offering high-speed parallel processing and dispensing with any pre-processing stages. The presented (1, 2, n) ESIS system generates n shares, including one essential share, such that any two shares that include the essential one, can reconstruct the initial secret image with no distortion. Any other unauthorized subset will not gain any information about the image. The scheme generates essential and nonessential shares that are of equal size, eliminating the need to concatenate sub-shares during the reconstruction of the secret image. The results verify that the secret image was completely retrieved in cases of authorized access, while full distortion occurred in cases of unauthorized access. The GT rotation angle serves as an additional authentication factor to validate the essential share and bolster the security. The optical ESIS system exhibits a high level of sensitivity to the changes in the GT rotation angle - that a variation of just 0.001 radians can cause the correlation coefficient to drop below 0.05.

Keywords Secret image sharing (SIS) · Unequal modulus decomposition · Gyrator transform (GT)

✉ Salem F. Hegazy
salem@niles.cu.edu.eg

✉ Salah S. A. Obayya
sobayya@zewailcity.edu.eg

Mohamed G. Abdelfattah
eng.mo.gamal@mans.edu.eg

[1] Department of Electronics and Communications Engineering, Faculty of Engineering, Mansoura University, Mansoura 35516, Egypt

[2] National Institute of Laser Enhanced Sciences, Cairo University, Giza 12613, Egypt

[3] Center for Photonics and Smart Materials, Zewail City of Science and Technology, Giza 12578, Egypt

1 Introduction

Cryptographic algorithms encode sensitive information into ciphertext using random keys to safeguard it from unauthorized access (Menezes et al. 2021; Paar and Pelzl 2009). In some scenarios, relying on a single user to access this sensitive information can pose a potential security vulnerability (Yan et al. 2021; Liu et al. 2016; Deng et al. 2015). To address this issue, Blakley and Shamir independently introduced the concept of secret sharing (Blakley 1979; Shamir 1979). Desmedt and Frankel developed this concept further with their formal introduction of threshold cryptosystems (Desmedt and Frankel 1990). Secret sharing enables the splitting of a secret into multiple shares, which prevents monopolistic access by a single user to confidential information (Ben-Or et al. 2019; Garg et al. 2012). It ensures protection even when some shares are missing or damaged (Zhang et al. 2010; Asmuth and Bloom 1983; Stinson and Paterson 2018). Secret image sharing (SIS) has become an essential means for protecting access to confidential images during distribution and reconstruction stages. In SIS, the image is encoded into a number of shares (also called shadows), which are distributed on a group of users. Among this group, only a qualified subset can collectively retrieve the image using their shares (Georgi et al. 2021; Shankar et al. 2020; Yan et al. 2020). The SIS scheme is typically realized as a threshold (k, n) system that decomposes a secret image into n shares (Thien and Lin 2002). To correctly retrieve the image, a minimum of k individual shares out of the n are required.

Most legacy schemes of threshold secret-sharing rely on complex mathematical operations running on computational systems (Shankar et al. 2020; Yang et al. 2023; Wu et al. 2020; Luo et al. 2023). However, in recent years, several optical techniques have been introduced to offer high-speed parallel processing in image encryption (Li et al. 2022; Abdelfattah et al. 2022; Su et al. 2021, 2020), and secret sharing (Deng et al. 2015, 2016; Li et al. 2018a; Lu et al. 2020). In 2015, an optical $(2, n)$ threshold scheme based on interference was proposed, which could only be applied to binary secret images (Deng et al. 2015). Deng et al. (2016) then presented an optical $(3, n)$ threshold technique using phased interferometry. Multilevel image authentication and Multiple-image encryption using ghost imaging and hyperplane threshold algorithm were also reported (Li et al. 2018a). Another optical (2, 3) threshold system was introduced by making use of the phase retrieval algorithm (Lu et al. 2020). Although that scheme was simple, a pre-verification process was necessary because the shares might be easily reproduced. All of the optical threshold schemes mentioned above assign the same authority level to participants. However, in many real-world applications, some participants have special privileges based on their status, role, or trust. In such cases, a multilevel or hierarchical structure becomes necessary. Li et al. presented in 2013 a (t, s, k, n) essential SIS (ESIS) algorithm, where n shares are categorized into two levels: s essential shares and $(n - s)$ nonessential ones. The qualified subset required to reconstruct the secret image should consist of a minimum of k shares, including at least t essential shares (Li et al. 2013). Subsequently, Yang et al. introduced an ESIS scheme that reduces the total size of shares using a conjunctive hierarchical approach (Yang et al. 2015). However, the schemes presented in Li et al. (2013); Yang et al. (2015) neglected two important issues: the generation of shares with unequal sizes and the concatenation of sub-shares.

Generating unequal-sized shadows may reveal sensitive information about the corresponding participant's importance, while concatenating sub-shadows may complicate the reconstruction process in practice (Li et al. 2018b; Wu et al. 2019). Li et al. (2016) introduced an ESIS scheme that overcomes the problem of unequal-sized shadows.

However, their scheme still has the issue of concatenating sub-shadows. Two schemes were then proposed over GF(2^8) that can solve both issues (Li et al. 2018b; Sardar and Adhikari 2020). However, these two schemes only work for grayscale images. More recently, Yadav and Singh (2022) introduced an ESIS scheme that can work with color images. However, this scheme suffers from interference if the threshold share number is an odd number and only operates well if it is an even number. All ESIS schemes, so far, have relied on complex mathematical operations performed on computational systems. This paper presents, to the best of our knowledge, the first optical ESIS system capable of sharing secret images among n participants, including one essential share. The novel (1, 2, n) ESIS system integrates both the unequal modulus decomposition (UMD) and the optical gyrator transform (GT). Its generated essential and nonessential shares are equal-sized, eliminating the need to concatenate sub-shares in the reconstruction process. While we demonstrate the key results of the presented system for color images, the scheme is entirely ready for binary and grayscale images. The presented system offers high-speed parallel processing and does not require separate pre-processing steps such as random permutations or a separate encryption stage, significantly reducing the system's complexity.

2 Preliminaries

The presented secret sharing system applies UMD to the secret image in the GT domain. Compared to other optical transforms, the GT rotation angle offers a highly sensitive key that can substantially augment the overall security of the system (Abuturab 2015). The integration of UMD and GT enhances the security of the scheme and eliminates the need for the pre-processing stage typically used in most secret sharing schemes. Here, we present a brief introduction to UMD and GT processes.

2.1 Gyrator transform

For a 2D image $g(x, y)$, the GT with a rotation angle γ can be defined by the linear transform: Rodrigo et al. (2007a)

$$\begin{aligned} G(u,v) &\equiv GT_{\gamma}\{g(x,y)\} \\ &\equiv \frac{1}{|\sin\gamma|}\iint g(x,y)\times K_{(\gamma)}\,\mathrm{d}x\mathrm{d}y, \end{aligned} \tag{1}$$

where (x, y) / (u, v) are the coordinates at the input / output planes. The kernel $K_{(\gamma)}$ is expressed as

$$K_{(\gamma)} = \exp\left[j2\pi\frac{(uv+xy)\cos\gamma - vx - uy}{\sin\gamma}\right]. \tag{2}$$

The rotation angle γ is the parameter that primarily controls the GT output. Compared to the Fourier transform, the rotation angle γ serves as a secondary key that enhances the security. This property renders GT widely used in optical image encryption (Singh and Sinha 2009; Rodrigo et al. 2007b). The GT is optically realized using three lenses inserted at certain distances (Rodrigo et al. 2007c). The inverse GT ($GT_{-\gamma}$) is equivalent to the GT with an angle of rotation $-\gamma$.

2.2 Unequal modulus decomposition

UMD is a technique that decomposes a 2D image into two complex-valued masks, which are independent (with unequal amplitudes and phases) (Abdelfattah et al. 2020). This can be explained referring to the representation in the complex plane as in Fig. 1.

Consider a complex vector $S(u, v)$ that represents a 2D image. We can express its amplitude and phase as $A = |S(u, v)|$ and $\phi = \arg\{S(u, v)\}$, respectively. As illustrated in Fig. 1, we can decompose $S(u, v)$ into two independent random vectors P_1 and P_2 with unequal amplitudes and phases. We can define these vectors using a simple geometrical deduction as follows

$$P_1 = \frac{Ae^{j\alpha}\sin(\beta - \phi)}{\sin(\beta - \alpha)}, \quad P_2 = \frac{Ae^{j\beta}\sin(\phi - \alpha)}{\sin(\beta - \alpha)}. \tag{3}$$

where $\alpha(u, v)$ and $\beta(u, v)$ denote two independent random functions that are generated uniformly over the interval $[0, 2\pi]$. The UMD process is represented by

$$\left[P_1(u, v), P_2(u, v)\right] \equiv \mathcal{UMD}_{\alpha,\beta}[S(u, v)], \tag{4}$$

where denotes that the UMD process $\mathcal{UMD}_{\alpha,\beta}$ is performed on $S(u, v)$ using two random functions $\alpha(u, v)$ and $\beta(u, v)$.

3 ESIS scheme

The proposed ESIS scheme is designed to decompose an initial secret image into n shares with two levels of importance. The n generated shares include one essential share and $(n - 1)$ nonessential shares. The scheme has numerous practical applications, such as maintaining the security of confidential images in financial institutions or the healthcare industry. For example, when a confidential image needs to be accessed by a department manager and one or more of his assistants, or when a medical image contains sensitive information about a patient that needs to be viewed by a doctor and at least one nurse, the proposed ESIS scheme can be employed to ensure that only authorized personnel can access the secret image.

In this section, we present the ESIS scheme, including the secret image sharing and reconstruction processes. The ESIS scheme is sketched in Fig. 2. The main objective of this process is to divide a secret image into a set of n shares, that are then distributed on a group

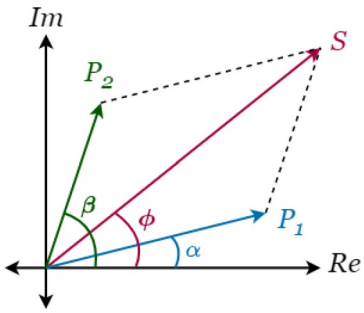

Fig. 1 Unequal modulus decomposition process. The amplitude and phase of every pixel in the 2D image is represented by a vector $S(u, v)$. The UMD process decomposes the vector $S(u, v)$ in the complex plane into two independent random vectors P_1 and P_2 with unequal amplitudes and phases

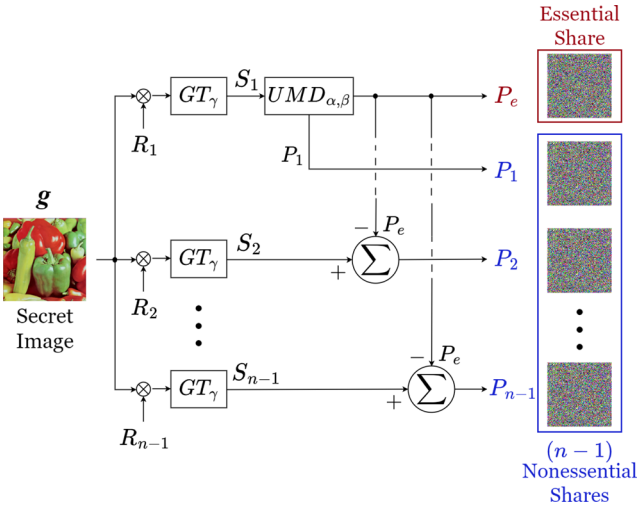

Fig. 2 Block diagram illustrating the essential secret image sharing (ESIS) scheme

of participants. In the (1, 2, n)-ESIS scheme, these n shares consist of one essential share and $(n-1)$ nonessential shares.

Let $g(x, y)$ be the secret color image which consists of R, G, B components (R, G, B denote red, green, and blue). The jth color component of this secret image ($j = \{R, G, B\}$) is multiplied by a random-phase mask (RPM) $R_{i,j}(x, y)$, where $i = 1, 2, 3, \cdots, (n-1)$. The output is gyrator-transformed at a rotation angle γ. The resulting function $S_{i,j}$ can be expressed as

$$S_{i,j}(u, v) = GT_\gamma \left\{ \sqrt{g_j(x, y)} \cdot R_{i,j}(x, y) \right\}. \tag{5}$$

Next, the first function $S_{1,j}(u, v)$ is analyzed using UMD process into two functions $P_{1,j}(u, v)$ and $P_{e,j}(u, v)$

$$\left[P_{1,j}(u, v), P_{e,j}(u, v)\right] \equiv \mathcal{UMD}_{\alpha,\beta}\left[S_{1,j}(u, v)\right]. \tag{6}$$

Here, $P_{e,j}(u, v)$ is considered as the essential share and $P_{1,j}(u, v)$ is regarded as one of the nonessential shares. The remaining nonessential shares $P_{i,j}(u, v)$, $i = 2, 3, ..., (n-1)$ can be directly obtained using

$$P_{i,j}(u, v) = S_{i,j}(u, v) - P_{e,j}(u, v). \tag{7}$$

According to Eqs. (6)and (7), we generate n shares including an essential share $P_{e,j}(u, v)$ and $(n-1)$ nonessential shares $P_{i,j}(u, v)$; $i = 1, 2, 3, \cdots, (n-1)$.

In the reconstruction process, a qualified subset of shares is required to recover the secret image correctly. A qualified subset consists of the essential share $P_{e,j}(u, v)$ and any one of the nonessential shares $P_{i,j}(u, v)$. Firstly, the function $S_{i,j}(u, v)$ is obtained by the coherent superposition of an essential and a nonessential shares as

$$S_{i,j}(u, v) = P_{i,j}(u, v) + P_{e,j}(u, v). \tag{8}$$

Next, the jth color component of the image is obtained by applying the inverse gyrator transform with the same rotation angle γ

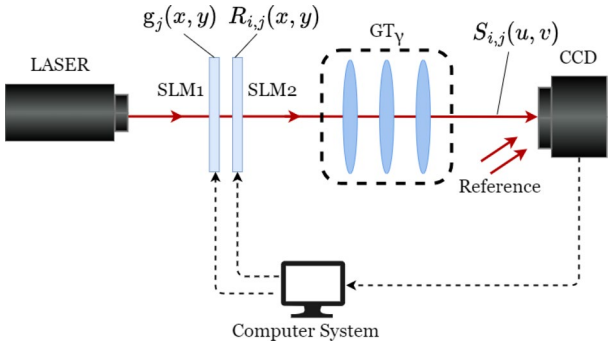

Fig. 3 Optical layout of the secret image sharing process. GT_γ: Gyrator transform of a rotation angle γ; *CCD*: Charged coupled device; and *SLM*: Spatial light modulator

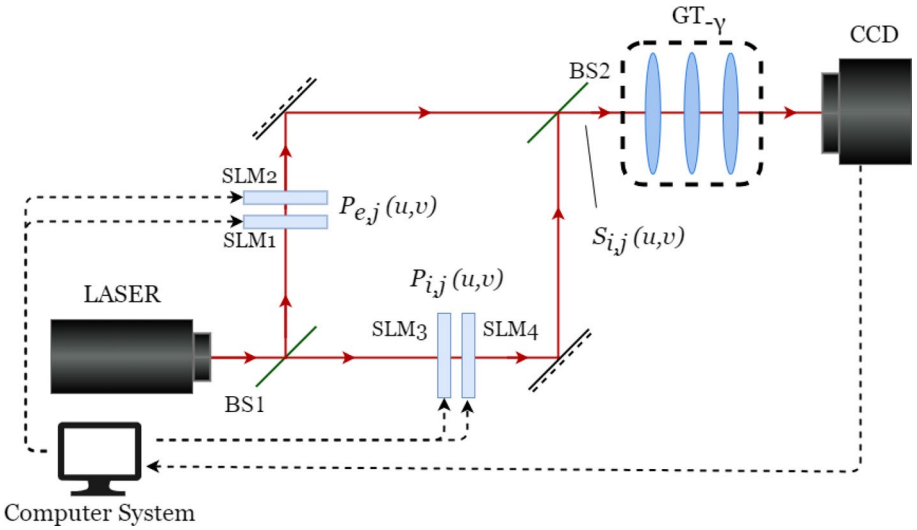

Fig. 4 Optical layout of the secret image reconstruction process. $GT_{-\gamma}$: Inverse gyrator transform of a rotation angle γ; *BS*: Beam splitter

$$g_j(x,y) = \left| GT_{-\gamma}\left\{ S_{i,j}(u,v) \right\} \right|^2. \tag{9}$$

4 Proposed optical ESIS setups

The optical setups for the secret image sharing and reconstruction processes are sketched in Figs. 3 and 4, respectively. The *R*, *G*, *B* color components of the secret image are processed independently, one after the other. In Fig. 3, a laser beam illuminates two spatial light modulators (SLMs) which display the functions $g_j(x,y)$ and $R_{i,j}(x,y)$. This constructs a random-phase-masked version of the *j*th color component of this image. The output passes through a GT system configured with a rotation angle γ. This produces the function $S_{i,j}(u,v)$ which is registered by a Charged Coupled Device camera (CCD camera). UMD operation

is then performed on a computing system to generate n shares. The in-line holography technique is run at the CCD-camera plane to register the phase information.

In Fig. 4, the magnitude and phase of the essential and nonessential shares are separately displayed on two SLM units placed in each of the two arms of a Mach-Zehnder interferometer. The coherent superposition of the two image shares takes place at a beam splitter BS2. The resulting spatially-modulated beam $S_{i,j}(u, v)$ propagates through the GT system configured with a rotation angle $-\gamma$, applying inverse GT. Next, the result is registered by a CCD camera for each color component.

In our scheme, the GT angle γ serves as a further key to improve the scheme security. Therefore, the GT rotation angle together with the essential share are distributed to the corresponding participant. To be able to recover the secret image, the essential share holder has to provide this key along with the essential share. This approach improves the security of the scheme in case hackers steal the essential share. This may be important in the scheme since it generates only one essential share. Through the analysis, the rotation angle γ is the same for all color components and shares. This speeds up the sequential secret sharing and reconstruction processes.

5 Numerical results

In this section, the feasibility and effectiveness of the presented (1, 2, n) ESIS scheme are demonstrated by numerical simulations. Without loss of generality, we have selected a (1, 2, 4) scheme as an example, in which the total number of shares is four ($n = 4$), including one essential share and three nonessential shares. The 256×256 color "Pepper" image (Fig. 5) is used as the input secret image. The random phase masks (RPMs) and UMD parameters ($R_{i,j}$, α_j, and β_j; where $i = 1, 2, 3$) are generated via a random routine. Each of the RPMs and UMD parameters has the dimensions 256×256 and is fair distributed over the $[0, 2\pi]$ interval. In our simulations, the GT rotational angle is set to $\gamma = 1.5$ rad.

We have applied the (1, 2, 4) ESIS scheme to the secret "Pepper" image shown in Fig. 5. The secret sharing phase generates four shares, including the essential share P_e shown in Fig. 6a, along with three nonessential shares P_1, P_2, and P_3 as depicted in Fig. 6b–d, respectively. It is evident that no useful information about the original secret image can be observed in the generated shares.

In the reconstruction phase of the (1, 2, 4) scheme, there are three qualified subsets, namely (P_e, P_1), (P_e, P_2), and (P_e, P_3). Each qualified subset consists of a pair of shares,

Fig. 5 The secret color "Pepper" image with 256×256 pixels

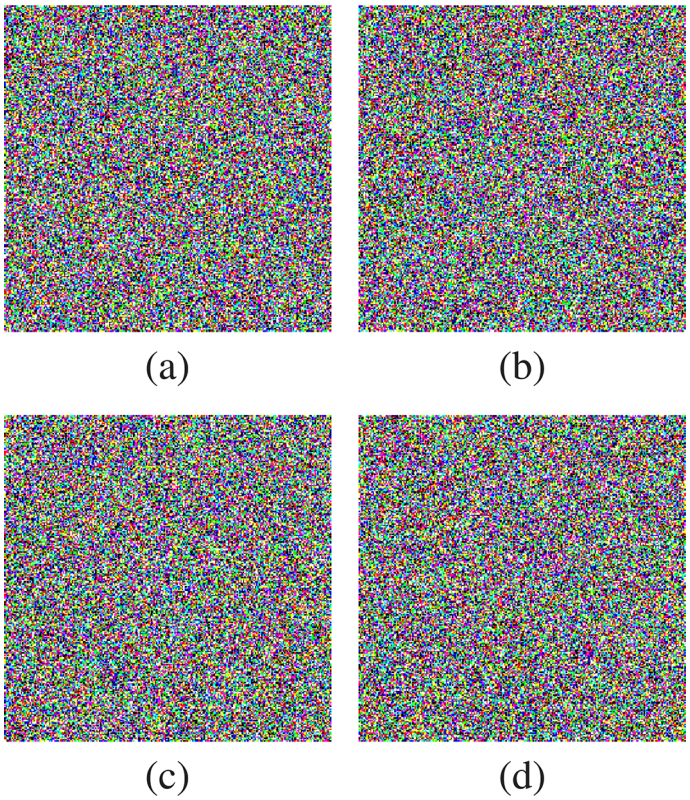

Fig. 6 Results of the (1, 2, 4) ESIS scheme **a** An essential share, **b**–**d** Three different nonessential shares

including the essential one. The reconstructed images resulting from using the three subsets independently are shown in Fig. 7a–c, respectively. It is evident that the secret image is correctly reconstructed in all three cases.

To assess the degree of similarity between the secret image and the reconstructed one, we use the correlation coefficient (CC):

$$CC = \frac{E\{[g - E(g)] \cdot [g_r - E(g_r)]\}}{\sqrt{E[g - E(g)]^2 \cdot E[g_r - E(g_r)]^2}}, \tag{10}$$

where g and g_r denote the original and retrieved image, respectively, and $E(\cdot)$ is the expectation. The CCs of the three reconstructed images in Fig. 7a–c are all equal to one, indicating that any qualified subset can successfully recover the initial secret image without any loss of quality.

For the ESIS scheme, it is essential that any unqualified subset of shares cannot reconstruct the secret image correctly. To further verify this, two numerical experiments have been conducted. Firstly, we have tested reconstructing the secret image using different pairs of nonessential shares. The recovered images obtained from employing the unqualified subsets (P_1, P_2), (P_1, P_3), and (P_2, P_3) are displayed in Fig. 8a–c, respectively. It is evident that the recovered images reveal no information about the

Fig. 7 Recovered secret image using the essential share P_e with the nonessential shares **a** P_1, **b** P_2, **c** P_3

initial secret image. This implies that using any pair of nonessential shares cannot reconstruct the secret image correctly.

Next, we have evaluated the ability to recover the secret image using a single share, whether it is an essential or nonessential share. Since the reconstruction process requires a subset of two shares as input, we have replaced the missing share with zero matrices. We have examined reconstructing the secret image using the individual shares P_e, P_1, P_2, and P_3 independently. The corresponding recovered images are presented in Fig. 9a–d. It is evident that no important information about the initial secret image can be discerned in the recovered images. This verifies that the secret image cannot be recovered when one of the two shares that make up the qualified subset is missing. Moreover, these results further demonstrate that our optical scheme does not suffer from the silhouette problem, as observed in most interference-based optical cryptosystems (Chen and Chen 2013).

To numerically evaluate the unsuccessful recovery of the secret image using unqualified subsets of shares, CC values of the restored images in Figs. 8 and 9 for the R, G, and B components are computed. The CC values are listed in Table 1. all values are less than 0.004, signifying that the presented scheme is highly secure, and that only qualified subsets of shares can enable successful reconstruction of the secret image. These CC values provide a measure of the similarity between the original and recovered images and highlight the importance of using qualified shares for accurate and reliable recovery.

The proposed scheme utilizes the GT angle γ as an additional key to verify the essential share and improve the security. To measure the sensitivity of the image sharing system to tiny variations in the rotation angle, we have performed the following numerical

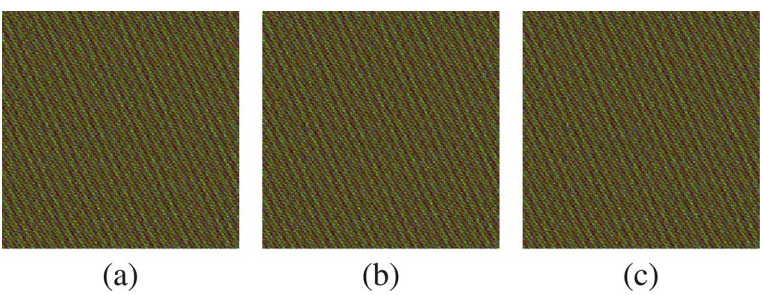

Fig. 8 Recovered secret images using two of the nonessential shares **a** P_1 and P_2, **b** P_1 and P_3, **c** P_2 and P_3

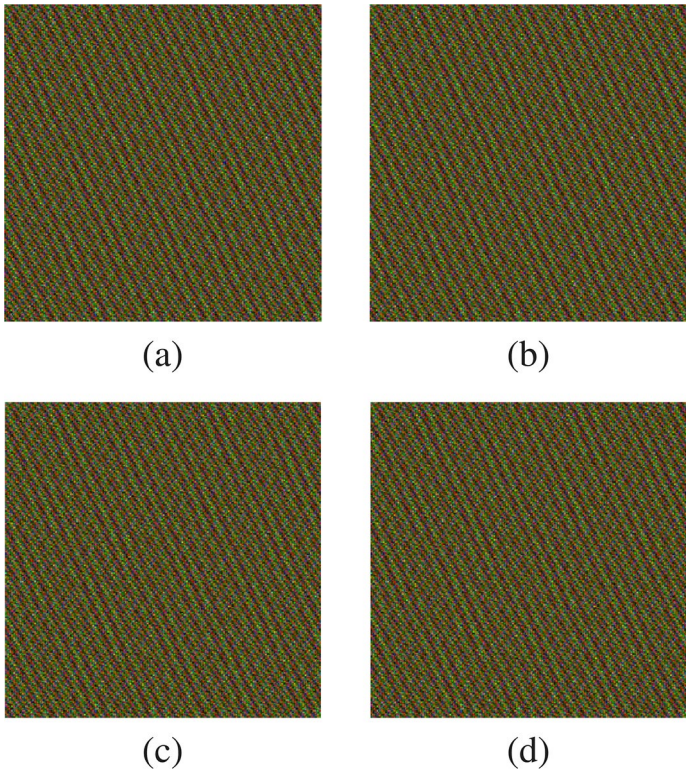

Fig. 9 Recovered secret images using only a single share **a** P_e, **b** P_1, **c** P_2, **d** P_3

experiment. The three qualified subsets associated with a deviated value of γ which is $(\gamma + \Delta R)$ are used to restore the original secret image, where ΔR represents the deviation from the correct value of γ ($\gamma = 1.5$ rad). For each of the three qualified subsets (P_e, P_1), (P_e, P_2), and (P_e, P_3), the CC curves of the recovered images are plotted against ΔR as shown in Fig. 10a–c, respectively. As observed, even a small deviation in the value of γ by $\Delta R = \pm 0.001$ rad results in a decrease in the CC values for all color components to be less than 0.05. Additionally, Fig. 11 depicts the recovered images obtained by deviating the GT angle by only 0.001 rad. The resulting images exhibit significant blurring and lack discernible details. These results demonstrate that the scheme is highly sensitive to even minor changes in the GT rotation angle, which enhances the security of the scheme.

To evaluate the robustness against noise attacks, we have contaminated the two shares of each qualified subset with zero-mean Gaussian noise using the following equation:

$$P' = P[1 + s \cdot G], \tag{11}$$

where P and P' represent the original share and the noise-affected share, respectively, G is a zero-mean Gaussian noise of a unity variance, and the parameter s is the strength factor representing the noise level. For the values: $s = 0.1$ and $s = 1$, the recovered secret images corresponding to using the noisy versions of the qualified subsets (P'_e, P'_1), (P'_e, P'_2), and (P'_e, P'_3) in the reconstruction process are depicted in Fig. 12a–c and Fig. 12d-f, respectively. It is clear that the content of the secret color image can be still recognized in

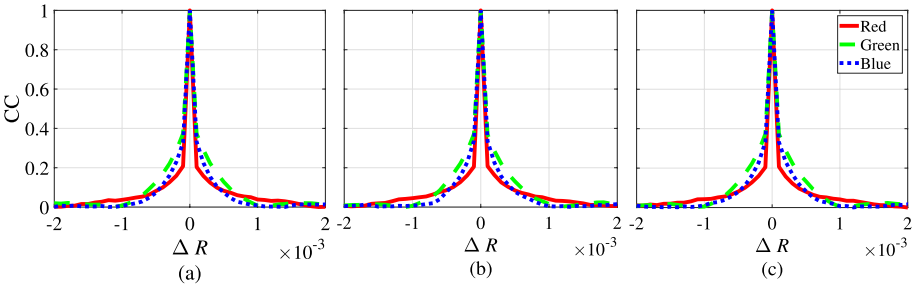

Fig. 10 CC curves of the recovered images versus the deviation in the GT rotation angle (ΔR) for the qualified subsets **a** P_e, P_1 **b** P_e, P_2 **c** P_e, P_3

Table 1 Correlation coefficients of the recovered images using unqualified subsets of shares

Subsets	Color		
	R	G	B
P_1, P_2	0.00032	0.00151	0.00287
P_1, P_3	0.00025	0.001589	0.00281
P_2, P_3	0.00026	0.00156	0.00281
P_e alone	0.00028	0.00159	0.00283
P_1 alone	0.00032	0.00153	0.00290
P_2 alone	0.00031	0.00157	0.00284
P_3 alone	0.00028	0.00154	0.00287

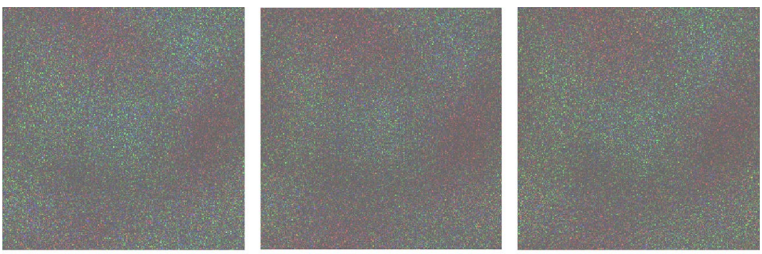

Fig. 11 Recovered secret images after deviating the GT angle by only 0.001 rad using qualified subsets **a** P_1 and P_2, **b** P_1 and P_3, **c** P_2 and P_3

the reconstructed images. The corresponding average CC values of the restored images in Fig. 12a–c, are (0.9475, 0.9918, 0.9716), (0.9450, 0.9920, 0.9725), and (0.9451, 0.9913, 0.9710), respectively, and for the recovered images depicted in Fig. 12d–f, are (0.6027, 0.7046, 0.6463), (0.6094, 0.7101, 0.6513), and (0.6056, 0.7138, 0.6486), respectively. These results verify the high robustness of the proposed scheme against Gaussian noise.

We also investigate the robustness of the proposed scheme against speckle noise. Each share of the qualified subsets (P_e, P_1), (P_e, P_2), and (P_e, P_3) is contaminated by speckle noise with zero mean and variances of $v = 0.05$ and $v = 0.5$. The corresponding reconstructed images are shown in Fig. 13a–f. The CC values of the recovered images in

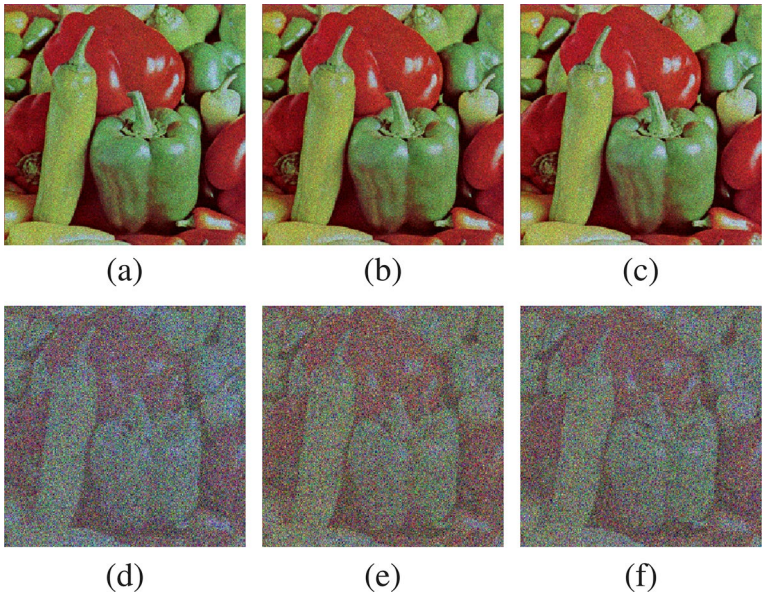

Fig. 12 Recovered secret images using the qualified subsets (P_e, P_1), (P_e, P_2), and (P_e, P_3) after being contaminated by zero-mean Gaussian noise of unit variance and strength factors: **a–c** $s = 0.1$ and **d–f** $s = 1$

Fig. 13a–c are (0.8179, 0.9673, 0.8988), (0.8174, 0.9690, 0.8981), and (0.8146, 0.9740, 0.8992) respectively. However, for the recovered images in Fig. 13d–f the CC values are (0.6006, 0.7611, 0.6867), (0.6080, 0.7758, 0.6826), and (0.6061, 0.7607, 0.6824). Although increasing the noise variance degrades the quality of the recovered images, they can still be easily recognized. These results demonstrate the high level of robustness of the proposed scheme against speckle noise.

6 Discussion

UMD is an effective and promising tool that can be utilized in various security applications. To the best of our knowledge, this is the first time that UMD has been used in a SIS scheme. By designing the SIS scheme using UMD, equal-sized shares can be achieved. The potential for using UMD in SIS schemes is limitless, and many data-sharing configurations can be designed using this tool. For instance, in the proposed scheme, the essential share can be further divided into two other essential shares using UMD. This results in a (2,3,n) ESIS scheme in which three shares, including two essential ones, are required in the reconstruction process. Using multiple stages of UMD can enhance the scalability of the sharing scheme to accommodate various real-world scenarios. However, increasing the number of stages also increases the scheme's complexity. Therefore, careful consideration should be given to the complexity of the sharing scheme. It is worth noting that designing the proposed ESIS scheme based on UMD yields equally-sized shares, eliminating the need to concatenate sub-shares during reconstruction. This improves the security and efficiency of the scheme (Li et al. 2018b, 2016). Nonetheless, one drawback of

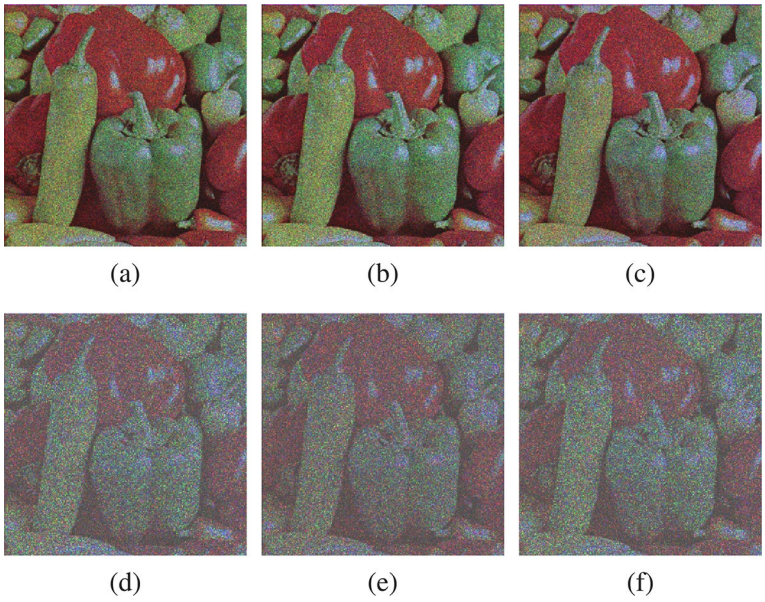

Fig. 13 Recovered secret images using the qualified subsets (P_e, P_1), (P_e, P_2), and (P_e, P_3) after being contaminated by zero-mean speckle noise of variances: **a**–**c** $v = 0.05$ and **d**–**f** $v = 0.5$

using UMD with SIS schemes is that the size of the generated shares may not be reduced compared to the original image.

While our proposed ESIS scheme offers several advantages compared to existing schemes, it is important to mention its main limitations. The proposed scheme requires an optical interferometric setup, which may pose challenges in practical scalability, and only works under coherent light illumination. While coherent light is indispensable in some known applications (e.g. phase-coded optical communications (El-Fiqi et al. 2016)), it is not an essential ingredient in the process of secret image sharing. This is compared to other approaches that are compatible with incoherent light sources. Exploring the use of incoherent light for SIS schemes, such as visual cryptography (Jiao et al. 2020; Yang et al. 2018), may offer more simple and scalable implementations.

7 Conclusion

In this paper, we have presented a novel approach to build optical ESIS that offers several advantages over existing ESIS schemes, including high-speed processing and simplified implementation. The scheme generates equal-sized essential and nonessential shares, eliminating the need to concatenate sub-shares in the reconstruction process. The numerical results confirm that only qualified subsets of shares can correctly reconstruct the secret image, while unqualified subsets result in noisy reconstructed images with a correlation coefficient not exceeding 0.003. Moreover, It is demonstrated that the scheme is highly robust against Gaussian noise and highly sensitive to minor changes in the GT angle, which

serves as an additional key to verify the essential share. The scheme effectively avoids the well-known silhouette problem widely present in interference-based cryptosystems.

Author Contributions The idea was initially proposed by MA who also performed the simulations. Theoretical formulation and data analysis were made by MA and SFH. The main manuscript text was written and revised by MA, SFH, and SSAO.

Funding Open access funding provided by The Science, Technology & Innovation Funding Authority (STDF) in cooperation with The Egyptian Knowledge Bank (EKB). No funding associated with this work.

Data availibility The data will be available upon request.

Declarations

Conflict of interest The authors would like to clarify that there is no financial/non-financial interests that are directly or indirectly related to the work submitted for publication.

Ethical approval Not applicable.

References

Abdelfattah, M., Hegazy, S.F., Areed, N.F., Obayya, S.S.: Compact optical asymmetric cryptosystem based on unequal modulus decomposition of multiple color images. Opt. Lasers Eng. **129**, 106063 (2020)

Abdelfattah, M.G., Hegazy, S.F., Areed, N.F., Obayya, S.S.: Optical cryptosystem for visually meaningful encrypted images based on gyrator transform and hénon map. Opt. Quant. Electron. **54**(2), 1–22 (2022)

Abuturab, M.R.: An asymmetric single-channel color image encryption based on hartley transform and gyrator transform. Opt. Lasers Eng. **69**, 49–57 (2015)

Asmuth, C., Bloom, J.: A modular approach to key safeguarding. IEEE Trans. Inf. Theor. **29**(2), 208–210 (1983)

Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali. pp. 351–371 (2019)

Blakley, G.R.: Safeguarding cryptographic keys. In: Managing Requirements Knowledge, International Workshop on. IEEE Computer Society, p. 313–313 (1979)

Chen, W., Chen, X.: Security-enhanced interference-based optical image encryption. Opt. Commun. **286**, 123–129 (2013)

Deng, X., Wen, W., Mi, X., Long, X.: Optical threshold secret sharing scheme based on basic vector operations and coherence superposition. Opt. Commun. **341**, 22–27 (2015)

Deng, X., Shi, Z., Wen, W.: Threshold secret sharing scheme based on phase-shifting interferometry. Appl. Opt. **55**(31), 8855–8859 (2016)

Desmedt, Y.G., Frankel, Y.: Threshold cryptosystems. In: Crypto'89: Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology. (1990)

El-Fiqi, A.E., Morra, A.E., Hegazy, S.F., Shalaby, H.M., Kato, K., Obayya, S.S.: Performance evaluation of hybrid DPSK-MPPM techniques in long-haul optical transmission. Appl. Opt. **55**(21), 5614–5622 (2016)

Garg, S., Goyal, V., Jain, A., Sahai, A.: Concurrently secure computation in constant rounds. In: Advances in Cryptology–EUROCRYPT 2012: 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings 31. Springer, pp. 99–116 (2012)

Georgi, P., Wei, Q., Sain, B., Schlickriede, C., Wang, Y., Huang, L., et al.: Optical secret sharing with cascaded metasurface holography. Sci. Adv. **7**(16), eabf9718 (2021)
Jiao, S., Feng, J., Gao, Y., Lei, T., Yuan, X.: Visual cryptography in single-pixel imaging. Opt. Express **28**(5), 7301–7313 (2020)
Li, P., Yang, C.N., Wu, C.C., Kong, Q., Ma, Y.: Essential secret image sharing scheme with different importance of shadows. J. Vis. Commun. Image Represent. **24**(7), 1106–1114 (2013)
Li, P., Yang, C.N., Zhou, Z.: Essential secret image sharing scheme with the same size of shadows. Digital Signal Process. **50**, 51–60 (2016)
Li, X., Meng, X., Yin, Y., Wang, Y., Yang, X., Peng, X., et al.: Multilevel image authentication using row scanning compressive ghost imaging and hyperplane secret sharing algorithm. Opt. Lasers Eng. **108**, 28–35 (2018)
Li, P., Liu, Z., Yang, C.N.: A construction method of (t, k, n)-essential secret image sharing scheme. Signal Process. Image Commun. **65**, 210–220 (2018)
Li, X., Mou, J., Cao, Y., Banerjee, S.: An optical image encryption algorithm based on a fractional-order laser hyperchaotic system. Int. J. Bifurc. Chaos **32**(03), 2250035 (2022)
Liu, Y., Zhang, F., Zhang, J.: Attacks to some verifiable multi-secret sharing schemes and two improved schemes. Inf. Sci. **329**, 524–539 (2016)
Lu, D., Liao, M., He, W., Xing, Q., Verma, G., Peng, X.: Experimental optical secret sharing via an iterative phase retrieval algorithm. Opt. Lasers Eng. **126**, 105904 (2020)
Luo, S., Liu, Y., Yan, X., Yu, Y.: Secret image sharing scheme with lossless recovery and high efficiency. Signal Process. **206**, 108931 (2023)
Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. Instructor, p. 202101 (2021)
Paar, C., Pelzl, J.: Understanding Cryptography: A Textbook for Students and Practitioners. Springer Science & Business Media, Berlin (2009)
Rodrigo, J.A., Alieva, T., Calvo, M.L.: Gyrator transform: properties and applications. Opt. Express **15**(5), 2190–2203 (2007)
Rodrigo, J.A., Alieva, T., Calvo, M.L.: Applications of gyrator transform for image processing. Opt. Commun. **278**(2), 279–284 (2007)
Rodrigo, J.A., Alieva, T., Calvo, M.L.: Experimental implementation of the gyrator transform. JOSA A **24**(10), 3135–3139 (2007)
Sardar, M.K., Adhikari, A.: Essential secret image sharing scheme with small and equal sized shadows. Signal Process. Image Commun. **87**, 115923 (2020)
Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
Shankar, K., Elhoseny, M., Kumar, R.S., Lakshmanaprabu, S., Yuan, X.: Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique. J. Ambient. Intell. Humaniz. Comput. **11**, 1821–1833 (2020)
Singh, N., Sinha, A.: Gyrator transform-based optical image encryption, using chaos. Opt. Lasers Eng. **47**(5), 539–546 (2009)
Stinson, D.R., Paterson, M.: Cryptography: Theory and Practice. CRC Press, Boca Raton (2018)
Su, Y., Xu, W., Zhao, J.: Optical image encryption based on chaotic fingerprint phase mask and pattern-illuminated fourier ptychography. Opt. Lasers Eng. **128**, 106042 (2020)
Su, Y., Xu, W., Li, T., Zhao, J., Liu, S.: Optical color image encryption based on fingerprint key and phase-shifting digital holography. Opt. Lasers Eng. **140**, 106550 (2021)
Thien, C.C., Lin, J.C.: Secret image sharing. Comput. Gr. **26**(5), 765–770 (2002)
Wu, Z., Liu, Y.N., Wang, D., Yang, C.N.: An efficient essential secret image sharing scheme using derivative polynomial. Symmetry **11**(1), 69 (2019)
Wu, Z., Liu, Y., Jia, X.: A novel hierarchical secret image sharing scheme with multi-group joint management. Mathematics **8**(3), 448 (2020)
Yadav, M., Singh, R.: Essential secret image sharing approach with same size of meaningful shares. Multimed. Tools Appl. **81**(16), 22677–22694 (2022)
Yan, X., Gong, Q., Li, L., Yang, G., Lu, Y., Liu, J.: Secret image sharing with separate shadow authentication ability. Signal Process. Image Commun. **82**, 115721 (2020)
Yan, X., Li, J., Pan, Z., Zhong, X., Yang, G.: Multiparty verification in image secret sharing. Inf. Sci. **562**, 475–490 (2021)
Yang, C.N., Li, P., Wu, C.C., Cai, S.R.: Reducing shadow size in essential secret image sharing by conjunctive hierarchical approach. Signal Process. Image Commun. **31**, 1–9 (2015)
Yang, N., Gao, Q., Shi, Y.: Visual-cryptographic image hiding with holographic optical elements. Opt. Express **26**(24), 31995–32006 (2018)

Yang, C.N., Li, P., Kuo, H.C.: (k, n) secret image sharing scheme with privileged set. J. Inf. Secur. Appl. **73**, 103413 (2023)
Zhang, Q., Wang, Q., Wei, X.: A novel image encryption scheme based on DNA coding and multi-chaotic maps. Adv. Sci. Lett. **3**(4), 447–451 (2010)