Mathematical Biosciences and Engineering

MBE, 21(3): 4762–4778.
DOI: 10.3934/mbe.2024209
Received: 29 October 2023
Revised: 02 January 2024
Accepted: 21 February 2024
Published: 29 February 2024

http://www.aimspress.com/journal/MBE

*Research article*

# Secure multimedia communication: advanced asymmetric key authentication with grayscale visual cryptography

**Tao Liu[1], Shubhangi Vairagar[2], Sushadevi Adagale[3], T. Karthick[4], Catherine Esther Karunya[5], John Blesswin A[6,*] and Selva Mary G[6,*]**

[1] Tianjin Sino-German University of Applied Sciences, Tianjin 300350, China
[2] Department of Artificial Intelligence and Data Science, Dr. D. Y. Patil Institute of Technology, Pimpri, Pune 411018, India
[3] Department of Computer Engineering, KJEI's Trinity Academy of Engineering, Pune 411048, India
[4] Department of Data Science and Business Systems, School of Computing, SRM Institute of Science and Technology, Kattankulathur 603203, India
[5] Research Scholar, Computer Science and Engineering, School of Computing, SRM Institute of Science and Technology, Kattankulathur 603203, India
[6] Directorate of Learning and Development, SRM Institute of Science and Technology, Kattankulathur 603203, India

* **Correspondence:** Email: johnblesswin@gmail.com, selvamaryg.rnd@gmail.com.

**Abstract:** The secure authentication of user data is crucial in various sectors, including digital banking, medical applications and e-governance, especially for images. Secure communication protects against data tampering and forgery, thereby bolstering the foundation for informed decision-making, whether managing traffic, enhancing public safety, or monitoring environmental conditions. Conventional visual cryptographic protocols offer solutions, particularly for color images, though they grapple with challenges such as high computational demands and reliance on multiple cover images. Additionally, they often require third-party authorization to verify the image integrity. On the other hand, visual cryptography offers a streamlined approach. It divides images into shares, where each pixel represented uniquely, thus allowing visual decryption without complex computations. The optimized multi-tiered authentication protocol (OMTAP), which is integrated with the visual sharing scheme (VSS), takes secure image sharing to the next level. It reduces share count, prioritizes image fidelity and transmission security, and introduces the self-verification of decrypted image integrity through asymmetric key matrix generators, thus eliminating external validation. Rigorous testing has

confirmed OMTAP's robustness and broad applicability, thereby ensuring that decrypted images maintain their quality with a peak signal-to-noise ratio (PSNR) of 40 dB and full integrity at the receiver's end.

**Keywords:** multimedia communication; visual cryptography; integrity verification; image encryption; visual sharing scheme

## 1. Introduction

The advent of digital banking has transformed the financial landscape, offering unparalleled convenience and speed when conducting financial transactions. However, this digital transformation has also exposed users to various security risks, from identity theft to unauthorized access to sensitive financial information. Traditional forms of authentication, such as passwords, personal identification numbers (PINs), and even biometric systems, need to be improved to thwart sophisticated cyberattacks. In addition to the need for heightened security, the banking sector faces the challenge of providing seamless and quick authentication processes. Cumbersome or time-consuming authentication methods can significantly impair the user experience, thus leading to customer dissatisfaction and a potential loss of business. Therefore, there is a pressing need for an authentication mechanism that is robust against various forms of cyberattacks and efficient in terms of computational resources and time. Moreover, the rising trend of joint account holdings for business partnerships or familial financial planning adds an additional layer of complexity to the authentication process. Joint accounts necessitate a multi-tiered authentication system that can accommodate multiple stakeholders while maintaining the highest levels of security.

Visual cryptography (VC), which focuses on the secure transmission of visual data, offers a promising avenue to tackle these challenges. By encrypting a secret image into multiple cover images or shares, VC allows for a secure yet simple way to authenticate users. However, the existing methodologies primarily concentrate on color images and require significant computational resources, thus making them less practical for real-time, high-security applications such as digital banking. VC, which is a subset of cryptography that focuses on the secure transmission of visual information, has emerged as a promising solution. Existing research has mainly concentrated on color images, offering protocols that divide a secret image into multiple shares or cover images [1]. The current state-of-the-art visual cryptography presents two significant challenges: high computational complexity and multiple cover image requirements. These challenges become even more pronounced in digital banking, where rapid and secure authentication is paramount. This research addresses these limitations by introducing an optimized multi-tiered authentication protocol (OMTAP) that uses grayscale visual cryptography. By exploiting the inherent properties of grayscale images, which contain only a single-color channel, this study proposes a novel methodology OMTAP that only requires 5X/3 color cover images for secure authentication, where X is the number of color channels. This approach significantly reduces the computational complexity and the number of required cover images. The proposed OMTAP protocol is particularly well-suited for digital banking applications. It allows for the distribution of secure image shares between the bank and individual or joint account holders. The secret image is revealed when all the shares are digitally stacked, providing a secure and efficient method to access banking services. This research contributes to the existing body of knowledge by offering a

more efficient and secure method for visual cryptographic authentication. It opens new avenues for the application of visual cryptography in digital banking, particularly for individual or joint account holders requiring multi-tiered authentication. The remainder of this paper is organized as follows: section 2 provides a detailed review of related work in visual cryptography and digital banking authentication; section 3 outlines the proposed methodology, followed by section 4, which presents the experimental results and discussions; and finally, section 5 states the conclusions.

## 2. Literature study

The dynamic landscape of digital security has necessitated innovative approaches to safeguard sensitive information. VC has emerged as a compelling solution in digital banking, where the confidentiality and integrity of user data are paramount. This cryptographic technique allows for the encryption of visual information so that decryption can be visually performed by overlaying encrypted pieces, known as "shares". Despite its promise, visual cryptography has challenges, mainly when applied to different types of images, such as grayscale and color images. The following literature review aims to comprehensively understand state-of-the-art visual cryptography by focusing on its applications and limitations in secure image transmission. By dissecting the findings from previous studies, this section will illuminate the critical challenges and gaps in the existing body of knowledge. These insights will serve as the scaffolding upon which this research builds its contributions. VC, which was initially introduced by Naor and Shamir, provided a unique method to encrypt visual information by dividing an image into multiple shares [2,3]. While these shares offer no discernible information individually, stacking them reconstructs the original image. Initially designed for binary images, VC has evolved to include grayscale and color images. However, this evolution of VC has introduced complexities, such as maintaining color fidelity in the reconstructed image [4]. One of the primary challenges in VC is ensuring the integrity of the reconstructed image. Since the secret is divided among several shares, altering even a single share can compromise the final image [5]. Traditional methods for integrity verification often involve additional shares or a trusted third party, thus adding complexity and potential security vulnerabilities [6]. In the analysis of prior research, the authors studied multiple shares typically generated based on the grayscale values of the secret image's pixels, further emphasizing the need for efficient grayscale schemes [7,8]. Each pixel in the secret image is often replaced by multiple subpixels, thereby increasing the size of the shares. This size increase poses challenges for efficient storage and transmission [9,10]. Using color images in visual sharing schemes (VSS) significantly increases the computational cost, thus emphasizing the need for optimization [11]. In the revealing phase, color VSS schemes commonly employ a color index table, thereby adding a layer to decryption [12]. Most VSS schemes produce binary shares, limiting their application to grayscale and color images. Pre-processing steps, such as halftoning, are commonly used but increase the computational burden [13,14]. Issues related to pixel expansion pose challenges for maintaining image fidelity and security. Some color VSS schemes use key shares and are secured by generating random shares. Additionally, natural cover images are employed to hide noise-like shares. Digital stacking of shares often involves logical exclusive OR (XOR) operations to reveal the secret images [15–17].

In light of these challenges, the current study aims to explore advanced VC protocols explicitly tailored for grayscale images in the context of digital banking. This research contributes to the existing body of knowledge by offering a more efficient and secure method for visual cryptographic

authentication. It opens new avenues to apply VC in digital banking, particularly for individual or joint account holders that require multi-tiered authentication. These protocols aim to offer secure encryption while providing mechanisms to ascertain the integrity and authenticity of the reconstructed image without added complexities.

## 3. Proposed methodology

The proposed OMTAP using VSS aims to address the challenges identified in the existing body of work, primarily focusing on the computational efficiency, integrity, and multi-tiered authentication in digital banking applications. The study introduces an optimized, multi-tiered, authentication protocol using visual sharing scheme (OMTAP-VSS), explicitly tailored for grayscale secret images. Three core objectives have been outlined for OMTAP-VSS: enhancing data security, preserving visual data quality, and incorporating an in-built integrity verification layer. Structured into three pivotal phases—secret encryption, secret decryption, and secret authentication—the protocol aims to offer a holistic solution. Unique features have been incorporated, such as a resistance to cheating attempts and the ability to flag inconsistencies in received data without additional shares or third-party verification. Thus, OMTAP-VSS demonstrates promise as a comprehensive solution to safeguard visual data in digital banking applications, as illustrated in the methodology presented in Figure 1.

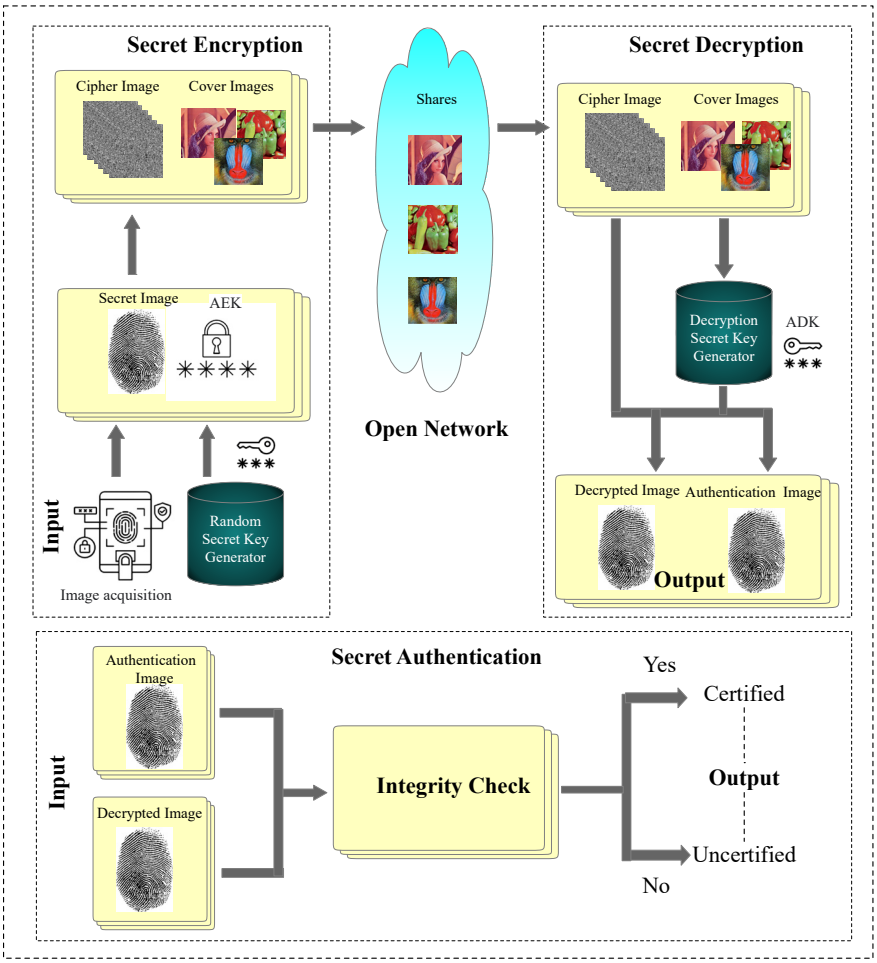


**Figure 1.** Architecture of proposed OMTAP.

*3.1. Secret encryption phase (SEP)*

In this phase, the secret image (S) is converted into shares (Sh). An asymmetric random key generator is used in this proposed OMTAP. The working of the secret encryption phase (SEP) is shown in Figure 2.

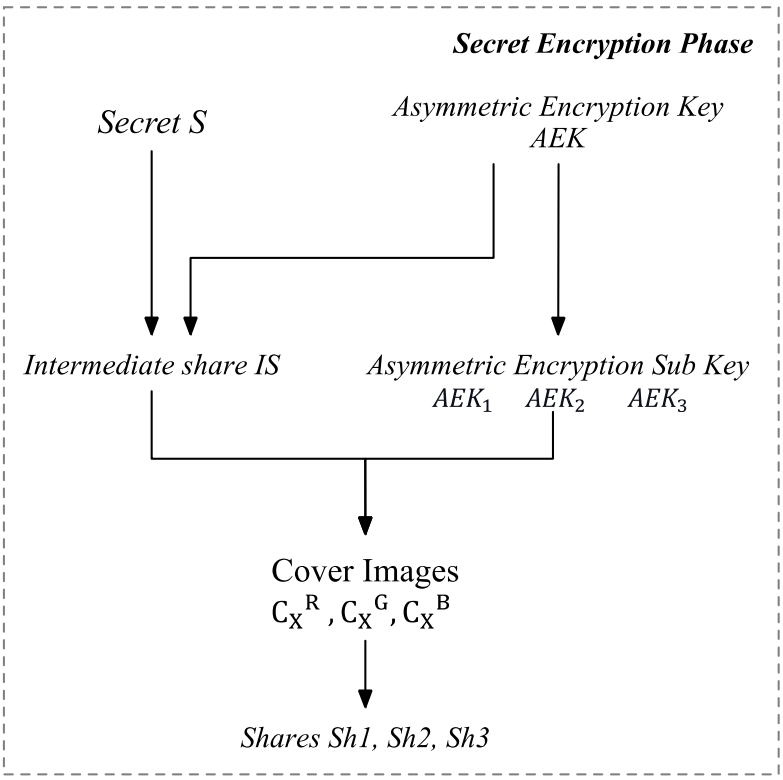


**Figure 2.** Flowchart of secret encryption phase.

An asymmetric encryption key generator is employed to create an encryption key (EK) matrix, which matches the dimensions of the grayscale secret image S. Subsets of the EK, known as asymmetric encryption key subsets (AEK), are further generated to add an extra layer of security to the generated shares. Algorithm 1 involves the generation of AEK through specific operations based on a predefined set of random prime numbers. This deliberate introduction of variability ensures the robustness of the encryption process, thus enhancing the security of the generated shares. Each pixel of the secret image S and each element of the EK matrix are processed using the Karatsuba fast multiplication (KFM) to produce intermediate share values (IS) for each pixel.

These IS values are encrypted versions of the secret image, while the AEK subsets act as encrypted keys. Then, the *IS* values and *AEK* subsets are embedded into the color channels of the cover images C1, C2, and C3 using the least significant bit (LSB) embedding technique [18,19]. This process generates the color share images Sh1, Sh2, and Sh3, which are subsequently transmitted to authenticated participants for secure communication. The algorithm for the secret encryption phase is given in Algorithm 1.

**Algorithm 1: Secret encryption**

$Input$: $One\ gray\ scale\ Secret\ image\ S\ and\ a\ set\ of\ three\ color\ cover\ images\ C1, C$
$each\ of\ dimensions\ of\ Size\ H \times W$
$Output$: $A\ collection\ of\ n\ color\ share\ images\ \{Sh1, Sh2, Sh3\}$
$begin$:
$Separate\ the\ color\ channels\ \ {C_X}^t\ from\ C_X,\ t \in \{R, G, B\},\quad X \in \{1,2,3\}$
$For\ every\ \ x\ \leftarrow 0: H-1:$
$For\ every\ \ y\ \leftarrow 0: W-1:$
$EK = \{m\ \ (m \times n)\}, where\ \ m, n \in \{7,11,13\}$

$$AEK_1 = \begin{cases} 0, & \forall\ EK_i \le m \\ 1, & otherwise \end{cases}$$

$$AEK_2 = \begin{cases} EK_i\ mod\ 10, & \forall\ EK_i \le m \\ EK_i\ /\ 10, & otherwise \end{cases}$$

$$AEK_3 = \begin{cases} EK_i/\ 10, & \forall\ EK_i \le m \\ EK_i\ mod\ 10, & otherwise \end{cases}$$

$IS\ = S\ \times\ EK$
${Sh_X}^p = {C_X}^p\ -\ mod({C_X}^p, 10)\ +\ IS\quad p \in \{1,2\}$
${Sh_X}^q = {C_X}^q\ -\ mod({C_X}^q, 10)\ +\ AEK_q\quad q \in \{1,2,3\}$
$end\ for$
$end\ for$
$For\ every\ \ Z\ \leftarrow 1:3:$
$Sh(:,:,1) = Sh_R$
$Sh(:,:,2) = Sh_G$
$Sh(:,:,3) = Sh_B$
$end\ for$
$end\ begin$

*3.2. Secret decryption phase (SDP)*

In the decryption phase, the focus shifts from generating shares to reconstructing the original secret image (S) from the received shares (RSh1, RSh2, and RSh3). The operational details of this phase are illustrated in Figure 3. Initially, these received shares are separated into their respective color channels, from which the reconstructing intermediate share (RIS) values and the asymmetric decryptions sub key sets (ADK1, ADK2, and ADK3) are extracted using the LSB extraction process [20]. The asymmetric decryption key (ADK) is generated, which is distinct from the AEK. Subsequently, the ADK and $RIS$ values are combined to produce the decrypted new message (DM), which essentially provides the pixel values for the reconstructed image.

Then, these pixel values are parsed into two different images, the decrypted image (DI) and the authenticated image (AI), thereby serving as the final outputs of the decryption process. The maximum threshold value, $T^{max}$ is determined as a constant multiple of the factors originating from the key values employed during the share construction process. For all multiplicative operations involved in the decryption of the secret, the KFM method is utilized [21]. The algorithm for the secret encryption phase is given in Algorithm 2.

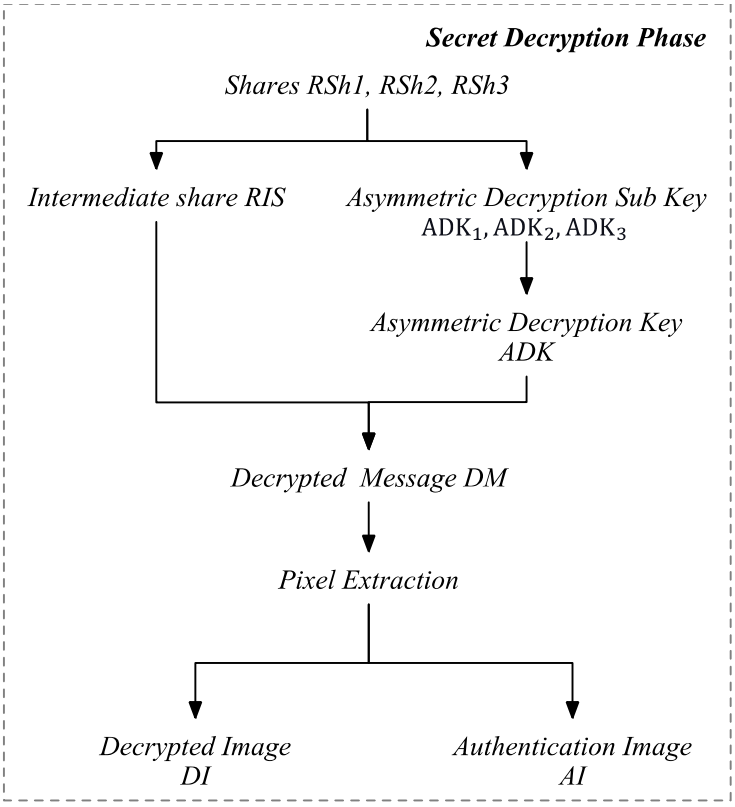


**Figure 3.** Flowchart of secret decryption phase.

**Algorithm 2: Secret decryption**

$Input: n\ Share\ images\ RSh1, RSh2, RSh3\ each\ of\ dimensions\ of\ Size\ H \times W$

$Output:\ Decrypted\ Secret\ Image\ DI\ and\ Authentication\ Image\ AI$

$begin:$

$Separate\ the\ color\ channels\ \ {C_X}^t\ from\ C_X,\ t \in \{R, G, B\},\quad X \in \{1,2,3\}$

$For\ every\ \ color\ channel\ t$

$For\ every\ \ x\ \leftarrow 0: H-1:$

$For\ every\ \ y\ \leftarrow 0: W-1:$

${RSh_X}^p = \ mod({C_X}^p, 10)\quad$ p $\in \{1,2\}$

$ADK^q = mod({C_X}^q, 10)\quad$ q $\in \{1,2,3\}$

$$ADK = \begin{cases} \dfrac{T_{max}}{ADK^2 \times 10 + \ ADK^3}, & \forall\ ADK^1 = 0 \\ \dfrac{T_{max}}{ADK^3 \times 10 + \ ADK^2}, & otherwise \end{cases}$$

$DM = (RSh\ \times\ ADK)$

$DI = DM\ mod\ 10^{\frac{n}{2}} \quad n\ =\ |DM|$

$end\ for$

$end\ for$

$end\ for$

$end\ begin$

### *3.3. Secret authentication phase (SAP)*

The proposed OMTAP-VSS incorporates a secret authentication phase (SAP) designed to ensure the integrity of the DI. In this context, integrity refers to the guarantee of data accuracy and consistency during the reconstruction process at the receiver's end. Importantly, this integrity check is not designed to protect against unauthorized access, but rather to confirm that the DI has not been altered or tampered with by a third party [23,24]. The process of integrity verification is depicted in Figure 4.

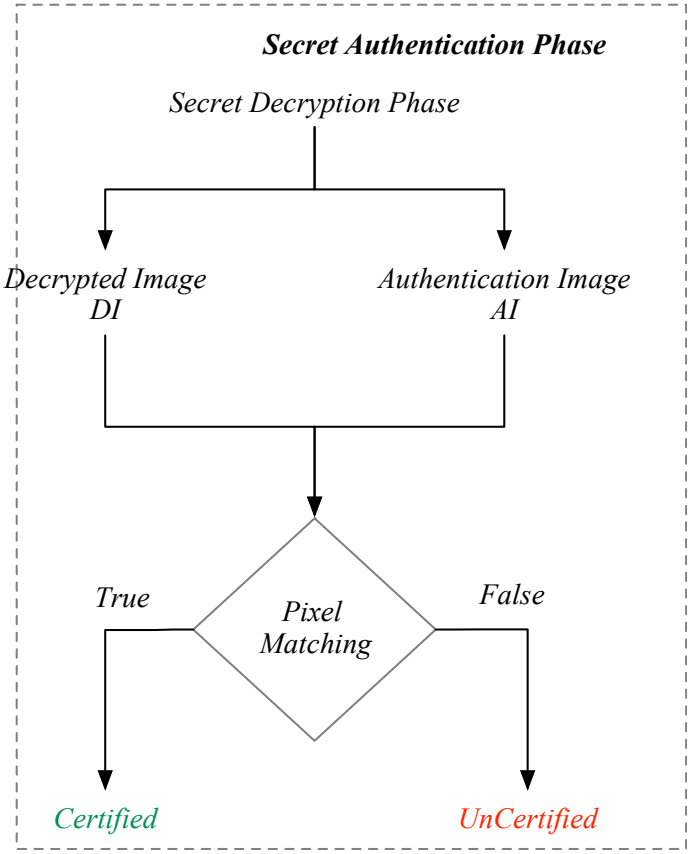


**Figure 4.** Flowchart of secret authentication phase.

During the decryption process, the received encrypted shares (RSh) are digitally superimposed. By leveraging the AEK, the DI is subsequently generated. To verify the integrity of the image, an AI is formulated. In this authentication phase, a pixel-by-pixel comparison between the DI and the AI is performed. If all pixels are verified as identical, the image is confirmed as authentic. Conversely, if any pixel mismatches are detected, the DI is deemed compromised, thus raising suspicion that one or more shares have been altered or tampered with. Under such circumstances, the randomly generated key values will fail to disclose the secret, thus preserving the communication's integrity [25–27].

The OMTAP-VSS offers a comprehensive framework for secure image transmission. This multi-phase approach, which is comprised of the SEP, SDP, and SAP, ensures robust security, high-quality image reconstruction, and an uncompromised integrity. While the SEP phase leverages asymmetric encryption keys and Karatsuba fast multiplication to create encrypted shares, the SDP phase focuses on reconstructing the original image from the received shares, thereby employing an asymmetric

decryption key distinct from the encryption key. The SAP phase introduces an additional layer of security by performing a pixel-by-pixel integrity check between the DI and the AI. Therefore, this integrated protocol provides a holistic solution for secure image communication, which is especially vital in sensitive sectors such as digital banking. The OMTAP-VSS protocol efficiently balances security and computational complexity, making it a promising candidate for real-world applications.

## 4. Experimentation and result analysis

In the experimental stage, simulations were conducted using MATLAB, with a focus on its image processing toolbox to execute various image algorithms. For the purposes of this study, the commonly used "Lena", "Pepper", and "Baboon" images served as the cover images and a thumb image considered to be secret image. The images are presented in Figure 5.

A thumb image representing a secret image was intended to be distributed among parties. An encryption key matrix, congruent in size to the secret image S, was constructed during the encryption process. This matrix encompassed the, which is crucial for encrypting individual pixels of the secret image.


**Figure 5.** Sample test images.

Moreover, the AEK was segmented into subkeys for further granularity. The encrypted pixels of the secret image and the AEK subkeys were seamlessly integrated into color cover images. This integration exploited the color channels of the cover images and employed the LSB embedding technique to achieve the fusion [21,28,29]. The entire journey of the secret image is pictorially depicted in Figure 6.

Figure 7 offers a comprehensive visualization of the secret decryption and secret authentication phase, specifically for the test images. In the decryption segment, pixel values from the received shares were meticulously extracted through the LSB extraction method. The extracted encrypted image pixels and the derived ADK, which were constructed from the subkeys, paved the way for the generation of the DM. This DM encapsulated the decrypted code bifurcated into the DI and the AI. Transitioning to the authentication phase, a meticulous pixel-by-pixel comparison between the DI and the AI was conducted. The authentication status was unequivocally conferred as "Certified" if a perfect match was observed across all pixels.

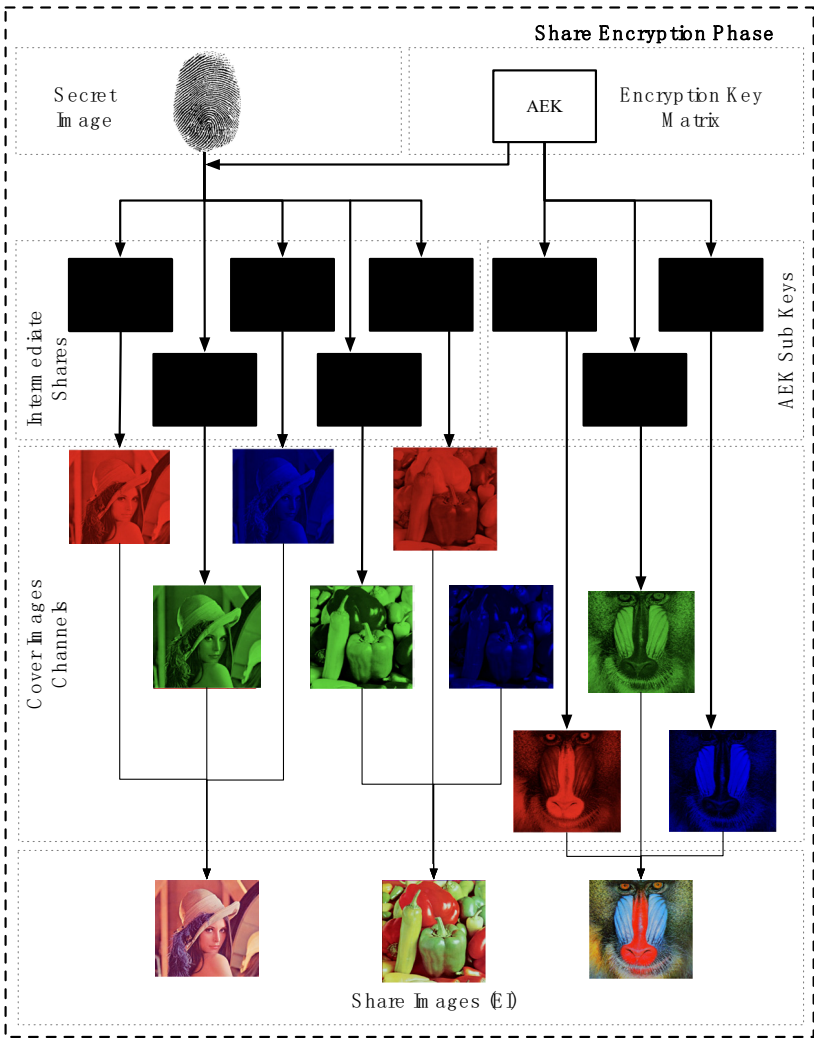


**Figure 6.** Life cycle of test images in secret encryption phase.

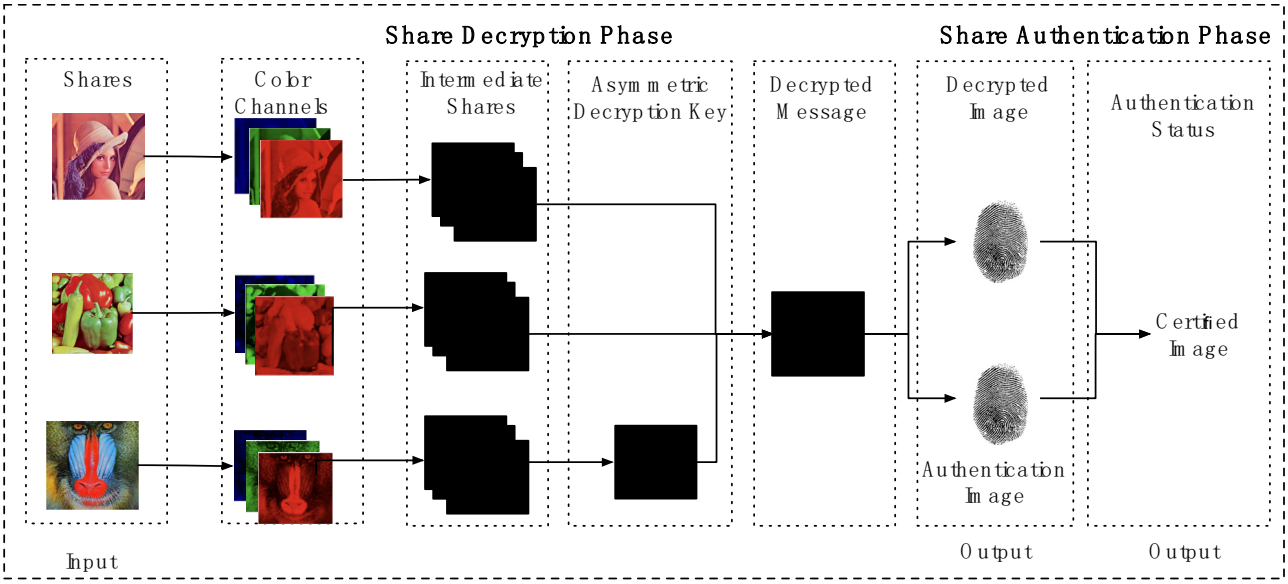


**Figure 7.** Life cycle of test images in secret decryption and secret authentication phase.

The proposed OMTAP safeguards the integrity through sophisticated encryption while creating shares. A unique AEK was generated and further segmented into AEK subsets, which were then distributed among the participants in the communication. This multi-tiered security structure ensured that the grayscale secret image (S) remained untouched and unaltered throughout the encryption and decryption phases.

### *4.1. Quality checking analysis*

To analyze the quality of the DI, benchmarks such as PSNR, mean squared error (MSE), and structural similarity index (SSIM) were utilized. A diminished MSE correlates to a heightened PSNR, suggesting a superior image quality [12,13,15]. When the MSE approaches zero, the images display significant similarity. Images boasting a PSNR above 25 dB are deemed of a high quality, and ascending values indicate a closer match to the original grayscale image. The SSIM acts as a gauge of structural similarity between the reconstructed and the original grayscale images, with values spanning from –1 to +1. A value of +1 confirms that the two images share identical structures. A lower MSE value indicates that the reconstructed image is of a higher quality and more similar to the original [6,11]. The quality of the cover images C1, C2, and C3 were compared with the shares Sh1, Sh2, and Sh3, and the analysis showed that the shares were good in quality and would not reveal any secret pixel value. The results of this comparison indicated that the shares exhibited good quality and were unlikely to reveal any secret pixel values. This suggests that the encryption and decryption processes within the proposed system maintain the integrity of the sensitive grayscale information. The comprehensive use of PSNR, MSE, and SSIM metrics provides a thorough and objective assessment, thereby ensuring that the decrypted images faithfully represent the original content while maintaining a high level of security in the transmission and reconstruction of grayscale images.

Figure 8 shows that the recorded MSE values range from a low of around 2.34 to a high of 4.68. Lower MSE values are more desirable, as they indicate closer resemblance between the two compared images. A higher PSNR value indicates that the share image is of a higher quality and closely resembles the original cover image. Across all the cover and share pairs, the proposed OMTAP method consistently outperformed the existing methods in terms of PSNR values [21,22]. This indicates that OMTAP offers a more effective transformation process, thereby producing shares that closely resemble the original cover images. The proposed OMTAP method has demonstrated its effectiveness in ensuring high-quality image reconstruction, thus making it a promising technique for future applications in secure image transmission and storage.

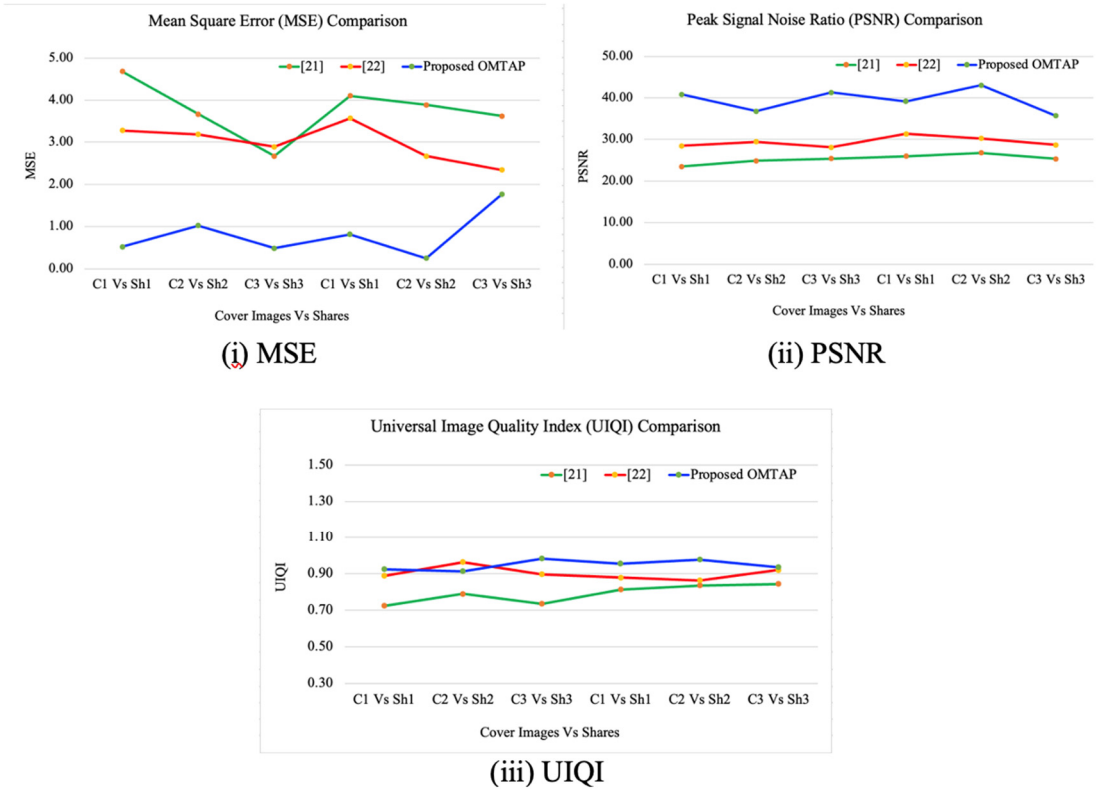


**Figure 8.** Quality analysis of shares in proposed OMTAP.

The UIQI values for the proposed OMTAP spanned between 0.91 and 0.98, demonstrating a high degree of quality and similarity in the proposed method's image reconstruction. The proposed OMTAP method consistently exhibited high UIQI values across all cover and share pairings, underlining its ability to produce shares that were in close resemblance to the original cover images [6]. This is indicative of the method's capability to retain significant structural and textural information of the original image. The consistent high performance of OMTAP across diverse image pairs reinforces its robustness and establishes it as a promising technique in visual sharing schemes. The original secret image and the DI were compared and the values were tabulated in Table 1.

**Table 1.** Quality analysis of decrypted image in proposed OMTAP.

| **Performance Metrics** | Test 1 | Test 2 | Test 3 | Test 4 |
|---|---|---|---|---|
| **MSE** | 0 | 0 | 0 | 0 |
| **PSNR** | +Inf dB | +Inf dB | +Inf dB | +Inf dB |
| **UIQI** | 1 | 1 | 1 | 1 |

Considering the presented performance metrics, it's evident that the proposed OMTAP methodology stands out in preserving the quality of the information across diverse grayscale secret images and color cover images. Impressively, there's a notable absence of data degradation throughout the processing phase and the metrics vouch for the precision of the reconstructions. More crucially, this superior data fidelity was attained without sacrificing security. The technique ensures the data's

integrity and confidentiality, thus positioning it as a formidable and dependable choice for applications emphasizing high-level security and quality. Hence, the proposed OMTAP offers a marked enhancement over conventional methods, especially in settings that prioritize impeccable data reconstruction combined with rigorous security protocols.

### *4.2. Computational complexity and color channels*

The proposed OMTAP has been meticulously designed to address challenges in the existing body of work, with a primary focus on computational efficiency, data integrity, and multi-tiered authentication, particularly in digital banking applications. It is noted that while computational operations are inherent in OMTAP, the protocol strategically leverages the KFM method, known for its efficiency in reducing basic operations. This choice was deliberate, aiming to strike a balance between computational complexity and the need for robust security. Similarly, the use of color channels for the cover images C1, C2, and C3 was accompanied by the LSB embedding technique. This approach mitigated pixel expansion issues and preserved the visual quality of the cover images. The suggested OMTAP divides a single grayscale image into $(5X + 3)$ share channels. When utilizing color cover images, which have three color channels - red, green, and blue - the equation $(5X + 3)/3$ results in three color shares for each grayscale secret image. This approach reduces the number of shares in comparison to grayscale shares. Unlike traditional VC methods, the proposed protocol minimizes the number of color shares, thus addressing concerns related to contrast and pixel expansion associated with typical VC approaches.

### *4.3. Integrity verification*

In the context of our research objectives, a key emphasis lies on the self-verification of the DI. The inclusion of a secret authentication phase adds an extra layer of security, thus ensuring the integrity of the DI without introducing significant computational overhead. This phase serves to confirm that the DI remains unaltered and has not been tampered with by any unauthorized third party, contributing to the overall robustness of the protocol. In essence, the protocol's design choices are geared towards a nuanced consideration of both computational efficiency and security. The focus on self-verification distinguishes OMTAP-VSS from traditional VC methods, and the protocol remains committed to providing a comprehensive solution for secure image communication in digital banking applications.

The generated color share images (Sh1, Sh2, and Sh3) appear natural, offering no indication of their role as shares or their underlying content. Consequently, even if an unauthorized individual were to acquire all the shares, reconstructing the original secret image would require passing through several security checks, including integrity verification. This illustrates the robustness of OMTAP to maintain data integrity under various conditions. The integrity checking was tested by faking one or more shares, and the results were recorded in Table 2.

Table 2 shows that the findings demonstrate that the OMTAP protocol is adept at identifying any compromised or altered shares, thereby validating its robust capabilities in preserving the integrity of the grayscale secret image (S). This test involves subjecting the system to various scenarios, represented by ten different tests (Test 1 to Test 10), each simulating potential security threats by either faking or tampering with one or more shares derived from the encrypted secret image. The results are recorded in Table 1, where each row corresponds to a specific test, and each column represents an

individual share. The entries in the table are marked as "T" if the share passed the integrity check and "F" if it failed. The ultimate objective is to determine whether the overall integrity of the grayscale secret image is certified based on the results of individual share checks. The protocol's success in identifying compromised or altered shares and its ability to withhold certification when integrity is compromised reflect its robustness to ensure the secure transmission and reception of sensitive data under various conditions. This makes OMTAP especially well-suited for scenarios where maintaining the integrity of sensitive grayscale images cloaked in color cover images is a crucial requirement [30].

**Table 2.** Integrity checking test result analysis.

| **Secret Image S** | **Test 1** | **Test 2** | **Test 3** | **Test 4** | **Test 5** | **Test 6** | **Test 7** | **Test 8** | **Test 9** | **Test 10** |
|---|---|---|---|---|---|---|---|---|---|---|
| Share 1 | T | F | T | T | T | T | F | F | T | T |
| Share 2 | T | T | F | T | T | T | F | F | F | T |
| Share 3 | T | T | T | F | T | T | F | T | F | T |
| **Certified** | Yes | No | No | No | Yes | Yes | No | No | No | Yes |

*4.4. Comparative analysis of proposed OMTAP vs. existing methods*

In the realm of VC, the selection of an appropriate method plays a pivotal role in determining the security, efficiency, and quality of encrypted image transmission. This study delves into a meticulous feature analysis, as illustrated in Table 3.

**Table 3.** Feature analysis of proposed CRVC vs. Existing methods.

| **Features** | **[11]** | **[21]** | **OMTAP** |
|---|---|---|---|
| Secret information type | Grayscale | Grayscale | Color |
| Stacking type | XOR | OR | XOR |
| Shares type | Random | Semantic | Semantic |
| Integrity verification by | 3rd party system | Additional share | Self-share |
| Verification type | Validation | Reliability | Reliability |
| Computational cost | High | Low | Low |
| Quality of the reconstructed image | Low | High | Identical |

In contrast to existing methods, Table 3 presents a detailed feature analysis of the proposed OMTAP. The categorization encompasses various aspects crucial for evaluating the performance and characteristics of the cryptographic techniques. The proposed OMTAP distinguishes itself by dealing with color secret information, utilizing XOR stacking for share combination, generating semantic shares, implementing self-share verification for integrity, and emphasizing reliability in the verification process. In comparison, existing methodologies focus on grayscale secret information, employ XOR and OR stacking, generate random and semantic shares, and rely on a 3rd party system and an additional share for integrity verification. Notably, OMTAP achieves a balance between low computational cost and identical quality reconstruction, setting it apart from [11], with its high computational cost resulting in low-quality reconstruction, and [21], with its low computational cost and high-quality reconstruction. The table provides a comprehensive insight into the distinctive

features of OMTAP, positioning it as a promising and efficient VC method for secure image transmission and reconstruction.

## 5. Conclusions

In the dynamic realm of VC, the introduction of the OMTAP marks a significant stride towards achieving enhanced security and data integrity. As digital landscapes become increasingly complex, the need for robust, efficient, and adaptive cryptographic methods intensifies. Through rigorous evaluations and comparative assessments, OMTAP has showcased its prowess to encrypt grayscale secret images using color cover images, ensuring both fidelity and safety. Its distinct approach, which emphasizes multi-tiered authentication and advanced integrity checks, sets it apart from existing methodologies, promising not just theoretical excellence but practical applicability across diverse sectors. The protocol's resilience against potential tampering, combined with its adaptability to various image formats, further underscores its potential to reshape the visual cryptographic landscape. As we conclude, it's evident that OMTAP doesn't merely aim to address the current challenges in the field, but also anticipates and prepares for future demands, thus making it a cornerstone in the evolution of visual data security.

## Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

## Conflict of interest

The authors declare there is no conflict of interest.

## References

1. A. Akanksha, H. Garg, S. Shivani, Privacy protection of digital images using watermarking and QR code-based visual cryptography, *Adv. Multimedia*, **2023** (2023). https://doi.org/10.1155/2023/6945340
2. M. Naor, A. Shamir, Visual cryptography, in *Advances in Cryptology—EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques Perugia*, (1995), 1–12. https://doi.org/10.1007/BFb0053419
3. F. Aswad, I. Salman, S. Mostafa, An optimization of color halftone visual cryptography scheme based on bat algorithm, *J. Intell. Syst.*, **30** (2021), 816–835.https://doi.org/10.1515/jisys-2021-0042
4. A. J. Blesswin, G. S. Mary, S. M. Kumar, Secured communication method using visual secret sharing scheme for color images, *J. Internet Technol.*, **22** (2021), 803–810.
5. E. Çiftci, E. Sümer, A novel steganography method for binary and color halftone images, *Peer J. Comput. Sci.*, **8** (2022), 1062. https://doi.org/10.7717/peerj-cs.1062

6. G. S. Mary, A. J. Blesswin, S. M. Kumar, Self-authentication model to prevent cheating issues in grayscale visual secret sharing schemes, *Wirel. Pers. Commun.*, **125** (2022), 1695–1714. https://doi.org/10.1007/s11277-022-09628-8
7. G. Ateniese, C. Blundo, A. De Santis, D. R. Stinson, Extended capabilities for visual cryptography, *Theor. Comput. Sci.*, **250** (2001), 143–161. https://doi.org/10.1016/S0304-3975(99)00127-9
8. I. F. Elashry, O. S. Faragallah, A. M. Abbas, S. El-Rabaie, F. E. A. El-Samie, A new method for encrypting images with few details using rijndael and RC6 block ciphers in the electronic code book mode, *Inf. Secur. J.*, **21** (2012), 193–205. https://doi.org/10.1080/19393555.2011.654319
9. J. L. Sian, H. C. Wei, A probabilistic model of visual cryptography scheme with dynamic group, *IEEE Trans. Inf. Forensics Secur.*, **7** (2012), 197–207. https://doi.org/10.1109/TIFS.2011.2167229
10. C. C. Lin, W. H. Tsai, Visual cryptography for gray-level images by dithering techniques, *Pattern Recognit. Lett.*, **24** (2003), 349–358. https://doi.org/10.1016/S0167-8655(02)00259-3
11. A. J. Blesswin, P. Visalakshi, Optimal visual secret sharing on electrocardiography images for medical secret communications, *Int. J. Control Theory Appl.*, **9** (2016), 1055–1062.
12. Q. Wang, A. J. Blesswin, T. Manoranjitham, P. Akilandeswari, G. S. Mary, S. Suryawanshi, A. C. E. Karunya, Securing image-based document transmission in logistics and supply chain management through cheating-resistant visual cryptographic protocols, *Math. Biosci. Eng.*, **20** (2023), 19983–20001. https://doi.org/10.3934/mbe.2023885
13. A. J. Blesswin, G. S. Mary, S. M. M. Kumar, Multiple secret image communication using visual cryptography, *Wireless Pers. Commun.*, **122** (2022), 3085–3103. https://doi.org/10.1007/s11277-021-09041-7
14. S. Gao, R. Wu, X. Wang, J. Wang, Q. Li, C. Wang, et al., A 3D model encryption scheme based on a cascaded chaotic system, *Signal Process.*, **202** (2023), 108745. https://doi.org/10.1016/j.sigpro.2022.108745
15. G. S. Mary, S. M. M. Kumar, Secure grayscale image communication using significant visual cryptography scheme in real-time applications, *Multimedia Tools Appl.*, **79** (2020), 10363–10382. https://doi.org/10.1007/s11042-019-7202-7
16. A. J. Blesswin, P. Visalakshi, A novel visual image confirmation (VIC) protocol using visual cryptography for securing ubiquitous bluetooth mobile communications, *Res. J. Appl. Sci.*, **9** (2014), 503–510. https://dx.doi.org/10.36478/rjasci.2014.503.510
17. J. S. Pan, T. Liu, H. M. Yang, B. Yan, Visual cryptography scheme for secret color images with color QR codes, *J. Vis. Commun. Image Representation*, **82** (2021), 103405. https://doi.org/10.1016/j.jvcir.2021.103405
18. Y. Cheng, Z. Fu, B. Yu, Improved visual secret sharing scheme for QR code applications, *IEEE Trans. Inf. Forensics Secur.*, **13** (2018), 2393–2403. https://doi.org/10.1109/TIFS.2018.2819125
19. S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, X. Tang, EFR-CSTP: Encryption for face recognition based on the chaos and semi-tensor product theory, *Inf. Sci.*, **621** (2023), 766–781. https://doi.org/10.1016/j.ins.2022.11.121
20. Y. Ren, F. Liu, T. Guo, R. Feng, D. Lin, Cheating prevention visual cryptography scheme using Latin square, *IET Inf. Secur.*, **11** (2017), 211–219. https://doi.org/10.1049/iet-ifs.2016.0126
21. G. S. Mary, A. J. Blesswin, S. M. M. Kumar, A self-verifiable computational visual cryptographic protocol for secure two-dimensional image communication, *Meas. Sci. Technol.*, **30** (2019), 125404. https://doi.org/10.1088/1361-6501/ab2faa

22. D. Zhang, L. Ren, M. Shafiq, Z. Gu, A privacy protection framework for medical image security without key dependency based on visual cryptography and trusted computing, *Comput. Intell. Neurosci.*, **2023** (2023), 6758406. https://doi.org/10.1155/2023/6758406
23. A. J. Blesswin, P. Visalakshi, A new semantic visual cryptographic protocol (SVCP) for securing multimedia communications, *Int. J. Soft Comput.*, **10** (2015), 175–182. https://dx.doi.org/10.36478/ijscomp.2015.175.182
24. R. Wu, S. Gao, X. Wang, S. Liu, Q. Li, U. Erkan, et al., AEA-NCS: An audio encryption algorithm based on a nested chaotic system, *Chaos Solitons Fractals*, **165** (2022), 112770. https://doi.org/10.1016/j.chaos.2022.112770
25. N. Rani, S. R. Sharma, V. Mishra, Grayscale and colored image encryption model using a novel fused magic cube, *Nonlinear Dyn.*, **108** (2022), 1773–1796. https://doi.org/10.1007/s11071-022-07276-y
26. M. Z. Salim, A. J. Abboud, R. Yildirim, A visual cryptography-based watermarking approach for the detection and localization of image forgery, *Electronics*, **11** (2022), 136. https://doi.org/10.3390/electronics11010136
27. A. Sherine, G. Peter, A. A. Stonier, K. Praghash, V. Ganji, CMY color spaced-based visual cryptography scheme for secret sharing of data, *Wireless Commun. Mob. Comput.*, **2022** (2022), 1–12. https://doi.org/10.1155/2022/6040902
28. L. Wang, B. Yan, H. M. Yang, J. S. Pan, Flip extended visual cryptography for gray-scale and color cover images, *Symmetry*, **13** (2020), 65. https://doi.org/10.3390/sym13010065
29. X. Wu, C. N. Yang, Probabilistic color visual cryptography schemes for black and white secret images, *J. Visual Commun. Image Representation*, **70** (2020), 102793. https://doi.org/10.1016/j.jvcir.2020.102793
30. S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, C. Wang, et al., Asynchronous updating boolean network encryption algorithm, *IEEE Trans. Circuits Syst. Video Technol.*, **33** (2023), 4388-4400. https://doi.org/10.1109/TCSVT.2023.3237136


AIMS Press