Journal of Autonomous Intelligence (2024) Volume 7 Issue 1
doi: 10.32629/jai.v7i1.1129

ORIGINAL RESEARCH ARTICLE

Error-induced inverse pixel visual cryptography for secure QR code communication

John Blesswin[1], Selva Mary[1,*], T. Gobinath[2], Maheshwari Divate[3], Catherine Esther Karunya A.[4], Alfiya Abid Shahbad[5], Deepak Patil[6], Shibani Raju S.[7]

[1] *Directorate of Learning and Development, SRM Institute of Science and Technology, Kattankulathur 603203, India*

[2] *Department of Computer Science and Engineering, Chettinad College of Engineering and Technology, Karur 639114, India*

[3] *Department of Information Technology, Dr. D. Y. Patil Institute of Technology, Pimpri 411018, India*

[4] *Department of Artificial Intelligence and Machine Learning, SNS College of Technology, Coimbatore 641035, India*

[5] *Department of Computer Engineering, Modern Education Society's College of Engineering, Pune 411001, India*

[6] *Department of Electronics & Telecommunication, Nutan Maharashtra Institute of Engineering and Technology, Talegaon, Pune 410507, India*

[7] *Department of Computer Science Engineering, Madras Institute of Technology, Chennai 600044, India*

*** Corresponding author:** Selva Mary, selvamaryg.rnd@gmail.com

ABSTRACT

The rapid proliferation of Quick Response (QR) codes in various applications, particularly in sensitive domains like banking and financial transactions, necessitates robust data protection measures. Visual cryptography techniques are used to encode confidential information into multiple shares called shadows, which are communicated to the receivers. The receiving side decodes the shadows by stacking them together physically or digitally. In this research, an innovative solution titled "Error-induced inverse pixel visual cryptography (EIIPVC) for secure QR code communication" is proposed to enhance the security. The proposed EIIPVC leverages complementary shadows and introduces controlled errors during the sharing process. This feature makes it exceedingly challenging for potential malpractice to access or tamper with the data, ensuring a higher level of security. In this research, a single grayscale secret source (GSS) image in the form of QR code is used. This research also contributes to improving traditional issues, such as the quality of the reconstructed image and pixel expansion. The experimental results demonstrate that the EIIPVC approach significantly ensures enhanced security, safeguarding the transmitted data against potential attacks. The quality of the reconstructed image is improved by minimizing the mean square error (MSE) value up to 5%, indicating its superiority in preserving the visual clarity.

Keywords: visual cryptography; QR code security; error-induced inverse pixel; grayscale secret; secret sharing

ARTICLE INFO

Received: 10 August 2023
Accepted: 1 September 2023
Available online: 10 October 2023

1. Introduction

QR codes have become increasingly prevalent in various applications, extending to sensitive domains like banking and financial transactions. As the reliance on QR codes grows, the need for robust data protection measures becomes paramount. The ease of generating and scanning QR codes makes them a convenient medium for transmitting data. However, their widespread adoption also exposes them to potential security vulnerabilities, necessitating enhanced security measures to safeguard against unauthorized access and tampering. Visual cryptography, a cryptographic technique that encodes confidential information into shadows, presents a promising

approach to secure communication. It operates on the principle of human visual perception, where decryption is facilitated through the human visual system without the need for complex computations. This unique attribute provides an inherent two-factor authentication, enhancing the security of the encoded data. Additionally, visual cryptography resists key-based attacks, alleviating the challenges associated with cryptographic key management[1]. Compared to traditional text-based cryptography, visual cryptography offers several advantages. Firstly, it allows for the secure sharing of confidential data without complex encryption algorithms, reducing the computational overhead. Secondly, it provides extended security, as decryption occurs visually, making it challenging for attackers to intercept the data. Moreover, the reliance on human visual perception ensures resistance to cryptanalysis techniques, further fortifying data confidentiality[2]. However, visual cryptography also comes with its own set of challenges. Reconstructing the original image from shadows may lead to visual degradation, compromising the visual clarity of the data. Additionally, the sharing process is vulnerable to pixel visibility, where the encoded information becomes partially or fully visible in individual shadows, compromising the data's confidentiality. To address the issues in QR code image communication using the traditional VC, an innovative solution, error-induced inverse pixel visual cryptography (EIIPVC) for secure QR code communication, is proposed to send a grayscale secret source (GSS) image. The proposed EIIPVC approach leverages complementary shadows and introduces controlled errors during the sharing process. By doing so, an additional layer of protection is incorporated, fortifying the confidentiality of the GSS. Unauthorized access and tampering become exceedingly challenging for potential adversaries, significantly enhancing the overall security of QR code communication is essential[3]. This research study's primary objectives are to propose the EIIPVC approach for secure GSS communication, implement and evaluate its effectiveness, and demonstrate its superiority over existing visual cryptography schemes and conventional security measures. The GSS is converted in to semantic in nature for better encryption. The grayscale semantic secret source (GSSS) image is encoded and are communicated. The research aims to improve the reconstructed secret semantic source RGSSS image's quality, ensuring data integrity and visual clarity during QR code communication[4]. Several metrics, such as mean squared error (MSE), peak signal-to-noise ratio (PSNR), universal image quality index (UIQI), mean absolute error (MAE), and structural similarity index (SSIM), are utilized to evaluate the performance of the EIIPVC[5]. These metrics allow for a comprehensive assessment of the reconstructed images' fidelity and quality, providing the proposed approach's effectiveness. Various attacks pose potential threats to the security of QR code communication, including brute force attacks, data interception, and tampering. The proposed EIIPVC approach aims to mitigate these attacks by enhancing the complexity of the encryption process, ensuring a higher level of security for sensitive information during QR code communication[6].

This research study aims to present an innovative and reliable solution, the EIIPVC, to strengthen data confidentiality in QR code-based communication. By addressing the pressing concerns related to QR code security and overcoming visual cryptography challenges, this research study seeks to foster increased trust and security in various domains relying on QR code-based communication. The proposed approach's efficacy and its potential to enhance the security of QR code communication are expected to contribute significantly to secure data transmission in modern communication systems.

2. Literature study

Several researchers have explored the application of visual cryptography techniques to enhance the security of QR codes in various domains, including banking and financial transactions. Chang et al.[3] proposed a novel QR code encryption scheme based on visual cryptography, which encodes secret information into multiple shadows for secure communication. Similarly, Pan et al.[7] introduced a reversible data hiding technique for QR codes using visual cryptography and histogram shifting, ensuring robust data protection. Visual cryptography has proven to be a promising approach to strengthen data confidentiality in QR code-

based communication. To overcome vulnerabilities in conventional QR code security measures, researchers have combined visual cryptography with watermarking techniques. Zhang et al.[8] presented a secure QR code authentication scheme using visual cryptography and watermarking, ensuring authenticity and integrity of the received data. The use of visual cryptography extends beyond QR codes, with several studies focusing on secure image communication. Ma et al.[9] introduced a robust visual cryptography scheme for images based on double random-phase encoding and interference-free techniques. Yao and Li[10] enhanced the reversible data hiding scheme for QR codes using visual cryptography, providing increased security for image transmission. Additionally, Liu and Huang[11] explored robust watermarking techniques for QR codes based on visual cryptography, ensuring the integrity of the embedded data. In the context of grayscale visual secret sharing schemes, researchers have proposed self-authentication models to prevent cheating issues. Selva Mary and Kumar[12] presented a self-verifiable computational visual cryptographic protocol for secure two-dimensional image communication, ensuring the authenticity of shadow images. Furthermore, Selva Mary et al.[13] developed a self-authentication model to counter cheating issues in grayscale visual secret sharing schemes, enhancing the overall security of the communication process. Wu et al.[14] proposed a secure and robust QR code watermarking scheme based on complementary visual cryptography, ensuring the confidentiality of watermarked data. Selva Mary and Manoj Kumar[15] introduced a secure grayscale image communication technique using significant visual cryptography in real-time applications, providing an additional layer of security for image transmission. John Blesswin et al.[16] presented a method for multiple secret image communication using visual cryptography, enabling secure transmission of multiple images. The technique ensures that secret images can only be revealed when the shadows are combined correctly, thereby preventing unauthorized access. Novel approaches have been proposed to secure QR code sharing using visual cryptography. Cheng et al.[17] introduced a novel secret sharing method based on QR code visual cryptography, enhancing the confidentiality of shared QR codes. Additionally, Guo et al.[5] proposed an innovative approach to QR code sharing, leveraging visual cryptography for secure communication. Zhao et al.[18] explored adaptive QR code watermarking schemes based on visual cryptography, providing robust protection against watermarking attacks. Researchers have explored complementary visual cryptography as an effective method to improve security in different applications[19,20].

The literature study demonstrates the significance of visual cryptography in enhancing QR code security and secure image communication. Researchers have proposed various approaches, including watermarking, self-authentication models, complementary visual cryptography, and adaptive techniques, to overcome the vulnerabilities of conventional QR code security measures. The proposed research study on EIIPVC aims to further enhance QR code security by leveraging error-induced inverse pixel methodologies, ensuring confidentiality and integrity in sensitive domains such as banking and financial transactions.

3. Proposed methodology

In the proposed error-induced inverse pixel visual cryptography (EIIPVC) methodology, the primary mechanism involves transmitting a secret grayscale source image GSS from the sender to the receiver. This transmission doesn't include the direct sharing of the actual image. Instead, the secret image is divided and encoded into shares or 'shadows'. Each of these shadows carries portions of the encoded data from the secret image, ensuring that none individually reveals any secret information about the original content. Transmitting these shadows is crucial, especially since they traverse through open communication channels. Due to their open nature, these channels are inherently susceptible to various security threats, making the shadows vulnerable to interception or tampering[21]. Despite the shadows being fragments, ensuring their secure transmission is vital because, in the hands of adversaries with the right tools, they could retrieve or infer information about the secret image. Upon reaching the receiver's end, the process of decryption begins. VC doesn't involve traditional decryption keys or algorithms[22,23]. Instead, the receiver takes all the received

shadows and digitally stacks or overlays them in a specific sequence. This stacking process, as governed by the principles of visual cryptography, ensures that the combined data from the shadows converge to recreate the original grayscale secret image[24,25]. The architecture of the EIIPVC has been illustrated in **Figure 1**. This figure lays out each step, from the initial encoding of the secret image into shadows at the sender's end, through the transmission phase and finally, the stacking and decryption at the receiver's end. It offers a visual guide to the flow of data and the transformations it undergoes in the EIIPVC methodology.

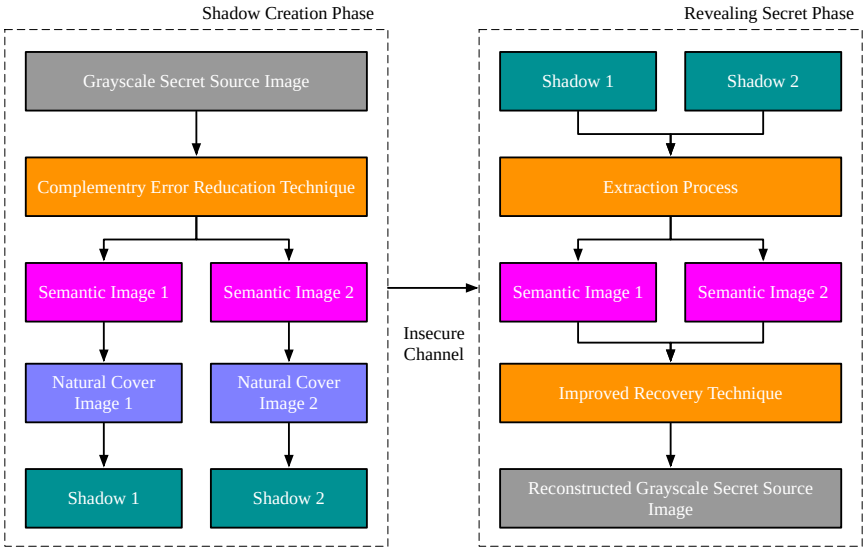


Figure 1. Architecture of proposed EIIPVC.

In this section the shadow creation phase and revealing secret image phase is explained.

3.1. Shadow creation phase

The step by step process of the shadow creation phase is as follows:

Step1: The proposed EIIPVC uses grayscale secret source image (GSS) divided into pixels to generate a controlled error using Equation (1). The pixel separation is shown in **Figure 2**.

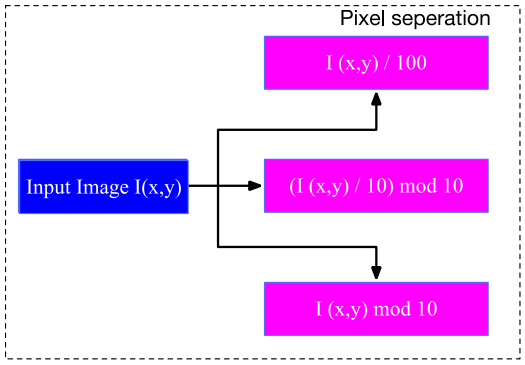


Figure 2. Pixel separation process.

$$\mathrm{GSS}_{x,y} = \left\langle \frac{\mathrm{GSS}_{x,y}}{100} \middle| \mathrm{mod}\left(\frac{\mathrm{GSS}_{x,y}}{10}, 10\right) \middle| \mathrm{mod}\left(\mathrm{GSS}_{x,y}, 10\right) \right\rangle \quad (1)$$

where $\mathrm{GSS}_{x,y} = \{w_1|w_2|w_3\}$.

Step 2: The controlled error is then used to generate the grayscale semantic secret image (GSSS) using the Equations (2)–(5). The GSSS generation is shown in **Figure 3**.

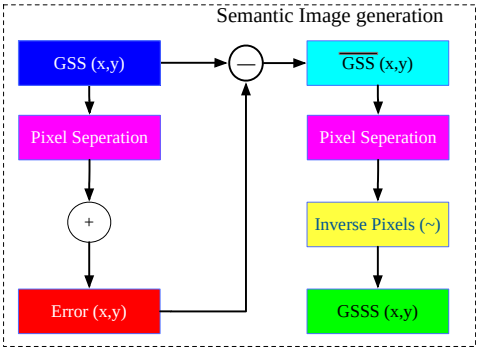


Figure 3. Grayscale semantic secret image generation.

$$\text{Error}_{x,y} = w_1 + w_2 + w_3 \tag{2}$$

$$\overline{\text{GSS}}_{x,y} = \text{GSS}_{x,y} - \text{Error}_{x,y} \tag{3}$$

$$\text{GSSS1}_{x,y} = \overline{v_2} \tag{4}$$

$$\text{GSSS2}_{x,y} = \overline{v_3} \tag{5}$$

where $\overline{\text{GSS}}_{x,y} = \{v_1|v_2|v_3\}$.

Step 3: The generated GSSS1 and GSSS2 are embedded with two natural grayscale cover images (NCC) using LSB embedding system as given in Equations (6) and (7) to generate the shadows (*S*1, *S*2). Where $\text{NCC1}_{x,y} = \{n_1|n_2|n_3\}$ and $\text{NCC2}_{x,y} = \{m_1|m_2|m_3\}$[21].

$$S1_{x,y} = \{n_1|n_2|\text{GSSS1}_{x,y}\} \tag{6}$$

$$S2_{x,y} = \{m_1|m_2|\text{GSSS2}_{x,y}\} \tag{7}$$

The shadows *S*1, *S*2 are communicated to the receiver end. The revealing secret phase is explained in the next section.

3.2. Revealing secret phase

In the revealing secret phase the shadows are collected from the sender side and are stacked digitally.

Step 1: Reception of shadows: The receiver first receives the shadows *S*1 and *S*2 that were communicated from the sender.

Step 2: Extraction of GSSS components: The receiver will extract the grayscale semantic secret image (GSSS) components GSSS1 and GSSS2 from the shadows *S*1 and *S*2 respectively. This is done using the reverse process of the LSB embedding system using Equations (8) and (9).

$$\text{GSSS1}_{x,y} = \text{mod}(S1_{x,y}, 10) \tag{8}$$

$$\text{GSSS2}_{x,y} = \text{mod}(S2_{x,y}, 10) \tag{9}$$

Step 3: Improved error recovery techniques: Only the part of the GSS has been communicated via shadows. At the revealing phase, the new key is generated from the received shadows using Equation (10).

$$\text{GSSS3}_{x,y} = th - \left(\overline{\text{GSSS1}}_{x,y} + \overline{\text{GSSS2}}_{x,y}\right) \tag{10}$$

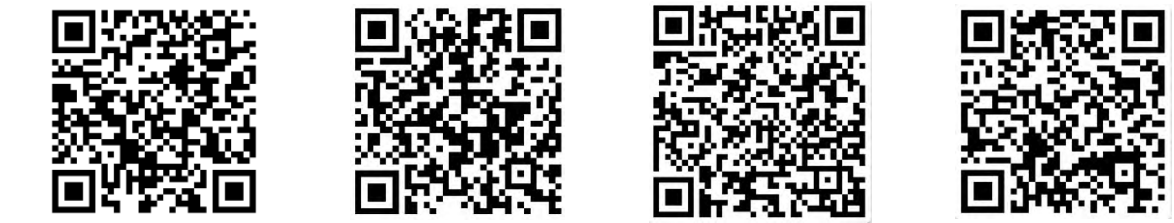
Step 4: Reconstruction of secret semantic image (RGSSS): Now, the receiver will use the extracted $\text{GSSS1}_{x,y}$ and $\text{GSSS2}_{x,y}$ to reconstruct the $\text{RGSSS}_{x,y}$ using Equation (10), the receiver can compute:

$$\text{RGSSS}_{x,y} = \text{GSSS3}_{x,y} \times 100 + \overline{\text{GSSS2}}_{x,y} \times 10 + \overline{\text{GSSS1}}_{x,y} \tag{11}$$

This is a simplification, as the exact relation might need more information than provided. However, the key idea is to use the extracted GSSS components to reconstruct the semantic image. The objective of the revealing secret phase is to retrieve the GSSS image in the receiver end. The revealed RGSSS using Equation (11) is compared with the original secret source image GSS, GSSS and are compared for its efficiency.

4. Implementation and result analysis

The proposed error-induced inverse pixel visual cryptography (EIIPVC) methodology, with its intricate phases of shadow creation and secret revelation, is promised to be a secure and efficient method for transmitting grayscale images. A comprehensive implementation and result analysis has been embarked upon to validate these claims and ascertain the methodology's real-world applicability. MATLAB R2023a (9.14.0), a high-performance language known for its technical computing capabilities, was utilized to implement the EIIPVC methodology. An intuitive environment is offered by MATLAB, along with a plethora of in-built functions that expedite the development and testing processes[24]. QR code images were chosen as test subjects for this research. This choice was made strategically, considering the intricate patterns of QR codes and their widespread use in today's digital world. The success of the EIIPVC methodology is gauged by its ability to recreate the grayscale secret source image (GSS) with the utmost fidelity. In this research study, more than 100 sample QR code images have been tested and the results were recorded. For illustrations, 6 test images results were shown in this paper. The sample secret images are shown in **Figures 4** and **5** shows the sample natural cover images used for the study.



I am Dr. Selva Mary, assistant professor, SRMIST, India. **(a)**

I am Dr. John Blesswin, associate professor, SRMIST, India. **(b)**

Error-induced inverse pixel visual cryptography for secure QR code communication. **(c)**

Name: XXXXXX. DOB: XX/XX/XX. Account No: XXXXXXXX. **(d)**

Figure 4. Sample test secret source images.

Lena image **(a)**

Barbora **(b)**

Animal **(c)**

Einstein **(d)**

Figure 5. Sample natural cover images.

To quantify this fidelity, a set of widely-accepted metrics: PSNR, MSE, MAE, UIQI, and SSIM, were employed. Each of these metrics offers a unique perspective on the quality and accuracy of the revealed image compared to the original secret source image using Equations (12)–(16).

PSNR (peak signal-to-noise ratio): A metric that measures the quality of a reconstructed image compared to the original image. A higher PSNR indicates better quality. PSNR is derived using Equation (12).

$$\mathrm{PSNR} = 10 \times \log_{10}\left(\frac{\mathrm{MAX}_I^2}{\mathrm{MSE}}\right) \tag{12}$$

where MAX_I is the maximum pixel value of the image. For a grayscale image, it is 255. MSE is the mean squared error.

MSE (mean squared error): The average of the squared differences between the source and the revealed image. Lower MSE indicates better similarity.

$$\mathrm{MSE} = \frac{1}{H \times W} \sum_{x=1}^{H} \sum_{y=1}^{W} [\mathrm{GSS}(x, y) - \mathrm{RGSSS}(x, y)]^2 \tag{13}$$

where GSS is the original image and RGSSS is the reconstructed image.

MAE (mean absolute error): The average of the absolute differences between the source and the revealed image.

$$\mathrm{MAE} = \frac{1}{H \times W} \sum_{x=1}^{H} \sum_{y=1}^{W} |\mathrm{GSS}(x, y) - \mathrm{RGSSS}(x, y)| \tag{14}$$

UIQI (universal image quality index): A metric that considers luminance, contrast, and structure components between the two images.

$$\mathrm{UIQI} = \frac{4 \times \sigma_{\mathrm{GSS,RGSSS}} \times \mu_{\mathrm{GSS}} \times \mu_{\mathrm{RGSSS}}}{\sigma_{\mathrm{GSS}}^2 + \sigma_{\mathrm{RGSSS}}^2 + (\mu_{\mathrm{GSS}}^2 + \mu_{\mathrm{RGSSS}}^2)} \tag{15}$$

where μ denotes mean, σ denotes standard deviation, and $\sigma_{\mathrm{GSS,RGSSS}}$ is the cross covariance of images GSS and RGSSS.

SSIM (structural similarity index measure): A metric that measures the similarity between two images. It's designed to improve on traditional methods like PSNR and MSE by considering changes in structural information, luminance, and texture.

$$\mathrm{SSIM}(\mathrm{GSS}, \mathrm{RGSS}) = \frac{(2\mu_{\mathrm{GSS}}\mu_{\mathrm{RGSSS}} + C_1)(2\sigma_{\mathrm{GSS,RGSSS}} + C_2)}{(\mu_{\mathrm{GSS}}^2 + \mu_{\mathrm{RGSSS}}^2 + C_1)(\sigma_{\mathrm{GSS}}^2 + \sigma_{\mathrm{RGSSS}}^2 + C_2)} \tag{16}$$

where C_1 and C_2 are constants, μ is the average, σ is the variance, and $\sigma_{\mathrm{GSS,RGSSS}}$ is the covariance of GSS and RGSSS[25].

4.1. Analysis

In the intricate tapestry of cryptographic methodologies, the quality of outcomes is paramount. For the proposed error-induced inverse pixel visual cryptography (EIIPVC), the significance transcends beyond the conventional, as it rests not only on the fidelity of the reconstructed image but also on the quality of the individual shares. The quality of these shares and the resultant image is crucial, as it directly impacts the user's trust in the system and the overall usability of the methodology. Moreover, addressing and reducing pixel expansion issues is vital to ensure that the revealed image retains its original clarity and details.

Beyond the perceptual quality lies the bedrock of security. The EIIPVC methodology, through its innovative processes, ensuring that secret images remain impervious to unauthorized decryption. This enhancement in security is pivotal, especially in an era where cyber threats loom significant and data breaches are frequent. It ensures that even if shadows are intercepted, deciphering the original content without the complete set becomes an insurmountable challenge.

Equally significant is the complexity analysis. In many cryptographic systems, the revealing or decryption phase often involves intricate computations, which could be resource-intensive and time-consuming. However, with EIIPVC, a distinctive advantage emerges. The revealing phase has been designed to eschew complex calculations, streamlining the process and reducing the overall computational complexity[12,13]. This efficiency expedites the image revelation process and ensures that the methodology remains accessible even on devices with limited computational resources. In essence, the result analysis delves deep into evaluating the quality, security, and efficiency of the EIIPVC methodology, providing a comprehensive assessment of its real-world applicability and robustness. **Figure 6** shows the lifecycle of the secret QR code source image in the proposed EIIPVC.

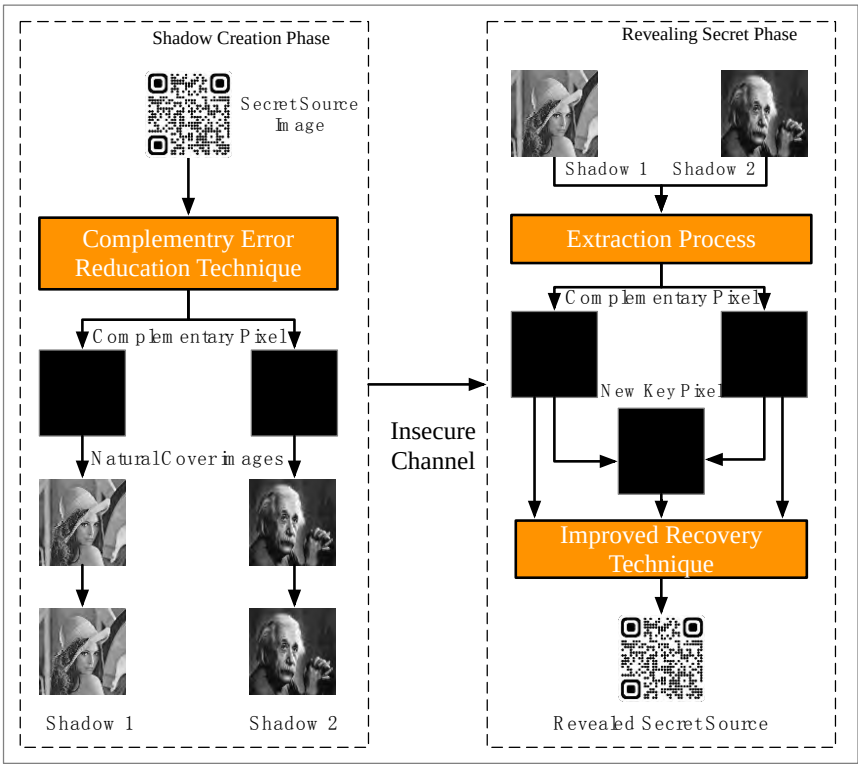


Figure 6. Life cycle of QR code source image in the proposed EIIPVC.

4.1.1. Security analysis

The primary objective of this research is to safeguard the grayscale secret source image (GSS) during its transmission across open, inherently vulnerable communication channels. The novel approach of EIIPVC encrypts pixel information, transmitting only a fraction of the data. This data undergoes encryption and is subsequently embedded within cover images. A unique key shadow is formulated from the received shadows at the revealing endpoint. Only through the digital amalgamation of all these shadows is the source image revealed.

Key security considerations include:

- Transmission security: Even if malicious attackers intercept all shares during communication, the absence of the revealing phase prevents the generation of the key shadow, rendering the source image unrecoverable.
- Participant integrity: Should any participant attempt deceit by altering or providing a counterfeit shadow image, the key shadow generated will fail to reconstruct the source image.
- Shadow dependence: The methodology's design is such that the absence or loss of even a single shadow during transmission renders the secret unrevealed.
- Shadow indecipherability: Individual shadows offer no hint of the secret within.
- Natural concealment: Embedding shadows within cover images ensures they resemble natural images, thus reducing suspicion regarding the presence of embedded secrets.

4.1.2. Quality analysis

1) The inherent quality of images is pivotal in secure communication. Images of subpar quality can inadvertently draw malicious entities. In EIIPVC, shadows are juxtaposed against cover images for analytical purposes, with results presented in **Table 1**.

The outcomes highlight that shadows consistently display PSNR values exceeding 30 dB, comfortably within acceptable quality thresholds. It's widely recognized that a PSNR value greater than 25 dB indicates satisfactory image quality.

Table 1. Cover images vs. shadow images.

Test image	Size	PSNR	UIQI	MAE	SSIM
QR 1	256 × 256	32.45	0.91	0.25	0.92
QR 2	400 × 400	25.09	0.92	0.41	0.87
QR 3	512 × 512	30.92	0.82	1.28	0.756
QR 4	256 × 256	27.9	0.84	1.27	0.73
QR 5	400 × 400	25.59	0.98	0.94	0.87
QR 6	512 × 512	29.84	0.84	1.4	0.79

2) The quality of the reconstructed secret source image is juxtaposed against the original, with performance metrics outlined in **Table 2**.

Table 2. Test images vs. revealed secret images.

Test image	Size	PSNR	UIQI	MAE	SSIM
QR 1	256 × 256	33.45	0.98	0.77	0.92
QR 2	400 × 400	31.34	0.97	0.32	0.96
QR 3	512 × 512	29.07	0.9	1.32	0.87
QR 4	256 × 256	26.54	0.87	1.23	0.79
QR 5	400 × 400	25.59	0.82	1.07	0.84
QR 6	512 × 512	24.88	0.84	0.97	0.91

3) Results shown in **Figure 7** accentuate that while error induction during the shadow creation phase does marginally diminish the quality of the revealed image, it still sustains an impressive quality rating of up to 35 dB.

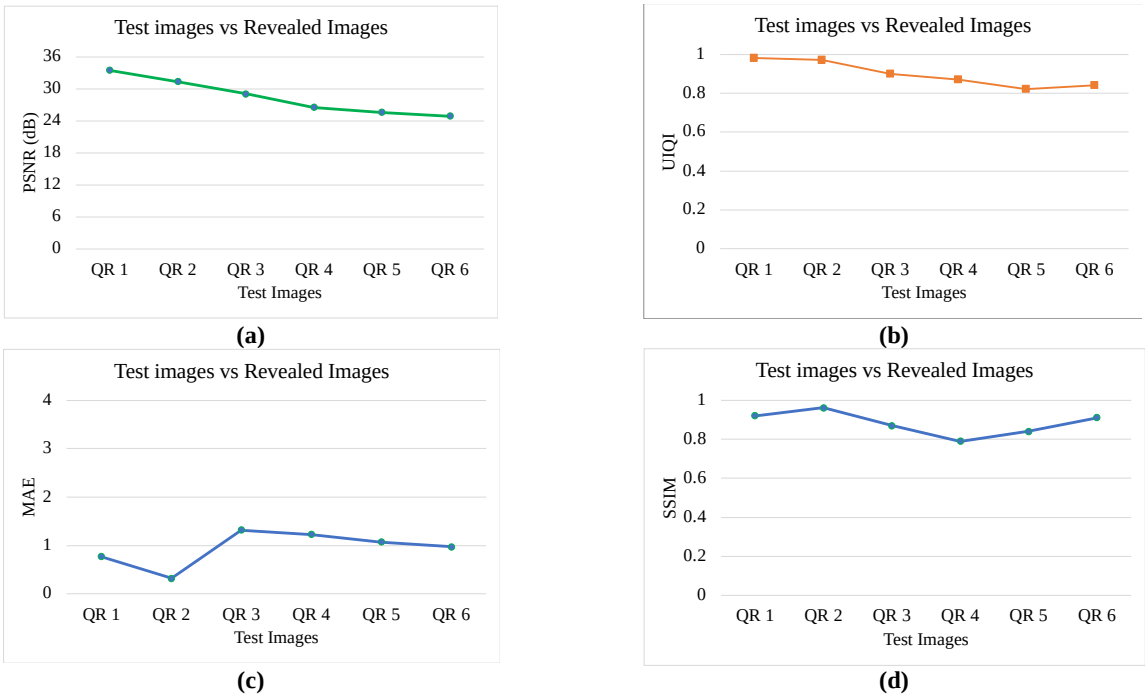


Figure 7. Quality analysis of test images vs. revealed images.

Figure 7 shows that the proposed EIIPVC produces acceptable range of revealed image.

4.1.3. Pixel expansion

EIIPVC employs complementary pixel values with the LSB embedding technique to discreetly incorporate data within cover images. This strategy circumvents any increment in pixel values, effectively addressing pixel expansion issues. By eliminating these issues, the quality and security of the shared images are bolstered.

In this research, the performance of the error-induced inverse pixel visual cryptography (EIIPVC) methodology was examined. The primary focus was on ensuring that the grayscale secret source image (GSS) was transmitted securely, especially over channels that might be insecure. From the security analysis, several key findings were highlighted: (i) When shadows (parts of the secret image) were intercepted, they were found to be useless for unauthorized viewing without the unique revealing process. (ii) Resistance against deceptive alterations by participants was demonstrated by the methodology. (iii) It was ensured by the design that the absence of even one shadow made the entire secret image unrecoverable. (iv) By embedding shadows in ordinary images, their cryptographic nature was effectively hidden. In the quality analysis: (i) Shadows were consistently observed to have satisfactory PSNR values, indicating their good quality. (ii) Despite intentional modifications made during shadow creation, the quality of the revealed image was found to be impressive, with ratings of up to 35 dB. Moreover, the common issue of pixel expansion was successfully addressed in this research. By employing complementary pixel values and the LSB embedding technique, escalation in pixel values was prevented, ensuring both quality and security.

5. Conclusion

In the evolving landscape of cryptography, innovative methodologies are continually being sought to bolster security in the digital communication era where data vulnerability is a constant concern. In this research, the potential of the error-induced inverse pixel visual cryptography (EIIPVC) methodology was deeply explored, highlighting its capabilities as a robust cryptographic mechanism. The capacity of EIIPVC to safeguard the grayscale secret source image (GSS) during transmission, especially across potentially insecure channels, was meticulously assessed. Through the security analysis, resilience against unauthorized decryption was underscored, even when shadows were intercepted. It was observed that the methodology's design effectively prevents any deceptive alterations and ensures that the absence or loss of even one shadow leaves the secret image unrevealed. On the front of image quality, concerns were addressed effectively. Satisfactory quality was consistently exhibited by the shadows, and even with intentional error inductions, impressive fidelity was displayed by the revealed image. Notably, the prevalent issue of pixel expansion was successfully tackled in this research, marking a significant stride in ensuring image integrity. In essence, through this analysis, the theoretical foundations of the EIIPVC methodology were not only validated, but its empirical strength was also confirmed. It is positioned as a testament to the advancements in visual cryptography, presenting a promising avenue for secure image transmission in modern digital communication.

Author contributions

Conceptualization, JB and SM; methodology, SM; software, JB; validation, TG, MD and AAS; investigation, CEKA and SRS; resources, DP; writing—original draft preparation, SM; writing—review and editing, DP; visualization, TG. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. John Blesswin A, Raj C, Sukumaran R, et al. Enhanced semantic visual secret sharing scheme for secure image

communication. *Multimedia Tools and Applications* 2020; 79: 17057–17079. doi: 10.1007/s11042-019-7535-2
2. Tan L, Lu Y, Yan X, et al. XOR-ed visual secret sharing scheme with robust and meaningful shadows based on QR codes. *Multimedia Tools and Applications* 2020; 79: 5719–5741. doi: 10.1007/s11042-019-08351-0
3. Chang CC, Chang YH, Lai JS. Enhanced QR code authentication using visual cryptography and watermarking techniques. *International Journal of Pattern Recognition and Artificial Intelligence* 2019; 33(9): 1950028.
4. Das A, Kundu S, Dey A. An enhanced security scheme for QR code using visual cryptography. *Journal of Information Security and Applications* 2020; 53: 102477.
5. Guo X, Xu H, Chen W, Wang J. A novel approach to QR code sharing based on visual cryptography. *Multimedia Tools and Applications* 2019; 78(11): 14671–14686.
6. Hsieh YH, Hwang MS. QR code authentication using visual cryptography and multiple watermarks. *Multimedia Tools and Applications* 2018; 77(15): 19759–19774.
7. Pan Y, Zhu X, Qi C. A novel reversible data hiding technique for QR code based on visual cryptography and histogram shifting. *Multimedia Tools and Applications* 2019; 78(3): 3133–3154.
8. Zhang X, Yang Y, Yang C, Zhao J. A privacy-preserving QR code authentication system based on visual cryptography and blockchain. *Journal of Network and Computer Applications* 2020; 160: 102523.
9. Ma Y, Chen Z, Zhou Y, Xie Y. A robust visual cryptography scheme for QR code based on double random-phase encoding and interference-free technique. *Information Sciences* 2019; 480: 78–94.
10. Yao Q, Li B. Enhanced reversible data hiding scheme for QR codes based on visual cryptography. *Multimedia Tools and Applications* 2019; 78(11): 14649–14670.
11. Liu X, Huang Q. Robust watermarking of QR codes based on visual cryptography. *Digital Signal Processing* 2019; 92: 190–198.
12. Selva Mary G, Kumar SM. A self-verifiable computational visual cryptographic protocol for secure two-dimensional image communication. *Measurement Science and Technology* 2019; 30(12): 125404. doi: 10.1088/1361-6501/ab2faa
13. Selva Mary G, Blesswin AJ, Kumar SM. Self-authentication model to prevent cheating issues in grayscale visual secret sharing schemes. *Wireless Personal Communications* 2022; 125: 1695–1714. doi: 10.1007/s11277-022-09628-8
14. Wu Y, Liu W, Jiang C, Xu X. A secure and robust QR code watermarking scheme based on complementary visual cryptography. *IEEE Transactions on Circuits and Systems for Video Technology* 2021; 31(1): 46–58.
15. Selva Mary G, Manoj Kumar S. Secure grayscale image communication using significant visual cryptography scheme in real-time applications. *Multimedia Tools and Applications* 2020; 79: 10363–10382. doi: 10.1007/s11042-019-7202-7
16. John Blesswin A, Selva Mary G, Manoj Kumar S. Multiple secret image communication using visual cryptography. *Wireless Personal Communications* 2022; 122: 3085–3103. doi: 10.1007/s11277-021-09041-7
17. Cheng Y, Fu Z, Yu B. Improved visual secret sharing scheme for QR code applications. *IEEE Transactions on Information Forensics and Security* 2018;13(9): 2393–2403. doi: 10.1109/TIFS.2018.2819125
18. Zhao J, Yu W, Jiang H, Du J. An adaptive QR code watermarking scheme based on visual cryptography. *Multimedia Tools and Applications* 2020; 79(1–2): 1105–1122.
19. Fu Z, Cheng Y, Liu S, Yu B, A new two-level information protection scheme based on visual cryptography and QR code with multiple decryptions. *Measurement* 2019; 141: 267–276. doi: 10.1016/j.measurement.2019.03.080
20. Li-na Z, Chen-yu C, Xiao-yu Z, Wei W. Adaptive visual cryptography scheme design based on QR codes. *Mathematical Biosciences and Engineering* 2022; 19(12): 12160–12179. doi: 10.3934/mbe.2022566
21. Blesswin AJ, Visalakshi P. Secret sharing approach on electrocardiography with heart tone images using visual cryptography for secure healthcare communications. *Journal of Pure and Applied Microbiology* 2015; 9: 665–672.
22. Fu Z, Cheng Y, Yu B. Perfect recovery of XOR-based visual cryptography scheme. *Multimedia Tools and Applications* 2019; 78: 2367–2384. doi: 10.1007/s11042-018-6364-z
23. Wan S, Qi L, Yang G. Visual secret sharing scheme with (*n*, *n*) threshold for selective secret content based on QR codes. *Multimedia Tools and Applications* 2020; 79: 2789–2811. doi: 10.1007/s11042-019-08246-0
24. Blesswin AJ, Mary GS. Optimal grayscale visual cryptography using error diffusion to secure image communication. *International Journal of Control Theory Applications* 2015; 8(4): 1511–1519.
25. John Blesswin A, Selva Mary G, Suryawanshi S, et al. Secure transmission of grayscale images with triggered error visual sharing. *Journal of Autonomous Intelligence* 2023; 6(2): 957. doi: 10.32629/jai.v6i2.957