Journal of Autonomous Intelligence (2023) Volume 6 Issue 2
doi: 10.32629/jai.v6i2.957

ORIGINAL RESEARCH ARTICLE

Secure transmission of grayscale images with triggered error visual sharing

John Blesswin[1], Selva Mary[1,*], Shubhangi Suryawanshi[2], Vanita Kshirsagar[2], Sarika Pabalkar[3], Mithra Venkatesan[4], Catherine Esther Karunya[5]

[1] *Directorate of Learning and Development, SRM Institute of Science and Technology, Kattankulathur 603203, India*
[2] *Department of Computer Engineering, Dr. D. Y. Patil Institute of Technology, Pimpri 411018, India*
[3] *Department of Information Technology, Dr. D. Y. Patil Institute of Technology, Pimpri 411018, India*
[4] *Department of Electronics and Telecommunication, Dr. D. Y. Patil Institute of Technology, Pimpri 411018, India*
[5] *Department of Artificial Intelligence and Machine Learning, SNS College of Technology, Coimbatore 641035, India*
*** Corresponding author:** Selva Mary, selvamaryg.rnd@gmail.com

ABSTRACT

In the digital era, data transfer plays a crucial role in various industries such as banking, healthcare, marketing, and social media. Images are widely used as a means of communication. The presence of cyber attackers poses a significant risk to data integrity and security during transmission. According to the cost of data breach report 2021, the healthcare industry has experienced the highest costs associated with data breaches, highlighting the need for robust security measures. Visual cryptography (VC) is a technique used to secure image data during transmission. It involves encrypting the image and dividing it into shares, which are then communicated to the intended recipients. Each individual share does not reveal any classified information. At the destination, the shares are digitally combined to reconstruct the original image. When implementing VC, several factors need to be considered, including security, computational complexity, and the quality of the reconstructed image. In this paper, a new method called progressive meaningful visual cryptography (PMVC) is proposed for transferring secret images. The PMVC method introduces an error instance that triggers meaningful shares generation. The proposed method ensures the quality of the reconstructed image by achieving a peak signal-to-noise ratio (PSNR) of up to 37 dB.

Keywords: meaningful shares; single grayscale secret; triggered error; visual cryptography

ARTICLE INFO

Received: 11 July 2023
Accepted: 25 July 2023
Available online: 17 August 2023

1. Introduction

In today's digital world, images and documents are transmitted widely and rapidly via email, social networks and across the internet. Protecting the sensitivity and confidentiality of the documents and images has become the primary issue while transmission. The participants of the communication may not aware that the image is accessed by the third party or not. Cyber attackers take the advantage of the weakness of the network and security features and try to access the data. In medical industry, the protected health information (PHI) needs security. PHI includes patient's profile, health information, credit card details, medical images and other images. The health information privacy and accountability act (HIPAA) standards provide guidelines to healthcare practitioners to take steps to secure health information against security risks. Surveys say that healthcare organizations experienced the highest average cost of a data breach, for the eleventh year in a row.

In 1994, Naor and Shamir have introduced VC. Visual cryptography (VC) is the encryption method used to provide security to the images. This method encrypts the image and divide the image into number of shares. Individual shares do not reveal the secret. The shares are then distributed to the participants and are stacked together to reveal the secret[1]. The traditional VC uses the transparencies to encrypt the image and are stacked together to reveal the image. Individual or less number of shares do not reveal the image. The decryption method of traditional VC does not require complex calculations since the decryption is done by the human eyes only. The quality of the shares and the reconstructed images become the key issues. Later, the researchers have improved the decryption process by digitally stacking the shares and by simple XOR operations[2]. The cost of the decryption is less and the quality becomes the concern. Moreover, the simplicity and efficiency of the proposed PMVC method make it suitable for real-time applications and scenarios where quick and secure transmission of sensitive images is required. The use of simple arithmetic operations and the elimination of complex calculations in the decryption process contribute to the overall efficiency of the PMVC method. Overall, the proposed PMVC method addresses critical concerns in image and document transmission, including security, quality, authenticity, integrity, and efficiency. By incorporating error instances and progressive generation of meaningful shares, PMVC provides an enhanced level of security while ensuring the quality and integrity of the transmitted images. These advancements contribute to the overall goal of secure and reliable communication in today's digital landscape.

VC consists of two methods namely, share generation phase and revealing phase. In the share generation phase the image is encrypted and are divided into shares. Shares are the images that will be distributed to the participants of the transmission[3]. The share images carry the encrypted pixels of the secret image. In the revealing phase, all the shares are stacked together to reconstruct the original image. Initially, physical stacking of transparent share layers was done to reconstruct the image. Later the images were digitally stacked using XOR operations[4]. The VC takes two forms of schemes such as (n, n) VC which takes all the n shares to reveal the secret and (k, n) VC takes k out of n shares can reveal the secret[5].

Extended visual cryptography (EVCS) is a technique where all shares generated are meaningful and contain partial information about the original secret image. A halftone secret image is concealed within two camouflaged halftone images[6]. The gray level values of the pixels in these camouflaged images are adjusted to match the pixel values of the secret image. By overlaying these camouflaged images, the secret halftone image can be visually revealed using human eyes. Another scheme described intelligent pre-processing techniques to enhance the quality of the recovered image[7]. This pre-processing can also be beneficial for other EVCS schemes. However, these existing schemes primarily focus on gray level images, and there is a need for research on applying visual cryptography techniques to color images.

Intensive research work on VC schemes exploits the use of binary, grayscale and color images as secret image. Also, the issues raised from the research play a vital role for further study. Pixels are divided into subpixels to generate shares that raised pixel expansion issues. Due to the pixel expansion issues, the quality of the shares reduced. When a share image shared with lower quality attracts the MA[8,9]. This leads the security threat to the shares in the open communication. Also, from the lower quality shares the reconstructed image also losses its quality. To address these issues researchers have used to methods to reduce the pixel expansion problem which reduces the quality of the image by generating meaningful shares[10,11]. The meaningful shares were generated by embedding the encrypted pixel into other images. Individual share images look like the normal image and carry the encrypted data. Individual shares do not disclose the data[3,12]. Thus the quality of the shares also maintained. In order to prevent the cheating issues, when an authorized participant cheats with others, the revealed image loss its integrity. To address this issue, researchers use trusted third parties to compare the original and revealed image[6,7,13–15]. Additional share images have been used by the authors to verify the integrity issues. This process led to complex computations at the revealing.

From the literature study, the following objectives are drawn: The secured VC scheme must:

(i) Provide security to the share images.
(ii) Reconstruct the secret image with acceptable quality range, also increase the quality of the share images.
(iii) Reduce pixel expansion issues in share images.
(iv) Reduce complex computations at the revealing phase.

In this paper, a new PMVC method is proposed and the outcomes achieved through the proposed research is listed as follows:

(i) Secure transmission of grayscale secret image to the destination.
(ii) Quality of the share images is maintained and the reconstructed image quality is also improved and the shares are shared as meaningful grayscale images to provide additional security.
(iii) No pixel expansion while generating shares.
(iv) Simple arithmetic operations are used to reduce the computational complexity.

In this paper, section 2 shows the design of the proposed scheme and its algorithm, section 3 explains the implementation and working of the proposed scheme with the analysis of the proposed algorithms and test results obtained from the sample test images. Also, the comparative analysis with the existing algorithms also analysed. In section 4, the proposed scheme is summarized and concluded.

2. Design of proposed CPS

The proposed PMVC scheme is designed to transfer a single grayscale secret image to the destination as encrypted shares. The shares are decrypted at the destination to reveal the secret image. The encrypted shares are generated in the share generation module and the decryption is done in the revealing module of the scheme. **Figure 1** shows the architecture of the PMVC scheme. The PMVC scheme consists of two modules namely, share generation module and revealing module.

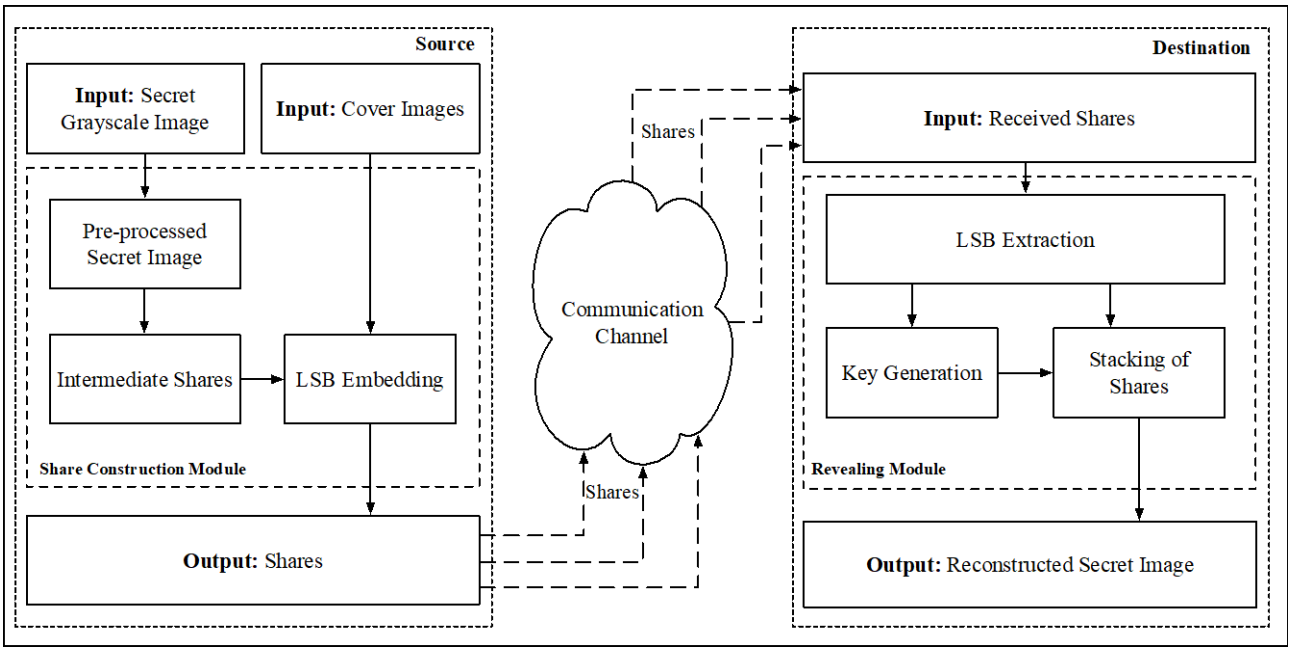

Figure 1. System architecture of proposed PMVC.

Figure 1 shows that the secret GSI is initially pre-processed to give meaningful progressive values to the pixels. This processing will help to generate meaningful shares. The proposed PMVC consists of two main

modules: share construction modules and revealing module. The PMVC aims to securely transmit a single gray scale image (GSI) from the sender to the receiver. The GSI has a size of R rows and C columns in a matrix format, with pixel values ranging from 0 to 255. The pre-processed secret image PSI is encrypted in the share construction module to generate share values. Using the cover images CI, the share values are covered and are generated meaningful shares at the source end.

At the receiver end, the shares are received from the participants. The encrypted pixel values are extracted from the shares using LSB extraction method. From the extracted values a new key share value is generated at the revealing module. Using the extracted share values and the generated key value, the secret pixel value is decrypted by digitally stacking the share values. The secret image can be reconstructed using the newly generated pixel value. If any of the share is altered or the participants cheated the share with fake share, the newly generated key value would not help to generate the secret image. The detailed working of the share generation module and the revealing module are explained below.

2.1. Share generation module

In this module, at the source the grayscale secret image and three grayscale cover images are used to encrypt and generate shares. The purpose of this module is to generate shares from the modified secret image while maintaining the security and confidentiality of the secret. By dividing the secret image into intermediate shares and embedding only a portion of the secret pixels within the cover images, the individual shares do not reveal the complete secret image (SI). This provides security to the shares and ensures that each share contains only partial information about the original secret image. At the destination, all the shares are collected from the participants to reveal the original secret image. The process of combining the shares and reconstructing the original image is typically done using appropriate techniques such as secret sharing or image reconstruction algorithms.

By triggering the secret pixels with error instances and clustering them based on their values, a meaningful image is generated from the modified secret image. This meaningful image contains clustered pixels that are similar in value, thereby creating a visual representation of the secret information. However, only a portion of the meaningful image pixels are embedded with the cover images to generate the shares, ensuring that the full secret is not revealed by any individual share. Overall, this algorithm ensures the generation of shares from a modified secret image while preserving the security and confidentiality of the original secret information.

The encryption process and the share construction are shown in Algorithm 1.

Algorithm 1 shows the working of the share construction phase.

Step 1: initially the SI is triggered with the errors (TE) to generate a modified pre-processed secret image (PSI).

Step 2: each pixel value of PSI is then divided into intermediate share pixel values $(IS1, IS2, IS3)$.

Step 3: to generate share $SI1$, a random key $(randomKey)$ is generated between $\{0, 1, 2\}$ and the $randomKey$ is embedded with the cover image $(CI1)$ using least significant bit (LSB) embedding technique.

Step 4: based on the $randomKey$, share $SI2\ and\ SI3$ are generated randomly from the $IS1, IS2\ and\ IS3$ using LSB embedding technique with the $CI2\ and\ CI3$.

The generated share images pixel ranges $SI1,\ SI2\ and\ SI3\ \in \{0, 1, 2, \ldots, 255\}$ and are communicated to the destination participants.

The secret pixels are triggered with the error instances which are calculated arithmetically. This triggered errors will form the clusters of pixels with similar values and generates a meaningful image. Part of the meaningful image pixels are embedded with the cover images to generate shares. Only part of the secret pixels

are converted as shares that provides security to the shares as the individual shares do not reveal the SI. At the destination all the shares are collected to reveal the secret.

Algorithm 1 Share Generation

1: $Input$: $Single\ Secret\ Image\ (SI)$
$Cover\ Images\ (CI^1, CI^2, CI^3)\ of\ size\ H \times W$

2: $Output$: $Share\ Images\ (SH^1, SH^2, SH^3) with\ of\ size\ H \times W$

3: $begin$:

4: $Foreach$ $a \leftarrow 1{:}H$

5: $Foreach$ $b \leftarrow 1{:}W$

6: $do\ until\ (a \leftarrow H\ and\ b \leftarrow W)$

7: $$Err_{a,b} \leftarrow \frac{SI_{a,b}}{100} + mod\left(\frac{SI_{a,b}}{10}, 10\right) + mod(SI_{a,b}, 10)$$

8: $$PI_{a,b} \leftarrow \begin{cases} SI_{a,b} - Err_{a,b}, & Err_{a,b} < 9 \\ SI_{a,b}, & Err_{a,b} = 9 \end{cases}$$

9: $$I1_{a,b} \leftarrow \frac{PI_{a,b}}{100}$$

10: $$I2_{a,b} \leftarrow mod\left(\frac{PI_{a,b}}{10}, 10\right)$$

11: $$I3_{a,b} \leftarrow mod(PI_{a,b}, 10)$$

12: $$Key_{a,b} \leftarrow randbetween(0,1)$$

13: $$S1_{a,b} \leftarrow {CI_{a,b}}^1 - mod\left({CI_{a,b}}^1, 10\right) + randKey_{a,b}$$

14: $$S2_{a,b} \leftarrow \begin{cases} {CI_{a,b}}^2 - mod\left({CI_{a,b}}^2, 10\right) + IS1_{a,b}, & randKey_{a,b} = 0 \\ {CI_{a,b}}^2 - mod\left({CI_{a,b}}^2, 10\right) + IS2_{a,b}, & randKey_{a,b} = 1 \end{cases}$$

15: $$S3_{a,b} \leftarrow \begin{cases} {CI_{a,b}}^3 - mod\left({CI_{a,b}}^3, 10\right) + IS2_{a,b}, & randKey_{a,b} = 0 \\ {CI_{a,b}}^3 - mod\left({CI_{a,b}}^3, 10\right) + IS3_{a,b}, & randKey_{a,b} = 1 \end{cases}$$

16: $End\ do$

17: $End\ For$

18: $End\ For$

19: End

2.2. Revealing module

In this module, all the received shares are collected and the secret pixel values are extracted using LSB extraction method. The detail process of revealing module is explained in Algorithm 2. The received shares could be facing the security attacks and hence marked as (ShI^1, ShI^2, ShI^3). In the revealing module the received shares from the participants are collected and the secret values are extracted using LSB extraction algorithm. From the extracted values, a $newKey$ is generated without which the secret cannot be constructed. From the obtained $newKey$ and the extracted intermediate share values, the secret is reconstructed. The working of the PMVC revealing module is depicted in Algorithm 2.

During the revealing module, shares are received from various participants. However, there is a possibility of malicious actors, both insiders and outsiders, participating in this phase. Malicious insiders are authenticated members who attempt to deceive others by tampering or modifying the received shares. On the other hand, malicious outsiders are unauthorized intruders who pretend to be authenticated members by providing fake shares. In this phase, the encrypted pixel values and a key are extracted from the received shares. Using the retrieved key, a new decryption key is generated. This decryption key is utilized to decrypt the pixel values, resulting in the reconstructed secret image (RSI). The algorithm presented in the PMVC revealing module

utilizes arithmetic computations for decryption and reconstruction of the secret image. If the received shares have been compromised by any attacks during transmission or storage, the algorithm will not reveal the correct RSI. It is important that the revealing module accounts for the presence of potential malicious actors in the revealing phase. Malicious insiders, who are authenticated members, may attempt to tamper with or modify the received shares to deceive others. Malicious outsiders, who are unauthorized intruders, may also participate by providing fake shares. The algorithm, however, focuses on extracting the encrypted pixel values and the key from the received shares and generating a new decryption key. This new key is then used to decrypt the pixel values and reconstruct the RSI.

Algorithm 2 shows the step by step process of the revealing phase.

Step 1: from the collected shares, each pixel is processed and the secret is extracted using LSB extraction algorithm. The extracted secret pixel ranges $ISh1_{a,b},\ ISh2_{a,b},\ ISh3_{a,b} \in \{0, 1, 2, \dots, 9\}$.

Step 2: a $newKey$ is generated from the extracted pixels. It is the key component of the revealing module without that the secret cannot be reconstructed.

Step 3: from the $newKey$ value and the received $ISh1_{a,b},\ ISh2_{a,b},\ ISh3_{a,b}$, the RSI is reconstructed using simple arithmetic operations.

The algorithm shown in this PMVC revealing module uses arithmetic computations for decryption. If the received $(ShI^1,\ ShI^2,\ ShI^3)$ are compromised by any attack, the algorithm do not reveal the RSI. In the next section, the implementation and analysis of the proposed scheme is explained.

Algorithm 2 Secret Revealing

1: $Input$: $Share\ Images\ (Sh^1, Sh^2, Sh^3) with\ of\ size\ H \times W$

2: $Output$: $Reconstructed\ Secret\ Image\ (RI)$

3: $begin$:

4: $Foreach$ $a \leftarrow 1{:}H$

5: $Foreach$ $b \leftarrow 1{:}W$

6: $do\ until\ (a \leftarrow H\ and\ b \leftarrow W)$

7: $S1_{a,b} \leftarrow mod(Sh^1{}_{a,b}, 10)$

8: $S2_{a,b} \leftarrow mod(Sh^2{}_{a,b}, 10)$

9: $S3_{a,b} \leftarrow mod(Sh^3{}_{a,b}, 10)$

10: $temp_{a,b} \leftarrow mod(S2_{a,b} + S3_{a,b}, 9)$

11: $Key_{a,b} \leftarrow \begin{cases} 9 - temp_{a,b}, & temp \neq 0 \\ 0, & otherwise \end{cases}$

12: $RSI_{a,b} \leftarrow \begin{cases} Sh2_{a,b} \times 100 + Sh3_{a,b} \times 10 + Key_{a,b}, & Sh1_{a,b} = 0 \\ Key_{a,b} \times 100 + Sh2_{a,b} \times 10 + Sh3_{a,b}, & Sh1_{a,b} = 1 \\ Sh3_{a,b} \times 100 + Key_{a,b} \times 10 + Sh2_{a,b}, & Sh1_{a,b} = 2 \end{cases}$

13: $End\ do$

14: $End\ For$

15: $End\ For$

16: End

3. Experimental result and analysis

The proposed PMVC is tested with different size images and the results are analyzed to verify the objectives have been achieved or not. The efficiency and effectiveness of the proposed PMVC outlined in this

research work is tested by coding and running the algorithm in MATLAB 7.10 tool. The set of images used to test the algorithm is shown in **Figure 2**.

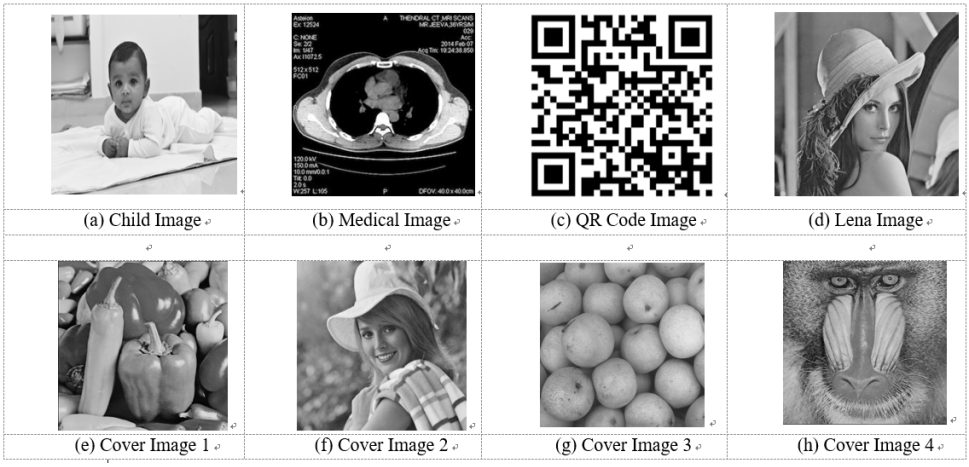

Figure 2. (a)–(d) sample secret grayscale test images; **(e)–(h)** sample grayscale cover images.

Figure 2a–d shows the secret images in grayscale and of size 256×256 and **Figure 2e–h** shows the grayscale cover images and of size 256×256. The cover images are common natural images that carry the contents of the secret image.

3.1. Lifecycle analysis

The proposed PMVC is tested and analysed with more than 100 sample test images of various types such as, financial documents, images that needs privacy etc. The experimental analysis is done using these images and the results are depicted in **Figure 3**. The proposed PMVC scheme has undergone extensive testing and analysis using a variety of sample test images to verify its objectives and evaluate its efficiency and effectiveness. The implementation and evaluation of the scheme were performed using MATLAB tool. The test images used in the experiments are diverse and encompass various types of images, including financial documents and images requiring privacy protection. The selection of a wide range of images helps assess the performance and robustness of the PMVC scheme across different image types and characteristics. The experimental analysis involved applying the PMVC algorithm to more than 100 sample test images. These images were processed using the implemented scheme, and the results were obtained and analyzed. The purpose of this analysis was to evaluate the performance of the PMVC scheme in terms of its ability to securely protect sensitive information in multi-view images.

Figure 3 shows the lifecycle of the secret image with the proposed PMVC. First, GSI, CI^1, CI^2 and CI^3 are considered as input to the proposed PMVC and the GSI is triggered with an error instance in individual pixels and the PSI is generated to give meaning to the GSI. The PSI is encrypted and the encrypted share values IS^1, IS^2 and IS^3 are generated. The IS^1, IS^2 and IS^3 $\in 0, 1, 2, \ldots, 9$ and are embedded with the CI^1, CI^2 and CI^3 using LSB embedding process and the shares S^1, S^2 and S^3 are generated.

At the destination, the shares Sh^1, Sh^2 and Sh^3 are received from the individuals and the secret values (ISh^1, ISh^2 and ISh^3) is extracted using LSB extraction process. From the share values, $newKey$ is generated and using the ISh^1, ISh^2, ISh^3 and $newKey$, the RSI is reconstructed.

The images obtained at various stages are analysed for its quality, security and computational resources. The following section shows the test analysis done on the images at various stages of life cycle.

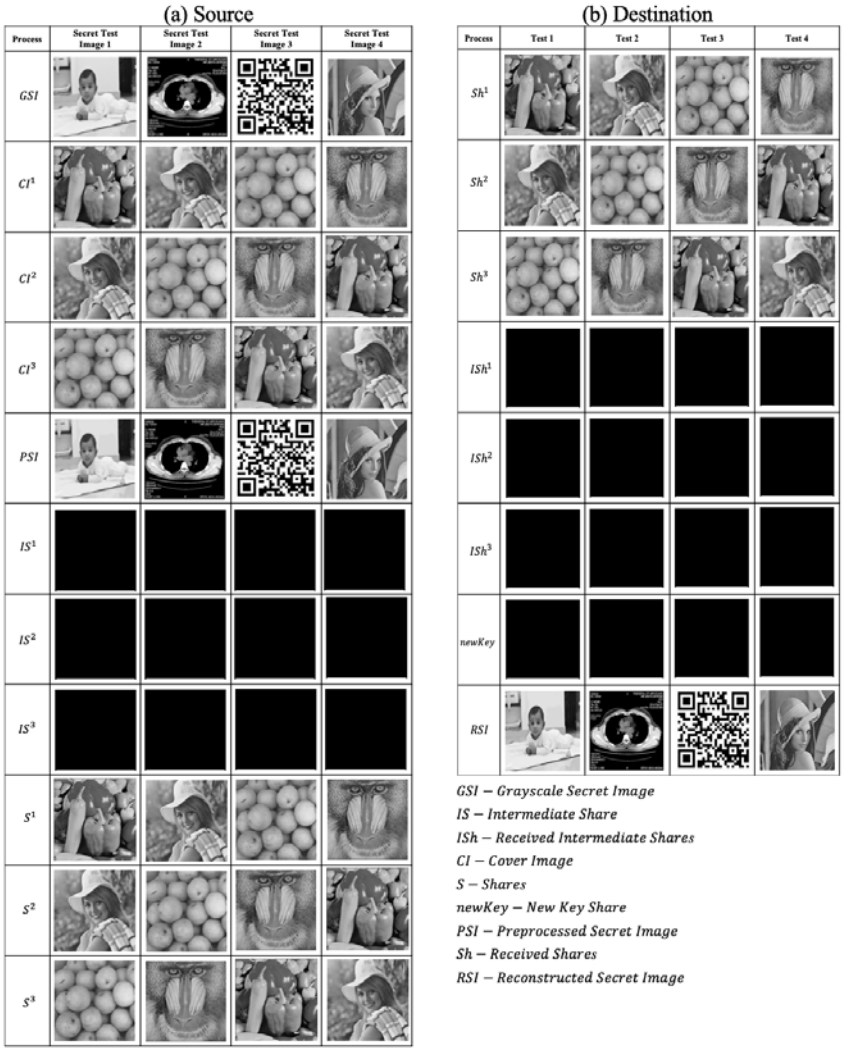

Figure 3. Lifecyle analysis of proposed PMVC.

3.2. Test analysis

3.2.1. Security

The efficiency of the proposed PMVC is measured based on the secure transmission of the secret image. This depends on the conditions such as; (i) *GSI* should be encrypted and sent as shares. (ii) individual shares do not disclose the *GSI*. (iii) shares should not be getting attention from the malicious users in the transmission. (iv) shares should not reveal the secret without the revealing phase. (v) cheating issues also need to be handled[16,17].

Condition 1: The proposed PMVC used the triggered error instance to convert the *GSI* with the meaning and the image pixels are divided and are embedded with the cover images randomly. This enables the shares with minimal values of GSI and the values are not representing the original GSI[18].

Condition 2: Suppose, if the shares are under malicious attack, the individual shares cannot reveal the GSI as only part of encrypted pixel value is available in any of the shares. The encrypted values and randomly distributed[19].

Condition 3: Shares looks like normal cover images and the quality of the images is maintained by the proposed PMVC. The quality of the images is explained in the following section. The encrypted pixel values are embedded with the cover images using LSB embedding algorithm. This reduces the chance for the malicious user to think the availability of secret message in the shares.

Condition 4: If the malicious attacker receives all the shares, the shares do not reveal the GSI without revealing phase. Only a part of the encrypted pixels are sent through the shares and the new key value of the pixel $newKey$ is generated at the destination revealing module. Using the shares and the newly generated key are stacked together to reconstruct the image[20].

Condition 5: If any of the authorised participant of the transmission tries to cheat others by modifying the share or data, the proposed PMVC generates the $newKey$ based on the cheating share and the GSI cannot be reconstructed[21].

3.2.2. Quality of images

Figure 4 shows that the secret image is transformed into progressive meaningful image with the triggered instance. This PSI quality is carefully maintained. The quality of the images is compared s using peak-signal-to-noise ratio (PSNR), the structural similarity index measure (SSIM), the mean square error (MSE) and the mean absolute error (MAE).

PSNR is measured as a ratio between the maximum pixel value and the value of noise that concerns the quality of its visual. It is measured in terms of decibels (dB). If both the images are of same quality PSNR tends to be infinite value. However if the PSNR value is more than 25 dB, then it is considered that the images are within the acceptable limit[22,23].

MSE is the measures of errors in the pixel values as average of the squares of the errors between pixels of the two images. If MSE tends to zero, then both the images are of same pixel values. However, MSE is directly proportional to the pixel differences between the images.

MAE is measured between the images with the maximum pixel value difference between the images. As like MSE, MAE also directly proportional to the pixel differences.

SSIM is considered to measure the perceived quality of the image. This measures the similarity between the two images based on the structural information. The value of SSIM ranges between $0\ to\ 1$ whereas 0 indicates “no similarity” and 1 indicates the “exact match” of the image structure. SSIM value with more than 0.85 is considered to be in acceptable range[10,11,15]. Acceptable range is the term used to mention that the images will not show the major differences or noise to the human eyes. Pixel differences for such images could be less than that of the images that are compressed[16]. The proposed PMVC uses the triggered instance of error to pre-process the image to generate a progressing VC technique for effective transfer of images. Sample PSI image is shown in **Figure 4**.

Table 1 shows that the share images $SI1,\ SI2,\ SI3$ and the cover images $CI1,\ CI2,\ CI3$ are having PSNR value more than 35 dB which is acceptable range. The SSIM shows that structural similarity shows that the images have not been disturbed with the GSI pixel information.

Secondly, the effectiveness of the proposed PMVC is measured based on the quality of the RSI. Sample RSI are compared with the respective GSI and the values are depicted in **Table 2**.

Figure 4 shows that the similar and range of image pixels are converted and grouped together and forms a cluster of pixels. Quality of images becomes the key factor in two situations. Firstly, PSI image is encrypted and the shares are generated using Algorithm 1. The shares are generated and the shares look like the cover images used[19]. When the shares are losing the quality, this leads to chances for cyber-attack. **Table 2** shows the comparative analysis of $CI1,\ CI2,\ CI3$ with the shares $SI,\ S2,\ S3$ with obtained metrics. The metrics are computed from by comparing the cover images with share images and are tabulated in **Table 2**.

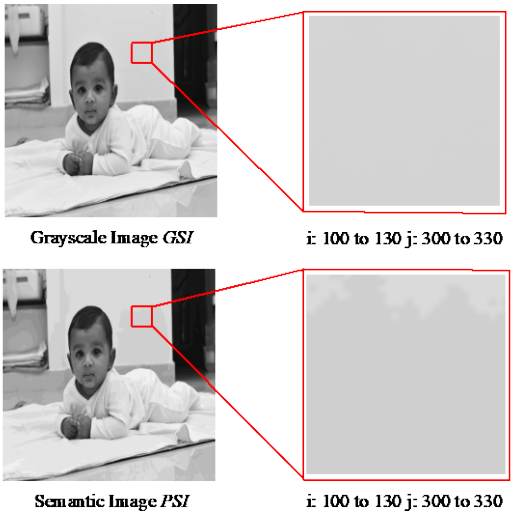

Figure 4. Progressive meaningful image.

Table 1. Quality analysis between cover images with share images.

Share vs cover image	PSNR	MSE	MAE	SSIM
$S1\ vs\ CI1$	+38.34093 dB	1.2187	3.00385	0.86032
$S2\ vs\ CI2$	+35.91239 dB	1.9576	3.23176	0.97113
$S3\ vs\ CI3$	+37.79463 dB	2.0364	3.87954	0.88249

Table 2. Quality analysis between $GSI\ and\ RSI$.

GSI	PSNR	MSE	MAE	SSIM
Baby image	+39.32875 dB	0.69347	2.39768	0.85863
Medical image	+40.89743 dB	0.66927	2.14781	0.99824
QR code image	+41.52133 dB	0.38765	1.73145	0.93672
Lena image	+40.40282 dB	0.68018	2.39273	0.86562

Table 2 shows quality metrics measured between the GSI and the RSI of various images. The results shows that the quality of the RSI with the respective GSI are in the acceptable range. It is observed that the RSI images are same as of the PSI images which are very similar to the GSI images. The PSNR ranges between 35 to 42 dB and the MSE ranges less than 0.7.

3.2.3. Pixel expansion

In the traditional VC, the pixels are divided into two subpixels and are embedded with the share images. Hence the size of the shares increases twice as the size of the cover images. This issue is called pixel expansion. The pixel expanded images attracts the cyber-criminals and creates a curiosity to look into the shares for any secret availability. In PMVC, the pixel values of the secret image are encrypted before embedding them with the cover images using the least significant bit (LSB) embedding algorithm. As a result, the size of the share images remains the same as that of the cover images.

By encrypting the pixel values before embedding them, PMVC provides an additional layer of security to the shares. The encrypted pixel values are not visually recognizable or distinguishable, making it difficult for unauthorized individuals to discern any hidden information within the shares. The absence of pixel expansion in PMVC helps mitigate the curiosity of potential attackers who might attempt to analyze the shares for potential secret availability. The uniform size of the shares, matching that of the cover images, makes it more challenging for cyber-criminals to identify the presence of hidden secrets and discourages their attempts to breach the security of the PMVC scheme. This characteristic of PMVC enhances the security and privacy

of the shared information, reducing the risk of unauthorized access or information leakage. By maintaining the same size for the shares as the cover images, PMVC addresses the concerns associated with pixel expansion in traditional VC, providing an added advantage in terms of security and confidentiality. Hence the size of the share images remains same as of the cover images. This provides additional security to the shares[12].

3.2.4. Computational complexity

The proposed PMVC uses simple arithmetic operations to reconstruct the RSI. For the size of $l \times h$ secret image, the time complexity for share generation is measures as $O(l \times h)$. This can be generalised as $O(n^2)$ if $l = h$. The algorithm uses simple arithmetic operations and random number generation which costs $O(1)$. Similarly, the complexity of the revealing module is also computed. Thus, the total time complexity measured as $O(n^2)$. However, the number of shares increases the requirement of space complexity. The proposed PMVC shares the secret with minimum 3 shares and the memory required to store and communicate the shares takes more space than the existing algorithms. The algorithm in PMVC utilizes basic arithmetic operations and random number generation, both of which have a time complexity of $O(1)$ since their computational requirements do not depend on the input size. Therefore, the time complexity of the share generation algorithm in PMVC can be considered to be relatively efficient. Similarly, the time complexity for the revealing module, which involves extracting the secret values and reconstructing the RSI, is also computed. The total time complexity of PMVC, considering both share generation and the revealing module, is measured as $O(n^2)$, which accounts for the computation involved in processing the shares and reconstructing the secret image. However, it is important to note that the space complexity of PMVC increases as the number of shares required for secure sharing also increases. The proposed PMVC scheme typically uses a minimum of 3 shares to distribute the secret. Storing and communicating these shares requires more memory space compared to existing algorithms that use fewer shares. The analysis of PMVC reveals that it requires minimal computational resources in terms of time and arithmetic computations. This makes it an efficient scheme for secure secret sharing. Additionally, PMVC improves security by utilizing a higher number of shares, which enhances the resilience against unauthorized access or information leakage. The analysis shows that the proposed PMVC requires minimum computations in terms of time and arithmetic computations and improves security while sending more number of shares[24–26].

3.3. Comparative analysis

The proposed PMVC is compared with the existing methods and the result is shown in **Table 3**.

Table 3. Comparative analysis of proposed PMVC with existing schemes.

Method	**[24]**	**[25]**	**[13]**	**[11]**	**[15]**	**Proposed PMVC**
Security	High	High	High	High	Very high	Very high
Quality of RSI	20–25 dB	20–27 dB	20–25 dB	25–35 dB	30–38 dB	35–42 dB
Share size	$(2n + l) \times N$	$N \times 1.15$	$(2n + n + I) \times N$	N	N	N
Pixel expansion	≥ 1	≥ 1	≥ 2	Nil	Nil	Nil
Complexity	Very high	Medium	High	Low	Low	Low
Number of shares	$n \geq 2$	$n \geq 2$	$n \geq 2$	$n = 2$	$n = 3$	$n = 3$
Share generation technique	Pixel replacement	Random based	Pixel replacement	Random based	Linear, pixel replacement	Random based, pixel replacement
Meaningful shares	Meaningless	Meaningless	Meaningful	Meaningless	Meaningful	Meaningful

In the comparative analysis, the proposed PMVC scheme is compared with existing methods, and the results are presented in **Table 3**. The comparison focuses on several key aspects, including security, quality of the reconstructed secret image (RSI), share generation technique, meaningful shares, share size, pixel expansion, complexity, and the number of shares. The comparison evaluates the performance of PMVC in relation to other techniques proposed by different authors. The objective is to assess the efficiency and security of the proposed PMVC scheme for the transmission of secret images. Here is a brief explanation of the parameters considered in the comparative analysis:

Security: the level of security provided by the PMVC scheme is compared with other existing methods. This includes analyzing the encryption techniques, resistance to attacks, and confidentiality of the shared secret image.

Quality of RSI: the visual quality of the reconstructed secret image (RSI) obtained through the PMVC scheme is evaluated. This involves assessing factors such as image clarity, fidelity, and preservation of important details.

Share generation technique: the approach used in generating the shares in PMVC is compared with other methods. This includes analyzing the algorithms, randomness, and robustness against tampering or unauthorized access.

Meaningful shares: the extent to which the shares in PMVC carry meaningful information is considered. Meaningful shares refer to the ability of individual shares to provide some visual context or partial information about the secret image, even without the need for reconstruction.

Share size: the size of the shares generated by the PMVC scheme is compared with other techniques. This parameter evaluates the efficiency and compactness of the shares, considering their storage requirements and transmission bandwidth.

Pixel expansion: the issue of pixel expansion, where the size of the shares exceeds that of the original image, is assessed in PMVC and compared to other methods. Minimizing pixel expansion is desirable as it helps maintain the privacy and secrecy of the shared information.

Complexity: the computational complexity of the PMVC scheme is analyzed and compared to other approaches. This includes evaluating the time complexity and arithmetic operations required for share generation and reconstruction.

Number of shares: the number of shares needed to distribute the secret image securely in PMVC is compared to other methods. The goal is to assess the trade-off between security and the overhead of additional shares.

The comparative study aims to demonstrate that the proposed PMVC scheme is efficient and provides secure transmission of secret images. By analyzing and evaluating these different parameters, researchers can highlight the advantages and strengths of PMVC over existing methods and further validate its effectiveness for privacy-preserving multi-view cryptography. **Table 3** shows that the proposed PMVC is efficient for the secure communication of grayscale image. The proposed PMVC shows that the quality of the RSI is higher than the existing schemes.

4. Conclusion

In this digital era, COVID 19 pandemic had educated the world to move towards digital transactions using quick response codes and communications in the form of images. Such images are transferred through the unprotected open network and being the victims of cyber-attacks. In the proposed PMVC, initially, an error instance is triggered to convert the secret image into progressive meaningful image to avoid the pixel errors

raised in share generation module. Thus, the quality of the RSI is maintained. Also, the proposed scheme do not have pixel expansion issues provide additional security and reduces the space complexity. The proposed PMVC generates $newKey$ in the revealing module. Using the received shares and the newly generated key, the RSI is reconstructed. This ensures that without the revealing module, RSI cannot be reconstructed. Thus the proposed PMVC shows the efficient approach to transfer a single grayscale image using grayscale cover images with minimum number of computations.

Author contributions

Conceptualization, JB and SS; methodology, SM; software, VK; validation, SP and CEK; writing—original draft preparation, SM; writing—review and editing, MV.

Conflict of interest

The authors declare no conflict of interest.

References

1. Harn L, Lin C. Detection and identification of cheaters in (*t*, *n*) secret sharing scheme. *Designs, Codes and Cryptography* 2009; 52(1): 15–24. doi: 10.1007/s10623-008-9265-8
2. Ateniese G, Blundo C, De Santis A, Stinson DR. Extended capabilities for visual cryptography. *Theoretical Computer Science* 2001; 250(1–2): 143–161. doi: 10.1016/S0304-3975(99)00127-9
3. Blesswin J, Raj C, Sukumaran R, Mary S. Enhanced semantic visual secret sharing scheme for the secure image communication. *Multimedia Tools and Applications* 2020; 79: 17057–17079. doi: 10.1007/s11042-019-7535-2
4. Deshmukh M, Nain N, Ahmed M. Efficient and secure multi secret sharing schemes based on boolean XOR and arithmetic modulo. *Multimedia Tools and Applications* 2018; 77(1): 89–107. doi: 10.1007/s11042-016-4229-x
5. Blundo C, Santis AD, Naor M. Visual cryptography for grey level images. *Information Processing Letters* 2000; 75(6): 255–259. doi: 10.1016/S0020-0190(00)00108-3
6. Eslami Z, Rad SK. A new verifiable multi-secret sharing scheme based on bilinear maps. *Wireless Personal Communications* 2012; 63(2): 459–467. doi: 10.1007/s11277-010-0143-0
7. Fu Z, Cheng Y, Yu B. Visual cryptography scheme with meaningful shares based on QR codes. *IEEE Access* 2018; 6: 59567–59574. doi: 10.1109/ACCESS.2018.2874527
8. Dehkordi MH, Farzaneh Y. A new verifiable multi-secret sharing scheme realizing adversary structure. *Wireless Personal Communications* 2015; 82(3): 1749–1758. doi: 10.1007/s11277-015-2310-9
9. Dehkordi MH, Ghasemi R. A lightweight public verifiable multi secret sharing scheme using short integer solution. *Wireless Personal Communications* 2016; 91(3): 1459–1469. doi: 10.1007/s11277-016-3539-7
10. Naor M, Shamir A. Visual cryptography. In: De Santis A (editor). *Advances in Cryptology EUROCRYPT'94*. Springer Berlin, Heidelberg; 1995. pp. 1–12.
11. Prisco R, Santis A. On the relation of random grid and deterministic visual cryptography. *IEEE Transactions on Information Forensics and Security* 2014; 9(4): 653–665. doi: 10.1109/TIFS.2014.2305574
12. Zhang D, Gu Z. A high-quality authenticatable visual secret sharing scheme using SGX. *Wireless Communications and Mobile Computing* 2021; 2021(4): 1–12. doi: 10.1155/2021/6660709
13. Zhang D, Zhu H, Liu S, Wei X. HP-VCS: A high-quality and printer-friendly visual cryptography scheme. *Journal of Visual Communication and Image Representation* 2021; 78: 103186. doi: 10.1016/j.jvcir.2021.103186
14. Mhala NC, Jamal R, Pais AR. Randomised visual secret sharing scheme for grey-scale and colour images. *IET Image Processing* 2018; 12(3): 422–431. doi: 10.1049/iet-ipr.2017.0759
15. Mary GS, 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
16. Mary GS, Kumar SM. Secure grayscale image communication using significant visual cryptography scheme in real time applications. *Multimedia Tools and Applications* 2019; 79(1): 10363–10382. doi: 10.1007/s11042-019-7202-7
17. Mary GS, 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
18. Mudia HM, Chavan PV. Fuzzy logic based image encryption for confidential data transfer using (2, 2) secret sharing scheme. *Procedia Computer Science* 2016; 78: 632–639. doi: 10.1016/j.procs.2016.02.110

19. Wu X, Liu T, Sun W. Improving the visual quality of random grid-based visual secret sharing via error diffusion. *Journal of Visual Communication and Image Representation* 2013; 24(5): 552–566. doi: 10.1016/j.jvcir.2013.03.002
20. Wang SJ, Tsai YR, Shen CC. Verifiable threshold scheme in multi-secret sharing distributions upon extensions of ECC. *Wireless Personal Communications* 2011; 56(1): 173–182. doi: 10.1007/s11277-009-9875-0
21. Wu X, Sun W. Random grid-based visual secret sharing with abilities of OR and XOR decryptions. *Journal of Visual Communication and Image Representation* 2013; 24(1): 48–62. doi: 10.1016/j.jvcir.2012.11.001
22. Sridhar S, Sathishkumar R, Sudha GF. Adaptive halftoned visual cryptography with improved quality and security. *Multimedia Tools and Applications* 2017; 76(1): 815–834. doi: 10.1007/s11042-015-3066-7
23. Yan B, Xiang Y, Hua G. Improving the visual quality of size-invariant visual cryptography for grayscale images: An analysis-by-synthesis (AbS) approach. *IEEE Transactions on Image Processing* 2018; 28(2): 896–911. doi: 10.1109/TIP.2018.2874378
24. Wang DS, Song T, Dong L, Yang CN. Optimal contrast grayscale visual cryptography schemes with reversing. *IEEE Transactions on Information Forensics and Security* 2012; 8(12): 2059–2072. doi: 10.1109/TIFS.2013.2281108
25. Jia X, Wang D, Nie D, Zhang C. Collaborative visual cryptography schemes. *IEEE Transactions on Circuits and Systems for Video Technology* 2016; 28(5): 1056–1070. doi: 10.1109/TCSVT.2016.2631404