International Conference on Advances in Management & Technology (ICAMT- March 2025)

RESEARCH ARTICLE OPEN ACCESS

Image Data Security with the Integration of Visual Cryptography and Bit-plane Color Image

Anil B. Alde
School of Technology
S.R.T.M.University, Sub-Campus,
Peth, Latur, Maharashtra, INDIA
PIN-413531
anilalde77@gmail.com,
https://orcid.org/0009-0000-8324-9888

Vikas T. Humbe
School of Technology
S.R.T.M.University, Sub-Campus,
Peth, Latur, Maharashtra, INDIA
PIN-413531
vikashumbe@gmail.com,
https://orcid.org/0000-0002-6503-424X

Abstract

Visual Cryptography (VC) it’s a kind of cryptography that makes use of a Human Visual System (HVS) to decrypt visual picture data without the need for any complex algorithms besides that bit-plane slicing is a method of decomposing an image into its constituent parts, making it easier to manipulate and process. This indicates methodology aims to raise the quality security ratio as well as to maintain a high-level quality with the resultant secret image as to the source secret image. This paper presents an integrated methodology of Visual Cryptography with bit-plane slicing for a color image to enhance the security ratio as well as to maintain the quality of the resultant secret image which exactly matches the source secret image. The experiment's findings using the suggested methodology increase the security ratio, calculate the high-quality results, and demonstrate outstanding outcomes when assessed using several quality criteria. The one that proposed methods achieved all stated objectives and calculated the results evaluated by several quality indicators demonstrating outstanding outcomes. In the future, any hybrid approach may be utilized with the proposed methodology to explore more applications for society by providing high-level security and authenticity for confidential data.

Keywords— Visual Cryptography (VC), Human Visual System (HVS), Random Grid Visual Cryptography (RG-VC), Mean Squared Error (MSE).

I. Introduction

Due to the growing reliance on digital communication and digital data storage, the significance of data security has increased exponentially in recent years. Traditional cryptographic methods utilize complex algorithmic techniques with substantial computational resources. Besides that, in recent years, Visual Cryptography offered an innovative, simple technique for encryption where an HVS can perform decryption without the participation of any other complex algorithms. This paper explores an integrated approach of Visual Cryptography with bit-plane color images and also explores a way of securing data protection.

A. Background

In 1994, M. Naor and A. Shamir presented VC [1]. It is a cryptographic method that encrypts information about visual images so that the HVS can decrypt it [2]. On the other hand, the bit-plane slicing technique decomposes an image into its constituent binary bit-planes. This approach is utilised in image processing tasks to handle bits of an image [3].

B. Motivation

The approach of integration of Visual Cryptography and bit-plane slicing of color images significantly enhances the security as well as improves the quality of encrypted images [4][5]. This approach gives robustness to the method to secure color images as well as provides an effective cryptographic technique for encryption and decryption.

C. Contribution

Integrating VC with granular encryption to decompose color images into their bit planes helps maintain image quality and security. This study provides qualitative insights into user experience and perception, offering valuable feedback for future development and refinement of the methodology.

II. Literature Review

A. Visual Cryptography

A VC Scheme creates two or more shares of an image, which are encrypted sections. There is no information leakage from a single sharing, and the scheme can handle color, grayscale, or binary pictures. Lately, error diffusion or halftone approaches have been used to improve image quality. These methods often introduce trade-offs between security and visual fidelity [6][7].

B. Bit-plane Slicing

Bit-plane slicing divides an image into a series of subparts of a binary image, in which each bit-plane shows a collection of universal positions of pixel values. Bit-plane is mostly used for image processing, compressing the image [8], detecting the edges of an image [9], watermarking [10], and image enhancement. The utilization of bit-plane in visual cryptography is limited but can potentially improve the encryption of color images [11] [12].

C. Qualitative Research in Visual Cryptography

In recent periods, qualitative cryptography and image processing research have been relatively scarce but essential for understanding user interaction and experience. Studies have shown that user feedback can greatly improve cryptographic techniques' usability and efficacy. This research attempts to fill the gap by integrating qualitative insights into developing visual cryptography techniques [13][14].

D. Integration of Visual Cryptography

Few studies have explored integrating visual cryptography with bit-plane slicing, primarily focusing on grayscale images. These studies demonstrate that bit-plane slicing can improve the granularity of encryption, but further research is needed to apply these concepts to color images effectively [15][16].

III. METHODOLOGY

A. Bit-plane slicing for the color image

A typical color image is constructed with RGB channels that are typically 24 bits per pixel, including 8 bits of the colors blue (B), green (G), or red (R). Figure 1 depicts the process of bit-plane slicing, which breaks down a 24-bit-plane color image into its binary form, one for each bit location in the three-color channels. [17].

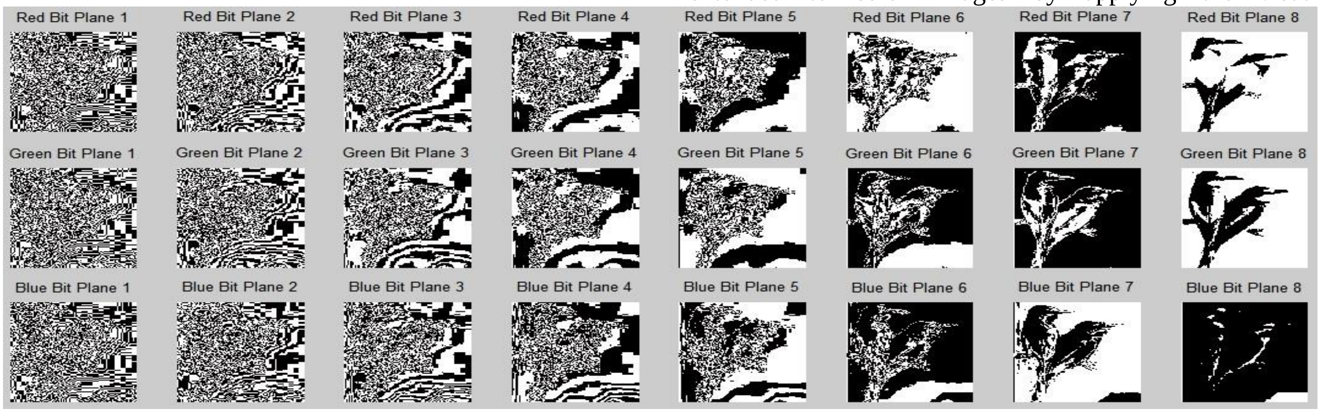


Figure 2. Bit-plane Slicing

I size of a color image M X N; each pixel value can be represented as:

$$I(x,y)=(R(x,y),G(x,y),B(x,y)) \tag{1}$$

These values can be further decomposed into 8 bit-planes as:

$$R(x,y)=\sum_{i=0}^{7}2^{i}R_{i}(x,y) \tag{2}$$

$$G(x,y)=\sum_{i=0}^{7}2^{i}G_{i}(x,y) \tag{3}$$

$$B(x,y)=\sum_{i=0}^{7}2^{i}B_{i}(x,y) \tag{4}$$

Where R(x, y), G(x, y), or B(x, y) are bit planes to channels that are blue, red, and green, respectively, as displayed in Figure 1.

B. Visual Cryptography Technique

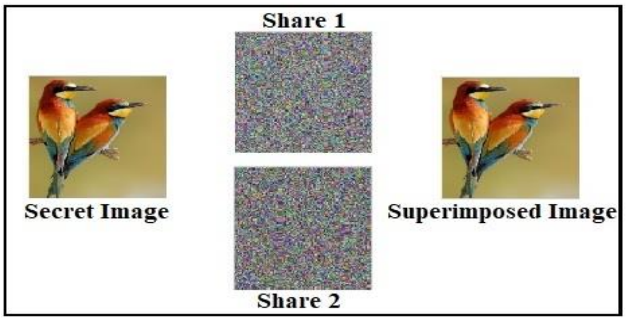


Figure 1. Visual Cryptography

One share constitutes a method where a hidden image is broken down into two or more parts. When these shares are superimposed one above another with proper alignment, then a secret image is revealed. This technique can be extended to color images by applying the visual cryptography scheme to each bit-plane and integrating them into two shares as shown in Figure 2 [18].

For a given bit-plane Pi, the shares S_{1i} and S_{2i} can represented as:

$$P_i=S_{1i}\oplus S_{2i} \tag{5}$$

Where P_i denotes the XOR operation.

C. Share generation

The Shares generated for each bit-plane are combined to form two shares of the color image. This process ensures that each share individually appears as random noise, while the combination of both shares reconstructs the initial picture as displayed in Figure 2 [19].

$$S_1=\bigcup_{i=0}^{23}S_{1i}$$

(6)

$$S_2 = \bigcup_{i=0}^{23} S_{2i} \tag{7}$$

D. Decryption process

The reconstructed bit-planes are combined to form the two final shares named Share 1 and Share 2. Decryption involves overlapping two shares with proper alignment to visually reconstruct the secret color image. The decryption process does not use any complex algorithms [20] and the process reveals the hidden picture by using the human visual system to decipher, which is illustrated in mathematical terms shown in equation (8)

$$I_{dest}(x,y) = \sum_{i=0}^{23} 2^{i} (S_{1i}(x,y) \oplus S_{2i}(x,y)) \tag{8}$$

E. Proposed Methodology

The proposed methodology, shown in Figure 3, aims to increase the security ratio to protect secret images from unauthorized persons.

The methodology elaborated with the following steps:

1. Assign the color image as the input and extract 8-bit planes from each Red, Green and Blue channel.
2. Create the two decrypted forms of shares for each bit-plane.
3. After that, integrate all share 1 of all bit planes to form a single composite share 1, and the same process is used to construct composite share 2.
4. Again, share 2 is separated into sections known as tiles or cells, which are then shuffled randomly.
5. Again, for further security, even-numbered row cells are rotated 180 degrees clockwise, and odd-numbered row cells are rotated clockwise.
6. While making all the changes in steps 4, 5 and 6, all adjustments are maintained in a key.
7. After doing all these things, send Share 1, Shuffle Share 2 and key towards the receiver side.
8. Towards the receiver side, a key is utilised to reconstruct the share 2 into its original form by rearranging all tiles into their proper order.
9. At last when Share 1 overlaps with Share 2, a secret color image is revealed.

IV. Experimental Results and Discussion

Experimental results of the integrated approach of Visual Cryptography with bit-plane generate color shares based on predefined patterns of Random Grid Visual Cryptography (RG-VC), which overcomes every disadvantage of conventional visual cryptography, including low contrast and pixel expansion [21].

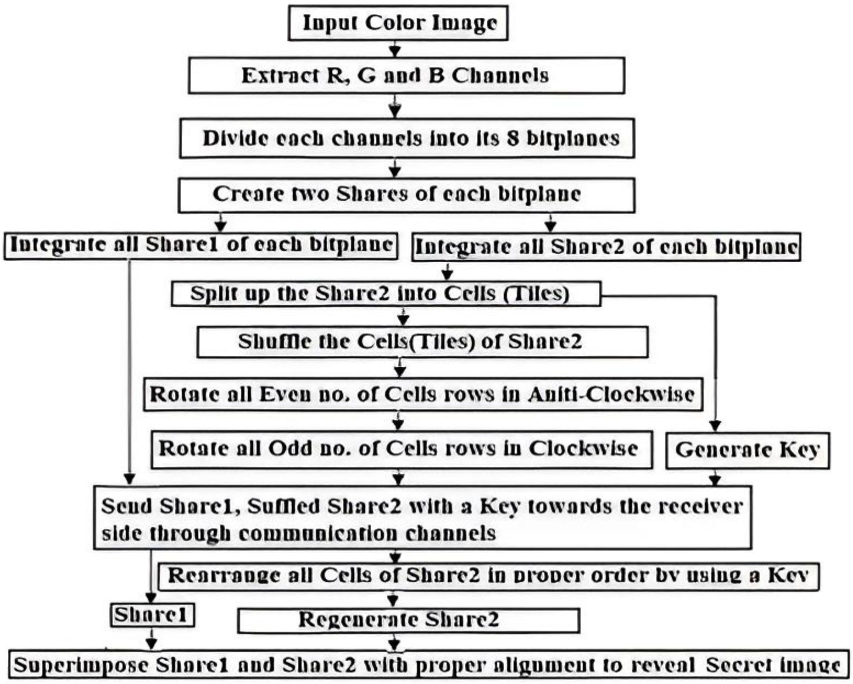

Input Color Image
Extract R, G and B Channels
Divide each channels into its 8 bitplanes
Create two Shares of each bitplane
Integrate all Share1 of each bitplane
Integrate all Share2 of each bitplane
Split up the Share2 into Cells (Tiles)
Shuffle the Cells(Tiles) of Share2
Rotate all Even no. of Cells rows in Aniti-Clockwise
Rotate all Odd no. of Cells rows in Clockwise
Generate Key
Send Share1, Suffled Share2 with a Key towards the receiver side through communication channels
Rearrange all Cells of Share2 in proper order by using a Key
Share1
Regenerate Share2
Superimpose Share1 and Share2 with proper alignment to reveal Secret image

Figure 3. Proposed Methodology

Additionally, it aids in creating a lossless hidden color image towards the recipient's side, as pictured in Figure 4.

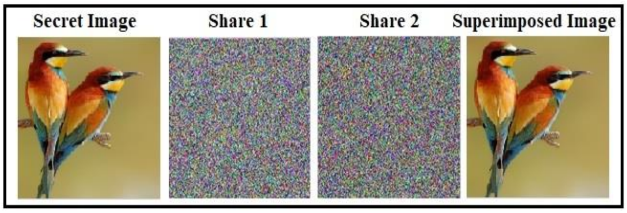


Figure 4 Experimental Result

A. Dataset

The proposed methodology was tested on a dataset of pictures with varying contents and complexity. The images were selected to cover different scenarios, natural scenes, artificial patterns, and images with high-frequency details.

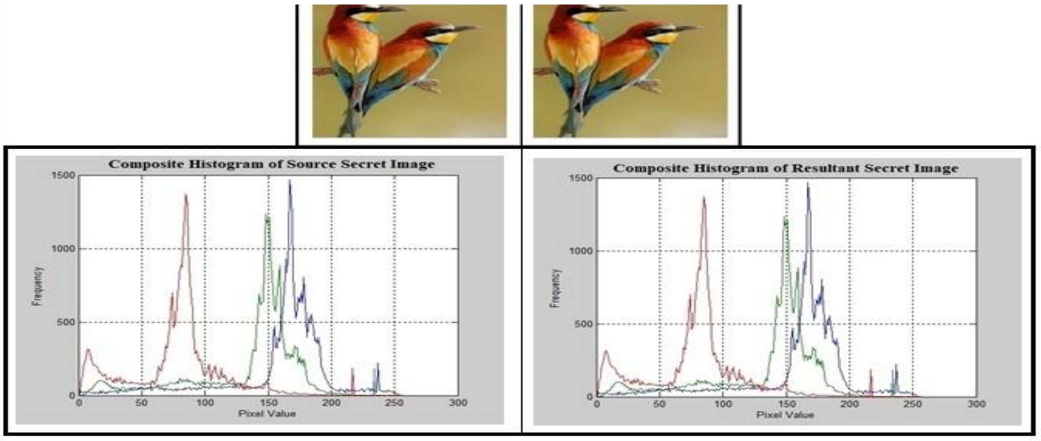
Figure 5. Histogram of Source and Resultant Image

The proportionate relationship between an image's dimensions is its aspect ratio. This ratio, which is determined by a formula, shows how the image's width and height compare.

$$AspectRatio=\frac{Width}{Height} \tag{9}$$

The aspect ratio of a resultant all-tested color secret is identical to their input secret image, indicating that the assessed outcomes are qualitative.

TABLE 1. EVALUATED RESULTS BY QUALITY METRICS



B. Analysis by Histogram

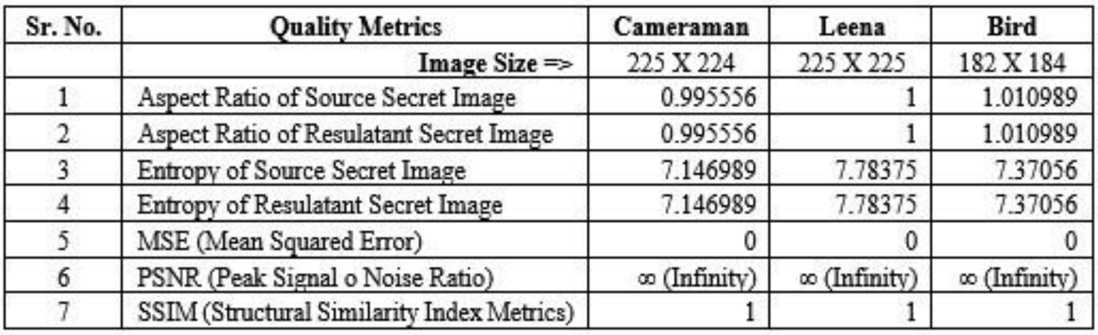
The histogram investigation is the most straightforward estimating instrument and can be noticed visually with the human eye. The suggested methodology's experimental findings demonstrate that the picture and histogram of the Source and the resultant secret image are the same as shown in Figure 5.

C. Quality Metrics

The results of the proposed methodology evaluated by different Quality Metrics, is suggested technique's results are assessed using various quality criteria to determine its overall performance. It produces excellent quality results on diverse types of images, as pictured in Table 1.

Entropy reflects an image's complexity & quantifies its information or randomness. The formula defines an image's entropy, which is determined by the probability distribution of pixel intensities.

$$H= \sum_{i=0}^{L-1} P_i \log_2 (P_i) \tag{10}$$



Sr. No.	Quality Metrics	Cameraman	Leena	Bird
	Image Size =>	225 X 224	225 X 225	182 X 184
1	Aspect Ratio of Source Secret Image	0.995556	1	1.010989
2	Aspect Ratio of Resulatant Secret Image	0.995556	1	1.010989
3	Entropy of Source Secret Image	7.146989	7.78375	7.37056
4	Entropy of Resulatant Secret Image	7.146989	7.78375	7.37056
5	MSE (Mean Squared Error)	0	0	0
6	PSNR (Peak Signal o Noise Ratio)	∞ (Infinity)	∞ (Infinity)	∞ (Infinity)
7	SSIM (Structural Similarity Index Metrics)	1	1	1

Where Pi indicates the likelihood of which ith intensity level and L is the intensity level (for example, 256 for an 8-bit image). Occurring in the image.

For the proposed methodology, quality results are generated for the entropy metrics because the value of all the resultant tested values of the concealed picture are identical to those of the secret photos.

The mean square difference between the source and final hidden images is known as the MSE., pixel per pixel. The following formula determines the MSE value:

$$MSE=\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{j=0}^{N-1}\left[I_{source}(x,y)-I_{dec}(x,y)\right]^2 \quad (11)$$

Were,

MN is the dimension of the image

$I_{source}(x,y)$ is its values of the source image at position (x, y).

$I_{dec}(x,y)$ is its resultant image value at the Position (x, y)

Make sure the final secret picture matches with the initial secret image since the resulting MSE value is zero and the absence a bit of micro-level difference between them.

The maximum inaccuracy between the secret image along with decrypted output image is determined by the Peak-Signal-to-Noise-Ratio (PSNR). It is measured in decibels (dB) as well as is generated from MSE. The formula calculates it:

$$PSNR=20\cdot\log_{10}\left(\frac{I_{max}}{\sqrt{MSE}}\right) \quad (12)$$

Where,

For 8-bit images, the maximum pixel value, or Imax, is 255. The PSNR value in the proposed methodology is infinity (∞) since the MSE value is zero. A greater PSNR typically indicates reconstruction quality. In the proposed method, the PSNR value for all resultant tested secret images is infinite, which suggests that all the resultant secret images are high-quality images.

The Structural Similarity Index Metrics (SSIM) measure the degree it is comparable to the final secret photos and the original. It is predicated on the degradation of structural information. The experimental result of all images for SSIM is 1, meaning that the resultant secret image matches the source secret image. This is how its SSIM index among x & y, two pictures, is calculated as follows:

$$SSIM(x,y)=\frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \quad (13)$$

Where,

μ_x and μ_y are the averages of images x & y.,

σ_x^2 and σ_y^2 are the modifications between images x and y.,

σ_{xy} represents the covariance of image x & image y,

C_1 and C_2 are constants to keep the division with a weak denominator stable.

D. Advantages of the proposed methodology

The proposed methodology of integration offers several advantages:

1) Enhanced Security: In the proposed methodology, a secret when an image is broken up into bit-planes, encrypting each bit-plane independently adds extra protection. The suggested approach offers higher security for color, grayscale, or binary images than conventional visual encryption systems. An attacker finds it more challenging to recreate an obscured image. Its use of 24-bit planes without the required shares.

2) Complexity: The proposed methodology involved handling 24-bit planes, which increases the complexity compared to traditional VC schemes for binary, gray, or color images. However, the increased complexity is justified by enhanced security and image quality.

3) High Image Quality Decryption: Using bit-plane slicing techniques ensures that the details with the final image are identical to those with the original hidden image while preserving the finished image's quality. The caliber of image reconstruction is high, as indicated by the PSNR and SSIM values. Using bit-plane slicing ensures the visual information is preserved during the encryption and decryption.

4) Computational Efficiency: The suggested methodology is both suitable for real-time applications and computationally efficient due to its simplicity of approach to visual cryptography and bit-plane slicing. Users found the methods to be computationally efficient and to have quick times for encryption and decryption, which makes them suitable for real-time applications.

E. Limitations and Future Work of the proposed methodology

The proposed methodology shows significant advantages, but it includes some limitations also, as:

1) Processing Time: Compared to traditional visual cryptography, the proposed methodology handles a 24-bit plane image, which increases the processing time in real-time applications. Future research includes optimizing the processing time to make the method more efficient.

2) Storage Requirement: Another limitation of the proposed methodology is that the storage of 24-bit planes for each color image increases the storage requirements. Future research could focus on developing compression techniques to reduce storage requirements.

3) Advanced Encoding: It develops more sophisticated visual cryptography schemes that can further enhance the security and quality of the decrypted images.

4) Hybrid Approaches: The proposed methodology is combined with other cryptographic techniques to create a hybrid system that offers even greater security and high-quality performance

V. Conclusions

The integrated approach of Visual Cryptography with bit-planes of the proposed methodology increases the ratio of security level as well as succeeds in preserving the receiver-side quality of the resulting secret color image. With zero MSE and infinite PSNR, the experiment results demonstrate that the proposed methodology preserves its quality with the decrypted image while guaranteeing both the original and final secret images remain identical. Additionally, randomization and shuffling of tiles enhance the system's overall security. Future work will focus on optimizing the computational efficiency, reducing storage space by utilizing compression techniques, adopting a hybrid approach of the proposed methodology with other efficient techniques, and exploring the application of the proposed methodology with various kinds of imagery, like satellite or medical imaging.

ACKNOWLEDGEMENT

The authors acknowledge the support from the MAHAJYOTI (MJPRF-2022), Nagpur and Swami Ramanand Teerth School of Technology, Sub-Campus, Peth, Latur, Nanded, for carrying out the study.

CONFLICTS OF INTEREST

The author declares that there are no conflicts of interest.

REFERENCES

[1] M. Naor and A. Shamir, "Visual Cryptography," in Advances in Cryptology — EUROCRYPT'94, Lecture Notes in Computer Science, vol. 950, Berlin: Springer-Verlag, 1994, pp. 1–12. [Online]. Available:https://doi.org/10.1007/3-540-58691-1_1

[2] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," Information and Computation, vol. 129, no. 2, pp. 86–106, 1996. [Online]. Available: https://doi.org/10.1006/inco.1996.0076

[3] R. De Prisco, A. De Santis, and D. R. Stinson, "On the use of visual cryptography for image authentication," in *Proc. IEEE Symp. Information Theory*, 1997, p. 409.

[4] M. S. Chandini, K. Kumar, and S. K. Mungara, "An Enhanced Visual Cryptographic Scheme for Color Image using Bit-Plane Slicing," International Journal of Engineering and Advanced Technology (IJEAT), vol. 9, no. 3, pp. 388–394, 2020. [Online]. Available: https://doi.org/10.35940/ijeat.C4895.029320

[5] J. Paknahad, M. Abbaspour, and H. Ebrahimi, "A new bit-plane-based visual cryptography scheme for color images," *Multimedia Tools and Applications*, vol. 75, no. 23, pp. 15889–15901, 2016. [Online]. Available: https://doi.org/10.1007/s11042-015-3071-1

[6] S. J. Shyu, "Image encryption by random grids," *Pattern Recognition*, vol. 40, no. 3, pp. 1014–1031, 2007. [Online]. Available: https://doi.org/10.1016/j.patcog.2006.09.010

[7] T. Chuman, H. Furukawa, and H. Kiya, "Block scrambling-based encrypted image verification with JPEG compression," in *Proc. IEEE Int. Conf. Image Processing (ICIP)*, 2017, pp. 3480–3484. [Online]. Available: https://doi.org/10.1109/ICIP.2017.8296915

[8] R. B. Johnson and A. J. Onwuegbuzie, "Mixed Methods Research: A Research Paradigm Whose Time Has Come," *Educational Researcher*, vol. 33, no. 7, pp. 14–26, 2004. [Online]. Available: https://doi.org/10.3102/0013189X033007014

[9] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 2nd ed. Prentice-Hall, Inc., 2002.

[10] M. Makbol and B. E. Khoo, "A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition," Digital Signal Processing, vol. 33, pp. 134–147, 2014. [Online]. Available: https://doi.org/10.1016/j.dsp.2014.06.008

[11] A. Kumar and A. Sinha, "Performance evaluation of bit-plane slicing based on digital image watermarking techniques," Journal of Visual Communication and Image Representation, vol. 41, pp. 218–231, 2016. [Online]. Available: https://doi.org/10.1016/j.jvcir.2016.10.009

[12] M. M. Rahman and M. M. Islam, "Digital image watermarking techniques: a review," *Information Technology Journal*, vol. 12, no. 8, pp. 1427–1441, 2013.

[13] J. W. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 4th ed. SAGE Publications, Inc., 2013.

[14] U. Flick, An Introduction to Qualitative Research, 6th ed. SAGE Publications, Inc., 2018.

[15] X. Wu and H. Xu, "Color visual cryptography scheme using meaningful shares," Journal of Visual Communication and Image Representation, vol. 23, no. 8, pp. 1225–1233, 2012. [Online]. Available: https://doi.org/10.1016/j.jvcir.2012.07.010

[16] C. C. Lin and W. H. Tsai, "Visual cryptography for color images using color decomposition," Image and Vision Computing, vol. 21, no. 6, pp. 479–485, 2003. [Online]. Available: https://doi.org/10.1016/S0262-8856(03)00003-5

[17] C. N. Yang and C. S. Laih, "New colored visual secret-sharing schemes," Designs, Codes and Cryptography, vol. 20, no. 3, pp. 325–335, 2000.

[Online]. Available: https://doi.org/10.1023/A:1008349310190

[18] C. C. Lin and W. H. Tsai, "Secret image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 73, no. 3, pp. 405–414, 2004. [Online]. Available: https://doi.org/10.1016/j.jss.2003.08.006

[19] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: survey and analysis of current methods," Signal Processing, vol. 90, no. 3, pp. 727–752, 2010. [Online]. Available: https://doi.org/10.1016/j.sigpro.2009.08.010

[20] Y. K. Lee and L. H. Chen, "High capacity image steganographic model," in Proc. IEEE Int. Conf. Image Processing (ICIP), 2000, vol. 3, pp. 252–256. [Online]. Available: https://doi.org/10.1109/ICIP.2000.899586

[21] R. Shyam and R. Sivakumar, "Random grid-based visual cryptography for gray images," Multimedia Tools and Applications, vol. 77, no. 5, pp. 6195–6212, 2018. [Online]. Available: https://doi.org/10.1007/s11042-017-4539-6