

# Bit-Plane Visual Cryptography: A Comparative Analysis of Binary and Gray Images in Terms of Quality, Security, and Computational Efficiency

Anil B. Alde<sup>1</sup>, Vikas T. humbe<sup>2</sup>

1. School of Technology, S. R. T. M. U. N., Sub-Campus, Peth, Latur, Maharashtra, INDIA
2. School of Technology, S. R. T. M. U. N., Sub-Campus, Peth, Latur, Maharashtra, INDIA

---

## ABSTRACT

In the digital world today, where the sharing of images is very common, guaranteeing the confidentiality and authenticity of the images is crucial. Visual encryption offers an important solution to the challenges of the safe transmission of images. As images are easily forged or manipulated, it becomes necessary to analyze different encryption techniques to determine which method offers the best protection against unauthorized access. Among the two techniques, besides the binary visual encryption, bit-plane gray has attracted significant attention. This research paper presents a comprehensive analysis of Visual Cryptography (VC) using bit-plane techniques for two types of images, namely binary and grayscale images. The objective of this study is to investigate VC schemes based on two types of images in terms of security, visual quality, computational complexity, and robustness. The research finding aims to highlight the strengths and limitations of each approach.

**KEYWORDS:** Visual Cryptography (VC), Mean Squared Error (MSE), Bit-plane

---

Date of Submission: 02-07-2025

Date of acceptance: 12-07-2025

---

## I. INTRODUCTION

Visual encryption is a method that helps to safely transmit images by breaking them in different smaller parts. These parts help to revolve the original secret image when they are combined correctly. This technique was introduced by Naor and Shamir in 1994 [1] and has since attracted attention to its simple but effective approach to image safety. Visual encryption works by dividing a secret image into a series of actions, which can be distributed to various people. Only when you combine a specific minimum number of actions is it possible to reveal the secret image as shown in Figure 1. This function makes visual encryption particularly useful in areas that require safe communications, such as military operations, confidential transactions, and safe sharing of data.

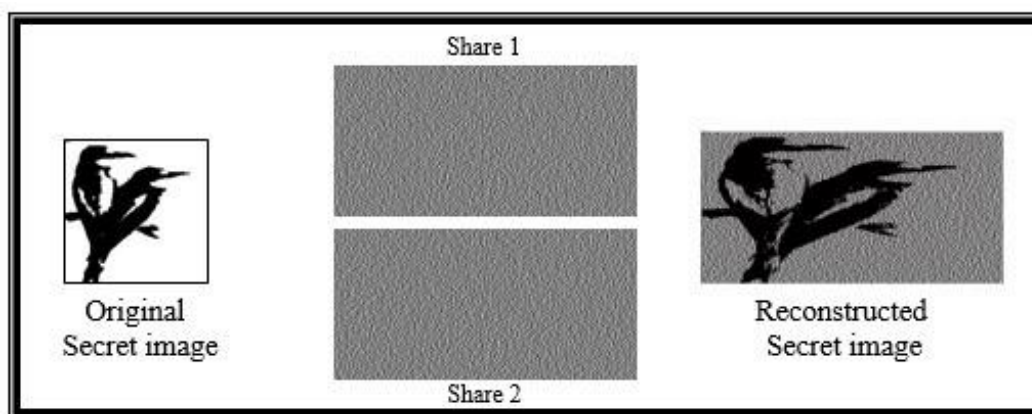


Figure 1: Traditional Visual Cryptography

Bit-plane VC extends this paradigm by decomposing images into binary bit-planes, enabling encryption of complex images such as grayscale and color images [2]. This approach enhances flexibility but introduces challenges related to image type, affecting visual quality, security, and computational efficiency [3].

Binary images, with their single-bit structure, are computationally efficient but limited in detail [4]. Grayscale image balances the details and the complexity [5], while color images, with multiple channels, offer

rich visuals but increase processing demands [2]. Despite extensive research, a systematic comparison of these image types in bit-plane VC is lacking. This paper addresses this gap by analyzing:

- Visual quality using MSE, PSNR and SSIM metrics.
- Security through entropy and correlation analysis.
- Computational efficiency via processing time measurements.

### **1.1 Background and Motivation**

Due to the world's rapid development and technology, everyone needs to do all operations in a fast and secure way. The rapid growth of digital data transmission securely and reliably is not done due to the possibility of hacking the world, but VC is a technique that gives security as well as reliability by encrypting visual information into shares that can only be decrypted when they are stacked together.

### **1.2 Problem Statement**

The traditional VC schemes have many drawbacks and limited applicability to binary images, grayscale images, with the additional challenges in terms of complexity and accuracy. To overcome all these drawbacks, new techniques have succeeded in overcoming these drawbacks, but each technique, based on the types of images, has its drawbacks.

### **1.3 Objectives**

The objectives of this paper are to describe the analyzed performance of VC using bit-plane for binary and gray images based on evaluating security, quality, and computational overhead to suggest optimal use of each image type.

### **1.4 Structure of the Paper**

This paper is structured as follows: Section 2 includes a literature review, Section 3 discusses the VC and bit-plane decomposition, Section 4 describes the methodology utilized in each image type, and Section 5 presents the experimental results for each image type of images. At last conclusion and future scope are included in section 6.

## **II. LITERATURE REVIEW**

Monoth and Anto [4] enhanced VC for binary images, achieving high contrast with minimal computational cost. Chen et al. [5] addressed pixel expansion in grayscale VC, improving quality. Hou [2] and Shyu [6] explored color image VC, noting challenges in share alignment. Recent works, such as Yan et al. [7], introduced adaptive share generation, while Lee and Chiu [8] proposed progressive VC for improved quality. Security enhancements include random grid VC [9] and extended VC schemes [10]. Other studies have explored efficiency [11], improved visual quality [12], and comprehensive surveys [13, 14]. However, comprehensive comparisons across image types remain limited.

## **III. FUNDAMENTALS OF VC AND BIT-PLANE DECOMPOSITION**

### **3.1 Visual Cryptography**

VC is a  $(k, n)$ -threshold scheme where an image is split into  $n$  shares, and at least  $k$  shares are needed for reconstruction [15]. Shares appear as random patterns, ensuring security without computational decryption. Applications include secure document sharing and authentication [3] [12].

### **3.2 Bit-plane Decomposition**

Bit-plane decomposition splits an image into binary layers, each representing a bit of pixel intensity. An 8-bit grayscale image yields eight bit-planes, with higher-order planes contributing more to visual content [16]. Color images, typically RGB, produce 24 bit-planes (8 per channel) [2]. This enables VC to encrypt complex images by processing each bit-plane independently [6].

#### **3.2.1 Bit-plane on Binary image**

The bit-plane technique is typically not applied to binary images because binary images contain only one bit per pixel (0 or 1). Since a binary image has only one bit-plane, that is the Most Significant Bit plane (MSB), there is no further decomposition possible in a binary image. However, VC encryption in binary images can be accomplished without using bit-plane decomposition, and it can be accomplished by codebook or random grid VC techniques.

### 3.2.2 Bit-plane on Gray and Color image

Generally bit-plane decomposition technique is used only for grayscale and color images, in which each pixel consists of 8 bits in a grayscale image and 24 bits in color image.

## IV. METHODOLOGY

### 4.1 Image types

We analyze two image types:

- Binary Images: Single-bit images (0 or 1), ideal for text or simple graphics [4].
- Greyscale Images: 8-bit images with 256 intensity levels [5].

### 4.2 Bit-plane VC Scheme

The bit-plane VC process includes:

1. Decomposition: Extract bit-planes from the input image (1 for binary, 8 for grayscale, 24 for color).
2. Share Generation: Apply a (2, 2)-threshold VC scheme to each bit-plane, creating two shares per plane [15].
3. Reconstruction: Stack shares to reconstruct bit-planes, combining them to form the final image.

### 4.3 Bit-plane methodology for Binary image

Since a binary image only has 0 or 1 values, its bit planes are trivial. Except the first bit-plane, which includes the meaningful information, and the rest of the other bit-planes from 1 to 7 include only zeros. So bit-plane decomposition technique is not suitable for performing on a binary image.

### 4.4 Codebook methodology on binary image

- Uses predefined patterns or matrices ( from a fixed codebook)
- The same pattern is always used for the same input pixel type (White or Black)

This method encodes and decodes shares using specified codebooks. Every block that makes up the hidden image is mapped to a code in the codebook. The codes in the codebook are used to generate shares [17]. This method uses a 2 by 2 matrix, sometimes known as a codebook, with codeword that are 2 X 2 sub-pixels in size, as seen in Fig. 2. It is challenging to create such a matrix for encryption, but [18]. This method creates a distorted dot image known as shares by encoding a secret image.

The Codebook of Visual Cryptography													
Secret Pixel	□ White Pixel group						■ Black Pixel group						
Share 1	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □
Share 2	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □
Stacked Shares	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □	■ □



**Figure 2: Codebook Pixels**

A white group with six instances and a black group with six cases are both included in this technique, as shown in Figure 2. One of the six cases in the share group is chosen at random to assign codewords to shares 1 and 2 if a pixel in the secret image is white. Conversely, black undergoes the same procedure. As illustrated in Figure 1, the size of the hidden picture [19][20] is equal to the size of the shared images Share 1 and Share 2.

### 4.5 Random Grid methodology on a binary image

- No Predefined patterns.
- Shares are generated randomly, pixel by pixel.
- The randomization happens at runtime, making the shares different every time.

Researchers developed a different Visual Secret Sharing (VSS) technique to get around the codebook's shortcomings. This scheme was first introduced by Kafri and Keren in 1987 [21], but it was ignored for 20 years until 2007 [22]. This method works by creating a random pixel grid out of the secret image. A grid of arbitrary black and white pixels makes up a share. The secret image is seen when the shares are piled together.

Random Grid Visual Cryptography						
Method	Secret Pixel	Incidence	R1	R2	Stacking Pixel	Light Transmission
Model 1	□	1/2	□	□	□	1/2
		1/2	■	■	■	
	■	1/2	□	■	■	0
		1/2	■	□	■	
Model 2	□	1/2	□	□	□	1/2
		1/2	■	■	■	
	■	1/4	□	□	□	 1/4
		1/4	□	■	■	
		1/4	■	□	■	
		1/4	■	■	■	
Model 3	□	1/4	□	□	□	 1/4
		1/4	□	■	■	
		1/4	■	□	■	
		1/4	■	■	■	
	■	1/2	□	■	■	0
		1/2	■	□	■	

**Figure 3: Random Grid Pixels**

This method assigns a color to each pixel, which is regarded as a grid, as seen in Fig. 3. The color of Grid R1 is assigned during the encryption process, followed by the color of Grid R2, which is complementary or the same as a reference to the matching pixel. Fig. 3 illustrates Kafri's system, which is expanded upon by Shyu [22]. R1 and R2 are the same color if the hidden image's pixel is white. It complements the black color grid in addition to that. When shares are piled on top of each other, this technique generates 50% black in white regions and 100% black in black areas.

If the pixel in Model 2 is white, then R1 and R2 have the same color, and when these shares overlap, the result is unicolor. The color of R2 is chosen at random if the pixel is black. When shares are overlapped one atop the other, this method produces 50% black in the white sections and 75% black in the black portions [1].

In Model 3, the color of R2 is assigned at random if the pixel is white; otherwise, R2 is complementary to R1 if the pixel is black. When shares overlap, this method produces 75% black in the white parts and 100% black in the black portions.

The likelihood that the secret pixel will be black in the shared image is 50% in all three models, regardless of the color of the pixel. This guarantees the secret image's protection. The three models' respective contrasts of 50%, 25%, and 25% are adequate for a viewer to detect the sensitive data in the stack image with the unaided eye.

#### 4.6 Methodology for gray image

In an 8-bit grayscale image, each pixel is an 8-bit binary value ranging from 0 to 255 values, that is, 0 to 8-1 values. The bit-planes are categorised from Most Significant Bits (MSBs) to Least Significant Bits (LSBs) as follows:

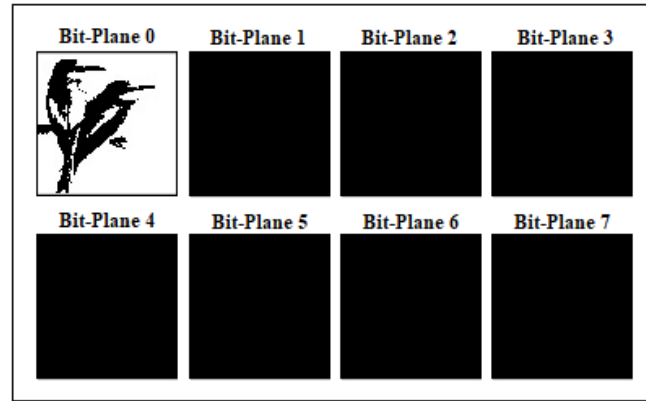
$$I(x, y) = b_7(x, y) \cdot 2^7 + b_6(x, y) \cdot 2^6 + \dots + b_0(x, y) \cdot 2^0 \quad (1)$$

Where  $b_n(x, y)$  represents the binary value of the  $n$ th bit-plane at pixel  $(x, y)$ . The lower bit-planes (LSBs) retain fine details with noise, whereas the higher bit-planes (MSBs) capture significant image structure [23].

### V. EXPERIMENTAL RESULTS

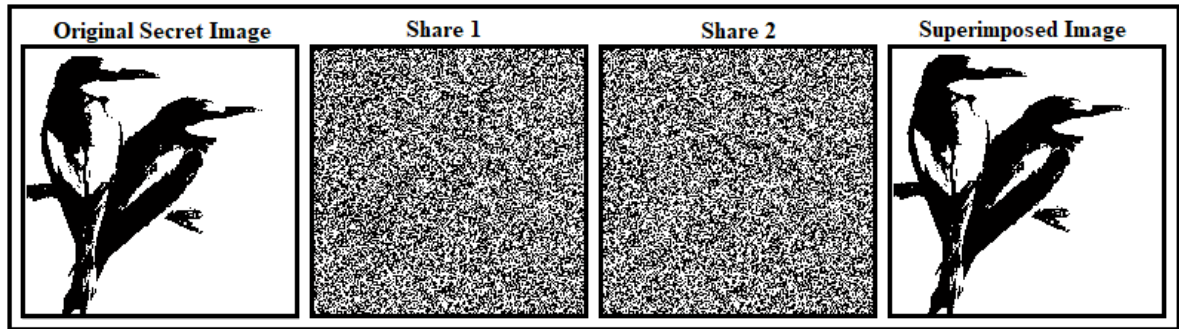
#### 5.1 Binary image

In a Binary image, the first bit-plane has meaningful information, which includes either zero (0) or one (1), and bit-plane 1 to 7 are always zero. The Following Figure shows bit-plane decomposition on a binary image.



**Figure 4: Binary Image Bit-Planes**

Figure 5 shows the original binary image, and it is divided into two shares such as Share 1 and Share 2. When Share 1 overlaps with Share 2, the original grayscale secret image is revealed.

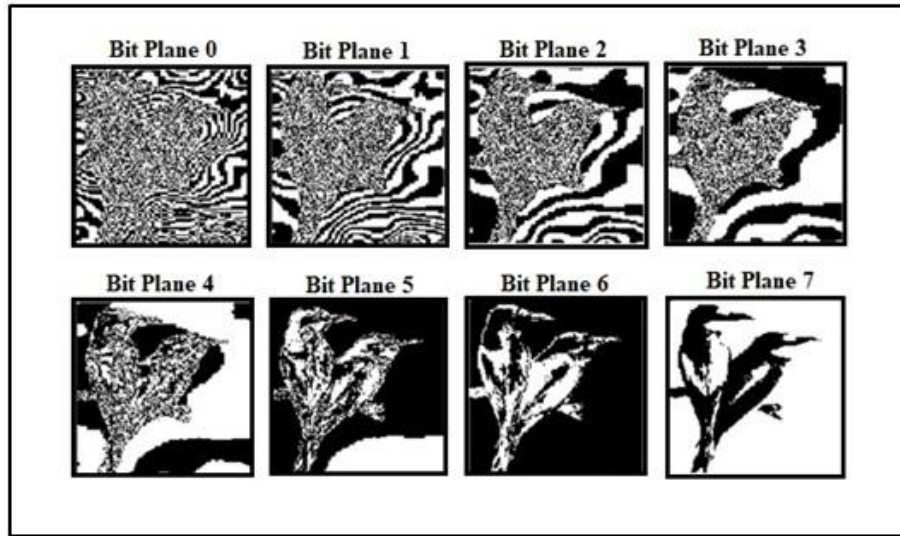


**Figure 5: Binary Input Secret Image, Share 1, Share 2, and Superimposed Image**



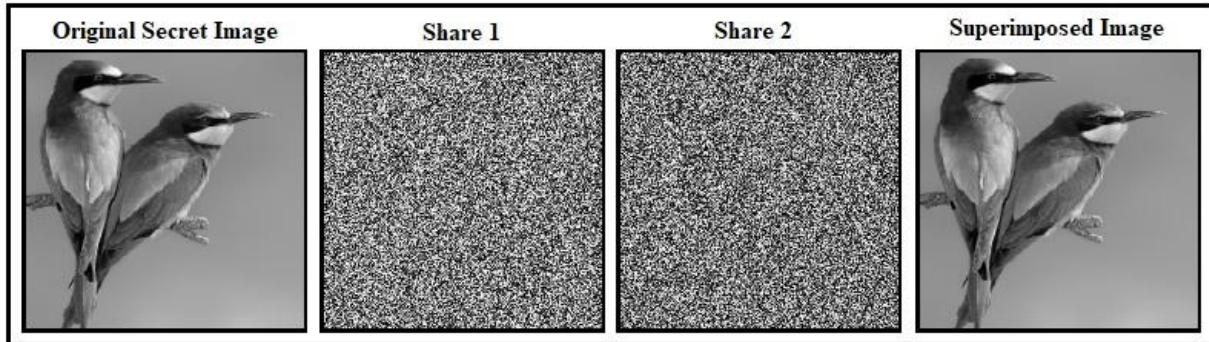
## 5.2 Grayscale Image

In a Grayscale image, all 0 to 7 bit-planes have meaning, which includes either 0 or 1. Figure 6 shows bit-plane decomposition on a grayscale image where bit-plane 7 show more meaningful information.



**Figure 6: Bit-Planes of Grayscale Image**

Figure 7 shows the original grayscale image, and using the visual cryptography technique, it is divided into two parts as Share 1 and Share 2. When Share 1 is overlapped on Share 2 with proper alignment, the original secret image is revealed.



**Figure 7: Grayscale Input Secret Image, Share 1, Share 2, and Superimposed Image**

## 5.3 Security Analysis

Share entropy was 7.9 bits for binary images, 7.7 bits for grayscale, and 8.0 bits for color images, approaching the ideal randomness value of 8 [24]. Low correlation coefficients ( $<0.05$ ) confirmed shared randomness across all types, ensuring robust security [25].

## 5.4 Computational Efficiency

Binary images were the fastest (0.10 s total processing time), followed by grayscale images (0.40 s). The generated MSE = 0 means a 100% lossless secret image is generated through the bit-plane technique, and if MSE is zero, then its PSNR value must be infinity. As MSE is zero, then its SSIM = 1, which means the similarity between the input and output image is the same.

**Table 1: Visual Cryptography and Computational Efficiency Metrics**

Image Type	MSE	PSNR (dB)	SSIM	Share Generation Time (Seconds)	Reconstruction Time (Seconds)
Binary	0	$\infty$	1	0.10	0.02
Grayscale	0	$\infty$	1	0.40	0.05

## 5.5 Discussions

Binary images excel in efficiency and quality due to their simplicity, making them suitable for resource-constrained systems [4]. Grayscale images balance detail and performance [5], while color images offer rich visuals but face alignment challenges [2]. Security is consistently high, with color images benefiting from increased bit-planes [6]. Compared to adaptive VC [7], our scheme is faster for binary images but slightly lags in color image quality compared to progressive VC [8]. Limitations include pixel expansion in color images, which future work could address through optimized share generation [12].

## VI. CONCLUSIONS AND FUTURE SCOPE

This study compared bit-plane VC across binary and grayscale images, highlighting trade-offs in quality, security, and efficiency. Binary images are optimal for efficiency, while gray or color images enhance visual details. Security remains robust across all types of images. Future research will explore machine learning for share optimization and hybrid VC schemes for improved performance.

## REFERENCES

- [1]. M. Naor and A. Shamir, "Visual cryptography," in Proc. Adv. Cryptology-Eurocrypt, vol. 950, pp. 1–12, (1995).
- [2]. Hou, Y. C. (2003). Visual cryptography for color images. Pattern Recognition, 36(7), 1619–1629. [https://doi.org/10.1016/S0031-3203\(02\)00246-2](https://doi.org/10.1016/S0031-3203(02)00246-2)
- [3]. Shyu, S. J. (2007). Efficient visual secret sharing scheme for color images. Pattern Recognition, 40(12), 3633–3651. <https://doi.org/10.1016/j.patcog.2007.04.015>
- [4]. Monoth, D., & Anto, S. (2008). A secure visual cryptographic algorithm for hiding secrets in images. International Journal of Computer Science and Network Security, 8(5), 1–6.
- [5]. Chen, W., Wang, J., & Jin, J. (2013). A grayscale visual cryptography scheme with perfect contrast. Information Sciences, 223, 325–336. <https://doi.org/10.1016/j.ins.2012.09.048>
- [6]. Shyu, S. J. (2006). Image encryption by random grids. Pattern Recognition Letters, 27(5), 317–325. <https://doi.org/10.1016/j.patrec.2005.08.012>
- [7]. Yan, Q., Deng, R. H., & Zhu, S. (2011). Adaptive visual cryptography scheme for general access structures. IEEE Transactions on Information Forensics and Security, 6(4), 1364–1374. <https://doi.org/10.1109/TIFS.2011.2161924>
- [8]. Lee, C. C., & Chiu, Y. K. (2011). Progressive visual cryptography with unexpanded shares. Optics Communications, 284(1), 97–102. <https://doi.org/10.1016/j.optcom.2010.08.073>
- [9]. Blundo, C., De Santis, A., Naor, M., & Stinson, D. R. (2000). Visual cryptography for general access structures. Information and Computation, 129(2), 86–106. <https://doi.org/10.1006/inco.1996.0072>
- [10]. Ateniese, G., Blundo, C., De Santis, A., & Stinson, D. R. (2001). Extended capabilities for visual cryptography. Theoretical Computer Science, 250(1–2), 143–161. [https://doi.org/10.1016/S0304-3975\(99\)00236-4](https://doi.org/10.1016/S0304-3975(99)00236-4)
- [11]. Lin, C. C., & Tsai, W. H. (2003). Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters, 24(1–3), 349–358. [https://doi.org/10.1016/S0167-8655\(02\)00268-7](https://doi.org/10.1016/S0167-8655(02)00268-7)
- [12]. Verheul, E. R., & van Tilborg, H. C. A. (1997). Improved contrast in visual cryptography. Designs, Codes and Cryptography, 11, 179–196. <https://doi.org/10.1023/A:1008285907003>
- [13]. Droogenbroeck, M. V., & Benedett, R. (2002). Visual cryptography schemes using rectangular shares. Pattern Recognition Letters, 24(1–3), 49–62. [https://doi.org/10.1016/S0167-8655\(02\)00239-0](https://doi.org/10.1016/S0167-8655(02)00239-0)
- [14]. Nakajima, M., & Yamaguchi, Y. (2002). Extended visual cryptography for natural images. Pattern Recognition, 38(11), 1920–1934. <https://doi.org/10.1016/j.patcog.2005.03.019>
- [15]. Naor, M., & Shamir, A. (1994). Visual cryptography. Advances in Cryptology—EUROCRYPT '94, 950, 1–12. <https://doi.org/10.1007/BFb0053419>
- [16]. Gonzalez, R. C., & Woods, R. E. (2002). Digital image processing (2nd ed.). Prentice Hall.
- [17]. Y. F. Chen, Y. K. Chan, C. C. Huang, M. H. Tsai, Y. P. Chu, "A multiple-level visual secret sharing scheme without image size expansion", Inform. Sci. 177 (21) pp. 4696–4710, (2007).
- [18]. T. H. Chen and K. H. Tsao, "Threshold visual secret sharing by random grids," J. Syst. Softw., vol. 84, no. 7, pp. 1197–1208, (2011).
- [19]. Y. Hou, S. Wei and C. Lin, "Random-Grid-Based Visual Cryptography Schemes," IEEE Transaction on Circuits and Systems for Video Technology, vol. 24, No. 5, May (2014).
- [20]. Chandramathi S., Ramesh Kumar R., Suresh R. and Harish S., "An overview of visual cryptography," Int. J. Comput. Intell. Tech., vol. 1, no.1, pp. 32-37, (2010).
- [21]. O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Opt. Lett., vol. 12, no. 6, pp. 377–379, Jun. (1987).
- [22]. S. J. Shyu, "Image encryption by random grids," Pattern Recognition., vol. 40, no. 3, pp. 1014–1031, (2007).
- [23]. Gonzalez, R. C., & Woods, R. E. (2018). Digital Image Processing (4th ed.). Pearson.
- [24]. Shannon, C. E. (1948). A mathematical theory of communication. Bell System Technical Journal, 27(3), 379–423. <https://doi.org/10.1002/j.1538-7305.1948.tb01338.x>
- [25]. Stinson, D. R. (1995). Cryptography: Theory and practice. CRC Press.