International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhanced Security and User Friendliness of Generated Shares Using Combination of Block Based Progressive Visual Secret Sharing Scheme and Pixel Value Differencing

Vishal V. Panchbhai[1], Dr. Suchita W. Varade[2]

Submitted:23/03/2023 **Revised:**27/05/2023 **Accepted:**11/06/2023

Abstract: In order to securely transfer confidential photos among participants, visual secret sharing (VSS) techniques are often used. Traditional VSS methods, however, have drawbacks in terms of security and usability. The suggested research has been investigating ways to provide meaningful shares that are user-friendly in order to solve these limitations. One approach combines a least significant bit (LSB)-based mechanism with a block-based progressive visual secret sharing system. The user experience might be negatively impacted by the poor visual quality of shares produced using this technique.

This research seeks to improve user-friendly shares' visual attractiveness by offering a unique way to address the issue of poor visual quality in user-friendly shares. The recommended solution combines the pixel value differencing method with a block-based progressive visual secret sharing system. By using this strategy, the shares' visual quality is considerably enhanced, producing a result that is more visually pleasing and satisfying for the participants.

The performance of suggested system is assessed using standard performance measure metrics. The recommended technique outperforms other ways in comparison to the findings, which were compared and contrasted.

***Keywords*:** *User friendly share, meaningful share, Progressive Visual Secret Sharing (PVSS) scheme, Block based Progressive Visual Secret Sharing (BPVSS) scheme, visual cryptography, Pixel Value Differencing (PVD*

1. Introduction

Throughout a contemporary era of communication, many individuals use the internet for distribute multimedia content via unsecured networks, where hackers might potentially get access to or steal this information.As a result, it is critical to send multimedia data discreetly via an open network. To the aforementioned difficulty, researchers devised a number of solutions based on steganography and cryptography. Although cryptography deals with the study of how to encrypt and decode data, steganography focuses on how to conceal data without affecting its functionality. Video and image data are too large for text-based encryption methods to handle effectively. Visual Cryptography (VC) is one way to the aforementioned problem.

VC systems are cryptographic methods for securely distributing confidential pictures among several users. Many different applications, including secure image transfer, watermarking, and privacy protection, make use of these techniques. The secret image is divided into shares in traditional VSS systems, which are subsequently given to participants. Only when a large enough number of shares are joined can the secret picture be recreated.

The visual cryptography technique was created in 1994 by Noar et al.[1]. A person who creates share using this technique is called dealer. By using a secret binary image, the dealer creates n shares, prints them on transparency, and then distributes them to n stakeholders. The human visual system (HVS) can decipher concealed secret picture information with only a simple stacking action of the shares. This approach is safe and easy to use, but it has certain drawbacks, like a pixel expansion issue, user unfriendly shares generation, low visual quality of the restored picture, etc. One of the methods offered by researchers to address the issues stated above is PVSS, which is free of the pixel expansion problem.

The PVSS method may either be block based or image based, both of which are distinct but complementary approaches. A complete secret image is used to create shares in image based PVSS [2]–[7], whereas in block based PVSS [8]–[11], individual, non-overlapping image blocks are used to create a complete secret image. Blocks of the secret image are revealed one at a time as BPVSS system [9] progressively reveals all of the information contained in each share. In image based PVSS, as the number of piled shares increases, it enhances contrast of rebuilt secret image.

[1, 2] *Department of Electronics and Telecommunication Engineering, Priyadarshini College of Engineering, Nagpur,(Maharashtra), India*
E-mail: vishal_panchbhai@rediffmail.com, swvarade@gmail.com

User friendly and noise-like shares may be generated using the BPVSS technique. Since the transmission of noiselike shares via the internet raises suspicion among intruders and is not very user friendly, thus meaningful share is a better alternative.

The BPVSS system produces user-friendly shares with low visual quality; thus, the adoption of steganography is the answer to the aforementioned issue. When steganography is used to conceal an image, the cover image's visual quality is far better than the meaningful shares produced by VSS schemes. When BPVSS and LSB are used together, the maximum contrast (as determined by the PSNR, that is standard for measuring performance) and entropy are roughly 31.79 dB and 7.69 [11]. This study suggests a strategy based on cryptography and steganography that uses the BPVSS and PVD technique to enhance the safety and look of the generated shares. Standard performance measures are utilized to ascertain the effectiveness of the proposed system.

The rest of this paper is put together as follows. In section 2, we take quick look at the research on how visual cryptography schemes can be used with steganography methods.

Section 3 discusses the suggested methodology for generating user friendly shares using BPVSS and PVD method. Section 4 contains the experimental findings and comments. Section 5 includes closing comments.

People have always wanted to communicate their data in a private and safe manner. People nowadays trade their personal information over the internet. Cryptography and steganography methods are used on the internet to encrypt and conceal data, respectively. Text based and image based messages are encrypted using different encryption algorithms[1], [4], [6], [9], [10], [12], [13]. Simply said, cryptography is the science of securing information, and steganography is the science of embedding secret. There are three categories of steganography approaches[14],and they are no key, symmetric key and asymmetric key steganography. The techniques to steganography [15], [16]that were mentioned before may be further classified into those that focus on the time domain and those that focus on the transform domain. The proposed system makes use of time domain steganography rather than transform domain steganography since time domain techniques need less time and power than transform domain approaches at secret image rebuild side. There are three methods of steganography that may be used in the time domain. They are Pixel Indicator (PI), Pixel Value Differencing (PVD), and Least Significant Bit (LSB).

Because cryptography or steganography alone cannot offer enough security and confidentiality, the answer to the aforementioned challenge is to use a hybrid technique. The table 1 below depicts many researchers' hybrid approaches to addressing the aforementioned challenge.

2. Literature Survey

Table 1 Comparison of different researcher'shybrid approach

Study	Encryption Technique	Steganography Technique	Secret (Message / Image)	Share Type	Pixel expansion
[17]	VC	LSB	Message / Image	User friendly	Available
[18]	AES & VC	LSB	Message / Image	Non user friendly	Available
[19]	Cipher using blowfish and VC	LSB	Message	User friendly	Available
[20]	VC and secret key	LSB	Message / Image	User friendly	Available
[11]	BPVSS	LSB	Image	User friendly	Not available
[21]	VC and DES	Bit-shifting and LSB	Message / Image	Non user friendly	Available
[22]	VC	Text Based	Message	Non user friendly	Available
[23]	VC	Text Based	Message	Non user friendly	Available

[24]	VC	Text Based	Message	Non user friendly	Available
[25]	Chaotic VC	DCT / DWT	Image	User friendly	Not available
[26]	Secret key and VC	Secret key	Message	User friendly	Available
[27]	AES	MPVD & LSB	Image	User friendly	Not available
Proposed System	BPVSS	PVD	Image	User friendly	Not available

3. Proposed System

First, decide how many shares will be generated in the proposed system and then use the BPVSS technique to create that amount of noiselike shares. Since this method avoids the issue of pixel expansion, the reconstructed secret image will retain the same visual quality of original secret image. Figure 1 is a block schematic of the proposed system, and Figure 2 is an example output from the proposed system on the dealer side.Becausenoiselike shares are not user friendly, pixel value differencing steganography is utilized to construct user friendly shares, which are then distributed among stakeholders. The following algorithm-1 explains how to build user friendly shares using the suggested method. When recovering a secret image, first remove the cover image from each stakeholder's share image before recovering the noiselike share. If recovered shares are stacked, a low visual quality secret image will be recovered; however, for accurate original secret image reconstruction, all noiselike shares are first preprocessed and then piled.

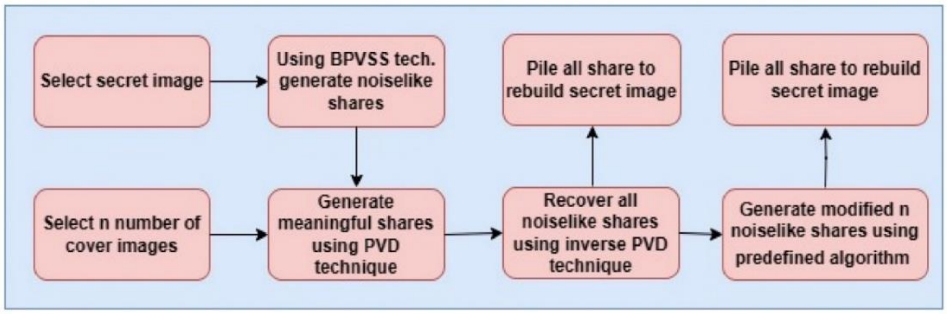
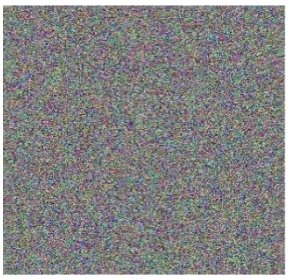


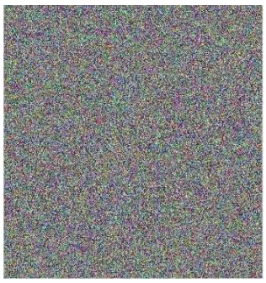
Fig 1: Proposed system block diagram

Using a standard performance metric, the reconstructed secret image's quality will be evaluated. Algorithm 2 illustrates how to reassemble a secret image, Figure 3 depicts the sample output of the proposed system at secret image reconstruction, and Figure 4 depicts histogram analysis of the cover image with and without embedded data.

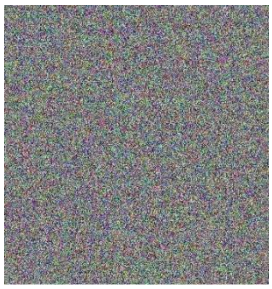
Secret Image



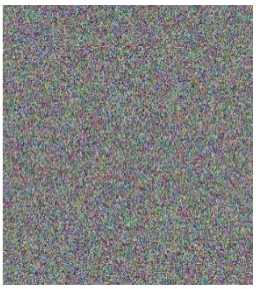
Share 1



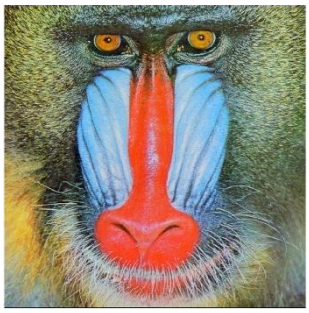
Share 2



Share 3



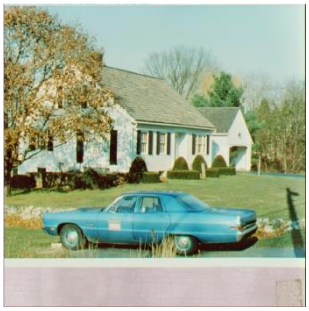
Share 4



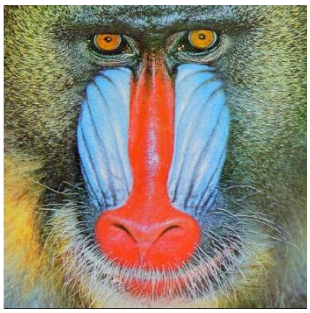
Cover 1

Cover 2

Cover 3



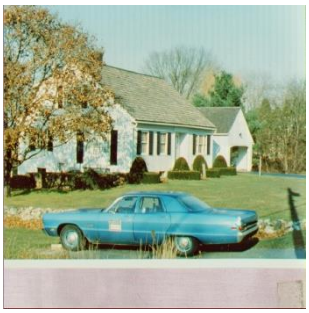
Cover 4



Share 1 Embedded in Cover 1

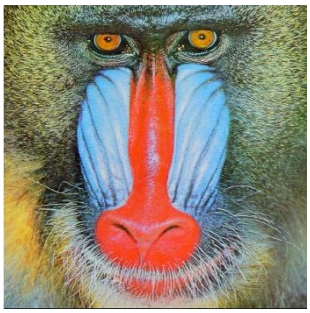
Share 2 Embedded in Cover 2

Share 3 Embedded in Cover 3



Share 4 Embedded in Cover 4

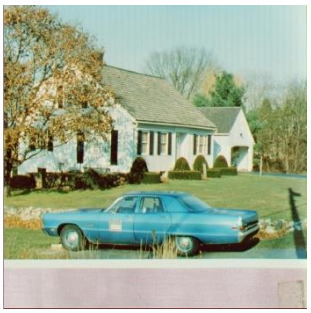
Fig 2: Proposed system sample output for color secret image (lena_color_256.tiff) at dealer side



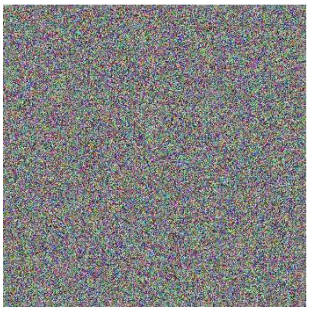
Share 1 Embedded in Cover 1

Share 2 Embedded in Cover 2

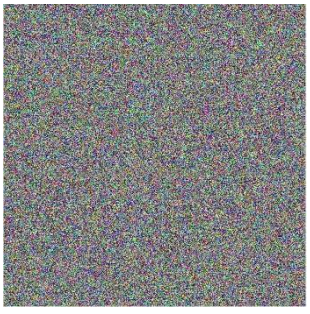
Share 3 Embedded in Cover 3



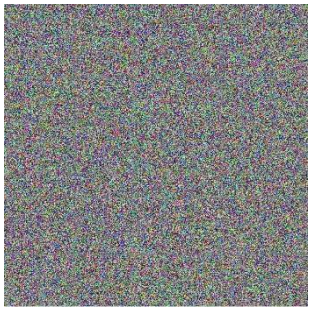
Share 4 Embedded in Cover 4



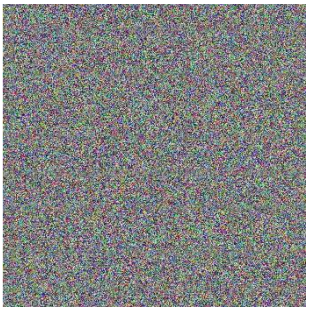
Recovered Share 1



Recovered Share 2



Recovered Share 3



Recovered Share 4


Processed Share 1


Processed Share 2


Processed Share 3


Processed Share 4

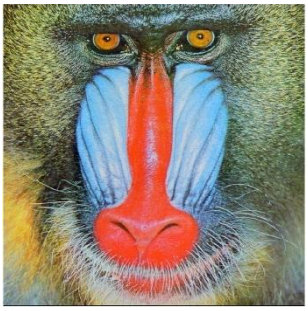

Unprocessed Piled Shares Output

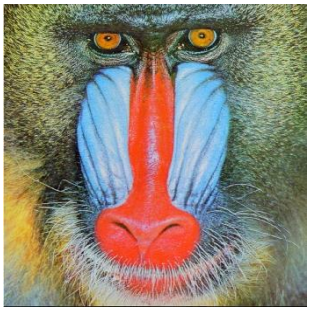

Processed Piled Shares Output

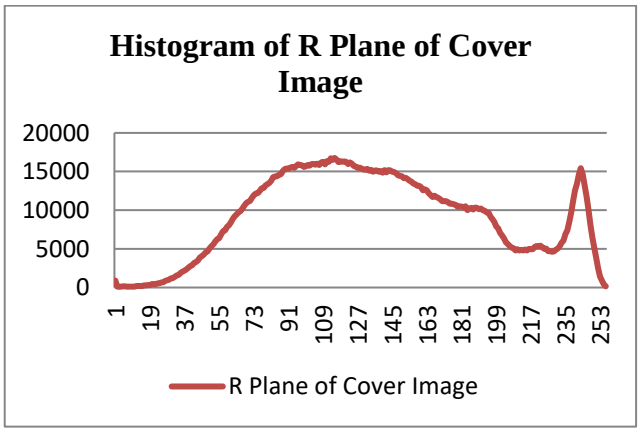
Fig 3: Propose system sample output at color secret image reconstruction side

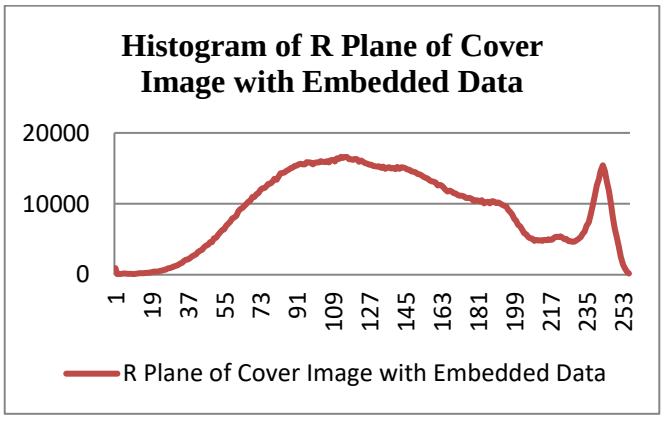
A) Generation of share using BPVSS technique

In the suggested system, n number of noiselike shares are generated from color secret image using BPVSS based approach[8].The BPVSS technology is able to expose a hidden picture block by block. The halftoning approach used in this study is bitslicing. The BPVSS


Cover 1


Share 1 Embedded in Cover 1





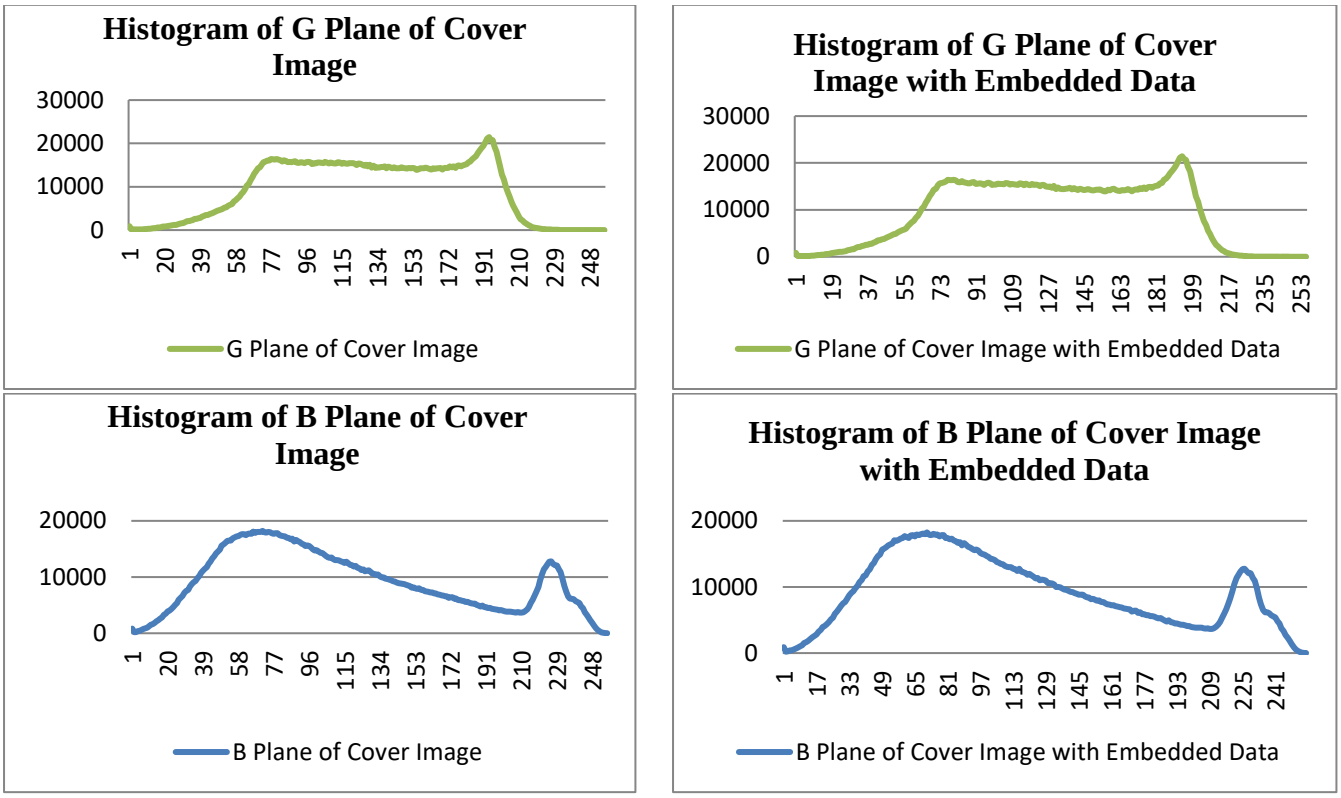
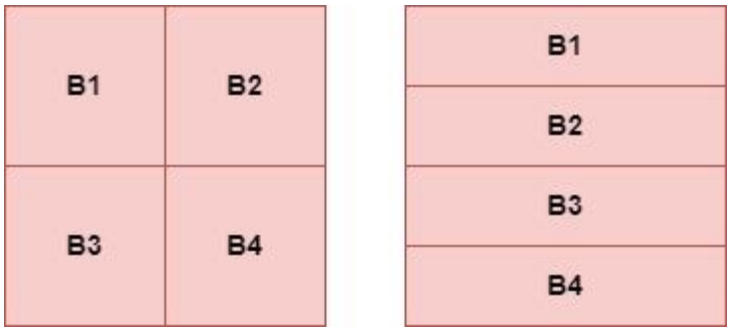


Fig 4: Histogram of cover image with and without embedded data

method has following stages: create n number of non-overlapping blocks (B_1, B_2,---,B_n) from whole secret image, say B, corresponding to the quantity of stakeholders. Examples of splitting patterns of secret image are shown in figure 5. Secret image splitting must satisfy the following equation number (1), according to description of BPVSS technique.



(a) (b)

Fig 5: Different image splitting patterns (a) pattern-1 (b) pattern-2

$$B = U\ B_i \qquad \text{for } 1 \le i \le n$$

$$B_i \cap B_j = NULL \quad \text{for } 1 \le i \ne j \le n \qquad (1)$$

Then, using the following equations (2) and (3), generate n+1 basis matrices of 2 x n size, with the C^0 matrix representing a block with white pixel and the C^m matrix representing a black pixel in each block.

$$C^0 = [M_{r1c1}]_{2xn} = \begin{cases} 0, & \text{if } r1=1,\ 1 \le c1 \le n \\ 1, & \text{if } r1=2,\ 1 \le c1 \le n \end{cases} \qquad (2)$$

$$C^m = [M_{r1c1}]_{2xn} = \begin{cases} 1, & \text{if } r1 = 1,\ 1 \le c1 = m \le n \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

Where m = 1, 2, 3, ----, n

Following table 2 shows basis matrices for noiselike share creation using BPVSS technique.

Table 2 Basis matrices for noiselike share creation using BPVSS technique

Matrices	$C^0 = \begin{bmatrix} 0\,0 \ldots\ldots 0\,0 \\ 1\,1 \ldots\ldots 1\,1 \end{bmatrix}$	$C^1 = \begin{bmatrix} 1\,0 \ldots\ldots 0\,0 \\ 0\,1 \ldots\ldots 1\,1 \end{bmatrix}$	$C^2 = \begin{bmatrix} 0\,1 \ldots\ldots 0\,0 \\ 1\,0 \ldots\ldots 1\,1 \end{bmatrix}$	------	$C^m = \begin{bmatrix} 0\,0 \ldots\ldots 0\,1 \\ 1\,1 \ldots\ldots 1\,0 \end{bmatrix}$
Explanation	For white pixel in all blocks use above matrix	For black pixel in this block use above matrix	For black pixel in this block use above matrix	-----	For black pixel in this block use above matrix

The secret image is then converted to a binary image using bit slicing halftoning method. Use the aforementioned basis matrices to process the pixels of each non-overlapping block separately.If pixel is white and originates from block B^m, use th C^0 basis matrix for share generation; otherwise, use the C^m basis matrix for share generation. To make it easier to predict the pixel value of the related shares, the proposed system picks at random one row from the C^0 basis matrix for white pixels and one row from the C^1 to C^m basis matrices for black pixels of the relevant block. As a result, there is a 50% chance that each row will be chosen, increasing share security.

B) Embed noiselike share in cover image using PVD method

The user friendly share has excellent visual quality and doesn't make data embedding look suspicious to outsiders. Thus, the PVDtechnology is used in proposed system forinsertingnoiselike shares in the cover image. The cover image's embedding capacity must be bigger than the secret image's size (in bits).Baboon, flowers, house and peppers are only some of examples of cover images utilized in proposed system. Size of each cover is 2048 x 2048 x 3. Below is presentation of the PVD technique for embedding a share in a cover image.

Step1: Select color noiselike share image

Step2: Separate planes of share

Step3: Convert each plane in serial stream of bits

Step4: Select cover image based on embedding capacity of image

Step5: Calculate the difference between two neighboring pixels in cover imagei.e.

$d = |P_{i+1} - P_i|$

Step 6: Use the following table to calculate how many bits should be hidden in the cover image.

Table 3 Number of bits to be encoded in cover image

Pixel Difference Range (With lower & Upper Limit)	**Lower limit of range (L_k)**	**Range**	**No. of Bits can be Embedded**
0—7	0	8	3
8—15	8	8	3
16—31	16	16	4
32—63	32	32	5
64—127	64	64	6
128—255	128	128	7

Step7: Select that numbers of bits from bit stream and convert it into decimal form

Step8: calculate addition of lower limit and decimal value of bits stream using following formula

d' = (bitvalue of secret image + Lower limit of range (L_k)) if $d \geq 0$

d' = - (bitvalue of secret image + Lower limit of range (L_k)) if $d < 0$

Step9: calculate difference between d' and d which is denoted by M. Also calculate floor and ceiling value of M using following formula

$M = d' - d$

$M\_Ceiling = (M/2)_{ceil}$

$M\_Floor = (M/2)_{floor}$

Step 10: Calculate modified pixel values of cover image (which is denoted by Q_{i+1} and Q_i)using following formula

$Q_{i+1} = P_{i+1} + M\_Floor$ for d modulo $2 \neq 0$

$Q_i = P_i - M\_Ceiling$ for d modulo $2 \neq 0$

$Q_{i+1} = P_{i+1} + M\_Ceiling$ for d modulo $2 = 0$

$Q_i = P_i - M\_floor$ for d modulo $2 = 0$

If bits of R-plane of secret image are 11100010111000101110000---- then following table gives different steps output

Table 4 Different steps output values of PVD algorithm

Pixel value of R-plane (cover image)	**130**	**138**	**140**	**143**	**142**	**144**	**142**	**148**
Pixel Difference (d)	8		3		2		6	
Pixel Difference Range	8-15		0-7		0-7		0-7	
Lower limit of range (l_k)	8		0		0		0	
No. of Bits can be Embedded	3		3		3		3	
Bits from stream	111		000		101		110	
Decimal equivalent of bit stream	7		0		5		6	
Calculate d'=l_k + Decimal bit stream value	(8+7) 15		(0+0) 0		(0+5) 5		(0+6) 6	
Calculate M=d'-d	7		-3		3		0	
M_Ceiling	4		-1		2		0	
M_Floor	3		0		1		0	
Modified cover image pixel values	127	141	140	143	141	145	142	148

Following algorithm-1 shows steps to generate user friendly shares, while algorithm-2 shows steps to rebuild secret image.

Proposed system algorithm-1(at share generation side)

Inputs: i) Color secret image

ii) Quantity of shares to be generated (n)

iii) n number of cover image

Output: n number of user friendly shares with embedded data

1) Choose the secret color image for which shares will be generated.

2) Decide the number of shares needed (n), and then divide the color secret image into n number of non overlapping blocks (m).

3) Create n noiselike shares using the BPVSS method.

4) Select n color cover image based on embedding capabilities. Using the PVD method, generate user friendly shares by inserting noiselike share data into the cover image.

5) Figure out a standard performance metric of generateduser friendly shares.

Proposed system algorithm-2 (at secret image rebuild side)

Input: All n number of user friendly shares

Output: i) Secret image with poor visual quality

ii) Secret image with original secret image visual quality

1) Choose all n number of user friendly shares

2) Use the inverse PVD technique to recover n noiselike shares after removing the cover image from all user friendly shares.

3) Create an original secret image by stacking n noiselike shares.

4) Apply a predefined algorithm to n noiselike shares to get modified n noiselike shares.

5) Generate the original secret image by piling n noiselike modified shares.

6) As a typical performance measure, calculate parameters such as structural similarity index, peak signal to noise ratio, andmean squared error of a rebuilt original secret image.

Above figure 2 and 4 demonstrate the suggested system output at share generation side and the secret image reconstruction side.

4. Results & Discussion

This study was conducted on an individual's Windows 10 HP laptop with MATLAB 2015a as software tool, with Intel i5 CPU and 8 GB RAM. Images from USC SIPI image database [28], chapter 6 of Digital Image Processing, 3rd edition by Gonzalez and Woods [29] and Wang's image database [30] were used for experiments. In Wang's image database total 1000 images are available.

The BPVSS approach is utilized in a proposed system for producing n noiselike shares. Noiselike shares don't provide visual information to the human visual system. The security of shares is increased when share structures become more random, but this also makes it difficult for shareholders and dealers to identify individual shares. Therefore, user-friendly sharing enters the scene. It resolves the aforementioned issue. To provide user-friendly sharing, the proposed system combines the BPVSS and PVD methods. The outcome of the proposed system for a color secret image is shown in figure 2 above. The spatial domain steganography technique used in the proposed system is PVD rather than LSB because 1) generated visual share quality is superior to LSB-based technique, and 2) it is very difficult for intruder to identify existence of embedded data through histogram analysis technique. Above figure 4 shows histogram analysis of cover image with and without embedded data.

Bit slicing technique is used in place of error diffusion method for halftoning in the proposed approach because 1) it needs fever time and computational power to rebuild the original secret image, and 2) inverse halftoning requires relatively less arithmetic calculation.

It has been discovered that the choice of a cover image for a certain share relies on 1) the quantity of bits available in the secret image planes, and 2) the embedding capability of the relevant cover image planes. If the capacity of embedding cover image is much more than the capacity of bits of secret image, then the PSNR value of the produced shares is excellent. Following table 5 shows different cover image embedding capacity according to respective planes. Furthermore, it has been discovered that the histogram analysis approach may be used to predict the presence of embedded data in a cover image when the number of consecutive pixel difference values in the image is greater than or equal to 128. Table 7 shows PSNR value comparison of proposed system with other method.

It has also been discovered that the size of the cover image is at least double the size of the secret image for successful embedding of total data. Time needed to reconstruct a secret image rises proportionately with secret image size.

In proposed system first Noiselike shares are reconstructed form meaningful shares using inverse PVD method then recovered shares are processed then it is stacked to get original color secret image. Therefore, overall time and power complexities required is more at secret reconstruction side.

Peak signal to noise ratio and entropy, respectively, are used as standard performance measures[31], [32] at the dealer side to assess the quality and safety of created shares. Entropy is a metric for measurement of randomness structure in images. Its value ranges from 0 to 8, where 0 denotes complete uniform structure and 8 denotes maximum randomness in an image.

Entropy values for user-friendly shares should be close to the entropy of cover image. Table 6 shows entropy comparison of proposed system with other method.

Similar to this, the structural similarity index, peak signal to noise ratio, and mean squared error used to evaluate the visual quality of the rebuilt secret image. The reading for all reconstructed secret image for MSE, PSNR and SSIM were zero, infinity and one respectively in the proposed system. Therefore, a rebuilt secret image has same visual quality just likeoriginal.Table8 shows proposed system performance analysis at secret image reconstruction side using standard performance measure.

5. Conclusion

To develop user-friendly shares in the proposed system, BPVSS and PVD based approaches are applied. The BPVSS approach was chosen for share creation because it is free of the pixel expansion issue, and the PVD technique was chosen because it produces a higher quality cover image with embedded data than the LSB technique. The entropy of user friendly shares are near to the entropy of a cover image without embedded data, making it difficult for an intruder to infer the presence of hidden data through histogram analysis. As a result, it indicates that the suggested solution improves cryptographic security. How to rebuild large secret images in less time using the inverse PVD approach is interesting and deserve further studying.

Table 5 Embedding capacity of different cover images

Cover Image Name	Cover Image Dimension	Data Hiding Capacity of Cover Image (Bits)		
		R-Plane	G-Plane	B-Plane
pool.jpg	128X128X3	25679	25492	25512
girl3.tiff	256X256X3	99865	99651	99642
house1.tiff	256X256X3	100339	101615	101859
girl2.tiff	256X256X3	102113	101712	102953
girl4.tiff	256X256X3	102596	103574	102317
pair.tiff	256X256X3	103028	102611	102737
lena_color_256.tiff	256X256X3	105103	106975	103782
tree.tiff	256X256X3	106947	108822	108049
woman_baby_original.tif	512X512X3	394733	394818	394845
color_bars.tif	512X512X3	397442	399134	395751
splash.tiff	512X512X3	398733	402210	400556
fruits.png	512X512X3	404158	406793	406627
flower.tiff	512X512X3	407076	410044	416173
strawberries_fullcolor.jpg	512X512X3	407914	407973	407420
airplane.png	512X512X3	407934	412946	403298
peppers.png	512X512X3	412649	413861	410205
top_left_flower.jpg	512X512X3	418334	418719	420319
lake.tiff	512X512X3	419077	438334	432180
house.tiff	512X512X3	421304	423985	417749
baboon.png	512X512X3	458946	470530	476319
monarch.png	512X768X3	610977	612012	612004
sails.png	512X768X3	640373	637953	637236
watch.png	768X1024X3	1215174	1214995	1207388
pappers_1024x1024.tiff	1024X1024X3	1581470	1594084	1585657
flower_1024x1024.tiff	1024X1024X3	1581690	1583714	1599812

house_1024x1024.tiff	1024X1024X3	1599812	1604513	1600049
baboon_1024x1024.png	1024X1024X3	1609898	1632298	1650199
flower_1536x1536.tiff	1536X1536X3	3548634	3551305	3566971
pappers_1536x1536.png	1536X1536X3	3549284	3562171	3550059
house_1536x1536.tiff	1536X1536X3	3568600	3577398	3565630
baboon_1536x1536.png	1536X1536X3	3595512	3626079	3649417
flower_2048x2048.tiff	2048X2048X3	6298349	6300310	6316216
pappers_2048x2048.png	2048X2048X3	6301946	6315222	6300381
house_2048x2048.tiff	2048X2048X3	6315547	6325213	6313954
baboon_2048x2048.png	2048X2048X3	6332719	6362041	6387999

Table 6 Entropy comparison of proposed system with other method (at share generation side)

	BPVSS and LSB based algorithm [11]				**BPVSS and PVD based algorithm**			
SecretImage	**Entropy**				**Entropy**			
	Share-1	**Share-2**	**Share-3**	**Share-4**	**Share-1**	**Share-2**	**Share-3**	**Share-4**
airplane.png	7.775116	7.693179	7.774665	7.553047	7.744439	7.676313	7.702091	7.49694
color_bars.tiff	7.77511	7.693152	7.77466	7.553017	7.74444	7.676295	7.702087	7.496938
fruits.png	7.775127	7.693177	7.774647	7.553047	7.744436	7.676312	7.70208	7.496924
girl2.tiff	7.725249	7.691688	7.772068	7.548632	7.743786	7.674386	7.692852	7.492246
girl3.tiff	7.725252	7.6917	7.772081	7.548734	7.743787	7.674387	7.692866	7.492271
girl4.tiff	7.725236	7.691644	7.771965	7.548681	7.743786	7.674383	7.692853	7.492242
house1.tiff	7.725304	7.69172	7.772042	7.548677	7.743786	7.67438	7.692856	7.492254
lake.tiff	7.775092	7.693173	7.774645	7.553028	7.744434	7.676302	7.702058	7.496926
lena_color_256.tiff	7.725242	7.691694	7.771975	7.548698	7.743786	7.674384	7.692841	7.492219
monarch.png	7.77564	7.693135	7.77486	7.553027	7.745466	7.677151	7.708019	7.497758
pair.tiff	7.725311	7.691617	7.772009	7.548727	7.743788	7.674384	7.69285	7.492248
pool.jpg	7.658762	7.679681	7.770208	7.534743	7.743702	7.674072	7.692041	7.489117
sails.png	7.775654	7.693128	7.774846	7.553033	7.74546	7.677147	7.707996	7.497746
splash.tiff	7.775107	7.693166	7.774657	7.553037	7.744434	7.676308	7.702079	7.496925
strawberries_fullcolor.jpg	7.775119	7.693153	7.774644	7.553043	7.744432	7.676313	7.702018	7.496986
top_left_flower.jpg	7.775108	7.693158	7.774643	7.553035	7.744435	7.676314	7.702063	7.496929
tree.tiff	7.725193	7.691679	7.772014	7.548646	7.743785	7.674382	7.692851	7.492221
watch.png	7.764169	7.692765	7.774409	7.553411	7.747349	6.094974	7.72857	7.508703
woman_baby_original.tif	7.775106	7.693164	7.774657	7.553046	7.744432	7.676302	7.702064	7.496918
Average=	**7.7501**	**7.691883**	**7.773458**	**7.55049**	**7.744419**	**7.592342**	**7.700165**	**7.495501**

Note that entropy of cover image without embedded data are 7.7437, 7.6739, 7.6914 and 7.4865 for baboon, flower, pappers and house image respectively.

Table 7 PSNR comparison of proposed system with other method (in dB) (at share generation side)

Secret Image	**BPVSS and LSB based algorithm**[11]				**BPVSS and PVD based algorithm**			
	PSNR				**PSNT**			
	Share-1	**Share-2**	**Share-3**	**Share-4**	**Share-1**	**Share-2**	**Share-3**	**Share-4**
airplane.png	31.83728	31.81899	31.74541	31.75179	47.89514	47.75222	48.06056	47.40143
color_bars.tif	31.83621	31.8175	31.7437	31.74651	47.89384	47.75373	48.05413	47.39442
fruits.png	31.83105	31.81208	31.74152	31.74641	47.89664	47.75189	48.06156	47.40216
girl2.tiff	31.83379	31.81917	31.75752	31.76393	53.48277	53.72495	54.20279	52.69785
girl3.tiff	31.83989	31.82574	31.76544	31.75956	53.48045	53.72532	54.20036	52.69579
girl4.tiff	31.84669	31.81441	31.77111	31.76658	53.47163	53.71535	54.19508	52.69684
house1.tiff	31.84134	31.81904	31.77949	31.77529	53.47446	53.71471	54.21124	52.68931
lake.tiff	31.83256	31.82118	31.74121	31.75716	47.89307	47.75411	48.05824	47.39543
lena_color_256.tiff	31.83864	31.81898	31.76173	31.75885	53.47786	53.71561	54.20611	52.69781
monarch.png	31.83111	31.81732	31.74107	31.74324	46.27714	46.05724	46.27293	45.83282
pair.tiff	31.83183	31.81198	31.77009	31.76395	53.46617	53.70871	54.20346	52.68939
pool.jpg	31.83532	31.82022	31.78975	31.76106	58.84305	59.70303	60.18113	58.21011
sails.png	31.83302	31.81928	31.73821	31.74744	46.279	46.05941	46.27263	45.8361
splash.tiff	31.83523	31.81673	31.7399	31.75389	47.8986	47.74911	48.06319	47.40276
strawberries_fullcolor.jpg	31.83746	31.82013	31.73792	31.74509	47.8963	47.75384	48.05251	47.3915
top_left_flower.jpg	31.83301	31.81427	31.74123	31.74204	47.89555	47.75519	48.05906	47.398
tree.tiff	31.83355	31.8139	31.76085	31.75184	53.47795	53.71569	54.20316	52.69888
watch.png	31.83341	31.81687	31.75102	31.75461	43.36902	11.43511	43.23055	42.85546
woman_baby_original.tif	31.83996	31.81792	31.75052	31.75256	47.89887	47.75793	48.0553	47.3914
Average=	**31.83586**	**31.81767**	**31.75409**	**31.75483**	**50.11934**	**48.48964**	**50.5181**	**49.5146**

Table 8 Proposed system performance analysis at secret image rebuilds side

Secret image	MSE of Rebuild Image	PSNR of Rebuild Image	SSIM of Rebuild Image
airplane	0	# infinity	1
color_bars.tif	0	infinity	1
fruits.png	0	infinity	1
girl2.tiff	0	infinity	1
girl3.tiff	0	infinity	1
girl4.tiff	0	infinity	1
house1.tiff	0	infinity	1
lake.tiff	0	infinity	1
lena_color_256.tiff	0	infinity	1

monarch.png	0	infinity	1
pair.tiff	0	infinity	1
pool.jpg	0	infinity	1
sails.png	0	infinity	1
splash.tiff	0	infinity	1
strawberries_fullcolor.j	0	infinity	1
top_left_flower.jpg	0	infinity	1
tree.tiff	0	infinity	1
watch.png	0	infinity	1
woman_baby_original.tif	0	infinity	1

It indicates rebuilt secret image has the same visual quality as the original.

References

[1] M. Naor and A. Shamir, "Visual cryptography," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 950, pp. 1–12, 1994, doi: 10.1007/BFB0053419.

[2] W. P. Fang and J. C. Lin, "Progressive viewing and sharing of sensitive images," *Pattern Recognit. Image Anal.*, vol. 16, no. 4, pp. 632–636, 2006, doi: 10.1134/S1054661806040080.

[3] W. P. Fang, "Friendly progressive visual secret sharing," *Pattern Recognit.*, vol. 41, no. 4, pp. 1410–1414, 2008, doi: 10.1016/j.patcog.2007.09.004.

[4] R. Wang, "Region Incrementing Visual Cryptography," *IEEE Signal Process. Lett.*, vol. 16, no. 8, pp. 659–662, 2009, doi: 10.1109/LSP.2009.2021334.

[5] S.-K. Chen, "Friendly progressive visual secret sharing using generalized random grids," *Opt. Eng.*, vol. 48, no. 11, p. 117001, 2009, doi: 10.1117/1.3262345.

[6] Y. C. Hou and Z. Y. Quan, "Progressive visual cryptography with unexpanded shares," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 11, pp. 1760–1764, 2011, doi: 10.1109/TCSVT.2011.2106291.

[7] A. Mohanasundaram and S. K. Aruna, "International Journal of Intelligent Networks Improved Henon Chaotic Map-based Progressive Block-based visual cryptography strategy for securing sensitive data in a cloud EHR system," *Int. J. Intell. Networks*, vol. 3, no. August, pp. 109–112, 2022, doi: 10.1016/j.ijin.2022.08.004.

[8] R. Z. Wang, Y. K. Lee, S. Y. Huang, and T. L. Chia, "Multilevel visual secret sharing," *Second Int. Conf. Innov. Comput. Inf. Control. ICICIC 2007*, pp. 283–286, 2007, doi: 10.1109/ICICIC.2007.401.

[9] Y. C. Hou, Z. Y. Quan, C. F. Tsai, and A. Y. Tseng, "Block-based progressive visual secret sharing," *Inf. Sci. (Ny).*, vol. 233, pp. 290–304, 2013, doi: 10.1016/j.ins.2013.01.006.

[10] N. C. Mhala, R. Jamal, and A. R. Pais, "Randomised visual secret sharing scheme for grey-scale and colour images," *IET Image Process.*, vol. 12, no. 3, pp. 422–431, 2018, doi: 10.1049/iet-ipr.2017.0759.

[11] V. V. Panchbhai and S. W. Varade, "Hybrid Approach to Enhance Security and Friendliness of Visual Secret Sharing Scheme," *Int. Conf. Emerg. Trends Eng. Technol. ICETET*, vol. 2022-April, 2022, doi: 10.1109/ICETET-SIP-2254415.2022.9791815.

[12] F. S. Abas and R. Arulmurugan, "Radix Trie improved Nahrain chaotic map-based image encryption model for effective image encryption process," *Int. J. Intell. Networks*, vol. 3, no. August, pp. 102–108, 2022, doi: 10.1016/j.ijin.2022.08.002.

[13] F. Thabit, O. Can, S. Alhomdy, G. H. Al-Gaphari, and S. Jagtap, "A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing," *Int. J. Intell. Networks*, vol. 3, no. July 2021, pp. 16–30, 2022, doi: 10.1016/j.ijin.2022.04.001.

[14] C. P. Sumathi, T. Santanam, and G. Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding," *Int. J. Comput. Sci. Eng. Surv.*, vol. 4, no. 6, pp. 9–25, 2013, doi: 10.5121/ijcses.2013.4602.

[15] N. Kaur and S. Behal, "A Survey on various types of Steganography and Analysis of Hiding Techniques," *Int. J. Eng. Trends Technol.*, vol. 11, no. 8, pp. 388–392, 2014, doi: 10.14445/22315381/ijett-v11p276.

[16] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, 2019, doi: 10.1016/j.neucom.2018.06.075.

[17] J. K. Mandal and S. Ghatak, "Secret image / message transmission through meaningful shares using (2, 2) visual cryptography (SITMSVC)," *Int. Conf. Recent Trends Inf. Technol. ICRTIT 2011*, pp. 263–268, 2011, doi: 10.1109/ICRTIT.2011.5972344.

[18] K. S. Seethalakshmi, B. A. Usha, and K. N. Sangeetha, "Security enhancement in image steganography using neural networks and visual cryptography," *2016 Int.*

Conf. Comput. Syst. Inf. Technol. Sustain. Solut. CSITSS 2016, pp. 396–403, 2016, doi: 10.1109/CSITSS.2016.7779393.

[19] Swathi, V. N. V. L. S. ., Kumar, G. S. ., & Vathsala, A. V. . (2023). Cloud Service Selection System Approach based on QoS Model: A Systematic Review. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 05–13. https://doi.org/10.17762/ijritcc.v11i2.6104

[20] S. H. Murad, A. M. Gody, and T. M. Barakat, "Enhanced Security of Symmetric Encryption Using Combination of Steganography with Visual Cryptography," *Int. J. Eng. Trends Technol.*, vol. 65, no. 3, pp. 149–154, 2018, doi: 10.14445/22315381/ijett-v65p227.

[21] M. A. Islam, M. A. A. K. Riad, and T. S. Pias, "Enhancing Security of Image Steganography Using Visual Cryptography," *Int. Conf. Robot. Electr. Signal Process. Tech.*, pp. 694–698, 2021, doi: 10.1109/ICREST51555.2021.9331225.

[22] S. Chavan and Y. B. Gurav, "Lossless Tagged Visual Cryptography Scheme Using Bit Plane Slicing for Image Processing," *Proc. Int. Conf. Inven. Res. Comput. Appl. ICIRCA 2018*, no. Icirca, pp. 1168–1172, 2018, doi: 10.1109/ICIRCA.2018.8596778.

[23] S. Roy and P. Venkateswaran, "Online payment system using steganography and visual cryptography," in *2014 IEEE Students' Conference on Electrical, Electronics and Computer Science*, 2014, pp. 1–5, doi: 10.1109/SCEECS.2014.6804449.

[24] V. Lokeswara and T. Anusha, "Combine Use of Steganography and Visual Cryptography for Online Payment System," *Int. J. Comput. Appl.*, vol. 124, no. 6, pp. 7–11, 2015, doi: 10.5120/ijca2015905494.

[25] S. S. More, A. Mudrale, and S. Raut, "Secure Transaction System using Collective Approach of Steganography and Visual Cryptography," *2018 Int. Conf. Smart City Emerg. Technol. ICSCET 2018*, pp. 1–6, 2018, doi: 10.1109/ICSCET.2018.8537262.

[26] M. Mostaghim and R. Boostani, "CVC: Chaotic visual cryptography to enhance steganography," *2014 11th Int. ISC Conf. Inf. Secur. Cryptology, Isc. 2014*, pp. 44–48, 2014, doi: 10.1109/ISCISC.2014.6994020.

[27] Y. K. Meghrajani and H. S. Mazumdar, "Hiding secret message using visual cryptography in steganography," *12th IEEE Int. Conf. Electron. Energy, Environ. Commun. Comput. Control (E3-C3), INDICON 2015*, pp. 1–5, 2016, doi: 10.1109/INDICON.2015.7443677.

[28] Muhammad Khan, Machine Learning for Predictive Maintenance in Manufacturing: A Case Study , Machine Learning Applications Conference Proceedings, Vol 1 2021.

[29] A. K. Shukla, A. Singh, B. Singh, and A. Kumar, "A Secure and High-Capacity Data-Hiding Method Using Compression, Encryption and Optimized Pixel Value Differencing," *IEEE Access*, vol. 6, pp. 51130–51139, 2018, doi: 10.1109/ACCESS.2018.2868192.

[30] "The USC-SIPI Image Database." https://sipi.usc.edu/database/database.php?volume=misc? (accessed May 20, 2020).

[31] Gonzalez and Woods, "DIP3/e—Book Images Downloads," *ImageProcessingPlace.com*. https://www.imageprocessingplace.com/DIP-3E/dip3e_book_images_downloads.htm (accessed Jul. 05, 2021).

[32] J. Li and J. Z. Wang, "Automatic linguistic indexing of pictures by a statistical modeling approach," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 9, pp. 1075–1088, 2003, doi: 10.1109/TPAMI.2003.1227984.

[33] V. V. Panchbhai and S. W. Varade, "A Review on Visual Secret Sharing Schemes for Binary, Gray & Color Image," *Biosci. Biotechnol. Res. Commun.*, vol. 13, no. 14, pp. 268–272, 2020, doi: 10.21786/bbrc/13.14/63.

[34] N. Ahmed, H. M. Shahzad Asif, and G. Saleem, "A Benchmark for Performance Evaluation and Security Assessment of Image Encryption Schemes," *Int. J. Comput. Netw. Inf. Secur.*, vol. 8, no. 12, pp. 28–29, 2016, doi: 10.5815/ijcnis.2016.12.03.