International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys.13, No.1 (Apr-23)

http://dx.doi.org/10.12785/ijcds/130176

Hiding Data in Binary Images Using Block-Diagonal Partition Pattern (BDPP)

Gyankamal J.Chhajed[1] and Bindu R. Garg[2]

[1]*Department of Computer Engineering ,(Research Scholar) BV(DU)COE, Pune, VPKBIET, Baramati, Pune, India*
[2]*Department of Computer Engineering ,BV(DU)COE, Pune*

Received 8 Jun. 2022, Revised 16 Dec. 2022, Accepted 6 Feb. 2023, Published 16 Apr. 2023

Abstract: Many pieces of information are exchanged in the form of binary pictures across many domains as a result of the paradigm shift from paper to electronic. This covers banking, economic dealings, military communication, and imaging in the medical field. In some circumstances, it is necessary to communicate sensitive information about photographs in a covert manner. On the other hand, unreadable watermarks are necessary to verify the authenticity and originality of an image.The two most commonly used methods for this purpose are steganography and watermarking, both of which ensure the imperceptibility of hidden information.It is challenging for binary images to hide data and to keep changes unnoticeable. A novel data hiding method for binary images is presented in this paper which uses Block-Diagonal Partition Pattern(BDPP).In this method, 3X3 pixels image blocks are partitioned diagonally. Black and white pixel counts within each partition before and after embedding are used to identify potential blocks. The connectivity between the pixels in each division is also examined in order to determine whether a block is suitable for carrying data bits that account for distortion. The chosen block's central pixel serves as the carrier for data bits. Since every block carrying the data satisfies the embeddability requirements both before and after concealing, the original picture is not required to retrieve the concealed data. Data is twice encrypted using this method to boost data security. The results show that our technique produces little distortion while being safe and having great hiding capabilities.

Keywords: Data Hiding,Encryption, Watermarking, Steganography, Block diagonal partition pattern

1. INTRODUCTION

The prevalence of the internet has expanded communication through digital media. For some applications, media material must be supplied covertly, while others demand that the ownership and veracity of the information be verified. Cryptography is typically used for such applications to convey information. However, attackers are attracted to cryptography because they are familiar with how important information is conveyed in the media. Sending information in a manner that is as undetectable as feasible is the answer to this problem. One technique that does this is information concealment. Digital media images could be colourful, binary, or gray scale.Because pixels in black and white graphics are only represented by one bit 0 or 1, concealing data without arousing suspicion is difficult. The only other option is to flip the selected binary image pixel if it does not match the data bit that has to be hidden. Otherwise, the selected pixel delivers data without altering colour. If a binary image's location is studied in relation to the human visual system, each pixel that has been reversed is clearly visible. The capacity of a black and white image to conceal data is constrained by this challenge. Therefore, achieving a balance between optical distortion and concealment capabilities is difficult. To hide data in black and white photos, many different data hiding techniques had been developed. To find the appropriate pixels for data obscurity, strategies made use of edge pixels, borders, blocks, transformation functions, and run lengths. Peak signal to noise ratio (PSNR), Mean square error (MSE), distortion matrix, and other metrics are used to assess the efficacy of data concealment techniques. Other characteristics such as concealing capacity, security, and resilience are used to assess data hiding schemes. The novelty of this technique lies in hiding data with maintained visual artifacts. Additionally this technique provides more block patterns available to hide data which improves hiding capacity compared to related method .This proposed technique also takes care of hidden data security by multilevel encryption and data extraction is possible without the original image. This paper proposes a novel data hiding method in black and white images which can be applied for steganography and authentication purposes. This method uses image blocks of order 3x3 and examines all diagonal partitions of a block applying different tests to qualify block to be embeddable. The black and white pixel counts in diagonal partitions and the type of connectivity among the pixels in a block are deciding factors to hide data in the block.

E-mail address: author 1, author 2, author 3

2. RELATED WORK

The literature is reviewed to determine the methods that are available for secret communication, authentication, steganography, and watermarking. Data concealment in binary text documents was initially accomplished by embedding data in a character's 8-connected border. It selected a predetermined set of pairs of border patterns with a length of five pixels for data embedding. The centre foreground pixel must be removed from one of the patterns in a pair, while one must be added to the other[1]. In exchange for better image quality, the scheme sacrifices some data hiding space. Any bit in the host image that is changed is guaranteed to be next to another bit with the same value as the modified bit. As a result, the hiding effect is virtually undetectable [2].For binary images, discrete cosine domain watermark embedding is examined. [3]. "Flippable" pixels are used to enforce specific blocks-based relationships to embed data without causing noticeable artifacts [4], [5], [6]. A method which can detect virtually all types of binary images while maintaining good visual quality [7]. This research also provides a variant of the suggested approach that can locate the modified region with good spatial precision. By employing a blind data hiding technique, it maintains the connectedness of pixels in a nearby area.Three transition criteria are imposed on a moving window of 3 X 3 pixels to determine the "flippability" of a pixel. In the data hiding process, the "embeddability" of a block is invariant[8]. There is a novel two-layer blind binary image authentication scheme that targets both overall authentication and tampering detection at the same time [9]. The morphological transform domain of binary images is the domain of a data hiding technique [10]. Run-length (RL) histogram modification is used to create alternate sequences of black and white RLs. The image is scanned from left to right and from top to bottom. By combining one black RL with its next white RL, one RL couple is created, resulting in the formation of RL couples [11].Several watermarking and steganographic techniques are reviewed and analyzed. The methods are based on image processing in the spatial and transform domain [12], [13], [14], [15], [16]. The technique minimizes a novel flipping distortion measurement that takes HVS and statistics into account [17]. For fragile embedding applications such as precise authentication, a data concealment approach is proposed. The purpose of image authentication is to ensure that an image hasn't been tampered with since it was left in the hands of a trustworthy party [18]. For the hybrid authentication approach, a new pixel-wise data concealing method is proposed. In both embedding and extraction, its main engine selects a large number of good DCPLs invariably[19].A general approach with nearly theoretical performance is proposed for embedding while reducing any additive distortion function[20]. Hugo, a new embedding algorithm for spatial-domain images, claims to hide seven times more data while providing comparable security to LSB matching [21]. A secret position matrix is designed to maximize hiding capacity using combination theory [22]. Using steganalytic methods, steganographic techniques were used to detect secret messages embedded in black and white images [23], [24], [25].In image based steganography, images are used as cover media to hide secret data [26]. LSB is unlikely to cause significant changes in the image. Visual secret sharing is identified as a risk of secret transmission due to the appearance of meaningful images or noise-like images in VSS. As a solution to this problem, a new Natural image based Visual Secret Sharing scheme was presented in [27]. By dividing the original picture into m by n blocks, it is ensured that any modified bits in the host image must have the same value as bits that are immediately adjacent to them. [28]. As presented in [29], the key idea concerns the concealment of information in images using Zigzag scanning patterns, which is a more complex steganographic algorithm encrypted yet again as shares by achieving authentication by embedding them into separate host images. [30] presents a novel technique for concealing data in binary text pictures.This technique limits the embedding to the edge pixels of all connected components.BST is used to compress a secret image in [31]. However, dividing the compressed data into different ranks depends on their significance. In order to protect the hidden information, a binary matrix and weight matrix are used [32]. To minimize designed embedded distortion and achieve higher security without sacrificing the image quality of embedding capacity, [33] identifies flippable pixels first and manipulates them in a certain manner to hide the message. It has been largely propped up by the growth of the internet. An Image Steganography scheme for different file formats is discussed in [34]. The password is encrypted for the purpose of protecting information in cryptography communication. It will be decrypted by the intended recipient. The matching of bit pairs and symmetric key cryptography are proposed in [35]. Watermark and original image pixels are arranged in pairs. Pixel value difference is used to weight the pixels. By breaking up the binary cover image into non-overlapping sub-blocks, it determines the ideal place to implant each secret bit for each sub-block[36].A block-based information concealing system for binary pictures exists that conceals more information in more intricate blocks.[37]. Data hiding is proposed with high capacity, which minimizes the flipping distortion as measured by the proposed distortion function [38]. The author of the proposal presented evidence that text data could be hidden in text documents through illustration files in formats such as DOC, PPT, TXT, and MATLAB script files [39].Object boundaries can be used to hide secret data embedded in binary cover images [40]. The coding tables are constructed based on HVS in appropriate blocks[41]. The binary host's edge region contains secure data that is incorporated in it. The best changeable pixels are found by dynamically adjusting the distance matrix and calculating the changeable score of each block.[42]. Digital watermark (DWM) implementation algorithms are developed and analyzed to increase their robustness. It is imperative that the same transformations be applied in compression of graphic documents in a stego-algorithm [43]. Secret text bits are embedded directly into the cover

image after encryption using a reference image. Secret text is written/printed on a white canvas and then converted into binary (BW) images in the second variant. There will be a unique reference image that will serve as the encryption key. The use of an extreme learning machine algorithm (ELM) to create a mathematically supervised model is proposed as a new method for image steganography[44].Robots may need to authenticate the images they capture. RDH schemes are capable of authenticating data and/or verifying who owns the data[45]. An improved method than LSB hiding is proposed to achieve information security using DKL algorithm[46]. A multi-class steganlysis method is proposed in[47] which uses SVM classifier to detect different types of steganography .A scheme based on block classification is proposed for hiding high capacity data in binary images. The block classification process identifies complex regions in an image where secret data can be embedded [48]. Hamming codes are used in a data-embedding algorithm, flipping only a small number of pixels in order to minimize visual distortion [49].By tracing the contours of the objects, edge-based grids are used to hide data. A contour segment was identified based on the L-shaped pattern to locate embeddable pixels [50]. Regression analysis model is proposed for performing efficient non-fuzzy operations [51]. Fuzzy Time Series Ordered Weighted Aggregation (OWA) and a more developed predictive model are used to show the validity of the proposed concept [52]. An RDH scheme has been proposed by mirroring the central pixel pattern pair (PPOCP) on the opposite side of the binary image [53]. A new scheme for reversibly hiding data in encrypted binary images has been proposed by joint pixel prediction and bisector compression [54]. To minimize distortion, a four-way scanning method has been proposed to find the best match in the hidden bitmap image [55]. The decision tree is used to find the most suitable block in the image to hide the 4-bit data using the four special location pixels pattern of 3X3 pixel blocks [56], [57].The count of black and white pixels in block partitions along the diagonals and the connectivity among the pixels in the same 3X3 block is used to declare the block's embedability[58].

From the study of related work, it is identified that there is scope in improvement in hiding capacity, security of hidden data maintaining visual artifacts. Again some existing techniques does book keeping for storing hidden data location information which reduces actual data hiding capacity. It is also observed that generally single level of encryption is applied to secure data and whole image scanning is required or in some cases original image is required to get the location of the hidden data while extraction.This finding opens the scope to develop more efficient technique which improves on existing results.

3. PROPOSED MODEL

Many block-based data hiding approaches took into account the entire image block pattern when determining whether a block was appropriate for data hiding. In this approach, the diagonal partitioning pattern of an image

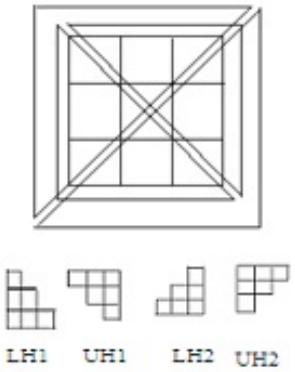

Figure 1. Diagonal partitions

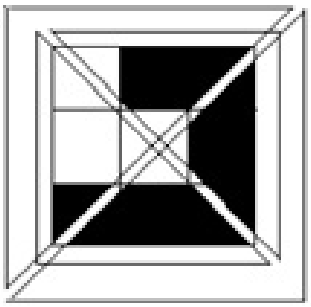

Figure 2. Figure 2. Sample pattern 011001111

block is inspected, and if it meets the requirements for choosing the block to conceal data, the block is chosen to carry information bits.

A. *Block processing*

An innovative method of processing a 3X3 block is suggested in this approach for concealing secret data bits. Fig. 1- 4 and tables 1-3 are used to explain the specifics of block processing. The block is divided into two lower and upper halves, as indicated in fig. 1, and they are referred as indicated. In each diagonal division, the number of black and white pixels is counted. Based on these counts, the preliminary appropriateness of a block to carry data is determined. Fig.3 depicts the diagonal divisions for the example in Fig.2.

Table 1 lists the black and white pixels count in each diagonal division of the example block in Fig. 2 before and after pixel flipping. There are three distinct count pairs before flipping, with the values being 3-3, 4-2, and 5-1, respectively, according to the entries in the table. In these pairs, the first number denotes the count of black pixels, while the second number denotes the count of white pixels.In table 2, these separate pairs are displayed as column headings. The entry in each relevant column for each 3X3 block pattern represents the quantity of these unique pairs that occur. The "Count" column shows count of distinct pairs.

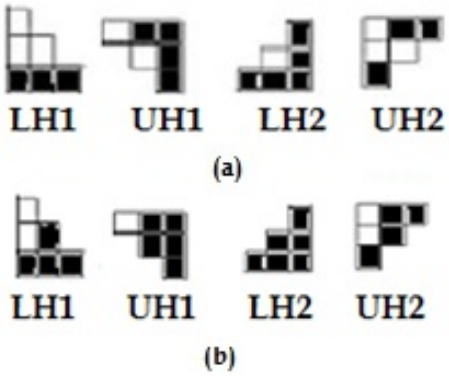

Figure 3. Pictorial representation of Diagonal partition for example Figure 2 (a) before and (b) after flipping

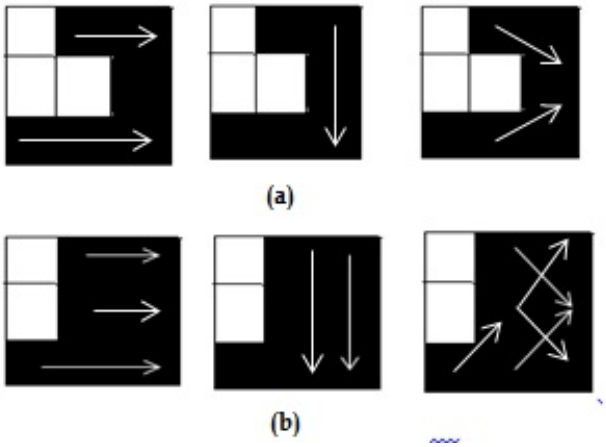

Figure 4. Connectivity for example Figure 2 (a) before and (b) after(b) embedding

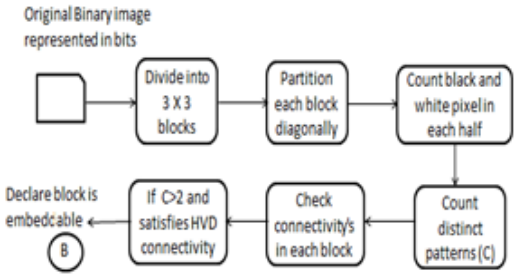

Figure 5. Embeddability test process for block

For the 3X3 pattern illustrated above, table 2 shows the entry for each column prior to embedding. The number of occurrences for the 3-3 pair occurring twice, the 4-2 pair occurring once, and the 5-1 pair occurring once are shown in the corresponding columns. The ”Count” value is ”3” since there are 3 unique pair entries available for that pattern. Similar to table 2, table 3 shows each column’s entry following embedding. In the accompanying columns, the frequency of the 4-2 pair occurring twice, the 5-1 pair occurring once, and the 6-0 pair occurring once is displayed. The ”Count” column’s value is ”3” due to the pattern’s availability of three different pair entries. If any two or more pixels in a block are connected horizontally(H), vertically(V), or diagonally(D), the connectivity along those three axes is tested. Figure 4 depicts ”HVD” connectivity in both its pre-embedded and embedded states for example figure 3. Since every type of connectivity exists in a block both before and after embedding, ”HVD” is written in the ”Connectivity” column of table 2 to reflect this.

If a block only has vertical connectivity, only ”V” will be listed in the ”Connectivity” column for that block. Therefore, the ”Count” column’s entry must be more than or equal to 2 and the ”Connectivity” column’s entry must be ”HVD” in order to designate blocks embeddable. The block processing sequence for evaluating a block’s embeddability is shown in Figure 5.The blocks are initially separated diagonally. For each of the upper and lower halves across both diagonals, the number of black and white pixels is counted, and the counts are paired. It is decided if a block is embeddable or not based on the number of distinct count pairs and the connection inside each block. The embeddable block designated by the letter ”B” is used in the embedding and extraction processes. Since the connection before and after embedding in the example being examined is ”HVD” and the count is 3, the block has passed the embeddability test and is deemed appropriate for transporting data bits.

B. Encryption

The suggested method strongly protects hidden data by applying encryption twice. The very first secret data and two distinct secret keys are required from a sender with the assumption that the sender and recipient will exchange the encryption keys. The secret data to be hidden is then encrypted using one of the encryption keys, like secret key 1, as seen in figure 6. A header that indicates the encrypted data’s length in binary bits is subsequently attached to the previously acquired encrypted data. The combined data is once more encrypted using key 2, the second encryption key. It is explained as follows.

Let X is the information to be embedded and is represented as the set of m characters .

$$X = x_1, x_2, ...x_m \tag{1}$$

Let K1,K2 are two different encryption keys where K1 and K2 are set of characters

$$K = K1, K2 \tag{2}$$

Let D be converted data bits represented as the set of n bits

$$D = d_1, d_2, d_3, ..., d_n \tag{3}$$

Let KB1 and KB2 be the keys in binary format

$$Enc_1 = D \oplus KB1 \tag{4}$$

TABLE I. Black and white pixel counts for the diagonal halves before and after flipping

Halves	Black pixel Count before flipping	White pixel Count before flipping	Black pixel Count after flipping	White pixel Count after flipping
UH1	4	2	5	1
LH1	3	3	4	2
UH2	3	3	4	2
LH2	5	1	6	0

TABLE II. Count for pairs , connectivity and distinct pair count for example figure 3

Label	Pattern	0-6	1-5	2-4	3-3	4-2	5-1	6-0	Connectivity	Count
(a)	011001111	-	-	-	2	1	1	1	HVD	3
(b)	011011111	-	-	-	-	2	1	1	HVD	3

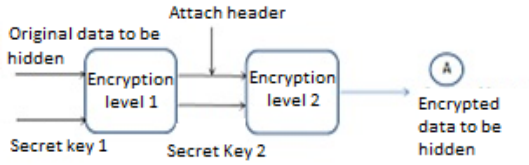

Figure 6. Encryption process

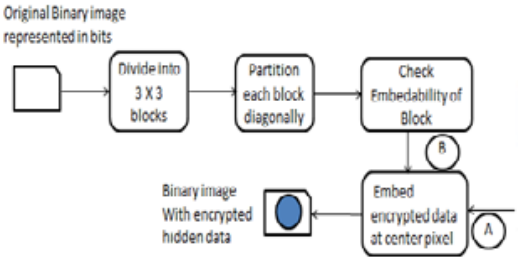

Figure 7. Embedding Process

Let H represents the header

$$AEnc_1 = Enc_1 + H \tag{5}$$

$$Enc_2 = AEnc_1 \oplus KB2 \tag{6}$$

C. Embedding and Extraction process

During the embedding procedure, first the user chooses an image to cover the secret data. Then the binary matrix is created from the given image. The chosen original image binary matrix is separated into non-overlapping 3x3 blocks.Block by block, the picture "I" is scanned to determine which blocks are suitable for holding data. These embeddable blocks are tallied, and the user is prompted to choose another image if the result is fewer than the required amount of bits to be embedded. This process is repeated until a suitable image is selected. A 3X3 pixel non-overlapping block is created from the selected image.Next, the block's embeddability is examined. One bit of the final encrypted data is embedded if the block passes the embeddability test. Depending on the bit that needs to be embedded, this is accomplished by inverting the central pixel if necessary. The image bit stream is transformed back into picture format and transmitted to the recipient when all the bits have been embedded. In figure 7, the embedding procedure is displayed. 'A' denotes encrypted data, while 'B' denotes an embeddable block. The extraction procedure is carried out at the receiver side in the manner seen in figure 8. 3x3 non-overlapping blocks are created from the received binary image. After that, each block is divided diagonally. Applying the same test that is used during embedding, each block is examined to see whether it is carrying data or not. The header length hidden bits are recovered from the central pixel by the receiver if block passes the test which is applied during embedding process. The length of the encrypted secret data bit stream is then determined by decoding the header by Key 2. In accordance with the length information, the appropriate size bit stream is extracted and decrypted using the Key 2 and then with first key, referred to as key1, to produce the original binary sequence of concealed secret data. To recover the original hidden data, the binary format of the secret data is translated back to text.

D. Algorithm for Encryption

1) Get Secret data and two different secret keys Key1 and Key2 as input.
2) Binaries the data and encryption keys.
3) Apply X-OR encryption on binary data and the secret key1.
4) Append header bits prior to encrypted data
5) Encrypt appended data with secret Key2 using X-OR operation
6) Stop

E. Algorithm for embeddability test of a block

1) Take the block and cut it into four equal half using a diagonal slice.
2) Count how many pixels are black and white in each diagonal division, then pair them.

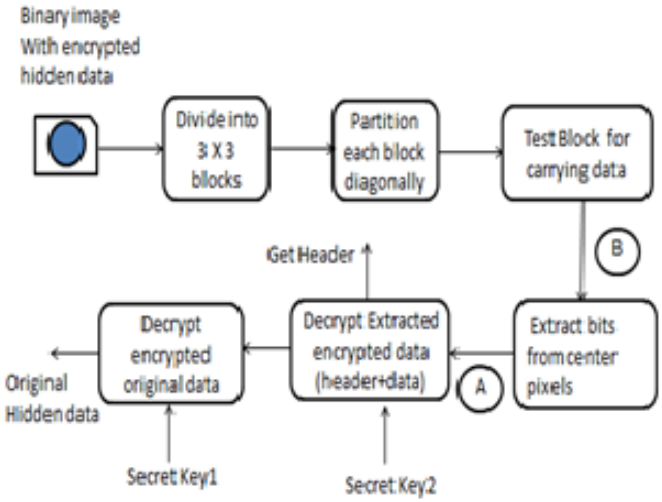

Figure 8. Extraction Process

3) For each block, count the number of distinct pairs before and after embedding.
4) Get the connectivity information for each block.
5) The block is said to pass the embeddability test if it has horizontal, vertical, and diagonal (HVD) connection and the number of distinct pairs is more than or equal to 2.
6) Stop

F. Algorithm for Embedding

1) Get suitable image and divide into 3X3 pixel blocks.
2) Represent block into binary matrix
3) Check whether the block passes the embeddability test in step three.
4) Match the centre bit to incorporate 1 bit of encrypted data by flipping it if necessary if the block passes the test in step 1 above.
5) Apply steps 3 and 4 to embed each encrypted data bit in the same manner.
6) stop

G. Algorithm for extraction

1) Get image with hidden data bits and divide into 3X3 pixel blocks.
2) Represent block into binary matrix
3) Evaluate the block's embeddability to see if it passes.
4) Extract the centre bit if the block passes the test in step 3.
5) Extract header size number of bits of the encrypted data bits in the same way applying step 3 and 4 .
6) The extracted header bits are then decrypted using the secret key2.
7) Get length of encrypted hidden data from the decrypted header and extract bits from further blocks in the same way applying step 3 and 4 and decrypt using secret Key 2.

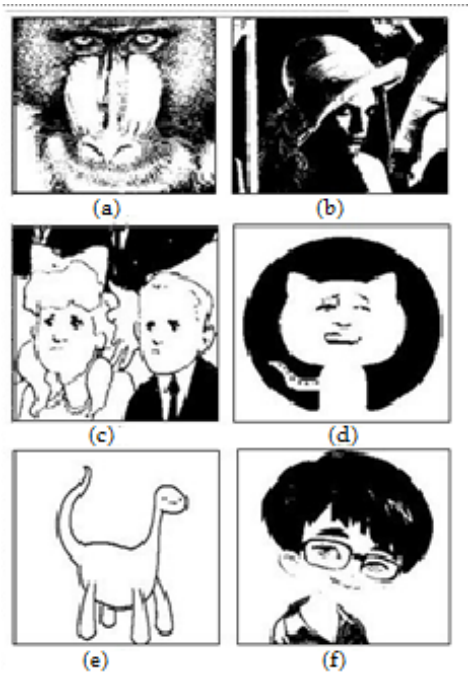

Figure 9. Original images before hiding data (a)Baboon (b)Lena(c)Cartoon(d)Cat(e) Dinosaur(f)Hero

8) Decrypt obtained decrypted data bit in above step by secret key 2 to get the original secret data bits in binary form.
9) Convert bit stream obtained in above step into to text form to get the hidden message.
10) stop

4. PERFORMANCE EVALUATION

The peak signal-to-noise ratio (PSNR) and Mean Squared Error (MSE) are two common metrics for evaluating the efficacy of data concealing strategies. After concealing data in a picture, a high PSNR value suggests less distortion. C is the cover picture of dimension M by N, and S denotes the image after data has been hidden in C while preserving the same dimension M by N. Location of pixel is denoted by (x,y) denotes the and x will have values 0 to M-1and y will have values 0 to N-1 respectively. The PSNR value is calculated as follows:

$$PSNR = 10.log_{10}\left[\frac{MAX^2}{MSE}\right] \tag{7}$$

$$MSE = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(C(x,y) - S(x,y))^2 \tag{8}$$

As discussed in [39] theses metrics are not suitable for binary image. The distortion induced by data hidden in the pixel in a binary image is measured by the influence of a

TABLE III. Result table after hiding data in Figure 9

Image	Image size	Embeddable block	Flipped pixel Count	Flipped pixel/ No. of hidden bits	MSE	PSNR	Distortion score
Baboon	225X225	1400	29	0.45	5.73	32.42	0.52
Lena	256X256	704	29	0.45	4.43	33.54	0.39
Cartoon1	257X196	798	28	0.44	5.56	32.55	0.40
Cat	225X225	327	30	0.47	5.93	32.27	0.38
Dinosaur	285X177	431	34	0.53	6.74	31.71	0.40
Hero	225X225	466	37	0.58	7.31	31.36	0.40

TABLE IV. Performance comparative study

Method	Image	Embeddable location	Flipped pixel	Distortion score
Ours	**Baboon(225X225)**	**1400**	**29**	**0.52**
[4]	Baboon(225X225)	1217	34	0.55
[5]	Baboon(225X225)	1338	31	0.51
[17]	Baboon(225X225)	856	33	0.61
[50]	Baboon(225X225)	739	35	0.63
Ours	**Lena(256X256)**	**704**	**29**	**0.39**
[4]	Lena(256X256)	851	27	0.37
[5]	Lena(256X256)	890	25	0.41
[17]	Lena(256X256)	687	30	0.57
[50]	Lena(256X256)	689	41	0.51
Ours	**Hero(225X225)**	**466**	**37**	**0.4**
[4]	Hero(225X225)	556	35	0.51
[5]	Hero(225X225)	583	32	0.41
[17]	Hero(225X225)	365	39	0.57
[50]	Hero(225X225)	177	Unsuitable	-

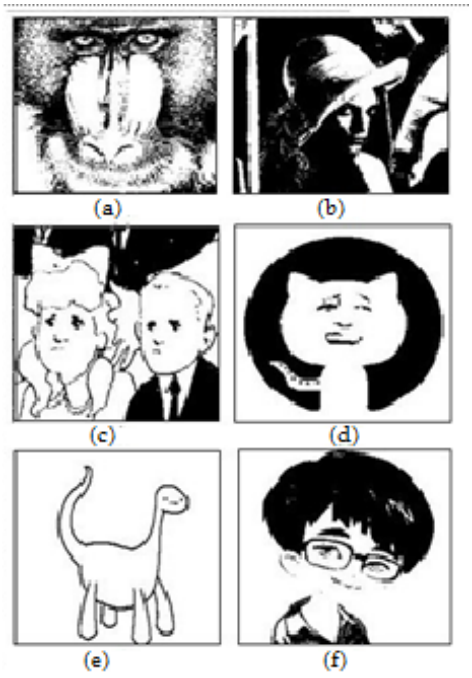

Figure 10. Images after 64 bits data embedding in figure 9 (a)Baboon (b)Lena(c)Cartoon(d)Cat(e) Dinosaur(f)Hero

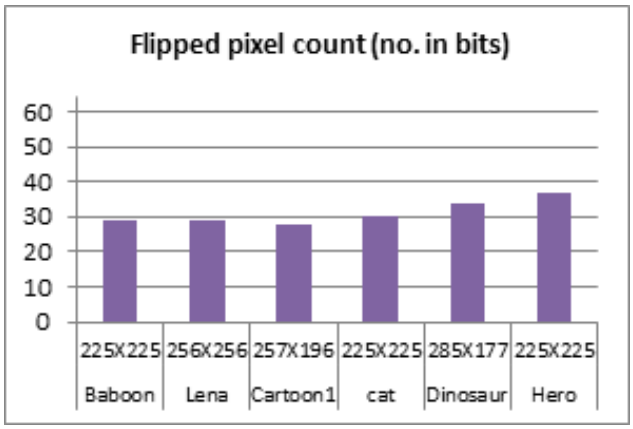

Figure 11. Performance analysis based on flipped pixel count

pixel value change on its adjacent 8 pixels. Average local distortion for each image calculated using the formulae in [39]. Define Di,j as the local distortion generated by a pixel xi,j due to its flipping, assuming the image size is 2M 2N:

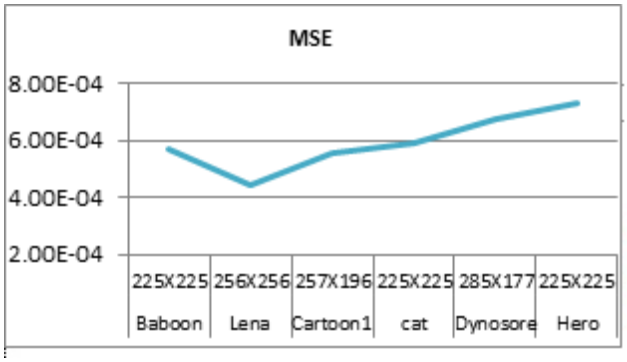

Figure 12. Performance analysis based on MSE

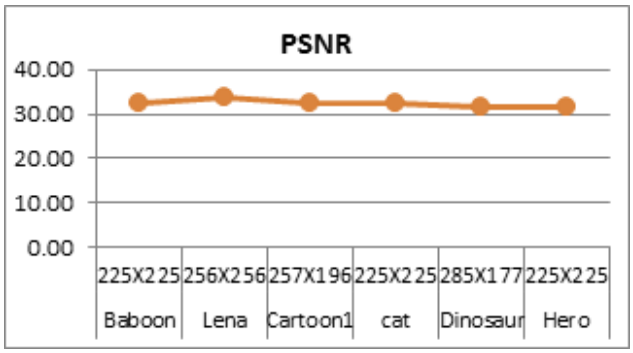

Figure 13. Performance analysis based on PSNR

$$D_{i,j} = \sum_{u=-1}^{1} \sum_{v=-1}^{1} \left| x_{i-u,j-v} - (1 - x_{i,j}) \right| \times k_{u+2,v+2} \qquad (9)$$

where i = 1, 2, . . . , 2M, j = 1, 2,... 2N, and 1-xi,j is the changed value of xi,j .The k represents influence weight matrix as follows:

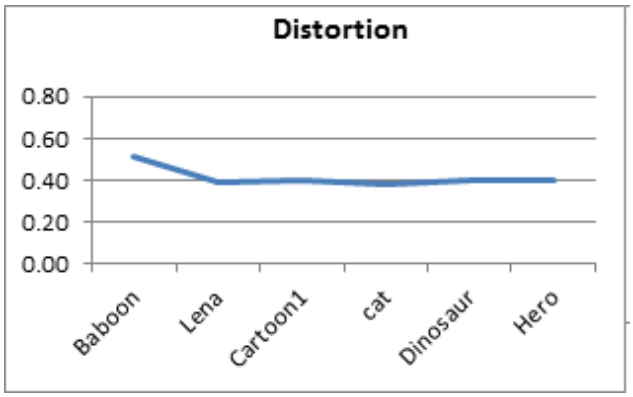

Figure 14. Performance analysis based on distortion factor

$$k = \begin{bmatrix} 1/12 & 1/6 & 1/12 \\ 1/6 & 0 & 1/6 \\ 1/12 & 1/6 & 1/12 \end{bmatrix}$$

$$D = \sum_{r=1}^{s} \frac{D_{i,j}^{r}}{s} \qquad (10)$$

Where Dri,j is the distortion introduced by r th flipped pixel and s represents the total number of flipped pixels. If the sequence of data bits to be hidden and sequence of 3X3 block pattern satisfying embeddability criteria matches then that data bits are hidden without image distortion. We used the MSE and PSNR as well as the average local distortion introduced owing to pixel flipping to test the set of standard photographs some images from [15].Results from tests conducted on the pictures in figure 9 are displayed in table 3. Figure 10 displays the pictures with the hidden secret information. The hidden data considered as ”success” , ”abc” is used as key 1 and ”xyz” is used as key 2. The length of the encrypted concealed data, including header, is 64 bits. The data is systematically concealed in blocks that pass the embeddability test. Figures 11 to 14 graphically display the test results.

The outcome reveals that less than 0.5 is scored for distortion and that around 50% of concealed data is incorporated without flipping pixels. If there are fewer uniform blocks in the images—all white or all black pixels in a block—the embeddability will be better. The design of the cover image and the order of the bits in the data to be hidden have a significant impact on how well this data hiding approach performs. The arrangement of the 3X3 blocks in the cover image and their order affect how well our method works.

The performance of our technique in comparison to other methods is displayed in Table IV. It has been found that our method offers more embeddable blocks, or locations where data can be hidden. To conceal data bits of the same size and order, relatively fewer pixels must be reversed. In addition, the distortion factor is comparable.

5. CONCLUSION

This research revealed a novel technique for concealing data in monochrome photographs. With this block-based approach, 3X3 blocks' diagonal partition patterns are examined to determine whether the block may hold data when embedded. Based on the number of black and white pixels in a block's diagonal half as well as the connectivity between the pixels in a 3X3 block as a whole, the data is hidden. As long as the connectivity of the pixels inside image blocks is retained, there will be little to no visual loss. This approach is more secure because encryption is used twice before hiding data in the image. According to the results, nearly half of the data bits are embedded without flipping the pixels, making it difficult

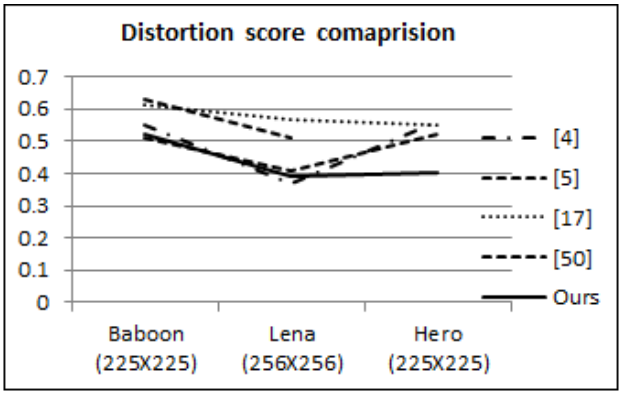

Figure 15. Comparative graph

to locate concealed data. As a result, this technique can be used for steganography for secret communication as well as watermarking, which handles authentication, copy control, and ownership declaration. This will prove to be a successful data hiding technique for binary images where data extraction does not require the original image.

References

[1] Q. G. Mei, E. K. Wong, and N. D. Memon, "Data hiding in binary text documents," in *Security and Watermarking of Multimedia Contents III*, P. W. Wong and E. J. D. III, Eds., vol. 4314, International Society for Optics and Photonics. SPIE, 2001, pp. 369 – 375.

[2] Y.-C. Tseng and H.-K. Pan, "Data hiding in 2-color images," *IEEE Transactions on Computers*, vol. 51, no. 7, pp. 873–880, 2002.

[3] H. Lu, X. Shi, Y. Q. Shi, A. C. Kot, and L. Chen, "Watermark embedding in dc components of dct for binary images," *Proc,IEEE Workshop on Multimedia Signal Processing*, pp. 300–303, 2002.

[4] M. Wu and B. Liu, "Data hiding in binary images for authentication and annotation," *IEEE Trans,Multimedia*, vol. 06, pp. 528–538, 2004.

[5] G. Chhajed, V. Inamdar, and V. Attar, "Steganography in black and white picture images," *IEEE Computer Society*, pp. 141–144, 2008.

[6] G. J. Chhajed and S. A. Shinde, "Efficient embedding in bw picture images," in *2010 2nd IEEE International Conference on Information Management and Engineering*, 2010, pp. 525–528.

[7] H. Y. Kim and R. L. de Queiroz, "Alteration-locating authentication watermarking for binary images," *Book Digital Watermarking*, pp. 125–136, 2005.

[8] H. Yang and A. C. Kot, "Pattern-based data hiding for binary image authentication by connectivity-preserving," *IEEE Transactions on Multimedia*, vol. 9, no. 3, pp. 475–486, 2007.

[9] Y. Huijuan and A. C. Kot, "Binary image authentication with tampering localization by embedding cryptographic signature and block identifier," *IEEE Signal Processing Letters*, vol. 13, no. 12, pp. 741–744, 2006.

[10] H. Yang, A. C. Kot, and S. Rahardja, "Orthogonal data embedding for binary images in morphological transform domain- a high-capacity approach," *IEEE Transactions on Multimedia*, vol. 10, no. 3, pp. 339–351, 2008.

[11] G. Xuan, Y. Q. Shi, P. Chai, X. Tong, J. Teng, and J. Li, "Reversible binary image data hiding by run-length histogram modification," *2008 19th International Conference on Pattern Recognition*, pp. 1–4, 2008.

[12] G. Chhajed, K. Deshmukh, and T. Kulkarni, "Review on binary image stegnography and watermarking -preserving," *International journal in computer Science and Engineering (IJCSE)*, vol. 03, pp. 3545– 3651, 2011.

[13] "Steganography and watermarking: Review," , author= [Atoum ,Mohammed Salem , journal= International Journal of Science and Research (IJSR), pages= 1713-1715, year=2018, volume=07, publisher=."

[14] H. Tao, L. Chongmin, J. Mohamad Zain, and A. N. Abdalla, "Robust image watermarking theories and techniques: A review," *Journal of Applied Research and Technology*, vol. 12, no. 1, pp. 122–138, 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1665642314716128

[15] C. S. T. Sumathi and G. Umamaheswari, "A study of various steganographic techniques used for information hiding," *International Journal of Computer Science Engineering Survey (IJCSES)*, vol. 04, pp. 9–25, 2013.

[16] H. Nagham, A. Yahya, A. Badlishah, and M. A.-Q. Osamah, "Image steganography techniques: An overview," *International Journal of Computer Science and Security (IJCSS)*, vol. 04, pp. 168–187, 2012.

[17] B. Feng, W. Lu, and W. Sun, "Secure binary image steganography based on minimizing the distortion on the texture," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 243–255, 2015.

[18] M. Guo and H. Zhang, "High capacity data hiding for binary image authentication," *2010 20th International Conference on Pattern Recognition*, pp. 1441–1444, 2010.

[19] H. Cao and A. C. Kot, "On establishing edge adaptive grid for bilevel image data hiding," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 9, pp. 1508–1518, 2013.

[20] T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 920–935, 2011.

[21] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Information Hiding*, R. Böhme, P. W. L. Fong, and R. Safavi-Naini, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 161–177.

[22] N.-I. Wu and M.-S. Hwang, "Development of a data hiding scheme based on combination theory for lowering the visual noise in binary images," *Displays*, vol. 49, pp. 116–123, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0141938216301512

[23] K. L. Chiew and J. Pieprzyk, "Blind steganalysis: A countermeasure for binary image steganography," in *2010 International Conference on Availability, Reliability and Security*, 2010, pp. 653–658.

[24] V. Rahmani and M. MohammadPour, "High hiding capacity

steganography method based on pixel indicator technique," in *2017 5th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS)*, 2017, pp. 144–149.

[25] B. Feng, J. Weng, W. Lu, and B. Pei, "Steganalysis of content-adaptive binary image data hiding," *Journal of Visual Communication and Image Representation*, vol. 46, pp. 119–127, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1047320317300081

[26] J. Rao and S. Patel, "A novel approach for enhancing image security and data hiding using nvss," in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 2016, pp. 1128–1133.

[27] M. Venkatesan, P. M. Devi, K. Duraiswamy, and K. Thiagarajah, "A new data hiding scheme with quality control for binary images using block parity," in *Third International Symposium on Information Assurance and Security*, 2007, pp. 468–471.

[28] R. Gayathri and V. Nagarajan, "Secure data hiding using steganographic technique with visual cryptography and watermarking scheme," in *2015 International Conference on Communications and Signal Processing (ICCSP)*, 2015, pp. 0118–0123.

[29] H. Tirandaz, R. Davarzani, M. Monemizadeh, and J. Haddadnia, "Invisible and high capacity data hiding in binary text images based on use of edge pixels," in *2009 International Conference on Signal Processing Systems*, 2009, pp. 130–134.

[30] Y.-K. Chan, Y.-A. Ho, C.-S. Tsai, and Y.-P. Chu, "Robust image hiding method," in *Proceedings of the 9th Joint International Conference on Information Sciences (JCIS-06)*. Atlantis Press, 2006/10, pp. 382–385.

[31] Y.-C. Tseng, Y.-Y. Chen, and H.-K. Pan, "A secure data hiding scheme for binary images," *IEEE Transactions on Communications*, vol. 50, no. 8, pp. 1227–1231, 2002.

[32] M. M. Honey and P. Reji, "A secure data hiding scheme for binary images," *International Journal Of Scientific Engineering Research(IJSER)*, vol. 7, no. 7, pp. 810–816, 2016.

[33] R.Poornima and R.J.Iswarya, "An overview of digital image steganography," *International Journal of Computer Science Engineering Survey (IJCSES)*, vol. 4, no. 1, pp. 23–31, 2013.

[34] S. N. Bal, M. R. Nayak, and S. K. Sarkar, "On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 5, pp. 552–561, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1319157817305153

[35] K.-H. Jung, "A data hiding method of binary images using pixel-value weighting," *Journal of the Korea Institute of Military Science and Technology*, vol. 11, pp. 68–75, 01 2008.

[36] P. L. Lin and P. W. Huang, "A data-hiding scheme for binary images with content-based hiding rates," *Proceedings of the 5th WSEAS International Conference on Signal Processing, Istanbul, Turkey*, pp. 40–45, 2006.

[37] B. Feng, W. Lu, and W. Sun, "High capacity data hiding scheme for binary images based on minimizing flipping distortion," in *Digital-Forensics and Watermarking*, Y. Q. Shi, H.-J. Kim, and F. Pérez-González, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 514–528.

[38] D. Bhattacharyya, A. Haveliya, and T.-h. Kim, "Secure data hiding in binary text document for authentication," *Applied Mathematics Information Sciences*, vol. 8, no. 1, pp. 371–378, 2014.

[39] C.-M. Wang, Y.-K. Chan, Y.-A. Ho, and C.-L. Wang, "Data compression adapted based binary image hiding method," vol. 1, no. 1, 2012, pp. 48–53.

[40] W. Ding and Y. Wang, "Data hiding in binary image with high payload," *Arabian Journal for Science and Engineering and Technology*, vol. 43, no. 12, pp. 7737—-7745, 2018.

[41] J. Chen, W. Lu, Y. Fang, X. Liu, Y. Yeung, and Y. Xue, "Binary image steganalysis based on local texture pattern," *Journal of Visual Communication and Image Representation*, vol. 55, pp. 149–156, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1047320318301317

[42] T.-H. Liu and L.-W. Chang, "An adaptive data hiding technique for binary images," in *Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004.*, vol. 4, 2004, pp. 831–833.

[43] G. Maji and S. Mandal, "Secure and robust image steganography using a reference image as key," vol. 8, no. 7. Springer, 2019, pp. 2828–2837.

[44] H. A. Atee, R. Ahmad, and R. A. Y. A. N. M., Noor, "Extreme learning machine based optimal embedding location finder for image steganography," *Journal of Visual Communication and Image Representation*, vol. 12, no. 2, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1047320318301317

[45] V. Manikandan and V. Masilamani, "Reversible data hiding scheme during encryption using machine learning," *Procedia Computer Science*, vol. 133, pp. 348–356, 2018, international Conference on Robotics and Smart Manufacturing (RoSMa2018). [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050918309888

[46] S. Udhayavene, A. T. Dev, and K. Chandrasekaran, "New data hiding technique in encrypted image: Dkl algorithm (differing key length)," *Procedia Computer Science*, vol. 54, pp. 790–798, 2015, eleventh International Conference on Communication Networks, ICCN 2015, August 21-23, 2015, Bangalore, India Eleventh International Conference on Data Mining and Warehousing, ICDMW 2015, August 21-23, 2015, Bangalore, India Eleventh International Conference on Image and Signal Processing, ICISP 2015, August 21-23, 2015, Bangalore, India. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050915014179

[47] T.-S. Nguyen, C.-C. Chang, and H.-S. Hsueh, "High capacity data hiding for binary image based on block classification," *Multimedia Tools and Applications*, vol. 75, no. 14, pp. 8513–8526, 2016. [Online]. Available: https://doi.org/10.1007/s11042-015-2768-1

[48] K. L. Chiew and J. Pieprzyk, "Binary image steganographic techniques classification based on multi-class steganalysis," in *Information Security, Practice and Experience*, J. Kwak, R. H. Deng, Y. Won, and G. Wang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 341–358.

[49] Y. Lee, H. Kim, and Y. Park, "A new data hiding scheme

for binary image authentication with small image distortion," *Information Sciences*, vol. 179, no. 22, pp. 3866–3884, 2009. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0020025509003272

[50] K. Deshmukh and G. Chhajed, "A steganographic method for data hiding in binary image using edge based grids," *International journal Computer Technology Applications 1369-1374 ISSN:2229-6093*, vol. 05, no. 04, pp. 1369–1374, 2014.

[51] B. Garg and R. Garg, "Enhanced accuracy of fuzzy time series model using ordered weighted aggregation," *Applied Soft Computing*, vol. 48, pp. 265–280, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1568494616303258

[52] B. Garg, S. Aggarwal, and J. Sokhal, "Crop yield forecasting using fuzzy logic and regression model," *Computers Electrical Engineering*, vol. 67, pp. 383–403, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790617305487

[53] X. Yin, W. Lu, J. Zhang, J. Chen, and W. Liu, "Reversible data hiding in binary images by flipping pattern pair with opposite center pixel," *Journal of Visual Communication and Image Representation*, vol. 70, pp. 1–13, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1047320320300663

[54] F. Li, L. Zhang, and W. Wei, "Reversible data hiding in encrypted binary image with shared pixel prediction and halving compression," *EURASIP Journal on Image and Video Processing*, vol. 2020, no. 1, pp. 1–21, 2020.

[55] G. J. Chhajed and B. R. Garg, "Novel approach to data hiding in binary images minimizing distortion," *Book Computational Vision and Bio-Inspired Computing*, pp. 587–598, 2021.

[56] G. J. Chhajed, Garg, and B. R., "Applying decision tree for hiding data in binary images for secure and secret information flow," *Cybersecurity Measures for E-Government Frameworks*, pp. 175–186, 2022.

[57] G. Chhajed and B. Garg, "Data hiding in binary images for secret and secure communication using decision tree," in *4th EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing*, A. Haldorai, A. Ramu, S. Mohanram, and R. Zgheib, Eds. Cham: Springer International Publishing, 2023, pp. 69–84.

[58] G. J. Chhajed and B. R. Garg, "Information security by hiding data in binary images based on block-diagonal partition pattern," *2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, pp. 1–6, 2022.

Gyankamal Chhajed Gyankamal obtained her B.E. Degree in Computer Science and Engineering and Postgraduate Degree (M.Tech.) in Computer Engineering . She is GATE qualified with 96.76 percentile and pursuing Ph.D. in Computer Engineering. She is approved Undergraduate and recognized Postgraduate teacher of S.P. Pune University. Her area of research is Data hiding in binary images for steganograpy and watermarking, Image processing, Medical appliations.

Bindu Garg Bindu has obtained PhD(CE) M.Tech(CSE) B.Tech(CSE) . She is professor and Head of CSBS and CSE dept. Working as Innovation Council head with aim of fostering and encouraging culture and creation of innovations. Her research area is Soft Computing , Data Mining,Forecasting Time Series Analysis, Cloud Computing