

^{1*}Sriharipriya K. C.²J. Christopher
Clement³Gerardine
Immaculate Mary⁴M. Supriya⁵Sivakumar
Annamalai⁶Somu Nikhil Reddy

Secure Pixel-Level Data Concealment: A Novel Approach for Securing Black and White Images within Color Images



Abstract: - In the era of rampant digital data transfer, concerns regarding the secure and reliable transmission of information persist, with numerous attempts at concealing and transporting data globally. Despite the plethora of existing techniques, issues persist, ranging from misinterpretation to malicious misuse of data during the transfer process. To address some of these challenges, this research introduces an innovative method centered on the modification of pixel data to embed concealed information. The primary objective is to alter pixel values in a manner that accommodates the storage of data pertaining specifically to black and white image pixel data. The proposed technique is designed to exclusively encode information related to two-pixel values, with careful adjustments made to ensure the masked image remains non-deceptive. Pixel values undergo subtle alterations to mitigate susceptibility issues associated with corner values, particularly at the border values of 254 and 255 for RGB values. The developed method presents a simplified yet robust data hiding technique, allowing the storage of black and white images within color images while achieving a high Peak Signal-to-Noise Ratio (PSNR) compared to standard ".png" images. Crucially, the developed approach addresses the challenge of minimizing drastic changes in pixel color, enhancing the overall fidelity of the stego image. Furthermore, the versatility of the proposed method is showcased by its potential to accommodate more than three images when the stego image size is appropriately large and segmented. A practical and efficient solution has been contributed to the persistent issues associated with secure data transfer, presenting a novel methodology for concealing black and white images within color images.

Keywords: Real time Image Processing, Image Enhancement, LSB substitution techniques, Data Hiding, Information Hiding.

I. INTRODUCTION

The growing requirement for data security has led to the development of novel masking algorithms and approaches that prevent users from decoding spilled data and using it for their own purposes. A method called "image hiding" allows you to incorporate hidden information into an image without affecting the original. A stego-image is the picture that conceals the secret info. Because the stego-image won't raise red flags, attacks can be avoided. However, the secret data concealed in the stego-image can be correctly decoded by the appropriate recipient. Image hiding has manifested in various forms, including spatial domain data hiding, where direct modification of pixel values occurs [1]. Compressed domain hiding involves both image compression and encoding layers, crucial for decoding the masked image [2-4]. Frequency domain hiding encodes images into the frequency domain, allowing masking before inverse transformation retrieves the encoded images [5]. Wavelet transform techniques, including those used in OFDM systems, play a role in encoding and decoding [6-8]. The goal of Hossein Najafi's neural network-based digital watermarking technique for picture hiding is to reduce the visual impact of images on human vision [9]. Wavelet transform methods were expanded to include encoding, transforming audio signals to .wav format, and concealing audio information inside pictures [10]. Using graph theories such as depth-first search, multibit assignment picture data hiding for palette images entails using palette colors to conceal secret data bits [11]. Data hiding capacity, image type applicability, visual quality as determined by low MSR and high PSNR values, and stenographic security are critical parameters for data concealing techniques [12]. Methods with high data hiding embedding capacity have been utilized for applications requiring high data capacity, even if it means trading off visual or image quality [13]. Robust image data hiding schemes consider statistical quantities to counter the effects of image compression [14]. Some

^{1*}Corresponding author: sriharipriya.kc@vit.ac.in

^{1,2,3,6}School of Electronics Engineering, Vellore Institute of Technology, Vellore, India.

⁴Department of Computer Science and Engineering, Stella Mary's College of Engineering, India

⁵Department of Safety & Fire Engineering, Excel Engineering College, India.

methods focus on image visual quality, modifying minimum points of the image histogram slightly to hide data [15]. Stenography security improvements include LSB matching in grayscale images [16] and identity-based authentication using secret image sharing schemes [17]. Methods proposing encoding each grayscale pixel into 8 bits result in limited data storage compared to newer encryption methods [18]. LSB substitution with gene programming incorporates a hybrid data hiding scheme but suffers from less data bit storage compared to image resolution [19].

Methods for storing medical data, using simple LSB substitution, may compromise data storage due to a bit-by-bit approach [20]. Adaptive data hiding in the frequency domain, though storing significantly more data, faces challenges with increased processing time [21]. Numerous studies create strategies based on least significant bits (LSBs), embedding message bits in 1-3-4 LSBs of red, green, and blue components in smooth picture areas and the least significant byte of chosen edge area pixels [22]. Block permutation and a stream cipher are combined in an enhanced reversible data hiding technique to provide high embedding rates and data security [23]. Our proposed method encrypts images using RGB concentrations, allowing storage of three distinct black and white images in one image, requiring both masked and unmasked images for data retrieval [24]. Dual image hiding approaches, such as lifting wavelet transform (LWT) and discontinuous wavelet transform (DCT), employ distinct methods for each individual image within the cover image [25]. Certain techniques make advantage of image histogram statistics, storing data using cumulative peak values and taking PSNR values into account to improve visual aspects [26]. Using texture as the comparison parameter, effective decoding techniques that use ANN and MPEG-7 texture decoders are presented to extract masked data from cover pictures [27]. When it comes to efficiency, a variety of techniques are used to hide data in photos, including difference expansion, interpolation, reversible concealing, and histogram shifting [28]. Data hiding techniques based on difference expansion (DE) face significant distortion resulting from message embedding [29]. Conventional image classification techniques remain applicable in feature-rich and diverse data situations [30]. Advanced deep learning (DL) techniques outperform these methods when there is sufficient data [31]. Issues arise in claiming increased accuracy with added layers in neural networks, with the vanishing gradient problem posing challenges [32]. Image enhancement using DWT, based on two approaches, combines region- and edge-based techniques for superior outcomes [33-35].

From the literature survey, several key problems in image hiding techniques emerge as illustrated below:

- The traditional method of encoding each grayscale pixel into 8 bits results in a significantly low amount of data storage compared to more recent encryption methods. This limitation hinders the potential for higher data embedding capacities.
- Hybrid data hiding schemes, such as those combining LSB techniques with gene programming or permutation methods, face challenges in achieving optimal data bit storage. Issues include suboptimal key-permutation determination and reduced data bit storage compared to image resolution.
- Existing methods for storing sensitive medical data, such as X-rays, ECG data, and personal details, using simple LSB substitution techniques result in limited data storage due to a bit-by-bit approach. While the approach ensures simplicity, it compromises the amount of data that can be securely stored.
- Some proposed methods utilize adaptive data hiding in the frequency domain, achieving significantly increased data storage. However, the trade-off involves extended processing times, impacting the practicality of these methods for real-time applications.

These identified problems underscore the diverse challenges in existing image hiding techniques, ranging from capacity limitations and security issues to trade-offs between efficiency and processing time. Addressing these issues is crucial for the development of robust and practical data hiding methods with broader applications and enhanced security features.

This study primarily focuses on how to increment and decrement the color values of individual pixels in an image without affecting the color of the entire pixel. Most colors may be created by combining the elements of red, green, and blue. Information storage can be achieved by representing pixel values in RGB terms and making minor adjustments to their intensities. Aligned with this principle, a program has been crafted to extract image features, focusing on pixel color in relation to RGB values. The adaptation of these RGB values is customized to the specific image for storage. Diverging from traditional LSB substitution methods, the proposed technique opts for the direct adjustment of color intensity. The paper outlines a simple approach for storing multiple black and white images within a single-color image. The design of the proposed method is presented in Section II. In Section III, the efficiency of the masking method is shown and tests on various examples are obtained. Section IV provides the conclusion.

II. PROPOSED METHOD

The proposed method necessitates the utilization of both the masked image and the unmasked image. It mandates a thorough comparison of the data pixels present in both images to retrieve the concealed data. Contrary to LSB substitution techniques, which serve no purpose with the original image and may arouse suspicion, users can attempt to extract the LSB bit of the pixel data, thereby exposing the encrypted data. However, in the current proposed system, the end user must possess access to the original image as a prerequisite. In this method of encrypting the image with data, simplicity prevails, and the data can pertain to another hidden image, specifically in black and white format. The encryption process initiates by converting the target image into black and white, where only two distinct pixel colors exist. Pixels with RGB values of 255 are considered white, while those with RGB values of 0 are deemed black. The initial step involves converting the image to black and white, especially if it is in color. Treating black and white as two values, the data undergoes incremental and decremental adjustments by a specified value. This ensures that even if an unauthorized user gains possession of the original image, retrieving hidden data remains a formidable challenge. To obtain the complete data without errors, end users must have access to the original image. The extraction process involves comparing each pixel color with respect to RGB values, enabling the retrieval of pixel data from the concealed image. The masked image, also referred to as the stego-image, is subsequently compared with the original image. Once this comparison is performed, users can extract the hidden data or image with confidence.

A. *Grayscale Transformation for Simplified Intensity Encoding*

If the provided image is in color, it undergoes a conversion process to become a grayscale image. In the context of a colored image, which comprises three color parameters represented by RGB, it can be conceptualized as a three-dimensional array. Since a grayscale image consists of only two colors—black and white—with different intensities for each color, the conversion process entails converting this three-dimensional array into a two-dimensional array. A basic equation can be used to convert a three-dimensional array to a two-dimensional array:

$$\text{Grayscale pixel value} = (R + G + B)/3 \quad (1)$$

where R, G, B - intensities of red, green and blue colors.

The 255 distinct intensities that must be encoded into the image require a larger magnitude change in pixel values. But narrowing the range to just two intensities lessens the amount of pixel value change that is necessary. The decrease can be achieved through the implementation of a threshold value, 128 in this case, which can be carefully selected as the center value between 0 and 255. As an alternative, using the threshold instead of the mean value results in a more sophisticated image encoding procedure. As a result, the final black-and-white image is encoded using conditional logic, whereby the pixel value is coded as "0" if the grayscale value is less than the threshold value and is coded as "255" if it exceeds the threshold. This methodology ensures a streamlined and efficient encoding process for the black and white image.

B. *Integration of Colorful Overlay (Transforming Grayscale to Colored Image):*

The final converted color image consists of two different color values, 0 and 255, organized in a two-dimensional array similar to binary values. It is important to remember that the masking procedure differs from the standard LSB substitution method. To accommodate these image values, the RGB intensities are modified rather than binary values being directly embedded into the least significant bit, or kth-bit, of the pixel data. In this transformative process, the adjustment of pixel values follows a precise methodology. For a pixel value of '0,' representing one-color intensity, such as the blue color value, is incremented by 1. It's important to address potential outliers and minimize susceptibility. If the 'B' value reaches its maximum at 255, an equivalent decrement of '1' is applied to mitigate abrupt changes in pixel color. A similar approach is adopted when the pixel value is '255.' In this case, the same color, 'B,' is selected, and its value is incremented by '2.' However, a cautious adjustment is made to account for unchanged values of 'B' at 254 or 255, where the value must be decremented by '2' to ensure a smooth transition. This precaution is essential to address ambiguity at outliers. For instance, if a value is at 255 and is incremented by 1, the result is 256, an invalid pixel color value. Therefore, it is considered as '0,' preventing an unintended and drastic alteration of the entire image pixel color. Fig. 1 illustrates the sequential flow of the proposed method.

C. Consolidating Monochromatic Imagery (Merging Multiple Black(BB) and White(WW) Images into a Unified Color Palette)

Three different hues are associated with different pixel values in the context of colored images. As a result, each color's intensity values can be changed independently. This guarantees that a single-colored image contains at least three distinct images. Different portions of the image can be treated to hide several images if the cover image is big enough. For example, the remaining pixel data (750x750), (800x800), and (500x500) are left unused if the cover image is 1000x1000 pixels and the concealed images are 250x250, 200x200, and 500x500. At least three more photos can be stored by iteratively going over these wasted pixels. Consequently, storing many photos is made easier by investigating the unused pixels.

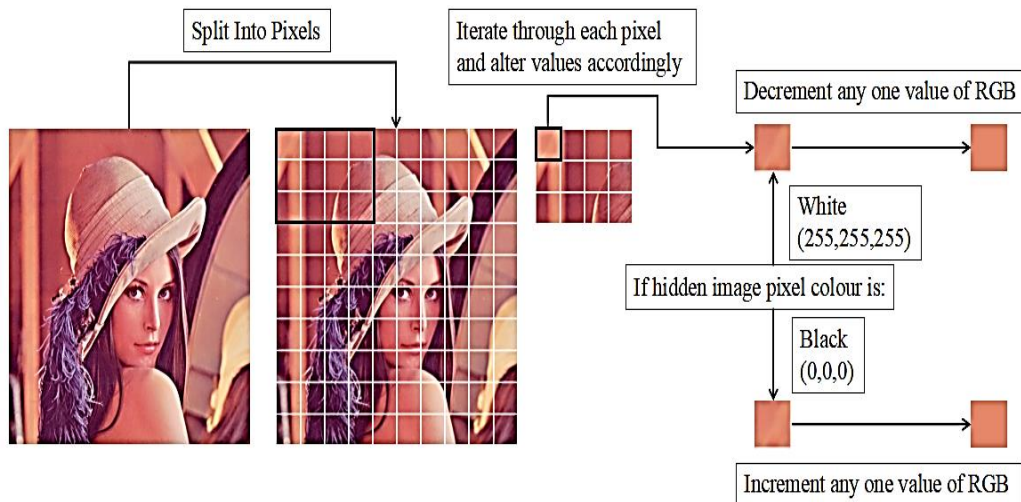


Figure 1. Flowchart of the proposed method

D. Analyzing the Stego-Image through Comparison with the Original Image

Upon transmission of the masked image to the intended user, access to the original image becomes imperative. The selection of an accessible original image holds a crucial role in this process. Data retrieval involves comparing the masked image with the original image. In scenarios where a single image is stored with respect to a unique color in RGB, the user can scrutinize each pixel value data to discern two distinct values. The conversion of data to an image follows a specific protocol: If the disparity between the original and masked pixel color values amounts to '1,' the pixel color is deemed as (0,0,0), while a difference of '2' designates the pixel color as (255,255,255). However, when multiple images are masked per color, direct data extraction yields multiple images. In such instances, knowledge of the individual images' dimensions is essential for effective image splitting. In the conducted test, three images were stored, aligning with the stego image's dimensions, as a noteworthy observation.

III. RESULTS AND DISCUSSIONS

The stored data size is at least three times that of the cover image pixels. In this context, the selected hidden data comprises images, resulting in the storage of three images. The subsequent results display an examination of commonly utilized test stego images for assessment.

A. Number of the bits stored

Test1:

Test Images:

Baboon (picture in BB and WW) = 32768 bytes

Peppers: 32768 bytes (BB and WW picture)

Airplane: (32768 bytes) (BB and WW image)

Colorized image of Lena (Stego image)

Test2:

Test Images:

Lena- (picture in BB and WW) = 32768 bytes

Peppers: 32768 bytes (BB and WW picture)

Airplane: (32768 bytes) (BB and WW image)

Colorized image of a baboon (Stego image)

Test3:

Test Images:

Baboon (picture in BB and WW) = 32768 bytes

Lena- (picture in BB and WW) = 32768 bytes

Airplane: (32768 bytes) (BB and WW image)

Colorized image of peppers (Stego image)

Test4:

Test Images:

Baboon (picture in BB and WW) = 32768 bytes

Peppers: 32768 bytes (BB and WW picture)

Lena- (picture in BB and WW) = 32768 bytes

Colorized image of an airplane (Stego Image)

Total number of bits stored in each test performed= $32768 \times 3 = 98304$ bytes.

B. Quantitative evaluation with values for PSNR and MSE

Three images, the maximum number that can be hidden and have the same size as the cover image, are allowed.

Table 1: Analysis Results for Stego Image ‘Lena’

Cover Image	No. of encoded images	PSNR (db)	MSE
Cover image	1	47.980531136122195	1.0352071126302083
Cover image	2	45.3972168280825	1.876543680826823
Cover image	3	43.798386493742676	2.711700439453125

Table 2: Analysis Results for Stego Image ‘Baboon’

Cover Image	No. of encoded images	PSNR (db)	MSE
Cover image	1	47.980531136122195	1.0352071126302083
Cover image	2	45.33118120776055	1.9052950541178386
Cover image	3	43.75258190892207	2.7404518127441406

Table 3: Analysis Results for Stego Image ‘Peppers’

Cover Image	No. of encoded images	PSNR (db)	MSE
Cover image	1	47.980531136122195	1.0352071126302083
Cover image	2	45.3972168280825	1.876543680826823
Cover image	3	43.742799450309484	2.746631622314453

Table 4: Analysis Results for Stego Image ‘airplane’

Cover Image	No. of images hidden	PSNR (db)	MSE
Cover image	1	48.91312360813345	0.8351567586263021
Cover image	2	45.812936524461946	1.7052447001139324
Cover image	3	44.071228206205284	2.546581268310547

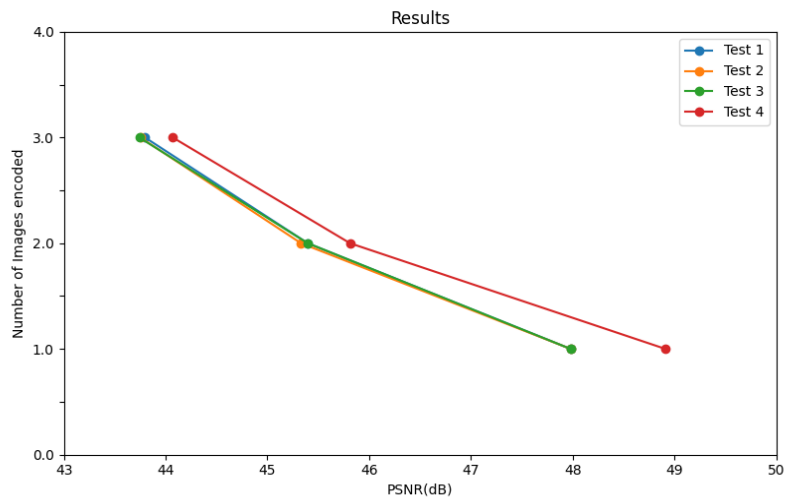


Figure 2. PSNR Vs. Number of images encoded

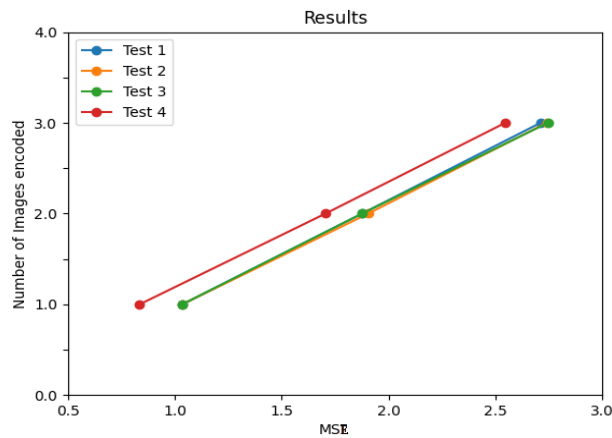


Figure 3. MSR Vs. Number of images encoded

Figure 2 and Figure 3 depicts the above-mentioned test results relative to number of images hidden vs. PSNR and MSE values. Retrieved images have a 100dB PSNR ratio, which implies the images are completely intact after encoding and decoding from cover image. The PSNR values of the proposed method have been compared with existing methods in Table 5 which assures that the proposed method is reliable and the same has been depicted in Figure 4, Figure 5 to Figure 8 shows that the hidden images test from 1 to 4.

Table 5: Comparison of proposed method with existing methods

METHODS	Classic LSB	SCC	PIT	FMM	CST	SHSI	Karim	Proposed Method		
								No. of images hidden		
								3	2	1
PSNR	49.82	49.97	50.09	46.04	48.74	57.26	49.95	43.84	45.48	48.21

Comparison of Proposed Method with Existing Methods

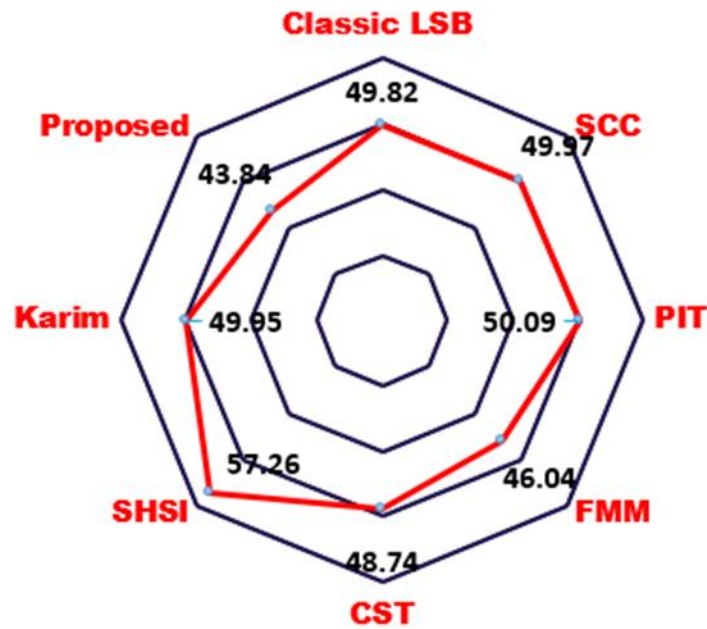


Figure 4. Comparison of proposed method to existing methods

C. Test Results

Look up table for below test results

STEGO IMAGE	Hidden Image 1	Hidden Image 2	Hidden Image 3
	BB and WW Converted hidden image 1	BB and WW Converted hidden image 2	BB and WW Converted hidden image 3
	Stego- image after masking image 1	Stego- image after masking images 1,2	Stego- image after masking images 1,2,3
	Retrieved Image 1	Retrieved Image 2	Retrieved Image 3



Figure 5. Images Hidden Test 1



Figure 6. Images Hidden Test 2

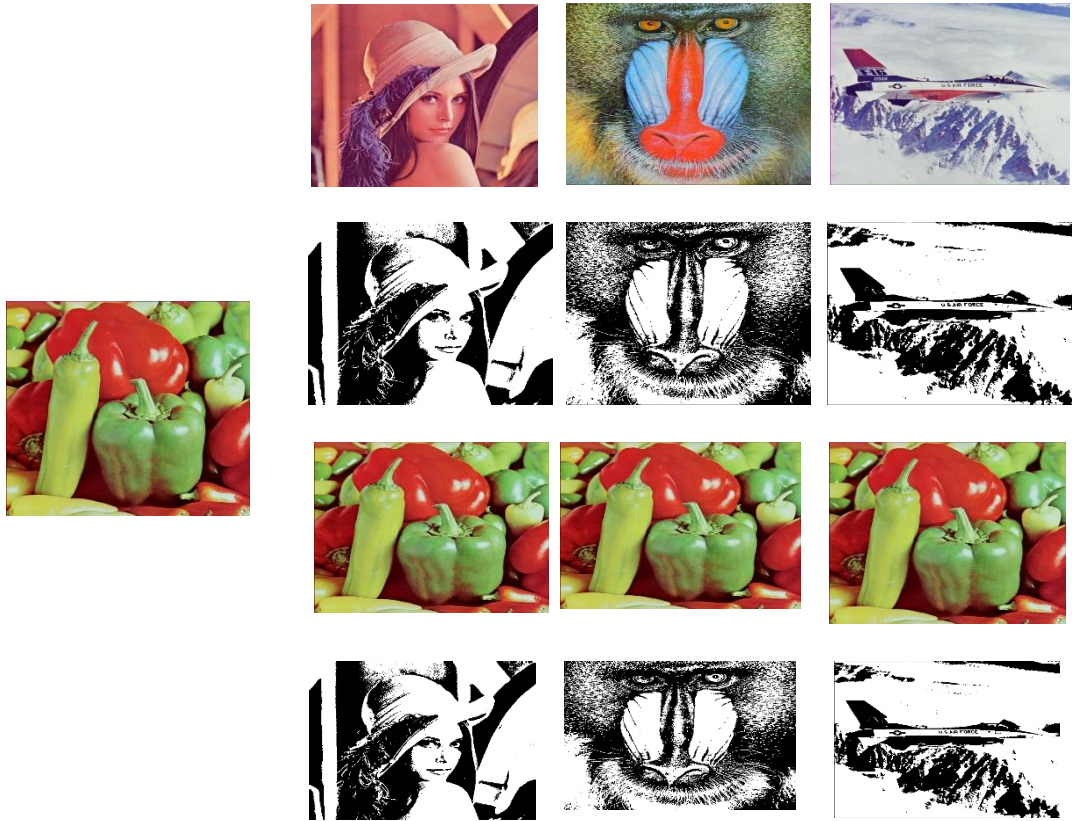


Figure 7. Images Hidden Test 3

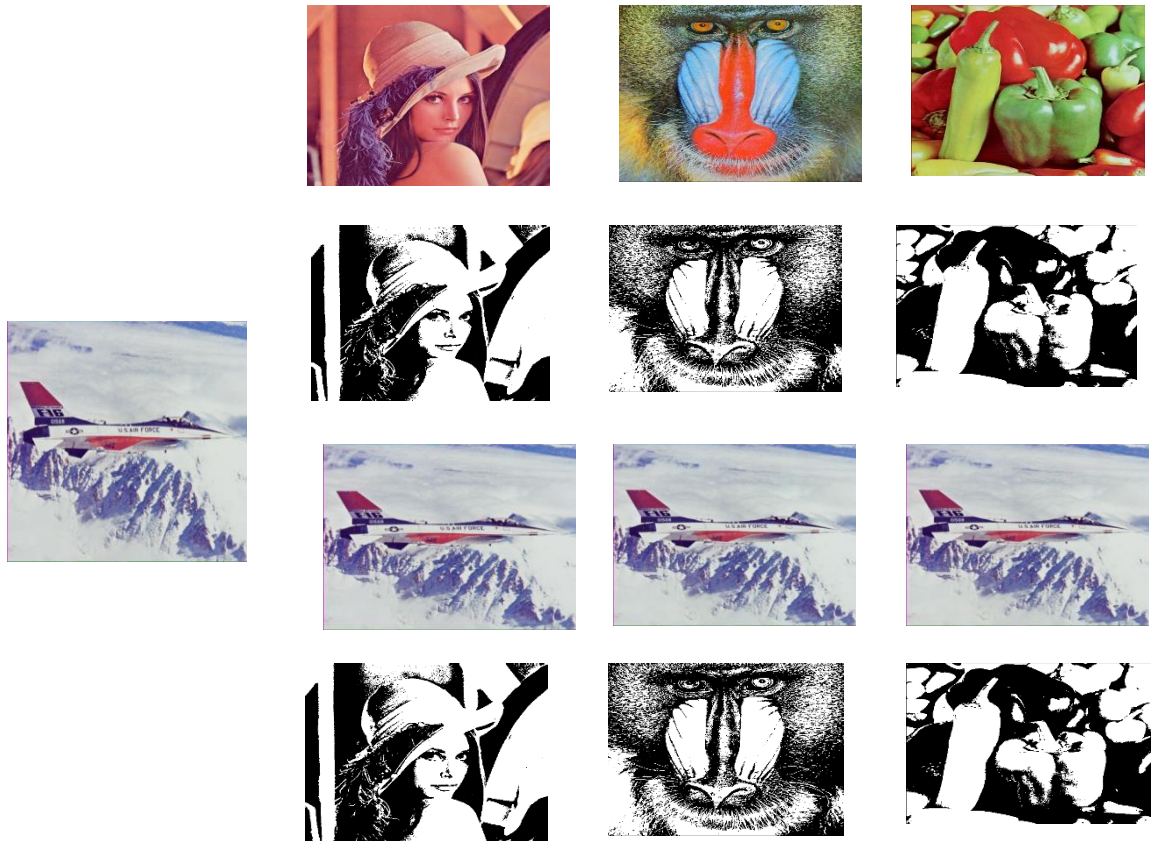


Figure 8. Images Hidden Test 4

IV. CONCLUSION

In an era dominated by digital data transfer, the persistent concerns surrounding secure information transmission have fueled the development of innovative concealment techniques. This research introduces a groundbreaking method that focuses on modifying pixel data to embed concealed information, specifically tailored for black and white image pixel data. The proposed technique exclusively encodes information related to two-pixel values, employing careful adjustments to mitigate susceptibility issues associated with corner values, particularly at RGB values of 254 and 255. This approach results in a simplified yet robust data hiding technique, allowing the storage of black and white images within color images. Notably, the developed method addresses the challenge of minimizing drastic changes in pixel color, thereby enhancing the overall fidelity of the stego image. Furthermore, the versatility of the proposed method is demonstrated by its potential to accommodate more than three images when the stego image size is appropriately large and segmented. This feature enhances the adaptability and scalability of the method in diverse applications. The method's efficiency is demonstrated through tests and comparisons, showcasing its potential for real-world applications. The proposed technique stands as a significant advancement in the field of data hiding, addressing key challenges and opening avenues for further exploration and refinement.

REFERENCES

- [1] J. Mielikainen, "LSB matching revisited," in *IEEE Signal Processing Letters*, vol. 13, no. 5, pp. 285-287, May 2006, doi: 10.1109/LSP.2006.870357.
- [2] Badr, S. and Noufal, P., 2016. Integrated data hiding and compression scheme based on SMVQ and FoE inpainting. *Procedia Technology*, 24, pp.1008-1015.
- [3] Chang, C.C., Kieu, T.D., Chou, Y.C., 2009. A lossless data embedding technique by joint neighboring coding, *Pattern Recognition* 42(7):1597- 1603
- [4] Chang, C.C., Kieu, T.D., Chou, Y.C., 2009a. Reversible information hiding for VQ indices based on locally adaptive coding, *Journal of Visual Communication and Image Representation* 20(1):57-64
- [5] S. Lee, C. D. Yoo and T. Kalker, "Reversible Image Watermarking Based on Integer-to-Integer Wavelet Transform," in *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 321-330, Sept. 2007, doi: 10.1109/TIFS.2007.905146.
- [6] Shen, S.Y. and Huang, L.H., 2015. A data hiding scheme using pixel value differencing and improving exploiting modification directions. *Computers & Security*, 48, pp.131-141.
- [7] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun and X. Lin, "Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 18, no. 4, pp. 497-509, April 2008, doi: 10.1109/TCSVT.2008.918761.
- [8] Mali, S.N., Patil, P.M. and Jalnekar, R.M., 2012. Robust and secured image-adaptive data hiding. *Digital Signal Processing*, 22(2), pp.314-323.
- [9] Zhicheng Ni, Yun-Qing Shi, N. Ansari and Wei Su, "Reversible data hiding," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354-362, March 2006, doi: 10.1109/TCSVT.2006.869964.
- [10] Lerch-Hostalot, D. and Megias, D., 2013. LSB matching steganalysis based on patterns of pixel differences and random embedding. *Computers & security*, 32, pp.192-206.
- [11] Wang, P., He, X., Zhang, Y., Wen, W. and Li, M., 2019. A robust and secure image sharing scheme with personal identity information embedded. *Computers & Security*, 85, pp.107-121.
- [12] Raju, K.U. and Prabha, N.A., 2021. Dual images in reversible data hiding with adaptive color space variation using wavelet transforms. *International Journal of Intelligent Unmanned Systems*.
- [13] Al-Omari, F.A., Al-Khaleel, O.D., Rayyashi, G.A. and Ghwanmeh, S.H., 2012. An innovative information hiding technique utilizing cumulative peak histogram regions. *Journal of Systems and Information Technology*.
- [14] Nipanikar, S.I. and Deepthi, V.H., 2017. Wavelet transform-based steganographic method for secure data communication using OFDM system. *International Journal of Intelligent Computing and Cybernetics*.
- [15] Najafi, H.L., 2010. A neural network approach to digital data hiding based on the perceptual masking model of the human vision system. *International Journal of Intelligent Computing and Cybernetics*.

- [16] Pratt, M.A., Konda, S. and Chu, C.H.H., 2008. Texture-based image steganalysis by artificial neural networks. *International Journal of Intelligent Computing and Cybernetics*.
- [17] Wu MN., Lin MH., Chang CC. (2004) A LSB Substitution Oriented Image Hiding Strategy Using Genetic Algorithms. In: Chi CH., Lam KY. (eds) *Content Computing. AWCC 2004. Lecture Notes in Computer Science*, vol 3309. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-30483-8_27
- [18] Singh, Arun Kumar, Juhi Singh, and Harsh Vikram Singh. "Steganography in images using lsb technique." *International Journal of Latest Trends in Engineering and Technology (IJLTET)* 5, no. 1 (2015): 426-430.
- [19] Mohamed, Marghny H., and Hussein I. Abul-Kasim. "Data hiding by lsb substitution using gene expression programming." *International Journal of Computer Applications* 975 (2012): 8887.
- [20] Karakiş, R., İ. Güler, I. Capraz, and Erhan Bilir. "A novel fuzzy logic-based image steganography method to ensure medical data security." *Computers in biology and medicine* 67 (2015): 172-183.
- [21] Lai, Bo-Luen, and Long-Wen Chang. "Adaptive data hiding for images based on haar discrete wavelet transform." In *Pacific-Rim Symposium on Image and Video Technology*, pp. 1085-1093. Springer, Berlin, Heidelberg, 2006.
- [22] Juneja, M., & Sandhu, P. (2013). An Improved LSB Based Steganography Technique for RGB Color Images. *International Journal of Computer And Communication Engineering*, 513-517.
- [23] N. A. Kumar, G. Shyni, Geno Peter, A. A. Stonier, and V. Ganji, "Architecture of Network-on-Chip (NoC) for Secure Data Routing Using 4-H Function of Improved TACIT Security Algorithm," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–9, Mar. 2022, doi: 10.1155/2022/4737569.
- [24] M., Marghny & Abulkasim, Hussein. (2012). Data Hiding by LSB Substitution using Gene Expression Programming. *International Journal of Computer Applications*. 45. 13-20.
- [25] Nipanikar, S.I., Deepthi, V.H. and Kulkarni, N., 2018. A sparse representation based image steganography using particle swarm optimization and wavelet transform. *Alexandria engineering journal*, 57(4), pp.2343-2356.
- [26] Rabie, T., Baziyad, M. and Kamel, I., 2018. Enhanced high capacity image steganography using discrete wavelet transform and the Laplacian pyramid. *Multimedia Tools and Applications*, 77(18), pp.23673-23698.
- [27] Hemalatha, S., Acharya, U.D. and Renuka, A., 2015. Wavelet transform based steganography technique to hide audio signals in image. *Procedia Computer Science*, 47, pp.272-281.
- [28] Swain, G., 2016. A steganographic method combining LSB substitution and PVD in a block. *Procedia Computer Science*, 85, pp.39-44.
- [29] Lu, T.C., Chang, C.C. and Huang, Y.H., 2014. High capacity reversible hiding scheme based on interpolation, difference expansion, and histogram shifting. *Multimedia tools and applications*, 72(1), pp.417-435.
- [30] Wu, H., Wang, H., Zhao, H. and Yu, X., 2015. Multi-layer assignment steganography using graph-theoretic approach. *Multimedia Tools and Applications*, 74(18), pp.8171-8196.
- [31] Aadhitya, S. V., and K. C. Sriharipriya. "Disease Detection and Diagnosis of Agricultural Plant Leaf Using Machine Learning." *International Journal of Electrical and Electronics Research* 11.3 (2023): 749-753.
- [32] A. Sherine and Geno Peter "A Novel Biometric Recognition System for Fingerprint Using Polar Harmonic Transform." *International Journal of Pharmaceutical Research*, vol. 13, no. 01, Jan. 2021. DOI.org (Crossref), <https://doi.org/10.31838/ijpr/2021.13.01.636>.
- [33] A. Sherine, Geno Peter, A. A. Stonier, K. Pragma, and V. Ganji, "CMY Color Spaced-Based Visual Cryptography Scheme for Secret Sharing of Data," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–12, Mar. 2022, doi: 10.1155/2022/6040902.
- [34] Mandal, Pratap Chandra, and Imon Mukherjee. "High capacity data hiding based on multi-directional pixel value differencing and decreased difference expansion." *Multimedia Tools and Applications* 81.4 (2022): 5325-5347.
- [35] Prabukumar, M., and J. Christopher Clement. "Compressed Domain Contrast and Brightness Improvement Algorithm for Color Images through Contrast Measuring and Mapping of DWT Coefficients." *International Journal of Multimedia and Ubiquitous Engineering* 8.1 (2013): 55-69.