Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Exposing the most match parity bit approach (MMPB-A) for data concealment in digital images

Kaznah Alshammari *

Department of Information Technology, Faculty of Computing and Information Technology, Northern Border University, Rafha 91911, Saudi Arabia

ARTICLE INFO

Article history:
Received 23 March 2024
Received in revised form
22 July 2024
Accepted 26 July 2024

Keywords:
Steganography
Least significant bit
Digital image concealment
Most match parity bit approach
Confidentiality

ABSTRACT

Steganography was originally developed to hide and transmit sensitive information. One major advancement in this field is the ability to hide data within digital images. Significant progress has been made, demonstrating effective methods for concealing data. Various techniques have been used, including statistical steganography, distortion techniques, and the Discrete Cosine Transform (DCT). However, the Least Significant Bit (LSB) method is particularly important and remains the most widely used. Researchers have developed methods based on these principles, such as pseudorandom permutation. This paper introduces the Most Match Parity Bit Approach (MMPB-A), which is based on the LSB method. MMPB-A strategically identifies the parity bits of selected pixels to embed information in cover images. It uses a six-bit encryption for each symbol, allowing ample space to hide information while preserving similarity and secrecy. Additionally, encoding hidden data indices in a three-bit code enhances data concealment and ensures greater confidentiality.

1. Introduction

Steganography was originally designed to conceal sensitive data but has since undergone a significant evolution, with one of its main accomplishments being the concealment of data within digital images (Pandey et al., 2021). This dynamic field has made significant progress, demonstrating robust strategies for effectively concealing data (Pandey et al., 2021). While other strategies have been used, such as statistical steganography, which uses the statistical characteristics of digital media, this method conceals information. Covert communication techniques include, for instance, subtly altering an image's histogram or incorporating data into audio signals' statistical characteristics; distortion techniques and the Discrete Cosine Transform (DCT) that is used in signal processing and compression to transform data from the temporal or spatial domain to the frequency domain. As the total of cosine functions with different frequencies and magnitudes, it depicts the original signal. The DCT, which is frequently used in image and video compression standards like JPEG and MPEG, lessens redundant data while maintaining perceptual quality (Taha et al., 2021); the Least Significant Bit (LSB) method has emerged as a fundamental approach in this arena that Using this technique, the bits of the secret message are substituted for the LSB of each pixel in an image or sample in an audio file. This technique can efficiently disguise data because the human eye and ear are not sensitive to minute variations in the LSB. It can be discovered, though, if the LSBs are significantly changed (Rahman et al., 2023). Indeed, despite the abundance of approaches available, the LSB method remains extremely popular.

In accordance with these advances, novel strategies such as pseudorandom permutation have been developed to enhance the efficacy of data concealment within digital images (Bouteghrine et al., 2021). The Most Match Parity Bit Approach (MMPB-A) is a significant new method based on the LSB technique. This paper presents MMPB-A as a novel data embedding method that focuses on analyzing the parity bits of selected pixels (Xiong et al., 2020).

The MMPB-A's strategic essence is based on its thorough examination of the most parity bits within specified pixels during the information embedding process. This strategic approach, which is based on the LSB method, ensures that hidden data are

* Corresponding Author.
Email Address: khaznah.Alshammari2@nbu.edu.sa
https://doi.org/10.21833/ijaas.2024.08.007
Corresponding author's ORCID profile:
https://orcid.org/0009-0000-0741-1732

seamlessly integrated into the cover image. Because of the adaptive nature of this technology, as well as the use of the LSB method, concealed data has become an essential and indistinguishable part of the overall image. MMPB-A employs a clever encoding of concealed data indices using a three-bit code, which adds an extra layer of anonymity to the concealed data. The selection of a three-bit code for indexes represents a careful balance between data security and embedding efficiency, transforming MMPB-A into a smart and strategic technique in the landscape of digital image steganography. In this paper, the MMPB-A is presented as a breakthrough solution for concealing data within digital images. MMPB-T provides a comprehensive and secure approach for concealing data while maintaining similarity and confidentiality by combining the effectiveness of the LSB method with unique encryption strategies and strategic embedding operations. MMPB-A is a testament to the continued pursuit of excellence in the field of data concealment within digital images as steganography advances.

The rest of the paper is structured as follows: Section 2 provides background information and discusses related work; Section 3 explains carriers and the process of embedding data into images; Section 4 describes the method for detecting skin in an image; and Section 5 outlines techniques for hiding data in digital images. Section 6 explains the methodology used in the study, while Section 7 demonstrates the validation of a hidden message ("Welcome") within a 24-bit BMP cover image. Finally, Section 8 concludes the paper and discusses its limitations.

2. Literature survey

Steganography is the study of how to conceal data from digital images, which has proven essential for modern data security and communication (Kumar et al., 2020). Through the impeccable embedding of concealed data within an image's pixels, this approach enables the delivery of sensitive information while upholding the appearance of normalcy (Gubbi, 2018). Numerous techniques have been developed for this purpose, with the LSB technique being one of the most widely used. The LSB of each pixel in the image is changed in LSB steganography to represent a chunk of the hidden data. This technique is popular because it is easy to use and has little effect on the host's perception, thereby making it a desirable option for discreet communication. Steganographic techniques are always evolving as a result of technological advances, and researchers are always looking for new ways to improve the capacity, security, and undetectability of information buried within digital images (Hashim et al., 2018).

Digital image data concealment requires a careful balancing act between keeping data concealed and not being discovered. Beyond LSB, researchers have investigated more sophisticated approaches, including spread spectrum and frequency domain techniques like DCT (Sushil and Srivastav, 2023). Altering the frequency components of an image or distributing the hidden data over several pixels increases the detectability of the embedded information. Furthermore, scientists have created advanced algorithms that deliberately select specific pixels or areas of the picture for data embedding, reducing the visual impact of the entire image while optimizing the amount of concealed information that can be stored. The continued investigation of these methods emphasizes the ongoing search for reliable and safe methods to incorporate data into digital images for a variety of uses, such as digital watermarking and secure communication (Ray and Roy, 2020).

3. Carriers and concealing data into images

Carriers for concealing data utilize a variety of methods and materials. Text documents can be changed by moving lines and words around, while HTML files can convey concealed data using extra spaces and invisible characters (Colati and Johnston, 2020). Null ciphers or open codes conceal secret messages within the seemingly innocuous text, as demonstrated by extracting the third letter of each phrase to disclose a concealed message. Word shifting and document layout alteration techniques can also be used to hide or reveal data (Taleby Ahvanooey et al., 2019). With regards to disk space, unused or slack space within file systems can be taken advantage of, and secret partitions can be formed. Another option is to use network protocols because the features inherent in packets, particularly TCP/IP, can be altered to embed data (Nour et al., 2021). The physical configuration of carriers, such as program code layout and circuitry, can be individually tagged by their designer. Furthermore, music and images provide scope for a variety of concealment methods, such as inserting data into unused space, altering compression algorithms, or adjusting features with minimal impact on human perception (Nour et al., 2021).

Data can be concealed in images using a variety of methods, including direct message insertion, selective embedding in areas that are harder to see, random scattering, and repetitive distribution across the image (Kondasinghe, 2021). Image structure and palette are two factors to consider when creating digital photographs, and these are represented as arrays of numbers that indicate light intensities at pixels. Typically, digital photographs may hold approximately 300 kilobits of data at resolutions of 640 x 480 pixels and 256 colors. Red, green, and blue are the main hues used in 24-bit photos, and their pixel representations add to the file size, making compression necessary for transmission. Whereas loss compression, as seen in JPEG photos, compromises some image fidelity in exchange for a smaller file size, lossless compression, found in GIF and eight-bit BMP images, permits precise reconstruction of the original message (Kondasinghe, 2021). Fig. 1 provides an example

showing how to employ hue and saturation modifications to conceal data within an image, thereby demonstrating the adaptability of these techniques. The saturation slider, an important tool in digital image processing, is crucial for managing color intensity. The saturation slider, which is based on the Hue, Lightness, and Saturation (HLS) Color Model, allows users to fine-tune the vividness of colors within a picture. This slider provides sophisticated control over an image's visual effect, ranging from white (no saturation) to various degrees of gray and brilliant, intense colors (full saturation). Positive saturation slider values increase color intensity, bringing out more vibrant hues, whereas negative saturation values reduce color intensity, resulting in a more subdued, grayscale appearance. Understanding how to use the saturation slider is critical in steganographic procedures to enable practitioners to subtly insert information without affecting the overall visual perception of the image. Colors in the HLS model are defined by components.

A: Normal image saturation B: Image saturation modification

Fig. 1: Hue and saturation modifications

3.1. Hue, lightness, and saturation model (HLS)

- **Hue:** This ranges from purple to red, yellow, green, cyan, blue, and back to purple on the horizontal plane of a square container.
- **Saturation:** Located on the square box's vertical axis, this describes how 'grey' the colors look (Jang et al., 2023).

The HLS model improves color choices and provides capabilities that the RGB model does not offer. It allows coding to identify whether a given RGB color has lighter or darker tones.

3.2. HLS model coding

- To characterize a color, hue is commonly stated as an angle between 0-360˚.
- Saturation is indicated by a value ranging from 0 to 1 (Jang et al., 2023).

Using this model in code enables functions that go beyond what RGB can achieve, improving color control and selection accuracy.

3.3. Median filter

- The median filter is a nonlinear technique that is often used in image processing to minimize 'salt and pepper' noise (Win et al., 2019).
- Unlike convolution, median filtering is more effective at simultaneously lowering noise and retaining image edges (Yin et al., 2020).

3.4. Region filling

To complete the region in Fig. 2, the following procedure was applied:

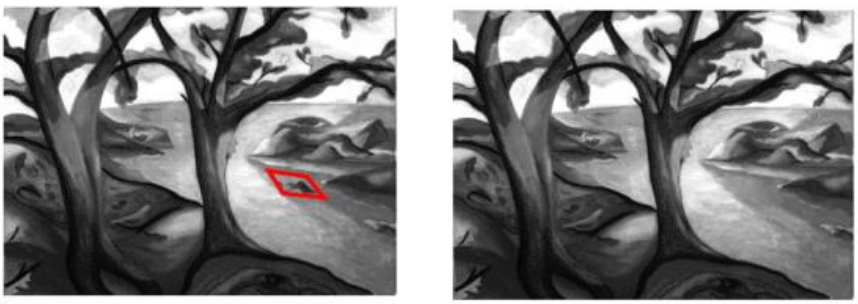
$$Xk = (Xk - 1 \oplus B) \cap Ac, k = 1,2,3, \ldots \quad (1)$$

where, $X0=P$ indicates the initial point within the region and B signifies the structurally symmetric element. The algorithm comes to an end at the iteration stage k if $Xk = Xk - 1$. The union of Xk and A includes both the filled set and its boundary. Meanwhile, the dilation process, if unbounded, may fill every region and the intersection at each step with Ac restricts the outcome to the interior of the region of interest (Li et al., 2022).

4. Finding skin

Recognizing unique restrictions associated with human skin appearance is part of the process of detecting skin in an image. The color of the skin is determined by a combination of blood (red) and melanin (yellow, brown), which limits the range of possible hues (Jamali et al., 2022). Because of the extra melanin, the skin is moderately saturated, with higher saturation, moving hues towards yellow. The skin filter eliminates desaturations by subtracting the camera system's zero response and transforming input R, G, and B values into log-opponent representation (Jamali et al., 2022). The green channel is used to express intensity. Smoothed texture and color planes are extracted using median

filters and texture amplitude computations. A skin filter that has been fine-tuned recognizes likely skin pixels based on proper hue, saturation, and modest texture amplitude (Vaz et al., 2020). Specific formulas determine the conversion from log-opponent to hue and saturation, with the range of considered hues adjusting with saturation. Because of skin reflectance qualities, some areas may appear desaturated or white, resulting in skin regions with holes. This problem is handled by undertaking region-filling morphological techniques (Jiang et al., 2023).



A: Initial point within the region B: Structurally symmetric element

Fig. 2: Region filling (Chu et al., 2021)

It is feasible to store three bits in each pixel to conceal an image within the LSBs of each byte in a 24-bit image, allowing for the concealment of 2,359,296 bits (294,912 bytes) of information in a 1,024 x 768 image (Harahap, 2021). Compression of the hidden message prior to embedding allows for the concealment of a significant amount of data while keeping the stego-image's visual look equal to the original. Without compression, the letter A can be hidden in three pixels. The modification involves only three underlined bits in the original raster data, illustrating that LSB requires only half of the bits in a picture (Hussain et al., 2021). Data hidden in the least and second-largest bits is undetectable to the naked eye.

Due to color constraints, controlling the LSBs in eight-bit images for steganography is difficult. Steganography software authors use various techniques to hide information in such photos, recognizing the importance of carefully selected cover images to avoid disclosing the presence of an embedded message in the final stego-image (Wang et al., 2022). When data are placed into the LSBs of raster data, the palette references to color entries are changed (Malik et al., 2023). Changes in palette position entries, for example, result in noticeable changes in the image in a simplified four-color palette (white, red, blue, and green) (Subramani and Veluchamy, 2023). The limitations of eight-bit images are apparent in the visibility of these shifts, especially when compared to minor alterations between adjacent color values (Fu et al., 2020).

5. Techniques for concealing data in digital images

This section provides details regarding a range of methods for concealing information within digital photographs (Baluja, 2019). Substitution systems, transform domain approaches, spread spectrum, statistical steganography, distortion techniques, and Bit-Plane Complexity Segmentation (BPCS) steganography are also under consideration. This section delves into substitution systems, transform domain approaches, and digital picture distortion techniques.

Substitution schemes, such as the widely used LSB approach, entail swapping out certain bits in a cover picture for those in a secret message. However, this approach is vulnerable to even minor image modifications and statistical abnormalities (Unkašević et al., 2019). To remedy this, the interval approach is presented, which enables random bit substitution whilst also improving robustness. A more advanced solution is pseudorandom permutation, which uses a pseudorandom number generator to disseminate information unexpectedly, thereby reducing the probability of collisions in longer messages. Furthermore, cover sections and parity bits propose partitioning the cover into discontinuous regions and embedding information in their parity bits (Unkašević et al., 2019).

Palette-based graphics, such as GIF and BMP, provide opportunities for steganography by encoding data in color palettes or picture data. Methods include adjusting LSBs and sorting palettes based on perceived similarity (Din, 2023). In predictive coding systems, dithering and quantization use the selective changing of cover pixels to preserve statistical features. Transform domain approaches, such as DCT steganography, conceal information in large image areas while remaining resistant to various attacks (Taha et al., 2021). Distortion techniques, such as changing selected cover pixels, provide perceptually tiny variations that reveal concealed information. Finally, the Most Match Parity Bit in Cover Image Technique offers a novel approach aimed at identifying the most identical bits in the LSBs when the cover image and secret message have full parity.

In summary, this thorough investigation provides insight into a wide range of steganographic techniques, each offering distinct benefits and tackling particular difficulties with regard to concealing data in digital images.

6. Methodology

The Most Parity Bit Technique, a breakthrough approach for concealing information within digital images, is introduced in the current paper. This novel approach is based on the detection of parity bits within a cover image and their alignment with secret message bits. The process involves several important steps, each precisely engineered to provide effective and secure data concealment, as follows.

Step 1: Encryption: To lay a solid foundation for information concealment (Cevik et al., 2023), this study initially addresses symbol encryption. Recognizing the pervasive representation of computerized symbols by eight bits in the ASCII code, a reconstruction of symbols using a six-bit coding has been undertaken. Because capital letters are not included in the coding, each symbol has 63 characters represented in a six-bit code. As a result, each symbol requires six bytes (two pixels) for concealment, assuming one bit is buried in one byte of the chosen pixels, as shown in Table 1.

Step 2: Hiding Location: The embedding procedure begins in the second row of the cover image, leaving the first three pixels unaffected. These initially unaltered pixels serve to hide the number of symbols used in the secret message. The row location of the embedded indices is determined by a mathematical calculation that takes into consideration the number of symbols, the width of the cover image, and a constant term.

$$P = ((N \times 2) \div W + 2)$$

where, P is The indices row position, N is the number of symbols, and $W$is the width of the cover image.

Each index is represented by three bits, ensuring that all secret symbols (1–8) have the anticipated range of indices. As a result, one pixel is used to hide each index by sequentially embedding one bit in the first bit of each byte of the selected cover pixel, as shown in Table 2.

Step 3: Type of Image Used: An essential component of the process is selecting one of the 24-bit BMP files for the cover images. This option is based on the Device-Independent Bitmap (DIB) format used for Windows bitmap files. This format ensures interoperability and broad applicability by making bitmaps easier to view on a variety of display devices (Zhang and Zhang, 2021).

Table 1: MMPB-A encryption strategy

Symbol	Decimal	Binary	Symbol	Decimal	Symbol	Binary	Decimal	Symbol	Binary	Decimal	Binary
Space	0	000000	S	20	>	010100	40	_	101000	60	111100
a	1	000001	t	21	=	010101	41	.	101001	61	111101
b	2	000010	u	22	[	010110	42	~	101010	62	111110
c	3	000011	V	23	]	010111	43	!	101011	63	111111
d	4	000100	w	24	?	011000	44		101100		
e	5	000101	x	25	%	011001	45		101101		
f	6	000110	y	26	;	011010	46		101110		
g	7	000111	z	27	@	011011	47		101111		
h	8	001000	#	28	0	011100	48		110000		
i	9	001001	$	29	1	011101	49		110001		
j	10	001010	and	30	2	011110	50		110010		
k	11	001011	‘	31	3	011111	51		110011		
l	12	001100	(	32	4	100000	52		110100		
m	13	001101	)	33	5	100001	53		110101		
n	14	001110	*	34	6	100010	54		110110		
o	15	001111	+	35	7	100011	55		110111		
o	16	010000	-	36	8	100100	56		111000		
p	17	010001	/	37	9	100101	57		111001		
q	18	010010	:	38	{	100110	58		111010		
r	19	010011	<	39	}	100111	59		111011		

Table 2: MMPB-A encryptions index

Number	Value
1	001
2	010
3	011
4	100
5	101
6	110
7	111
8	000

Step 4: Embedding Process: Each symbol is concealed in two pixels throughout the embedding process, thereby totaling six bytes. Because each symbol consists of six bits, one byte out of the two chosen pixels can contain one bit of the symbol concealed. Testing the parity between the first bit of the embedded symbol and the eighth bit of the first byte of the two chosen pixels is the first step in the procedure. The bits that come after are tested one after the other. The procedure entails evaluating the seventh bit of each byte of the specified pixels until a match is found if parity is not established. The approach involves looking at the first, second, and third LSBs to find the most appropriate parity when parity cannot be determined. This adaptive strategy ensures that the secret message is concealed in the most similar or the same locations within the cover image, giving messages plenty of space to be seen while remaining undetectable.

Step 5: Extraction Process: The decoding procedure starts by reading the first three pixels of the first row after obtaining the compromised image to ascertain the quantity of concealed symbols. Subsequently, an established equation is used to determine the index positions. Until the number of read pixels equals the number of embedded symbols, the indices are sequentially read. Then, following

their preset places, the decoder extracts the encoded data starting from the second row.

The Most Parity Bit Technique is a flexible and all-encompassing approach for concealing data in images. Through the combination of encryption, well-chosen concealing locations, careful image selection, and an adaptive embedding process, the method provides a safe and effective means of data concealment. It ensures that large amounts of data can be concealed within the cover image with little noticeable or statistical alteration.

7. Validation of a secret message (Welcome) within a 24-bit BMP cover image

This section presents the validation of MMPB-A for Data Concealment in Digital Image. This validation process includes using the approach for secret message concealing. Concealing the secret message example is **t**o illustrate the application of the Most Parity Bit Approach, the concealment of the secret message (Welcome) within a 24-bit BMP cover image is considered. The decimal representation of this word is '24 5 12 3 15 13 5' and in the binary system this translates to '011100000101 001100 000011 001111 001101 000101'.

To conceal the first letter of the message (W) in the cover image, the encoding process begins with the first binary value (011100). This binary sequence is embedded in the first two pixels of the second row of the cover image. The encoder initiates a test on the 8th bit of each byte within these pixels with the aim of establishing parity. However, if complete parity is not achieved with this bit, the encoder attempts to establish parity using the 8th bit of the same pixels (Fig. 3). To conceal the second letter of the message (e) in the cover image, the second binary value (000101) was tested for parity in the second two pixels. The encoding takes an index for it because it was found using the 5th bit of the cover image (Fig. 4). Then, as shown in Fig. 5, the same process is applied for the third binary value (001100) to conceal the third letter of the message (l) in the cover image.

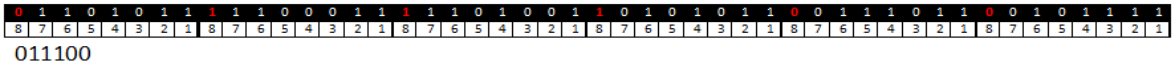


Fig. 3: Concealing the letter 'W' in the cover images

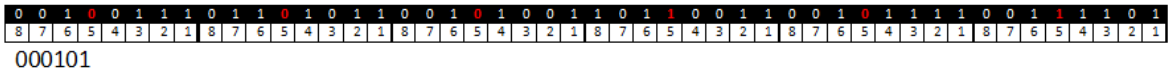


Fig. 4: Concealing the Letter 'E' in the Cover Images

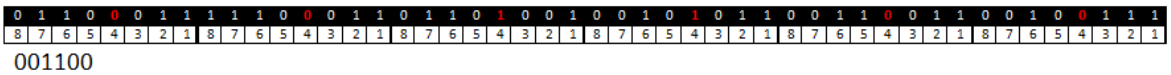


Fig. 5: Concealing the Letter 'I' in the Cover Images

To conceal the fourth letter of the message (C) in the cover image, the encoding process begins with the fourth binary value (000011). However, if no full parity is detected in the next two pixels, the encoder will not continue to another pixel and will check for the greatest parity possible in the LSBs (1st, 2nd or 3rd bits) of these two pixels and flip any that do not have the same values (Fig. 6).

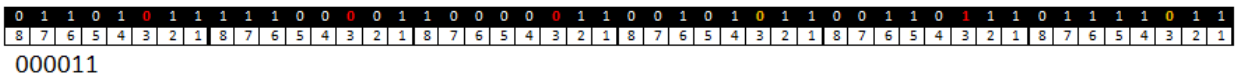


Fig. 6: Concealing the letter 'C' in the cover images

To conceal the fifth, sixth, and seventh letters of the message (O, M, and E) in the cover image with the binary values '001111,' '001101' and '000101,' the process continues when parity is found or when the most parity in the two specified pixels is found and indices are assigned (Figs. 7, 8, and 9).

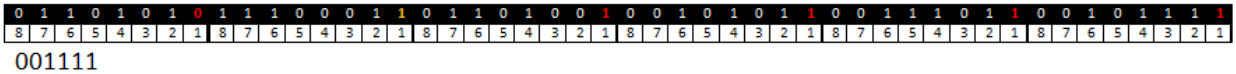


Fig. 7: Concealing the letter 'O' in the cover images

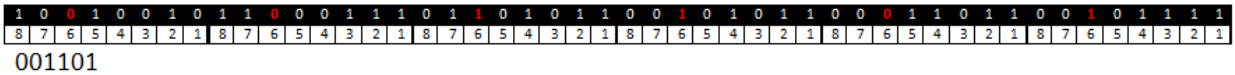


Fig. 8: Concealing the letter 'M' in the cover images

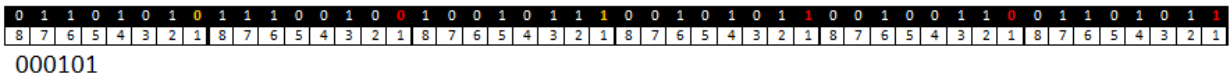


Fig. 9: Concealing the letter 'E' in the cover images

To conceal the values of the indexes in the cover image using binary encoding (Table 3), each index must be inserted into a pixel in the first row, following the final row of the hidden secret data. Each index is discretely inserted within the first bit of each byte in the pixels supplied. It is important to note that each of these indices is going to be encoded with three bits (Fig. 10).

Table 3: Encoding the index array

Encoding index	8	5	4	3	1	6	1
Message letter numbers	1	2	3	4	5	6	7
Message letters	W	e	l	c	o	m	e

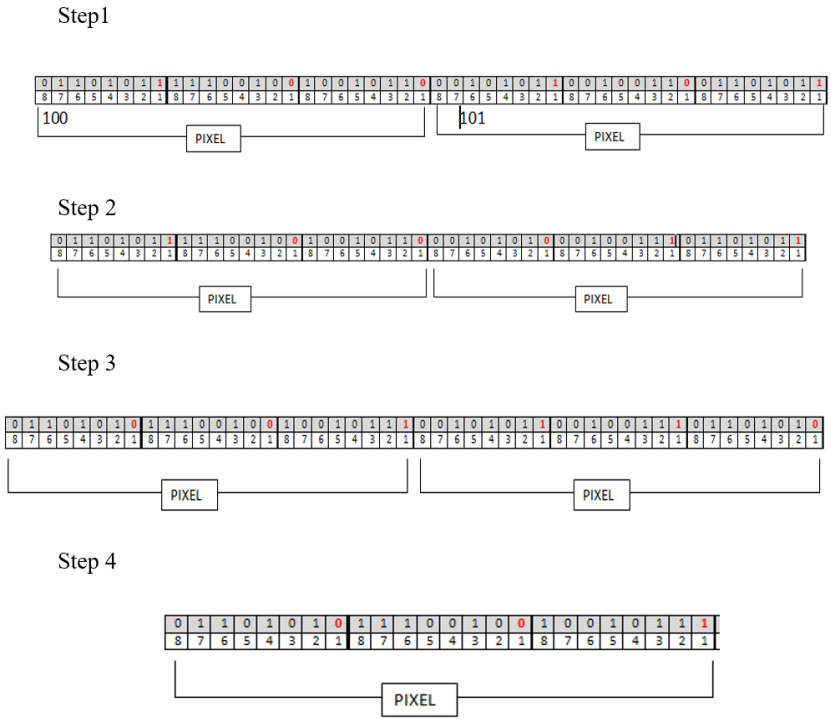


Fig. 10: Concealing the Index within the cover image

8. Conclusion

Steganography exemplifies humanity's age-old pursuit of concealing and communicating secret information. Various strategies in this discipline have evolved over time, with digital image concealment emerging as an important milestone. The success of digital image steganography is noteworthy, demonstrating the development of robust and powerful methods for covertly embedding information. The popularity of the LSB technique demonstrates its dominance in this domain through alternative approaches such as statistical steganography, distortion techniques, and the DCT, which have also contributed to the breadth of steganography methodologies.

Among these advances, this paper has proposed a revolutionary technique called the MMPB-A, which builds on the basis of the LSB method. This novel method focuses on determining the parity bits of selected pixels to discretely insert information within cover pictures. Encrypting each symbol with a six-bit code not only gives a large domain for concealing information but also increases similarity and secrecy. Furthermore, encoding hidden data indices in a three-bit code provides another layer of secrecy, thereby increasing the possibility of information hiding. The MMPB-A's continuous advancement of steganography techniques demonstrates the dynamism of this discipline and its ongoing relevance in the realm of information security, which was applied in the example that involved concealing the word 'Welcome' in an image.

8.1. Limitation

Data concealment was performed at the message (Welcome) using the Match Parity Bit Approach (MMPB-A) procedures to conceal this message in the digital image. However, this may be insufficient to thoroughly assess the message's functionality (Welcome). It is therefore strongly urged that a live experiment be constructed, as well as the MMPB-A be applied in various scenarios.

Funding

This work is supported by the Deanship of Scientific Research, Northern Border University, Arar, Kingdom of Saudi Arabia, under grant number "NBU-FFR-2024-2467-01."

Acknowledgment

The author extends their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, Kingdom of Saudi Arabia, for funding this research work through project number "NBU-FFR-2024-2467-01."

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Baluja S (2019). Hiding images within images. IEEE Transactions on Pattern Analysis and Machine Intelligence, 42: 1685-1697. https://doi.org/10.1109/TPAMI.2019.2901877 **PMid:30835212**

Bouteghrine B, Tanougast C, and Sadoudi S (2021). Novel image encryption algorithm based on new 3-d chaos map. Multimedia Tools and Applications, 80: 25583-25605. https://doi.org/10.1007/s11042-021-10773-8

Cevik T, Cevik N, Rasheed J, Asuroglu T, Alsubai S, and Turan M (2023). Reversible logic-based hexel value differencing—A spatial domain steganography method for hexagonal image processing. IEEE Access, 11: 118186-118203. https://doi.org/10.1109/ACCESS.2023.3326857

Chu Y, Li M, Coimbra CF, Feng D, and Wang H (2021). Intra-hour irradiance forecasting techniques for solar power integration: A review. IScience, 24: 103136. https://doi.org/10.1016/j.isci.2021.103136 **PMid:34723160 PMCid:PMC8531863**

Colati G and Johnston L (2020). Digital files and carrier media. In: Harvey DR and Mahard MR (Eds.), The preservation management handbook: A 21st century guide for libraries, archives, and museums: 287-306. Rowman and Littlefield Publishers, Lanham, USA.

Din R (2023). Comparison of steganographic techniques of spatial domain and frequency domain in digital images. Borneo International Journal, 6(3): 109-118.

Fu Q, Di X, and Zhang Y (2020). Learning an adaptive model for extreme low-light raw image processing. IET Image Processing, 14: 3433-3443. https://doi.org/10.1049/iet-ipr.2020.0100

Gubbi T (2018). Patch-based denoising with k-nearest neighbor and SVD for microarray images. In: Silhavy R (Ed.), Software engineering and algorithms in intelligent systems. CSOC2018 2018. Advances in Intelligent Systems and Computing, 1(763): 132-147. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-319-91186-1_15

Harahap ISA (2021). Least significant bit (LSB) modification analysis with alternate insertion message technique on image media. Journal Basic Science and Technology, 10(3): 78-85. https://doi.org/10.35335/jbst.v10i3.1756

Hashim MM, Rahim MSM, Johi FA, Taha MS, and Hamad HS (2018). Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats. International Journal of Engineering and Technology, 7(4): 3505-3514.

Hussain M, Riaz Q, Saleem S, Ghafoor A, and Jung KH (2021). Enhanced adaptive data hiding method using LSB and pixel value differencing. Multimedia Tools and Applications, 80: 20381-20401. https://doi.org/10.1007/s11042-021-10652-2

Jamali H, Castillo LT, Morgan CC, Coult J, Muhammad JL, Osobamiro OO, Parsons EC, and Adamson R (2022). Racial disparity in oxygen saturation measurements by pulse oximetry: Evidence and implications. Annals of the American Thoracic Society, 19(12): 1951-1964. https://doi.org/10.1513/AnnalsATS.202203-270CME **PMid:36166259**

Jang J, Badloe T, Sim YC, Yang Y, Mun J, Lee T, Cho YH, and Rho J (2020). Full and gradient structural colouration by lattice amplified gallium nitride Mie-resonators. Nanoscale, 12(41): 21392-21400. https://doi.org/10.1039/D0NR05624C **PMid:33078822**

Jiang S, Yan W, Cui C, Wang W, Yan J, Tang H, and Guo R (2023). Bioinspired thermochromic textile based on robust cellulose aerogel fiber for self-adaptive thermal management and dynamic labels. ACS Applied Materials and Interfaces, 15(40): 47577-47590. https://doi.org/10.1021/acsami.3c11692 **PMid:37756210**

Kondasinghe CM (2021). A system to preserve metadata using steganography. Ph.D. Dissertation, University of Colombo School of Computing, Colombo, Sri Lanka.

Kumar M, Kumar S, and Nagar H (2020). Comparative analysis of different steganography technique for image or data security. International Journal of Advanced Science and Technology (IJAST), 29(4): 11246-11253.

Li X, Wang D, and Saeed T (2022). Multi-scale numerical approach to the polymer filling process in the weld line region. Facta Universitatis, Series: Mechanical Engineering, 20(2): 363-380. https://doi.org/10.22190/FUME220131021L

Malik A, Ali M, Alsubaei FS, Ahmed N, and Kumar H (2023). A color image encryption scheme based on singular values and chaos. CMES-Computer Modeling in Engineering and Sciences, 137(1): 965-999. https://doi.org/10.32604/cmes.2023.022493

Nour B, Mastorakis S, Ullah R, and Stergiou N (2021). Information-centric networking in wireless environments: Security risks and challenges. IEEE Wireless Communications, 28(2): 121-127. https://doi.org/10.1109/MWC.001.2000245 **PMid:34366719 PMCid:PMC8340877**

Pandey D, Wairya S, Al Mahdawi RS, Najim S ADM, Khalaf HA, Al Barzinji SM, and Obaid AJ (2021). Secret data transmission using advanced steganography and image compression. International Journal of Nonlinear Analysis and Applications, 12(Special Issue): 1243-1257.

Rahman S, Uddin J, Zakarya M, Hussain H, Khan AA, Ahmed A, and Haleem M (2023). A comprehensive study of digital image steganographic techniques. IEEE Access, 11: 6770-6791. https://doi.org/10.1109/ACCESS.2023.3237393

Ray A and Roy S (2020). Recent trends in image watermarking techniques for copyright protection: A survey. International Journal of Multimedia Information Retrieval, 9(4): 249-270. https://doi.org/10.1007/s13735-020-00197-9

Subramani B and Veluchamy M (2023). Bilateral tone mapping scheme for color correction and contrast adjustment in nearly invisible medical images. Color Research and Application, 48(6): 748-760. https://doi.org/10.1002/col.22887

Sushil V and Srivastav S (2023). A data safety approach based on image steganography. In the International Conference on IoT, Communication and Automation Technology, IEEE, Gorakhpur, India: 1-6. https://doi.org/10.1109/ICICAT57735.2023.10263742

Taha NA, Al Saffar A, Abdullatif AA, and Abdullatif FA (2021). Image Steganography using dynamic threshold based on discrete cosine transform. Journal of Physics: Conference Series, 1879(2): 022087. https://doi.org/10.1088/1742-6596/1879/2/022087

Taleby Ahvanooey M, Li Q, Hou J, Rajput AR, and Chen Y (2019). Modern text hiding, text steganalysis, and applications: A comparative analysis. Entropy, 21(4): 355. https://doi.org/10.3390/e21040355 **PMid:33267069 PMCid:PMC7514839**

Unkašević T, Banjac Z, and Milosavljević M (2019). A generic model of the pseudo-random generator based on permutations suitable for security solutions in computationally-constrained environments. Sensors, 19(23): 5322.

https://doi.org/10.3390/s19235322
PMid:31816914 PMCid:PMC6929088

Vaz R, Frasco MF, and Sales MGF (2020). Photonics in nature and bioinspired designs: Sustainable approaches for a colourful world. Nanoscale Advances, 2(11): 5106-5129. https://doi.org/10.1039/D0NA00445F
PMid:36132040 PMCid:PMC9416915

Wang X, Liu C, and Jiang D (2022). An efficient double-image encryption and hiding algorithm using a newly designed chaotic system and parallel compressive sensing. Information Sciences, 610: 300-325. https://doi.org/10.1016/j.ins.2022.08.002

Win NN, Kyaw K, Win T, and Aung P (2019). Image noise reduction using linear and nonlinear filtering techniques. International Journal of Scientific and Research Publications, 9(8): 816-821. https://doi.org/10.29322/IJSRP.9.08.2019.p92113

Xiong Q, Zhang X, Liu W, Ye S, Du Z, Liu D, Zhu D, Liu Z, and Yao X (2020). An efficient row key encoding method with ASCII code for storing geospatial big data in HBase. ISPRS International Journal of Geo-Information, 9(11): 625. https://doi.org/10.3390/ijgi9110625

Yin H, Gong Y, and Qiu G (2020). Fast and efficient implementation of image filtering using a side window convolutional neural network. Signal Processing, 176: 107717. https://doi.org/10.1016/j.sigpro.2020.107717

Zhang YJ and Zhang YJ (2021). Image storage and communication. In: Zhang YJ (Ed.), Handbook of image engineering: 269-276. Springer, Singapore, Singapore. https://doi.org/10.1007/978-981-15-5873-3_7