Proceedings of CONF-MLA 2024 Workshop: Securing the Future: Empowering Cyber Defense with Machine Learning and Deep Learning
DOI: 10.54254/2755-2721/94/2024MELB0058

Advancements in Spatial Domain Image Steganography: Techniques, Applications, and Future Outlook

Jiajun Ye

Aberdeen Institute of Data Science and Artificial Intelligence, South China Normal University, Guangzhou, China

u08jy22@abdn.ac.uk

Abstract. Image steganography, a technique for transmitting secret information hidden within images over public networks undetected, serves as a discreet alternative to cryptography in the field of information security. This article explores new steganography techniques based on the Least Significant Bit (LSB) method, widely recognized for its simplicity in embedding secret data by altering the least significant bit of pixels in the spatial domain. The performance of these LSB-based methods is critically assessed using criteria such as Peak Signal-to-Noise Ratio (PSNR), embedding capacity, and histogram analysis. A comprehensive review of recent literature provides a foundation for this evaluation, highlighting advancements and identifying areas for future improvement. Additionally, the article discusses practical applications of LSB-based steganography in healthcare, government operations, and cloud storage, suggesting directions for further research and development in this subtly powerful area of data security.

Keywords: Data hiding, image steganography, LSB.

1. Introduction

The exponential growth of the Internet has significantly enhanced the way information is disseminated globally, bringing information security to the forefront of digital communication challenges. Cryptography and steganography are pivotal in safeguarding data against unauthorized access and manipulation. While cryptography encrypts information, making it secure but conspicuous and thus susceptible to targeted attacks, steganography offers a stealthier solution. This method embeds sensitive information within images, making it virtually undetectable to the naked eye. Historical instances, such as the use of invisible inks during the American Revolutionary War and the ancient Greek practice from which the term 'steganography' originates, underscore the long-standing value of concealing information in plain sight [1].

Research Problem: Despite its advantages, steganography faces several challenges that limit its effectiveness and application. The primary issue revolves around the balance between invisibility and the amount of data that can be securely hidden without detection. The least significant bit (LSB) technique, although popular for its simplicity, must evolve to address modern digital communication's complexities and vulnerabilities. Additionally, as digital steganography becomes more sophisticated, there is an increasing need to develop methods that can withstand new types of steganographic detection and attacks, ensuring that hidden data remains secure even under scrutiny.

DOI: 10.54254/2755-2721/94/2024MELB0058

This Article's Contribution: This article delves into the realm of image steganography, particularly focusing on advancements in LSB-based techniques. Initially, it introduces the spatial domain image steganography technology, setting the stage for a deeper exploration of LSB steganography foundations. Subsequently, recent advancements in LSB techniques are meticulously reviewed, illustrating how they adapt to and address the evolving demands of information security. The practical applications of these techniques in fields such as commerce and medicine are then discussed, highlighting the diverse potential of steganography beyond traditional security scenarios. Finally, the article synthesizes these findings and suggests potential future research directions, aiming to propel the field of steganography towards more robust and versatile applications.

2. Overview of Spatial Domain Image Steganography Techniques

2.1. Distinction between spatial and frequency domain

There are two domains can be used in hiding information: spatial domain and frequency domain. It is necessary to convert the cover image into its corresponding frequency domain coefficients before embedding a message in the transform domain. Improved information concealing capability and safety are offered by embedding frequency coefficients [2]. It including Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT) and Discrete Wavelet Transformation (DWT). The secret information can be hidden in the spatial domain by using the cover picture pixels, for example, by swapping out secret bits for regular pixels. It including simple LSB steganography, pixel value differencing (PVD) and so on.

2.2. Popularity and characteristics of LSB steganography

Figure 1's data comes from [5], it's clear that The LSB methodology was the most frequently utilized method especially in 2022, which is 22 times. Because of its speed and ease of use in image-based [4]. That's why this paper discusses it. As show in the Figure 1.

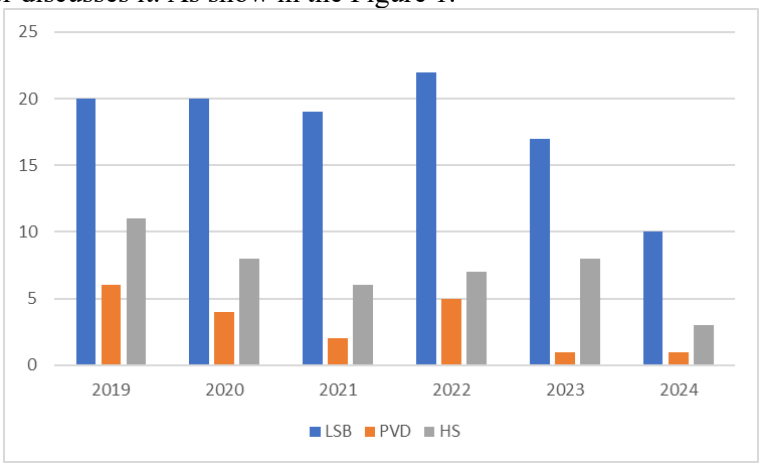

Figure 1. Usage of steganography technology [5].

DOI: 10.54254/2755-2721/94/2024MELB0058

2.3. Common images and datasets used

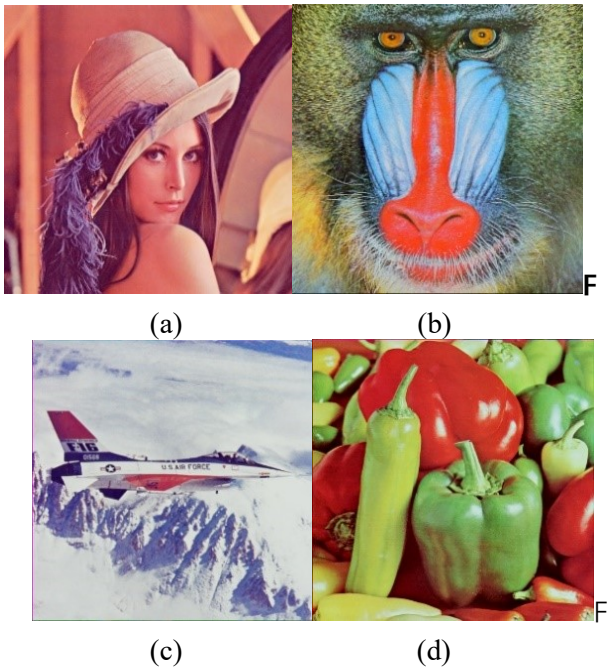

Figure 2. Common images: (a) Lena, (b) Baboon, (c) Jet, (d) Peppers (Photo credit: Original).

As show in the Figure 1 and table 1. To evaluate the performance of a steganography technique, researchers typically use standard images such as 'Lena', 'Baboon', 'Jet' and 'Peppers' in Figure 2. for experimentation and analysis. These images appear in different sizes and types in different datasets. There are several commonly used datasets in the field of image steganography [21] and [22]:

Table 1. Dataset Overview.

Dataset	Total amount of data(sheet)	Size	Type
BOSSBase	10000	512*521	Grayscale image
BOWS2	10000	512*512	Grayscale image
COCO	330000	640*640*3	Grayscale image
USC-SIPI	170	512*512	Color image

2.4. Evaluation criteria

Here are some criteria used to evaluate the security and performance of a steganography technique.

2.4.1. Embedded capacity. It is defined as the greatest amount of data that may be concealed in a picture. The embedding algorithm and cover image property have an impact on the capacity value, and a variety of sophisticated techniques that improve capacity were put forth, albeit at the expense of some other considerations [6].

$$AEC(bpp) \triangleq \frac{\text{Total embedded bits}}{\text{Total number of pixels in the image}} \quad (1)$$

2.4.2. Imperceptibility. To improve Imperceptibility, the gap between the cover image and the stego image needs to be narrowed. The statistic that is most frequently used to assess any type of steganography is the Peak Signal to Noise Ratio (PSNR). This metric is assessed by first determining the stego image's mean square error (MSE), and then applying equation (3) [6]. In formula (2), P is long, Q is wide, U (e, f) is cover image and V (e, f) is stego image.

DOI: 10.54254/2755-2721/94/2024MELB0058

$$MSE \triangleq \frac{\sum_{e=1}^{P} \sum_{f=1}^{Q} [U(e,f)-V(e,f)]^2}{P \times Q} \quad (2)$$

In formula (3), Umax is maximum variation in image U's pixel values (e, f), a higher PSNR value denotes a greater quality reconstruction of the stego image [6].

$$PSNR \triangleq 10\log_{10} \frac{U_{max}^2}{MSE} \quad (3)$$

2.4.3. Histogram. A histogram displays the frequency of a specific pixel intensity value throughout the entire image. As the pixel value changes, its histogram also changes, and analysts determine whether information is hidden in the image by comparing the difference between the histogram of the cover image and the histogram of the stego image. Narrowing the gap between the two histograms can effectively reduce the possibility of hidden information being discovered [6].

3. LSB Steganography Technique

LSB method is a steganography technique which can be used in spatial domain. It usually replaces the cover image's least significant bit with the hidden information. This method usually has very little change in pixel values. The primary benefit of this method is that because the amplitude variation of the pixel values is limited by ±1, altering the LSB plane has no effect on how humans perceive the overall quality of the image.

Here gives an example on how to use LSB method to replace the least significant bit in a grey image which come from [8]. The grey color values or the binary values of the image is like:

01010010
01001010
10010111
11001100
11010101
01010111
00100110
01000011

And it hided the "Z" in the cover image, the binary value of "Z" is 10110101 [8]. Here is the image after hiding the "Z", it is called stego image.

01010011
01001010
10010111
11001101
11010100
01010111
00100110
01000011

In this example, it only changed three LSBs in the cover image, it really hard to be found by human's eyes, so that is the feasibility of this method. This method also can be used in RGB image.

To better understand original LSB, the completed processes of hiding and extracting information will be shown.

DOI: 10.54254/2755-2721/94/2024MELB0058

3.1. The hiding process

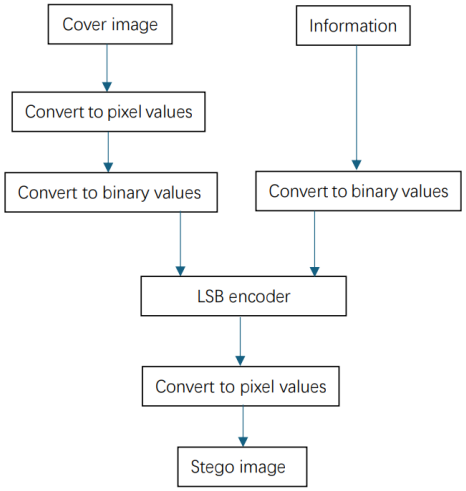

Figure 3. The hiding process [9].

The completed process of hiding information into the cover image is Figure 3. Firstly, the information is needed as well as the cover image which is used to be the carrier to stash data. Secondly, the original image will be changed to pixel values. In addition, the pixel value of the image and the information which needed to be stashed will be converted to binary values at the same time. Then the LSB encoder will be used, its function is similar with the example given earlier in this paper, is to replace the cover image's LSB with the binary values of the data which needed to hided. After that, the binary values will be converted to the pixel values. Finally, the pixel values will be restored to an image, and that is called stego image which contains the hidden data.

3.2. The extracting process

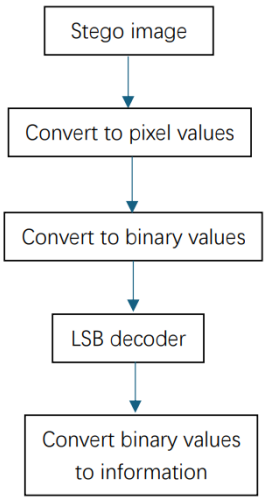

Figure 4. The extracting process [9].

The completed process of extracting information from the stego image is Figure 4. Completely opposite to the embedding process, this process will get information from the stego image. Firstly, the stego image is needed which has the hidden data. Secondly, the input image will be converted to pixel values. Thirdly, the pixel value of the image will be changed to binary values. The fourth step will use the LSB decoder which has the reverse function as the LSB encoder, it can take the LSB from the stego

DOI: 10.54254/2755-2721/94/2024MELB0058

image. That is, the location where the hidden information is located. Fifthly, the binary values or the least bits will be converted to the secret information.

But the basic LSB method has some disadvantages. The primary drawbacks include deficiencies in filtering, compression, geometric assaults, tampering, and resilience [10]. It also shows low embedded capacity because it only replaces few bits, which means it hides little data. Based on its shortcomings, this paper gives some improved methods which related to LSB steganography technique in the next section.

4. Recent Improvements Related to LSB

This section tries to provide a summary about some improved methods which about LSB, showing its improved in PNSR, embedded capacity or some other parts.

4.1. The methos about xor and lsb

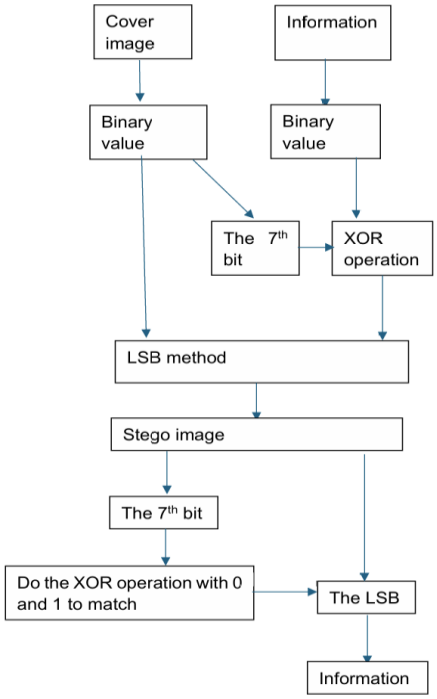

Figure 5. Steganography using LSB and XOR operation (Photo credit: Original).

As show in the Figure 5. T. Bhuiyan and et al introduced a new way to hide data by using LSB method and XOR in RGB image in 2019. In the embedding process, this method like the basic one at first, it changes the cover image and the secret information to the binary value, then it makes the 7th bits of Red, Green and Blue components and the binary values of information which will be hidden to do XOR operation and replaces the LSBs with the result of XOR operation. To extract the data, the 7th bits need to do XOR with 1 and 0, and match the results with the LSBs, collecting the matched bits, finally get the completed data. Fewer time is needed to do with this method. The average PNSR are 64.977dB and 70.92dB for the image size of 256*256 and 512*512 in hiding 1,024 byte.

DOI: 10.54254/2755-2721/94/2024MELB0058

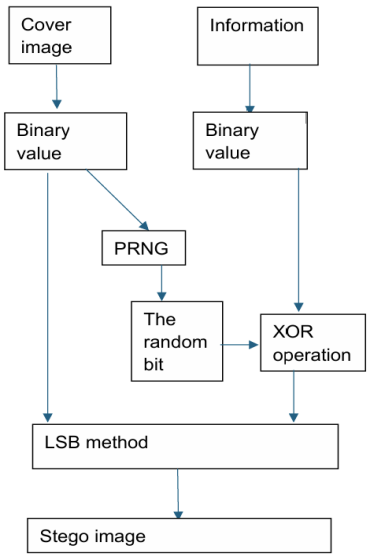

Figure 6. Steganography using LSB, XOR operation, and PRNG (Photo credit: Original).

As show in the Figure 6. U. A. Md. E. Ali and et al also created a method which based on XOR and LSB. It also converts the data and cover image to binary values, but it does not choose the 7th bit to do the XOR operation. It uses A Pseudo Random Number Generator (PRNG) which is a way to choose a bit from the first bit to the seventh bit randomly, and does XOR operation with data, then replace the output with the LSB in RGB image. The extracting process is to make the chosen bit to do XOR operation with LSB in the stego image again to get the information. Although compare to the original LSB steganography technique, its PSNR does not develop, it makes the attackers more difficult to get the correct data and improve its security.

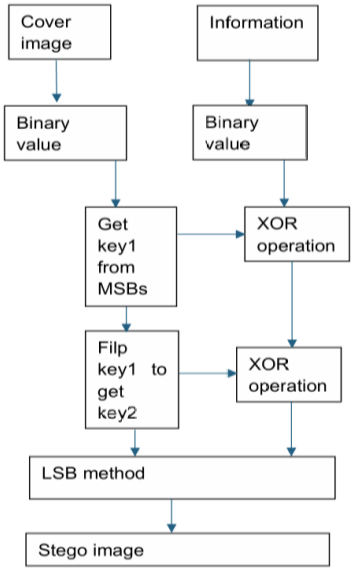

Figure 7. Steganography using double XOR operations and LSB (Photo credit: Original).

As show in the Figure7. A. Ahmed and et al presented a double XOR and LSB-based steganography method. It does XOR operation twice and uses LSB method. A string of bits is taken from cover image's most significant bit (MSB)s having the same length in hidden messages which called key1, and does the first XOR operation with hidden message. Then it flips the key1 to get key2, and does the XOR operation

DOI: 10.54254/2755-2721/94/2024MELB0058

between the message which has done a XOR operation before and key2. Finally, the message will be embedded into the image. It can also use to reverse way to get the message. The experiments shows the PSNR of this method are between 33.95dB and 55.67dB in hiding data from 200 byte to 1000 byte in 256*256, 512*512 and 1024*1024 three type of image sizes. Although it doesn't show very good PNSR, it improved the capacity.

4.2. The methods about PVD and LSB

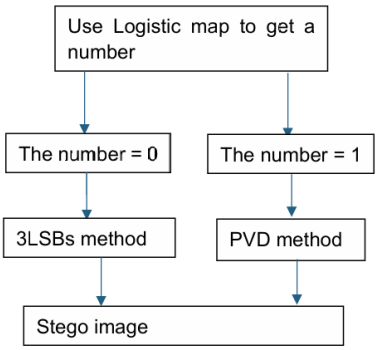

Figure 8. Steganography using LSB, PVD and Logistic map (Photo credit: Original).

As show in the Figure 8. S. Prasad and et al used PVD, LSB and Logistic map to design a method for image steganography in grayscale image. Logistic map is an algorithm which can generate a secret binary sequence. In this strategy, the result which logistic map provides will be used to judge which basic way to embed data. If it is 1, it uses the PVD method, or it uses the 3LSBs method which is way to replace the 3 LSBs in the cover image. The study illustrated the average PNSR of it is 38.7925dB in 512*512 size. In addition, it has been proved by the presented experimental results that it is a safe way to hide information.

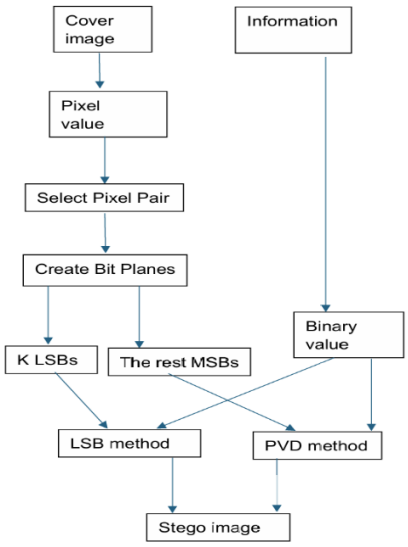

Figure 9. Simultaneous use of PVD and LSB steganography on one pixel bit (Photo credit: Original).

As show in the Figure 9. K. H. Jung proposed a method which used the PVD technique and LSB technique in the same image at the same time. Two bit planes will be created in the continuous pixels at first. After that, it uses a formula to divide it into the k LSBs and the MSBs excluding the rest. Use PVD steganography technique to hide the data on the first most significant bits, and then use LSB steganography technique on the k least bits. This method has an embedding capacity of 1,052,641 bits

DOI: 10.54254/2755-2721/94/2024MELB0058

and an average PSNR of 32.61 dB which confirmed by tests. It improves the embedding rate and is not easily detected and noticeable by the human eye. And it has gained better robustness, allowing for the insertion of two different messages and making it more difficult for attackers to detect and extract information.

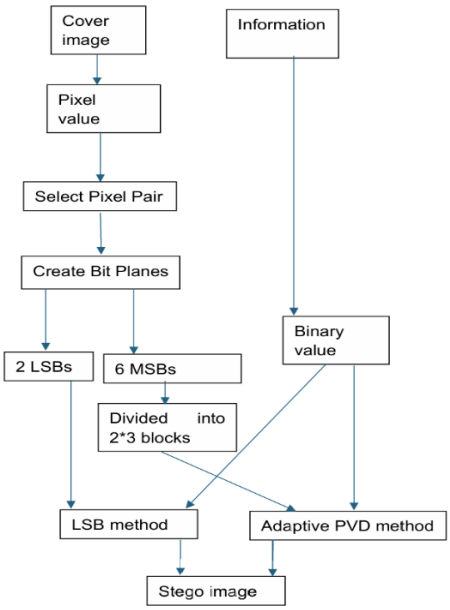

Figure 10. Simultaneous use of adaptive PVD and LSB steganography on one pixel bit (Photo credit: Original).

As show in the Figure 10. S. Singh devised an improved method which based on Jung's one. It replaced the original PVD method with adaptive pixel value differencing method. This strategy first converts the information and cover image into binary values, dividing binary values of cover image into the first six MSBs and the last two LSBs, which are then divided into 2 × 3 non overlapping blocks. The first four hidden data bits are hidden in the first six MSBs by using adaptive PVD method, that is, PVD steganographic method is used to hide data in the diagonal and vertical directions, and the last 12 bits are hidden in the last two LSBs, still using LSB steganographic method to hide data. Finally, the two nonoverlapping blocks are merged and converted into binary, converted into pixel values, and finally the stego image is obtained. The extraction method is also completely opposite. First, it is converted into binary numbers, and then divided into 2 × 3 non overlapping blocks. The last two bits directly extract the hidden information, while the first six MSBs non overlapping blocks extract the data using the adaptive PVD extraction method, concatenate them together, and obtain the complete hidden data. Experimentations indicates that this method may conceal 139,224 bits and offers an average PSNR 1.47 dB higher than the current Jung strategy.

DOI: 10.54254/2755-2721/94/2024MELB0058

4.3. The methods about cryptography and LSB

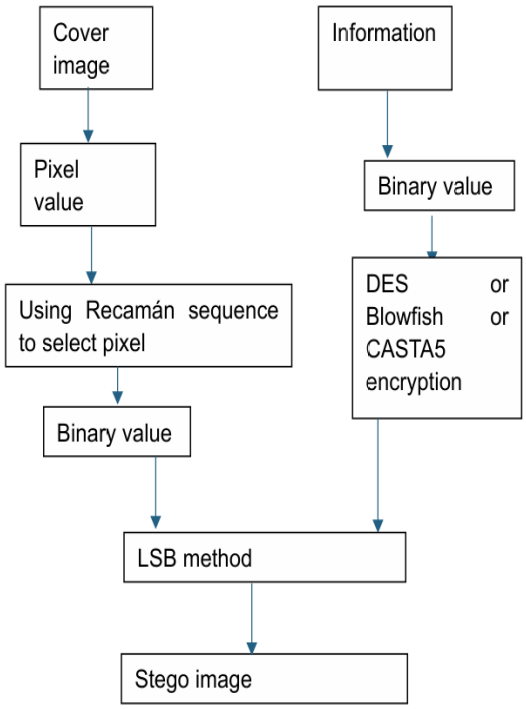

Figure 11. Steganography using LSB, Recamán's sequence, and encryption method (Photo credit: Original).

As show in the Figure 11. S. Farrag and et al suggested an Recamán's sequence -based method which contain LSB steganographic technique and cryptography. Although the Recamán's sequence is an intriguing and easily defined sequence of integers, its potential strength against steganalysis is demonstrated by the ensuing complexity. The sequence is like {1, 3, 6, 2, 7, 13, 20, 12, 21, 11, 22, 10, 23, 9, 24, 8, 25, 43, 62, 42, 63}. In this method, it first uses the cryptographic methods to encrypt the data, such as Blowfish, DES and CAST5 method. Then according to Recamán's sequence, embed one bit of encrypted data in the least significant bit of the three color channels (red, green, blue) at each specified pixel position by using the LSB method. The studies explain the PNSR of it is 62.86 dB by using DES cryptographic method. What's more, in the image's size of 512*512, it can insert 53000 characters. And it shows the safety and big capacity again.

DOI: 10.54254/2755-2721/94/2024MELB0058

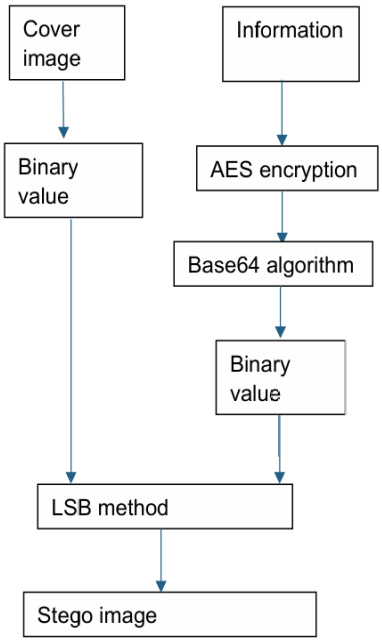

Figure 12. Steganography using LSB, AES algorithm, and Base64 algorithm (Photo credit: Original).

As show in the Figure 12. F. Anwar and et al implemented a method which using AES, LSB method and Base64 algorithm to have image steganography. AES is an algorithm which used in cryptography. Base64 is also an algorithm that uses 64 ASCII characters as its character set. These characters include uppercase letters A-Z, lowercase letters a-z, numbers 0-9, as well as plus signs (+) and slashes (/). Map ASCII code to its character set [11]. This scheme uses AES to encrypt message, then Base64 method is used to deal with encrypted information. After that, it will be converted to binary values and replace the LSB in cover image. The procedure of extracting is on the contrary. The studies illustrate the PSNR of it is higher than 53 dB on average, and the quality of the nice stego image is also displayed by the histogram analysis.

4.4. The method about dual image and LSB

As show in the Figure 13. G. Maji and et al presented a method used two images, the reference image and cover image. The reference image is used for auxiliary encoding process and will not be directly used for hiding data [12]. This method divides the reference image into multiple blocks, assigns an n-bit code to each block, and then matches or adjusts the information that has been converted into binary values with the blocks of the reference image. After that, the LSB method will be used to hide the message which has matched the blocks to the cover image [13]. Finally, it encrypts using public-private key encryption technology. It will send the two images to the receiver, and the receiver will use both of them to get the data. Its PNSR is greater than 62 dB which confirmed by experiment. What's more, it shows little changes between the cover image and stego image, and between basic reference image and the embedded reference image in the histograms.

DOI: 10.54254/2755-2721/94/2024MELB0058

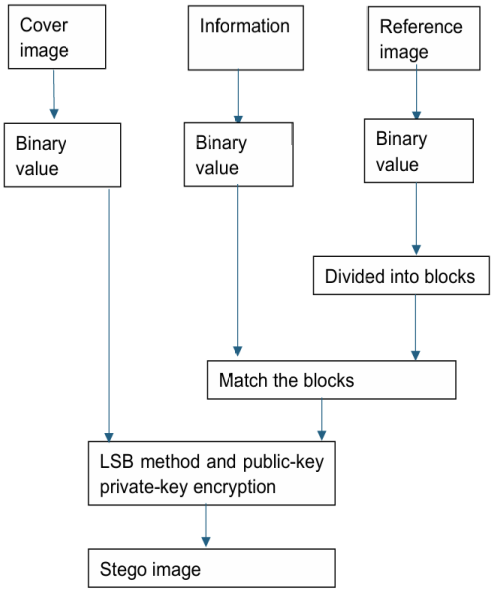

Figure 13. Steganography using LSB and reference image (Photo credit: Original).

As show in the table 2. Here is an overview of these methods from the fourth section.

Table 2. Overview of the LSB-based methods.

Method	Feature	PNSR	Other advantage
[14]	Using XOR operation and LSB method	256*256 size: 64.977 dB 512*512 size: 70.92 dB	Both sizes can hide 1,024 bytes
[15]	Using XOR operation, PRNG and LSB method	The same as the original LSB method	Improve the security
[16]	Using double XOR operation and LSB method	256*256–1,024*1,024 (hiding 200-1000 byte) size: 33.95 dB - 55.67 dB	Improve the capacity
[17]	Using PVD method, Logistic map and 3LSBs method	512*512 size: 38.7925 dB	A safe way to hide information
[18]	Using PVD method and LSB method in the same pixels at the same time	32.61 dB	Embedding capacity: 1,052,641 bits
[19]	Using adaptive PVD method and LSB method in the same pixels at the same time	34.08 dB	Embedding capacity:1,191,865
[20]	Using Recamán's sequence, cryptography and LSB method	512*512 size by using DSE cryptographic method: 62.86 dB	Embedding capacity: 53000 characters (512*512 size)
[21]	Using AES, base64 algorithm and LSB method	Higher than 53 dB	The quality of stego image is good in histogram analysis
[22]	Using reference image, cover image and LSB method	Higher than 62 dB	The quality of stego image and reference image are good in histogram analysis

DOI: 10.54254/2755-2721/94/2024MELB0058

5. Relevant Applications

The internet is mostly used by the medical industries to facilitate the remote exchange of digital medical information between clinics and hospitals as well as to offer e-health services to patients. Medical record access facilitates successful remote diagnosis and allows many clinicians to share patient data. To provide a safe way to sent and receive information, the LSB-based method is a good choose.

Numerous e-Government initiatives are effectively meeting the demand for communication. Steganography algorithms are popular and easier to use techniques that shield uniqueness by preventing unwanted parties from accessing shared materials. In article, it used PVD and LSB-based to assure security.

People more and more use the network devices to save privacy information, so the could storge is becoming important in our life. To increase the security of cloud services, the zero-trust (ZT) concept was recently put out. The LSB-based method shows huge ability in ZT cloud in study.

6. Conclusion

This article has provided a comprehensive analysis and summary of recent advancements in LSB-based image steganography techniques by examining a wide array of methodologies, including XOR operation-based, PVD-based, cryptography-based, and those utilizing reference images and image segmentation. Through meticulous evaluation based on criteria such as PSNR, histogram integrity, and embedding capacity, it has been determined that while these methods demonstrate notable improvements over traditional LSB techniques in various aspects, they also present distinct limitations that warrant further enhancement.

Future Research Directions: Looking ahead, there are several promising avenues for advancing LSB steganography. Firstly, integrating LSB techniques with evolving cryptographic methods presents a viable strategy for enhancing the security and robustness of steganographic systems. As cryptographic technologies continue to advance, their incorporation into LSB steganography could yield more secure and efficient methods capable of withstanding emerging security threats. Additionally, given the predominant focus on 2D images, expanding the application of LSB steganography to include 3D images represents a significant opportunity for broadening the utility and applicability of this technology. Furthermore, in response to the increasing sophistication of steganalysis tools, enhancing the resistance of LSB methods against steganalysis should be prioritized to maintain the confidentiality and integrity of hidden information. These suggested directions not only aim to fortify the effectiveness of LSB steganography but also seek to ensure its relevance in the rapidly evolving landscape of digital security.

References

[1] Doshi R, Jain P, Gupta L 2012 Steganography and its applications in security International Journal of Modern Engineering Research (IJMER) 2(6) 4634–4638

[2] Nisha C D, Monoth T 2020 Analysis of spatial domain image steganography based on pixel-value differencing method Soft Computing for Problem Solving: SocProS 2018 Volume 2 ed Springer Singapore pp 385–397

[3] Simmons G J 1984 The prisoners' problem and the subliminal channel Advances in Cryptology: Proceedings of Crypto 83 ed Springer US pp 51–67

[4] Alhomoud A M 2021 Image steganography in spatial domain: Current status, techniques, and trends Intelligent Automation & Soft Computing 27(1)

[5] Ley M 2002 The DBLP computer science bibliography: Evolution, research issues, perspectives International symposium on string processing and information retrieval ed Springer Berlin Heidelberg pp 1–10

[6] Maji G, Mandal S, Sen S, Debnath N C 2018 Dual image based LSB steganography 2018 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom) ed IEEE pp 61–66

[7] Zhu X, Huang Y, Wang X, Wang R 2023 Emotion recognition based on brain-like multimodal hierarchical perception Multimedia Tools and Applications 1-19

DOI: 10.54254/2755-2721/94/2024MELB0058

[8] Singh A K, Singh J, Singh H V 2015 Steganography in images using LSB technique International Journal of Latest Trends in Engineering and Technology (IJLTET) 5(1) 426–430
[9] Bandekar P P, Suguna G C 2018 LSB based text and image steganography using AES algorithm 2018 3rd International Conference on Communication and Electronics Systems (ICCES) ed IEEE pp 782–788
[10] Bhuiyan T, Sarower A H, Karim R, Hassan M 2019 An image steganography algorithm using LSB replacement through XOR substitution 2019 International Conference on Information and Communications Technology (ICOIACT) ed IEEE pp 44–49
[11] Zhu X, Guo C, Feng H, Huang Y, Feng Y, Wang X, Wang R 2024 A Review of Key Technologies for Emotion Analysis Using Multimodal Information Cognitive Computation 1-27
[12] Ahmed A, Ahmed A 2020 A secure image steganography using LSB and double XOR operations International Journal of Computer Science and Network Security 20(5) 139–144
[13] Prasad S, Pal A K 2019 Logistic map-based image steganography scheme using combined LSB and PVD for security enhancement Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2018 Volume 3 ed Springer Singapore pp 203–214
[14] Jung K H 2018 Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane Journal of Real-Time Image Processing 14 127–136
[15] Singh S 2020 Adaptive PVD and LSB based high capacity data hiding scheme Multimedia Tools and Applications 79 18815–18837
[16] Farrag S, Alexan W 2019 Secure 2d image steganography using recamán's sequence 2019 International Conference on Advanced Communication Technologies and Networking (CommNet) ed IEEE pp 1–6
[17] Anwar F, Rachmawanto E H, Sari C A 2019 StegoCrypt scheme using LSB-AES base64 2019 International Conference on Information and Communications Technology (ICOIACT) ed IEEE pp 85–90
[18] Ogundokun R O, Abikoye O C 2021 A safe and secured medical textual information using an improved LSB image steganography International Journal of Digital Multimedia Broadcasting 2021(1) 8827055
[19] Halder T, Karforma S, Mandal R 2019 A block-based adaptive data hiding approach using pixel value difference and LSB substitution to secure e-governance documents Journal of Information Processing Systems 15(2) 261–270
[20] Wang R, Zhu J, Wang S, Wang T, Huang J, Zhu X 2024 Multi-modal emotion recognition using tensor decomposition fusion and self-supervised multi-tasking International Journal of Multimedia Information Retrieval 13(4) 39
[21] Subramanian N, Elharrouss O, Al-Maadeed S, Bouridane A 2021 Image steganography: A review of the recent advances IEEE Access 9 23409–23423
[22] Muhammad K, Sajjad M, Mehmood I, Rho S, Baik S W 2016 A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image Multimedia Tools and Applications 75 14867–14893