Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications

Journal homepage:
https://akademiabaru.com/submit/index.php/arca/index
ISSN: 2462-1927



Application of the Canny Filter in Digital Steganography

Alaa Jabbar Qasim Almaliki[1], Sajad Muhil Abd[2], Inam Abdullah Lafta[3], Roshidi Din[1,*], Osman Ghazali[1], Jabbar Qasim Almalik[4], Sunariya Utama[1]

[1] School of Computing, Universiti Utara Malaysia (UUM), Sintok, Kedah Darul Aman, Malaysia
[2] AL-Muthanna University, AL-Muthanna, Iraq
[3] Middle Technical University, Institute of Technology, ICT Department, Baghdad, Iraq
[4] Ashur University, Department of Medical Instrumentation Technique Engineering College, Baghdad, Iraq

ARTICLE INFO

Article history:
Received 16 January 2024
Received in revised form 20 March 2024
Accepted 19 April 2024
Available online 17 May 2024

Keywords:
Steganography; Visual Perceptibility; Canny Filter; LSB Substitution

ABSTRACT

Substitution methods, LSB variants used in steganography on bitmap images, increase their effectiveness as the carrier images becomes noisier, that is, images with strong color variations between adjacent pixels reduce the human visual perceptibility threshold for detecting alterations. Sensitive information can thus be hidden with significantly greater efficacy and efficiency (in terms of perceptibility and quantity). Precisely for such effects, in a work on steganography prior to this, the necessary and used witness carriers were classified into four groups, according to their noise level, obtaining what was called Image Category [1]. However, quantifying such a property in an image with reasonable certainty, through analysis methods, turns out to be a costly task, requiring support tools, steganographic emulations, perceptibility measurements, previous experience, etc. In the context of the current R&D work on steganography, it was possible to similarly categorize any image, but without human intervention. This paper explains how this process was systematized, detecting noise level intervals that were assigned to the Image Category, which was done using Canny filters and subsequent weighting of the obtained image. Such a proposal brings a significant advantage when implementing substitution-based steganography systems.

1. Introduction

As is well known, digital steganography involves studying, researching, analyzing [1,2], and implementing techniques that allow the hiding of information or software objects in other objects, called carriers, with the aim of being sent from a sender to a receiver, to achieve covert transmission. The basic idea is to send sensitive or secret information embedded in an innocently appearing carrier, which goes unnoticed along with the act of transmission itself. Currently, there are other goals and purposes in the application of steganography, which do not necessarily imply "covert communication"; however, this, along with the storage of hidden information, is one of the major

* *Corresponding author.*
E-mail address: roshidi@uum.edu.my

https://doi.org/10.37934/arca.35.1.2130

application areas and is the focus of this work. However, what is strictly necessary for the understanding of the work itself, representing a significant automated improvement directly applicable to steganography aimed at covert communication (and/or storage), will be mentioned. Preferred carriers derive from the effectiveness of techniques that exploit the limitations of human senses (sight and hearing), immediately suggesting that the most suitable files are multimedia types: images, audio, and video; although they are not exclusive, it depends on the technique applied [3-5]. Among them, this work focuses on the use of bitmap image carriers in 24-bit BMP format. In summary, an carrier image can be used to hide any message or software object (file) from the view of intruders, encoding it as subtle changes in the colors of the pixels (their RGB components) that the human eye should not perceive; in such a way that the message embedded in the carrier, called a stego-carrier, can be transmitted to a human target without being detected; to then apply the reverse process (decoding) so that the receiver can recover and use the sent message. Other steganographic methods take advantage of the inability of software applications to detect the presence of foreign objects (files) "inserted" in carriers [6]. Such methods, while they can use any carrier image (including executables), have weaknesses that put them at a significant disadvantage compared to substitution techniques. Figure 1 shows a general scheme of the steganography system.

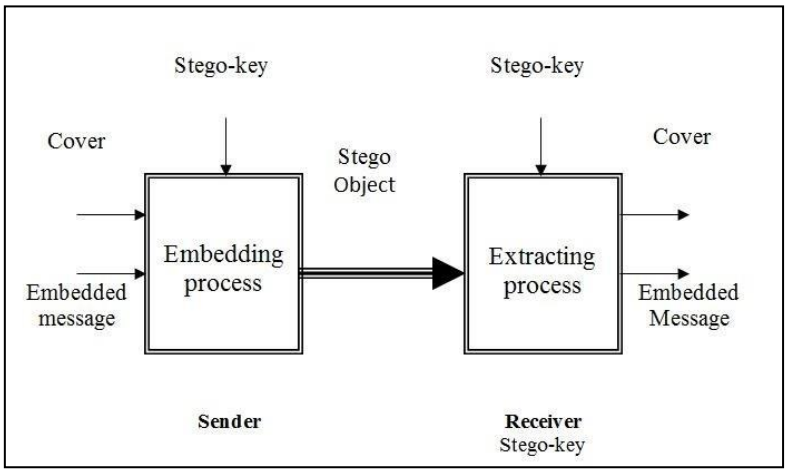


Fig. 1. General model of a digital steganography system

2. Substitution Methods on Images

Substitution methods in the realm of image steganography present an intriguing technique for concealing information within multimedia files. This approach leverages the inherent characteristics of digital images, where certain data regions are deemed "less significant" or "less perceptible to the senses." Such areas offer the perfect canvas for embedding hidden messages without altering the perceptible qualities of the image to the naked eye. The essence of this technique lies in manipulating the least significant bits (LSBs) of the color component bytes within an image. By substituting these LSBs with bits from the message intended to be concealed, information can be seamlessly integrated into the carrier image, thus maintaining its original appearance to casual observers [1-5].

The least significant bit substitution method, particularly the 1-bit technique [6-12], stands out for its simplicity and effectiveness. It operates on the principle that changing the least significant bit of a pixel's color value—be it red, green, or blue—will result in minimal visual alteration. Since these bits have the least impact on the color's intensity, the modifications are virtually undetectable to the human eye, especially when the carrier image is not a monochrome or single-color image. This

subtlety allows the embedded message to remain hidden within the visual noise of the image's color variations [12-14].

However, this method is not without its limitations. The capacity of the information that can be concealed is directly proportional to the number of bits used from each pixel's color value for embedding. In the case of the 1-bit LSB technique, only up to 12.5% of the image's data can be allocated for the hidden message. This constraint has spurred the development of advanced variants of the LSB method, which utilize more than one bit per color component, effectively increasing the embedding capacity. For instance, employing two least significant bits doubles the storage space for the hidden message to 25%, albeit at the risk of making the alterations slightly more perceptible under scrutiny or with the aid of digital tools designed to detect such changes.

The perceptibility of these modifications is a critical factor in steganography. It has been the subject of extensive research, leading to the identification of four acceptable levels of perceptibility based on the degree of bit substitution and the category of the image. As the research suggests, using more than one least significant bit for embedding purposes escalates the perceptibility but remains within acceptable limits, provided no sophisticated detection tools are employed. This balance between concealment capacity and perceptibility underscores the nuanced trade-offs inherent in steganographic practices.

The effectiveness of steganography is significantly influenced by the characteristics of the carrier image. Images with high levels of visual noise, characterized by abrupt color changes between adjacent pixels, offer the most effective cover for embedding messages. The "noisier" the image, the more effectively it can mask the steganographic alterations, making detection more challenging. Conversely, images with uniform color zones or those that are monochromatic are less suited for this purpose, as any modifications are more likely to stand out, rendering the concealed information more detectable.

Substitution methods employed in image steganography highlight a fascinating interplay between data concealment techniques and the perceptual limitations of human vision. By judiciously manipulating the digital fabric of images, steganography enables the covert transmission of information, secured not by encryption alone but by blending imperceptibly into the visual noise of everyday digital media. This field continues to evolve, with ongoing research aimed at enhancing the capacity for concealed messages while minimizing the risk of detection, thus broadening the scope and efficacy of steganographic practices in the digital age [15-25].

3. Carrier Image Categorization

A methodical and controlled empirical process was carried out on numerous images, using support tools, steganographic emulations using numerous LSB variants, measuring perceptibility, and with prior experience. Four witness images were selected, defining for them, with quite certainty, four Categories, respectively, classified by their noise level. Now arises the need to carry out a process with analogous results to the previous one, but in a systematic way, so that it can be applicable to any carrier, but without human intervention [26].

4. Systematized Categorization

The intricate process of detecting discontinuities such as points, lines, and edges in digital images is a foundational aspect of image processing and analysis. This task, predominantly centered around edge detection, serves as a crucial step in various applications, from computer vision to digital image enhancement and steganography. MATLAB© Toolbox emerges as a powerful suite offering

specialized functions for edge detection, including the notable "edge" function. This function is engineered to transform grayscale images into binary images that starkly highlight the edges or discontinuities present, thereby converting subtle gradients into distinct boundaries that are easier to analyze or manipulate.

Edge detection is a fundamental technique in the field of image processing and computer vision, serving as a crucial step in understanding the geometric and spatial structures within digital images. It plays a vital role in various applications, including object detection, image segmentation, pattern recognition, and machine vision systems. The essence of edge detection lies in its ability to identify significant transitions in gray levels across adjacent pixels. These transitions often mark the boundaries of objects, distinguishing them from the background or other objects within the image. By detecting these edges, algorithms can infer the presence, shape, and position of objects in an image, which is essential for further analysis or processing.

MATLAB, a high-level language, and interactive environment used for numerical computation, visualization, and programming, offers robust tools for edge detection through its Image Processing Toolbox. Among these tools, the "edge" function is particularly noteworthy for its versatility and efficiency in highlighting the contours of objects in a digital image. This function transforms a grayscale input image into a binary image that represents the detected edges, where the edges are indicated by white pixels (ones) on a black background (zeros).

The MATLAB edge function supports six different edge detection methods, each with unique algorithms and suited for various types of images and analysis needs:

- Sobel Method: This method employs a pair of 3x3 convolution kernels to estimate the gradient magnitude of the image at each pixel. The Sobel filter is particularly effective in highlighting horizontal and vertical edges, making it well-suited for images with clear, straight boundaries.
- Prewitt Method: Like the Sobel method, the Prewitt method uses convolution kernels to compute the image gradient. However, it applies different weights, offering a slight variation in edge detection sensitivity. This method is advantageous for detecting edges in images with softer transitions.
- Roberts Method: The Roberts cross operator utilizes a pair of 2x2 convolution kernels to calculate a simple, quick estimate of the gradient. It is highly sensitive to diagonal edges but less so to horizontal or vertical lines, making it suitable for images with prominent diagonal features.
- Laplacian Method: This method involves a second-order derivative approach, detecting areas where the gradient of the image intensity changes rapidly. It is isotropic, meaning it treats all directions equally, and is effective for highlighting fine detail in images.
- Zero-cross Method: Based on the Laplacian of Gaussian filter, this method identifies edges by looking for zero crossings after filtering the image with a Laplacian operator. It is particularly useful for images where the background and objects have varying levels of brightness.
- Canny Method: Developed by John F. Canny, this technique is designed to be an optimal edge detector. It uses a multi-stage algorithm to detect a wide range of edges in images. The Canny method is renowned for its ability to minimize error rates, accurately detect true edges, and precisely localize edge points. It achieves this through Gaussian filtering, gradient calculation, non-maximum suppression, and hysteresis thresholding.

Each of these methods has its advantages and is selected based on the specific requirements of the image analysis task at hand. For example, the Canny method is widely used for its robustness and accuracy in edge detection across various applications, while the Sobel and Prewitt methods are preferred for their simplicity and effectiveness in specific scenarios.

In the context of image processing and computer vision, understanding and choosing the appropriate edge detection filter is crucial. It can significantly impact the outcome of the subsequent analysis, whether it's for object recognition, image segmentation, or enhancing the features of an image for better visualization. As such, MATLAB's edge function and its array of filters provide a powerful toolkit for researchers, developers, and practitioners in the field to harness the full potential of edge detection in their work.

The application of these filters not only aids in the visualization of image structures but also plays a significant role in the field of steganography, particularly in the selection of substitution methods for embedding hidden information. By analyzing the edge details and overall noise pattern of a carrier image, researchers can determine the most suitable steganographic technique to use, aiming for optimal concealment while minimizing the risk of detection. This process involves quantifying the results obtained from the edge detection filters, establishing a correlation with predefined image models or categories 1, 2, 3, and 4. Such quantification is typically achieved by calculating the ratio of edge pixels to the total image size, which essentially measures the density of discontinuities or the "noise" level in the image.

The significance of edge detection extends beyond mere image analysis to the realm of Computer Security, particularly in enhancing the efficacy and efficiency of steganographic methods. By accurately categorizing the carrier image based on its edge characteristics and noise levels [4]., it becomes feasible to tailor the steganographic approach to ensure that hidden information is both effectively concealed and resilient to stegoanalysis attacks. This adaptability is crucial for maintaining the secrecy and integrity of the embedded data, especially in scenarios where the detection of such information could have adverse implications [26-31].

The ongoing research and development in this domain are aimed at designing sophisticated algorithms that leverage edge detection results to improve the application of substitution steganographic techniques. This innovative work seeks to refine the process of embedding information within digital images, striving for a balance between perceptibility, the quantity of hidden data, and robustness against detection methods. By incorporating advanced image processing techniques, such as edge detection [19], into the development of steganographic algorithms, researchers are paving the way for more secure and efficient methods of information concealment.

Edge detection serves as a cornerstone in both image processing and steganography, enabling the detailed analysis of digital images and informing the selection of optimal methods for data embedding. The meticulous study of edges and discontinuities not only enhances our understanding of image content and structure but also significantly contributes to the advancement of secure communication practices within the field of Computer Security. Through the integration of edge detection algorithms and steganographic techniques, the research community continues to explore innovative solutions that promise greater efficacy in hiding and protecting sensitive information in an increasingly digital world.

Table 1
Normalized sums for each witness carrier using the Canny filter

Carrier	Cat.	Weighting
Dhay.bmp	1	0.0633
Kia.bmp	2	0.0788
Horse.bmp	3	0.1220
Uum.bmp	4	0.1566

Based on the above, it is concluded that the indicated edge filter using the Canny algorithm is to implement the categorization of carrier images. Table 1 appears to present the results of an edge detection process performed on four different digital images, referred to as "witness carriers," using the Canny edge detection filter. The table is broken down into three columns: Carrier, Category (Cat.), and Weighting.

- **Carrier:** This column lists the filenames of the bitmap images (.bmp) that were analyzed. Each filename presumably corresponds to a unique image.
- **Category (Cat.):** This column classifies each image into a category numbered from 1 to 4. These categories could represent different types of images or levels of complexity in terms of their content and texture. For instance, Category 1 could be simpler images with fewer edges, and Category 4 could be complex images with many edges.
- **Weighting:** This column presents the normalized sum calculated for each image after applying the Canny filter. The normalized sum is a quantitative measure of the edges detected by the filter. It is normalized because it likely represents the ratio of edge pixels to the total number of pixels in the image, thus allowing for comparison between images of different sizes.

The data shows a progressive increase in the weighting from Category 1 to Category 4. This suggests that the complexity or the number of detectable edges in the images increases with the category number. The image Dhay.bmp, in Category 1, has the lowest weighting at 0.0633, indicating it might have fewer or less pronounced edges. In contrast, Uum.bmp, in Category 4, has the highest weighting at 0.1566, suggesting it has many or very pronounced edges.

This table could be part of a steganographic analysis where the edge detail of potential carrier images is being assessed to determine their suitability for hiding information. Images with higher weightings (more edges) might be better carriers for steganographic purposes because the additional detail can help disguise the alterations made to embed secret information. The goal would be to select an image with enough complexity to conceal a message but not so much that the message becomes difficult to retrieve or the image arouses suspicion.

In Figure 2 showcases a comparative display of four distinct images categorized by complexity and their corresponding edge-detected versions processed by the Canny filter. Each row represents a different category, with the original image on the left and its edge detection result on the right. Starting with "Dhay.bmp" in Category 1, the original image depicts a child with a simple background. The Canny filter output shows minimal edges, indicating lower complexity and noise levels, in line with Category 1's characteristics. Moving to "Kia.bmp" in Category 2, the original image of a vehicle with moderate background detail yields a higher edge count, signifying a slight increase in complexity, as expected for images in this category. The third row, "Horse.bmp" under Category 3, displays a dynamic image of a horse. The resulting edge detection reveals a substantial number of edges, reflecting the increased complexity and the higher noise potential, making it suitable for Category 3. Finally, "Uum.bmp" falls into Category 4 and shows a scenery image with a complex structure. The Canny filter output presents a dense web of edges, indicating a high level of detail and noise, thus fitting into the most complex category.

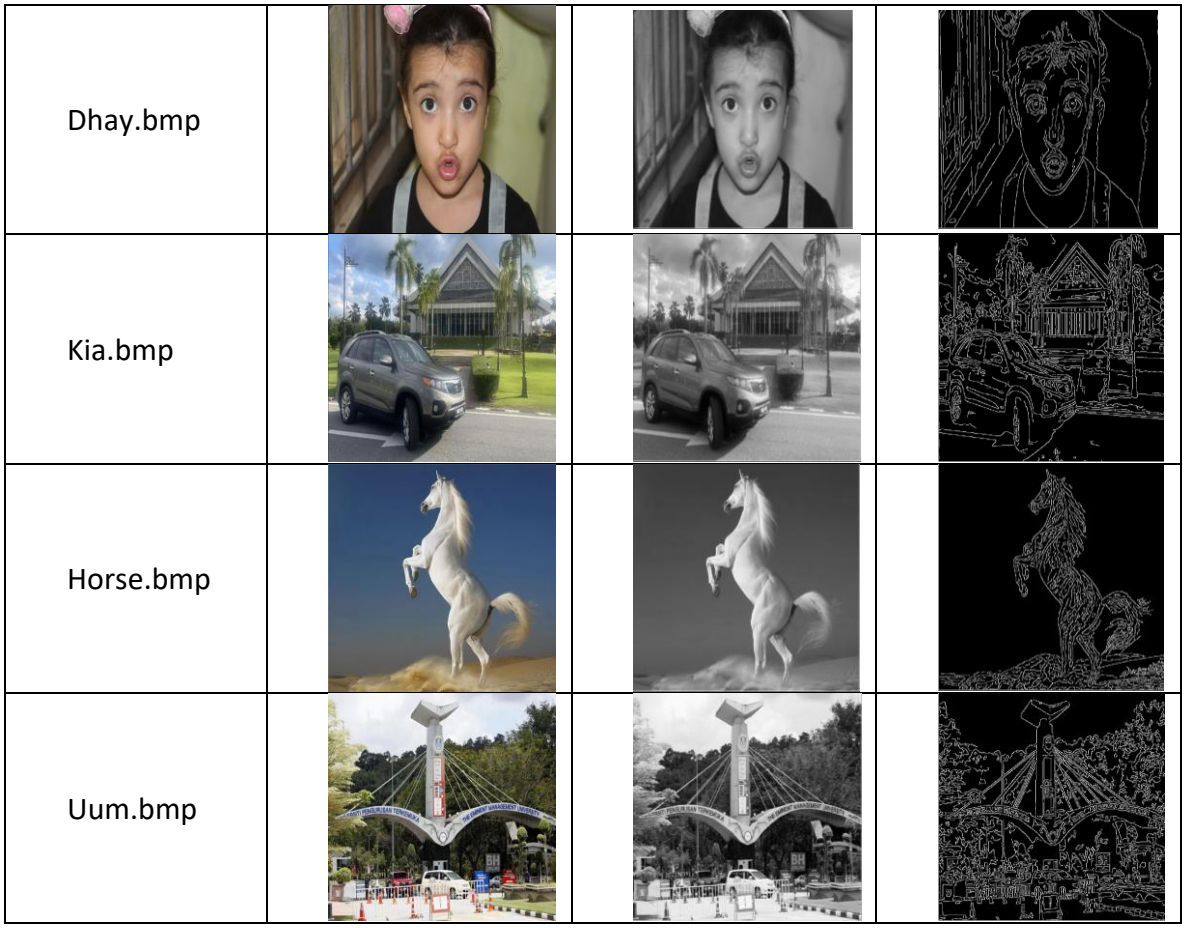


Fig. 2. Witness carriers, Cat. 1,2,3,4; to the right their result after the Canny filter

This visual representation aids in understanding how the Canny filter highlights the structural complexity of images, which is crucial for applications like image processing, computer vision, and particularly steganography, where choosing an appropriately complex carrier image can enhance the concealment of information.

5. Determination of Category Ranges

The ranges of values that allow the automatic categorization of an image, after having applied the Canny filter and weighting, were determined. These ranges were determined through various tests with pattern or witness images, and then the process was tested with others to verify its efficacy, obtaining very satisfactory results. The obtained ranges are representative and proportional to the number of edges or the amount of noise in each image [32-36].

Table 2
Ranges to determine categories.

Category	Ranges
Cat.1	Less than 0.075
Cat.2	0.075 - 0.099
Cat.3	0.1 - 0.125
Cat.4	Greater than 0.12

Table 2 displays the categorization ranges for images based on their edge density, which is calculated after applying the Canny edge detection filter. The table presents four distinct categories (Cat.1 through Cat.4) with corresponding edge density ranges. These ranges are determined through a process of testing with pattern or witness images. The Canny filter is known for its effectiveness in identifying true edges, due to its use of Gaussian filtering to reduce noise, calculation of the intensity gradients, and application of double thresholding to determine potential edges.

- Category 1 includes images with the least number of edges or noise, denoted by a normalized weighting less than 0.075. These images are likely to have fewer details and less complex structures. Consequently, they might not be ideal for certain image processing applications that rely on clear edge information, such as object recognition.
- Category 2 consists of images with a slightly higher degree of edge detail, with normalized weightings between 0.075 and 0.099. These images might have more texture or detail compared to Category 1 but still maintain a relatively low level of complexity.
- Category 3 is for images with normalized weightings from 0.1 to 0.125, indicating a moderate level of edge detail. These images are likely to have more complex features and could be better suited for more advanced image processing tasks that require distinct edge information.
- Category 4 captures images with the highest amount of edge detail, having a normalized weighting greater than 0.12. Images in this category are characterized by high levels of detail and noise, making them potentially the most suitable for steganography and other applications that benefit from a high density of edges.

By establishing these ranges, the table provides a systematic approach to image categorization based on edge density. This categorization can be particularly useful in fields like steganography, where the effectiveness of data concealment can depend on the amount of detail or noise within the carrier image. The higher the category, the more likely the image is to successfully hide additional data within its structure without detection. Images with higher edge density can obscure the alterations made by steganographic processes, thereby providing better cover for hidden information.

6. Conclusion

The article concludes that the application of the Canny filter for categorizing carrier images in digital steganography presents a significant advancement. This method allows for the automatic classification of images based on noise levels, optimizing the selection of substitution methods for embedding secret information. Through empirical testing and algorithm development, the research demonstrates the effectiveness of this approach, offering a systematic way to enhance data concealment techniques.

References

[1] Chan, Chi-Kwong, and Lee-Ming Cheng. "Hiding data in images by simple LSB substitution." *Pattern recognition* 37, no. 3 (2004): 469-474. https://doi.org/10.1016/j.patcog.2003.08.007

[2] Liao, Xin, Qiao-yan Wen, and Jie Zhang. "A steganographic method for digital images with four-pixel differencing and modified LSB substitution." *Journal of visual communication and image representation* 22, no. 1 (2011): 1-8. https://doi.org/10.1016/j.jvcir.2010.08.007

[3] Patidar, Vinod, N. K. Pareek, G. Purohit, and K. K. Sud. "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption." *Optics communications* 284, no. 19 (2011): 4331-4339. https://doi.org/10.1016/j.optcom.2011.05.028

[4] Swain, Gandharba. "Digital image steganography using nine-pixel differencing and modified LSB substitution." *Indian Journal of Science and Technology* (2014): 1444-1450. https://doi.org/10.17485/ijst/2014/v7i9.27

[5] Jung, Ki-Hyun, and Kee-Young Yoo. "Steganographic method based on interpolation and LSB substitution of digital images." *Multimedia Tools and Applications* 74 (2015): 2143-2155. https://doi.org/10.1007/s11042-013-1832-y

[6] Fridrich, Jiri, and Meng Long. "Steganalysis of LSB encoding in color images." In *2000 IEEE International Conference on Multimedia and Expo. ICME2000. Proceedings. Latest Advances in the Fast Changing World of Multimedia (Cat. No. 00TH8532)*, vol. 3, pp. 1279-1282. IEEE, 2000..

[7] Fridrich, Jessica, Miroslav Goljan, and Rui Du. "Reliable detection of LSB steganography in color and grayscale images." In *Proceedings of the 2001 workshop on Multimedia and security: new challenges*, pp. 27-30. 2001. https://doi.org/10.1145/1232454.1232466

[8] Dumitrescu, Sorina, Xiaolin Wu, and Nasir Memon. "On steganalysis of random LSB embedding in continuous-tone images." In *Proceedings. International conference on image processing*, vol. 3, pp. 641-644. IEEE, 2002.

[9] Dumitrescu, Sorina, Xiaolin Wu, and Zhe Wang. "Detection of LSB steganography via sample pair analysis." In *Information Hiding: 5th International Workshop, IH 2002 Noordwijkerhout, The Netherlands, October 7-9, 2002 Revised Papers 5*, pp. 355-372. Springer Berlin Heidelberg, 2003. https://doi.org/10.1007/3-540-36415-3_23

[10] Mielikainen, Jarno. "LSB matching revisited." *IEEE signal processing letters* 13, no. 5 (2006): 285-287. https://doi.org/10.1109/LSP.2006.870357

[11] Laskar, Shamim Ahmed, and Kattamanchi Hemachandran. "High Capacity data hiding using LSB Steganography and Encryption." *International Journal of Database Management Systems* 4, no. 6 (2012): 57. https://doi.org/10.5121/ijdms.2012.4605

[12] Khudher, Israa Mohammed. "LSB steganography strengthen footprint biometric template." *Восточно-Европейский журнал передовых технологий* 1, no. 9-109 (2021): 58-65. https://doi.org/10.15587/1729-4061.2021.225371

[13] Rasmi, A., and M. Mohanapriya. "HIGH DATA EMBEDDING USING LSB AND PIXEL INTENSITY BASED METHODS." *International Journal of Advanced Research in Computer Science* 8, no. 7 (2017).

[14] Abikoye, Oluwakemi Christiana, and Roseline Oluwaseun Ogundokun. "Efficiency of LSB steganography on medical information." *International Journal of Electrical and Computer Engineering (IJECE)* 11, no. 5 (2021): 4157-4164. https://doi.org/10.11591/ijece.v11i5.pp4157-4164

[15] Hamming, R.W., Coding and Information Theory. Prentice-Hall Englewood Cliffs. 1980.

[16] Roth, Mark A., and Scott J. Van Horn. "Database compression." *ACM sigmod record* 22, no. 3 (1993): 31-39. https://doi.org/10.1145/163090.163096

[17] Bender, Walter, Daniel Gruhl, Norishige Morimoto, and Anthony Lu. "Techniques for data hiding." *IBM systems journal* 35, no. 3.4 (1996): 313-336.

[18] Swanson, Mitchell D., Bin Zhu, and Ahmed H. Tewfik. "Robust data hiding for images." In *1996 IEEE Digital Signal Processing Workshop Proceedings*, pp. 37-40. IEEE, 1996.

[19] Marvel, Lisa M., Charles G. Boncelet, and Charles T. Retter. "Spread spectrum image steganography." *IEEE Transactions on image processing* 8, no. 8 (1999): 1075-1083. https://doi.org/10.1109/83.777088

[20] Petitcolas, Fabien AP, Ross J. Anderson, and Markus G. Kuhn. "Information hiding-a survey." *Proceedings of the IEEE* 87, no. 7 (1999): 1062-1078. https://doi.org/10.1109/5.771065

[21] Chandramouli, Rajarathnam, and Nasir Memon. "Analysis of LSB based image steganography techniques." In *Proceedings 2001 international conference on image processing (Cat. No. 01CH37205)*, vol. 3, pp. 1019-1022. IEEE, 2001.

[22] Cvejic, Nedeljko, and Tapio Seppanen. "Increasing robustness of LSB audio steganography using a novel embedding method." In *International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004.*, vol. 2, pp. 533-537. IEEE, 2004. https://doi.org/10.1109/ITCC.2004.1286709

[23] Tseng, Hsien-Wen, and Chin-Chen Chang. "High Capacity Data Hiding in JPEG-Compressed Images." *Informatica* 15, no. 1 (2004): 127-142. https://doi.org/10.15388/Informatica.2004.050
[24] Ker, Andrew D. "Steganalysis of LSB matching in grayscale images." *IEEE signal processing letters* 12, no. 6 (2005): 441-444. https://doi.org/10.1109/LSP.2005.847889
[25] Li, Xin, Louis J. Kerofsky, and Kristine Elizabeth Matthews. "Scalable layered coding in a multi-layer, compound-image data transmission system." U.S. Patent 6,898,313, issued May 24, 2005.
[26] Qasim, Alaa Jabbar, and Farah Qasim Ahmed Alyousuf. "History of image digital formats using in information technology." *QALAAI ZANIST JOURNAL* 6, no. 2 (2021): 1098-1112. https://doi.org/10.25212/lfu.qzj.6.2.41
[27] Din, Roshidi, Rosmadi Bakar, Sunariya Utama, Jamaluddin Jasmis, and Shamsul Jamel Elias. "The evaluation performance of letter-based technique on text steganography system." *Bulletin of Electrical Engineering and Informatics* 8, no. 1 (2019): 291-297. https://doi.org/10.11591/eei.v8i1.1440
[28] Din, Roshidi, Massudi Mahmuddin, and Alaa Jabbar Qasim. "Review on steganography methods in multi-media domain." *International Journal of Engineering & Technology* 8, no. 1.7 (2019): 288-292.
[29] Alyousuf, Farah Qasim Ahmed, Roshidi Din, and Alaa Jabbar Qasim. "Analysis review on spatial and transform domain technique in digital steganography." *Bulletin of Electrical Engineering and Informatics* 9, no. 2 (2020): 573-581. https://doi.org/10.11591/eei.v9i2.2068
[30] Din, Roshidi, Alaa Jabbar Qasim, Shapina Abdullah, and Shamsul Jamel Elias. "Analysis Review on Image Compression Domain." *International Journal of Engineering & Technology* 8, no. 1.7 (2019): 293-296.
[31] Qasim, Alaa Jabbar, Roshidi Din, and Farah Qasim Ahmed Alyousuf. "Review on techniques and file formats of image compression." *Bulletin of Electrical Engineering and Informatics* 9, no. 2 (2020): 602-610. https://doi.org/10.11591/eei.v9i2.2085
[32] Din, Roshidi, and Alaa Jabbar Qasim. "Steganography analysis techniques applied to audio and image files." *Bulletin of Electrical Engineering and Informatics* 8, no. 4 (2019): 1297-1302. https://doi.org/10.11591/eei.v8i4.1626
[33] Din, Roshidi. "Comparative Analysis of Methods for Digital Steganography in Images." *Borneo International Journal eISSN 2636-9826* 6, no. 3 (2023): 119-127.
[34] Din, Roshidi. "Comparison Of Steganographic Techniques of Spatial Domain and Frequency Domain in Digital Images." *Borneo International Journal eISSN 2636-9826* 6, no. 3 (2023): 109-118.
[35] Utama, Sunariya, and Roshidi Din. "Performance Review of Feature-Based Method in Implementation Text Steganography Approach." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 28, no. 2 (2022): 325-333. https://doi.org/10.37934/araset.28.2.325333
[36] Din, Roshidi, and Sunariya Utama. "The Design Review of Feature-based Method in Embedding the Hidden Message in Text as the Implementation of Steganography." *Borneo International Journal eISSN 2636-9826* 6, no. 3 (2023): 88-95.