[1] Mr. Harshal V. Patil

[2] Dr. Vaibhav P. Sonaje

A Study of The Performance of Various Media for Information Security Via LSB Steganography Method for Text Messaging

Journal of Electrical Systems

Abstract: - The growing prevalence of online data sharing has brought forth a critical concern pertaining to information security. It is imperative to secure confidential data during internet communication. Steganography, which entails the scientific and artistic principles of disguising messages within various media such as images, audio, and video, has been widely employed as a means of safeguarding sensitive information from malicious actors. One widely-used method in LSB-based steganography for secure data transmission is highlighted in this paper. This study presents a thorough examination of different LSB-based steganography methods for embedding textual data into various media files, including images, audio, and video. The primary goal of this research is to evaluate the efficiency of these algorithms for different file sizes and media types, with a specific focus on criteria such as PSNR and MSE.

Keywords: Steganography, Cover-object, Stego-object, Stego-key, LSB, PSNR, MSE.

Introduction:

The importance of conveying sensitive information securely has been a topic of much discussion for several years. Confidential data are the lifeblood of any institution or organization, making security measures a top concern for firms that handle confidential information. The primary concern when selecting a communication security system is the level of safety it provides. Steganography, the art of secret communication, involves hiding information from unauthorized third parties[1].

Strategography is a tool that serves as an integral part of digital media files, allowing both producer and recipient to access and utilize relevant information. While cryptography aims to protect sensitive data, strategography takes this a step further by providing a means to conceal messages within that data, making it impervious to detection. However, unlike cryptography, strategography does not rely on any specific code or technique for encoding or decoding messages, allowing for greater flexibility and adaptability [2].

a) Basic Steganography Model:

The following Figure 1 illustrates a steganography model that encompasses a message intended to be concealed by the sender. This message may take on numerous formats; including plain text, images, audio files, or other file types. To remove the confidential message from the Stego-file, the receiver must possess a password known as a stego-key. The stego-file, or cover-file, encapsulates the secret information. Cover objects may take on a variety of media, including audio, video, and image files[3].

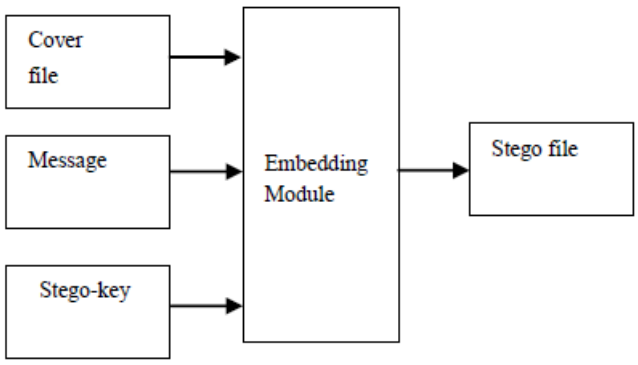

Figure.1 Basic Steganography Model

Basic terms for Steganography [5]

- **Cover Object/File:** The primary object or file to which the covert message will be attached.
- **Secret Data/Message:** These are the confidential details that need to be inserted into the cover object.
- **Stego Object/File:** The altered cover object that contains the hidden message.
- **Stego Key:** The term "Stego Key" refers to a confidential code or key that is essential for the successful encoding and decoding of information during communication between the sender and receiver.

[1] *Research Scholar, Sandip University Nashik India. Email: harshal4patil@gmail.com, ORCID - 0009-0004-3754-1027

[2] Department of Computer Science & Application, SOCSE, Sandip University, Nashik, India,
Email: vaibhav.sonaje@sandipuniversity.edu.in

Embedding Algorithm: This denotes to the method or technique used to cover the confidential information within the cover object.

b) Types of Steganography[5]:

- **Image steganography:** Image steganography is a method of concealing confidential messages within an image to produce a stego-image.
- **Audio steganography:** Unused bits in audio files can be utilized to embed hidden messages, as every file has unused bits or areas where a message can be concealed.
- **Video steganography:** Video steganography is a process that entails the separation of a video into its audio and image frames, with the information concealment occurring within the audio file.
- **Text steganography:** Text steganography involves embedding a message in a text file through formatting. This technique relies on line-shift, word-shift, and feature coding, but it is not robust as reformatting the text will destroy the concealed content.
- **Network steganography:** In network strategography, network protocols such as TCP, UDP, ICMP, and IP establish communication between entities through object-oriented programming. The OSI layer network model includes a hidden channel enabled when the strategy is implemented.

Literature Review:

In our scholarly endeavor, we conducted an extensive review of various steganography techniques by examining numerous research papers. These papers exhibit significant potential and possess a promising future scope. Through our comprehensive analysis, it became apparent that an overwhelming majority of steganography-related research has been conducted in recent years. For the current era, concepts like StegnoGraphy have been widely accepted based on the established principles of Least Significant Bit (LSB) from conventional devices.

Arora et al. [4] explored the fundamentals of the LSB International Journal of Safety and Security Engineering method for steganography, examining crucial aspects for instance the PSNR, MSE, and data-concealment capacity. Arora and his team [6] conducted a thorough examination and assessment of various methods for concealing information within images through steganography. This research presents a comparative examination of various image steganographic methods, taking into account crucial aspects such as high data capacity, continuous clearness, strength, temperature confrontation, and computational difficulty.

According to a study conducted by Emad[7], the Graphic Arts Society developed a strategic algorithm in collaboration with Graeskel and Color Images' intelligent web-based transform (IWT) tool to securely embed sensitive information within the LSBs of high-quality images. The purpose of this processing was to enhance the data's robustness and resistance to tampering. By leveraging advanced data protection capabilities provided by cutting-edge technology, the society aimed to achieve these objectives.

Ahmed A. and Ahmed A [8] have successfully implemented the encryption and steganography algorithm for a two-stage process, involving the Gupta cryptosystem and XOR binary operations. The resulting image is encrypted and adheres to the LSB steganography paradigm. The process of embedding encrypted bits within the image involves using the least significant bits of every pixel to create a hidden message that is not visible to the naked eye. However, this message remains intact and can be extracted and decrypted using appropriate algorithms.

Additionally, Danny Adiyan et al. explored the use of steganography with the Vigenère cipher and analyzed the relationship between image file size and the amount of information that can be inserted [9]. Their research provided a thorough examination of the Least Significant Bit substitution technique in steganography.

Marēla and others. [10] Human beings make use of coded messages for secure communication, and hence important messages need to be encrypted according to a key that has both mathematical and cryptographic significance. At the beginning, they tried to convey secret messages through a text character, thereby fulfilling the requirement of encryption. Subsequently, encrypted messages were sent in the form of encrypted codes. The sender ensured that the message was encrypted securely before being transmitted, and the encrypted message was decrypted and read by the recipient using LSB method.

According to Elharrouss et al. [11], the k-means clustering algorithm can be utilized to implement a secret image steganography technique that effectively safeguards the privacy of the hidden image. The authors exhibited that the k-means algorithm can be employed to encode the secret image without any loss of its original features. This was achieved by embedding the secret image within the cover image, resulting in a complete and unaltered secret image. To ensure the privacy of the hidden image, the authors gathered data from numerous regions and applied the k-means algorithm to analyze the data. The peak signal-to-noise ratio (PSNR) was employed as a measure of image quality. Although the proposed algorithm was anticipated to maintain the desired level of image quality, it did not fully meet the anticipated expectations.

Indrayani, Nugroho, and Hidayat [12] utilize a small number of bits to efficiently manipulate and quantize signals. Various algorithms have been proposed based on these visual concepts. To ensure the credibility of the validity of the bits, the differences and improvements in the audio signal quality were analyzed. Specifically, the importance of the LSB pattern, LSB + 1, LSB + 2, and LSB + 3 was emphasized. Evaluations are conducted using metrics such as resolution-based classification and synthesis capability, peak signal-to-noise ratio (PSNR), and bit error rate (BER). The results demonstrate superior quality, high-resolution synthesis capability, and significantly better PSNR values compared to other methods, particularly LSB + 3.

According to Datta and Bandyopadhyay [13], the use of Least Significant Bit (LSB) encoding poses a security risk to the sanitization process of data encryption, making it susceptible to hacking attacks. To address this issue, they developed a robust steganography tool called ELSB, which operates nonsequentially on nonsecret data and focuses on making the encryption process more resistant to attacks. The objective of this tool is to reduce the security vulnerabilities of LSB-based encryption and enhance the clearness of the data analysis by dividing the data into three levels of abstraction. In addition, they obtained a 7-bit "6-bit ASCII representative" to enhance the capabilities of the tool. In comparison, the proposed encoding method aims to maintain the integrity of the data during data analysis, requiring various loading methods for the objects and incorporating the steganography tool into the system's architecture to enhance its capacity.

Abdelsaatiri and Abushama [14] have proposed a novel strategy for auditory steganography, which utilizes the concept of a parity-check matrix to detect the presence of LSBs in a given audio signal, with the goal of hiding secret messages in the audio domain. The algorithm utilizes a modified algorithm and an audio steganography tool to quantize and analyze the results, providing an image of the LSBs in the proposed method. The authors emphasize that the method is based on individual sound recognition, as opposed to host-based audio signal processing, and thus it is not capable of detecting any sound.

According to Mandal et al[15], a novel audio steganography technique was devised that strengthened the security and invisibility of the LSB method by encoding message bits into the Least Significant Bit of stereo-audio samples with stego-keys. Marva Tareek and Vaseem[16] have implemented an audio steganography scheme using a private message with AES-128 encryption and an encrypted map-generated LSB-based approach to embed data into audio. They have used MSE, PSNR, waveform plots, and perceptual evaluations to measure the performance of the scheme. Dasgupta and colleagues[17] introduced the Hash-based LSB (HLSB) method for video steganography. This method separated the confidential data into three parts and embedded each part in the LSB of the RGB cover frames.

Bhole et al.[18] projected a method for hiding data using LSB and byte randomization that increases payload capacity by making blue pixels more visually appealing than red and green pixels. The HLSB method achieved a PSNR value between 42.66 and 45.67 dB, surpassing the traditional LSB method. According to Lou et al.[19], a strategic graph was developed during the jam session that employs a reversed histogram-transformation function, which is integrated into a regular-exponential (RS) and x2-detection function. This representation demonstrates the mathematical representation of the desired inverse function.

Zhang et al.[20] Unlike other embedding techniques, BCH encoding-based embedding is employed to transform data objects within the heterogeneous dataset. In this context, the embedding is designed to decrease the dimensionality of the input blocks and increase the quality of the data. The result is a private and confidential data representation that is effective in preserving sensitive information. Compared to other embedding techniques, this method exhibits superior act in terms of inserting size.

Algorithm Used:

Least Significant Bit (LSB):

The use of diverse means in the field of disseminating information has resulted in a significant decrease in the primacy of coding as a skill. In this context, the presence of secret messages encoded within each line of the representative binary string is an essential feature, as evidenced by its inclusion in the Cover-object file within each object in the sequence [21,22]

a. LSB Algorithm for Image Encoding and Decoding:

Encoding Algorithm:

1. Examine the cover image and decode the concealed text message.
2. Transform the text message into a binary format.
3. For each pixel in the cover-image, determine the Least Significant Bit.
4. Replace the Least Significant Bit of every pixel in the cover-image with the consistent bit from the secret-message.
5. Generate the resultant stego-image.

Decoding Algorithm:

1. Analyze the steganographic image.
2. Examine the Least Significant Bit for each pixel in the steganographic image.
3. Extract the bits and convert each 8-bit sequence into characters.
4. Generate a steganographic image to retrieve the original hidden text message.

b. LSB Algorithm for Audio Encoding and Decoding:

Encoding Algorithm:

1. The text to be embedded is inputted.
2. The text is converted into a binary format.
3. The WAV audio file is read as a cover file to determine the header and total count size.
4. The size of the message is determined. If the size of the message is larger than the count size, the message "message is too big" is displayed, and a smaller message is selected.
5. The audio sample is selected, and the key is hidden. The code of the text is then converted into the WAV file using the LSB algorithm.
6. The process is repeated until the entire message is embedded in the audio.

Decoding Algorithm:

1. The stego file, which contains the embedded audio, is read.
2. The LSB is extracted from the audio sample.
3. The key is retrieved from the audio samples, and if it matches, the hidden message is extracted; otherwise, the message "no message is hidden" is displayed.
4. All LSB position bits are stored in an array.
5. The array is arranged into rows and columns, converted to binary hex, and then to ASCII characters.
6. The secret message is displayed.

c. LSB Algorithm for Video Encoding and Decoding:

Encoding Algorithm:

1. Analyze the video files (.mp4) as the cover file.
2. Transcode the desired text into binary code.
3. Segregate the video files (.mp4) into individual video frames.
4. Transform the video frames into visual images.
5. Selection of a random set of images to act as the cover art.
6. Identification of the video frame's pixels that will be randomly embedded with the secret message using the knight tour algorithm.
7. Employ the use of encrypted secret messages within the video bits by incorporating the sophisticated LSB encoding technique.
8. Transformation of the image into video frames.
9. Combination of the video frames.
10. The resulting output will be a steganographic video.

Decoding Algorithm:

1. Initiate playback of the steganographic video and disassemble it into individual frames.
2. Transform the video frames into visual images.
3. Identify the selected images that will serve as cover art.
4. Undertake the task of identifying the distinct pixels utilized in encoding the concealed message employing the knight-tour algorithm.
5. Utilize the Least Significant Bit (LSB) technique to extract encrypted messages from bits.
6. Decode the hided message using the subtraction method.
7. The covert message remains undisclosed.

Experimental Results and Performance Analysis:

A. Methodology/Experimental Procedure

The LSB algorithms were simulated using the Python programming language, employing various media files to facilitate the simulation. Performance metrics, such as PSNR and MSE, were utilized to evaluate the effectiveness of the chosen method.

The purpose of this performance evaluation was to assess the effectiveness of LSB steganography algorithms by conducting an embedding methodology, as shown in Figure-2

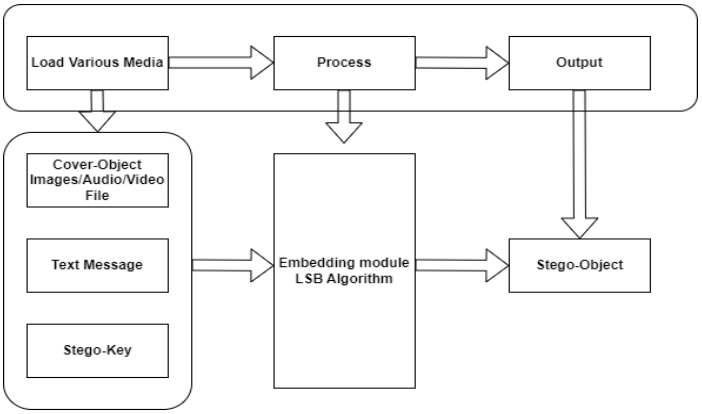

Figure-2 Embedding Methodology of the Selected Steganography Algorithms

The primary objective of this performance evaluation was to gauge the efficacy of LSB steganography algorithms through the implementation of an extraction methodology, as showed in Figure-3.

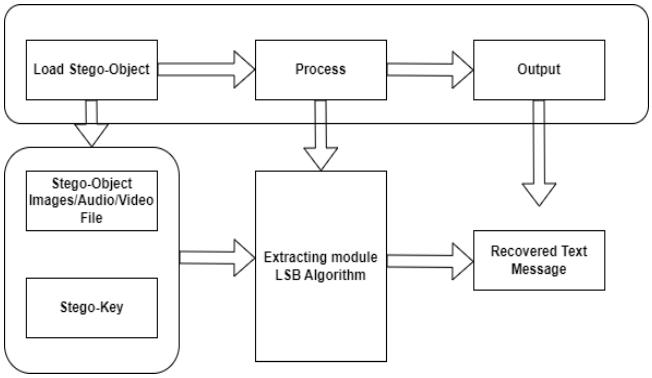

Figure-3 Extracting Methodology of the Selected Steganography Algorithms

B. Assessment Criteria

There is various error metrics are employed in the performance evaluation, such as:

Mean Square Error (MSE):

The Cover-object and the Stego-object exhibit distinct variations, which are contingent upon the extent of distortion. The assessment of the object's features is conducted using the Mean Squared Error (MSE) [25].

$$MSE = \frac{\sum_{M,N} \left[I1(m,n) - I2(M,N) \right]^2}{M \times N}$$

The number of rows and columns in the input image are represented by M and N, respectively

Peak Signal-to-Noise Ratio (PSNR):

The decibel (dB) scale is utilized, where the objective is to optimize the voice and signal quality. The PSNR is a commonly used metric for comparing the results of different objects, and it provides a high level of confidence in the accuracy of these comparisons[25].

$$PSNR = 10 \log_{10} \frac{256^2}{MSE}$$

The PSNR is used in conjunction with the MSE to determine the quality of an image. The PSNR is calculated by the ratio of the maximum possible pixel value to the MSE. A PSNR value that is higher indicates a superior image quality, while a lower value suggests a lower image quality. The LSB technique is used to reduce the MSE value by quantizing the pixel values of the image.

C. Results and Performance Analysis

To analyze the results, various media, including images, audio, and video files of different sizes, were utilized for experimentation with the LSB steganography algorithms. The following table and graph were employed to showcase the PSNR and MSE of the selected algorithms for various media.

Sr. No	Cover File Type	Cover File Size in MB	Text Message	MSE	PSNR in db
1	Image	1	Welcome To Sandip University Nashik	8.9	98.63
		2		3.88	102.23
		5		1.59	106.1
		10		1.45	108.49
2	Audio	1		1.29	97.48
		2		0.19	98.59
		5		0.073	101.36
		10		0.029	105.58
3	Video	1		6.04	90.32
		2		5.64	90.61
		5		5.53	90.72
		10		5.25	90.95

Table 1 exhibits the PSNR and MSE of the selected algorithms for various mediae

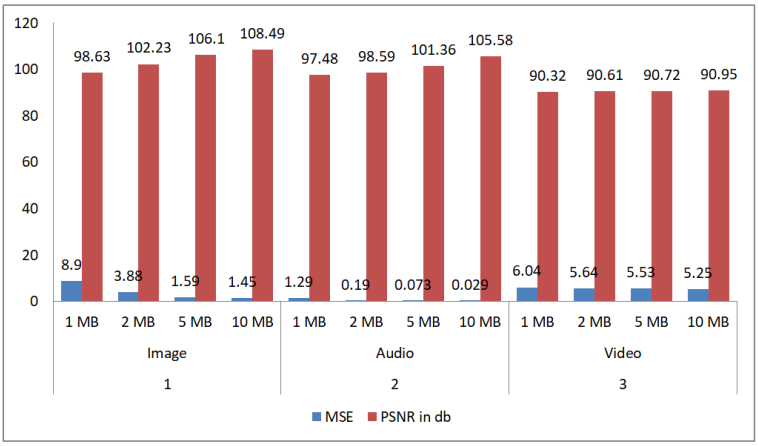

Figure 4 showcases a graph depicting the PSNR and MSE of the selected algorithms for different media

Conclusion:

Last significant bit (LSB) tampering is a technique used to secure data transmission by surreptitiously conveying confidential messages and information. It is not a foolproof method of ensuring data security, but it is highly effective for the purpose of evading detection and obtaining results, particularly in the context of steganography. The application of LSBs is highly advantageous to individuals who require the secure transmission of data, as it is a highly efficient and practical method of achieving this objective.

This paper explores the applications of LSB algorithm in the field of Steganography. Specifically, the LSB algorithm has been developed and implemented in line with the objectives of Steganography. In this context, various techniques of LSB encoding and decoding have been demonstrated through experiments and their results have been evaluated. The performance of LSB algorithm on different mediums has been assessed using measures such as MSE and PSNR. The LSB algorithm has been extensively tested using data embedded using the algorithm, and the PSNR values serve as an indicator of the excellence of the stego-object.

REFERENCES

[1] N. Gopalakrishna Kini, Vishwas G. Kini and Gautam, "A Secured Steganography Algorithm for Hiding an Image in an Image." Integrated Intelligent Computing, Communication and Security, Studies in Computational Intelligence 771, 539-546 (2019).

[2] Imra Aqeel and Muhammad Babar Suleman, "A Survey on Digital Image Steganography Approaches," INTAP, CCIS 932, 769-778 (2019).

[3] Mr. Harshal V. Patil, Dr. Vaibhav P. Sonaje, Dr. Bhojaraj H. Barhate, Dr. Vipin Y. Borole, "Evaluation of the Transform Domain DCT and Spatial Domain LSB Steganography Algorithms' Performance: International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 11 Issue: 11, October 2023, pp. 800-808.

[4] Arora, A., Singh, M.P., Thakral, P., Jarwal, N. (2016). "Image steganography using enhanced LSB substitution technique." 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), Waknaghat, India, pp. 386-389. https://doi.org/10.1109/PDGC.2016.7913225

[5] Mr. Harshal V. Patil, Dr. Vaibhav P. Sonaje, Dr. Bhojaraj H. Barhate, "Literature Review: Information Security A Comparative Analysis of Steganography Algorithms: International Journal Of Innovative Research In Technology ISSN: 2349-6002 Volume: 10 Issue: 05, October 2023, pp. 418-423
[6] Arora, H., Bansal, C., Dagar, S. (2018). "Comparative study of image steganography techniques." 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, pp. 982-985. <https://doi.org/10.1109/ICACCCN.2018.8748451>
[7] Elshazly, E., Abdelwahab, S., Abouzaid, R., Zahran, O., Elaraby, S., Elkordy, M. (2018). "A secure image steganography algorithm based on least significant bit and integer wavelet transform." Journal of Systems Engineering and Electronics, 29(3): 639-649. <https://doi.org/10.21629/JSEE.2018.03.21>
[8] 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.
[9] Adiyan, Z., Purboyo, T.W., Nugrahaeni, R.A. (2018). "Implementation of secure steganography on jpeg image using LSB method." International Journal of Applied Engineering Research, 13(1): 442-448.
[10] Marella, Pranay, Jeremy Straub, and Benjamin Bernard. "Development of a Facial Feature Based Image Steganography Technology." 2019 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, 2019.
[11] Elharrouss, Omar, Noor Almaadeed, and Somaya Al-Maadeed. "An Image Steganography Methodology Based on k-Least Significant Bits (k-LSB)." Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). IEEE, 2020.
[12] Indrayani, Rini, Hanung Adi Nugroho, and Risanuri Hidayat. "Evaluation of MP3 Steganography Utilizing a Modified LSB Method." Proceedings of the 2017 International Conference on Information Technology Systems and Innovation (ICITSI). IEEE, 2017.
[13] Datta, Biswajita, Prithwish Kumar Pal, and Samir Kumar Bandyopadhyay. "Multi-bit Data Hiding in Randomly Selected LSB Layers of an Audio." Proceedings of the 2016 International Conference on Information Technology (ICIT). IEEE, 2016.
[14] Abdelsatir, El-Tigani B., Narayan C. Debnath, and Hisham Abushama. "A Multilayered Scheme for Transparent Audio Data Hiding." Proceedings of the 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA). IEEE, 2015.
[15] Mandal, Ashis Kumar, et al. "An Approach for Enhancing Message Security in Audio Steganography." Proceedings of the 16th International Conference on Computer and Information Technology. IEEE, 2014.
[16] Elkandoz, Marwa Tarek, and Wassim Alexan. "Logistic Tan Map Based Audio Steganography." Proceedings of the 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA). IEEE, 2019.
[17] Dasgupta, Kousik, J. K. Mandal, and Paramartha Dutta. "Hash-based Least Significant Bit Technique for Video Steganography (HLSB)." International Journal of Security, Privacy and Trust Management (IJSPTM) 1.2 (2012): 1-11.
[18] Bhole, Ashish T., and Rachna Patel. "Steganography over Video File Using Random Byte Hiding and LSB Technique." Proceedings of the 2012 IEEE International Conference on Computational Intelligence and Computing Research. IEEE, 2012.
[19] Lou, Der-Chyuan, and Chen-Hao Hu. "LSB Steganographic Method Based on Reversible Histogram Transformation Function for Resisting Statistical Steganalysis." Information Sciences 188 (2012): 346-358.
[20] Zhang, Rongyue, et al. "An Efficient Embedder for BCH Coding for Steganography." IEEE Transactions on Information Theory 58.12 (2012): 7272-7279.
[21] Vijay Kumar Sharma and Vishalshrivastava. "A Steganography Algorithm for Hiding Images by Improved LSB Substitution with Minimized Detection." Journal of Theoretical and Applied Information Technology, vol. 36, no. 1, 2012.
[22] Neeta Deshpande and Snehal Kamalapur. "Implementation of LSB Steganography and Its Evaluation for Various Bits." 2004.
[23] Beenish Mehboob and Rashid Aziz Faruqui. "A Steganography Implementation." IEEE, 2008.
[24] A. Shjul and U. Kulkarni. "A Secure Skin Tone-Based Steganography Using Wavelet Transform." IJCTE 3 (2011): 16-22.
[25] Neeta Deshpande and Snehal Kamalapur. "Implementation of LSB Steganography and Its Evaluation for Various Bits." 2004.
[26] Binny and Anu Maddulety Koilakuntla. "Hiding Secret Information Using LSB-Based Audio Steganography." 2014 International Conference on Soft Computing and Machine Intelligence.