A SURVEY OF IMAGE STEGANOGRAPHY USING LEAST SIGNIFICANT BIT (LSB)

Oluwayomi AWE [1], Oyenike Adunni OLUKIRAN[2], Olukayode AIYENKO [3] Fatimoh Abidem TAOFEEK-IBRAHIM [4]
[1] Department of Computer Science, University of Lagos, Lagos, Nigeria
[2] Department of Mathematical and Computing Sciences,
KolaDaisi University, Ibadan, Nigeria
[3]Department of Computer Science, Lagos State University, Lagos, Nigeria
[4] Department of Computer Science, Federal Polytechnic Offa, Kwara State, Nigeria
[1]aweyomi@gmail.com, [2]oyenikeolukiran@koladaisiuniversity.edu.ng, [3]royalgrace@yahoo.com, fatty_fatty2@yahoo.com.au

Keywords: *Image steganography, Least Significant Bit, Executable file, Steganalysis*

Abstract: One of the extensively applied methods for well-secured communication is steganography, which is also referred to as secret writing. A variety of techniques such as the application of invisible ink and masking the secret text inside an inconspicuous text existed during the early days. Steganography helps to conceal information between the sender and intended recipient so that others are not aware of the message's presence in the information. Digital steganography applies to different media like executable files, images, audio and videos, text and games. This paper conducted a literature review on different algorithms for image steganography using LSB techniques. A suggestion was made to show how the LSB technique can be further enhanced.

1. INTRODUCTION

Steganography is a method of the security system through obscurity, which involves the hiding of existence of a message between the sender and intended recipient, this technique has been used to hide secret messages in various types of files, including digital images, audio and video[1]. The most general application of steganography is hiding information from one file within the information of another file. For instance, cover carriers, such as images, audio, video, text, or code represented digitally [2], hold the hidden information so that its existence will not be discovered by the third party or the untargeted receiver. The hidden information may be plaintext, ciphertext, images, or information hidden into a bitstream [3]. The cover carrier and the hidden information create a stego-carrier. The covered image where the message is hidden is referred to as STEGO, this aids the elimination or reduction of suspicion.

Steganalysis is a technique that is used in identifying hidden messages in images [4]. Although steganography is not a newly discovered field, it has become gradually more significant in the current digital world where information is frequently or effortlessly exchanged using the Internet, email, and other means using computers [5]. Steganography is most valuable where human rights are been hampered, military, anti-forgery and so on [6]. Steganalysis helps the security analyst, forensic experts to keep track of covered messages [7]. There are numerous reasons why steganography is used, it can be used to communicate with complete freedom even under conditions that are censored or monitored [8]. It can also be used to protect private communications where the use of cryptography is normally not allowed or would raise suspicion.

Image steganalysis involves the hiding of data inside cover images for security [9]. Images

possess a lot of visual redundancy because our eyes do not usually consider subtle changes in colour in an image region. One can use this redundancy to hide text, audio or even image data inside cover images without making significant changes to the visual perception [10]. Image steganography is becoming popular on the internet these days since a stenographic image, which looks like any other image, attracts less attention than an encrypted text and a secure channel [11].

Several image steganalysis techniques have been employed such as least significant bit pixel value differencing, histogram-based, texture-based, spread spectrum-based, labelling or connectivity method and so on [12]. Among the image steganography techniques, LSB remains the most common and easiest approach for message hiding [13]. In this method, a message is hidden in the least significant bits of image pixels. Also, changing the LSB of the pixels does not introduce much difference in the image and thus the stego-image looks similar to the original image [14].

2. LITERATURE REVIEW

2.1 Steganography

Steganography is a system that includes concealing a message in a reasonable bearer, e.g., picture, sound and video document. The steganography network gets to a great extent from the flag and picture handling network. The less successive commitments from the cryptography and data hypothesis networks don't generally utilize a similar wording, and this can make it difficult to see the associations between various works.

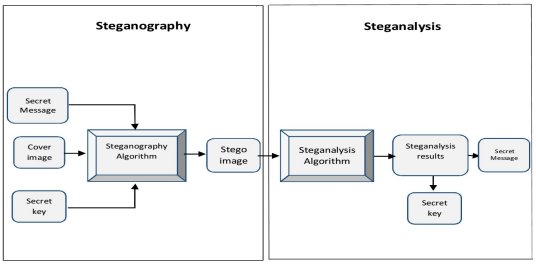

Figure 1: Steganography and Steganalysis

Figure 1 shows the Steganography and Steganalysis process.

In steganography, the presence of the message is mystery, the correspondence channel is considered as open and the message itself is not typically altered to oppose an assailant independent from anyone else (even though it tends to be scrambled). The purpose is to cover up the message and also hide a harmless substance with the goal that any spy would have no doubts.

In Figure 2, an instance of steganography for which the stowing away of the message is imperceptible to the human eye. It is critical to recognize steganography from cryptography, first: cryptography goes for altering the message with the goal that it moves toward becoming difficult to peruse to an overhang dropper. It is of no worry to cryptography that the scrambled message may look suspicious. Steganography may not change the message however, just shrouds it in a medium, with the goal that it won't raise doubts.

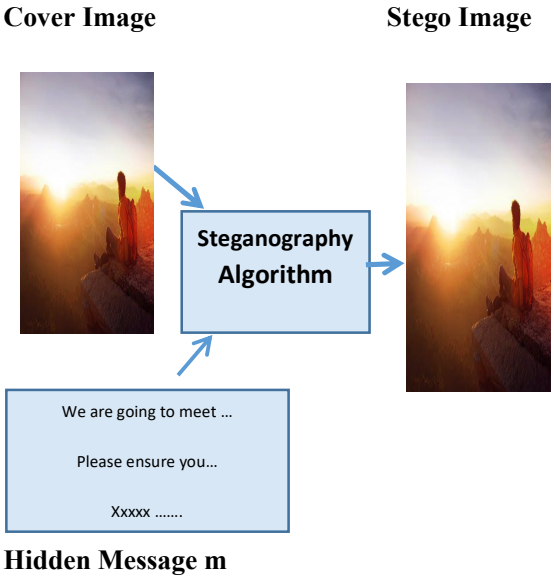

Figure 2: A Straightforward Outline of Steganography for a Picture [15].

The generalized attack against end-of-file can be simply identified in the rSteg, OpenStego and StegoTool.

2.1.1 Retransmission Steganography (rSteg)

rSteg is an intra-protocol hybrid network steganography technique, which is proposed for a wide class of protocols that use retransmission mechanisms [16]. The main invention of RSTEG is not to acknowledge a successfully received packet to intentionally invoke retransmission [17]. The retransmitted packet of user data then carries a steganogram in the payload field. A typical protocol that employs a retransmission mechanism based on timeouts obligates the receiver to acknowledge each received packet. When the packet is not successfully received, no acknowledgment is sent [18]. After the timeout expires and the sender has not received the acknowledgment the packet is retransmitted. RSTEG can be applied to all retransmission mechanisms in TCP namely Retransmission Timeout (RTO) Fast Retransmit/Recovery (FR/R) or Selective ACK (SACK). It requires modification to both the sender and the receiver.

2.1.2 OpenStego

This is an open-source steganography software developed in a java environment [19]. It provides two functionality data hiding as well as watermarking. The OpenStego is used to attach any type of secret message file to cover files [20]. BMP, GIF, JPEG, JPG, PNG, WBMP are the supported file types for cover. After finishing one can save the output stego file in PNG format. Similarly, this software is used to obtain secret data from the above output file. Security can be given by producing passwords.

2.1.3 StegoTool

Stego Tool is a software that allows a user to embed hidden data inside a carrier file, such as an image or video, and later extract that data [21]. It is not necessary to conceal the message in the original file at all. Thus, it is not necessary to modify the original file. If a given section is subjected to successive bitwise manipulation to generate the ciphertext, then there is no evidence in the original file to show that it is being used to encrypt a file.

2.2 Image Steganography Techniques

The image steganography technique involves the hiding of the data in the image format, image is embedded with the information or message to send and converted into stego-image [22]. There are numerous techniques for image steganography:

2.2.1 Spatial Domain Technique

The techniques use the pixel grey levels and their colour values directly for encoding the message bits [9]. These techniques remain the simplest schemes in terms of embedding and extraction complexity. The major drawback of these methods is the amount of additive noise that creeps in the image which directly affects the Peak Signal to Noise Ratio and the statistical properties of the image [23]. All version of the spatial domain technique of image steganography changes the image pixel value by some or all bits for hiding the message [24]. The very simplest technique in this spatial domain is the Least Significant Bit (LSB) in which the value of the pixels changes without many distortions. The main advantage of using the spatial domain technique in image steganography is that a large amount of data can be stored in the image and the original message cannot be degraded easily [25]. But there are some limitations to this method as the data can be lost if the image is manipulated in the LSB technique and the data can easily be destroyed by very simple attacks or intrusions [26]. The broad classification of the spatial domain methods includes: Least Significant Bit (LSB), Edges Based Data Embedded Method (EBE), Pixel Value Differencing (PVD), Mapping Pixel to Hidden Data Method, Labeling or Connectivity Method, Histogram Shifting Method (HSM), Texture Based Method (TBM) and. Pixel Intensity Based Methods (PIBM) [27].

2.2.2 Transform/Frequency Domain Method

It is one of the techniques used for the hidden exchange of information in the frequency domain and it also can be referred to as the study of invisible communication that deals with the

methods of hiding the existence of the communicated message [28]. The covering or hiding of message in this method is more complex [29]. There are various techniques and methods are built to provide the hiding of data into an image [30]. For the domain of embedding techniques, many algorithms and method has been suggested in the transform domain techniques [31]. Embedding data in the frequency domain is stronger rather than embedding the data in the time domain signal. Most of the data in today's system are embedded in the time or frequency domain of image steganography rather than the spatial domain as it provides various advantages over spatial technique [32]. In this technique, the message or the actual data is hidden in that part of the image which is less exposed to cropping, compression, and processing [33]. Examples of transform or frequency domain techniques include Discrete Fourier Transformation (DFT), Discrete Wavelet Transformation (DWT), Discrete Cosine Transformation (DCT), Discrete Fourier transformation (DFT), Embedding in Coefficient Bits, and Reversible Method or Lossless (DCT) [34].

2.3 Least Significant Bit (LSB) Approach

This is a steganography technique in which a message is inside an image by replacing the least significant bit of the image with the bits of a message to be hidden [35]. By modifying only the first most right bit of an image, a secret message can be inserted and it also makes the picture unnoticeable, but if the message is too large it will start modifying the second rightmost bit and so on and an attacker can notice the changes in the picture [36]. The least significant bit (LSB) insertion is a popular and easy approach to embed information in an image file. In this technique, the LSB of a byte is replaced with an M‟ s bit. To the human eye, the stego image looks identical to the carrier image [37]. To a computer, an image file is simply a file that shows different colours and intensities of light on different areas of an image. The best type of image file to hide information inside is a 24 Bit BMP (Bitmap) image [38]. Although 24 Bit images are best for hiding information due to their size. Some people may choose 8 Bit BMP‟ s or possibly another image format such as GIF. The reason being is that posting of large images on the internet may arouse suspicion. The least significant bit i.e. the eighth bit is used to change to a bit of the secret message. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue colour components as shown in Figure 3.

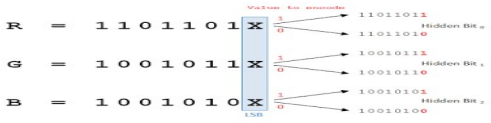

Figure 3: Sample of LSB for RGB Component [39].

2.4 RELATED WORK

[40] developed an enhanced LSB-image steganography system using the hybrid canny-Sobel edge detection. The system devised a method for increasing the payload of secret messages in an image. The edge area was used to accommodate more message bits because the image edge area can better tolerate pixel value changes. Also, Canny and Sobel's detectors were combined to get a wider edge area. The two-detector combined method provided a larger edge area for a greater payload of messages while maintaining the imperceptibility of stego-images.

[1] designed a novel blind statistical steganalysis technique to detect the Least Significant Bit (LSB) flipping image steganography. First, a novel method of pixel colour correlativity analysis in Pixel Similarity Weight (PSW) was achieved. In the second phase, filtered out image pixels according to statistically detected suspiciousness, thereby excluding neutral pixels from the steganalysis process. At the Third phase, ranking suspicious pixels according to their statistically detected suspiciousness and determining the influence of such pixels based

on the level of detected anomalies. Fourth, the capability to classify and analyze pixels in three-pixel classes of flat, smooth and edgy, thereby enhancing the sensitivity of the steganalysis. Fifth achieved an extremely high-efficiency level of 98.049% in detecting 0.25bpp stego-images with only a single dimension analysis.

[22] proposed a comprehensive review on dynamic key-based LSB technique for image steganography image. All the applications and algorithms of image steganography were discussed in the study. The system showed how steganography is better than various other methods used for secure communication over the Internet. The system was implemented using MATLAB and also verified the results. PSNR parameter was employed to evaluate the performance of the system.

[27] came up with a new image steganography method based on the spatial domain. The secret message was embedded randomly in the pixel location of the cover image using Pseudo-Random Number Generator (PRNG) of each pixel value of the cover image instead of embedding sequentially in the pixels of the cover image. This randomization was expected to increase the security of the system. The proposed method applied two layers (Blue and Green), as (2-1-2) layer, and the byte of the message was embedded in three pixels only in this form (3-2-3). From the experimental results, it was shown that the proposed method achieved a very high Maximum Hiding Capacity (MHC), and higher visual quality as indicated by the Peak Signal-to-Noise Ratio (PSNR).

[41] improved upon the LSB technique for colour images by embedding the information into three planes of RGB image in a method that enhanced the quality of the image and also the system achieved high embedding capacity. The proposed method of Least Significant bit (LSB) for secret message insertion was made based on the sensitivity of human eyes to various colour wavelengths. This selective approach induced lower noise and high security for transferring images. The LSB approach replaced the least significant bit of the pixel in the cover image. The earlier approaches used to hide the secret message for coloured images lead to high noise in the stego-image due to this the secret information is susceptible to be detected. But our proposed method results in better image quality, secure and reliability as the image was sliced into three planes i.e. Red, green and blue then inserted the message in each plane based on colour sensitivity. The PSNR value of the system outperformed existing steganography methods.

[42] presented a novel data-hiding technique based on the LSB technique of digital images. The steganography dealt with hiding text in an image file using the Least Significant Bit (LSB) technique. The LSB algorithm was implemented in the spatial domain in which the payload bits were embedded into the least significant bits of the cover image to derive the stego-image.

[43] investigated different methods of Steganography with comparative analysis of different methods. From this analytical survey, this study concluded that all methods have advantages and limitations. The strong and weak points of these techniques were mentioned briefly so that researchers in steganography gain prior knowledge in designing these techniques and their variants. The next plan suggested is to develop a steganography system that is robust to different types of attacks, and also a design system that can be enhanced for other data files like audio, video and text.

[44] used two methods of image domain and transform domain for image steganography. The use of the LSB algorithm for the image domain decreased the MSE value and increased the PSNR value when increasing the bit substitution. The system was simulated on MATLAB and the results showed the effect of different message bit for hiding bit and analysis effect on the results.

[8] developed a system with a high capacity data embedding approach by the combination of Steganography and cryptography. In the process,

a message was first encrypted using the transposition cipher method and then the encrypted message is embedded inside an image using the LSB insertion method. The combination of these two methods enhanced the security of the data embedded. This combinational methodology satisfied the requirements such as capacity, security and robustness for secure data transmission over an open channel. A comparative analysis was made to demonstrate the effectiveness of the proposed method by computing the Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). The study analyzed the data hiding technique using the image performance parameters like Entropy, Mean and Standard Deviation. The stego images were tested by transmitting them and the embedded data are successfully extracted by the receiver.

[45] designed a new approach for LSB Based Image Steganography using Secret Key. In the study, hidden information was stored into different positions of LSB of an image depending on the secret key. The Peak Signal-to-Noise Ratio (PSNR) was used to measure the quality of the stego-images. The value of PSNR gave better results because the proposed method changes a very small number of bits of the image. The obtained results showed that the proposed method results in LSB based image steganography using a secret key which provided good security issue and PSNR value than general LSB based image steganography methods.

4. SUMMARY AND DISCUSSION

In image steganography, several tools use the same base which is LSB to perform extraction but there is a need for a more enhanced LSB algorithm that can be used to extract the hidden messages. The generalized attack against end-of-file can easily be detected in the rSteg, OpenStego and StegoTool. It is Image-Stegano that is more secured than others because of the Edge Least Significant Embedding. This paper performed a general literature review of LSB method of image steganography. It was identified that all tools cannot detect other hidden messages despite that they are using a generic LSB algorithm, these tools sometimes are prone to attack despite having a secret key. Hence, it is necessary to perform a comparative analysis on tools used in the LSB approach to investigate the aspects to be considered for future improvement.

5. CONCLUSION

Steganography is a technique of hiding secret information into an innocent-looking cover media known as stegogramme such that an unintended observer will not be aware of the existence of the hidden messages. With steganographic techniques, it is possible to hide information within images, audio, video files or text which is perceptually undetectable. The advancement in information technology, particularly in networks such as internet, digital multimedia applications and mobile communication has uncovered new prospects for steganography and information hiding techniques. Several techniques of steganography have been used by different researchers for information security tasks. This paper gave a clear picture of the current trends in image steganography using LSB Algorithm.

REFERENCES

[1] A. M. Chaeikar, S. S., Zamani, M., Manaf, A. B., & Zeki, "PSW statistical LSB image steganalysis," *Multimed. Tools Appl.*, pp. 1–32, 2017.

[2] A. Awad, M. F. M. Mursi, and A. K. Alsammak, "Data hiding inside JPEG images with high resistance to steganalysis using a novel technique : DCT-M3," *Ain Shams Eng. J.*, vol. 9, no. 4, pp. 1965–1974, 2018.

[3] S. V Desai, M. B & Patel, "Performance Analysis of Image Steganalysis against Message Size, Message Type and Classification Methods," in *IEEE International Conference on Advances in Electronics, Communication and Computer Technology*, 2016, pp. 295–302.

[4] P. C. Mandal, "An Extensive Review of Current Trends in Steganalysis," *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 1, no. 7, pp. 215–220, 2012.

[5] S. Vyas, A. O & Dudul, "Study of Image Steganalysis Techniques," *Int. J. Adv. Res.*

Comput., vol. 6, no. 8, pp. 8–12, 2015.

[6] B. Memon, N. & Sankur, "Steganalysis Using Image Quality Metrics ˙," in *IEEE Transactions on Image Processing*, 2003, vol. 12, no. 2, pp. 221–229.

[7] E. Olson, L. Carter, and Q. Liu, "A Comparison Study Using StegExpose for Steganalysis," *Int. J. Knowl. Engineering*, vol. 3, no. 1, pp. 8–12, 2017.

[8] S. A. Laskar and K. Hemachandran, "A Review on Image Steganalysis techniques for Attacking Steganography," *Int. J. Eng. Technol.*, vol. 3, no. 1, pp. 3400–3410, 2014.

[9] M. J. Sravanthi, G. S, Sunitha, B. Riyazoddin, S. M & Reddy, "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method," *Glob. J. Comput. Sci. Technol. Graph. Vis.*, vol. 12, no. 15, pp. 1–8, 2012.

[10] L. Rathika, B. Loganathan, M. P. Scholar, T. Nadu, and T. Nadu, "Approaches and Methods for Steganalysis – A Survey," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 6, no. 6, pp. 433–438, 2017.

[11] A. Fatnassi, H. Gharsellaoui, and S. Bouamama, "An Optimal Steganalysis Based Approach for Embedding Information in Image Cover Media with Security," *Int. J. Comput. Inf. Eng.*, vol. 10, no. 6, pp. 1245–1249, 2016.

[12] A. Tiwari, S. R. Yadav, and N. K. Mittal, "A Review on Different Image Steganography Techniques," *Int. J. Eng. Innov. Technol.*, vol. 3, no. 7, pp. 121–124, 2014.

[13] K. J. Devi, "A Secure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique by," 2013.

[14] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB Steganography via Sample Pair Analysis," in *IEEE Transactions on Signal Processing*, 2003, vol. 51, no. 7, pp. 1995–2007.

[15] Y. Miche, P. Bas, A. Lendasse, C. Jutten, and O. Simula, "Advantages of Using Feature Selection Techniques on Steganalysis Schemes," *9th Int. Work. Artif. Neural Networks, IWANN'2007*, pp. 606–613, 2007.

[16] W. Mazurczyk, M. Smolarczyk, and K. Szczypiorski, "Retransmission steganography applied," in *Proceedings - 2010 2nd International Conference on Multimedia Information Networking and Security, MINES 2010*, 2010, pp. 846–850.

[17] D. R. Tej, Y. M. Shankar, and T. S. Madhuri, "Steganography Using Matlab," *Int. J. Adv. Eng. Res. Sci.*, vol. 2, no. 4, pp. 19–24, 2015.

[18] S. Sandeep, S. & Aman, "A Review on the Various Recent Steganography Techniques A Review on the Various Recent Steganography Techniques," *Int. J. Comput. Sci. Netw.*, vol. 2, no. 6, pp. 142–156, 2015.

[19] S. M. Kunjir, S. D. Patil, S. Jabeen, S. V Bhosale, and D. Y. P. A. C. S. College, "Review On Stenography Tools," *Int. Res. J. Eng. Technol.*, vol. 03, no. 10, pp. 1223–1225, 2016.

[20] K. Amarendra, V. N. Mandhala, B. C. Gupta, G. G. Sudheshna, and V. V. Anusha, "Image steganography using LSB," *Int. J. Sci. Technol. Res.*, vol. 8, no. 12, pp. 906–909, 2019.

[21] A. K. Dodo, B. Y. Baha, and U. A. Bukar, "A Comparison Between Different Image Steganography Algorithms," *Dutse J. Pure Appl. Sci.*, vol. 2, no. 1, pp. 81–85, 2016.

[22] D. Karte, B. & Bharti, "Dynamic Key-based LSB Technique for Steganography," *Int. J. Comput. Appl.*, vol. 167, no. 13, pp. 9–14, 2017.

[23] K. & Ravneet and K. Bhavneet, "A Study and Review of Techniques of Spatial Steganography," *Int. J. Sci. Res.*, vol. 4, no. 4, pp. 3198–3203, 2015.

[24] V. Rejani, R., Murugan, D. & Krishnan, "Comparative Study of Spatial Domain Image Steganography Techniques," *Int.J. Adv. Netw. Appl.*, vol. 7, no. 2, pp. 2650–2657, 2015.

[25] S. Sahu, A. K & Monalisa, "Digital image steganography techniques in spatial domain : A study Available Online through CODEN : IJPTFI Review Article," *Int. J. Pharm. Technol.*, vol. 8, no. 4, pp. 5205–5217, 2017.

[26] F. Akhter, "A Novel Approach for Image Steganography in Spatial Domain," *Glob. J. Comput. Sci. Technol. Graph. Vis.*, vol. 13, no. 7, pp. 1–6, 2013.

[27] F. A. Emam, M. M., Aly, A. A & Omara, "An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection," *Int. J. of computer Adv. Sci. Appl.*, vol. 7, no. 3, pp. 361–366, 2016.

[28] P. B. Desai and P. S. Bhendwade, "Image Steganography Using LSB Algorithm," *Int. J. Adv. Res. Electr. Electron. Instrum. Eng.*, vol. 5, no. 8, pp. 6883–6890, 2016.

[29] N. Ghoshal and J. K. Mandal, "Image Authentication Technique in Frequency Domain based on Discrete Fourier Transformation (IATFDDFT)," in *Proceedings of ICCS*, 2010, pp. 144–150.

[30] D. Divya, A. & Thenmozhi, "Steganography : Various Techniques In Spatial and Transform Domain," *Int. J. Adv. Sci. Res. Manag.*, vol. 1, no. 3, pp. 81–89, 2016.

[31] K. S. Sadasiva and A. Damodaram, "Color Image Steganographic Technique in Spatial

Domain," *Int. J. Innov. Res. Comput.*, vol. 3, no. 10, pp. 10318–10321, 2015.

[32] N. Manibharathi, S. Krishnaprasad, and S. Famila, "Transform Domain Technique in Image Steganography for Hiding Secret Information," *Int. J. Eng. Res. Technol.*, vol. 3, no. 2, pp. 1255–1260, 2014.

[33] P. Hemalatha, S., Acharya, U. D., Renuka, A., & Kamath, "A Secure Color Image Steganography in Transform Domain," *J. Cryptogr. Inf. Security*, vol. 3, no. 1, pp. 17–24, 2013.

[34] S. K. Bhattacharjee, H., & Bandyopadhyay, "Frequency Domain Approach of Image Steganography," *Int. J. Innov. Res. Inf. Secure.*, vol. 3, no. 02, pp. 9–16, 2016.

[35] R. Joshi, L. Gagnani, and S. Pandey, "Image Steganography With LSB," *Int. J. Adv. Res. Comput. Engineering Technol.*, vol. 2, no. 1, pp. 228–229, 2013.

[36] T. Saqer, W. & Barhoom, "Steganography and Hiding Data with Indicators-based LSB Using a Secret Key," *Engineering, Technol. Appl. Sci. Res.*, vol. 6, no. 3, pp. 1013–1017, 2016.

[37] Nidhi, "Image Steganography Using Enhanced LSB Technique," *Int. J. Sci. Eng. Res.*, vol. 7, no. 12, pp. 253–258, 2016.

[38] M. H. Mohamed and L. M. Mohamed, "High Capacity Image Steganography Technique based on LSB Substitution Method," *Appl. Math.Inf.Sci*, vol. 266, no. 1, pp. 259–266, 2016.

[39] K. Shabnam, S. & Hemachandran, "LSB based Steganography using Bit masking method on RGB planes," *Int. J. Comput. Sci. Inf. Technol.*, vol. 7, no. 3, pp. 1169–1173, 2016.

[40] D. R. Ignatius, M. Setiadi, and J. Jumanto, "An Enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel Edge Detection," *Cybern. Inf. Technol.*, vol. 18, no. 2, pp. 74–88, 2018.

[41] S. Amritpal, A. & Harpai, "An Improved LSB based Image Steganography Technique for RGB Images," in *IEEE International Conference on Electrical, Computer and Communication Technologies*, 2015, pp. 1–4.

[42] V. S. Singh, A. K., Juhi, & Harsh, "Steganography in Images Using LSB Technique," *Int. J. Latest Trends Enigeering Technol.*, vol. 5, no. 1, pp. 426–430, 2015.

[43] P. Palak, P & Yask, "Survey on Different Methods of Image Steganography," *International J. Innov. Res. Comput.*, vol. 2, no. 12, pp. 7614–7618, 2014.

[44] S. Gupta, H., Kumar, R., & Changlani, "Steganography using LSB bit Substitution for data hiding," *Int. J. Adv. Res. Comput. Sci. Electronic Eng.*, vol. 2, no. 10, pp. 676–680, 2013.

[45] S. M. M. Karim, S. Rahman, and I. Hossain, "A new approach for LSB based image steganography using secret key A New Approach for LSB Based Image Steganography using Secret Key," in *Proceedings of 14th International Conference on Computer and Information Technology*, 2011, pp. 22–24.