Survey on latest methods / development in the field of steganography

Dhruv Gajjar, Manthan Jani

Urvashi chaudhari

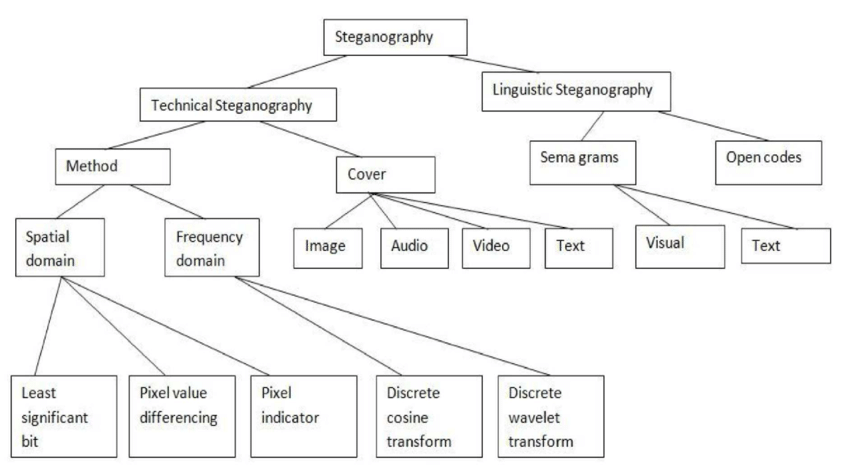
25 March 2022

1. Abstract

This survey is carried out on the studies which proposes and implements an upgrade to plain LSB - based picture steganography.This study presents a quick overview of how to increase stegoimage quality using cutting-edge approaches and also focuses on enhancing the security. A survey of several strategies for these approaches was conducted.We acknowledge a number of qualitatively diverse methods to steganalysis in practice.The algorithms and performance factors of these systems will be thoroughly examined, providing guidance for their future research endeavours.

2. Introduction

Steganography is the art of hiding data [Message, image, audio] in another carrier object [image, video, audio] and prevents intruder from suspecting hidden information in our carrier object. Steganography is classified as under.



Encryption or random mapping is better preferred over just hiding the data in carrier object as it is the only obstacle in interpretation of our information and thus increase the security, confidentiality and integrity of our secret information from possible unauthorized user.

3. Summary

A novel LSB inversion method to improve the quality of final image is proposed for 1011[1].Four message bits 1011 are to be hidden into four cover image pixels 10001100, 10101101, 10101011 and 10101101.After plain LSB steganography, stego-image pixels are

10001101, 10101100, 10101011 and 10101101. Two pixels i.e. the first and second of the cover image have changed. Now, we see that the second and third LSB of three cover image

pixels are 0 and 1respectively. For two of these three pixels, LSB has changed. If we

invert the LSB of these three pixels, cover image pixels will be 10001100, 10101101, 10101011 and 10101100. Now, there is only one pixel of stego-image which differs from cover image i.e. the last one. Thus, the PSNR would increase improving the quality

of stego-image. For correct de-steganography, we need to store the fact that we have inverted the LSBs of those pixels in which the second and third LSB are 0 and 1 respectively.

RC4 algorithm with LSB replacement[3].Following steps describes how RC4 algorithm is used to generate random cover image pixels. To generate the random sequence, a stego-key is used, which can be stored into the cover image or supplied to the receiver separately.

1) Step 1: Calculate the size of the message Image.

2) Step 2: Select the cover image at least 8 times the size of the message image.

3) Step 3: Pixilate both the images and convert to binary form.

4) Step 4: Generate array of cover image locations for selected stego-key using RC4 algorithm.

5) Step 5: Replace the LSBs of cover image pixels in the sequence generated in step 4,

with message image bits

First,in this algorithm [4] we find the set of all prime numbers that are required to decompose a pixel value in a k-bit coverimage, i.e., we need to find a number n∈Ν such that all possible pixel values in the range 2,0[ − ]1 k can be represented using first n primes in our n-bit prime number system.After finding the primes, we create a map of k-bit (classical binary decomposition) to n-bit numbers (prime decomposition), n > k , marking all the valid representations in our prime number system. Next, for each pixel of cover image choose a (virtual) bit plane, say pth bit-plane ( p < n) , embed secret data bit into that particular bit plane.After embedding the secret message bit, we convert the resultant sequence in prime number system back to its value (in binary number) and get our stego-image.

A new approach is proposed to detect LSB steganography embedded in digital signals, and

to estimate the length of the hidden message length. The estimate is remarkably accurate under mild assumptions that are true for continuous signals. The estimation error is analyzed in terms of the degree that the input signals deviate from the assumptions, and error bounds are given. Experiments are conducted on a set of continuous-tone images. Empirical observations made in the simulations agree with our analytic results[5].

Here the LSB approach is combined with the F5 algorithm and matrix embedding which is applied on both spatial and frequency domain of an image . In Spatial domain the message bits are inserted in the LSB of each pixel in an image but in the frequency domain the message bits are embedded in the quantized DCT coefficients. Flipping LSBs is an unnatural activity that introduces vivid artifacts into the histogram [6].

Here the secret key and Red matrix are initiated for decision making[7]. Then it is replaced with either the green and blue matrix. XOR operation is done at least a significant bit of an image. 8 bit random key and the pixel 1 of the 2nd bit of the red matrix are XOR with the pixel. XOR of bit 1 and 0 bit is 1. So the pixel must satisfy and send to the encrypted message and that encrypted message will hide the value from the 1st LSB bit of the pixel 1. If the answer is 0 while XOR operation is done then the pixel will skip but the next step is continued with the same 8 bit random key.

Algorithm used to insert data image into the cover image:[8]

Step 1: Read the cover image.

Step 2: Bit slice cover image to Red, Green and Blue Planes and show Image histogram.

Step 3: Read 6 text images to be hidden.

Step 4: Select images one by one to be hidden in Red, Green and Blue planes and arrange text images in interleaved manner.

Step 5: Replace bits of Cover image in order of 2:2:4 of the LSB in three planes (i.e. Red, Green and Blue planes) with the bits of message image.

Step 6: Display the reconstructed image after the encoding process. Step 7: Determine PSNR of the cover image.

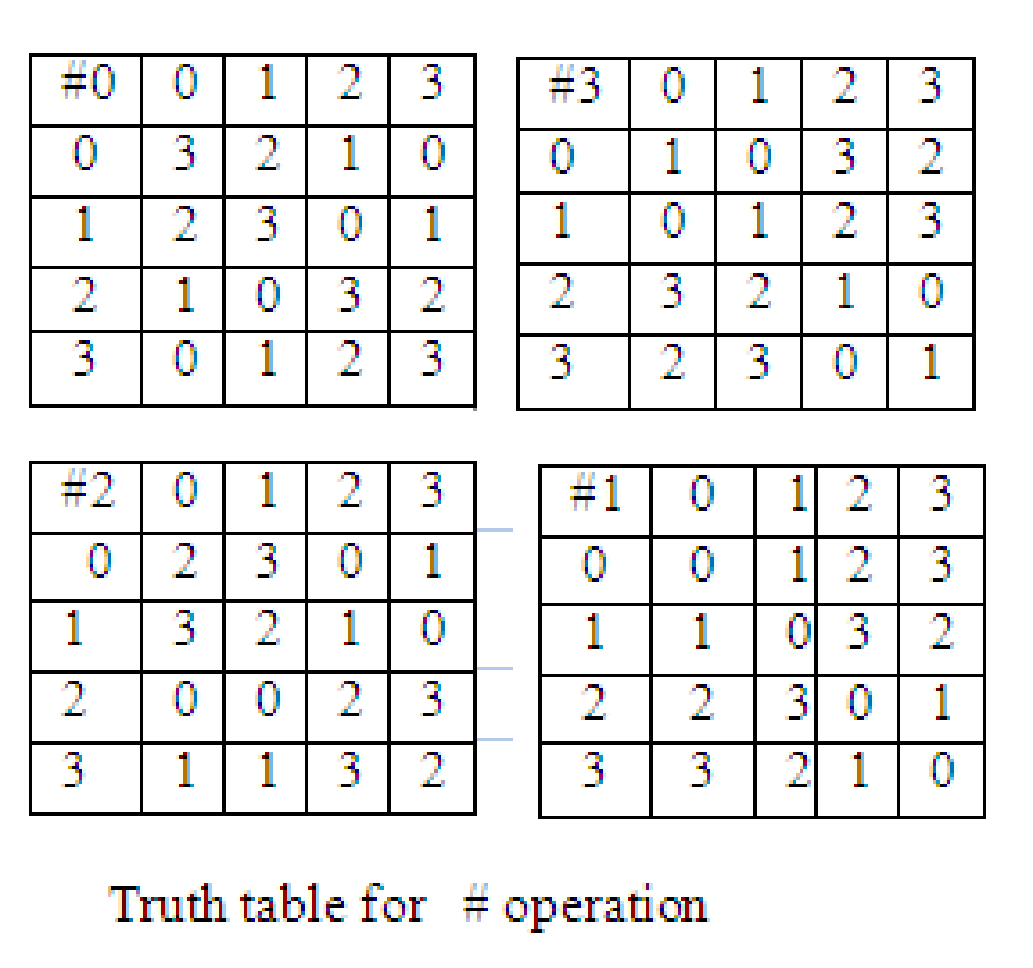
To measure the imperceptibility of steganography several metrics are used[9]. The metrics indicates how similar (or different) the stego-image is compared with CVR. The following metrics are used in the literature including the work of : Mean Squared Error (MSE) is computed by performing byte by byte comparisons of the CVR and stego-image.Where M, N are the number of rows and columns in the CVR matrix, fij is the pixel value from CVR, and gij is the pixel value from the stego-image. Higher value of MSE indicates dissimilarity between compared images. Bit error rate (BER) computes the actual number of bit positions which are changed in the stego-image compared with CVR.

An encryption method is investigated and is provided as one of the final options for the user[10]. The purpose here is not to use or develop a secure cryptographic method but to use a relatively simple method, which contains a key in order to more randomly distribute the message over the image

In the proposed method, a block size of 128 bits with a 128-bit-key is used[11]. At the start of every session, the sender randomly generates the symmetric key and shares it with the receiver through one of the symmetric key distribution methods. Furthermore, to ensure the production of the cipher text, which has the same length as the plain text length, we have used CTS operation mode of AES. CTS stands for CipherText Stealing mode, that handles any length of plain text and produces cipher text whose length matches the plain text length. The data encoding procedure is very plain; the sender encrypts the compressed data block using the randomly generated key and generates the ciphered data block.

y it can give a significant influence on imperceptibility messages[12]. The inverted LSB technique is based on the LSB 2-bit pattern. There are those that use patterns on the 5th and 6th bits of LSB, some use the 2nd and 3rd bit patterns of LSB. The inverting process is done from the calculation of changes in pixel values if iverted bits are done, so before inverted bits the profits must be calculated first.

In A New Approach for Data Hiding with LSB Steganography [13] proposed system is based on pseudorandom numbers using a truth table that works on 4 states(0,1,2,3).



Hiding a secret message into image(proposed system works on RGB scale):

* Red component value will be divided into 4 parts P1,P2,P3,P4 each of two bits
* P1 will decide the truth table out of 4.
* P2, P3 will decide the row and column in the table, meaning how many bits of the message to hide in the message.
* P4 will decide in which value the message is hidden in the LSB of BLUE or GREEN component of the image.

Hiding a secret image into image(proposed system works on GRAY scale):

* Take two consecutive pixels from the carrier image and divide the first pixel into 4 parts P1, P2, P3, and P4.
* P1 will decide if the message should be hidden in the second pixel or not.
* P2 will decide the table out of 4.
* P3 and P4 will decide the row and column, mean number of LSB bits to use for hiding.

A Novel Secure Model: Image Steganography with Logistic Map and Secret Key [14] have proposed a steganography model based on random embedding in LSB of image in controlled manner. The security of the proposed lies on the randomness of message insertion.Random number will be generated by xn + 1 = μ.xn.(1 − xn), where μ will be a factor to generate chaotic behaviour. Seed value will be our key.

A-new-approach-for-LSB-based-image-steganography-Karim-Rahman [15] have proposed a steganography based on a symmetric cryptography. To hide the information, the cover image (RGB scale) is divided into 3 part red, green and blue component. Key and red component will be used for encryption. Secret key is XOR with the red matrix resultant bit will decide, in which component of the image the message bit will be hidden i.e., Blue or green component. If the resultant XOR is 0 then hide the bit in LSB of blue and if 1 then hide the bit in green. To retrieve the message, get the key, take red matrix and XOR with it, if the resultant bit is 1 then note the LSB of green and if 0 then note the LSB of blue component.

Manoj Kumar Ramaiya , Naveen Hemrajani , Anil Kishore Saxena in their proposed steganography method [16] used symmetric encryption using SDES, resulting in increased security for the embedded message. For encoding of the secret image input the pixel one by one in the des encoding function will generate the encoded secret image. Divide each pixel of the secret image into 4 parts/2 bit each. Insert these pixel values into the LSB position of the first four pixels in the cover image one by one. For decoding take 2 bits LSB from each pixel value of stego image. Concatenated four 2bit LSB get 8 bits of encrypted secret image. These 8 bits are input to the decoding Function using the same parameter but keys value used in reverse order getting the first pixel value of the secret image. Size of the secret image taken is 64X64 and embedding capacity of 25%, and PSNR (average of all experiments)= 53.9DB.

Shubhi Mittal, Shivika Arora, Rachna Jain in their research [17] have proposed a steganography method based on Asymmetric cryptography. Algorithm used for encryption is RSA. Message will be encrypted using a public key and generate a cipher text and will be embedded in the carrier image. Retrieve the message just by taking lsb from the carrier message and generate cipher text. Decryption of cipher text will be done only by private key. Prime number size advised 100 digit or more. Future developments can be used for image, audio, video steganography.

Image Steganography on Gray and Color Image using DCT Enhancement and RSA with LSB Method [18] have proposed a steganography method which uses RSA and DCT for encryption and enhancement of the carrier image. Take an image RGB or GRAY scale, pick two large primes and calculate the totient function. Now encrypt the message using a public key. Calculate LSB of every pixel of the input image. Perform LSB on the input image to embed text into the original RGB image. LSB = mod((I(i, j)). Where I am Encrypted image and i, j is the size of the picture. Set back LSB of the red image with every bit of the message to be hidden individually. Apply DCT on Stego image for enhancement. This process can apply on both grayscale or color images. For color image change RGB to YCBCR format. Take the Y component of the image and find the maximum value within a matrix. Split the picture into blocks of blocksize. Apply DCT on the local block, then find the ratio of local block. Find the value of local background illumination. Finally, merge the blocks with row and column. Apply block processing on merged blocks. Alter YCBCR to RGB image to get a final enhanced stage image. Extraction is done using a private key after retrieving the cipher text. DCT will be used in enhancement and will provide more security against steganalysis.

Image Steganography Using AES Encryption and Least Significant Nibble [19] have proposed another Steganography method using symmetric key encryption with the help of Java AES library. First message is encrypted using AES then Nibbles from each byte of the message are extracted. The most significant nibble is extracted first, followed by the least significant nibble. The lower nibble of each image byte are then masked and the message nibble is then stored in the image nibble. This is done using the formula, Image Byte = (Image Byte AND 0xF0) OR Message Nibble.

Extraction is done by first extracting the contents of the least significant nibbles of the first 16 image bytes. This gives us the encrypted message then we can decrypt the message using the key used for encryption.

Enhancing security of images by Steganography and Cryptography techniques [20] uses a double random phase encoding (DRFE) algorithm and uses steganography technique as pre-processing layer to secure the image. Processing time is adequate and immune to noise (an essential factor taken into consideration during wireless communication).

In the paper, Assessment of composite materials on encrypted secret message in image steganography using RSA algorithm [21], they have used asymmetric RSA to insert the secret message in the blue component of the RGB image. Message will be converted to cipher text then will be embedded into each LSB of the carrier image. To recover the secret message, extract the LSB bit of all the BLUE components, first combine the 8 bits and apply the decryption algorithm for RSA to rebuild the message.

An Image Steganography Algorithm using LSB Replacement through XOR Substitution [22], has proposed a LSB based image steganography in RGB image domain. Entered message each bit will be XOR with the Second bit of the RGB values. To recover the encoded message take the second bit in image of each RGB value and again XOR it with respective LSB, this way we can retrieve the message.

High Capacity data hiding using LSB Steganography and Encryption [23], proposed method depicts a typical cryptographic system based on classical encryption techniques i.e. substitutions and transpositions. Transposition technique changes the order of the letters in a message. Letter frequencies are preserved in the ciphertext. Encrypted messages will be hidden in the image. Key will be our transposition table. Encrypted messages will be embedded in RGB for each components in LSB. To retrieve the message note LSB of each RGB value and reconstruct the encrypted message. Only the authorized user can decrypt the message using a shared key.

A Novel Steganography Method for Image Based on Huffman Encoding [24] paper give’s an method that how Hoffman coding can be used to build your steganographic model. First identify if the whether your cover image size greater than eight time the size of your secret image. If condition satisfies go ahead or else find new cover image. Calculate Huffman coding table of the secret image. Find the Huffman encoded binary bit stream of secret-image by applying Huffman encoding technique using Huffman table obtained. Calculate size of Huffman encoded bit stream. Store the size of the stream in first 8X8 block of the cover image. Change the LSBs of the cover image excluding the first 8 X 8 block of pixels for every bit of Huffman encoded bit stream found. Change the LSBs of the cover image to embed the Huffman table found in excluding the first 8 X 8 block of pixels and the pixels used. Result obtain is stego image. To extract the message read first 8X8 pixel from stego image and use it to construct the Huffman table. With the help of Huffman table we can reconstruct the message. Compression is lossless.

Compressive optical steganography via single-pixel imaging [25] is proposing a steganography scheme based on single pixel imaging architecture. Proposed systems apparatus consist of a Bucket detector, a DLP, a host image, a ADC (analog-to-digital converter). Scheme work in the frequency domain. Secret image is Fourier transformed to its respective modulated pattern (or Fourier based fringes) and then projected on the host image with the help of DLP and the stego image (i.e., Host image + Modulated pattern) is extracted using a single bucket detector. Before projecting the modulated patterns onto the host image it is randomly mapped (so the random position is our key to extract our secret image) so that only authorized users can extract the message. In these research thesis they have brought compressive sensing into the domain of steganography for the first time.

Results cc value between host-image and stego-image noted- 0.9776 cc value between secret image and extracted image noted- 0.9956.

4. Conclusion

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sr  No. | Paper | type | algorithm | Performance factor mentioned | Future work  mentioned | Secret  Type(specified) |
| 1 | An improved inverted LSB image steganographhy | LSB based steganography | inversion bits algorithm | PSNR=55.2(DB) | other bit combinations of cover image pixels  can be considered. | Image |
| 2 | Detecting LSB  Steganography in  Color and Gray-  Scale Images | LSB based steganography | RS steganography | NA | RS Steganalysis for palette images can be applied | Image |
| 3 | Enhancing the Security and Quality of  LSB based Image Steganography | LSB based steganography | RC4 algorithm with LSB replacement | PSNR=55.25(DB) | three  bits can be considered which provides 8 different bit patterns  improving the possibilit | Image |
| 4 | An LSB Data Hiding Technique Using Prime Numbers | LSB based steganography | Embedding Algorithm | Max PSNR = 10(log(L^2/WSE)) | NA | Image |
| 5 | Detection of LSB steganography via sample pair analysis | LSB based steganography | Sample pair Algorithm | εm = |X2m+1| − |Y2m+1|.(i.e the accuracy of the hidden message length) | NA | Both |
| 6 | Relating the embedding efficiency of LSB Steganography  techniques in Spatial and Transform domains | LSB based  steganography | F5 Embedding  algorithm | PSNR=56.2 | matrix  embedding with binary hamming codes to get better embedding efficiency which still can be improved with other  codes also. | Gray-scale images |
| 7 | Design of Image Steganography using LSB XOR Substitution Method | LSB based  steganography | LSB XOR substitution method | PSNR  Input image 34.413(DB) Carrier image 53.7558(DB) | NA | RGB images |
| 8 | An Improved LSB based Image Steganography Technique for RGB Images | LSB based steganography | Algorithm to insert data image into the cover image | PSNR  55.9238(DB) | In future, random plane selection can be utilized for replacing bits with Least significant Bit (LSB) | RGB images |
| 9 | Enhanced Data Hiding Capacity Using LSB-Based Image Steganography Method | LSB-Based Image Steganography | Embedding  algorithm | SNR(1-bit)  96.6594 | Future work should focus on hardware implementation of more complex random-based LSB mechanisms, as well as optimizing the design speed and power | Image |
| 10 | Evaluation of Various LSB based Methods of Image Steganography on GIF File Format | LSB based  steganography | Knapsack | NA | security of the steganography method being used can be increased as the data hiding capacity increases . | GIF |
| 11 | New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check | LSB based  steganography | Data encryption -AES (Advanced Encryption Standard) | NA | the proposed method can bd combined with ACM encryption. | Image |
| 12 | Image Steganography using Inverted LSB based on 2nd, 3rd and 4th LSB pattern | LSB based steganography | LSB based on 2nd 3rd and 4th lsb | PSNR(dB)=  51.1558 | NA | Image |
| 13 | A New Approach for Data Hiding with LSB Steganography | LSB based steganography | Pseudorandom  Number 4 state table | NA | Can work with Image hiding in RGB Scale. | Both |
| 14 | A Novel Secure Model: Image Steganography with Logistic Map and Secret Key | LSB based steganography | Random insertion of message bit. Key will be the seed value | PSNR=55.91DB (number of message bits 233016) | NA | Text |
| 15 | A-new-approach-for-LSB-based-image-steganography-Karim-Rahman | LSB based  steganography | Symmetric cryptography | PSNR=53.7(DB) | NA | Both |
| 16 | Security Improvisation in Image Steganography using  DES | LSB based  steganography | Symmetric  Cryptography  DES | PSNR=53.9(DB) | NA | Image |
| 17 | PData Security using RSA Encryption Combined  with Image Steganography | LSB based  steganography | Asymmetric  Cryptography  RSA | NA | Can be implemented in audio, video and image | text |
| 18 | Image Steganography on Gray and Color Image using DCT Enhancement and RSA with LSB Method | LSB based  Steganography and DCT | Asymmetric  Cryptography  RSA  And DCT | PSNR=  63.01  (average of proposed algorithm) | Can use this algorithm in 3D image | both |
| 19 | Image Steganography Using AES  Encryption and Least Significant Nibble | LSB based  steganography | Symmetric  Cryptography  AES | PSNR=50.152 for 128 byte, 48.769  For 256 byte, 46.860 for 512 bytes and 44.525 for 1024 bytes | NA | text |
| 20 | Enhancing security of images by Steganography and  Cryptography techniques | LSB based  steganography | DOUBLE RANDOM PHASE ENCODING | PSNR=29.65 | NA | Image |
| 21 | Assessment of composite materials on encrypted secret message in image steganography using RSA algorithm | LSB based steganography | Asymmetric Cryptography RSA | Embedding processing time=0.0253205(average in ms), Extraction processing time=0.0257037 | NA | Text |
| 22 | An Image Steganography Algorithm using LSB Replacement through XOR Substitution | LSB based steganography | XOR operation | PSNR=61.998 | NA | Text |
| 23 | High Capacity data hiding using LSB Steganography and Encryption | LSB based  steganography | Symmetric key using transposition encipherment | PSNR=51.60(average result of experiment performed) | The method can be further extended for more data hiding techniques | Text |
| 24 | A Novel Steganography Method for Image Based on Huffman Encoding | LSB based steganography | Huffman coding | PSNR=57 (in DB) | NA | Text |
| 25 | Compressive optical steganography via single-pixel imaging | Single pixel imaging based steganography | GPRA and CO | CC of host,stego= 0.9776 | NA | Image |

5. Work-cited

1) TY - BOOK AU - Akhtar, Nadeem PY - 2014/02/07 T1 - An improved inverted LSB image steganography DO - 10.1109/ICICICT.2014.6781374

2) J. Fridrich, M. Goljan and Rui Du, "Detecting LSB steganography in color, and gray-scale images," in IEEE MultiMedia, vol. 8, no. 4, pp. 22-28, Oct.-Dec. 2001, doi: 10.1109/93.959097.

3) N. Akhtar, P. Johri and S. Khan, "Enhancing the Security and Quality of LSB Based Image Steganography," 2013 5th International Conference and Computational Intelligence and Communication Networks, 2013, pp. 385-390, doi: 10.1109/CICN.2013.85.

4) S. Dey, A. Abraham and S. Sanyal, "An LSB Data Hiding Technique Using Prime Numbers," Third International Symposium on Information Assurance and Security, 2007, pp. 101-108, doi: 10.1109/IAS.2007.37.

5) umitrescu, S., Wu, X., Wang, Z. (2003). Detection of LSB Steganography via Sample Pair Analysis. In: Petitcolas, F.A.P. (eds) Information Hiding. IH 2002. Lecture Notes in Computer Science, vol 2578. Springer, Berlin, Heidelberg. <https://doi.org/10.1007/3-540-36415-3_23>

6) Malathi, P., and T. Gireeshkumar. "Relating the embedding efficiency of LSB steganography techniques in spatial and transform domains." *Procedia Computer Science* 93 (2016): 878-885.

7) Wu, Nan-I., and Min-Shiang Hwang. "Data Hiding: Current Status and Key Issues." IJ Network Security 4.1 (2007): 1-9.

8) A. Singh and H. Singh, "An improved LSB based image steganography technique for RGB images," 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2015, pp. 1-4, doi: 10.1109/ICECCT.2015.7226122.

9) Gupta, Himanshu, Ritesh Kumar, and Soni Changlani. "Enhanced data hiding capacity using LSB-based image steganography method." *International Journal of Emerging Technology and Advanced Engineering* 3.6 (2013): 212-214.

10) Tiwari, Namita, and Dr Madhu Shandilya. "Evaluation of various LSB based methods of image steganography on GIF file format." International Journal of Computer Applications 6.2 (2010): 1-4.

11) Elmasry, Wisam. "New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check." Sādhanā 43.5 (2018): 1-14.

12) Rafrastara, Fauzi Adi, et al. "Image Steganography using Inverted LSB based on 2 nd, 3 rd and 4 th LSB pattern." *2019 International Conference on Information and Communications Technology (ICOIACT)*. IEEE, 2019.

13)Prashanti, G., and K. Sandhyarani. "A new approach for data hiding with LSB steganography." Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2. Springer, Cham, 2015.

14)Ulker, Mehtap, and Bilgehan Arslan. "A novel secure model: Image steganography with logistic map and secret key." 2018 6th International Symposium on Digital Forensic and Security (ISDFS). IEEE, 2018.

15)Karim, SM Masud, Md Saifur Rahman, and Md Ismail Hossain. "A new approach for LSB based image steganography using secret key." 14th international conference on computer and information technology (ICCIT 2011). IEEE, 2011.

16)Ramaiya, Manoj Kumar, Naveen Hemrajani, and Anil Kishore Saxena. "Security improvisation in image steganography using DES." 2013 3rd IEEE International Advance Computing Conference (IACC). IEEE, 2013.

17)Mittal, Shubhi, Shivika Arora, and Rachna Jain. "PData security using RSA encryption combined with image steganography." 2016 1st India International Conference on Information Processing (IICIP). IEEE, 2016.

18)Singh, Yash Kumar, and Sudhanshu Sharma. "Image steganography on gray and color image using DCT enhancement and RSA with LSB method." 2016 International Conference on Inventive Computation Technologies (ICICT). Vol. 3. IEEE, 2016.

19)Sheth, Utsav, and Shiva Saxena. "Image steganography using AES encryption and least significant nibble." 2016 International Conference on Communication and Signal Processing (ICCSP). IEEE, 2016.

20)Bukhari, Sadaf, et al. "Enhancing security of images by Steganography and Cryptography techniques." 2016 Sixth International Conference on Innovative Computing Technology (INTECH). IEEE, 2016.

21)Karthikeyan, N., et al. "Assessment of composite materials on encrypted secret message in image steganography using RSA algorithm." Materials Today: Proceedings (2021).

22) Bhuiyan, Touhid, et al. "An image steganography algorithm using LSB replacement through XOR substitution." 2019 International Conference on Information and Communications Technology (ICOIACT). IEEE, 2019.

23) Laskar, Shamim Ahmed, and Kattamanchi Hemachandran. "High Capacity data hiding using LSB Steganography and Encryption." International Journal of Database Management Systems 4.6 (2012): 57.

24)Al-Mazaydeh, Wa'el Ibrahim A. "Image steganography using LSB and LSB+ Huffman code." International Journal of Computer Applications 99.5 (2014): 17-22.

25)Zhang, Chenggong, et al. "Compressive optical steganography via single-pixel imaging." Optics Express 27.9 (2019): 13469-13478.