ISSN: 2321-8363
Impact Factor: 6.308
(An Open Accessible, Fully Refereed and Peer Reviewed Journal)

Analytical Study of Image Steganography Techniques in the Context of Present Scenario

Ravi Saini[1]; Kamaldeep Joshi[2]; Rajkumar Yadav[3]; Rainu Nandal[4]

[1]*Research Scholar, UIET MDU Rohtak, ravigpsanghi@gmail.com*
[2]*Assistant Professor, UIET MDU Rohtak, kamalmintwal@gmail.com*
[3]*Assistant Professor, UIET MDU Rohtak, rajyadav76@rediffmail.com*
[4]*Assistant Professor, UIET MDU Rohtak, rainu_nandal@yahoo.com*

DOI: 10.5281/zenodo.6787159

Abstract

Today is the world of Internet Technology. Internet technology becomes our part of life and making many changes of our real life. Most of the people have smart phones and they are using various applications like Whatsapp, Facebook, Paytm, Phone Pay, Twitter etc. in their daily routine life with the help of Internet Technology. All these types of applications needs some form of information transfer between two persons or between one person and server. As the various applications are used for information sharing, so the risk of various attacks and unwanted access by some person also increases. To avoid these types of attacks and authorized access information hiding is very crucial concept. In the today scenario, information is shared in digital form. So, to protect this digital information is quite crucial. Information Hiding is the technology of camouflaging the vital data which uses cover file, digital image processing, cryptography, signal processing, compression techniques etc. for the safety of information. In this paper, we will do the analytical study the various approaches of image steganography in the present scenario.

***Keywords**:* Image, Steganography, Cryptography.

1. Introduction

The secure way of information sharing over the network is the need of time for commercial purpose, military purpose, industries, copyright protection etc. So, to find some way to communicate covertly over the network is the need of the time. So, to fulfill this demand, the concept of Steganography is very important which is based upon the concept of hiding the existence of message [Rodrigues *et al.* (2004)].

Steganography is the technique which hides any type of information within some cover media. The word Steganography is combination of two Greek words “Steganos” and “Graph”. Steganos means “hidden or covered” and Graph means “to write” [Gutub and Fattani (2007)]. So, we can say that Steganography means hidden or covered writing. Steganography has also been used in the ancient times by the use of invisible ink, microdots, lime or any other citrus liquids, some meaningful paragraph whose every fixed letter sequence form the secret message etc. [Norman (1973), Kahn (1973), Johnson *et al.* (1998)]. The example of steganography is given below:

SIVAM AND ADISH DINED HAPPILY.

If receiver extracts the second letter of each word of the above message then he will get the secret message “INDIA” [Eugene and Edward (1999)].

We can also obtain the secret communication in Steganography by using image file, audio file or video file and inserting the message in carrier media such that the alteration in carrier media is not seen by human eye in open environment [Amirtharajan *et al.* (2010a)]. Simmons was the person who initially describes this concept in 1983[Simmons (1983)]. This concept was further described in detail by Anderson in [Anderson (1996a)]. Cryptography is also used for secure communication but it somewhat different from Steganography. Both Steganography and Cryptography is used for secure transfer of information between two nodes. Cryptography is the technique that changes the meaning of message such that it is not understandable by intermediate person whereas Steganography is the technique which hides the information itself within some cover media like image file, audio file, and video file etc. so that this information is not visible to the third party [Anderson and Peticolas (1998)]. We can achieve highly secure communication if we use blend of Cryptography and Steganography for information transfer.

Image file is the excellent cover media for hiding the information. There are many image steganography techniques that have been developed for secure information transfer [Johnson *et al.* (2001)]. Firstly, if we apply some cryptography approach to alter the plain file into cipher file and after that the cipher file is transferred using some steganography technique then we will get very good result which provide dual layer security to our information [Abbas (2010), Amritharajan *et al.* (2010b), Amritharajan *et al.* (2010c), Bender *et al.* (1996), Peter (2002)]. The steganographic model is given in Figure 1. Here, the cover file is file in which data is concealed. Cover file may be text file, video file, audio file and image file. The message is inserted in the cover file using insertion algorithm. The message is inserted using stego key which is shared between sender and receiver only. The cover file after the insertion of message becomes the stego file. The retrieval algorithm is applied on the stego file at the receiver end to get the original information. There will be very minute alteration between cover object and stego object so that human eye cannot detect the difference between them.

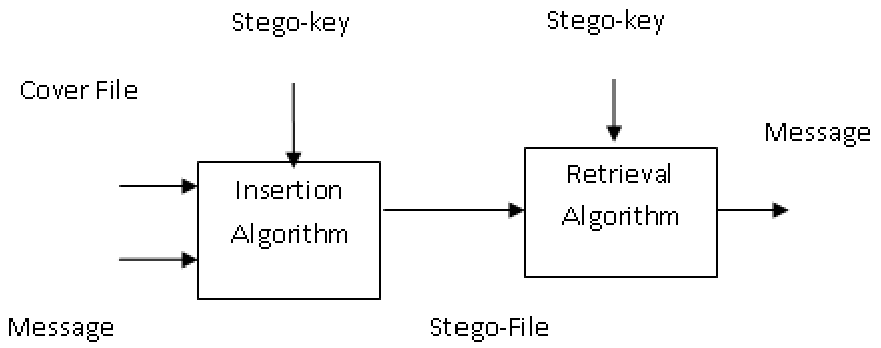

Fig. 1. Steganography Model.

2. Information Hiding Techniques

We can divide information hiding techniques into three categories:

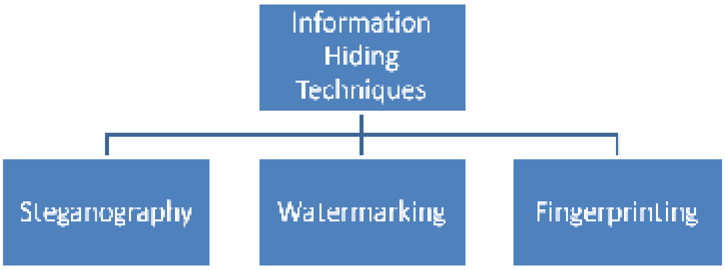

Fig. 2. Information Hiding Techniques

2.1 Steganography

Steganography is the technique which hides the any type of information within some cover file like image object, video object, audio object and text object. The word Steganography is combination of two Greek words "Steganos" and "Graph". Steganos means "hidden or covered" and Graph means "to write" [Gutub (2007)]. So, we can say that Steganography means hidden or covered writing.

2.2 Watermarking

Watermarking is the process in which we insert some type of vital message like owner details (name, age, company detail, address) in the digital object so that its authentication can be done properly and the copyright of the owner is protected. Watermarking is the very crucial technique for protection of the digital data present on the network [Hartung and Kutter (1999)].

2.3 Fingerprinting

Fingerprint is the impression given by human finger on some paper or other media [Lindkvist (2000)]. In today scenario, it is used for marking attendance, secure authentication, aadhaar verification, banking purpose etc. It is used for removing the forgery attacks on the owner of some valuable thing [Brassil (1994)]. It is also very crucial that we should protect the fingerprint data. It is also very challenging to protect the fingerprint data in today scenario as it is available on the server and can be accessed by third party over the network.

3. Steganography Vs Cryptography

Today life is going at the fast rate and the reason behind this fast life is the use of technology specially internet. Everyone is looking to move at rapid rate due to the use of internet in his life. Everyone is affected by the internet either directly or indirectly. Digital data play very crucial role in this era of internet. Today, digital data is used at the tremendous level, so the security of digital data also becomes very critical issue. There are two types of techniques which solve our problem of secure digital data up to some extent. These two techniques are known as Cryptography and Steganography. Both provide solution to the problem of secure information transfer but there is difference between both the technologies. Cryptography is the technique that changes the meaning of message so that it is not understandable by intermediate person whereas Steganography is the technique which hides the information within some cover object so that this information is not visible to the attacker [Anderson and Peticolas (1998)]. Steganography is better than cryptography because steganography decrease the chances of suspicion over the data transfer. Steganography protects both information and source of information whereas cryptography protects information only [Stalling (2005)]. We can achieve highly secure communication if we use blend of Cryptography and Steganography for information transfer [Judge (2001), Krenn (2004)].

4. Image Steganography Techniques

The digital steganography has been used since 1998 in the modern era. The most popular and traditional approach for using steganography in recent time is LSB which hides the message in last bits of every pixel of the images. There are many techniques that have been invented since LSB. In this section, we will explore some techniques of image steganography from 2016 to 2020.

[Subhedara and Mankarb (2016)] suggested new method of data hiding in the frequency domain. This technique uses the concept of QR factorization and redundant discrete wavelet transform (RDWT) for concealing the message. RDWT allows avoiding various problems that occurred in energy level change in the input signal. QR factorization decreases the computational complexity of the algorithm. This technique improves the efficiency in the form of imperceptibility, hiding capacity and robustness.

[Zhou *et al*. (2016)] proposed new approach of image steganography. This approach uses blend of cryptography and steganography. The RSA algorithm of cryptography is used in combination of improved LSB method for providing two layer of security. It also uses the concept of digital security and secure key for providing additional level of security. It will provide higher value of PSNR than classical LSB method.

[Son (2016)] proposed new method for image steganography which is based on 2k correction method and Canny Edge detector. It also uses the Huffman coding table as secret key which is shared with receiver party. Canny edge detector selects the edge pixels of the image where the data is to be inserted. The selected pixels are then sorted in some order. After that Huffman coding and 2k correction method is applied for achieving the target. It provides better imperceptibility, hiding capacity and less alteration in the image.

[Dadgostar and Afsari(2016)] offered new method of image steganography which is depends upon fuzzy system and modified LSB method. The method suggests that the insertion of message in edge areas is better as compared to the plain areas because the change in edge pixels is unnoticeable as compared to the plain areas. Fuzzy based edge detector system find the edge pixels where the message is to be inserted and modified LSB method to covert the message in the cover file.

[Jiang *et al.* (2016)] suggested two new approaches of image steganography in collaboration with quantum physics. This approach gives us new idea of quantum steganography. In quantum steganography, the data would be hidden in quantum slices or quantum images. This paper gives two new techniques for hiding the data in quantum slices. In one approach, the data is hidden by using tradition LSB method and in another approach data is hidden using block of pixels. It gives balance between embedding payload data and stego image quality.

[Jain and Lenka(2016)] proposed new approach of hiding the patient sensitive information in medical images. This technique also uses blend of cryptography and steganography for providing duplex layer of security. This technique uses classical LSB method for hiding the patient information. Various analyses have also been done on the basis of PSNR, MSE and Histogram. This approach shows its importance in the field of biomedical.

[Bhasme *et al.* (2016)] proposed another approach for securing the e- Payment System using combination of cryptography and steganography. Blowfish Algorithm is used for achieving the target of cryptography. It is helpful for reducing the risk of Phishing and can provide very high security in E-Commerce.

[Kaur *et al.* (2016)]proposed new method of image steganography which depends upon hybrid approach. It modifies the traditional LSB method of secure communication. It increases the data capacity to be hidden in the image. It uses the LZW compression scheme to compress the data that is to be hidden in the cover file. It provides very minute alteration in the cover object so that the change is not visible by HVS.

[Swain (2016a)]suggested two new approaches of data hiding in spatial domain. In one approach, he hide one bit in one pixel whereas in another approach he hide two bits in one pixel. He used the concept of flipping of pixels bits group. After flipping of pixel bits groups, the property of cover image does not change a lot. The final analysis shows the improvement in security features.

[Makwana and Chudasama(2016)] developed another technique which is based on dual steganography. In this technique, both cryptography and steganography is used for securing the data. It provides duplex layer of security. It provides good value of PSNR value. Its implementation is complex.

[Thenmozhi and Devi (2016)] offered another new approach for hiding the data within cover image. This technique uses the blend of the compression and steganography. Compression of the message is to be hidden has been done by using SPIHT. After compressing of the data, it is embedded using LSB method. PSNR and MSE analysis is also done in the result analysis part.\par

[Setiadi *et al.* (2017)] proposed a new approach of image steganography in frequency domain for securing the banking transactions. It uses both the cryptography and steganography collectively for dual security. Cryptography techniques One Time Pad and Vernam, Chiper is used by author in conjunction with Discrete Cosine Transform (DCT) . Result analysis includes PSNR, MSE and NCC analysis. The author also claimed that it is resistant to compression process.

[Muhammad et al. (2017a)] offered another technique for secure communication through image as cover file. It uses adaptive LSB substitution method for insertion and retrieval of the message. It uses multi level encryption algorithm (MLEA) on secret message before hiding the message in image. The two level encryption algorithm (TLEA) is also applied on the secret key for better results. The results shows better level of security, good hiding capacity, less computational complexity and less distortion in image quality.

[Debnath *et al.* (2017)] offered another approach in the field of image steganography using quantum physics. It uses the concept of quantum dot cellular automata (QCA). It uses the reversible procedure for encoding and decoding of the message to be hidden. Feymen Gate is also used in this technique for achieving reversible features. Traditional LSB method is used for hiding the data. MATLAB is used for giving the input to QCA circuit. MSE, SNR and PSNR have also been calculated to show its effectiveness.

[Muhammad *et al.* (2017)] suggested new approach of concealing information using image steganography. Mortan Scanning LSB Method is applied for converting the data within the cover object. The data is concealed in I plane of cover image in HSI form. The three layer encryption algorithm (TLEA) is also applied on the secret data before camouflaging it in the cover object for providing supplementary layer of security. Results shows gain in performance with respect to the state of art approaches.

[Rajendran and Doraipandian (2017)] proposed another method of image steganography on the basis of Chaotic Map and classical LSB Method. One dimensional Logistic System is used to generate the chaotic map for concealing the data. The pixels for insertion of the message is chosen randomly for increasing the security of the data. PSNR and Histogram analysis has been done in the result part of the paper. The proposed method shows the improvement over the other traditional methods.

[Ardiansyah *et al.*(2017)] suggested a new approach for data hiding in the cover file. The approach uses the coupling of cryptography with steganography. It uses 3 DES for changing the plaintext message into cipher text message. Discrete Wavelet Transform (DWT) is used to convert the cover image into 4 subbands. The data is hidden in the three subbands LH, HL, HH using classical LSB method. Inverse DWT is applied at the receiver end to extract the required message. PSNR, MSE and NC analysis have been done in the last to show the strength of the proposed approach.

[Heidari *et al.* (2017)]offered another approaches of hiding the data within RGB image using quantum processing and traditional LSB approach. The author proposed three approaches on RGB image. The first algorithm hides the data in one channel using classical LSB method, the second algorithm hide the data using LSB and Xor operation. The third algorithm hides the data within two channels of the cover image. The result analysis include MSE, PSNR, BER and Histogram analysis.

[Chakraborty *et al.* (2017)] proposed a new approach in the field of image steganography. It uses modified median edge detector (MMED) to select the parts of the image where the data can be inserted without unnoticeable alteration in the cover file. It provides higher data payload with very less distortion in the image. It also increase the security features of the image. Results shows the improvement over the classical approaches.

[Miria and Faezb (2017)] suggested a new approach for hiding the information in cover image using Genetic Algorithm and Transform Domain. GA and Transform domain select the areas where the information is to be hidden. The message would be inserted using the classical approach of LSB. The encryption is also used in coupling with steganography for providing dual layer of security. It will show very less distortion in the image quality.

[Soleymani and Taherinia (2017)] offered another approach of hiding the scanned document image into another cover object. The halftoning algorithm is used for converting the scanned document image into sparse matrix of binary sequence. This binary sequence is hidden in the cover image pixels three LSBs. The pixels which are sensitive to HVS is not chosen for insertion of message. The approach shows the better embedding rate.

[Mohammed *et al.* (2018)] suggested new method which uses seven segment display pattern is used as secret key. The message is inserted on the basis of seven segment display pattern. This approach depends upon LSB Technique but offered a novel approach for camouflaging the secret information by generating a highly secure secret key constructed from any available digital object. It provides high imperceptibility and full capacity embedding of covert data.

[Mukherjee *et al.* (2018b)] suggested a new method which is based on the uses Mid Position Value and Arnold Transform. The covert communication is achieved by using Arnold Transform. It also uses the middle value of picture element for insertion and retrieval of the secret code. It promotes high embedding capacity and imperceptibility.

[Joshi *et al.* (2018)] proposed a new technique for covert communication in spatial domain. This technique is based on 7th bit of pixel for insertion and retrieval of the message. The maximum variation in the picture element value of cover image will range from +2 to -2. This technique embeds two bits in each pixel. It will take two things into account, one is current pixel value and one is its successive value. It provides finer value of PSNR value than some traditional methods like LSB Method, SCC Method, PIT Method, FMM Method etc. The author has also shown the histogram analysis of cover object and stego object which shows very less deviation in picture element values of cover image.

[Kasapbas and Elmasry (2018)] proposed another method for securing the information over the internet. This is color image based steganography technique. This technique make use of LSB method and encryption method at the same time. Compression of the message to be concealed is also being done before applying cryptography and steganography. CRC – 32 checksum, Gzip compression, AES, Chi - Square analysis used in this technique. This approach improves the visual features of stego image.

[Swain (2018b)] suggested a new approach of concealing the information by using image as cover media. This approach uses the blend of LSB technique and PVD technique. It will provide higher data capacity and less distortion in the image quality. Pixel Difference Histogram (PDH) analysis is applied in this technique for evaluating the performance the proposed technique for secure communication.

[Hu *et al.* (2018)] suggested another approach in the field of image steganography. This technique uses the concept of neural network. Two neural networks generator and extractor are used for achieving the goal of steganography. The message to be inserted is mapped into the noise vector. This vector is inserted in the host image using generator neural network without any alteration in the image. The extractor neural network extracts the message from stego image. The result shows the improvement over the state of art approaches.

[Muhammad *et al.* (2018c)] offered another approach of image steganography which makes use of adaptive LSB method. The secret message is passed through image scrambler which converts it into encrypted secret message. Iterative magic matrix encryption algorithm (IMMEA) is used for the purpose of encryption of the message. The cover image is converted into HSV Color space. The encrypted message is inserted in the V plane of the color space. The result shows the effectiveness of the approach with respect to the state of art techniques. It will increase the imperceptibility level and decrease the chances of deviation by open eye.

[Zhang *et al.* (2018)] proposed another approach of image steganography in frequency domain. It uses the latent dirichlet allocation (LDA) topic classification and discrete cosine transform. LDA topic classification classifies the images from image database. The selected images from one group are applied for DCT. The message to be inserted is converted into binary sequence and classified into the different segment. The cover object from the group which matches with the segment of message is selected for insertion of the message. The result shows the robustness of the technique against various steganalysis attacks.

[Gaurav and Ghanekar (2018)] suggested another technique of image steganography which is based on Canny edge detection, dilapidation morphological operator and XOR operation. Canny edge detection selects the edge pixels for insertion of the message. Dilapdation morphological operator optimizes the selected pixels. Finally XOR technique is used for alteration in the LSB of the selected pixels. The results shows the better hiding capacity, imperceptibility, robustness and less computational complexity.

[Liao *et al.* (2018)] proposed another approach of image steganography using reference table. Traditional methods using reference table uses the concept of Two Dimensional reference table for insertion of the message. The author has proposed two methods using x-dimensional reference table. First method uses cubic reference table for its implementation. The second method uses cubic reference table and pixel value difference method for its implementation. The result shows the effectiveness of the proposed techniques with respect to traditional techniques.

[Younus and Hussain (2019)] offered new method which uses Vigenere Cipher and Huffman Coding for achieving the covert communication. Huffman Coding is used for devising the insertion and retrieval algorithm. It also uses compression and encryption of the data for securing the data. It provides Better PSNR Value and high embedding capacity.

[Li *et al.* (2019)] suggested new method which automatically generates steganography features of image. It uses image caption model for generating the features of image in natural language automatically. Dynamic Synonym Substitution algorithm is used for generating the alternate words with their synonyms for the generation of sentence. Subjective evaluation is also being done for this approach. Some popular metrices also being used for image description evaluation like BLEU, METEOR, ROUGE etc. It increases capacity and provide security against the Steganalysis.

[Liu and Lee (2019)] suggested a new method which uses three neighbor pixels for insertion of message. The intermediate picture element value in the block is subtracted from the maximum and minimum picture element value. The required bits are inserted in the maximum pixel value and minimum pixel value as per the deviation with the middle picture element value. At the receiver end, the specified pixels are read in row and column order and the difference are calculated. If the difference is maximum while reading in rows, it is recorded as 1. If the difference is maximum while reading in column it is recorded as 0. It provides better PSNR value.

[Sarmah and Kulkarni (2019)] offered a new approach which is based on frequency domain for achieving covert communication. This technique uses improved Cohort Intelligence for secure communication. Cohort is used in this technique which is collection of candidates. Each candidate is expressed by number of factors. Every candidate also monitors another candidate for its respective properties. Its computational time is less. It has very less embedding capacity.

[Kaw *et al.* (2019)] suggested a new method which is used for hiding patient information in the image. It prevents unauthorized access to client's sensitive data. The original patient information image will act as cover image. Patient information is secured in the medical images using data algorithm. This algorithm is combination of two parts pixel permutation and pixel replacement. OPR i.e. Optimal Pixel Repetition is also used in this technique for insertion and extraction of the sensitive data within medical image.

[Maniriho and Ahmed (2019)] suggested a new approach which firstly the cover object is divided into blocks of size 2x1. Then, calculate the deviation between picture element in each block i.e. d=z-y. Identify all values which satisfy the first condition (i.e 0<d<=2) and second condition (i.e -1>=d>=-2). Now, the trace table is generated. Assign value 0 to the pair if above conditions satisfy. If the pairs are unchanged then assign the value 1. Find modified difference d'=d+b where b is the secret bit. Compute z'=d'+z where z' is the stego pixel. At the receiver end, the message is extracted by modulus function. Calculate d''= z'-y', If TRT= 0 then message bit is d'' mod 2 else message bit is not present.

[Zhang *et al.* (2019)] offered another approach of covert communication. This technique uses Joint Distortion Measurement for insertion and retrieval of the message. It works only on binary image. Distortion Measurement measures the flipping effect of pixels. It means that if we change the neighbor pixels then what affect occurs on image. If we measure the flippability of the pixel precisely then the encoder can flip the suitable pixel smartly such that all LSB of the specified pixels by secret key will be secret message. At the receiver end, the LSB of all the specified pixels are extracted which will be the required message.

[Li *et al.* (2019)] suggested another new method of data hiding which is based on reversible data hiding (RDH) approach. This method will depend on bidirectional shifting and double-way prediction. This approach also uses prediction error histogram. The peak point bins are selected from prediction error histogram for insertion and retrieval of the camouflaged data. The message would be inserted in the peak point bins so that there would be very less unnoticed distortion in the image. The technique increases the embedding capacity but reduces the PSNR value a little bit.

[Parmar *et al.* (2019)] offered another approach of data hiding which works on RGB images. It is based on odd and even based steganography. The pixel shifting process is applied on the selected cover object. The image is preprocessed and converted into different RGB plane. Then the message is inserted into the different components using odd and even parts. The improved LSB approach is used to achieve the data hiding. It improves some image steganography metrices.

[Ahmed *et al.* (2019)] proposed another method in the field of image steganography using quantum theory. This new method uses the S–boxes in integration with quantum walks. Quantum walks Substitution boxes

(QWsSB) are used in this approach. QWsSB control the functioning of insertion and reterival algorithm. Result analysis shows the better security, hiding capacity and good visual stego image.

[Qu *et al.* (2019)] proposed another approach of quantum based image steganography. This approach hides the data in quantum images. This approach provides two methods for secure communication. First method uses single pixel for embedding and coding (1, 3, 2). It is called SPE (1, 3, 2) coding. It will insert two qubits in three LSBs of carrier image. The second method uses multiple pixels for embedding and coding (1, 3, 2). It is called MPsE(1 ,3 ,2) coding. Result analysis shows better imperceptibility, hiding capacity and security.\par

[Biswas and Bandyapadhay (2020)] suggested new method of data hiding in images. This technique is based on frequency domain and also uses the concept of Genetic algorithm. This technique also uses the concept of Hash Algorithm and Encryption technique. It will decompose the every bit stream of each plane of cover image into 4 bits each. Random multiple bits are used to embedding of the data. Genetic algorithm is used to increase the robustness of the algorithm. The distortion in the stego image is very less using this technique.

[Liao *et al.* (2020)] proposed another method of image steganography in RGB images. Embedding Channel Payload Probability is used for analyzing different channels for RGB image. The modification probability of all the three channels is increased for getting better performance. It also uses the concept of clustering of embedding impacts on different channels. This technique provides better resistance against steganalysis attacks on color images.

[Liu *et al.* (2020a)] suggested another method of image steganography which is based on halftone image. The pairs of halftone images are selected for data hiding. The pixels pairs are swapped in such a way that there would be very less change in the image. The distortion measurement is also proposed to measure the deviation in the stego object. Further, syndrome-trellis code (STC) is used to minimize the deviation in the stego object. The results show finer imperceptibility, hiding capacity and high security.

[Kadhim *et al.* (2020)] proposed another method of image steganography in frequency domain. It uses the concept of machine learning and dual tree complex wavelet transform (DT- CWT). The DT- CWT will generate the different bands of the cover image. Machine learning technique is used to minimize the retrieval error during extraction of the message. Result analysis includes Retrieval Error, PSNR, SSIM, Bits per Pixel, CF and Histogram Analysis. It will provide better imperceptibility and hiding capacity.

[Gutub and Ghamdi (2020)] offered new method for multimedia image steganography. It will give emphasis on improving the counting based secret sharing for great shares. It will remove some defects of share reconstruction phase by introducing new distribution model. Key size of 64 bits, 128 bits and 256 bits are used in this technique. It is simple and fast technique. It provides reliability and robustness of stego image.

[Sahu and Swain (2020)] suggested another reversible image steganography technique. It hides the data using dual layer approach. It also uses the modified LSB approach for insertion of the message. In the first layer, the method hides two bits in the pixel using modified LSB method and generates intermediate pixel pair (IPP). In the second layer, four bits are hidden using IPP. It provides the better value of universal image quality index (QI) and structural similarity index (SSIM). It will provide better hiding capacity and imperceptibility.

[Shankar *et al.* (2020)] proposed another approach of image steganography in conjunction with cryptography. It also uses the concept of Discrete Wavelet Transformation (DWT). At the first step, the cover image is transformed using DWT. DWT creates many sub bands of the image. This process creates many shadows of the image. These shadows will be encrypted and decrypted using optimal Homomorphic Encryption technique. It will provides better security when compared with other techniques.

[Liu at al. (2020b)] proposed another method of image steganography in frequency domain. It uses Discrete Wavelet Transform and deep learning of neural network. Dense Set Neural Network Model from deep learning is used to select the images from image dataset. This dataset are applied for DWT which generate the DWT coefficients. These DWT coefficients are applied for Zigzag scan which generate the feature sequence. The secure message is also divided into different segments of length feature sequence. The information segments are inserted in the image with the same length of feature sequence. It provides better robustness and security than state of art methods.

[Subhedar and Mankar (2020)] suggested another approach of image steganography which is based on machine learning and framelet wavelet transformation. Singular Value Decomposition (SVD) of Machine Learning is used to select the image group from image set. After that image group is transformed by framelet wavelet transformation. It will generate the various framelet coefficients in which the secret message sequence is inserted. It provides better robustness and imperceptibility.

[Kadhim *et al.* (2020)] proposed another way of data hiding in images in frequency domain. It uses the concept of dual tree complex wavelet transform and machine learning techniques. DT – DWT converts the cover image into various wavelet coefficients. The machine learning classifier selects those wavelet coefficients which meet with the property of secret message. The super pixel algorithm hides the secret message in the selected coefficients. This method provides good hiding capacity, better imperceptibility, robustness and security.

[Pak *et al.* (2020)] suggested another method of image steganography using traditional LSB method. Improved 1 D Chaotic Map is used in this approach for generating various features of cover image. Secret message is hidden in the color image using classical LSB method. The proposed method is analyzed using logistic map, sine map and simulation evaluation. It provides better performance than some other methods.

[Luo et al. (2020)] proposed another method of image steganography in frequency domain. It uses the concept of deep learning, real time images and DCT. The real time images are searched online by using deep learning. The images which meet some specific features are searched by deep learning. These searched images are transformed by DCT for generating different coefficients. The message is inserted by using hash sequence generation. This approach provides better hiding capacity, robustness and higher retrieval accuracy.

5. Analysis of Related Work

There are generally five parameters on the basis of which we assess any steganography technique. These parameters are hiding capacity, robustness, tamper resistance, perceptual transparency and computational complexity. In this section, we assess the various techniques of image steganography that we have studied in the last section on the basis of these five parameters. The hiding capacity, robustness and tamper resistance should be high for a good algorithm. The perceptual transparency and computational complexity should be less for a good algorithm. We will rate three parameters of hiding capacity, robustness and tamper resistance, by three categories, Excellent, High and Normal. We will analyze perceptual transparency and computational complexity by three categories, low, normal and high. We will also analyze the types of different studied technique. We will classify them into four types, spatial domain, frequency domain, quantum steganography and dual steganography (Coupled with cryptography). Table 1 shows the various techniques with their types and parameters. Figure 3 shows the details of various domains used in various papers by using graph in three dimensional. Figure 4 shows the number of paper reviewed year wise.

Table 1. Various Image Steganography Techniques with various Parameters

Author Name	Type	Hiding Capacity	Robustness	Tamper Resistance	Perceptual Transparency	Computational Complexity
Subhedara (2016)	Frequency	High	High	Normal	Low	Normal
Zhou (2016)	Dual	Normal	Normal	Normal	Low	High
Son (2016)	Frequency	Excellent	Normal	Normal	Low	High
Dadgostar(2016)	Frequency	Normal	Normal	Excellent	Low	Normal
Jiang (2016)	Quantum	Excellent	Excellent	Normal	Low	High
Jain (2016)	Dual	Excellent	Normal	Excellent	Normal	Normal
Bhasme (2016)	Dual	Normal	Excellent	Excellent	Normal	High
Kaur (2016)	Frequency	Excellent	Normal	Normal	Low	Low
Swain (2016)	Spatial	Excellent	Normal	Excellent	Normal	Low
Makwana (2016)	Dual	Excellent	Normal	Normal	Normal	High
Thenmozhi(2016)	Spatial	Excellent	Normal	Normal	Low	Low
Setiadi (2017)	Dual	Normal	Normal	Excellent	Normal	High
Muhammad(2017)	Dual	Excellent	Normal	Normal	Low	Low
Debnath(2017)	Quantum	Normal	Excellent	Normal	Low	Normal
Muhammad(2017)	Dual	Excellent	Normal	Normal	Low	High
Rajendran(2017)	Spatial	Excellent	Normal	Normal	Low	Normal
Ardiansyah(2017)	Dual	Excellent	Excellent	Normal	Low	High
Heidari(2017)	Quantum	Excellent	Normal	Normal	Normal	Normal
Chakraborty(2017)	Frequency	Normal	Excellent	Excellent	Normal	Normal
Miria(2017)	Dual	Excellent	Normal	Excellent	Low	High

Soleymani(2017)	Spatial	Excellent	Normal	Normal	Low	Normal
Mohammed(2018)	Spatial	Excellent	Normal	Normal	Low	High
Mukherji(2018)	Frequency	Excellent	Normal	Normal	Low	Normal
Joshi(2018)	Spatial	Excellent	Normal	Normal	Low	Normal
Kasapbas(2018)	Dual	Normal	Normal	Normal	Low	Normal
Swain(2018)	Spatial	Excellent	Normal	Normal	Low	High
Hu(2018)	Frequency	Normal	Excellent	Normal	Low	Normal
Muhammad(2018)	Dual	Normal	Excellent	Excellent	Low	High
Zhang(2018)	Frequency	Normal	Excellent	Normal	Normal	Normal
Gaurav(2018)	Frequency	Excellent	Excellent	Normal	Normal	Low
Liao(2018)	Spatial	Normal	Normal	Normal	Low	Normal
Younus(2019)	Dual	Excellent	Normal	Normal	Low	Normal
Li(2019)	Spatial	Excellent	Excellent	Excellent	Normal	Normal
Liu(2019)	Spatial	Normal	Normal	Normal	Low	Normal
Samrah(2019)	Frequency	Normal	Normal	Normal	Low	Low
Kaw(2019)	Spatial	Normal	Excellent	Normal	Low	Normal
Maniriho(2019)	Spatial	Excellent	Normal	Normal	Low	Normal
Zhang(2019)	Spatial	Excellent	Excellent	Normal	Low	High
Li(2019)	Spatial	Excellent	Normal	Normal	Normal	High
Parmar(2019)	Spatial	Excellent	Excellent	Normal	Normal	High
Anmed(2019)	Quantum	Excellent	Excellent	Normal	Low	Normal
Qu(2019)	Quantum	Excellent	Excellent	Excellent	Low	High
Biswal(2020)	Frequency	Normal	Excellent	Normal	Low	High

Liao(2020)	Spatial	Normal	Normal	Excellent	Normal	Normal
Liu(2020)	Spatial	Excellent	Excellent	Normal	Low	High
Kadhim(2020)	Frequency	Normal	Excellent	Excellent	Low	Normal
Gutub(2020)	Spatial	Normal	Excellent	Excellent	Low	Low
Sahu(2020)	Spatial	Excellent	Normal	Excellent	Low	High
Shankar(2020)	Dual	Normal	Excellent	Excellent	Low	High
Liu(2020)	Frequency	Normal	Excellent	Excellent	Low	Normal
Subhedar(2020)	Frequency	Normal	Excellent	Excellent	Normal	High
Kadhim(2020)	Frequency	Excellent	Excellent	Excellent	Low	High
Pak(2020)	Spatial	Excellent	Normal	Normal	Low	Low
Luo(2020)	Frequency	Excellent	Excellent	Excellent	Normal	High
Subhedara 2016)	Frequency	High	High	Normal	Low	Normal
Zhou (2016)	Dual	Normal	Normal	Normal	Low	High
Son (2016)	Frequency	Excellent	Normal	Normal	Low	High
Dadgostar(2016)	Frequency	Normal	Normal	Excellent	Low	Normal
Jiang (2016)	Quantum	Excellent	Excellent	Normal	Low	High
Jain (2016)	Dual	Excellent	Normal	Excellent	Normal	Normal
Bhasme (2016)	Dual	Normal	Excellent	Excellent	Normal	High
Kaur (2016)	Frequency	Excellent	Normal	Normal	Low	Low
Swain (2016)	Spatial	Excellent	Normal	Excellent	Normal	Low
Makwana (2016)	Dual	Excellent	Normal	Normal	Normal	High
Thenmozhi(2016)	Spatial	Excellent	Normal	Normal	Low	Low
Setiadi (2017)	Dual	Normal	Normal	Excellent	Normal	High

Muhammad(2017)	Dual	Excellent	Normal	Normal	Low	Low
Debnath(2017)	Quantum	Normal	Excellent	Normal	Low	Normal
Muhammad(2017)	Dual	Excellent	Normal	Normal	Low	High
Rajendran(2017)	Spatial	Excellent	Normal	Normal	Low	Normal

Table 1. Various Image Steganography Techniques with various Parameters

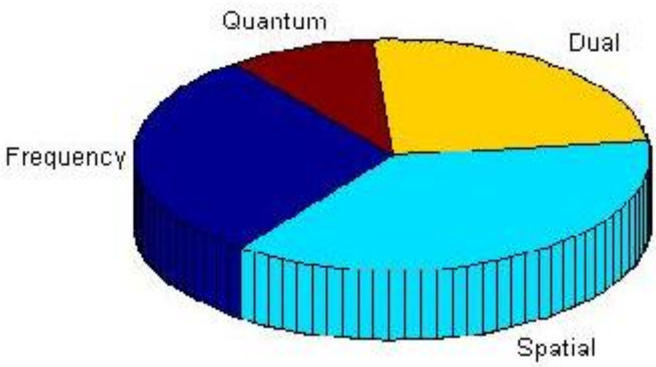

Fig. 3. Various Domains of Image Steganography.

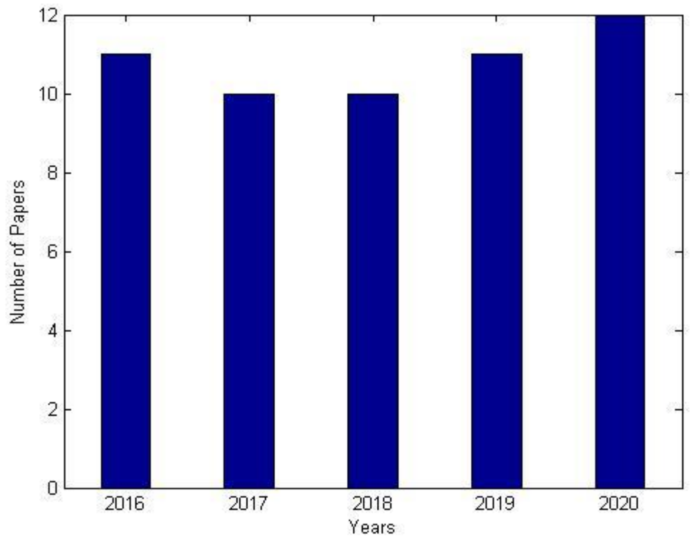

Fig. 4. Yearwise Reviewed Papers.

6. Conclusion and Future Scope

In this paper, we have done analytical study of various techniques of image steganography in the present scenario. We have studied fifty four techniques from year 2016 to 2020 in various domains. All the above techniques revolve around the various parameters of steganography. All these techniques are designed to optimize the various parameters. We have also analyzed these techniques on the basis of various parameters. We have also used the graph by using MATLAB for visualizing the various techniques. In the future, we will work to develop some contemporary technique which will enhance various steganography parameters.

References

[1] Abbas, C; Joan, C; Kevin, C; Paul, M.K. (2010): Digital Image Steganography: Survey and Analysis of Current Methods.Signal Processing (Elsevier), 90(3), pp 727–752.
[2] Ahmed, A. ; Latif, A.E. ; Attya, B. ; Andraca, S.E. (2019) : A novel image steganography technique based on quantum substitution boxes", Optics and Laser Technology (Elsevier), 116 , pp 92-102.
[3] Amirtharajan, R..; Akila, R.; Deepikachowdavarapu, P.(2010): A Comparative Analysis of Image Steganography. International Journal of Computer Applications, 2(3), pp 41-47.
[4] Amirtharajan, R.; Ganesan, V.; Jithamanyu, R.; Rayappan, J.; Bosco, B. (2010). An Invisible Communication for Secret Sharing against Transmission Error. Universal Journal of Computer Science and Engineering Technology, 1(2), pp 117-121.
[5] Amirtharajan, R.;,Krishnendra, N.; Harish, J. (2010) : Info Hide – A Cluster Cover Approach. International Journal of Computer Applications, 3(5), pp 11-18.
[6] Anderson, R.J. (1996): Stretching the Limit of Steganography in Information Hiding. Springer Lecture Notes in Computer Science,1174, pp 39-48.
[7] Anderson, R.J.; Peticolas, F.A.P. (1998): On the Limits of Steganography. IEEE Journal on Selected Areas in Communications, 16(4), pp 474-481.
[8] Aqeel, I.; Suleman, M.B. (2019): A Survey on Digital Image Steganography Approaches. Fisrt International Conference on Intelligent Technologies and Applications (Springer) and Computer and Information Science book series (CCIS), 932, pp 769–778.
[9] Ardiansyah, G; Sari, C.A.; Setiadi, D.R. ;Rachmawanto, E.H. (2017): Hybrid method using 3-DES, DWT and LSB for secure image steganography algorithm . 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE),(IEEE), Yogyakarta, Indonesia.
[10] Bender, W.; Gruhl, D.;Morimoto, N.; Lu, A. (1996): Techniques for Data Hiding , IBM System Journal, 35(4), pp 313–336.
[11] Bhasme, S.; Abu, A.; Gandhi, K.; Phadnis, R. (2016): Visual Cryptography and Steganography Techniques for Secure E-Payment System , International Research Journal of Engineering and Technology (IRJET), 3(3).
[12] Biswas, R.; Bandyapadhay, S.K.(2020): Random selection based GA optimization in 2D-DCT domain color image steganography , Multimed Tools and Applications (Springer), 74, pp 7101–7120.
[13] Brassil, J; Low, S; Maxemchuk, N. ; Garman, L.O. (1994): Electronic Marking and Identification Techniques to Discourage Document Copying. Proceedings of IEEE Infocom 94,13 (8), pp 1278–1287.
[14] Chakraborty, S. ; Jalal, A.S.; Bhatnagar, C. (2017) : LSB based non blind predictive edge adaptive image steganography. Multimedia Tools and Applications (Springer), 76(3), pp 7973–7987.
[15] Dadgostar H.; Afsari, F (2016): Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB. Journal of Information Security and Applications(Elsevier), 30, pp 94-104.
[16] Debnath, B.; Das, J.C. ; Debashis, D. (2017): Reversible logic-based image steganography using quantum dot cellular automata for secure nanocommunication. IET Circuits, Devices and Systems, 11(1), pp 58-67.
[17] Eugene, T.L.; Edward, J.D. (1999): A Review of Data Hiding in Digital Images. 52nd Annual International Conference of Information Science and Technology (IS and T) PICS, California, United States.
[18] Gaurav, K. ; Ghanekar, U (2018). : Image steganography based on Canny edge detection, dilation operator and hybrid coding. Journal of Information Security and Applications (Elsevier), 41, pp 41-51.

[19] Gutub, A. ; Ghamdi, M.A. (2020): Hiding shares by multimedia image steganography for optimized counting-based secret sharing. Multimedia Tools and Applications (Springer), 79, pp 7951–7985.

[20] Gutub, A.;Fattani M.(2007): A Novel Arabic Text Steganography Method Using Letter Points and Extensions. World Academy of Science, Engineering and Technology, 1(3), pp. 502-505.

[21] Hartung, F; Kutter, M. (1999): Multimedia Watermarking Techniques. Proceedings of IEEE, 87(7), pp 1079-1107.

[22] Heidari, S.; Pourarian, M.R. ; Gheibi, R. ; Naseri, M.; Houshmand, M. (2017) : Quantum Red–Green–Blue Image Steganography. International Journal of Quantum Information, 15(5).

[23] Hu, D.; Wang, L. ; Jiang, W. ; Zheng, S. ; Li, B. (2018): A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks. IEEE Access, 6, pp 38303-38314.

[24] Jain, M.; Lenka, S.K. (2016) : Diagonal queue medical image steganography with Rabin cryptosystem , Journal of Brain Informatics (Springer), 3(1), pp 39-51.

[25] Jiang, N.; Zhao, N.; Wang, L. (2016): LSB Based Quantum Image Steganography Algorithm, ,International Journal of Theoretical Physics (Springer),55(3), pp 107–123.

[26] Johnson, N.F.; Duric, Z.; Jajodia, S. (2001): Information Hiding: Steganography and Watermarking - Attacks and Countermeasures. Kluwer Academic Publishers.

[27] Johnson, N.F.; Duric, Z.; Jajodia, S. (2001): Information Hiding: Steganography and Watermarking - Attacks and Countermeasures. Kluwer Academic Publishers.

[28] Johnson, N.F.; Jajodia, S.(1998): Exploring steganography: Seeing the Unseen. IEEE Computer, 31(2), pp. 26-34.

[29] Joshi, K.; Gill, S.; Yadav, R.. (2018): A New Method of Image Steganography Using 7th Bit of a Pixels Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image. Journal of Computer Networks and Communications (Hindawi).

[30] Judge, J.C. (2001): Steganography: Past, Present and Future. Global Information Assurance Certification Paper (GIAC), SANS Institute.

[31] Kadhim, I.J. ; Premaratne, P. ; Vial, P.J. (2020) : Improved image steganography based on super-pixel and coefficient-plane-selection. Signal Processing (Elsevier), 171, pp 187-194

[32] Kadhim, I.J.; Premaratne, P. ; Vial, P.J. (2020) : High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform. Cognitive Systems Research (Elsevier), 60, pp 20-32.

[33] Kasapbas, M.C.; Elmasry, W. (2018) : New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check . Indian Academy of Sciences(Sadhana), pp 43- 68.

[34] Kaur, D.; Verma, H.K.; Singh, R.K. (2016): A Hybrid Approach of Image Steganography . International Conference on Computing, Communication and Automation (ICCCA), (IEEE), Noida, India.

[35] Kaw, J.A. ; Loan, N.A.; Parah; S.A.; Muhammad, K.; Sheikh, J.A.; Bhat, G.M. (2019) : A Reversible and Secure Patient Information Hiding System for IoT Driven e- Health. International Journal of Information Management (Elsevier), 45, pp 262-275.

[36] Khan, D.(1973): The Codebreakers: The Story of Secret Writing, New American Library.

[37] Krenn,R.(2004):Steganography and steganalysis . Internet Publication, Available at: http://www.krenn.nl/univ/cry/steg/article.pdf.

[38] Li, L.; Chang, C.C.; Chen, H. (2019): An Improved Bidirectional Shift-Based Reversible Data Hiding Scheme Using Double-Way Prediction Strategy, Security and Communication Networks.

[39] Li, M.; Mu, K.; Zhong, P.; Wen, J.; Xue, Y.(2019): Generating Steganography Image Description by Dynamic Synonym Substitution , Signal Processing (Elsevier), 164, pp 193-201.

[40] Liao, X. ; Guo, S. ; Yin, J. ; Wang, H.; Li, X. ; Sangaiah, A.K. (2018) : New cubic reference table based image steganography. Multimedia Tools and Applications (Springer), 77(5), pp 10033- 10050.

[41] Liao, X. ; Yu, Y. ; Li. B.; Li, Z.; Qin, Z. (2020): A New Payload Partition Strategy in Color Image Steganography. IEEE Transactions on Circuits and Systems for Video Technology, 3(3), pp 685-696.

[42] Lindkvist, T. (2000): Characteristics of Some Binary Codes for Fingerprinting, 3rd International Workshop on Information Security(Springer), Wollongong, Australia.

[43] Liu, H.H.; Lee, C.M. (2019): High-Capacity Reversible Image Steganography Based on Pixel Value Ordering , EURASIP Journal on Image and Video Processing (Springer).

[44] Liu, Q.; Xiang, X. ; Qin, J. ; Tan, Y., Tan, J.; Y. Luo (2020): Coverless steganography based on image retrieval of DenseNet features and DWT sequence mapping. Knowledge-Based Systems (Elsevier), 192.

[45] Liu, W. ; Yin, X. ; Lu, W., Zhang, J.; Zeng, S.;.Mao, M. (2020) : Secure halftone image steganography with minimizing the distortion on pair swapping. Signal Processing (Elsevier), 167.

[46] Luo, Y. ; Qin, J. ; Xiang, X.; Tan, Y.; Liu, Q. ; Xiang, L. (2020): Coverless real-time image information hiding based on image block matching and dense convolutional network. Journal of Real-Time Image Processing (Springer), 17(5) , pp 125–135.

[47] Makwana J.; Chudasama, S.G. (2016): Dual Steganography: A New Hiding Technique for Digital Communication. International Journal of Advanced Research in Electrical, Electronics and Insrtumentaion Engineering. 5(4), pp 3184 – 3188.

[48] Maniriho, P.; Ahmad, T. (2019): Information Hiding Scheme for Digital Images Using Difference Expansion and Modulus Function. Journal of King University – Computer and Information Sciences (Elsevier), 31, pp 335-347.

[49] Miria, A.; Faezb, K. (2017): Adaptive Image Steganography based on transform domain via genetic algorithm. Journal of Optik (Elsevier), 145, pp 158-168.

[50] Mohammed, A.;-Husainy F.A.; Abbas, H.; Sewadi, A.(2018): Full Capacity Image Steganography using Seven-Segment Display Pattern as Secret Key. Journal of Computer Science, 14(6), pp 753-763.

[51] Muhammad, K. ; Ahmad, J.; Rehman, N.U.; Jan, Z.; Sajjad, M. (2017) : CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. Multimedia Tools and Applications (Springer), 76, pp 8597–8626.

[52] Muhammad, K. ; Ahmad, J.; Rho, S.; Baik, S.W. (2017): Image steganography for authenticity of visual contents in social networks, Multimedia Tools and Applications, 76, pp 18985–19004.

[53] Muhammad, K. ; Sajjad, M. ; Mehmood, I; Rhod, S. ; Baika, S.W. (2018) : Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. Future Generation Computer Systems (Elsevier), 86, pp 951-960.

[54] Mukherjee, S.; Roy, S.; Sanyal, G. (2018): Image Steganography Using Mid Position Value Technique . International Conference on Computational Intelligence and Data Science (ICCIDS) (Elsevier), 132, pp 461-468.

[55] Norman, B.(1973): Secret Warfare: The Battle of Codes and Ciphers, Dorset Press.

[56] Pak, C. ; Kim, J. ; Ann, K.; Kim, C.; Kim, K. ; Pak, C. (2020): A novel color image LSB steganography using improved 1D chaotic map", Multimedia Tools and Applications (Springer), 79, pp 1409–1425.

[57] Parmar, B.; Siyag, M.; Batan, S.(2019): Enhancement of Image Security Using Even Odd Image Steganography , Journal of the Research Gujrat Society, 21(15), pp 527-531.

[58] Peter, W. (2002): Disappearing Cryptography: Information Hiding: Steganography and Watermarking. 2nd International Workshop on Information Hiding, California, United States.

[59] Qu, Z. ; Cheng, Z. ;Wang , X. (2019): Matrix Coding-Based Quantum Image Steganography Algorithm . IEEE Access, 7, pp 35684-35698.

[60] Rajendran, S.; Doraipandian, M. (2017): Chaotic Map Based Random Image Steganography Using LSB Technique. International Journal of Network Security, 19(4), pp 593-598.

[61] Rodrigues,J.M.;. Rios, J.R.; Puech,,W. (2004): SSB-4 System of Steganography Using Bit 4, 5th International Workshop on Image Analysis for Multimedia Interactive Services (WIAMIS) , Lisboa, Portugal.

[62] Sahu, A.K. ; Swain, G. (2020): Reversible Image Steganography Using Dual-Layer LSB Matching. Sensing and Imaging (Springer), 21. pp 263-285.

[63] Sarmah, D.K; Kulkarni, A. J. (2019): Improved Cohort Intelligence – A High Capacity, Swift and Secure Approach on JPEG Image Steganography. Journal of Information Security and Applications (Elsevier), 45, pp 90-106.

[64] Setiadi, D. M.; Rachmawanto, E.H.. ; Sari, C.A. (2017) : Secure Image Steganography Algorithm Based on DCT with OTP Encryption, Journal of Applied Intelligent System, 2(1).

[65] Shankar, K. ; Elhoseny, M. ; Kumar, R.S.; Lakshmanaprabu, S.K. ; Yuan, X. (2020): Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique . Journal of Ambient Intelligence and Humanized Computing (Springer), 11, pp 1821–1833.

[66] Simmons,G.J. (1983): The Prisoners Problem and the Subliminal Channel, 3rd International Cryptography Conference (Crypto'83), California, United States.

[67] Soleymani, S.H. ; Taherinia, A.H. (2017): High capacity image steganography on sparse message of scanned document image (SMSDI). Multimedia Tools and Applications, 76, pp 20847–20867.

[68] Stalling, W. (2005): Cryptography and Network Security Principles. PHI Publication, Delhi.

[69] Subhedar, M. S.; Mankar, V.H. (2020) : Secure image steganography using framelet transform and bidiagonal SVD", Multimedia Tools and Applications (Springer), 79, pp 1865–1886.

[70] Subhedara, M.S.; Mankarb, V.H. (2016) : Image steganography using redundant discrete wavelet transform and QR factorization. Computers and Electrical Engineering (Elsevier), 54, pp 406-422.

[71] Sun, S. (2016): A novel edge based image steganography with 2k correction and Huffman encoding. Information Processing Letters (Elsevier), 116(2), pp 93-99.
[72] Swain, G. (2018) : High Capacity Image Steganography Using Modified LSB Substitution and PVD against Pixel Difference Histogram Analysis. Journal of Computer Networks and Communications (Hindawi).
[73] Swain, G. (2016) : Digital Image Steganography using Variable Length Group of bits Substitution. Proceeding of Computer Science (Elsevier), 85, pp 31 –38.
[74] Thenmozhi, M. J.; Devi, T.M. (2016) : A New Secure Image Steganography Using LSB and Spiht Based Compression Method. International Journal of Engineering Research and Science (IJOER), 2(3), pp 80 – 85.
[75] Younus, Z. S.; Husssain, M.K. (2019) : Image Steganography using Exploiting Modification Direction for Compressed Encrypted Data. Journal of King Saud University- Computer and Information Sciences, Article in Press.
[76] Zhang, J.; Lu, W.; Yin, X.; Liu, W.; Yeung, Y. (2019): Binary Image Steganography based on Joint Distortion Measurement. Journal of Visual Communication and Image Recognization (Elsevier), 58, pp 600-605.
[77] Zhang, X. ; Peng, F. ; Long, M. (2018) : Robust Coverless Image Steganography Based on DCT and LDA Topic Classification. IEEE Transactions on Multimedia, 20(12) ,pp 3223 – 3238.
[78] Zhou, X.; Gong, W.; Fu, W.; Jin, L.J. (2016): An improved method for LSB based color image steganography combined with cryptography, 15th International Conference on Computer and Information Science (ICIS)(IEEE), Okayama, Japan.

A Brief Author Biography

Ravi Saini – Ravi Saini has received his M.Tech degree from UIET, MDU Rohtak. He is currently pursuing his Ph.D from UIET, MDU Rohtak. He got Gold Medal during his M.Tech. Currently, he is working as Assistant Professor at GCW Gurawra (Rewari). His research area includes cryptography, steganography and image processing. He has more than 25 publications in different journals and conferences.

Kamaldeep Joshi – Kamaldeep Joshi has received his Ph. D Degree from UIET, MDU Rohtak. Currently, he is working as Assistant Professor at UIET MDU Rohtak. His research area includes neural network, biometric security, cryptography and steganography. He has more than 40 publications in different journals and conferences.

Rajkumar Yadav – Rajkumar Yadav has received his Ph. D Degree from UIET, MDU Rohtak in 2011. Currently, he is working as Assistant Professor at UIET MDU Rohtak. His research area includes information hiding, cryptography and steganography. He has more than 60 publications in different journals and conferences.

Rainu Nandal – Rainu Nandal has received his Ph. D Degree from UIET, MDU Rohtak. Currently, he is working as Assistant Professor at UIET MDU Rohtak. His research area includes DBMS security, network security etc. He has more than 30 publications in different journals and conferences.