Asian Journal of Research in Computer Science

10(3): 33-52, 2021; Article no.AJRCOS.70381
ISSN: 2581-8260

Secure Data Transfer over Internet Using Image Steganography: Review

Dakhaz Mustafa Abdullah[1*], Siddeeq Y. Ameen[1], Naaman Omar[1], Azar Abid Salih[1], Dindar Mikaeel Ahmed[1], Shakir Fattah Kak[1], Hajar Maseeh Yasin[1], Ibrahim Mahmood Ibrahim[1], Awder Mohammed Ahmed[2] and Zryan Najat Rashid[2]

[1]Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq.
[2]Sulaimani Polytechnic University, Sulaimani, Kurdistan Region, Iraq.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2021/v10i330243
Editor(s):
(1) Dr. Francisco Welington de Sousa Lima, Universidade Federal do Piauí, Brazil.
Reviewers:
(1) Muhammad Sajjadur Rahim, University of Rajshahi, Bangladesh.
(2) Hiroyuki Hisamatsu, Osaka Electro-Communication University, Japan.
(3)Vani V, Bangalore Institute of Technology, India.
Complete Peer review History: http://www.sdiarticle4.com/review-history/70381

Review Article

Received 01 May 2021
Accepted 06 July 2021
Published 06 July 2021

ABSTRACT

Whether it's for work or personal well-being, keeping secrets or private information has become part of our everyday existence. Therefore, several researchers acquire an entire focus on secure transmitting secret information. Confidential information is collectively referred to as Steganography for inconspicuous digital media such as video, audio, and images. In disguising information, Steganography plays a significant role. Traditional Steganography faces a further concern of discovery as steganalysis develops. The safety of present steganographic technologies thus has to be improved. In this research, some of the techniques that have been used to hide information inside images have been reviewed. According to the hiding domain, these techniques can be divided into two main parts: The spatial Domain and Transform Domain. In this paper, three methods for each Domain have been chosen to be studied and evaluated. These are; Least Significant Bit (LSB), Pixel Value Difference (PVD), Exploiting Modification Direction (EMD), contourlet transform, Discrete Wavelet Transformation (DWT), and, Discrete Cosine Transformation (DCT). Finally, the best results that have been obtained in terms of higher PSNR, Capacity, and more robustness and security are discussed.

**Corresponding author: E-mail: Fairoz.kareem@dpu.edu.krd;*

Keywords: Steganography; cryptography; robustness; security; spatial domain; transform domain.

1. INTRODUCTION

In today's communication technology, photographs play a critical role in various disciplines, including military, social networking, and biometric systems. Sensitive photos are exchanged via unsecured networks, making it difficult to conceal them from outsiders [1]. The issue of hidden data communication has persisted throughout history. While cryptography is an efficient method of securing confidential data by rendering it unreadable to unauthorized parties, the act of communicating with encrypted communications attracts attention [2]. This can be troublesome for a communication channel being watched by a third party, who can terminate contact between the two parties at the slightest suspicion [3].

Meanwhile, research indicates that encryption alone may not be adequate to secure secret communication [4]. Personal messages demand an invisible communication route that, in some instances, must be completely anonymous. As a result, a technique for concealing information is required [5,6].

For millennia, the art of concealing information has been evolving, and innovation and progress have always followed information security to ensure the message reaches the intended destination without being tampered with [7]. Historically, cryptography and Steganography have been the two primary ways for safeguarding, concealing, and transmitting messages [8,9]. Since the inception of the Internet, one of the most critical communication and information technology aspects has been information security [10]. It is vital to safeguard this data when it is transmitted across unsecured networks [11]. As a result, there is a need for creating technologies that will assist in preserving the integrity of digital information and ensuring the owners' intellectual property rights. This has resulted in a meteoric rise in the field of information concealment [12,13].

Cryptography is the art and science of creating ciphers to encode/encrypt communications and information so that only authorized communication parties can interpret and decrypt them [14]. On the other hand, Steganography is a technique for concealing personal data and communications by embedding them in a cover material (image/audio/video) that prevents hackers from discovering them [15,16]. Approaches for picture steganography have been classified as spatial domain and frequency domain techniques [17]. Steganography techniques may be utilized to create an excellent tool for data exfiltration, network assaults, and concealed communication between private parties [18]. The purpose of these strategies is to cover personal data (stereograms) within an innocent-looking carrier, such as user communications [19].

These days, Hacking has become a huge issue. Secure data transmission or communication over the Internet is problematic because of security issues [20]. In the course of the ages, information security has made many signs of progress [21]. Two new approaches for safe data transfer over the years are Steganography and cryptography [22]. Cryptography is the technique of text encryption, while Steganography is used to hide text within a multimedia element as if it were nothing [21]. Steganography secures the data as if someone sees the file because human senses cannot recognize or sense the data within a multimedia element. They cannot perceive that some secret message has hidden within it [23].

In the current world of communication, IoT is an emerging technology [24]. The safe data transfer in the IoT environment, as IoT devices are growing every day, is the biggest problem [25]. Single-board computers (SBCs) or microcontrollers transfer data to another IoT device [26]. The data obtained from these devices should be sent extremely safely to prevent some ethical problems because of lower processing power and storage capability [27]. There are several encryption methods used to transmit data between IoT devices. However, there are clear opportunities for eavesdroppers to suspect encrypted information [28]. Steganography Mechanism is used to prevent suspicion like an additional layer of protection from adding more secure data transfers [29]. Based on IoT device capabilities, low complexity pictures disguise data with various hidden algorithms [30].

In the lives of individuals, the Internet now plays a significant role [31]. The world is connected via the Internet. Any data transmitted or transmitted over the Internet is possible. The Internet, called the Internet of Things, also connects things [32]. Safety is an uncompromising feature. Encryption

helps secure the data to a certain extent. Further, Picture Steganography is beneficial if data in the shape of an image must be discreetly sent [33,34].

The progress of the Internet and technology makes communication of information faster and easier [35]. Without data safety, eavesdroppers can illegally obtain private and secret information, which might cause serious harm to any organization [36]. That means that the data should be secure and protected from hackers while sharing confidential data [37].

For safe transmission of data over the Internet, data transmission is crucial in high safety and secrecy; the certainty of information is the most critical problem for network and internet communications [38, 39]. The information must be converted into a cryptic format to safeguard the data transferred from attackers [40]. Various methods are used during transmission for ensuring data privacy, such as Steganography and cryptography [41].

Rapid technological advancements and availability of sources have led to a great deal of essential knowledge being transmitted between individuals on the Internet in a few seconds [42]. Since the information is silent and delicate, it must be protected and maintained by general confidentiality [43]. Many approaches and techniques may be used, so data worthy of security can be retained [44]. The only downside is that it is exceptionally costly to preserve this anonymity [45]. A far more straightforward approach to hide this critical information from any other source and to send it through the Internet might be by utilizing Steganography technology [46]. Text, music, or even pictures might be the other source [47].

Because of the constant technological progress, data may be transferred from one area to another [48]. The data will be hacked more probable by the attacker at the same time [49]. Numerous techniques, such as cryptography and Steganography, safely transport the data to the target [50]. Because of its great quantity and relevant information, the data is the most critical item nowadays for an individual in an organization [51]. However, it is vulnerable and more subject to assault [52]. Steganography securely hides chosen files in a filesystem, such that an attacker cannot detect their presence without the associated access keys [53]. There are still vulnerabilities that cause an attacker's threat. B+trees are fast indexing and performance improvement methods [54,55].

The Internet of Things (IoT) is a realm where data is sent every second. The safety of this data is a complicated issue; however, cryptography and steganography techniques help minimize security difficulties [56]. These approaches are essential for user authentication and data confidentiality [57].

Much information is transmitted over the Internet in the current day. To preserve privacy, this information must be securely sent [58]. Many ways are created to convey this information without third-party interception securely. Steganography is also approaching for the secure transmission of data. In Steganography, it is disguised from the third party that there is protected information [48,59]. Only sender and recipient know about the delivery of secret information [60]. In Steganography, information is incorporated into a certain cover media such as text, picture, audio, video, etc. [61]. The picture is used as a cover for hiding hidden data in image steganography [62]. The most popular approach for picture steganography consists of the least essential bits (LSB), changed by secret message bits, of image pixels [63]. The LSB approaches have numerous restrictions, which lead to the development of several other ways of picture steganography [64]. This approach is the Pixel Indicator Technique [65].

Secure data transfer through the Internet is a critical component of data exchange because data is a significant asset in internet communication [66]. Therefore, data security plays a crucial role in disseminating and transmitting information via unsecured networks [67]. Also, it entails protecting data against different kinds of threats, such as infiltration or illegal Internet access. Various technology is used to enhance data security sent over the Internet, such as encryption, Steganography, watermarking, or Fingerprinting [68]. Steganography uses the compression of data and encryption to improve data security. It is suitable for many data formats such as text, picture, audio, or video [69]. Data compression techniques such as Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT) are utilized to provide more security and information privacy as various transformations [70].

The Internet's use is now evolving every day [71]. Data from diverse sources to other countries is one of the significant applications of the Internet. There are serious problems with data protection during data transfer via the Internet [72]. In data protection, two approaches are employed. Crystallization and Steganography. Cryptography and Steganography are utilized in our suggested system to make the data safer [73]. Encryption and decryption are the fundamental functions of cryptography. More than 4 Times are encrypted here. The secret communication is essentially encrypted by an encryption key in the cryptography process. For transmitting a message, the sender utilizes the encryption key [74]. On the other hand, the recipient should be aware of the encryption key to decrypt the message for original data. Instantly Steganography is the method secret data may be hidden through digital media coverage, such as audio, image, video, and text [75].

The security of information on mobile phones is complex when vast volumes of data are shared over the Internet [76]. Cryptography and Steganography can provide secure information transmission. Cryptography is a technology providing specific communication encryption techniques. Steganography is a technique for hiding the information through the image message so that another person is unaware of the presence of the news in addition to the person addressed [77].

A mobile telephone user may transmit the message with multimedia subjects, including photos, audio, or video clips, using a Multimedia Messaging System (MMS) [78]. On the other hand, hidden communication has become an essential subject for debate, which has become more and more important today as the Internet develops. Steganography is one of the ways introduced for secret communication [79,80]. This is, therefore, an intriguing concept for Steganography in MMS. One of the difficulties with steganography methods is that the password key between the sender and receiver of encrypted data is sent between steganography [81,82]. High security of multimedia data is necessary for the current environment. This safe and secure method should ensure the network's secrecy, authenticity, and integrity [83]. In an electronic communication environment, the sensitive information sent through the Internet is compromised via Phishing. In various applications, cryptographic methods are used to safeguard data transfer against malicious assaults [84].

Now information is transmitted over the Internet, and there are enough hackers to hack this information because the data has been transmitted via covert methods [85]. The data is encrypted with cryptographic techniques, and a third-party adversary may see the text, and the information can be retrieved using cryptanalysis [86]. The main difficulty with the application of cryptography is that unauthorized users see the chip text. By employing Steganography, we may prevent this [87]. Various methods for hiding information in Steganography are available. When data is integrated into the picture, transformation techniques produce more noise [88]. The LSB insert method is used to insert bits into a frame through random number generators to prevent distortion of the noise in the image [89].

This paper aims to evaluate the most popular techniques used for Steganography and reviewed performance in terms of Peak Signal to Noise Ratio (PSNR), embedded capacity, and high robustness.

The rest of the paper is structured as follows—section II Brief review about Steganography. Section III & IV is about spatial Domain and transform Domain and its techniques reviewed in this paper. A variety of practical steganography techniques implementations reviewed in Section V. Assessment and recommendations in section VI. a conclusion about the article is provided in Section VII.

2. STEGANOGRAPHY: A BRIEF REVIEW

Steganography is a technology that conceals critical information within video, audio, or picture files and then transmits it [90] [91]. A hidden message can be hidden within a piece of trustworthy information and conveyed without anybody being aware of it. Steganography prevents unauthorized individuals from viewing the news since it is concealed within a carrier and travels through the carrier. The message's carrier can be plaintext, audio, pictures, video, or the web [92]. In today's digital world, information security and covert data transmission are evolving at a breakneck pace. It enables the distribution of essential multimedia files by creating identical data copies. While sending secret information and files over the Internet is an insecure process, everyone has something to conceal [93]. On the other hand, today's Steganography is substantially more complex, allowing users to cover vast quantities of data.

These types of Steganography are frequently used in conjunction with cryptography to secure the information twice; first, the secret message is encrypted and then buried, so that an adversary must first locate the data (an often tricky operation in and of itself), as seen in Fig. 1, and then decrypt it [12].

Several scholars have examined and investigated steganography approaches in recent years, producing numerous outstanding steganography algorithms. Traditional steganography algorithms may be classified according to their embedding domain as spatial domain algorithms or transform domain algorithms, as seen in Fig. 2 [95].

3. SPATIAL DOMAIN TECHNIQUES

A two-dimensional matrix can be used to represent a picture, with each element representing pixel intensity. Spatial Domain refers to the state of two-dimensional matrices that represent an image's intensity distribution. This approach directly manipulates the picture pixel. This approach conceals the secret data by substituting selected bits from the cover picture with the personal message's bit value. Steganography techniques are classified into several categories according to their embedding domains, including least significant bit (LSB)-based approaches, pixel value differencing (PVD)-based systems, and Exploiting Modification Direction (EMD)-based approaches [96]. In this article, we will discuss only three strategies in the Spatial Domain: (LSB), (PVD), and (EMD).

3.1 Least Significant Bit (LSB)

LSB is a method that is commonly employed in spatial domain steganography. This strategy is straightforward to execute. The idea is to simply substitute the message bit for the host image's lowest bit value. Typically, both the message and the picture are transformed to an 8-bit binary integer to facilitate it [97]. As a result, the LSB technique often results in a high payload. After concealing the hidden message, the cover picture is almost identical to the image under examination. For example, suppose we are attempting to disguise the character 'A' within an 8-bit image. In that case, the binary representation for the eighth consecutive pixels from the image's top-left corner is as follows.

00110111 11101001 10001010 00100111
11001010 10101001 11001010 00110111

Then, successively (from left to right), the binary representation of the letter 'A' (01100101) is embedded in the LSB's of the comparable binary pattern of pixels. Eventually, the bits will generate the following way [98]:

00110110 11101001 10001011 00100110
11001010 10101001 11001010 00110111

3.2 Pixel Value Difference (PVD)

This approach divides the cover picture into blocks that do not overlap. This time, we're going to use the pixel difference between the split blocks [99]. A significant difference value should be taken into account in the edge area, while a small difference value should be taken into account in the smooth area. The human eye is more sensitive to noise in a smooth region than in an edge area. As a result, the difference value is substituted with another value to incorporate the secret message bits. This approach is highly invisible and has a large capacity for embedding [100].

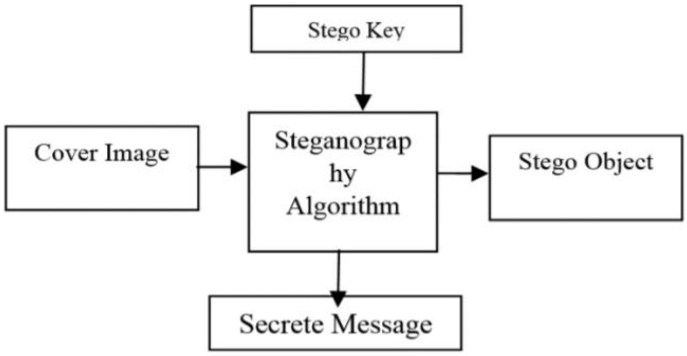

Fig. 1. Available steganography system [94]

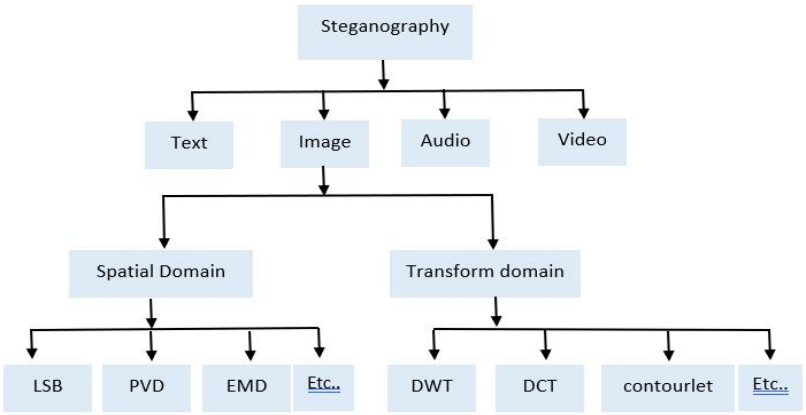

Fig. 2. Types of Steganography techniques

3.3 Exploiting Modification Direction (EMD)

Zhang and Wang (2006) proposed the Exploiting Modification Direction (EMD) methodology, which partitions the picture into various groups of n pixels to enter the secret digit into the (2n + 1)-are encoding system [101]. Where n is a system parameter (n ≥ 1), because each group has n pixels, there are 2n + 1 potential modifications (include one case in which no pixel is changed). As a result of this concept, no more than one pixel is increased or lowered by one. As a result, it has a high stego-image quality. To map these 2n + 1 situations, the embedding and extraction technique must specify a one-to-one extraction function [102].

4. TRANSFORM DOMAIN TECHNIQUES

Another option is to transform domain-based Steganography to conceal confidential data within the cover picture without being recognized by humans. Despite its complexity, this strategy is more efficient in suppressing information inside a picture by utilizing numerous algorithms and transformations [103]. This methodology operates by embedding the data in the signal's frequency domain, which is more robust than time-domain embedding principles. As a result, it is often referred to as the embedding technique, and numerous methods have been proposed. At the moment, the most robust steganographic systems work in the area of transformations. Transform Domain Techniques are preferable to spatial domain techniques because they conceal information in places less susceptible to compression, cropping, and image processing. Discrete Wavelet Transformation (DWT), Discrete Cosine Transformation (DCT), Contourlet Transform, Wavelet Transform, and Fourier Transform are all effective techniques in the transform domain [104]. We will concentrate on these three approaches in this article (Contourlet Transform), (DWT), and (DCT).

4.1 Contourlet Transform

Do and Vetterli presented the contourlet transform as a novel two-dimensional picture sparse representation technique in 2002. It can simultaneously assess the direction and size of each picture and accurately portray the texture and Contour of the photograph [105]. The contourlet transform's primary principle is to extract multiscale directional information. The contourlet transform is an objective measure of an image's two-dimensional performance in two dimensions since it can make degeneration in any direction and at any size. The contourlet transform has a variety of advantageous properties, including multiresolution, directionality, localization, and anisotropy, and it overcomes the wavelet transform's inadequacy with directed data. A subset of the Discrete Wavelet Transform is the Contourlet Transform (DWT) [106]. The contourlet transform is accomplished using a Pyramidal Directional Filter Bank (PDF). The first phase employs the Laplacian pyramid (LP) to break down the 2D data into a low pass and high pass sub-band. In contrast, the angular decomposition stage uses directional filter banks (DFBs) to generate directional forms. CT is a directional representation of the signal that enables the inclusion of several directions for different signal scales while achieving near-critical sampling [107].

4.2 Discrete Wavelet Transformation (DWT)

DWT is a technique for segmenting information contained in a picture into the approach and signal detail. The LL bands include low pass coefficients and copying techniques and additional information about various sub-signals showing vertical, horizontal, or diagonal information or changes in an image. There are numerous approaches for expressing pictures to approach and signal features in the DWT method, one of which is wavelet Haar. A wavelet counting procedure may be utilized to characterize a view using Wavelet Haar [108]. Coefficients of the Haar DWT are calculated using horizontal and vertical operations. Horizontal operations decompose a picture into low-frequency (L) and high-frequency (H) bands (H). L is computed by averaging the horizontal values of the cover image's two successive pixels (i.e., left to right), whereas H is obtained by subtracting the two [109].

4.3 Discrete Cosine Transformation (DCT)

One of the most often used and successful image transformation techniques for converting a picture from the spatial to the frequency domain. The DCT coefficients are adjusted according to the secret data bits in basic DCT-based Steganography. The concept is divided into its appropriate high, medium, and low-frequency components using DCT steganography. The most critical details are found in the low-frequency sub-bands, whereas the highest quality details are found in the high-frequency bands [110]. It converts the picture from the spatial to the frequency domain and splits it into three frequency areas, namely low frequency (FL), middle frequency (FM), and high frequency (HF) (FH). FL and FH are abbreviations for the lowest and highest frequency components, respectively. To make lossy compression methods more resilient, FM is employed as the embedding zone. As a consequence, the transformation's security is rather good. In Steganography, DCT divides a picture into 8*8 pixels blocks and then works from left to right and top to bottom in the blocks [98].

5. LITERATURE REVIEW

Recently, many works have been implemented using steganography techniques. So, in this section, some of these works will be elaborated as follows:

A- EMBEDDING CAPACITY: The term "embedding capacity" refers to the quantity of information that may be hidden inside a cover picture. Robustness refers to the ability to recover the stego-original image's confidential information independently of the kind of processing used, e.g., cropping, scaling, and filtering. Additionally, these goals may include protection against steganalysis and the integrity of hidden data. In an ideal world, a steganography algorithm would increase embedding capacity while preserving the confidentiality and integrity of hidden data.

B- PSNR: The metric peak signal-to-noise ratio (PSNR) is used to determine the efficiency of the suggested technique for concealing one picture inside another. When confidential data is incorporated in Steganography. PSNR is a metric that quantifies the noise ratio between the stego picture and the original image. The better quality of the photo is when the PSNR value is more outstanding.

C- ROBUSTNESS: Robustness refers to the ability of embedded data to remain intact when the stego-image is subjected to transformations such as linear and nonlinear filtering, random noise addition, blurring or sharpening, rotations and scaling, decimation or cropping, lossy compression, and conversion from digital to analog and then back to digital.

D- SECURITY: Security refers to safeguard the data while also maintaining the user's privacy by preventing unwanted access. Steganography is a kind of security that conceals the presence of confidential data. It has worked on hiding sensitive data (text, picture, audio, or video) inside another text, image, audio, or video (the cover).

5.1 Literature Based on High Capacity

Subong et al. [111] propose a steganographic image technique in which the secret message's bit information replaces the LSBs of the cover image's RGB (red, green, blue) bytes, similar to many other LSB image steganographic techniques, except that the secret message's bits go through a series of assessed and scored bit rotation and inversion operations before being replaced. The recommended methodology produced less when comparing the PSNR and MSE values of the stego picture generated by this recommended method to the present four bits per byte replacement approach of LSB

Replacement and Adaptive LSB Embedding algorithms distortion. However, the proposed technique does not considerably improve security robustness.

A technique for picture steganography, Elharrouss et al. [112] developed a method based on LSB coding. To conceal a picture within another. The suggested process begins by combining the cover picture with the photos to be suppressed using the k-LSB approach. An area detection procedure utilizing the local entropy filter has been proposed to determine the region containing the concealed pictures. After retrieving the covered picture, an image quality improvement approach was used to correct any picture degradation caused by the concealing methods. PSNR was 32.83 dB.

Swain [113] suggests two PVD approaches based on overlapping 12-pixel blocks. The first methodology embeds and extracts data using an adaptive quantization range table and modular arithmetic. The second methodology embeds and extracts data using a defined quantization range table and an addition/difference method. The experimental results indicate that the proposed adaptive PVD technique has a greater embedding capacity (2,335,661) and a better PSNR (42.97) than current adaptive PVD methods. Still, the suggested non-adaptive PVD approach has a greater embedding capacity than current non-adaptive PVD techniques.

Zhou & Cao [114] proposed a steganography technique combining PVD and matrix pattern (MP) based on the difference of pixel texture, in which the former is classified into two parts, and the binary message is then embedded in the edge portion of the blue layer of the image without extracting the original image; the latter algorithm generates MP representing 95 characters. The blue layer's fourth to sixth bits are utilized for the MP algorithm, while the remaining bits are used for the PVD algorithm. Consequently, it was demonstrated that it supports a variety of embedded message formats, is more resistant to detection, and possesses a high level of security. PSNR was 46.27, and the message capacity was 53,986.

Saha et al. [115] suggested EEMDHW, Extended EMD-based steganography based on a Hashed-Weightage Array. Each of the cover image's K pixels contains two 2KN-any numbers, where N is the pixel's bit count. As a result, the payload is entirely interchangeable when used in this way. The embedding is carried out using a dynamic weighting array. This array is generated pseudo-randomly by running the message pixels through the eliminative hashing method. The experimental findings indicate that the methodology outperforms current state-of-the-art methods in embedding capacity (payload) and decreased cover picture quality distortion. Steganography performed using the RS attack demonstrates that the suggested approach's embedding is unidentifiable up to a 3 bits per pixel (bpp) embedding rate. PSNR was 39.50.

By separating the n cover-pixels into two groups, Liu et al. [116] introduce an enhanced GEMD(generalized exploiting modification direction). The approach can increase GEMD's embedding capability from n+1 to n+2 n bpp. The experimental findings indicate that the technique also produces high-quality stego-images. Additionally, they provide an approach for generalizing the improved GEMD by separating n cover-pixels into k groups. This generalized extended GEMD may further improve embedding capacity by increasing the parameter k; but, as k grows, the PSNR decreases. This methodology may embed secret data using a suitable k to strike a compromise between the embedding capacity and the quality of stego pictures.

Elshazly et al. [117] proposed a novel approach for GEMD image steganography based on PSS-IB to alleviate the drawbacks of previous EMD approaches. Two essential criteria in steganography procedures are the quality of the stego-image and the capacity of the embedding payload. The proposed approaches embed data at a rate of 3 x 0.5 x LVMA (up to 9 bpp), which is more than the R = 3 x (n + 1)/n of the GEMD technique. The techniques proposed are simulated in MATLAB, developed, then implemented using XSG on the Spartan 3E Kit. Simulations and tests reveal that the proposed methodology can embed a big payload (up to 2,359,296 bits) while preserving a high-quality stego-image (up to 50.15 dB).

Thanks and Surekha [118] present a color picture steganography algorithm based on the (FRT) Finite Ridgelet Transform and (DWT). The FRT is used to generate the Ridgelet coefficients for each color channel in the cover color image. A single-level DWT is used to create the various wavelet coefficients, which are then modified to generate the stego color image using the encrypted channel values from the secret color image. Arnold scrambling is utilized to encrypt

channels of a hidden color picture in the suggested approach. The proposed methodology is evaluated on various standard color photographs, and the findings indicate that the stego picture is more invisible than the previous methodology. Additionally, the suggested approach has a high embedding capacity.

5.2 Literature-based High PSNR

To get the best results, Anwar et al. [119] suggest an approach that combines LSB-steganography with AES and Base64 encryption. This combination of techniques is effective. This is shown by the highest average PSNR value of around 60 dB in private images with an original size of 780x1040. At the same time, the lowest average PSNR value is 256x256 photographs with a file size of 23 kb is around 48 dB. The AES and Base64 encryption algorithms are used to increase data security sent across susceptible and unprotected networks.

Rafrastara et al. [120] propose modifying the inverted LSB approach based on the second, third, and fourth LSB bits. The strategy is tested by assuming that each pixel of the cover picture is pinned to one message bit. According to the testing results, the proposed approach improved the quality of the stego picture created. The suggested technique can enhance the quality of stego pictures by minimizing the number of changes in pixel values. It can eventually be utilized to add message payload as the quality increases.

AlWatyan et al. [121] suggested an automated approach for secure communication with two layers of security. Data is encrypted using a Java-developed encryption mechanism called Character Bit Shuffler (CBS) at the first level. The encrypted information is then concealed within a picture using the Least Significant Bit (LSB) approach, which alters only the last bits of the picture pixels. The LSB approach has the advantage of being accessible and maintaining the image's quality.

Astuti et al. [122] present a straightforward and secure method for hiding messages using LSB methods. The XOR procedure is performed three times to encrypt the message before it is placed on the LSB. Three MSB bits are used as keys in XOR operations to assist the encryption and decryption of communications. The findings of this investigation demonstrate that this approach secures messages while being extremely simple to use. The stego picture also has a good imperceptibility quality, with a PSNR value greater than 50 dB.

Maji et al. [123] proposed A system in which one or more LSB bits of selected pixels are used based on the difference in pixel intensity between adjacent pixels in the cover image's two image blocks. Secret bits are encrypted using OTP and a randomly generated pre-shared key. Because these encrypted bits are entirely random and resemble noise, the system is immune to a wide variety of statistical attacks. Comparative simulations using many well-known PVD-based approaches demonstrate favorable results for visual imperceptibility and a variety of quality parameters, such as MSE (0.0637), PSNR (60.08), and capacity (3088) bit.

Saleh and Amirmazlaghani [124] provide a unique multiplicative picture steganography methodology for embedding hidden data in a cover picture without altering it explicitly. To do this, they use the contourlet transform to break down the image and separate the high-frequency sub-bands into blocks of coefficients. The personal data is then embedded using an embedding coefficient. During the extraction step, we employ a Gaussian scale mixing distribution to precisely extract the embedded data. Experiments demonstrate that our suggested methodology can achieve imperceptibility while being undetectable by a comparable steganalysis methodology.

Reshma et al. [125] describe a pixel prediction algorithm based on picture steganography that uses the SVNN classifier and contourlet transform. The proposed technique conceals sensitive data using the input as a medical image and the CT as a mask. To begin, the image's effective pixels are identified using an error-based trained SVN. The classifier is fine-tuned using either the GA or the MS Algorithm. The contourlet embeds the secret message into the input picture using the embedding strength and the CT coefficient. Finally, depending on the CT coefficient, the personal statement and the input picture are retrieved. The suggested work is experimented on using various noises in photographs, and the images utilized in the analysis are obtained from the BRATS database. The proposed methodology delivers superior performance for measures such as correlation coefficient, PSNR, and SSIM with values of 89.3253 DB, 1, and 1 for the picture without employing noise. By introducing noise to the

concept, the correlation coefficient, PSNR, and SSIM achieve 48.578, 0.6123, and 0.9934.

Nevriyanto et al. [126] describe a picture steganography approach based on the Discrete Wavelet Transform and Singular Value Decomposition. Using a text file as a watermark, transform it into an image and insert it into the cover picture. They analyze the performance of this approach and compare it to others such as the Least Significant Bit, the DCT, and the DWT using the Peak Signal to Noise Ratio and Mean Squared Error. The findings of this experiment indicated that the DWT and Singular Value Decomposition perform better together than the LSB, the DCT, and the DWT alone. Peak Signal Noise Ratios of 57.0519 and 56.9520, respectively, are obtained using DWT and Singular Value Decomposition procedures. While Mean Squared Error-values produced using these methods are 0.1282 and 0.1311.

5.3 Literature-based Robustness

Kukharska et al. [127] combined the PVD technique with the Arnold transformation to build steganographic ways to hide data in BMP digital images. To improve the robustness of steganographic alterations. The usage of keys and the equally likely distribution of the steganographic container blocks and message components all contribute to the greater security of the steganographic message throughout its disguised transit via open communication channels. The keys' space is proportionate to the picture container's size. The Arnold transformation period value is the inverse of this number. In the sample Lena.bmp, the power of the keyspace is 383. A PVD steganographic approach combines two Arnold transformations on a previously separated picture to hide information.

Shehab et al. [128] proposed a technique based on the breakdown of the host image using the Contourlet transform's lowest energy sub-bands (4 levels), scrambling the watermark image with the Ikeda identifying new locations using a modified Arnold Cat map. This improves security and safety while also making Hacking more difficult or impossible. Compared to prior comparable attempts, the obtained data show that the offered technique is more resistant to attacks and more effective. The embedding area is also expanded by using the lowest energy sub-bands, and this feature will be investigated in future work with color imagery.

Li and Chao [129] proposed a secure and blind watermarking approach based on a non-subsampled contourlet transform and Schur decomposition. The cover image is decomposed using the two-level non-subsampled contourlet transform, and the low pass sub-band is chosen for watermark insertion to increase its robustness. Before integrating the watermark into the cover picture, it is jumbled using logistic chaotic and Arnold transformations to improve security. Additionally, by utilizing a quantification process, invisibility is accomplished. The encrypted watermark sequence can be obtained during the watermark extraction step without access to the host image. The suggested blind watermarking methodology beats several popular watermarking techniques regarding invisibility, robustness, and payload. Scalability and low pass filtering performance, on the other hand, may be enhanced further.

Najafi & Khaled [130] proposed a secure and robust picture watermarking approach based on singular value decomposition (SVD) and sharp frequency localized contourlet transforms (SFLCT). The SVD and SFLCT are applied to both watermarked and original photographs, and noticeable results for watermarking demands are generated by exploiting the SVD's characteristics and the SFLCT's benefits. Because most SVD-based watermarking techniques are sensitive to ambiguity attacks and have a false positive issue, this criticism may be addressed without adding extra steps to the watermarking algorithm. The suggested solution is safe and resistant to ambiguity attacks. The technique is simulated, and its resilience to various forms of assaults is evaluated. Compared to some contemporary schemes, this one exhibits a high level of imperceptibility, capacity, and robustness, making it an excellent choice for image processing applications.

Subhedar and Vijay [131] present three significant matrix factorization algorithms and the contourlet transform for Steganography in the transform domain. The security of image steganography is generally known to be primarily defined by the stego image's undetectability when analyzed by a site analyzer to identify the presence of buried secret information. Good imperceptibility means that the eavesdropper cannot detect the concealed information; nevertheless, the stego image may be analyzed using specific statistical tests while being broadcast over the channel. The secret is stored in the matrix factorized components of the cover

image's contourlet coefficients, decomposed using singular value decomposition (SVD), QR factorization, and nonnegative matrix factorization (NMF). The various studies look at the impact of matrix decomposition techniques on essential picture steganography properties such as imperceptibility, robustness to different image processing procedures, and universal steganalysis performance. Compared to current research, the suggested image steganography method has superior imperceptibility, large capacity, and low detection accuracy. Additionally, a comparison of three matrix factorization algorithms is provided and assessed.

Giri & Rumaan [132] describe a blind wavelet-based color picture watermarking technique that improves robustness and imperceptibility. The methodology mentioned above considers the intrinsic neighborhood connection attribute of the image's pixels for watermark insertion using a block-level method. The watermark's pixels are implanted in a specific region in this case. A pseudorandom sequence is used to organize the picture blocks for watermark insertion. Only the components with a higher frequency are utilized. In each example, the watermark is a 32 X 32 grayscale picture. The experimental findings indicate that the provided strategy is more resilient and transparent than specific previous state-of-the-art procedures.

Rabie et al. [133] introduce a high-capacity picture concealing system that improves the quality of stego images. This novel concealment technique uses a multi-scale Laplacian pyramid of the cover picture in the Discrete Wavelet Transform (DWT) domain. All Previously published work either increased capacity at the expense of stego quality or improved stego quality at the cost of accommodation, although at a lower power. The suggested strategy will boost the hiding capability of the cover picture by concealing in the highest-level Laplacian pyramid of the DWT low-frequency band utilizing a curve fitting adaptive area technique in the spectral magnitude discrete cosine transform domain. In comparison to competing approaches, the suggested process achieves a higher level of visual authenticity and capacity. Comparative experimental findings demonstrate that the recommended technique surpasses contemporary methods regarding payload capacity and various picture quality metrics. Its resistance further shows the suggested scheme's robustness to data loss and noise manipulation, geometric distortions and Checkmark assaults, and steganalysis detection assaults.

Abdelkader and AlTamimi [134] suggested a unique method for concealing the data of a hidden image by utilizing Discrete Cosine Transform (DCT) features in conjunction with a linear Support Vector Machine (SVM) classifier. The DCT characteristics are used to reduce the amount of redundant information in the image. Additionally, DCT is employed to incorporate the secret message using the RGB's least significant bits. Each byte in the cover image is altered to the point that it cannot be perceived by human sight. The SVM is employed as a classifier to accelerate the concealment process using DCT characteristics. The proposed strategy is adopted, and the resulting improvements are considerable. Additionally, performance analysis is performed using the MSE, PSNR, NC, processing time, capacity, and robustness factors.

5.4 Literature-based High Security

Murugan and Ragupathy [135] present the Discrete Wavelet Transform (DWT), which has several benefits over existing transform techniques such as (DCT) (Discrete Cosine Transform). This is due to the scalability of the quality, the interest in area coding, the low bit rate transmission that enables high-speed operation, and the compatibility with the Visual System used by humans, which gives high perception quality. Geometric attack introduces synchronization issues between the initial picture and the retrieved stego picture during the detection technique, which modifies their locations. Wavelet Space - frequency attribute of localization - analyzes image characters skillfully, adding additional strength to attacks such as geometric. This characteristic increases the embedding area while also increasing security. As a result, DWT produces a high level of imperceptibility and a PSNR in the region of 30-54 dB.

Zhang et al. [136] present a novel coverless picture steganography technique based on the DCT and Latent Dirichlet Allocation topic categorization to increase the robustness and capacity to resist picture steganography. To begin, the picture database is classified using the LDA topic model. Second, photos associated with a single subject are picked, and an 8*8 block DCT transform is applied to them. Then, using

the relationship between the Direct Current coefficients in neighboring blocks. Finally, an inverted index is constructed containing the feature sequence, dc, coordinates of the place, and the picture path. To achieve picture steganography, the secret information is transformed into a binary series and segmented. The picture with the feature sequence matching the personal information segments is chosen as the cover image based on the index. Following that, the recipient receives all cover photos. Throughout the procedure, no alteration is made to the source photographs. The experimental findings and analyses demonstrate that the proposed technique can evade detection by current steganalysis methods, is more resistant to conventional image processing, and is more resistant to subjective detection than current coverless picture steganography techniques. Meanwhile, it is somewhat immune to geometric assault. It has significant application potential in the secure transfer of large amounts of data in a big data environment.

Arunkumar et al. [137] present a complete picture steganographic technique based on a combination of the Redundant Integer Wavelet Transform (RIWT), Discrete Wavelet Transforms (DCT), Singular Value Decomposition (SVD), and the chaotic logistic map. Because RIWT is a consistent shift approach, this suggested methodology achieves reversibility and robustness. A higher degree of imperceptibility was attained by combining SVD and DCT with singleton value embedding. Additional security was provided by encrypting sensitive medical pictures using the chaotic logistic map, which further improved the technique's resilience. The suggested scheme's efficacy was compared to comparable methods published before using common characteristics such as imperceptibility, robustness, and resistance to multiple geometric transformation assaults. This methodology was found to be superior to other ways. Validation was conducted using the UCID benchmarking database.

Kaur and Butta [138] developed a unique hybrid methodology for undetectable and resilient picture steganography in the context of secure data exchange. The innovation of this work lies in the laborious adjustment of the Discrete Cosine Transform's (DCT) higher frequency coefficients to retain the image's perceptual quality, followed by the embedding of secret bits through random locations chosen by the deterministic Coupled Chaotic Map (CCM). All of the test suites developed by the National Institute of Standards and Technology, DIEHARD, ENT, and TestU01 validate that the CCM map is random. The experimental findings reveal that the suggested methodology produces high-quality stego-images with a zero Bit Error Rate when the embedding capacity is maximized (EC). Malevolent users cannot exploit the recommended approach, and it beats standard steganography approaches in terms of EC and Peak Signal to Noise Ratio.

Table 1. Table of comparison

Ref	Table of Comparison				
	year	Image size	Size of Secret data	Methods	PSNR
Anwar et al [119]	2019	1040*780	2 kb.txt	LSB	52.19 dB
AlWatyan et al [121]	2017	100*100	1857 bytes	LSB	54.16 dB
Swain [113]	2018	512*512	2357010 bit	PVD	42.91
Zhou & Cao [114]	2019	1024*768	53294 bit	PVD	46.59
Maji et al. [123]	2019	256*256	3088 bit	PVD	60.08 dB
Saha et al. [115]	2020	512 * 512	4 bpp	EMD	34.74 dB
Elshazly et al. [117]	2018	512 * 512	2,359,296 bits	GEMD	50.15 dB
Saleh& Amirmazlaghani [124]	2017	512*512	16384 bit	contourlet	52.8 dB
Subhedar & Vijay [131]	2019	512*512	image 512*512	CT-QR	56.67 dB
Thanki & Surekha [118]	2018	256*256	1572864 bit	DWT & FRT	58.99 dB
Rabie et al [133]	2018	512*512	20.48 bpp	DWT-LPAR	43 dB
Murugan and Ragupathy [135]	2019	512*512	45.8 kb	DWT	48.85 dB
Kaur & Butta [138]	2021	512*512	212,890	DCT	33.04 dB
Arunkumar et al [137]	2019	512*512	Secret image size 256 *256	SVD & DCT	50.12 dB

Qu et al. [139] offer a unique quantum picture steganography algorithm. The EMD embedding technique is a practical embedding approach that involves embedding the secret digit from a (2N + 1)-are notational system into a carrier pixel-group made up of N pixels, with just one carrier pixel raised or reduced by 1. The feasibility of designing a specialized quantum circuit to accomplish the EMD embedding is high. Some simulations based on MATLAB are also provided to assess the new algorithm's performance. It can be demonstrated that the proposed method has high imperceptibility and security by examining the visual effect between the original carrier pictures and the equivalent stego pictures, comparing histogram graphs, and calculating PSNR and BER values.

6. CONCLUSION

To transmit essential data safely and confidentially, there are two methods: either hiding or encrypting information. The science of data hiding is called Steganography. The data could be hidden in digital media such as (pictures, audio, and video). With the continuous development in Steganography, with traditional data masking techniques, there is a risk that the confidential data will be exposed. In this research, we review some of the methods used to hide information inside images. These techniques can be divided into two main parts, Spatial Domain, and Transform Domain. Also, each technique is divided into several algorithms, which are Least Significant Bit (LSB), Pixel Value Difference (PVD), Exploiting Modification Direction (EMD), contourlet transform, Discrete Wavelet Transformation (DWT) and, Discrete Cosine Transformation (DCT). We reviewed the best results in terms of highest PSNR, capacity, and more robustness and security. As shown from the results obtained by the researchers, we can determine the best two methods: CT-QR by [64] and DCT [71], which are reviewed in this paper.

As a future direction in this field, we suggest working on Blockchain-based image steganography for updating and sharing COVID-19 data in decentralized hospitals' intelligence architecture.

7. ASSESSMENT AND RECOMMENDATION

Several methods and algorithms have been used in the literature for hiding data, as observed from the previous section. Also, many criteria can be used to assess the accuracy of the method. The most well-known standards are (PSNR, capacity, robustness, and security) as it is challenging to obtain the highest value in terms of all mentioned criteria. Therefore, it was challenging for the researchers to devise new methods to balance these criteria to get the highest importance. Accordingly, we divided the literature into four sections: (PSNR, capacity, robustness, and security).

Researchers [111-118] tried to obtain high capacity via using several algorithms, where the highest embedding capacity was obtained by [118], which was 2,359,296 bits, while [113] reached 2,357,010 bits. However, we recommend the researcher's method [118] because the researcher could retain the PSNR, which was 51.15. although the (PSNR) value obtained by [117] was 58.99, the embedding capacity was less than the previously mentioned methods, reaching 1,572,864 bits.

On the other hand, to obtain the highest value for (PSNR), the researcher [123] achieved the highest value of PSNR, which was 60.08, but the embedding capacity was only 3088 bits. However, this method may not be helpful for cases that required high embedding capacity.

Hence, we can notice many ways to obtain high values for inclusion and (PSNR). Still, robustness and security must be verified to ensure that unauthorized persons cannot view the information that has been hidden. As noted in Table 1, the method that is presented by [131], which managed to obtain the highest value in terms of robustness by embedding an image (512 * 512) and (PSNR) was 56.67 with high robustness. While To obtain high security, the best results were obtained by the work presented by [138], where it was able to embed an image size (256 * 256), and the value (PSNR) was 50.12.

Through our review of the previous works, we recommend both methods [131] and [138] since they could obtain high Security and PSNR.

DISCLAIMER

The products used for this research are commonly and predominantly use products in our area of research and country. There is absolutely no conflict of interest between the authors and producers of the products because we do not

intend to use these products as an avenue for any litigation but for the advancement of knowledge. Also, the research was not funded by the producing company rather it was funded by personal efforts of the authors.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Rajendran S, Doraipandian M. "Chaotic map based random image steganography using lsb technique," IJ Network Security. 2017;19:593-598.
2. Ismael HR, Ameen SY, Kak SF, Yasin HM, Ibrahim IM, Ahmed AM, et al. "Reliable Communications for Vehicular Networks," Asian Journal of Research in Computer Science. 2021;33-49.
3. A. Khaldi, "Steganographic Techniques Classification According to Image Format," International Annals of Science. 2020;8: 143-149.
4. Abdullah RM, Ameen SY, Ahmed DM, Kak SF, Yasin HM, Ibrahim IM. et al. "Paralinguistic Speech Processing: An Overview," Asian Journal of Research in Computer Science. 2021;34-46.
5. Haref QM, Taha MS, M. Rahim MS, Hashim MM, Ahmad AMB. Rifa'i, Categorization of spatial domain techniques in image steganography: A revisit," Journal of Advanced Research in Dynamical and Control Systems. 2021;10: 1538-1551.
6. Ibrahim IM, Ameen SY, Yasin HM, Omar N, Kak SF, Rashid ZN, et al. "Web Server Performance Improvement Using Dynamic Load Balancing Techniques: A Review," Asian Journal of Research in Computer Science. 2021;47-62.
7. Ahmed DM, Ameen SY, Omar N, Kak SF, Rashid ZN, Yasin HM, et al. "A State of Art for Survey of Combined Iris and Fingerprint Recognition Systems," Asian Journal of Research in Computer Science. 2021;18-33.
8. Osuolale AF. "Secure data transfer over the internet using image cryptosteganography," Int. J. Sci. Eng. Res. 2017;8:1115-1121.
9. Maulud DH, Ameen SY, Omar N, Kak SF, Rashid ZN, Yasin HM, et al. "Review on Natural Language Processing Based on Different Techniques," Asian Journal of Research in Computer Science. 2021;1-17.
10. Salih AA, Ameen SY, Zeebaree SR, Sadeeq MA, Kak SF, Omar N, et al. "Deep Learning Approaches for Intrusion Detection," Asian Journal of Research in Computer Science. 2021;50-64.
11. AL_Zubaidy MA, AL Janaby AO, Ameen SY. "5G Scheduling Algorithm For Capacity Improvement Using Beam Division at Congested Traffic," Journal of Engineering Science and Technology. 2021;16:1977-1990.
12. Khuma ZN. "Secure Data Transfer using RSA and Steganography; 2019.
13. Mohammed K, Ameen S. "Performance investigation of distributed orthogonal space-time block coding based on relay selection in wireless cooperative systems;" 2019.
14. Fawzi LM, Alqarawi SM, Ameen SY, Dawood SA. "Two Levels alert verification technique for smart oil pipeline surveillance system (SOPSS)," International Journal of Computing and Digital Systems. 2019;8: 115-124.
15. Das R, Chatterjee P. "Securing data transfer in IoT employing an integrated approach of cryptography & steganography," in Proceedings of the International Conference on High Performance Compilation, Computing and Communications. 2017;17-22.
16. Al-Sultan MR, Ameen SY, Abduallah WM. "Real time implementation of stegofirewall system," International Journal of Computing and Digital Systems. 2019;8: 498-504, 2019.
17. Al Janaby AO, Al-Omary A, Ameen SY, Al-Rizzo HM. "Tracking high-speed users using SNR-CQI mapping in LTE-A networks," in International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), 2018;1-7.
18. Othman A, Ameen SY, Al-Rizzo H. Dynamic switching of scheduling algorithm for," International Journal of Computing and Network Technology. 2018;6.
19. Awadh WA, Hashim AS. "Using steganography for secure data storage in cloud computing," International Research Journal of Engineering and Technology (IRJET). 2017;4.
20. Ameen SY, Ali ALSH. "A comparative study for new aspects to quantum key

distribution," Journal of Engineering and Sustainable Development. 2018;11:45-57.
21. Fawzi LM, Ameen SY, Alqaraawi SM, Dawwd SA. "Embedded real-time video surveillance system based on multi-sensor and visual tracking," Appl. Math. Infor. Sci. 2018;12:345-359.
22. Ali ZA, Ameen SY. "Detection and prevention cyber-attacks for smart buildings via private cloud environment," International Journal of Computing and Network Technology. 2018;6:27-33, 2018.
23. Hamed ZA, Ahmed IM, Ameen SY, "Protecting Windows OS Against Local Threats Without Using Antivirus," relation. 2020;29:64-70.
24. Fawzi LM, Ameen SY, Dawwd SA, Alqaraawi SM. "Comparative study of ad-hoc routing protocol for oil and gas pipelines surveillance systems," International Journal of Computing and Network Technology. 2016;4.
25. Farhan FY, Ameen SY. "Improved hybrid variable and fixed step size least mean square adaptive filter algorithm with application to time varying system identification," in 2015 10th System of Systems Engineering Conference (SoSE), 2015;94-98.
26. Othman A, Ameen SY, Al-Rizzo H. "A new channel quality indicator mapping scheme for high mobility applications in LTE systems," Journal of Modeling and Simulation of Antennas and Propagation. 2015;1:38-43.
27. Othman A, Othman SY, Al-Omary A, Al-Rizzo H. "Comparative performanceof subcarrier schedulers in uplink LTE-A under high users' mobility," International Journal of Computing and Digital Systems. 2015;4.
28. Othman A, Ameen SY, Al-Rizzo H. "An energy-efficient MIMO-based 4G LTE-A adaptive modulation and coding scheme for high mobility scenarios," International Journal of Computing and Network Technology. 2015;3.
29. Ameen SY. "Advanced encryption standard (AES) enhancement using artificial neural networks," Int J of Scientific & Engineering Research. 2014;5.
30. Zeebaree S, Ameen S, Sadeeq M. "Social media networks security threats, risks and recommendation: A case study in the kurdistan region," International Journal of Innovation, Creativity and Change. 2020; 13:349-365.
31. Yahia HS, Zeebaree SR, Sadeeq MA, Salim NO, Kak SF, Adel AZ, et al., "Comprehensive survey for cloud computing based nature-inspired algorithms optimization scheduling," Asian Journal of Research in Computer Science. 2021;1-16.
32. Ageed ZS, Zeebaree SR, Sadeeq MM, Kak SF, Rashid ZN, Salih AA, et al. "A survey of data mining implementation in smart city applications," Qubahan Academic Journal. 2021;1:91-99.
33. Al Janaby AO, Al-Omary A, Ameen SY, Al-Rizzo H. "Tracking and Controlling High-Speed Vehicles Via CQI in LTE-A Systems," International Journal of Computing and Digital Systems. 2020;9: 1109-1119.
34. Ageed ZS, Zeebaree SR, Sadeeq MA, Abdulrazzaq MB, Salim BW, Salih AA, et al. "A state of art survey for intelligent energy monitoring systems," Asian Journal of Research in Computer Science. 2021; 46-61.
35. Abdulqadir HR, Zeebaree SR, Shukur HM, Sadeeq MM, Salim BW, Salih AA, et al. "A study of moving from cloud computing to fog computing," Qubahan Academic Journal. 2021;1:60-70.
36. Shukur H, Zeebaree S, Zebari R, Zeebaree D, Ahmed O, Salih A. "Cloud computing virtualization of resources allocation for distributed systems," Journal of Applied Science and Technology Trends. 2020;1:98-105.
37. Sharif KH, Ameen SY. "A Review of Security Awareness Approaches With Special Emphasis on Gamification," in 2020 International Conference on Advanced Science and Engineering (ICOASE). 2020;151-156.
38. Abdulla AI, Abdulraheem AS, Salih AA, Sadeeq M, Ahmed AJ, Ferzor BM, et al. "Internet of things and smart home security," Technol. Rep. Kansai Univ. 2020;62:2465-2476.
39. Abdulraheem AS, Salih AA, Abdulla AI, Sadeeq M, Salim N, Abdullah H, et al. "Home automation system based on IoT; 2020.
40. Salih AA, Zeebaree S, Abdulraheem AS, Zebari RR, Sadeeq M, Ahmed OM. "Evolution of mobile wireless communication to 5G revolution," Technology Reports of Kansai University. 2020;62:2139-2151.

41. Khalid LF, Ameen SY. "Secure Iot integration in daily lives: A review," Journal of Information Technology and Informatics. 2021;1:6-12.
42. Dino HI, Zeebaree S, Salih AA, Zebari RR, Ageed ZS, Shukur HM, et al. "Impact of Process Execution and Physical Memory-Spaces on OS Performance," Technology Reports of Kansai University. 2020;62: 2391-2401.
43. Ageed ZS, Zeebaree SR, Sadeeq MM, Kak SF, Yahia HS, Mahmood MR. et al. "Comprehensive survey of big data mining approaches in cloud systems," Qubahan Academic Journal. 2021;1:29-38.
44. Abdulrahman LM, Zeebaree SR, Kak SF, Sadeeq MA, Adel AZ, Salim BW, et al. "A state of art for smart gateways issues and modification," Asian Journal of Research in Computer Science. 2021;1-13.
45. Yazdeen AA, Zeebaree SR, Sadeeq MM, Kak SF, Ahmed OM, Zebari RR. "FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review," Qubahan Academic Journal. 2021;1:8-16.
46. Malallah H, Zeebaree SR, Zebari RR, Sadeeq MA, Ageed ZS, Ibrahim IM, et al. "A comprehensive study of kernel (issues and concepts) in different operating systems," Asian Journal of Research in Computer Science. 2021;16-31.
47. Abdullah DM, Ameen SY. "Enhanced Mobile Broadband (EMBB): A review," Journal of Information Technology and Informatics. 2021;1:13-19.
48. Ibrahim IM. "Task scheduling algorithms in cloud computing: A review," Turkish Journal of Computer and Mathematics Education (TURCOMAT). 2021;12:1041-1053.
49. Zebari IM, Zeebaree SR, Yasin HM. Real time video streaming from multi-source using client-server for video distribution," in 2019 4th Scientific International Conference Najaf (SICN). 2019;109-114.
50. Yasin HM, Zeebaree SR, Zebari IM. "Arduino based automatic irrigation system: Monitoring and SMS controlling," in 2019 4th Scientific International Conference Najaf (SICN). 2019;109-114.
51. Zeebaree S, Yasin HM. "Arduino based remote controlling for home: power saving, security and protection," International Journal of Scientific & Engineering Research. 2014;5:266-272.
52. Zeebaree S, Zebari I. "Multilevel client/server peer-to-peer video broadcasting system," International Journal of Scientific & Engineering Research. 2014;5:260-265.
53. Taher KI, Saeed RH, Ibrahim RK, Rashid ZN, Haji LM, Omar N, et al. "Efficiency of semantic web implementation on cloud computing: A review," Qubahan Academic Journal. 2021;1:1-9.
54. Amanuel SVA, Ameen SYA. "Device-to-device communication for 5G security: A Review, Journal of Information Technology and Informatics. 2021;1:26-31.
55. Zebari S. Yaseen NO. "Effects of parallel processing implementation on balanced load-division depending on distributed memory systems," J. Univ. Anbar Pure Sci. 2011;5:50-56.
56. Sadeeq MM, Abdulkareem NM, Zeebaree SR, Ahmed DM, Sami AS, Zebari RR. "IoT and Cloud computing issues, challenges and opportunities: A review," Qubahan Academic Journal. 2021;1:1-7.
57. Aziz ZAA, Ameen SYA. "Air pollution monitoring using wireless sensor Networks," Journal of Information Technology and Informatics. 2021;1:20-25.
58. Kareem FQ, Zeebaree SR, Dino HI, Sadeeq MA, Rashid ZN, Hasan DA, et al. A survey of optical fiber communications: challenges and processing time influences," Asian Journal of Research in Computer Science. 2021;48-58.
59. Omer MA, Zeebaree SR, Sadeeq MA, Salim BW, Mohsin SX, Rashid ZN, et al. "Efficiency of malware detection in android system: A survey," Asian Journal of Research in Computer Science. 2021;59-69.
60. Rashid ZN, Zeebaree S, Sengur A. Novel remote parallel processing code-breaker system via cloud computing," ed: TRKU; 2020.
61. Rashid ZN, Zeebaree SR, Shengul A. Design and analysis of proposed remote controlling distributed parallel computing system over the cloud," in 2019 International Conference on Advanced Science and Engineering (ICOASE). 2019; 118-123.
62. Rashid ZN, Zebari SR, Sharif KH, Jacksi K. "Distributed cloud computing and distributed parallel computing: A review," in International Conference on Advanced Science and Engineering (ICOASE). 2018;167-172.

63. Rashid ZN, Sharif KH, Zeebaree S. "Client/Servers clustering effects on CPU execution-time, CPU usage and CPU Idle depending on activities of Parallel-Processing-Technique operations," Int. J. Sci. Technol. Res. 2018;7:106-111.
64. Jijo BT, Zeebaree SR, Zebari RR, Sadeeq MA, Sallow AB, Mohsin S, et al. "A comprehensive survey of 5G mm-wave technology design challenges," Asian Journal of Research in Computer Science. 2021;1-20.
65. Abdullah SMSA, Ameen SYA, Sadeeq MA, Zeebaree S. Multimodal emotion recognition using deep learning, Journal of Applied Science and Technology Trends. 2021;2:52-58.
66. Sadeeq MA, Zeebaree S. Energy management for internet of things via distributed systems," Journal of Applied Science and Technology Trends. 2021;2: 59-71.
67. Maulud DH, Zeebaree SR, Jacksi K, Sadeeq MAM, Sharif KH. "State of art for semantic analysis of natural language processing," Qubahan Academic Journal. 2021;1:21-28.
68. Hasan DA, Hussan BK, Zeebaree SR, Ahmed DM, Kareem OS, Sadeeq MA. The impact of test case generation methods on the software performance: A review," International Journal of Science and Business. 2021;5:33-44.
69. Shukur H, Zeebaree SR, Ahmed AJ, Zebari RR, Ahmed O, Tahir BSA, et al. "A state of art survey for concurrent computation and clustering of parallel computing for distributed systems," Journal of Applied Science and Technology Trends. 2020;1:148-154.
70. Yasin HM, Zeebaree SR, Sadeeq MA, Ameen SY, Ibrahim IM, Zebari RR, et al. IOT and ICT based Smart Water Management, Monitoring and Controlling System: A Review," Asian Journal of Research in Computer Science. 2021;42-56.
71. Jacksi K, Ibrahim RK, Zeebaree SR, Zebari RR, Sadeeq MA. "Clustering documents based on semantic similarity using HAC and K-mean algorithms," in 2020 International Conference on Advanced Science and Engineering (ICOASE). 2020;205-210.
72. Sadeeq MA, Abdulazeez AM. "Neural networks architectures design, and applications: A review," in 2020 International Conference on Advanced Science and Engineering (ICOASE). 2020; 199-204.
73. Ageed ZS, Ibrahim RK, Sadeeq M. "Unified ontology implementation of cloud computing for distributed systems," Current Journal of Applied Science and Technology. 2020;82-97.
74. Sulaiman MA, Sadeeq M, Abdulraheem AS, Abdulla AI. "Analyzation study for gamification examination fields," Technol. Rep. Kansai Univ. 2020;62:2319-2328.
75. Hassan RJ, Zeebaree SR, Ameen SY, Kak SF, Sadeeq MA, Ageed ZS. et al., "State of art survey for iot effects on smart city technology: challenges, opportunities, and solutions," Asian Journal of Research in Computer Science. 2021;32-48.
76. Sadeeq M, Abdulla AI, Abdulraheem AS, Ageed ZS. "Impact of electronic commerce on enterprise business," Technol. Rep. Kansai Univ. 2020;62:2365-2378.
77. Haji SH, Zeebaree SR, Saeed RH, Ameen SY, Shukur HM, Omar N, et al. Comparison of Software Defined Networking with Traditional Networking," Asian Journal of Research in Computer Science. 2021;1-18.
78. Alzakholi O, Shukur H, Zebari R, Abas S, Sadeeq M. "Comparison among cloud technologies and cloud performance," Journal of Applied Science and Technology Trends. 2020;1:40-47.
79. Ageed Z, Mahmood MR, Sadeeq M, Abdulrazzaq MB, Dino H. "Cloud computing resources impacts on heavy-load parallel processing approaches," IOSR Journal of Computer Engineering (IOSR-JCE). 2020;22:30-41.
80. Dino HI, Zeebaree SR, Hasan DA, Abdulrazzaq MB, Haji LM, Shukur HM. "COVID-19 Diagnosis Systems Based on Deep Convolutional Neural Networks Techniques: A Review," in 2020 International Conference on Advanced Science and Engineering (ICOASE). 2020; 184-189.
81. Izadeen GY, Ameen SY. "Smart Android Graphical Password Strategy: A Review," Asian Journal of Research in Computer Science. 2021;59-69.
82. Zebari RR, Zeebaree SR, Sallow AB, Shukur HM, Ahmad OM, Jacksi K. Distributed Denial of Service Attack Mitigation using High Availability Proxy and Network Load Balancing," in 2020 International Conference on Advanced

Science and Engineering (ICOASE). 2020; 174-179.
83. Sallow A, Zeebaree S, Zebari R, Mahmood M, Abdulrazzaq M, Sadeeq M. "Vaccine tracker," SMS reminder system: Design and implementation; 2020.
84. Haji SH, Ameen SY. "Attack and Anomaly Detection in IoT Networks using Machine Learning Techniques: A Review," Asian Journal of Research in Computer Science. 2021; 30-46.
85. Sadeeq MA, Zeebaree SR, Qashi R, Ahmed SH, Jacksi K. "Internet of Things security: a survey," in 2018 International Conference on Advanced Science and Engineering (ICOASE). 2018;162-166.
86. Abdulazeez AM, Zeebaree SR, Sadeeq MA. "Design and implementation of electronic student affairs system," Academic Journal of Nawroz University. 2018;7:66-73.
87. Sallow AB, Sadeeq M, Zebari RR, Abdulrazzaq MB, Mahmood MR, Shukur HM, et al. "An investigation for mobile malware behavioral and detection techniques based on android platform," IOSR Journal of Computer Engineering (IOSR-JCE). 2020;22:14-20.
88. Mohammed SM, Jacksi K, Zeebaree SR. Glove Word Embedding and DBSCAN algorithms for Semantic Document Clustering," in International Conference on Advanced Science and Engineering (ICOASE). 2020;1-6.
89. Hasan BMS, Ameen SY, Hasan OMS. Image Authentication Based on Watermarking Approach," Asian Journal of Research in Computer Science. 2021;34-51.
90. Singh PK, Tripathi P, Kumar R, Kumar D. Secure Data Transmission," International Research Journal of Engineering and Technology. 2017;4:217-222.
91. Hussain M, Wahab AWA, Idris YIB, Ho AT, Jung KH. "Image steganography in spatial domain: A survey," Signal Processing: Image Communication. 2018;65:46-66.
92. Kothari L, Thakkar R, Khara S. "Data hiding on web using combination of Steganography and Cryptography," in 2017 International Conference on Computer, Communications and Electronics (Comptelix). 2017;448-452.
93. Reddy VL. "Improved Secure Data Transfer Using Video Steganographic Technique," International Journal of Rough Sets and Data Analysis (IJRSDA). 2017;4: 55-70.
94. Yahaya MM, Ajibola A. "Cryptosystem for Secure Data Transmission using Advance Encryption Standard (AES) and Steganography," International Journal of Sci-entific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN: 2456-3307. 2019;5: 317-322.
95. Wang J, Cheng M, Wu P, Chen B. "A Survey on Digital Image Steganography," Journal of Information Hiding and Privacy Protection. 2019;1:87.
96. Emad E, Safey A, Refaat A, Osama Z, Sayed E, Mohamed E. "A secure image steganography algorithm based on least significant bit and integer wavelet transform," Journal of Systems Engineering and Electronics. 2018;29:639-649.
97. C. Irawan, C. A. Sari, and E. H. Rachmawanto, "Hiding and securing message on edge areas of image using LSB steganography and OTP encryption," in 2017 1st International Conference on Informatics and Computational Sciences (ICICoS), 2017, pp. 1-6.
98. AlKhamese AY, Shabana WR, Hanafy IM. "Data security in cloud computing using steganography: a review," in 2019 International Conference on Innovative Trends in Computer Engineering (ITCE). 2019;549-558.
99. Ruchi R, Ghanekar U. "A Brief Review on Image Steganography Techniques," in Proceedings of the International Conference on Advances in Electronics, Electrical & Computational Intelligence (ICAEEC); 2019.
100. Goyal S, Nehra MS. "Image Steganography Technique to Increase Security of Images: A Review; 2019.
101. Younus ZS, Hussain MK. "Image steganography using exploiting modification direction for compressed encrypted data," Journal of King Saud University-Computer and Information Sciences; 2019.
102. Leng HS, Tseng HW. "Generalize the EMD scheme on an n-dimensional hypercube with maximum payload," Multimedia Tools and Applications. 2019;78:18363-18377.
103. Abduallah WM, Rahma AMS. "A review on steganography techniques," American Scientific Research Journal for

Engineering, Technology, and Sciences (ASRJETS). 2016;24:131-150.
104. Arora H, Bansal C, Dagar S. "Comparative study of image steganography techniques," in 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 2018;982-985.
105. Wu X, Li J, Tu R, Cheng J, Bhatti UA, Ma J. "Contourlet-DCT based multiple robust watermarkings for medical images," Multimedia Tools and Applications. 2019;78:8463-8480.
106. Zeebaree DQ, Abdulazeez AM, Hassan OMS, Zebari DA, Saeed JN. "Hiding Image by Using Contourlet Transform," ed: press; 2020.
107. Hameed AS. "High Capacity Audio Steganography Based on Contourlet Transform," Tikrit Journal of Engineering Sciences. 2018;25:1-7.
108. Cahya R, Arief P, Novriza A, Kohei A. "Noble Method for Data Hiding using Steganography Discrete Wavelet Transformation and Cryptography Triple Data Encryption Standard: DES," International Journal of Advanced Computer Science and Applications. 2018; 9.
109. Muhuri PK, Ashraf Z, Goel S. "A novel image steganographic method based on integer wavelet transformation and particle swarm optimization," Applied Soft Computing. 2020;92:106257.
110. Latef AA. "Color Image Steganography Based on Discrete Wavelet and Discrete Cosine Transforms," *Ibn AL-Haitham* Journal for Pure and Applied Science. 2017; 24.
111. Subong RA, Fajardo AC, Kim YJ. "LSB Rotation and Inversion Scoring Approach to Image Steganography," in 2018 15th International Joint Conference on Computer Science and Software Engineering (JCSSE). 2018;1-4.
112. Elharrouss O, Almaadeed N, Al-Maadeed S. "An image steganography approach based on k-least significant bits (k-LSB)," in 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). 2020;131-135.
113. Swain G. "Adaptive and non-adaptive PVD steganography using overlapped pixel blocks," Arabian Journal for Science and Engineering. 2018;43:7549-7562.
114. Zhou L, Cao Y. "Combined Algorithm of Steganography with Matrix Pattern and Pixel Value Difference," in 2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET). 2019;6-10.
115. Saha S, Chakraborty A, Chatterjee A, Dhargupta S, Ghosal SK, Sarkar R. "Extended exploiting modification direction based steganography using hashed-weightage Array," Multimedia Tools and Applications. 2020;79;20973-20993.
116. Liu Y, Yang C, Sun Q. "Enhance embedding capacity of generalized exploiting modification directions in data hiding," IEEE Access. 2017;6:5374-5378.
117. Elshazly E, Abdelwahab SA, Fikry R, Zahran O, Elaraby S, El-Kordy M. "FPGA implementation of image steganography algorithms using generalized exploiting modification direction and pixel segmentation strategy," in 2018 35th National Radio Science Conference (NRSC). 2018;258-265.
118. Thanki R, Borra S. "A color image steganography in hybrid FRT–DWT domain," Journal of information security and applications. 2018;40:92-102.
119. Anwar F, Rachmawanto EH, Sari CA. StegoCrypt Scheme using LSB-AES Base64," in 2019 International Conference on Information and Communications Technology (ICOIACT). 2019;85-90.
120. Rafrastara FA, Prahasiwi R, Rachmawanto EH, Sari CA. "Image Steganography using Inverted LSB based on 2 nd, 3 rd and 4 th LSB pattern," in 2019 International Conference on Information and Communications Technology (ICOIACT). 2019;179-184.
121. AlWatyan A, Mater W, Almutairi O, Almutairi M, Al-Noori A. "Security approach for LSB steganography based FPGA implementation," in 2017 7th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), 2017;1-5.
122. Astuti YP, Rachmawanto EH, Sari CA. "Simple and secure image steganography using LSB and triple XOR operation on MSB," in *2018 International Conference on* Information and Communications Technology (ICOIACT). 2018;191-195.
123. Maji G, Mandal S, Debnath NC, Sen S. Pixel value difference based image steganography with one time pad encryption," in 2019 IEEE 17th International Conference on Industrial Informatics (INDIN). 2019;1358-1363.

124. Saleh F, Amirmazlaghani M. "A Novel Multiplicative Steganography Technique in Contourlet Domain," in 2017 14th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC). 2017; 105-110.
125. Reshma V, Kumar RV, Shahi D, Shyjith M. Optimized support vector neural network and contourlet transform for image steganography," Evolutionary Intelligence. 2020;1-17.
126. Nevriyanto A, Sutarno S, Siswanti SD, Erwin E. "Image steganography using combine of discrete wavelet transform and singular value decomposition for more robustness and higher peak signal noise ratio," in 2018 International Conference on Electrical Engineering and Computer Science (ICECOS). 2018;147-152.
127. Kukharska N, Lagun A, Polotai O. "The Steganographic Approach to Data Protection Using Arnold Algorithm and the Pixel-Value Differencing Method," in 2020 IEEE Third International Conference on Data Stream Mining & Processing (DSMP). 2020;174-177.
128. Shehab JN, Abdulkadhim HA, Allbadi Y. Blind image watermarking scheme based on lowest energy contourlet transform coefficient and modified arnold cat/ikeda maps," Indonesian Journal of Electrical Engineering and Computer Science. 2021;21:196-207.
129. Li JY, Zhang CZ. "Blind watermarking scheme based on Schur decomposition and non-subsampled contourlet transform," Multimedia Tools and Applications. 2020; 79:30007-30021.
130. Najafi E, Loukhaoukha K. "Hybrid secure and robust image watermarking scheme based on SVD and sharp frequency localized contourlet transform," Journal of information security and applications. 2019;44:144-156.
131. Subhedar MS, Mankar VH. "Image steganography using contourlet transform and matrix decomposition techniques," Multimedia Tools and Applications. 2019;78:22155-22181.
132. Giri KJ, Bashir R. "A block based watermarking approach for color images using discrete wavelet transformation," *International* Journal of Information Technology. 2018;10:139-146.
133. Rabie T, Baziyad M, Kamel I. "Enhanced high capacity image steganography using discrete wavelet transform and the Laplacian pyramid," Multimedia Tools and Applications. 2018;77:23673-23698.
134. Abdel Qader A. A novel image steganography approach using multi-layers DCT features based on support vector machine classifier," The International Journal of Multimedia & Its Applications (IJMA). 2017;9.
135. Murugan GVK, Subramaniyam RU. "Performance analysis of image steganography using wavelet transform for safe and secured transaction," Multimedia Tools and Applications. 2019;1-15.
136. Zhang X, Peng F, Long M. "Robust coverless image steganography based on DCT and LDA topic classification," IEEE Transactions on Multimedia. 2018;20: 3223-3238.
137. Arunkumar S, Subramaniyaswamy V, Vijayakumar V, Chilamkurti N, Logesh R. SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images," Measurement. 2019;139:426-437.
138. Kaur R, Singh B. "A hybrid algorithm for robust image steganography," Multidimensional Systems and Signal Processing. 2021;32:1-23.
139. Qu Z, Cheng Z, Liu W, Wang X. "A novel quantum image steganography algorithm based on exploiting modification direction," Multimedia Tools and Applications. 2019; 78:7981-8001.

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sdiarticle4.com/review-history/70381