IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 3 January 2023, accepted 13 January 2023, date of publication 16 January 2023, date of current version 23 January 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3237393

SURVEY

A Comprehensive Study of Digital Image Steganographic Techniques

SHAHID RAHMAN[1], JAMAL UDDIN[1], MUHAMMAD ZAKARYA[2,3], (Senior Member, IEEE), HAMEED HUSSAIN[4], AYAZ ALI KHAN[5], AFTAB AHMED[2], AND MUHAMMAD HALEEM[6]

[1]Department of Computer Science, Qurtuba University of Science and Information Technology, Peshawar 29050, Pakistan
[2]Department of Computer Science, Abdul Wali Khan University, Mardan 23200, Pakistan
[3]Faculty of Computing and Information Technology, Sohar University, Sohar 311, Oman
[4]Department of Computer Science, University of Buner, Khyber Pakhtunkhwa, Buner 19280, Pakistan
[5]Department of Computer Science, University of Lakki Marwat, Khyber Pakhtunkhwa, Lakki 28420, Pakistan
[6]Department of Computer Science, Kardan University, Kabul 1003, Afghanistan

Corresponding author: Muhammad Haleem (m.haleem@kardan.edu.af)

This work was supported in part by the Kardan University, Kabul, Afghanistan; and in part by the Abdul Wali Khan University, Mardan, Pakistan.

ABSTRACT Steganography surpasses other mechanisms of securing data from potential threats. The modern digital arena calls for robust information hiding techniques and, thus, it has always been a flash point for researchers and academicians. Nowadays, transmission is susceptible to numerous hacks while sharing secret information through typical correspondence channel. Accordingly, everybody needs the classification, respectability, and realness of his or her privileged information. Particularly, different techniques are used to take on these security issues like advanced declaration, computerized mark, and cryptography. Nevertheless, these strategies alone cannot be negotiated. Steganography is a revolution where current information compression, data hypothesis, spread range, and cryptography advancements are integrated to meet the requirements for protection of data over the Internet. This study investigates and critically analyses various existing cover steganography techniques and identifies the valuable region that everyone can be benefited. Moreover, we present a comprehensive overview of the fundamental concepts with in the domain of the steganographic methods and steganalysis. These systems have been depicted in numerous areas of the steganography such as spatial space, transform domain, and adaptive space. Moreover, each space has its particular traits. A few regularly involved techniques for improving the steganographic security and upgrading steganalysis capacity are elaborated, summed up; and conceivable examination patterns are talked about. We also systematically separate different methodologies in our review and show their pros and cons, qualities, challenges and significance.

INDEX TERMS Steganography, data concealing, cover objects, image quality assessment metrics.

I. INTRODUCTION

The cutting-edge security mechanism is indispensable for confidential communication in every walk of life that is regulated by the internet. Therefore, steganography, which is one of the arts and sciences of concealing information from unauthorized access, has acquired a lot of consideration, recently. Steganography has its roots from two different Greek words: steganos, that means covered and graphy, that means writing. Figure 1 shows the basic model of the steganography method. It is considered as ''to establish an invisible communication technique to hide information from the observer'' [1]. It aims at concealing one's secrete data by embedding it in readable data called cover data. Steganography is the specialty of passing information on that cannot be recognized or identified [2]. Histaiacus, in fact, shaved a slave's head and inked a hidden note on his skull in the 5th century [3], which is considered one of the oldest technique of Steganography.

A Chinese old technique for secret composition was endorsed to Cardan Grille (1501-1576) [4]. Furthermore, Unsatisfactory Ciphers, imperceptible ink procedures, and Microdots, were also uncommonly renowned steganographic

The associate editor coordinating the review of this manuscript and approving it for publication was Yiming Tang.

strategies during World War II. For a long period, such types of techniques are used for secret communication [5]. Currently, the fine art of advance cover steganography can be considered as the valuable hiding secret information mechanism using digital media [6]. Hameed et al. [7] described for achieving the confidentiality of the secret information, the speciality of cover steganography is used. Different experts characterize advanced steganography as an undertaking of concealing computerized data in stealthy channels so one can cover some data and expect recognition of this secret data [8].

A better cover steganography system has the ability to encrypt a secret message in such a manner that no one can be suspicious of it, detect secret information within the image, or cover objects [9]. Normally, there are a few sorts of advanced media, which can be utilized for concealing privileged data like pictures, video, sound, and text as displayed in Figures 2 and 3. These advanced media have various qualities to implant privileged data [10], where the best mechanism for installing cover objects ought to have two essentials to be imperceptible to any unapproved assailants and the object or medium ought to be famous [11].

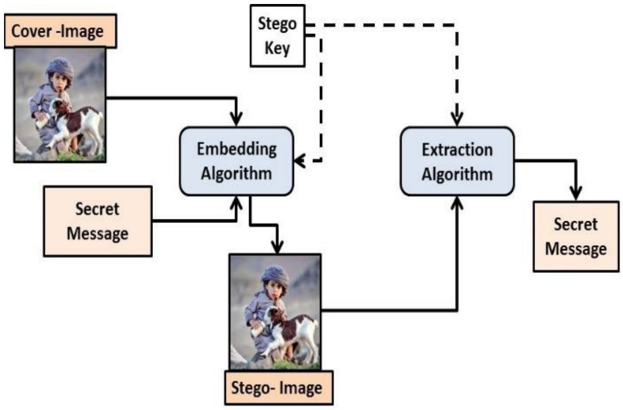

FIGURE 1. Normal Structure of the Steganography.

The key contributions of this survey article can be summarized as follows:

- We study investigates and critically analyses various cover steganography techniques and identifies the valuable region that everyone can be benefited of.
- We offer an overview of various procedures and cutting-edge strategies that have been suggested by the numerous scientists. in numerous areas of steganography such as spatial space, transform domain, and adaptive space.

We separate different methodologies in our review and show their qualities. Nevertheless, the majority of the methods introduced in the existing research were profoundly centred on the spatial space. Spatial space procedures rely entirely upon the pixels of the picture for information inserting. To accomplish the target of cover steganography, most of time direct control of the pixels is achieved. Consequently, less tedious and basics procedure is spatial space. However, this study closes for certain proposals and allies for the caries-situated component.

The rest of this survey article is organized as follows. In section II, we describe the basic concepts, types, and applications of the Steganography approach. Various approaches of the image Steganography are deliberated in section III. In section IV, a comprehensive analysis of various image Steganography techniques is presented along with their merits and demerits. Performance evaluation metrics are defined in section V. An analysis of the security for the mentioned Steganography methods is presented in section VI. Various challenges and future directions for the Steganography techniques are deliberated in section VII. Finally, section VIII conclude this survey.

II. BASIC CONCEPTS AND TERMINOLOGIES

A. DIGITAL MEDIUMS OF STEGANOGRAPHY

Depending upon a cover object steganography techniques used generally five types for embedding secret messages. Which are explained one by one respectively.

1) IMAGE STEGANOGRAPHY

For inserting the encoded data, a picture is utilized. In this sort of steganography, image pixels are utilized for encrypting secret message bits. Due to its generous measure of respective bits, the image is a widely used object and thought to be the best cover [12].

2) NETWORK STEGANOGRAPHY

The type of Network Steganography is the kinds of steganography, which are used network protocols as cover object such as IP, TCP, ICMP and UDP and so on. Information is concealed in a couple of fields of the header of TCP/IP bundles that is open or never used [13].

3) AUDIO STEGANOGRAPHY

This kind of audio steganography is tied in with concealing a mystery message in the Audio. It is a method used to get the transmission of privileged conceals its presence. It additionally may give privacy to secret messages assuming that the message is encoded. It used some digital plans like as WAVE, AVI, MPED, MIDI or etc. [14].

4) VIDEO STEGANOGRAPHY

Video steganography is a part of information stowing away, which is a strategy that embeds messages into cover contents and is utilized in many fields like clinical frameworks, policing security, access control, and so forth. DCT changes ordinarily alter values 8.667 - 9. Shroud the information in every one of the images in the video and utilized which isn't recognizable by the HVS. Mp4, MPEG, H.264, and AVI etc. are the formats utilized by video steganography [15], [16].

5) TEXT STEGANOGRAPHY

In this kind of the text steganography, it is a component of concealing mystery text messages inside one more message as a covering message or creating a cover message connected with the first mystery message. [17].

B. BASIC STRUCTURE OF STEGANOGRAPHY

The fundamentals of Steganography are made up of three mechanisms, which are shown in Figure 2 and explained below.

The Cover or Carrier: For encrypting the secret information, the cover item can be an image (spat, jpg, bmp, png, and so on), an mp3 (sound documents), a message record, a video record, and, surprisingly, a TCP/IP bundle too.

The Message: It can be a simple text or content, a secret image, an audio or video that is going to be transmitted securely.

The Key: Key based steganography is also play a vital role. In the time of encoding and decoding key is used and it tends to be an instance, dark light or irregular numbers, and so forth. depending upon when we encrypting secret message. Key is only to communication body and also gives more robustness, tough time to attackers etc.

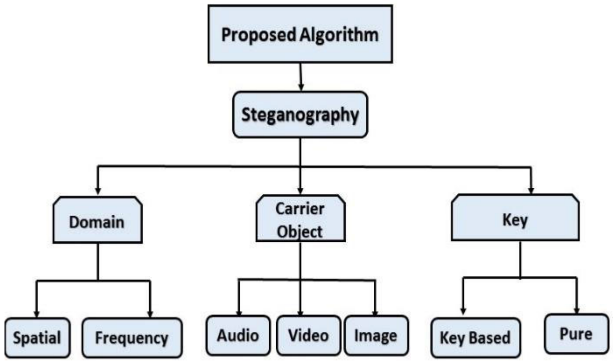

FIGURE 2. Image Steganography Classification

Confidential data is concealing within the image in a way that the attackers cannot detect the secret information. Embedded image can be obtained through encrypted algorithm. When an embedded image is created from encrypted algorithm then must have a little distortion that no clever eye can be detect. The message can be extracted from stego media through decrypted algorithm. Figure 3 shows the Taxonomy of image steganography and also shows the Domains, Mediums and Techniques used in various domain for different object for Steganography.

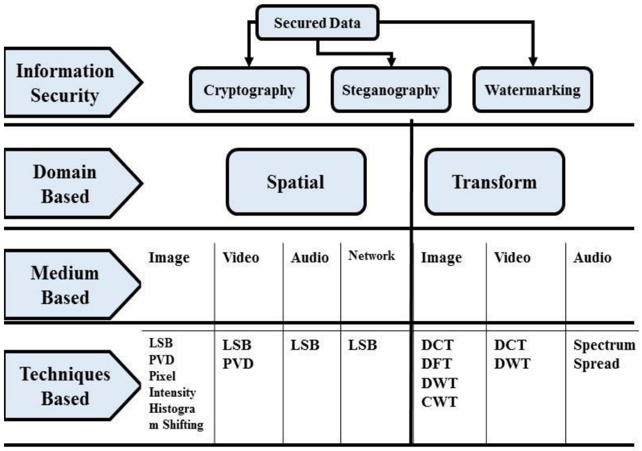

FIGURE 3. Taxonomy of Steganography techniques.

Table 1 shows different criteria of the Watermarking, Cryptography, and Steganography methods which are mainly used for up to date information security. It also explains the basics needs of the said areas which is strongly required for researchers who want to work and use any of them to conceal their useful data for security purposes.

C. APPLICATION OF STEGANOGRAPHY

Simply, if anyone wants to embed confidential information within any cover object steganography can be used anytime. There are many motivations to conceal information, yet they generally come into the longing to keep unapproved people from arriving at the information or after charming mindful of the presence of a secret data. It can stand utilized viably in the programmed observing of music or radio notice and so on [18]. There are a few different applications, which can utilize steganography to maintain their substitutions of mystery messages [19], including:

- Protection of Data Alteration
- Modern computer and networking technology
- Media
- Data Base System
- Intelligence services or Intellectual Properties.
- groups and companies
- Medical imaging systems
- Securing multimodal biometric data.
- Digital Watermarking
- E-Commerce
- Corporations with trade secrets to protect.
- Military and defense communication.
- Steganography may become limited under laws because of government suspect that some lawbreakers use it.

In sum up, some critically analysis about various applications of image steganography is that the one file type of cover communication for steganography image is widely used. Therefore, for secure communication image is used in everywhere for communication between end users. Therefore, it is necessary to analyzed image that which type of image are suitable for which area. There is some key point to be noted about image.

Secret Correspondences; The utilization steganography doesn't expose secret correspondence and thusly gaps investigation of the source side, message, and beneficiary. Confidential, outline, or other touchy data can be communicated without alarming expected attackers.

Component Labeling Components can be implanted inside a picture, like the names of people in a photograph or areas on a guide. Duplicate the stego-picture additionally duplicates the implanted elements in general and just gatherings who

TABLE 1. Areas used for information security or hiding.

Criterion	Areas for Information Hiding		
	Watermarking	**Cryptography**	**Steganography**
Cover selection	Regularly video, audio or image	No need due only hides the content of the message, not required	Mainly digital Images, audio and video but mostly images, mean Any digital object
Origin	Contemporary era or modern	Antique procedure or Very ancient	Also the earliest method but very popular these days due its functionality Very ancient
Output	Concealment object	Encoded writing	Output
Authentication	Absolutely yes	Indeed	No or not at all
Objective	Contented validation and copyright protection	Encoded message	Covert message or communication channel
Imperceptibility	Must be high	Not required	Must be high
Robustness	Must be high	Not required	Must be high
Visibility	It can be visible or invisible depending upon the type of watermarking	Permanently visible due its procedure	Permanently visible due its procedure
High Payload	high	Not required	high
Attacks	Some common Image processing attacks: such is pepper and salt noise, cropping & rotation attack, sharpening attack, temporal modification, median filtering attack, quantization etc.	Some normal Cryptanalysis assaults: Such is known-plaintext assault, animal power assault, man in the centre assault, birthday assault, picked plaintext assault, figure text just assault, timing assault, word reference assault and so forth.	Common Steganalysis attacks: Such is Pixel difference histogram (PDH) attack, RS (regular and singular) analysis, sample pair analysis (SPA) etc.
Key	Elective or no need optional	Required	Elective
Merits	It offers both validations also, uprightness, alongside secrecy.	It bargains both authentication and integrity, along with confidentiality.	None separated from the source also, recipient can think the presence of the
Demerits	Usually payload is very low	Demerit because communication visible to the outsider or naked eye	Steganography itself alone cannot give validation and respectability
Purpose is lost	Assuming the watermark is invalidated or on the other hand strongly altered	If the communication is decrypted then the purpose is loss	Note that its purpose is lost if the intruder knows the communication channels

have the deciphering stego-key will actually want to concentrate and view the highlights.

Copyright Security Duplicate insurance systems that predict information, by and large advanced information, from being simulated.

So the widely image type is may be used for almost is png, jpeg etc. file types. However, image is very important for communication because one image is better than hundreds of words.

D. MEASURING ALGORITHM FOR IMAGE STEGANOGRAPHY METHODS

Any image steganography technique can be evaluated using the following measuring algorithm shown in Table 1 [20].

Imperceptibility: After concealing technique into a carrier object, detectable quality will be degraded into the implanted picture as compared with the cover media.

Payload: How much confidential information can be incorporated into the cover object?

Robustness: Information should remain in place after covering; this demonstrates how powerful the embedded picture is against any passive and active steganography methods that can be used.

Temper Protection: It should be challenging to alter the mystery message after it has been gotten into an inserted media.

Calculation: What sum over the top it is computational to embed and give up a covered message?

TABLE 2. Evaluating parameters or measuring algorithm.

Measures	Advantages	Disadvantages
Perceptual transparency (HVS)	Should be high	Should be low
High capacity (Pay load)	Should be high	Should be low
Calculation Complexity	Should be low	Should be high
Robustness	Should be high	Should be low
Temper protection	Should be high	Should be low

Table 2 elaborates on the assessing boundaries or estimating calculations for steganography, which are the essential standards of the steganography, and will be broken down into various existing strategies in view of these estimating calculations, which are displayed in Table 1.

E. SOME CHALLENGES OF IMAGE STEGANOGRAPHY

For steganography strategies, it is vital the assessments of the encoded picture to be utilized to implant the message into the cover picture without fluctuating its different characteristics [21]. After that, the output image is termed as stego or encrypted image. It is necessary that the encrypted image should be dissident from perceptible alteration and any obscure cannot have the choice to track down these movements and need to control that is implanted image as an ordinary picture, however the favoured data sent through this image stay secure. All cover steganography structure faces the significant difficulties based on the given three major criteria of steganography, which also displayed in Figure 4.

- **Size of payload:** Maximum hiding size of secret information into cover objects. Is the most extreme concealing limit conceivable relying upon the cover object for stowing away? Steganography points adequate implanting limit. High payload and robustness is regularly inconsistent because it is very complicated to achieve both of them simultaneously which is needed [22], [23].
- **Perception of the image:** it is necessary that an encrypted image should produce a high perception and that how an original and encrypted image is remain same [24].
- **Toughness for attackers:** it is strongly necessary to give a tough time against different type of attacks from assailants, which recognize steganography methods. The stego picture ought to give power against picture handling strategies like pressure, editing, resizing, etc; the point at to restricted data ought not to be much annihilated on the off chance that any of these Steganalysis strategies are performed on stego picture [25].

In this manner, the ideal steganographic strategy should satisfy the above all the targets as high limit, great visual picture quality, and imperceptibility. Nonetheless, most frequently, cover steganographic methods are defenceless against assailants due the contortion artefacts in the image and better steganographic methods have a great perception of the image due to embedding message up to some limits. Subsequently, how to accomplish all the basics needs of steganography as large embedding capacity, great perception of the image, and imperceptibility is a genuinely moving examination issue because of the inconsistencies of the both secret message bits and image pixels [26].

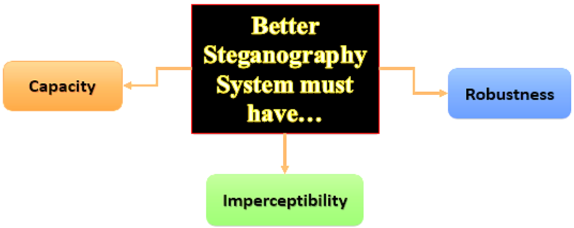

FIGURE 4. Exchange between Robustness, Imperceptibility, and Capacity.

III. IMAGE STEGANOGRAPHY APPROACHES

In below the most significant steganographic methods are critically investigated which is used image as cover medium by tending to the categorization of cover steganography. In light of the idea of inserting, there are different steganographic procedures accessible based on cover or image media containing frequency, spatial, distortion, and filtering and masking. In the Distortion or spread range, the privileged information is duplicated by a pseudo commotion succession and afterward regulated prior to installing in the encrypted medium. Spatial or picture space procedures use bitwise strategies that apply bit inclusion and clamour control utilizing basic systems, While the change region is portrayed as the difference in a particular image into its repeat confession trailed by alteration on the unseemly various pieces of that particular image. Moreover, the adaptive, sifting, or concealing nature could probably be presented or demonstrated in the information, in particular, inserting plans in many different ways, for instance, the number and quantity of pieces embedded in a pixel, the idea of acclimation to be made, picking the objective pixels of the cover picture [27]. The elaboration of steganographic approaches are given below one by one respectively:

A. APPROACHES OF SPATIAL DOMAIN

In spatial steganography, in particular, those having distinguishing implementations obtainable, all immediate change a couple of bits in the image pixel regard (value) disconnected from secured data. Spatial space plans are more flexible about human visual system and can give a better image quality with acceptable embedding limit than transform domain [28]. It is the most straightforward method of information inserting in advanced pictures in which pixel esteems could possibly be changed straightforwardly in order to encode the mystery message bits. This should be noted that the primary steganographic plans going underneath the spatial area strategy including Least Significant Bit substitution (LSB), Pixel Value Differencing (PVD), Quantization based, Gray Level modification, Multiple Bit-planes, Exploiting Modification Direction (EMD), and Palette based steganography patterns and approaches [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39].

Some standard approaches of spatial domain are given below:

- Method of content or texture
- EBE (Edges based embedding method)
- Method of Pixel intensity
- LSB (Least significant bit)
- Shifting methods of Histogram
- Hidden data pixel mapping method
- RPE (Random pixel embedding method)
- Connectivity method or labelling
- Pixel value differencing (PVD)
- Cyclic steganography randomization methods
- Gray level modification and MLE

Some pros and cons of spatial methods are:

Pros:

- Payload size is extreme
- Less degradation of the cover object.
- Can give a better quality images

Cons or Weaknesses:

- Embedded information can be loss if having less temper protection or high computation
- Hidden information can be actually dense by open attacks in the event that there is no power.

B. TRANSFORM DOMAIN

In this procedure, we first use modification to the picture from spatial space in the repeat region, cover the secret message and alteration over it into the spatial area. Furthermore, in order to cover information using these frameworks, unmistakable computations and variations are associated with pictures, which augmentation its diverse excellence [40], [41]. Note that this technique is believed to be meaningfully more grounded and standardized than the spatial space strategies in light of the fact that these techniques cover information in those regions of the picture that are less feeble by picture strain, managing, and editing [42]. These systems are less arranged to quantifiable assaults and picture debasement is likewise kept as we made alteration and modification to co-fit in the alteration space, nevertheless, we observed that they have almost cut down the consignment and payload and are, therefore, not enough good in contradiction of altering, turn, understanding, and confusion. Thus, a few transform area techniques are used in cover steganography, which are DWT, DCT, DFT, IWT, and CWT [43], [44], [45], [46], [47], [48]. Fundamentally, to handling the normal picture activities and lossy stress this sort of method is more vigorous. Figure 5 shows the concealing information utilizing the DWT-based techniques:

Some most widely used Transform domain approaches are as follows:

- DFT
- DWT
- Reversible method or lossless
- DCT
- Coefficient bits embedding

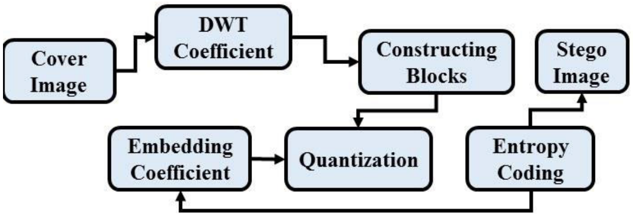

FIGURE 5. Block Diagram of DWT for data hiding.

C. DISTORTION OR ALTERATION TECHNIQUES

Techniques In this scheme, we have required data on the major cover picture in the midst of the keeping method where the decoder abilities are utilized to check and monitor for control amongst the central cover image. Moreover, its aim is also to check the embedded image with a particular slice to restore the secret message. This should be kept in mind that the encoder enhances a party of development to the shelter challenge. Consequently, the required data is being figured out as being gotten by the standard twisting [49]. Through exploiting this construction, a stego difference or question is made through relating and implementing a particular strategy for change of the cover image.

This development of fluctuations and modification is further utilized to revise the issue message that, in fact, is expected to communicate [50]. Note that the message is, in fact, programmed and encoded in pseudo-thoughtlessly picked pixels. This should be noted that on the off chance that the stego-image is spellbinding in relationship with that particular cover image or picture at the prearranged and specified message pixel, for instance: (a) the message bit is a ”1.” generally, and (b) the message bit is a ”0.” The encoder can change the ”1” respect pixels in such a course, to the point that the certified assets and characteristics of the picture are not negatively impacted or influenced. Although, the requirement for transferring and moving the cover picture controls the potential gains of this structure. In any steganographic structure, the cover picture should certainly not be used at least a time or two. In the event that an attacker changes the stego-picture by changing, scaling, or turning, the beneficiary

TABLE 3. Spatial Domain Techniques.

Spatial Domain			
Techniques used	**Advantages**	**Disadvantages**	**Review**
HS-Histogram Shifting [14], [23].	High limit and acquired security, also, great quality The low commotion also, a high limit	A little bit shifting but in rare case	Improvement in execution because of the extraordinary quality that doesn't impacted by the pieces which included.
Least Significant Bits [13-16]	Better hiding capacity Sufficient security and	Due to the limited imperceptibility Low quality	Increasing in security and decreasing in processing time.
PB-Palette Based [24]	less noise and better quality	Due to embedding without any loss give us better quality	PB
PIM-Pixel Intensity Modulation[26]	Each 3×3 window has one person rather than four is lead us to a High limit	Imperceptibility problem in rare case	For enhancing the quality its performance in PSNR and MSE is very good
QB-Quantization Based [25]	Average capacity	High BER considering the way that the typical BER is consumed by using the proposed technique.	When the palette size increased then image quality will increased
Pixel Value Differencing [17-22]	If grey scale and coloured images is used as cover object then image quality will be increased.	While utilizing low-thickness objects since it needs perception precision the Low PSNR and high MSE	The proposed strategy has a superior impalpability in view of the development of the new worth.

can absolutely and basically recollect it? Usually, assuming the message is encoded with ruin evaluating the information, the change can even be exchanged and the central message can be improved [51].

D. ADAPTIVE DOMAIN

This technique hides information by signifying a picture in basically the same manner as paper watermark. This structure encodes the information in the huger districts than covering it into the commotion level. The encrypted data is more crucial for cover the image. They are more joined into the image when watermarking strategies can be related without the feeling of dread toward picture harm considering pressure. It is likewise called ''Measurements Aware-encryption'' Filtering or concealing strategies. This strategy assesses the picture measurable worldwide qualities prior to endeavouring to interface with the image frequency coefficients [52]. The filtering and masking techniques have some merits and demerits as described below:

Merits:

- Fundamentally, the said method is considerably more remarkable when contrasted with the most un-critical piece relocating concerning strain since the data is covered into obvious cuts of the picture.

Demerits:

- Techniques can be related just unnecessarily faint or dim scale pictures and confined, making it difficult to 24 pieces.

Tables 3 and 4 shows the pros and cons of the procedures utilized in both spatial and transform area:

Table 5 shows the basics properties or criteria of the steganography in different domains. It also helps to the researchers that which properties in which domain can be obtain up to some limits. It is also give the clear direction for researchers to choose any domain for steganography.

Figure 6 shows the ratio between the presented domains for researchers to choose the domain for Cover

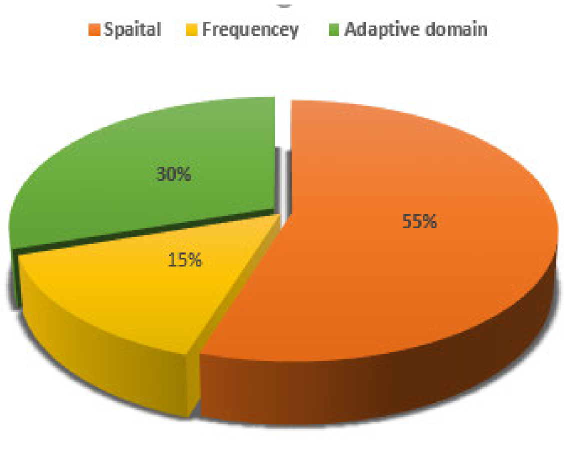

FIGURE 6. Illustration ratio to choose the domain.

TABLE 4. Methods used in frequency domain.

Transform Domain			
Techniques used	**Advantages**	**Disadvantages**	**Review**
DFT [30]	Better quality and high payload	Temper protection	PSNR values usually high.
DWT [24-27]	Robustness and image quality is better	Assuming the rising number of pieces in histograms it is exceptionally perplexing in calculations	made the power high and furthermore high PSNR and low MSE
DT-CWT [33]	Utilizations of low fix size brings about bigger number of individual patches in the cover picture the High limit	High BER in light of the fact that rising in number of patches will create more sub-pictures and quantization mistakes.	compared to the cover image High PSNR and good SSIM
IWT [31-33]	High limit and security. High power subsequent to applying assault and salt and peppers commotion	A decent exhibition in implanting and quality in view of the great presentation in PSNR.	
DCT [27-34]	Better performance in embedding process. High capacity and less distortion	Quality not considered by the author	Better security because of high PSNR and great covering limit.

TABLE 5. Comparisons of spatial, frequency, and adaptive domains.

Properties	**Domains**		
	Spatial	**Transform**	**Adaptive**
Numerical detectability (Histogram etc.)	Informal or easy	Tough or hard	Tough or hard
Computational Complication or complexity	Fewer or less	High	Algorithm Depended
Layout or format	Dependent	Independent	Independent
Capacity or Payload	Extraordinary or high up to some limits	Limited or even partial	Varies or differ from both domain depend on algorithm
Management of Pixel or Manipulation	Through or direct	Indirect	In line methods or used
Imperceptibility	Low	High	Highly controllable
System category	Simple	Complex	Algorithm dependent
Focus: Visual **Capacity** **Payload** **Detectability**	High High Moderate	High Moderate High	High Moderate High
Robustness	Highly prone	Less	Algorithm dependent
Geometric Attacks	Highly vulnerable	Resistant	Highly resistant
Virtual features integrity	Maintainable	Less	Maintainable
Non-structural Attacks	Detectable	detectable	Difficult

steganography because up-to-date for image steganography researchers widely used spatial domain.

IV. LITERATURE REVIEW

For data concealment the uses of some cover mediums such as audio, image, video etc steganography is a high-level examination region over the web. Until now, different methodologies for advanced steganography have been proposed which are depend on LSB replacement, edge based connected, and pixel pointer based embedded method. Each approach enjoys their connected benefits and hindrances. A few techniques have high payload cut-off points and incredible delicate quality and fogginess rely upon the picked cover for disguised or obscure data, hiding (Spatial space) however more powerless against attacks (Noise throwing, rotation, disturbance, resizing, etc) while others plans are solid against verifiable or factual attacks up to this point they have cut down payload limit. This infers there is dependably a trade-off between the three main criteria of steganography (Payload, Imperceptibility& Robustness).

Hence, the fundamental thought of steganography is to conceal the actual presence of the mysterious correspondence from the assailants. With propels advancement of this advance age of technology, cover steganography has some conceivable outcomes Today, cover steganography play a vital role in different advance areas such as Smart areas, IoT empowered industry applications, military applications, clinical imaging, and so forth. Naturally, steganography is a sort of two-sided deal. Because of the property of imperceptibility, steganography is additionally popular among solitary components for secret correspondence. Because of the property of honesty of digital images, analysts have favoured pictures as the transporter signal for concealing privileged information.

Additionally, the presence of repetitive pixels in a picture makes it significantly more appropriate for installing privileged data. Nonetheless, a large portion of the strategies introduced in the writing were exceptionally centred on the spatial or area. Spatial space procedures rely entirely upon the pixels of the picture for information encryption. To accomplish the main target and desirable output of cover steganography direct control of the pixels method used mostly. Basic and less tedious domain methods for cover steganography are spatial area. Subsequently, we summed up numerous techniques with their connected benefits and impediments in light of picture steganography, which is examined individually given below.

A novel Multi-Pixel Differencing (MPD) is a method for information embedding that was proposed by Jung, K. H., et al. It processes a total refinement evaluation of four square pixels and uses an additional two pixels to scale the perfection of each pixel. It employs a multi-pixel differencing architecture for information covering and is employed for low refinement and the LSB overall for high intricacy. Exploratory dataset is so heavily required, but its strength is in its simplicity of calculation [53].

Yang, et al. proposed a novel method for information hiding whereby it locates the area of the image that has the most darkness using LSB. Utilizing 8-pixel coordinate schemes, it converts the image to a two-crease picture and explains each difference. Therefore, the method anticipated a high count to find a drop in area, its transparency, and has not tried to produce a high surface kind of image. Stockpile of images that it is covering is completely endless [54].

Mahdi et al. Proposed one more novel an image steganography system, declaration of the close to home pixel of the expected picture locale and considering LSB replacement. The security where secret key is consolidated by LSB of pixels this method is focused to update. A Secret message should be disguised on the off chance that it makes the sporadic numbers and picks the locale by consolidating. The method's premise, however, is its security of hiding messages in stego-pictures; it has not yet been considered to be a perceptual straightforwardness [55].

Another novel cover picture steganography method was developed by Babita et al., which would scramble the 4 LSB of each RGB channel for its intended uses. Apply concentrates on constricting to preserve the possibility of the stego picture, and in the end, subsequently encodes the cover and stego picture refinement as key information. The stego-picture is added with essential information to bind the attempted information in the disconnecting step. Moreover, various requirements to control the stego-key makes the diverse thought of applying channels. The colossal issue of the proposed plot is covering the cut-off of high-restricted information [56].

For concealing pictures, that covers data in different channels of the cover picture in a cyclic manner a new Stego Cyclic concealing (SCC) system is proposed. Suppose the 1st secret bit is encrypted in pixel 1 of the red channel, 2nd secret bit is in pixel 2 in the green channel and 3rd bit is encrypted in pixel 3 in the blue channel and so forth. The basic vulnerability to the proposed system is that the process of the embedding message in a specific position. So aggressors can without a very remarkable stretch track down this methodology assuming secret information from two or three pixels is successfully isolated [57].

A novel cover steganography method, in which the two channels are used as a data channels and one channel is used as a marker which is consider a high embedded method called Pixel Indicator technique. It embedded the both coordinates of the data in a predefined way. The essential result shows a better security and sensitive in nature due to the organization of the embedding message and key exchange. The major weak reason for this technique is consider possible and also probably going to have pictures and marker bits that can achieve a low payload. It conceals the proper measure of pixels in the cover picture which is the chance of the noise and distortion of the image and the image become baseless in perception. The key point of the focusing for attackers in this proposed system is that the calculation in a manner of the embedding bits in cover image which lead to the extraction of the message very easily. Furthermore, the proposed produced a bad stego image, which is recognized by human visual system very easily [58].

A cover steganography that produced a better and enhanced the security of the steganographic method by adding the key concept in the embedding process. In the proposed method, green and blue channel is used as information channels and red channel and key is used as marker. The special information pieces are implanted either in green or in the blue channels considering covered key pieces and red channel LSBs. Tolerating either the piece of the red channel LSB or the mystery key piece is 1, then, the LSB of the green channel is uprooted with secret message bits, in any case, the LSB of the blue channel is supplanted by the mystery piece. The most critical of this strategy is the utilization of the mystery key. On the off chance that the aggressors get the mystery key, the special, information can undoubtedly accomplish [59].

A more effective and novel cover picture steganography method based on the Multilevel Encryption and Grey-Level Modification algorithms for hiding sensitive information. In this cutting-edge area, the security of data between two gatherings is a crucial concern. The suggested plot is a workable approach for RGB images that takes declining or faint aspect change (GLM) and staggered encryption into account in order to address these concerns (MLE). The secret key and data are encrypted with the MLE technique, planning to the Grey or dim level of the image. The uses of this manner embedding process with such algorithm can lead to create obscure for the attacker that cannot extract all privileged data. Therefore, the proposed method is give efficient and effective steganographic method. The principle benefits of the proposed work on the nature of stego pictures, high intangibility, cost-adequacy, and improved security. Besides, the usage of MLE and picture rendering adds different security levels to the said method. The attacks of the scaling, distortion, etc are the major weakness on proposed method. Therefore, if such attacks are applied on stego image then it will not extract the entire message easily [60].

Wang et al projected a prestigious steganographic method susceptible to PVD and modulus work, which performs better than anything in the PVD plot and is more secure against the RS recognising confirmation attack. This strategy concealed 51,219 bytes while extending the zenith growth of two PSNR characteristics of disturbance to 44.15 dB. In order to record the data from the implanted information, it abuses the other two constant pixels. This achieves more crucial adaptability, suitable for selecting the best remaining two pixels in the case of mutilation. The PSNR was widened (up to 8.9%) more by this method than by the direct PVD method. This method makes use of a further growing structure to alter the warning of the pixel join in order to maintain the spacing within the same range as the implanting system [61].

By giving certain extents of restricted information based on pixel-match diversity, Joo et al. demonstrated an improvement for method. The experiments with this technique showed that the capability histogram had a form that was more similar to the cover image and was challenging to identify by histogram evaluation. The implanting limit of this system isn't any larger than Wang et al.'s technique, despite the way it handled the shapes in the capability histogram; instead, the inserting request is different for the odd and notwithstanding, implanting zones [62].

Khan et al. suggested a positive and novel cover steganographic approach (M-LSB-SM) for securely and thoughtfully concealing images. The restricted intelligence is divided into four sub-squares and processed by MLEA, making the attack on this computation terrifying and, as a result, paralysing the system for Steganalysis, resulting in a conventional PSNR of 47.93 dB signed up for more than 150 images. They claim that their suggested strategy is capable of producing stego photos of a sufficient quality that meet the highest standards of the most recent security frameworks and customers. The computation is quick, easy to do, and has a nice balance of subtlety and security. As a result, steganographic apps are more likely to accept it. Generally, a couple of extra administrations are viable in broadening MLE calculation and payload restriction [63].

An image steganography method, which produced a novel high security and better perception of the image. In this method, the use of bit reversal concept the quality of the image is improved. The process of this algorithm, after LSB embedding, upset the most critical portion of the cover image. If it is compare with some adjusting lsb bits then the image quality reduced. In contrast with plain LSB strategy, a lesser number of LSBs of the cover picture are changed in this way when working on the PSNR of stego-picture. Putting the bits' design for which reversed LSB's are achieved will lead to acquire the best quality image. The strongest point of this method is the uses of the RC4 algorithm. To accomplish the isolated from everything message picture bits into cover picture pixels as opposed to putting away them successively is the motivation behind RC4 algorithm [64].

The authors produced better and novel cover steganography methods within the recent couple of years, which show a better direction of the cover steganography. Primarily, they show the fundamental causes of the cover steganography by achieving the basics criteria of steganography by increasing the size of the payload with image pixels [65].

In this paper, the authors give an extensive survey of steganography and cryptography ideas. Anyhow, they give a better survey and the exploration of different steganography techniques and their ideas, improvements. They also give the pros and cons of different steganography procedures. In the area of steganography, their work likewise gives the idea with respect to the future explores but still have some missing ideas and future direction that is need for cover steganography [66].

In the research work, the authors have given a better and novel method of image steganography by using the equipment in image. In this study, they show that hiding a secret message in image needs a deepest calculation and encrypting a message in such a manner fast and secure the cover steganography concepts [67]. In this paper, the authors give a safety by using three layers. They used a very clever method by using pseudo random arbiter generator for ordering the pixels' bits and after that hiding a message using LSB. However, this exploration work shows that embedding a secret message using LSB needs a deepest strategy and a clever calculation of the bits [68].

In this paper the authors proposed better Least Significant Bits replacement technique for concealing mystery picture data document into a shading picture. Many digital mediums are uses for hiding the secret message that to elaborates that this method is reasonably better. However, they used a discharge based image steganography involving LSB for hiding the secret message and getting the robustness and better image quality. For achieving, the high embedding message for different types of image and estimation of execution boundaries like PSNR and MSE [69].

The proposed framework fixed the shortcoming of the Essential LSB picture steganography strategy and present novel method. In this review, the makers used a set of six basic redesigns, explicitly: CRC-32 checksum, AES encryption, header data, and pseudo-eccentric pixel choice system thinking about the improvement of the pieces, and eight bpp presenting calculation [70]. The creators accomplished a few models of cover steganography, for example, security and calculation intricacy yet separated the others.

In this exploration work, the creators presented the close study and execution assessment of different picture steganography strategies using various kinds of cover media ((like BMP/JPEG/PNG, etc) with the discussion of their archive plans [71]. They used multiple types of image for encryption of secret message for cover steganography but still have vulnerable to different attacks such is cropping, scaling etc.

In this research, a new steganography method has been suggested with the goal of enhancing the installation limit and providing a solution to the problem with Shukla et al. OPVD's strategy's inspection stage. It is communicated through PVD and flexible least huge piece (LSB) replacement. Depending on the size of the image, it is divided into 33 or 33 squares of pixels in addition to 22 squares. One pixel in a square serves as the reference pixel when 4-bit LSB replacement is used. From that point, distinction esteems between the focal pixel and each neighbour pixel are determined. In light of these distinction esteems, versatile LSB replacement in the adjoining pixels is implemented. After the computation was completed, it was discovered that the hiding limit was incredibly large, for instance, 1055441 pieces at 4.025 bpp with a decent PSNR value of 32.63 dB. Additionally, it has been confirmed that the suggested approach withstands RS examination firmly and PDH inquiry pitifully. Cryptography can be used to increase the message's security. Although AES is unquestionably the most reliable cryptographic algorithm, using it would result in fewer communications being disguised since each letter must be split into 8 doubles rather than only 7. This also leads us to the conclusion that a cryptographic computation as safe as AES and able to address a person in seven parts would be extremely helpful [72].

In this paper, novel method near execution investigation of LSB, MSB, and PVD strategies utilized in picture Steganography was performed. The LSB procedure gives higher PSNR and SSIM esteems than the MSB and PVD strategies with lower MSE than the other two methods. Future examination can be equipped towards exploring the implanting limit, security, and computational intricacy of every strategy [73].

With the development of correspondence improvement, data sharing is becoming fundamental piece of current life. The researchers' primary concerns are security and breaking point, supposing an instance of image steganography to occur. For covert correspondence via the Web, a method with enough security and the capacity to conceal a significant percentage of data in the cover picture is anticipated. In order to receive the message from the gatecrasher, the suggested cover steganography approach, which comprises a pseudo-random number generator for unexpected pixels and a contact decision, is introduced. The suggested technique provides greater security and a high embedding limit differentiated with the delayed repercussions of the previous LSB processes, according to exploratory data. The technology provides extra generated security and a high embedding limit thanks to the two-layer PRNG in pixel and cycle level and a single byte in each pixel. The method may very well be considered an effective steganographic technique as it achieves the goals of the steganographic framework [74].

In order to introduce the limited data into the shaded cover picture safely, this work introduces three bits of the flexible LSB+3 type I and type II approaches. The suggested approaches use encoded data and a moving cycle to inject data into the cover picture with two layers of protection. The development of the LSBXYZ approach leads to the creation of adaptive LSB+3 type II processes and flexible LSB+3 type I procedures. The suggested technique creates a similarity between the cover image and the stego image. The adaptable LSB+3 type II method generates a 5.73% PSNR. Moreover, we have expanded installing effectiveness, give protection from Steganalysis assaults, and get high stego picture quality [75].

Table 6 shows the critical evaluation up to various thirty techniques with their advantages and disadvantages and furthermore dissected in light of estimating algorithms (Payload, Imperceptibility, Robustness, Temp assurance, calculation) which is the fundamental standards of any steganography method, which is additionally displayed in Table 2.

The methods introduced in Table 6 are basically examined in light of assessment models of steganography like limit, strength, temper security, and calculation, which nearly cover the assessment standards dependent upon certain cut off points. In this way, to assess sensibly the presentation of different steganography strategies, it is required to

TABLE 6. Ciritical analysis of image steganographiy methods with their pros and cons.

Ref.	Techniques	Pros	Cons	Analysis based on				
				Capacity	Robustness	Perception	Temp protection	computatio
Singh et al. [76]	Changed LSB replacement for colour images	Imperceptibility, High Security, and quality image upto some extent	payload cut off and weakness of measurable assaults	x	✓	x	x	✓
Abbood et al. [77]	further developed LSB for RGB images	Great security, incredible quality and robustness	Payload, Weaknesses	x	✓	✓	x	✓
Kalita et al. [78]	LSBSubstitution through XOR Substitution	Great Security and Great picture quality	Concealed information excessively Low	x	✓	x	x	✓
Ghanbari et al. [79]	Multi Stego for dark scale images	High Limit and short distortion	susceptibility to various assaults	✓	✓	x	x	x
Abdali et al. [80]	Esteem differencing utilizing contiguous pixel and LSB replacement technique	great security, subtlety, and robustness	Concealed information excessively low and weakness of measurable assaults	x	✓	✓	x	✓
Khan.M et al. [81]	GLM and MLE	great intangibility, times Valid and robustness	faintness to various attacks such is editing, scaling and disorder	x	✓	x	✓	✓
K.Muh. et al. [83]	Pattern bits combinations along with (Stego-Key) using LSB	Hidden Data	Hidden Capacity is Low	x	x	x	x	x
K., Ahmad et al. [84]	Dim area of picture with LSB substitution	Obliging for plane region with solid restriction of article grounded dataset	Great computation compulsory and not took a stab at high surface zones	x	✓	x	x	x
Shyla, N et al. [85]	LSB substitution with Median Filtering	High hidden capacity	Computationally confusing in Stego-key essential	✓	x	x	x	x
Rinki et al. [86]	Colour Cycle steganography	Concealing information diverse straits	Surrounding is a proper cyclical and methodical way, effectively can extricated in the event that a couple of spot separated	✓	x	✓	x	x
Gutub et al. [87]	PIT	Great hidden data better imperceptibility	consignment limit is totally dependent on cover picture and pointer bits	✓	✓	✓	x	x
K. Sajjad et al. [88]	GL-M & MLE	high indistinctness, times Saving and robustness	vulnerability to various assaults (editing, scaling and clamour)	x	✓	✓	✓	✓
Maniriho et al. [89]	concealing text in picture utilizing five modulus method	Achievement of strength and great nature of stego images	If expanding the window size, then will be decline payload	✓	x	✓	x	x

TABLE 6. *(Continued.)* **Ciritical analysis of image steganographiy methods with their pros and cons.**

Shyla, N et al. [90]	pixel-esteem differencing and modulus work	High Capacity, and good Image quality	vulnerability to different attacks	✓	x	✓	x	x
Kumar et al. [91]	safeguarding pixel-regard differencing histogram with modulus work	Enhanced Security and perception transparency	Hidden data too low	x	✓	✓	x	✓
Shahanag et al. [92]	histogram preserving using pixel pair matching	Higher limit and Better Quality	vulnerability to different attacks	✓	x	✓	x	✓
Patil et al. [93]	modulus function and pixel-value differencing	Embedding capacity and the security	Insight and weakness to various attacks(Noise, editing)	✓	✓	x	x	✓
MK Sajajd et al. [94]	MLE and achromatic component of an image	Security and good imperceptibility	visual quality, payload cut off and weakness of factual assaults	x	✓	✓	x	✓
Zakaria et al. [95]	Data Mapping and LSB Substitution	Embedding capacity and visual quality	Temper protection and computation	✓	✓	✓	x	x
Ulker et al. [96]	logistic map and secret key	High security, payload, Visual quality	Vulnerabilities(noise, copping) computation	✓	x	✓	✓	x
Hussain et al. [97]	Pixel Values Differencing with Adaptive LSB	Histogram of both unique and stego picture is dependably same	for experimental results too small data sets	✓	✓	x	x	x
Tappe et al. [98]	MPD with LSB	Same as PVD yet in some way or another is important from normal PVD techniques	Limited data sets, and Threshold, both sides Stego key require	✓	✓	x	x	x
Neamah et al. [99]	LSB replacement with Irregular pixel selection	Great safety for message in Stego-image	deprived of thoughtful Visual Quality in Arbitrary pixel assurance	x	✓	x	✓	x
Shanthakumari et al. [100]	An extraordinary strategy for picture steganography In spatial area utilizing last two pieces of pixel esteem	Partial changes in cover-image.	Vulnerabilities to different attacks	✓	x	✓	✓	x
Kumar et al. [101]	An Edge versatile course of action for Region choice and LSBMR for information	Enhanced Visual Quality and security of secret message	Hidden data too low	x	✓	x	✓	x
Anbu et al. [102]	Developing histogram-based adaptable information stowing away by embedding expectations	Image quality and acceptable capacity	Security risks	✓	x	✓	x	✓
Lu, et al. [103]	Invertible ANN	High payload and security	Low quality	✓	✓	x	✓	x
Shah et al. [104	Genetic algorithm having a flexible chromosome structure	Better quality, robust	Computation, payload	x	✓	✓	✓	x

TABLE 6. *(Continued.)* Ciritical analysis of image steganographiy methods with their pros and cons.

Hamza et al. [105]	Pattern matching	Better quality and payload	Temper protection and transparency	✓	✓	✓	x	x
Yassin et al. [106]	IWT and MSB	Robust and payload	Perception and T- protection	✓	✓	x	x	✓
Yassin et al. [107]	RSA and compression	Robust and payload	Quality low and computation and Transparency	✓	✓	x	x	x
Sonar et al. [108]	Hybrid RR, AQVD, QVC	Robust, quality and resistance against attacks	Low payload and computation	x	✓	✓	✓	x
Wani et al. [109]	Deep Learning	Robust, T-protection transparent	Low payload and computation	x	✓	✓	✓	x
Gaffar et al. [110]	Golden ratio and non-subsampled contourlet transform	Enhanced Visual Quality and security of secret message	Hidden data too low	x	✓	x	✓	x
Dhawan et	S2OA & DESAE model	Partial changes	Vulnerabilities to	✓	x	✓	✓	x
al. [111]		in cover-image.	different attacks					
Setiadi et al. [112]	Dilated H-edge detection Improved capacity LSB	Great safety for message in Stego-image	poor of thoughtful Visual Quality in Random pixel declaration	x	✓	✓	x	x

expound the adequate rules for further developing the procedures on the grounds that the assessment measures may likewise lead us to the right deportment. However, the fundamental measures Payload implies making the most extreme concealing limit conceivable relying upon the cover object for stowing away. Robustness explains how a stego picture opposes various steganography assaults and it ought to likewise give heartiness against picture handling strategies like treating, editing, scaling, and so on the grounds that steganography might experience the ill effects of various latent and dynamic assaults. Perceptiveness infers how the stego-picture is unclear from the cover media noticeably because stenographic strategies produce a high perceptual picture.

Temper security is a moving issue to change the limited data after it has been gotten into the encrypting media. Whereas Calculation truly intends that, the amount it is computationally expensive to encode and disentangle secret messages. The benefits and burdens of assessment rules of steganography are displayed in Table 2. However, in sum-up the above discussions, the main purpose of this research work is to identify the best and valuable domain for research work in image steganography for secure communication. Therefore, this research work presents a comprehensive study of image steganography in spatial, frequency, and adaptive domains based image steganography. In this study, we investigated to critically analyzed various cover steganography techniques and to identify the valuable region that everyone can be benefited more. So the importance of this research work is that the researchers to choose the domain for Cover steganography because for image steganography researchers widely used spatial domain and up-to-date direction is to machine learning (unsupervised learning) and deep learning architectures.

The above critically analysis presented in literature have many limitations about basic criteria because every method have their related pros and cons but not fulfill the reliability between the criteria. The main problem is the reliability between criteria because some methods gets one or two criteria but broke down the others, so this the main limitations. So in the best of my knowledge two main points is arises; it is necessary to make a hybrid algorithm for cover steganography while the other is some machine learning or deep learning concepts for making suitable cover steganographic algorithms for secure communication.

V. PERFORMANCE EVALUATION

A. HIDING LIMIT OF SECRET MESSAGE

In detail, the inserting limit (or payload limit) relies upon a steganography plot and the idea of the chose cover picture. It is the essential needs for cover steganography to keep the balance about the size of inserting message and the cover object bits without changing the fidelity of the cover object because visual quality is basics requirement. The limit is the quantity of pieces implanted in every pixel and is tended to by bits per pixel (bpp) or in relative rate as illustrated in the following formula:

$$\text{Payload(bpp)} = \frac{\text{No. of embedded bits}}{\text{Total pixels in a cover image}}$$

TABLE 7. Image quality assessment metrics.

S.no	Quality Assessment Metrics	Purposes
1.	$\mathbf{PSNR} = \mathbf{10log_{10}}\left(\frac{\mathbf{C_{max}}{}^{2}}{\mathbf{MSE}}\right) \quad Eq.1$ PSNR is the essential boundary that is utilized for computation of the cover picture as well as how much the cover and stego-picture are the same [113]. The equation for PSNR is given where C is the cover picture, as shown in Eq. 1.	Unit for PSNR is decibel dB. In the event that the worth of PSNR is under 30dB shows a low idea of the quality item and it gets a recognizable change which should be visible to the unaided eye. Greater than 40dB PSNR shows the great nature of the objects.
2.	$\mathbf{MSE} = \frac{\mathbf{1}}{\mathbf{MN}} \sum_{\mathbf{x=1}}^{\mathbf{M}} \sum_{\mathbf{y=1}}^{\mathbf{N}} (\mathbf{S_{x,y}} - \mathbf{C_{x,y}}) \quad Eq.2$ Mean Square Error will be equal if C(x, y) == S(x,y) cover and stego objects. If MSE value is 0 then both objects are considering same. Where C is the cover image and S is the stego-image. While N and M is the dimension of the object and x, y are the counter of the loop, as shown in Eq. 2 [114].	It shows the difference between the cover-image and stego-image. It is also compute the mean square error between the stego-image and cover-image.
3.	$\mathbf{RMSE} = \left(\frac{1}{N}\right) \sqrt{\sum_{\mathbf{x=1}}^{\mathbf{N}} (\mathbf{C_x} - \mathbf{S_x})^{\mathbf{2}}} \quad Eq.3$ Root Mean Square Error (RMSE) measures the distinction between the cover and stego pictures after extraction. Where C and S are the cover and stego pictures and N is picture estimation as shown in Eq. 3 [115].	The RMSE is the method that measures the quantity of the difference between cover and stego images
4.	$\mathrm{MAE} = \left(\frac{1}{\mathrm{Mx\ N}}\right) \sum^{\mathrm{M-1}} \sum^{\mathrm{N-1}} \lvert \mathrm{C(x,y)} - \mathrm{S(x,y)} \rvert \quad Eq.4$ Mean Outright Mistake is the rule to gauge the presentation opposing the assaults. Where M and N is the cover and stego objects, while C(x,y) and S(x,y) is the dim level of the pixel as shown in Eq. 4 [114], [116].	It measures the difference between encrypted and Cover images. Where M and N is the cover and stego objects, while C(x,y) and S(x,y) is the gray level of the pixel.
5.	$\mathrm{SSIM(X,Y)} = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x{}^2 + \mu_y{}^2 + C_1)(\sigma_x{}^2 + \sigma_y{}^2 + C_2)} \quad Eq.5$ SSIM used three main parts brightness, structure and contrast to calculate both stego and cover image. Where σx2 and σy2 are the variances for x,y respectively, as well σxy is the co-variance for x and y while µx and µy are mean for x,y, respectively; as illustrated in Eq. 5 [114], [116].	SSIM is utilized to compute the difference, design, and splendour between both cover and stego objects. Where σx2 and σy2 are the differences for x, and y individually, also σxy is the co-fluctuation for x and y while µx and µy are the mean for x, and y separately.
6.	$\mathbf{NCC} = \frac{\sum_{\mathbf{x=1}}^{\mathbf{M}} \sum_{\mathbf{y=1}}^{\mathbf{N}} (\mathbf{S(x,y)} * \mathbf{C(x,y)})}{\sum_{\mathbf{x=1}}^{\mathbf{M}} \sum_{\mathbf{y=1}}^{\mathbf{N}} \mathbf{S(x,y)^2}} \quad Eq.6$ Normalized Cross Correlation is used to calculate the quality between the cover and stego objects. Where S and C are the stego and cover objects, while M and N is the object dimension as shown in Eq. 6 [115], 117].	It gives value in the scope of 0 and 1. If the NCC value is 1 then it means that both cover and stego objects are same, while if the values become 0 it means both objects are absolutely different.

B. SOME QUALITY ASSESSMENT METRICS ANALYSIS FOR STEGO IMAGE

In order to effectively evaluate the quality of stego-images, various evaluation metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), Root Mean Square Error (RMSE), Mean Absolute Error (MAE), Normalized Cross Correlation (NCC), and Structural Similarity Index (SSIM) are used [97], [98]. Many image qualities of assessment metrics are used for encrypted image and any one can be utilize for measurement of the image. Regularly used image quality assessment metrics for stego and cover image are given in Table 2 below:

VI. ANALYSIS OF SECURITY

Due to several factors to obtain, a better security for steganography is not a simple and insignificant task. Here the most usual Steganalysis strategies are shortly examined.

A. HISTOGRAMS ANALYSIS OF PIXEL DIFFERENCE

Histogram is an amount of the measure of happenings of pixels regarding specific pixel bits. The primary changes between the cover and stego picture during the inserting system of the mystery messages can be distinguished utilizing histogram examination to identify steganography techniques. Furthermore, if a little change or contract detected between cover and stego image then it is easier for attacker to find that this is steganography method. However, if the cover and stego image histogram is remaining same then it is harder to attacker to identify it. Utilizing the PVD-based steganographic techniques, it might be an expected trademark to uncover the secret message of those stego images due to pixel contrast histogram. Because of its proper quantization steps and decent partition of installing unit. Hussain et al. [118] demonstrated that PVD plot [119] inevitably presents a rare unnecessary step in the histogram of the distinctions between two constant pixels in each encrypted edge. However, it strongly needed to ration the limit of embedding message into cover image while hiding a large payload to identify and investigate the said stuffs. Therefore, it is strongly necessary to embed the secret message up to some limit to save the reliability between the criteria of cover steganography [120].

B. VULNERABILITIES TO COVER STEGANOGRAPHY OR EXTENSIVE STEGANALYSIS

For the detection of Steganography methods, Steganalysis is a met recognition technique as in it very well may be changed in the wake of preparing on embedded and original images to recognize any steganographic strategy no matter what the inserting area. The exploit is tracking down a fitting arrangement of delicate measurable amounts (a component vector) with ”recognizing” capacities. NN (Neural Network), Clustering calculations, and different instruments of soft computing can be utilized to observe the right edges and build the recognition model from the gathered information [121]. All-inclusive Steganalysis is otherwise called blind Steganalysis, which is an innovative way to deal with assault the stego pictures with practically no earlier information about the kind of the utilized steganographic calculation. These visually impaired finders are assembled utilizing AI, for example, to find a little bit change between the cover and stego image or objects a type of classifier or mechanism is prepared. Many tools are used by attackers to identify the basics highpoint of cover steganography [122], [123] and the spatial rich model SRM [124], a list of capabilities named discrete cosine change leftover (DCTR) was proposed [125] for steganalysis of JPEG pictures where the discovery accuracy is assessed utilizing the negligible complete mistake likelihood under equivalent priors and is given by the following formula:

$$P_E = \min_{P_{FA}} \frac{1}{2}\left(P_{FA} + P_{MD}\right),$$

where PFA and PMD are the false anxiety and missed detection probabilities, respectively.

C. CONSISTENT AND REMARKABLE STEGANALYSIS

It is very complex to reveal and compute the fragile connections between several pseudorandom modules present in the picture (i.e. LSB plane or the picture). Suppose for eight-digit dim scale image with pixel values from the setting point P = 0-255. The spatial connection is fixed utilizing a discrimination function f that allots real number f (x1, x2, x3. . . xn) ∈ Rn to a social event of pixels G = (x1, x2, x3. . ., xn). The limit f is mathematically depicted as shown in the following formula:

$$f\left(x_1, \ldots, x_n\right) = \sum_{i=1}^{n-1}\left(\left|x_{i+1} - x_i\right|\right),$$

For the discrimination function f set G is larger value, which is considered as a nosier group that measures the smoothness of G. Typically in LSB process, the distortion and noisiness is increased if the embedding message is increased as compared to cover image bits. In familiar images, flicking the gathering G will even more often lead to an expansion in the separation function f slightly than a letdown. In this way, the complete number of usual gatherings is bigger than the absolute number of solitary gatherings its allow us to mean the complete amount of ordinary gatherings for a positive covering m as Rm (in precents of all get-togethers), and leave Sm alone the general number of particular gatherings. The worth of Rm is roughly equivalent to that of R−m, and the equivalent should be valid for Sm and S−m on account of guess of the steganalysis strategy for hiding place picture taking an alternate pace of embedding message to accomplish the given below:

$$R_m \cong R_{-m} \text{ and } S_m \cong S_{-m}.$$

Shortly, the principle thought of the RS-Steganalysis takes advantage of the connection of descriptions in the spatial space and is relevant to maximum business steganographic programming items. Additionally, it can be reached out to variations of LSB inserting in records of range pictures and quantized DCT coefficients in JPEG documents is the standards of RS-Steganalysis.

D. DATA SETS USED FOR IMAGE STEGANOGRAPHY

A steganographic dataset is a variety of media objects comprising of cover objects and comparing steganographic objects, with varieties in boundaries connected with the items and steganographic strategies utilized, applied reliably across all items''. In our definition, items might incorporate computerized record types like text, picture, sound, and video. Theoretically, there are no appropriate datasets for picture steganography but some are SIPI and IPP etc. are used [126]. In this manner datasets utilized in existing writing have been developed regularly by the writers utilizing public space pictures.

Image steganography and steganalysis methods examined in the writing depend on utilizing a dataset(s) made in view of cover pictures got from the public space, through the procurement of pictures from Web sources, or physically. This issue frequently prompts difficulties in approving, benchmarking, and recreating detailed methods in a predictable way. It is our view that the steganography/steganalysis research local area would profit from the accessibility of normal datasets, hence advancing straightforwardness and scholarly honesty.

Nonetheless, we contend that utilizing public space pictures presents the gamble of the trustworthiness of such pictures being compromised, as the shortfall of steganographic content isn't known deduced.

During our examination, we found that there were various methodologies used to develop the datasets utilized in writing corresponding to steganography and steganalysis.

Normal datasets are broadly utilized in various spaces, for example, artificial intelligence, image processing, digital protection, and man-made reasoning, etc. Normal datasets that are openly accessible permit specialists to approve, benchmark, and duplicate procedures recently announced or proposed, in this manner advancing straightforwardness and respectability of scholarly exploration. A few well-known models incorporate FVC2002 (Maio, Maltoni, Cappelli, Wayman, and Jain, 2002) utilized in biometrics, PhysioBank Data sets (Goldberger, et al., 2000) comprising physiological datasets, and UCI KDD datasets (Hettich and Narrows, 1999) utilized in information mining etc [127].

One of the restrictions we experienced was during the picture procurement process. Due to the on-location photography strategy, a few pictures caught must be rejected from the dataset. Subsequently, just a little part of the dataset (16%) addresses indoor pictures. We feel that there must be harmony among indoor and outside pictures, in any event, to have a genuine portrayal of certifiable applications.

Over the span of the investigation, different occasions were logged (date, time, implanting rate, and the way to ancient rarity) and all singular antiquities made were hashed (MD5) for approval purposes. This permitted us to check that the Cover pictures and Steganographic pictures were not similar after the implanting system. Furthermore, this also affirm that the specific payload could be recovered when the instruments utilized had this capacity. Toward the finish of the trial, the last dataset we organized comprised of 14,000 pictures altogether, which incorporates the first cover pictures, pre-processed cover pictures, and the last Steganographic pictures.

VII. FUTURE DIRECTIONS AND CHALLENGES

To accomplish a fair negotiation between the payload, robustness, and perception and so forth is a challengeable test and investigation for any steganographers to devise cover steganography methods. There are some acceptable steganographic methods deployed, but these procedures are viewed as presented to at least one types of Steganalysis. There is no such steganography strategy accessible that can accomplish the previously mentioned properties because steganography need the reliability between these properties. Since these properties are totally unrelated with one another, in this way, it is still a clear challenge for steganographers, if focusing for one essential parameters will be lead us to uncover or broke down the others, which needs dependability between the essential assessment models of cover steganography. It is a basic need for cover steganography to develop a better method to perceive the conflict between the steganography and steganalysis. In steganography, the message is embedded into the advanced media instead of encoding it. The advanced media contents, called the cover, are not set in stone by anyone, the message concealed in the cover can be recognized by the one having the genuine key. The message in the message after the collector gets the information. That permits steganography to secure the implanted data after it is unscrambled. Steganography is consequently more extensive than cryptography. Signal handling region incorporates separating, de-noising strategy, obstruction concealment, radar signal handling, electromagnetic wave engendering, and remote correspondence frameworks.

Subsequent to checking on the writing in Image Steganography, the writer has made the enclosed proposals that could be the promising headings before long, which are given below:

1) The availability of extraordinary computational setup is an important issue in today advance era. Consequently, using the powerful and better models of steganography methods with proper higher payload and robust image steganography techniques can be achieved.
2) To achieve high security objectives, Watermarking, Cryptography and Steganography play a vital role in this advance internet world. Because in watermarking can be find the embedded regions, cryptography hide the content of secret message and steganography having no knowledge of the embedded message or existing

data and make its undetectable to everyone. Hence, to achieve high capacity, better imperceptibility, and better security the researcher strongly activists to make better or combining the methods available in spatial domain.

3) On behalf of embedding more bits that are secret and avoiding the smoother regions of the image; adaptive base image steganography methods more focus on the texture regions of the image. Without bringing on any defacement in the non-edge or smooth regions of the images, it will be motivating to perceive and need to increase the payload limits by developing a better cover steganography method.
4) For better Image Steganography technique additional capable direction is the uses of 3D images as cover object. Since the vast majority of the works, using 2D images has been done up to date in this area. Subsequently, the utilization of three aspect means 3D images can fundamentally expand the concealing proportion more than two aspect images because of its extra dimension. Extremely inadequate strategies were made by the specialists to insert the mysterious pieces in of three aspect images (3D). Consequently, the researchers have to advise that the use of three dimension images for data encryption to increase the reliability between the basics criteria of steganography in the future.
5) Working on MLEA and Magic Matrix extension to make the method more reliable. To develop some improved mechanisms, future work should be investigating an image steganography and some cryptography concepts to make a hybrid robust method. Future work must explore Cover Steganography with some Machine learning and Deep Learning concepts to make a framework or architecture for selecting appropriate cover objects for suitable conceal message. And to make an educated system able for hiding data within the cover media to direct which cover object is suitable for which type of secret information. The authors also currently engaged for finding more ways such are unsupervised learning (ML), related concepts of Deep Learning to tackle some limitations, statistical and image processing attacks to generates high quality and reliable free stego images.
6) A few creating patterns of steganography are outlined as follows.
    - Decreasing encrypting alteration and expanding implanting effectiveness.
    - Adaptively choosing the encrypting areas.
    - Encoding information in the picture creation process.
    - Working mutually with computerized criminology.
    - Forfeiting the slightly while protecting the measurements.
    - Distinguishing the kind of steganography, the preowned boundaries.

VIII. CONCLUSION

In this study, we explained different previous research works, categorization of the steganography and also checked on the ideas, applications, difficulties, and techniques for cover steganography. Mainly, the fundamental ideas and creating history of cover steganography were shortly re-examined. Then, at that point, we endeavoured to stretch a summary of the utmost significant steganographic approaches by tending to the grouping of cover or image steganography that use advanced images as a cover media. At last, we gave short depictions of a few measurements utilized in quality assessment of steganography strategies. This paper gives a broad assessment of different cover steganography methods in each domain. Moreover, the scientific categorization of cover steganography strategies and the quality assessment measurements are contended. The primary changes between the cover and stego picture during the inserting system of the covert messages can be distinguished utilizing Histogram examination to identify steganography techniques. Hence, in this review, particular steganographic researches were expected and were requested into different techniques. Similar quantities of new application zones are perceived like web dealing with a record, compact correspondence security, cloud security, etc.

The comprehension of the steganographic guidelines drives positively controls us to see new zones and to work on its applications in the truly existing application areas also. Further, the current issues and promising future gradations are additionally featured. From a definitive contest between steganography and steganalysis, a side-effect, specifically a characteristic picture model, might be gotten, which is helpful to the two sides. For the model, the steganographic side can use the model to protect picture insights, while the steganalysis side can utilize the model to analyzed assuming any measurement goes inappropriate. It might likewise be valuable in other related fields, for example, computerized criminology. In abstract, Alice wishes to securely send information to Lace whatever number as could be expected under the circumstances, while Wendy attempts to neither insult a guiltless cover medium nor let a solitary stego medium inform past. It appears to be that the opposition between steganography and steganalysis will go on and on forever without any problem. At last, in this period of digitization, steganography is thriving at a quicker pace. Accordingly, the authors have faith that the proposed paper can uphold numerous specialists. It is also being not just understanding the foundation subtleties of cover steganography but additionally taking their thoughts forward more.

ACKNOWLEDGMENT

The authors would like to thank each of the adherents for their fundamental and specific overview of this investigation work and their critical help and way. They would also like to thank the supportive remarks and ideas of the observers.

REFERENCES

[1] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 474–481, May 1998.

[2] I. Diop, S. M. Farss, K. Tall, P. A. Fall, M. L. Diouf, and A. K. Diop, "Adaptive steganography scheme based on LDPC codes," in *Proc. 16th Int. Conf. Adv. Commun. Technol.*, Feb. 2014, pp. 162–166.

[3] G. Kipper, *Investigator's Guide to Steganography*. Boca Raton, FL, USA: CRC Press, 2003.

[4] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, Mar. 2019.

[5] A. Yahya, *Steganography Techniques for Digital Images*. Cham, Switzerland: Springer, 2019.

[6] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[7] M. A. Hameed, M. Hassaballah, S. Aly, and A. I. Awad, "An adaptive image steganography method based on histogram of oriented gradient and PVD-LSB techniques," *IEEE Access*, vol. 7, pp. 185189–185204, 2019.

[8] D. Artz, "Digital steganography: Hiding data within data," *IEEE Internet Comput.*, vol. 5, no. 3, pp. 75–80, May 2001.

[9] E. Zielińska, W. Mazurczyk, and K. Szczypiorski, "Trends in steganography," *Commun. ACM*, vol. 57, no. 3, pp. 86–95, 2014.

[10] R. Din, O. Ghazali, and A. J. Qasim, "Analytical review on graphical formats used in image steganographic compression," *Indonesian J. Elect. Eng. Comput. Sci.*, vol. 5, no. 3, pp. 401–408, 2017.

[11] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26–34, Feb. 1998.

[12] A. D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Process. Lett.*, vol. 12, no. 6, pp. 441–444, Jun. 2005.

[13] J. Kour and D. Verma, "Steganography techniques—A review paper," *Int. J. Emerg. Res. Manage. Technol.*, vol. 3, no. 5, pp. 132–135, 2014.

[14] A. Sharp, Q. Qi, Y. Yang, D. Peng, and H. Sharif, "A video steganography attack using multi-dimensional discrete spring transform," in *Proc. IEEE Int. Conf. Signal Image Process. Appl.*, Oct. 2013, pp. 182–186.

[15] S. D. Hu and U. K. Tak, "A novel video steganography based on non-uniform rectangular partition," in *Proc. 14th IEEE Int. Conf. Comput. Sci. Eng.*, Aug. 2011, pp. 57–61.

[16] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26–34, Feb. 1998.

[17] B. Khosravi, B. Khosravi, B. Khosravi, and K. Nazarkardeh, "A new method for pdf steganography in justified texts," *J. Inf. Secur. Appl.*, vol. 45, pp. 61–70, Apr. 2019.

[18] S. Jeevitha and N. A. Prabha, "A comprehensive review on steganographic techniques and implementation," *ARPN J. Eng. Appl. Sci.*, vol. 13, no. 17, pp. 4780–4791, 2018.

[19] E. T. Lin and E. J. Delp, "A review of data hiding in digital images," in *Proc. PICS*, vol. 299, Apr. 1999, pp. 274–278.

[20] P. V. K. Borges, J. Mayer, and E. Izquierdo, "Robust and transparent color modulation for text data hiding," *IEEE Trans. Multimedia*, vol. 10, no. 8, pp. 1479–1489, Dec. 2008.

[21] M. A. Hameed, "A high payload steganography method based on pixel value differencing," Dec. 2019. [Online]. Available: https://ssrn.com/abstract=3500443

[22] G. Swain, "High capacity image steganography using modified LSB substitution and PVD against pixel difference histogram analysis," *Secur. Commun. Netw.*, vol. 2018, pp. 1–14, Sep. 2018.

[23] I. J. Kadhim, P. Premaratne, and P. J. Vial, "High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform," *Cognit. Syst. Res.*, vol. 60, pp. 20–32, May 2020.

[24] V. Korzhik, N. D. Cuong, and G. Morales-Luna, "Cipher modification against steganalysis based on NIST tests," in *Proc. 24th Conf. Open Innov. Assoc. (FRUCT)*, Apr. 2019, pp. 179–186.

[25] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho, and K.-H. Jung, "Image steganography in spatial domain: A survey," *Signal Process. Image Commun.*, vol. 65, pp. 46–66, Jul. 2018.

[26] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Hallorana, "Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, Mar. 2019.

[27] J.-C. Joo, H.-Y. Lee, and H.-K. Lee, "Improved steganographic method preserving pixel-value differencing histogram with modulus function," *EURASIP J. Adv. Signal Process.*, vol. 2010, no. 1, Dec. 2010, Art. no. 249826.

[28] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognit. Lett.*, vol. 24, nos. 9–10, pp. 1613–1626, Jun. 2003.

[29] H.-C. Wu, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," *IEE Proc. Vis., Image, Signal Process.*, vol. 152, no. 5, p. 611, 2005.

[30] C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 488–497, Sep. 2008.

[31] C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, "Varied PVD+LSB evading detection programs to spatial domain in data embedding systems," *J. Syst. Softw.*, vol. 83, no. 10, pp. 1635–1643, Oct. 2010.

[32] X. Liao, Q.-Y. Wen, and J. Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution," *J. Vis. Commun. Image Represent.*, vol. 22, no. 1, pp. 1–8, Jan. 2011.

[33] Y.-P. Lee, J.-C. Lee, W.-K. Chen, K.-C. Chang, I.-J. Su, and C.-P. Chang, "High-payload image hiding with quality recovery using tri-way pixel-value differencing," *Inf. Sci.*, vol. 191, pp. 214–225, May 2012.

[34] M. Khodaei and K. Faez, "New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing," *IET Image Process.*, vol. 6, no. 6, pp. 677–686, Aug. 2012.

[35] C. Balasubramanian, S. Selvakumar, and S. Geetha, "High payload image steganography with reduced distortion using octonary pixel pairing scheme," *Multimedia Tools Appl.*, vol. 73, no. 3, pp. 2223–2245, Dec. 2014.

[36] J. Chen, "A PVD-based data hiding method with histogram preserving using pixel pair matching," *Signal Process., Image Commun.*, vol. 29, no. 3, pp. 375–384, Mar. 2014.

[37] K.-H. Jung and K.-Y. Yoo, "High-capacity index based data hiding method," *Multimedia Tools Appl.*, vol. 74, no. 6, pp. 2179–2193, Mar. 2015.

[38] G. Swain, "Adaptive pixel value differencing steganography using both vertical and horizontal edges," *Multimedia Tools Appl.*, vol. 75, no. 21, pp. 13541–13556, Nov. 2016.

[39] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," *Comput. Sci. Rev.*, vols. 13–14, pp. 95–113, Nov. 2014.

[40] A. Nandal, H. Gamboa-Rosales, A. Dhaka, J. M. Celaya-Padilla, J. I. Galvan-Tejada, C. E. Galvan-Tejada, F. J. Martinez-Ruiz, and C. Guzman-Valdivia, "Image edge detection using fractional calculus with feature and contrast enhancement," *Circuits, Syst., Signal Process.*, vol. 37, no. 9, pp. 3946–3972, Sep. 2018.

[41] A. Nandal and V. Bhaskar, "Fuzzy enhanced image fusion using pixel intensity control," *IET Image Process.*, vol. 12, no. 3, pp. 453–464, Mar. 2018.

[42] A. K. Sharma, A. Nandal, A. Dhaka, and R. Dixit, "A survey on machine learning based brain retrieval algorithms in medical image analysis," *Health Technol.*, vol. 10, no. 6, pp. 1359–1373, Aug. 2020.

[43] N. Ghoshal and J. K. Mandal, "A novel technique for image authentication in frequency domain using discrete Fourier transformation technique (IAFDDFTT)," *Malaysian J. Comput. Sci.*, vol. 21, no. 1, pp. 24–32, Jun. 2008.

[44] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. De Natale, and A. Neri, "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain," *Signal Process., Image Commun.*, vol. 26, no. 1, pp. 1–12, Jan. 2011.

[45] W. Chun-Peng, W. Xing-Yuan, and X. Zhi-Qiu, "Geometrically invariant image watermarking based on fast radial harmonic Fourier moments," *Signal Process., Image Commun.*, vol. 45, pp. 10–23, Jul. 2016.

[46] H. M. Reddy and K. B. Raja, "High capacity and security steganography using discrete wavelet transform," *Int. J. Comput. Sci. Secur.*, vol. 3, no. 6, p. 462, 2009.

[47] S. P. Jakhar, A. Nandal, A. Dhaka, B. Jiang, L. Zhou, and V. N. Mishra, "Fractal feature based image resolution enhancement using wavelet–fractal transformation in gradient domain," *J. Circuits, Syst. Comput.*, vol. 32, no. 2, Jan. 2023, Art. no. 2350035.

[48] A. Dhaka, A. Nandal, H. G. Rosales, H. Malik, F. E. L. Monteagudo, M. I. Martinez-Acuna, and S. Singh, "Likelihood estimation and wavelet transformation based optimization for minimization of noisy pixels," *IEEE Access*, vol. 9, pp. 132168–132190, 2021.

[49] D. Kumar, A. B. Joshi, S. Singh, V. N. Mishra, H. G. Rosales, L. Zhou, A. Dhaka, A. Nandal, H. Malik, and S. Singh, "6D-chaotic system and 2D fractional discrete cosine transform based encryption of biometric templates," *IEEE Access*, vol. 9, pp. 103056–103074, 2021.

[50] A. Z. Aos, A. W. Naji, S. A. Hameed, F. Othman, and B. B. Zaidan, "Approved undetectable-antivirus steganography for multimedia information in PE-file," in *Proc. Int. Assoc. Comput. Sci. Inf. Technol. Spring Conf.*, Apr. 2009, pp. 437–441.

[51] P. Kruus, C. Scace, M. Heyman, and M. Mundy, "A survey of steganography techniques for image files," *Adv. Secur. Res. J.*, vol. 5, no. 1, pp. 41–52, 2003.

[52] M. C. Trivedi, S. Sharma, and V. K. Yadav, "Analysis of several image steganography techniques in spatial domain: A survey," in *Proc. 2nd Int. Conf. Inf. Commun. Technol. Competitive Strategies*, Mar. 2016, pp. 1–7.

[53] K.-H. Jung, K.-J. Ha, and K.-Y. Yoo, "Image data hiding method based on multi-pixel differencing and LSB substitution methods," in *Proc. Int. Conf. Converg. Hybrid Inf. Technol.*, Aug. 2008, pp. 355–358.

[54] C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 488–497, Sep. 2008.

[55] A. U. Islam, F. Khalid, M. Shah, Z. Khan, T. Mahmood, A. Khan, U. Ali, and M. Naeem, "An improved image steganography technique based on MSB using bit differencing," in *Proc. 6th Int. Conf. Innov. Comput. Technol. (INTECH)*, Aug. 2016, pp. 265–269.

[56] W.-J. Chen, C.-C. Chang, and T. H. N. Le, "High payload steganography mechanism using hybrid edge detector," *Expert Syst. Appl.*, vol. 37, no. 4, pp. 3292–3301, Apr. 2010.

[57] H. Motameni, M. Norouzi, M. Jahandar, and A. Hatami, "Labeling method in steganography," *World Acad. Sci., Eng. Technol.*, vol. 24, pp. 349–354, Jun. 2007.

[58] V. M. Viswanatham and J. Manikonda, "A novel technique for embedding data in spatial domain," *Int. J. Comput. Sci. Eng.*, vol. 2, no. 2, pp. 233–236, 2010.

[59] H. Yang, X. Sun, and G. Sun, "A high-capacity image data hiding scheme using adaptive LSB substitution," *Radioengineering*, vol. 18, no. 4, pp. 509–516, 2009.

[60] M. T. Parvez and A. A.-A. Gutub, "RGB intensity based variable-bits image steganography," in *Proc. IEEE Asia–Pacific Services Comput. Conf.*, Dec. 2008, pp. 1322–1327.

[61] C.-M. Wang, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, "A high quality steganographic method with pixel-value differencing and modulus function," *J. Syst. Softw.*, vol. 81, no. 1, pp. 150–158, Jan. 2008.

[62] J.-C. Joo, H.-Y. Lee, and H.-K. Lee, "Improved steganographic method preserving pixel-value differencing histogram with modulus function," *EURASIP J. Adv. Signal Process.*, vol. 2010, no. 1, Dec. 2010, Art. no. 249826.

[63] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," *Multimedia Tools Appl.*, vol. 75, no. 22, pp. 14867–14893, 2016.

[64] S. A. Arshiya, "A comparative study of recent steganography techniques for multiple image formats," *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 1, pp. 11–25, Jan. 2019.

[65] R. Pooja, "Analysis of image steganographic techniques," *Int. J. Comput. Appl.*, vol. 114 no. 1, pp. 11–17, 2015.

[66] A. Anupriya, "Performance evaluation of secrete image steganography techniques using least significant bit (LSB) method," *Int. J. Comput. Sci. Trends Technol.* vol. 6, no. 2, pp. 160–165, Apr. 2018.

[67] W. Elmasry, "New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check," *Sādhanā*, vol. 43, no. 5, pp. 1–14, May 2018.

[68] M. H. Abood, "An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms," in *Proc. Annu. Conf. New Trends Inf. Commun. Technol. Appl. (NTICT)*, Mar. 2017, pp. 86–90.

[69] S. Yadav, P. Yadav, and A. K. Tripathi, "Image steganography on color image using SVD and RSA with 2–1–4-LSB technique," in *Proc. Int. Conf. Comput. Power, Energy Inf. Commuincation (ICCPEIC)*, Mar. 2017, pp. 164–169.

[70] S. S. Kumar and S. V. Sylish, "Image steganography in high entropy regions using a key modified LSB for improved security," in *Proc. Int. Conf. Comput. Methodolog. Commun. (ICCMC)*, Jul. 2017, pp. 1104–1108.

[71] R. Bhardwaj and V. Sharma, "Image steganography based on complemented message and inverted bit LSB substitution," *Proc. Comput. Sci.*, vol. 93, pp. 832–838, Jan. 2016.

[72] B. Mandal, A. Pradhan, and G. Swain, "Adaptive LSB substitution steganography technique based on PVD," in *Proc. 3rd Int. Conf. Trends Electron. Informat. (ICOEI)*, Apr. 2019, pp. 459–464.

[73] A. O. Modupe, A. E. Adedoyin, and A. O. Titilayo, "A comparative analysis of LSB, MSB and PVD based image steganography," *Int. J. Res. Rev.*, vol. 8, no. 9, pp. 373–377, Sep. 2021.

[74] U. M. E. Ali, E. Ali, M. Sohrawordi, and M. N. Sultan, "A LSB based image steganography using random pixel and bit selection for high payload," *Int. J. Math. Sci. Comput.*, vol. 3, pp. 24–31, 2021, doi: 10.5815/ijmsc.2021.03.03.

[75] S. Solak and U. Altınışık, "Image steganography based on LSB substitution and encryption method: Adaptive LSB+3," *J. Electron. Imag.*, vol. 28, no. 4, Aug. 2019, Art. no. 043025.

[76] L. He, F. Gao, W. Hou, and L. Hao, "Objective image quality assessment: A survey," *Int. J. Comput. Math.*, vol. 91, no. 11, pp. 2374–2388, Nov. 2014.

[77] A. Singh and H. Singh, "An improved LSB based image steganography technique for RGB images," in *Proc. IEEE Int. Conf. Electr., Comput. Commun. Technol. (ICECCT)*, Mar. 2015, pp. 1–4.

[78] E. A. Abbood, R. M. Neamah, and S. Abdulkadhm, "Text in image hiding using developed LSB and random method," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 4, p. 2091, Aug. 2018.

[79] M. Kalita, T. Tuithung, and S. Majumder, "An adaptive color image steganography method using adjacent pixel value differencing and LSB substitution technique," *Cryptologia*, vol. 43, no. 5, pp. 414–437, Sep. 2019.

[80] H. Ghanbari-Ghalehjoughi, M. Eslami, S. Ahmadi-Kandjani, M. Ghanbari-Ghalehjoughi, and Z. Yu, "Multiple layer encryption and steganography via multi-channel ghost imaging," *Opt. Lasers Eng.*, vol. 134, Nov. 2020, Art. no. 106227.

[81] N. M. Abdali and Z. M. Hussain, "Reference-free detection of LSB steganography using histogram analysis," in *Proc. 30th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2020, pp. 1–7.

[82] Accessed: Apr. 23, 2021. [Online]. Available: https://sipi.usc.edu/database/

[83] Accessed: Apr. 23, 2021. [Online]. Available: https://www.kaggle.com/datasets

[84] K. Muhammad, J. Ahmad, H. Farman, Z. Jan, M. Sajjad, and S. W. Baik, "A secure method for color image steganography using gray-level modification and multi-level encryption," *Trans. Internet Inf. Syst.*, vol. 9, no. 5, pp. 1938–1962, 2015.

[85] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, "CISSKA-LSB: Color image steganography using stego key-directed adaptive LSB substitution method," *Multimedia Tools Appl.*, vol. 76, no. 6, pp. 8597–8626, 2017.

[86] N. Shyla, K. Kalimuthu, and N. Shylaashok, *Augmentation of Novel Algorithm for Secured Information Hiding With Pixel Mapping*, vol. 5110. Wythenshawe, U.K.: EasyChair, 2021.

[87] K. Rinki, P. Verma, and R. K. Singh, "A novel matrix multiplication based LSB substitution mechanism for data security and authentication," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5510–5524, Sep. 2022.

[88] P. Mathivanan and A. B. Ganesh, "Colour image steganography using XOR multi-bit embedding process," in *Proc. Int. Conf. Energy, Commun., Data Anal. Soft Comput. (ICECDS)*, Aug. 2017, pp. 1980–1988.

[89] A. A.-A. Gutub, "Pixel indicator technique for RGB image steganography," *J. Emerg. Technol. Web Intell.*, vol. 2, no. 1, pp. 56–64, 2010.

[90] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," *Multimedia Tools Appl.*, vol. 75, no. 22, pp. 14867–14893, 2016.

[91] P. Maniriho and T. Ahmad, "Information hiding scheme for digital images using difference expansion and modulus function," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 31, no. 3, pp. 335–347, Jul. 2019.

[92] N. Shyla, K. Kalimuthu, and N. Shylaashok, *Augmentation of Novel Algorithm for Secured Information Hiding With Pixel Mapping*, vol. 5110. Wythenshawe, U.K.: EasyChair, 2021.

[93] A. P. Kumar, L. Gajjela, and N. R. Sai, "A hybrid hash-stego for secured message transmission using stegnography," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 981, no. 2, Dec. 2020, Art. no. 022014.

[94] A. Shahanaghi, M. A. Akhaee, S. Sarreshtedari, and R. Toosi, "Optimum group pixel matching strategies for image steganography," in *Proc. 18th Int. ISC Conf. Inf. Secur. Cryptol. (ISCISC)*, Sep. 2021, pp. 89–94.

[95] M. M. Patil, "Modulus function and pixel value differencing coupled with modified pixel indicator based secret data hidding method," *Int. J. Adv. Sci. Eng. Technol.*, vol. 4, no. 2, pp. 26–29, 2016.

[96] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," *Multimedia Tools Appl.*, vol. 75, no. 22, pp. 14867–14893, 2016.

[97] A. Zakaria, M. Hussain, A. Wahab, M. Idris, N. Abdullah, and K.-H. Jung, "High-capacity image steganography with minimum modified bits based on data mapping and LSB substitution," *Appl. Sci.*, vol. 8, no. 11, p. 2199, Nov. 2018.

[98] M. Ulker and B. Arslan, "A novel secure model: Image steganography with logistic map and secret key," in *Proc. 6th Int. Symp. Digit. Forensic Secur. (ISDFS)*, Mar. 2018, pp. 1–5.

[99] S.-P. Lu, R. Wang, T. Zhong, and P. L. Rosin, "Large-capacity image steganography based on invertible neural networks," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2021, pp. 10816–10825.

[100] P. D. Shah and R. S. Bichkar, "Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure," *Eng. Sci. Technol., Int. J.*, vol. 24, no. 3, pp. 782–794, Jun. 2021.

[101] A. Hamza, D. Shehzad, M. S. Sarfraz, U. Habib, and N. Shafi, "Novel secure hybrid image steganography technique based on pattern matching," *KSII Trans. Internet Inf. Syst. (TIIS)*, vol. 15, no. 3, pp. 1051–1077, 2021.

[102] N. I. Yassin and E. Houby, "EM image steganography technique based on integer wavelet transform using most significant bit categories," *Int. J. Intell. Eng. Syst.*, vol. 15, pp. 499–508, 2022.

[103] S.-P. Lu, R. Wang, T. Zhong, and P. L. Rosin, "Large-capacity image steganography based on invertible neural networks," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2021, pp. 10816–10825.

[104] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, "Hiding data using efficient combination of RSA cryptography, and compression steganography techniques," *IEEE Access*, vol. 9, pp. 31805–31815, 2021.

[105] R. Sonar and G. Swain, "A hybrid steganography technique based on RR, AQVD, and QVC," *Inf. Secur. J., Global Perspective*, vol. 31, no. 4, pp. 1–20, 2022.

[106] M. A. Wani and B. Sultan, "Deep learning based image steganography: A review," *WIREs Data Mining Knowl. Discovery*, Nov. 2022, Art. no. e1481, doi: 10.1002/widm.1481.

[107] A. Gaffar et al., "A high capacity multi-image steganography technique based on golden ratio and non-subsampled contourlet transform," *Multimedia Tools Appl.*, vol. 81, pp. 24449–24476, Mar. 2022, doi: 10.1007/s11042-022-12246-y.

[108] S. Dhawan, R. Gupta, H. K. Bhuyan, R. Vinayakumar, S. K. Pani, and A. K. Rana, "An efficient steganography technique based on S$_2$OA & DESAE model," *Multimedia Tools Appl.*, pp. 1–29, Sep. 2022.

[109] D. R. I. M. Setiadi, "Improved payload capacity in LSB image steganography uses dilated hybrid edge detection," *J. King Saud Univ., Comput. Inf. Sci.*, vol. 34, no. 2, pp. 104–114, 2022, doi: 10.1016/j.jksuci.2019.12.007.

[110] I. Avcibas, N. Memon, and B. Sankur, "Steganalysis using image quality metrics," *IEEE Trans. Image Process.*, vol. 12, no. 2, pp. 221–229, Feb. 2003.

[111] A. Almohammad and G. Ghinea, "Stego image quality and the reliability of PSNR," in *Proc. 2nd Int. Conf. Image Process. Theory, Tools Appl.*, Jul. 2010, pp. 215–220.

[112] Q. Huynh-Thu and M. Ghanbari, "Scope of validity of PSNR in image/video quality assessment," *Electron. Lett.*, vol. 44, no. 13, pp. 800–801, Jun. 2008.

[113] T. Chai and R. Draxler, "Root mean square error (RMSE) or mean absolute error (MAE)," *Geosci. Model Develop. Discuss.*, vol. 7, no. 1, pp. 1525–1534, 2014.

[114] U. Sara, M. Akter, and M. S. Uddin, "Image quality assessment through FSIM, SSIM, MSE and PSNR-A comparative study," *J. Comput. Commun.*, vol. 7, no. vol. 3, pp. 8–18. 2019.

[115] F. Zhao, Q. Huang, and W. Gao, "Image matching by normalized cross-correlation," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, May 2006, p. 2.

[116] J.-C. Yoo and T. H. Han, "Fast normalized cross-correlation," *Circuits, Syst. Signal Process.*, vol. 28, pp. 819–843, Dec. 2009.

[117] D.-M. Tsai and C.-T. Lin, "Fast normalized cross correlation for defect detection," *Pattern Recognit. Lett.*, vol. 24, pp. 2625–2631, Nov. 2003.

[118] M. Hussain, Q. Riaz, S. Saleem, A. Ghafoor, and K.-H. Jung, "Enhanced adaptive data hiding method using LSB and pixel value differencing," *Multimedia Tools Appl.*, vol. 80, no. 13, pp. 20381–20401, May 2021.

[119] C. G. Tappe and A. V. Deorankar, "An improved image steganography technique based on LSB," *Int. Res. J. Eng. Technol. (IRJET)*, vol. 4, no. 4, pp. 1234–1237, 2017.

[120] R. M. Neamah, J. A. Abed, and E. A. Abbood, "Hide text depending on the three channels of pixels in color images using the modified LSB algorithm," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 10, no. 1, p. 809, Feb. 2020.

[121] R. Shanthakumari and S. Malliga, "Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm," *Multimedia Tools Appl.*, vol. 79, nos. 5–6, pp. 3975–3991, Feb. 2020.

[122] V. Kumar, P. Rao, and A. Choudhary, "Image steganography analysis based on deep learning," *Rev. Comput. Eng. Stud.*, vol. 7, no. 1, pp. 1–5, Mar. 2020.

[123] T. Anbu, M. M. Joe, and G. Murugeswari, "A comprehensive survey of detecting tampered images and localization of the tampered region," *Multimedia Tools Appl.*, vol. 80, no. 2, pp. 2713–2751, Jan. 2021.

[124] D. M. Chandler, "Seven challenges in image quality assessment: Past, present, and future research," *ISRN Signal Process.*, vol. 2013, pp. 1–53, Feb. 2013.

[125] W. Lin and C.-C. J. Kuo, "Perceptual visual quality metrics: A survey," *J. Vis. Commun. Image Represent.*, vol. 22, no. 4, pp. 297–312, May 2011.

[126] X. Zhang and S. Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security," *Pattern Recognit. Lett.*, vol. 25, no. 3, pp. 331–339, Feb. 2004.

[127] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognit. Lett.*, vol. 24, nos. 9–10, pp. 1613–1626, Jun. 2003.

[128] W. Luo, F. Huang, and J. Huang, "A more secure steganography based on adaptive pixel-value differencing scheme," *Multimedia Tools Appl.*, vol. 52, nos. 2–3, pp. 407–430, Apr. 2011.

[129] J. Fridrich and M. Goljan, "Practical steganalysis of digital images: State of the art," *Proc. SPIE*, vol. 4675, pp. 1–13, Apr. 2002.

[130] R. Atta and M. Ghanbari, "A high payload steganography mechanism based on wavelet packet transformation and neutrosophic set," *J. Vis. Commun. Image Represent.*, vol. 53, pp. 42–54, May 2018.

[131] T. Pevny, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 215–224, Jun. 2010.

[132] J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 868–882, Jun. 2012.

[133] V. Holub and J. Fridrich, "Low-complexity features for JPEG steganalysis using undecimated DCT," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 219–228, Feb. 2015.

[134] J. Fridrich and M. Goljan, "Practical steganalysis of digital images: State of the art," in *Proc. SPIE*, vol. 4675, pp. 1–14, Apr. 2002.

SHAHID RAHMAN received the bachelor's degree in mathematics, physics, and computer science from the University of Swat, Khyber Pakhtunkhwa, Pakistan, the M.S. degree in computer science from Abasyn University Peshawar (AUP), and the M.Sc. degree in computer science from Islamia College University, Peshawar. He is currently pursuing the Ph.D. degree in computer science with the Qurtuba University of Science and Technology, Peshawar. He is also working as a Lecturer with the Department of Computer Science, University of Buner, Khyber Pakhtunkhwa. He has over eight years of experience in academia and research. He has published several research papers in leading journals and conferences. His current research interests include software engineering, cryptography, steganalysis and steganography, computer vision, machine learning, and deep learning.

JAMAL UDDIN received the M.Sc. degree from the University of Peshawar, Pakistan, in 2005, the M.Phil. degree from HITEC University at Taxila, Taxila, Pakistan, in 2013, and the Ph.D. degree in information technology with specialization in data mining, software engineering, artificial intelligence, and machine learning from the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia (UTHM), in 2017. He belongs to Mardan, Khyber Pakhtunkhwa, Pakistan. From 2008 to 2017, he was with the teaching profession at various national (HITEC Taxila, Gandhara Institute of Technology, Peshawar, and Professional College of Commerce, Peshawar) and foreign institutions (PSS Sana'a, Pakistan Embassy, Yemen, and UTHM, Johor, Malaysia). He has been working as an Assistant Professor and the Director ORIC of the Qurtuba University of Science and Information Technology, Peshawar, Pakistan, since September 2017. He has published in reputed computer science journal articles, book chapters, and conference proceedings. He is a reviewer of different research journals. Total 19 of his M.S. students are graduated. He is currently supervising several M.S. and Ph.D. national and international scholars. His research interests include clustering, rough set theory, classification, prediction, categorical data, and fractional order ODE's/PDE's. He is an Assistant Editor of *HEC Category Y Science Journal "The Sciencetech."*

MUHAMMAD ZAKARYA (Senior Member, IEEE) received the Ph.D. degree in computer science from the University of Surrey, Guildford, U.K. He is currently an Assistant Professor with the Faculty of Computing and Information Technology (FCIT), Sohar University, Oman. Previously, he was an Assistant Professor with the Department of Computer Science, Abdul Wali Khan University Mardan (AWKUM), Pakistan. His research interests include cloud computing, mobile edge clouds, the Internet of Things (IoT), performance, energy efficiency, algorithms, and resource management. He has deep understanding of the theoretical computer science and data analysis. Furthermore, he also owns deep understanding of various statistical techniques, which are largely used in applied research. His research has appeared in several international conferences, journals, and transactions of repute. He is a TPC Member of few prestigious international conferences, including CCGrid, GECON, and UCC. He is also an Associate Editor of IEEE ACCESS journal, *Journal of Cloud Computing* (Springer), and *Journal of Cluster Computing* (Springer), and aGuest Editor of *Cluster Computing* journal (Springer). He is the Program Director of the iFuture, a leading Research Group, AWKUM, which has research collaboration with the Clouds Laboratory, The University of Melbourne, Australia, and the IoT Laboratory, Cardiff University, U.K. He was listed in the world's top 2% scientists list, in 2020 and 2021.

HAMEED HUSSAIN received the bachelor's degree in information technology from Gomal University Dera Ismail Khan, Pakistan, in 2007, and the M.S. and Ph.D. degrees in computer science from the COMSATS Institute of Information Technology (CIIT), Pakistan, in 2009 and 2017, respectively. He is the author of several international publications. He is an active researcher. His research interests include optimization, machine learning, fog and edge computing, real-time systems, resource allocation, and load balancing in high performance computing.

AYAZ ALI KHAN received the Ph.D. degree in computer science from Abdul Wali Khan University, Pakistan. He is currently an Assistant Professor with the Department of Computer Science, University of Lakki Marwat, Pakistan. His research interests include cloud computing, mobile edge clouds, the Internet of Things (IoT), performance, energy efficiency, algorithms, and resource management. He has deep understanding of the theoretical computer science and data analysis. Furthermore, he also owns deep understanding of various statistical techniques, which are largely used in applied research. His research has appeared in several international conferences, journals, and transactions of repute.

AFTAB AHMED received the Ph.D. degree in electronic engineering from the University of York, U.K., in 2019. He is currently a Lecturer with the Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan. His research work is related to improvement in performance in ultra-dense high-capacity networks. His research interests include radio resource management, topology management to improve system performance and overall energy efficiency in ultra-dense high-capacity wireless networks, and machine learning.

MUHAMMAD HALEEM is currently an Assistant Professor with the Department of Computer Science, Faculty of Engineering, Kardan University, Kabul, Afghanistan. His research interests include the Internet of Things, machine learning, and data analytics.