A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method

SHAHID RAHMAN¹, JAMAL UDDIN², HABIB ULLAH KHAN³, HAMEED HUSSAIN⁴, AYAZ ALI KHAN⁵, AND MUHAMMAD ZAKARYA⁶ (Senior Member, IEEE)

¹Department of Computer Science, Qurtuba University of Science and Information Technology, Dera Ismail Khan 29050, Pakistan
²Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Doha, Qatar
³Department of Computer Science, The University of Buner, Buner 19280, Pakistan
⁴Department of Computer Science, University of Lakki Marwat, Lakki Marwat 28420, Pakistan
⁵Department of Computer Science, Abdul Wali Khan University Mardan, Mardan 23200, Pakistan

Corresponding author: Habib Ullah Khan (habib.khan@qu.edu.qa)

This work was supported in part by the Qatar National Library, Doha, Qatar; in part by the Qurtuba University of Science and Technology, Peshawar, Pakistan; and in part by the Qatar University under Grant IRCC-2021-010.

ABSTRACT Communication has become a lot easier in this era of technology, development of high-speed computer networks, and the inexpensive uses of Internet. Therefore, data transmission has become vulnerable to and unsafe from different external attacks. Every communication body wants to secure their data while communicating over the Internet. The internet has various benefits but the main demerit is the privacy and security and the transmission of data over insecure network or channel may happen. Various techniques used for secure communication in order to address these issues, steganography plays an important role. Steganography is the process of obfuscation that makes something incomprehensible and unclear. Different image steganography research methods are proposed recently but each has their advantages and disadvantages and still have necessity to develop some better image steganography mechanisms to achieve the reliability between the basics criteria of image steganography. Therefore, the proposed work, in this paper, is based on the Least Significant Bit (LSB) substitution method. The LSB substitution method can minimize the error rate in embedding process and can achieve greater reliability in criteria, using novel algorithm based on value difference. In this paper, we proposed a novel technique in steganography within the digital images such is RGB, Gray Scale, Texture, Aerial images to achieve higher security, imperceptibility, capacity, and robustness as compared with existing methods. The experimental outcomes of the suggested approach prove further developed strength and justify the feasibility of our research. Through numerical simulations, we observed that the proposed strategy outperformed the next-best current methodology by 5.561 percent in terms of PSNR Correlation score. Additionally, the proposed approach achieved a 6.43 percent better score in PSNR with a variable measure of code inserted in similar images with distinct dimensions. Furthermore, encrypting the same amount of information in images of varying sizes resulted in approximately 6.77 percent improvements. Embedding different sizes of a particular secret message in a different image (such as Gray, Texture, Aerial and RGB images) came out with about 5.466 percent of better score.

INDEX TERMS Image steganography, LSB, image quality assessment metrics, histogram analysis, image, capacity, robustness.

I. INTRODUCTION

Recently, the cost of information exchange has reduced significantly due to modern and state-of-the-art communication technologies and infrastructure. As a result of this
improvements, the interpersonal communication has become very easy. However, if information are not protected, then criminals may exploit it during transmission. Therefore, along with the convenience it provides, this also creates excessive demand for verification and security sources; therefore, stressing the role of information security [19]. For example, let us take the example of information exchange between government institutions and military. If some confidential information is openly posted online, it could be easily deciphered and exploited by criminals, thereby jeopardizing the national security [35]. Therefore, promising information protecting technology is essentially needed in addition to cryptography and steganography. In fact, Steganography has become more relevant in this situation. Steganography is mostly used to conceal hidden messages that would otherwise be difficult to detect. Nobody will be able to surmise that a secret message has been sent [4].

However, the current development in digitization has urged the creation of a huge measure of data. Putting away, sending, and sharing this secret data over an open and uncertain correspondence channel is, in fact, yet a perplexing test. Therefore, the cover steganography comes into the art of science by conveying restricted information in a suitable interactive media transporter, e.g., image, sound, and video records. In fact, this is the game of embedding secret information in a manner that no one or attacker can detect and read the secret data or information.

The objective of the cover steganography depends on how to hide the presence of the encrypted message and vice versa. Moreover, the cover Steganography has different valuable applications in various fields. Hence, it is an addition, not a replacement. Notwithstanding, similar to some other techniques, it may also be exploited [12]. Figure 1 shows the fundamental steps which are essential for encoding and decoding the message and then sending it through the communication channel.

In today’s advance era of digital world, the majority of today’s cover objects for concealing the secret message are multimedia objects such as Image, Audio, video, Text, and Network Protocol etc. as a cover media [14]. So cover media is a place where we actually store secret information. In digital medium for steganography based on cover media, there are six different types of steganography techniques used for embedding secret message depending upon a cover object i.e., text, image, email, network, video, and audio – as shown in Figure 2. Each of these types is explained in the subsequent discussion.

The text steganography hides information inside a text file. It involves changing the format of the text, generating random text, selecting random text, and/or generating some rules of grammar to get some readable text etc. In Image Steganography, we are having an image that, in fact, helps in hiding data within the image. It is one of the most widely used method for hiding the data. This is due to the fact that in an image, there are huge number of pixels of digital representation. Therefore, it is easy to hide secret data within the image. The secret information is concealed in audio signals via audio steganography, which modifies the binary sequences of the associated audio files. We can conceal any type of data in digital video format using the video steganography. This type of steganography has the benefit of making it relatively simple to embed vast amount of data. We can infer that it combines audio and visual steganography. Similarly, the network steganography is a technique that uses many network protocols for embedding the secret information such as TCP/IP, UDP, ICMP, and many others. Information is hidden within the header file of the TCP/IP packets and some fields are optional or not important. Finally, another type of steganography is the Email Steganography which is not very well-known steganography. Note that the Email which contains file embedded within hidden information using steganography can be an extremely tedious activity to identify the hidden information [9], [14].

Now let us take a look at numerous characteristics that a steganography approach must, essentially, and should, potentially, process. Defending it from assailants, Steganography is one of the significant and complex mechanisms utilized for safely moving a covert message in an impalpable way [32]. In fact, this does not amend the scheme of the encrypted message rather covers it within a cover-image. The principal objective of the steganography is to incorporate high payload, power, and better intangibility and temper the original message as shown in Figure 3 and Table 1. The payload demonstrates the measure of information encrypted in the cover.
image and is characterized in bits per pixel (bpp). Robustness shows the degree of trouble looked at by assailants through removal of privileged data that secure from any lawbreakers or attackers. Noiselessness or perception implies perceptibility that is estimated through utilizing distinctive picture or image quality evaluation measurements like Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Metric (SSIM) and so on. For example, little perceptible contortion between unique and stego pictures and higher PSNR score addresses top caliber of the stego-images [27].

The spatial domain techniques adjust the gray level of the cover image for concealing confidential information. A high payload and better result in stego-images can be obtained in spatial area procedures. However, for strength and better flawlessness against image preparing activities (trimming, scaling, and Noise assaults) and factual assaults, various research methods have been developed in spatial domain such as: (i) Modified LSB Matching technique [1]; (ii) Enhanced Modified Signed Digit (EMSD) [25]; (iii) Development of the Least Significant Bit (DLSB) [3]; (iv) Pixel Indicator Technique (PIT) [18]; (v) LSB-S and Neighboring Pixel Value Differencing [20]; (vi) Inverted LSB using Adaptive Pattern Technique [2]; and (vii) Pixel Value Differencing (PVD) technique [28] etc. These methods are for the most part utilized and worked well in image steganography and applications because of their better strength against factual steganalysis [10], [11]. However, these techniques have unacceptable amount of embedding message, that consequently result in stego of bad quality images, and computation complexity when contrasted with other spatial domain techniques.

This should be noted that encoding the mysterious message bits into the stego-image LSB is quite, possibly, the most regular method which is used in the cover steganography. It is significant for information concealing system and used commonly because of its plainness. Moreover, this changes the base fundamental bit of the stego-image pixels, which changes simply the tone of the hiding. In fact, this is assumed as a rare or slight change, which cannot be seen by the naked eyes. This process is done either by shuffling shape or improvement base. The Red, Green, and Blue (RGB range 0-255, and per pixel Depth=24 bits) channels are used due to the fact that RGB having three channels can cover more embedded message. After that, the first three channels are separated from the cover image and the secret message bits are embedded with the LSBs of one of the three channels. Then, the said channels are put close together to make the stego-image [33].

The secret data is typically concealed in one of the RGB channels i.e. blue channel that is less discernible by the Human Visual System (HVS) [5]. The least significant bit replacement plans have large embedding capacity and enhanced intangibility (depending on the choice of the cover image), although they are more powerless against steganalysis assaults [21], [29]. Figure 4 elaborates the basic concepts of the LSB based embedding process by taking a cover image and selecting a pixel while, subsequently, then dividing it into RGB components. On the one hand, the binary representation of the RGB component shows the pixel binary value of each component. On the other hand, a secret message is selected and then transformed into the American Standard Code for Information Interchange (ASCII) value, subsequently, then transformed to binary and finally embedded into each RGB components. To supplant all the LSB bits of pixels inside the cover image with secret bits, the LSB replacement strategy is non-trivial and complicated [17]. Therefore, it embeds the fixed-length secret pieces in a similar fixed length LSBs of pixels as displayed in Figure 5. However, embedding how many bits per pixel in each RGB is dependent on the steganographers. The major and fundamental three contributions of the research conducted in this work are as given below.

- We design and create a step-by-step data exploitation framework;
- Through real datasets, we assess, validate, and then contrast the proposed method with earlier approaches and published findings.

In coming sections, the remaining paper is organized in the given manner. In Section II, we elaborate the literature review and the state-of-art-art methods of the steganography technology. The elaboration of the suggested approach is given in Section III. Furthermore, the experimental settings, datasets, and evaluation findings and outcomes are given in Section IV. Lastly, the key findings, limitations, and future work are deliberated in Section V.

II. RELATED WORKS

Ancient Greeks developed steganography about 484-425 BC. The ruler of the Miletus, Histaeus, shaved the head of one of his legal slaves before tattooing a puzzling phrase or drawing on it. When the slave’s hair started to grow back, again the slave was moved to Aristagoras in order to give the slave the secret text. The slave’s head was once more shaved to continue the enigmatic message when he arrived at his
destination [7]. From that time to date, numerous experts and current steganography procedures have been created and utilized for image steganography. There are many applications available in many fields of cover steganography for drives like data stowing away secret data. In next sections, some of the LSB based Image steganographic techniques have been briefly described and critically analyzed.

Before coming to the critical analysis of different steganographic techniques, let us start to elaborate the basic concepts of the Least significant bit image steganography technique which is the most popular and widely technique to hide the secret message. More precisely, as shown in Figure 4, let us call and assume the given image as a digital image. Moreover, every digital image is the finite sets of digital values called pixels. A pixel is actually a short for a particular image’s element. So, each pixel has one color at a time and whenever more color often together to make more colors and thousands and millions of pixels make an image. However, the proposed method also used the RGB color model due to the three channels because it is very valuable for embedding more secret data. This should be noted that the RGB color model is an additive colors model due to the fact that in this model Red, Green, and Blue light are combined in different based and to regenerate a broad area of colors. In fact, each color having values of binary value. The depth of the bits per pixel in RGB colors model is 24 bits, which means every color is having an 8 bits’ representation [24].

However, when we are working with the binary values, then the Most Significant Bit (MSB) and the Least Significant Bit (LSB) methods are used. The left most bit is the MSB and the right most bit is the LSB which is shown in Figure 5 below. Now, if we change the left most significant bit then it will have a large impact on the final value. For example, as shown in Figure 5, if we have the range of 255 and the binary representation of 255 which is 8 consecutive ones.

Now, if we change the left most bit from 1 to 0 then the decimal value change from 255 to 127. We can see in the figure that they have a large impact on the final values. While in other hand, if we change the right most bit, then it will have a less impact on the final value. Furthermore, if we change the value from 1 to 0 then the value changes from 255 to 254. Therefore, we can see the final value impact is approximately 0.00002% which is very less than as compared to the impact caused by the MSB. To summarize this discussion, the main point is that if we modify the MSB, then it will have high influence and effect over the last and final value. However, if we change the LSB, then it will have less impact; and, consequently, this less impact on the final value of the LSB is called the LSB based Image steganography [13].

In fact, the least Significant bit steganography (LSBS) involves overwriting the bits with the lowest arithmetic value. Therefore, this technique is very used for Audio, Video, text, and Image based steganography. Let us consider a simple example to explain the LSB clearly. Suppose a secret message letter ‘A’ having the binary representation which is 1 followed by 5 zeros and then 1 – as shown in Figure 6. Consider that the RGB color model and let us select 3 pixels for the hidden secret message. We can see that the secret letter bits are hidden in the selected pixel of the image and is shown as bold and red colored. Therefore, the requirement of the LSB steganography is that the stego and cover image after embedding process should be identical and free from any suspected change which can be seen by any naked eye [23].

In Figure 6, the LSBs are changed in red bold places of pixels. It shows that the pixels are changed. Human spectators will not be able to recognize the cover and stego images if blue channel is used for embedding. All the pixels of the encoded image will be considered 1 value isolated from the cover image. With encoding higher bits, the plain exploitation of the cover image happens, abolishing the point of encoding. In Table 2, the most relevant researches of the LSB substitution-based techniques are critically analyzed. The techniques presented in Table 2 are critically analyzed based on different evaluation criteria of steganography such as capacity, robustness, temper protection, and computation which almost cover the evaluation criteria up to some limits. Therefore, to evaluate reasonably the performance of various steganography methods, it is mandatory to elaborate the acceptable criteria for improving the techniques because the evaluation criteria may also lead us to the correct direction. However, the basic criteria capacity means making maximum hiding capacity possible depending on the cover object for hiding.

This should be noted that robustness elaborates that how a stego image resists against different steganography attacks and should also provide robustness against image processing techniques such as cropping, scaling, and tempering etc. Due to the fact, that steganography may suffer from different passive and active attacks. Similarly, perception means that how the cover and encrypted image remains same perceptibly because it should produce a high perceptual image.

**TABLE 1. Evaluations criteria for the Steganography [7], [24].**

| Criteria               | Advantages | Disadvantages |
|------------------------|------------|---------------|
| Perceptual transparency (HVS) | High       | Low           |
| Capacity               | High       | Low           |
| Calculation complexity  | Low        | High          |
| Robustness             | High       | Low           |
| Temper protection       | High       | Low           |

This table elaborates the essential needs for any image steganographic method, that how to critically investigate the performance and value-ability of the method. This is due to the fact that if someone develops a image steganographic method and focuses only on one parameter and ignore the others then, potentially, they breached the basic needs of the

---

VOLUME 10, 2022

S. Rahman et al.: Novel Steganography Technique for Digital Images Using the LSB Substitution Method
steganography. Therefore, as shown in Table 1, it is the evaluation criteria for any image steganography method that how to calculate the effectiveness and efficiency of the method. In the proposed technique, we design a novel and upgraded procedure in digital images such is RGB, Texture, Gray-scale, and Aerial image, to make it more powerful and secure that no exposed eye can identify. The Least Significant Bit (LSB) method is one of the well-known and widely used strategies that is applied for steganography. Additionally, the prominent technique for present day steganography is to use the LSB of image pixel data. In the LSB based steganography it is required to replace all secret bits with the LSB pixels bit of the cover object. Therefore, the LSB embeds the fixed-length secret bits in comparative fixed-length LSBs of pixels. The proposed method and its performance is measured with four unique perspectives as explained later in Section III and Section IV.

A. CRITICAL ANALYSIS OF EXISTING IMAGE STEGANOGRAPHY METHODS

The Pixel Indicator System (PIT) is that approach in which one particular and specific channel is implemented for sign;
TABLE 2. Analysis of different LSB based Image Steganography and other most relevant methods.

| S No | Method used | Advantages | Disadvantages | Analysis Based on |
|------|-------------|------------|---------------|------------------|
|      |             |            |               | Capacity | Perceived | Computation | Reusability | Transparency |
| 1    | Modified LSB substitution for RGB Images | High Security, quality and perception | payload limit and vulnerability of statistical attacks | × | ✓ | ✓ | ✓ | ✓ |
| 2    | Improved LSB for RGB images | High security, great quality and robustness | Payload, Vulnerabilities (noise, cropping) computation | ✓ | ✓ | ✓ | × | × |
| 3    | LSB Replacement through XOR Substitution | High Security and Good image quality | Hidden data too Low | × | × | × | ✓ | ✓ |
| 4    | Multi Stego for gray scale images | High Capacity and low distortion | vulnerability to different attacks | ✓ | × | × | × | × |
| 5    | Value differencing using adjacent pixel and LSB substitution technique | High security, imperceptibility, and robustness | Hidden data too low and vulnerability of statistical attacks | × | ✓ | ✓ | ✓ | × |
| 6    | GL Modification and MLB | high imperceptibility, times Saving and robustness | weakness to different assaults such as cropping, scaling and noise | ✓ | × | × | × | ✓ |
| 7    | LSB | High Security and Good image quality | visual quality, payload limit and vulnerability of statistical attacks | × | × | × | ✓ | ✓ |
| 8    | LSB substitution with Random pixel selection | High security for message in Stego-image | without thinking about Visual Quality in Random pixel determination | × | ✓ | ✓ | × | ✓ |
| 9    | PIT | High hidden data better imperceptibility | payload limit is absolutely dependent upon have image and pointer bits | ✓ | × | × | × | × |
| 10   | Improving histogram based flexible data hiding by inserting predictions | Larger embedding capacity & better image quality | Security risks | ✓ | × | × | ✓ | ✓ |
| 11   | Generating Data Hiding Method for Gray Scale Image to get Multi Stego-image based | High capacity and low distortion | weakness to different assaults (cropping, scaling and noise) | ✓ | × | × | × | × |
| 12   | Inserted LSB using Adaptive Pattern | Imperceptibility Embedding capacity is more | vulnerability to different attacks | ✓ | × | × | × | × |
| 13   | DLSB Dynamic Stego key | application of a dynamic key of the DLSB High Security | Hidden data too low | × | ✓ | × | ✓ | ✓ |

however, the other remaining two channels are implemented for inserting disguised data as a bit of a predefined cycle way which updates the power of the proposed approach [26]. This technique also avoids the fundamental trade burden and additional costs. In fact, the major and key feeble justification behind this technique is that the payload is absolutely liable to the cover image and pointer bits considering which the payload might be diminished. The PIT method stores away a settled amount of bits in each and every pixel. This may acquire additional modifications in the image that implants higher amount of covered bits in every pixel.

In [26], the author proposed a clever method of information concealing utilizing multi stego-images to accomplish high limits with low disfigurement [26]. In each scenario, the primary image’s pixels generate four additional pixels. Using the modified LSB in coordinating approach, the constrained data are masked on all of the sent pixels. After that, all pixels are modified again to reflect the defacement’s failure. The primary image is separated into four distinct secret images, each of which covers one digit per pixel. Through modifying the Exchange Carrier Object (EC) for each of the various stego-images and combining the LSB coordinating with the Pixel Value Differencing, the authors hope to develop reversible steganography (PVD).

A spatial adaptive domain color image steganography technique is shown which utilizes the LSB replacement and adjoining pixel esteem differing idea [1], [16]. Using a block layout of 3 by 3 pixels, the technique utilizes all the edge pixels in all possible ways. Three stages make up the suggested process: (i) XOR of data encoding; (ii) the embedding process of encoded bits while utilizing the PVD and the LSB substitution; and (iii) the extraction. The exploratory outcomes of this research work demonstrate that the recommended technique has accomplished an extremely high inserting limit of approximately 3.498 per pixel bits (ppb) with PSNR values 38.23 dB. From this exploration work, it was seen that the cover image determination exceptionally affects the results of a steganography strategy. This study work actually needs some proficient cover image choice strategy that can likewise be consolidated with the proposed technique in order to get a further developed and improved outcome.

In image steganography, the Pixel Value Differencing (PVD) is a grounded method that has a high limit (utilizing range table). However, it experiences histogram-based steganalysis assault [20], [28]. Applying an irregular key of equal size, the One Time Paid (OTP) encryption is the most secure when we need to consolidate the imports of PVD with the safety of OTP. Prior to inserting an arbitrary created key is utilized to ascent the mysterious message bits. Furthermore, the authors proposed to conspire doesn’t utilize a range table to expand the cover image utilizing 2 × 2 non-covering pixel blocks. When contrasted with some notable procedures, the consequence of this examination work shows that this plan
TABLE 3. PSNR metric values of the proposed method on different sizes of message that are embedded in different images of same dimensions.

| S. No | Different RGB Images of same dimension 512 x 512 | PSNR values in dB of the proposed method |
|-------|-----------------------------------------------|------------------------------------------|
| 1     | Image [1], [512 x 512] on different sizes of secret message (4, 6, 8, 10, 12, 14, 16 KB’s) | On 4 kb PSNR value is 90.243 On 6 kb PSNR value is 76.033 On 8 kb PSNR value is 79.223 On 10 kb PSNR value is 80.143 On 12 kb PSNR value is 70.023 On 14 kb PSNR value is 83.023 On 16 kb PSNR value is 89.043 |
| 2     | Image [2], [512 x 512] on different sizes of secret message (4, 6, 8, 10, 12, 14, 16 KB’s) | On 4 kb PSNR value is 94.223 On 6 kb PSNR value is 76.113 On 8 kb PSNR value is 88.043 On 10 kb PSNR value is 80.043 On 12 kb PSNR value is 81.323 On 14 kb PSNR value is 85.023 On 16 kb PSNR value is 87.013 |
| 3     | Image [3], [512 x 512] on different sizes of secret message (4, 6, 8, 10, 12, 14, 16 KB’s) | On 4 kb PSNR value is 86.022 On 6 kb PSNR value is 74.042 On 8 kb PSNR value is 75.043 On 10 kb PSNR value is 70.013 On 12 kb PSNR value is 82.041 On 14 kb PSNR value is 85.013 On 16 kb PSNR value is 90.243 |
| 4     | Image [4], [512 x 512] on different sizes of secret message (4, 6, 8, 10, 12, 14, 16 KB’s) | On 4 kb PSNR value is 88.033 On 6 kb PSNR value is 74.041 On 8 kb PSNR value is 73.012 On 10 kb PSNR value is 76.043 On 12 kb PSNR value is 82.041 On 14 kb PSNR value is 85.013 On 16 kb PSNR value is 90.243 |
| 5     | Image [5], [512 x 512] on different sizes of secret message (4, 6, 8, 10, 12, 14, 16 KB’s) | On 4 kb PSNR value is 80.043 On 6 kb PSNR value is 84.012 On 8 kb PSNR value is 83.067 On 10 kb PSNR value is 85.049 On 12 kb PSNR value is 86.567 On 14 kb PSNR value is 84.534 On 16 kb PSNR value is 86.043 |
| 6     | Image [6], [512 x 512] on different sizes of secret message (4, 6, 8, 10, 12, 14, 16 KB’s) | On 4 kb PSNR value is 89.043 On 6 kb PSNR value is 78.098 On 8 kb PSNR value is 75.067 On 10 kb PSNR value is 70.684 On 12 kb PSNR value is 83.233 On 14 kb PSNR value is 86.423 On 16 kb PSNR value is 87.745 |
| 7     | Image [7], [512 x 512] on different sizes of secret message (4, 6, 8, 10, 12, 14, 16 KB’s) | On 4 kb PSNR value is 80.042 On 6 kb PSNR value is 81.045 On 8 kb PSNR value is 84.098 On 10 kb PSNR value is 88.033 On 12 kb PSNR value is 85.332 On 14 kb PSNR value is 82.324 On 16 kb PSNR value is 90.423 |
| 8     | Image [8], [512 x 512] on different sizes of secret message (4, 6, 8, 10, 12, 14, 16 KB’s) | On 4 kb PSNR value is 91.421 On 6 kb PSNR value is 83.045 On 8 kb PSNR value is 84.098 On 10 kb PSNR value is 87.423 On 12 kb PSNR value is 88.567 On 14 kb PSNR value is 83.379 On 16 kb PSNR value is 89.415 |

gives a better quality cover picture or image. To expand the concealing limit with more bits per pixel, the OTP method could be joined with edge recognition methods as a future direction.

In [8] and [30], the authors elaborate the most essential elements of the image steganography which are high inserting limit and adequate visual image quality which are talked about largely. To implant restricted information, the proposed calculations is another limit information concealing procedure which is dependent on the Least Significant Bit (LSB) replacement and Enhanced Modified Signed Digit (EMSD) procedures. Particularly, the inserting limit of the proposed calculation is around 262,144 to 786,432 bits bigger than comparative calculations as the EMSD. Likewise, the combination of the EMSD and the LSB replacement calculations give greater security to privileged information, high payload, and get appropriate stego-image quality.

A new strategy for image steganography was proposed in [25]. In [25] and [2], the primary characters of the covert message are changed over to twofold bits, and afterward edge locales are distinguished. However, the randomization mounted is the principle trademark in the proposed calculation [25]. From the test results, it is reasonable that calculation is strong to insert the covert message information into RGB shading image, though edge pixels, irregularity, and variable mounting boundaries are utilized for security reasons against visual assaults and histogram-based assaults [2]. Also, image quality upgrades will be explored to work on the imperceptibility of the cover picture or image.

The execution of the LSB-based piece flipping approaches has been further investigated, and our proposed method concludes the work presented in [6]. The bit flipping approach hasn’t been used to hide images, although previous research has shown that it increases intangibility by about 9 dB in gray-scale images. In this investigation, the bit flipping approach is used to shade pictures by implanting messages with the most extreme restriction, and it appears that the bit flipping technique performs splendidly in shading pictures using the RGB model. This demonstrates how well the bit flipping algorithm under consideration performs when applied to both gray-scale and covert images.

Further details can be read in [22] for color image steganography that are, in fact, utilizing the multi-level encryption (MLE) and the gray-level modification (GLM) approaches. Prior to planting it to the grey levels of the cover image, the secret key and confidential Intel are encoded using MLE computation. The main benefits of the suggested work come from the employment of GLM, Secret Key, and MLE by the writers. The essential advantages of the proposed plan are chipped away at the nature of stego images, high intangibility, cost-feasibility, and further developed energy. Though, the research work adds and improves the security layers and also increases the direction of the cover steganography. In the Development of LSB Steganography (DLSB) method used the LSB based cover steganography for embedding the secret message and comparisons of the cover and secret bits [21]. The amount of pixels in the image is equivalent to the greatest number of bits that can be covered. The use of dynamic key is the main objectives of the proposed work which provide a better security. Though, it is not possible to detect this little change between original and proposed value by naked eye or human visual system.

However, the least difficult procedure among the spatial space strategies is the LSB replacement strategy where the
LSB of every pixel value is utilized to insert the information [3]. In the LSB replacement strategy, the covert message is encoded by turning around, trading, and round right moving with an arbitrary key or without a key [31]. The LSB advantages of pixel forces are changed with the message bits. The amount of pixels utilized for inserting information is equivalent to the number of bits in the message file. This value is put away in the last rows of the image in the same ways the message is inserted. In Table 2, the most relevant LSB based techniques and various image steganography methods in spatial domain are critically analyzed based on the basics evaluation criteria of the steganography which is shown above in Table 1.

**B. SUMMARY OF THE LITERATURE REVIEW**

In Table 2, different image steganography techniques in the spatial domain are critically investigated based on the basic criteria of steganography in detail. In summary of various steganographic procedures the significant kinds and order of steganography have been proposed in the literature during the most recent couple of years. We have basically broken down various image steganographic techniques which demonstrate that the graphical nature of the image is degraded when the secret information is expanded up to a possible utilizing LSB-based scheme.

Arguably, each technique has their pros and cons based on the image steganography using the LSB substitution technique. Because some technique has brought down payload boundary (payload boundary means that how many size of secret message we can embed) and some have broken down other criteria of steganography and also have vulnerabilities to different attack such as cropping, scaling, and tampering etc. The reliability between the basic criteria of image steganography is also required [15]. Suppose, as shown in Table 2, an existing method (given in S. No 1 – the Modified LSB substitution for RGB Images) has covered some evaluation criteria such as imperceptibility, and temper protection; but, has broken down other criteria like payload, computation, and robustness. Furthermore, enormous amounts of implanting techniques can give indication of change of the image by means of careful investigation of the reasonable properties of disorder or perceptibility analysis. However, a lot of cover steganography procedures are proposed, in the literature, till now.

Therefore, the selection of a particular technique depends on its efficiency. It tends to be seen in the literature that the LSB Substitution method with some measure of encryption is the better one among other image steganographic procedures in spatial area such as Pixel Value Differencing, Pixel Intensity Technique, Edge Based Detection, and Histogram shifting etc. Thus, to improve the limitations of the existing methods we still needs the reliability between various steganography evaluation criteria. The selection of an appropriate encrypted objects and the way of the embedding of secret message bits in cover object is still needed. However, the proposed work compared with some existing methods of the image steganography by using the basic evaluation criteria, Image Quality Assessment Metrics (IQAM) and different perspectives (details are given later in Section IV) to make it reliable and to achieve the greatest nature of stego images and a better and reliable steganographic procedure.

**III. THE PROPOSED MODEL**

In today’s advanced technological world, keeping the integrity, authenticity, security and confidentiality of the secret information over the internet is hot issues. Different techniques are proposed, but they do not fulfill the need of secret data due to the advancement of technologies. So new treats focus us to develop new methods. Therefore, steganography is the best method used today for sending and receiving using any communication channels through internet. Because, it hides the secret message in a particular manner such that no one can detect the hidden information. In this paper, we are having a novel and significantly improved steganographic approach which is used in the RGB color space. For the importance and motivation of the proposed algorithm, we tested the proposed method with different perspectives, and taking different and various image types (i.e Texture, Aerial, and gray scale images) and also tested using different and same sized of messages which are given below in result section in details.

**A. THE PROPOSED ALGORITHM**

For the proposed algorithm, the mathematical model and notations are as given below:

- Secret message is denoted by $SM$ with $SM_{i,j}$ defines the value location of the message
- $CI$ represent Cover image with $Ci_{i,j}$ which define the pixel value location
- $TI$ demonstrate the transform image with $TI_{i,j}$ demonstrate the value location of that image
- $FI$ denote the flipped image with value location of that image represent as a $FI_{i,j}$
- $SMdv$ represents the differing value of secret message
- $Rc, Gc, Bc$ represent the Red, Green and Blue channels of the Image
- $SM_{mg}$ represents the stego image and the location of the value is defining with $SM_{mg_{i,j}}$

For the entire proposed algorithm, the equations from 1 to 6 function named as alpha ($\alpha$), Beta($\beta$), Gamma ($\gamma$), theta($\theta$), Delta ($\delta$), Omega($\omega$) are used in the following manner:

$$FI = \alpha(TI)$$  \hspace{1cm} (1)
$$Rc, Gc, Bc = \beta(FI)$$ \hspace{1cm} (2)
$$SMdv = \gamma(SM, Rc)$$ \hspace{1cm} (3)
$$SMdv' = \omega(SMdv)$$ \hspace{1cm} (4)
$$Bc' = \delta(Bc)$$ \hspace{1cm} (5)
$$SM_{mg} = \theta(SMdv', Bc')$$ \hspace{1cm} (6)
The above six functions are used for the whole embedding and extracting algorithm of the proposed method. First we used $\hat{I}$ accepts flipped image and then $T_I$ transforms image. The $\beta$ divides the transformed image ($T_I$) into $R_c, G_c$, and $B_c$ channels and here the $R_c$ is used for calculating difference between secret message and $B_c$ channels for embedding the secret message. The third function $\gamma$ is used for calculating difference of $R_c$ channel and secret message $SM$ as ASCII code of a letter. For robustness, the proposed algorithm used MLEA (which gives us $SM_{dv}$) difference values is encrypted using the $\omega$ function. Now before jump to embedding the message a MATLAB function Magic Matrix is used for shuffling the $B_c$ (blue) channel using the function $\delta$ which return $B_c'$. And finally the $S_{img}$ is achieved using the last function $\theta$ using the proposed algorithm by the embedding encoded difference values $SM_{dv}$ in the shuffled $B_c'$ blue channel. Now to extract the hidden message from stego image the reverse process of the proposed method can be achieved using the following functions as same as embedding process.

$$CI = \alpha - 1(mg)$$

$$c, c, c = \beta - 1(TI)$$

$$c' = \delta - 1c$$

$$dv' = \theta - 1(Bc')$$

$$SM = \gamma - 1(SM_{dv}, c)$$

$$SM_{dv} = \omega - 1(SM_{dv}')$$

### TABLE 4. Comparisons of the proposed method with other related and state-of-the-art existing methods using the PSNR metric values.

| Name and Dimension | Secret message in KB’s | Cipher in | Md-LSB | Improved LSB for RGB | LSB Replacement through XOR | Mul-Stego for G-Scale | V-D using adjacent pixel LSB | Gl. Mod & MLE | Proposed method (NSLB-St) |
|-------------------|------------------------|-----------|--------|----------------------|---------------------------|----------------------|---------------------------|---------------|--------------------------|
| 512 x 512         |                        | RGB      | 4000   | 68.554               | 65.534                    | 65.787               | 78.764                    | 77.098        | 84.897                  |
| 6000              |                        | RGB      | 6000   | 65.987               | 66.876                    | 67.999               | 79.098                    | 79.090        | 81.098                  |
| 8000              |                        | RGB      | 8000   | 65.098               | 65.876                    | 67.090               | 79.078                    | 74.076        | 76.088                  |
| 10000             |                        | RGB      | 10000  | 55.098               | 56.098                    | 60.988               | 65.988                    | 71.0897       | 72.908                  |
| 12000             |                        | RGB      | 12000  | 67.098               | 66.096                    | 67.0898              | 65.0978                    | 67.977        | 69.099                  |
| 14000             |                        | RGB      | 14000  | 79.980               | 61.098                    | 62.099               | 63.098                    | 64.099        | 65.909                  |
| 16000             |                        | RGB      | 16000  | 80.343               | 81.098                    | 81.080               | 83.080                    | 84.909        | 83.999                  |
| Average           |                        | RGB      | 59.165 | 62.6653              | 64.0187                  | 64.0187              | 69.31497                   | 71.04839      | 73.42829                |
|                     |                        |          |        |                      |                           |                      |                           |               | 75.24729                |

### B. SHUFFLING THE BLUE CHANNEL USING MAGIC MATRIX (MM)

The Magic matrix is a Matlab function having very valuable properties. Suppose $a = magic(n)$ will return an $n \times n$ matrix with equal numbers of rows and columns constructed from 1 integer through $n^2$. In order to create a valid matrix, the $n$ order must be a scalar greater than 3. It doesn’t contain any repeated number and if we take the sum of all rows, columns and diagonal are same. To take benefit from the properties of magic matrix we can use to Shuffle the cover image pixels. More precisely, to clear the concept of magic matrix (MM) lets take a visualize example as shown in Figure 7. Suppose that the patterns or the concept in MM is visually examined with orders between 9 and 24 images. The resulting patterns of MM show us that it uses 3 different algorithms or procedures which totally depended on whether the value of mod($n$, 4) is 0, 2 or odd.

### C. THE MULTI LEVEL ENCRYPTION ALGORITHM

Before embedding the secret information into cover image MLEA embeds the secret information. To increase...
the security or robustness of the secret data MLEA applies various encoded activities on it. So, these valuable activities are used in proposed method. The steps and block diagram of the MLEA is given as follows:

- Taking XOR of all bits by 1.
- Taking 8 bits’ combination and replace the 1st four bits with the last four bits.
- For every 8 bits’ combination take the left circular shift.
- Finally, divide the whole array into two blocks and then taking the XOR on the bases of block one and block two in such as manner that if block \( i \equiv 1 \) then assume the XOR of block two \( i \) by 1.

To summarize the discussion, in the proposed method first we take a cover image; and then we flipped and transposed the selected cover image. After that, we convert it to the three channels, Red, Green, Blue. Then blue channel is used for embedding the secret message, then divided into four equals block and shuffled using Magic Matrix while red channel is used for calculating the differencing values between the red channel and secret message bits. Now the different values are then encoded using Multi-Level Encryption Algorithm (MLEA) to make the cipher. In the last, the encoded different values in a cyclical mode (two bits per block) are embed- ded into the blue channel which is divided into 4 equals shuffled blocks. After embedding the secret data into the blue channel then re-arrange the pixel of the sub- images of the blue channel then combining the RGB channel. After combining the RGB channel re-flip into its original form and get a stego image. Therefore, in proposed method, various terms like flipping, transpose, MLEA, Magic Matrix, and LSB concepts are used for embedding secret message within the image.

D. THE EMBEDDING ALGORITHM

The given steps in Algorithm 1 elaborate the whole embedding process:

E. THE EXTRACTION ALGORITHM

The Extraction algorithm is explained using a step-by-step procedure as given below in Algorithm 2. This should be noted that the Extraction algorithm is the reverse of the embedding algorithm. The given steps elaborate the encrypted progression, respectively.

IV. ANALYSIS OF RESULTS AND EXPERIMENTAL ENVIRONMENT

The Proposed technique experimentally assessed with the given different perspectives based on data sets of bench- mark RGB (aerial, texture, and gray scale) images downloaded from University of Southern California-Signal and Image Processing Institute (USC-SIPI) database website for evaluating the proposed method with existing methods [3], [34]. We took different images named; image1-12 shown in the Figure 9. For implementation MATLAB R2014a are used for proposed method, Modified LSB substitution for RGB Images [2], Improved LSB for RGB images [13], LSB Replacement through XOR Substitution [6], Multi Stego for gray scale images [26], Value differencing using adjacent pixel and LSB substitution technique [20], LSB bit flipping method [6], GL Modification and MLE [22], LSB hybrid hiding model method [17] etc. Therefore, many explorations and experimentation was directed as to fully survey and investigate the usefulness of the suggested technique. This method is experimented by 165 smooth and edgy image of different dimensions and sizes. The Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Normalized Cross Correla- tion (NCC), Histogram Analysis (HA), Structural Similarity Index (SSIM), and Root Mean Square Error (RMSE) are some of the image assessment metrics which are most widely utilized to assess various techniques similar to the proposed approach. For showing the motivation and importance of the proposed method also do Histogram Analysis (HA) of some cover an stego images.

The entire quantitative evaluation of this research work is faltering strategized by the given viewpoints (Perspectives):
Algorithm 1 The Embedding Process

**Inputs:** A cover image

**Outputs:** A stego image

**Step-1:** Take a cover image, flip and then transform the original image.

**Step-2:** Convert the flipped image into three channels which are red, green, and blue (RGB).

**Step-3:** To hide the secret message into blue channel and the red channel is used for deciding differentiation among messages and the intensity of the pixel.

**Step-4:** The blue channel is then divided into four same blocks and then every block is adjusted using a notable matrix which is Magic (a particular function of the Matlab that return a matrix having no rehashed numbers and its summations of every column, row, and diagonals are the same). Then again, the confidential information (ASCII codes) is deducted from the relating pixel values of the red channel.

**Step-5:** Now different values are then encoded using the proposed Multi-Level Encryption Algorithm (MLEA). In the last, the encoded different values in a cyclical mode (two bits per block) are embedded into the blue channel which is shuffled in step 4.

**Step-6:** After embedding the secret data into the blue channel, then, we re-arrange the pixel of the sub-images of the blue channel then combining the RGB channel. After combining the RGB channel re-flip into its original form and get a stego image.

**Return** a stego image

Algorithm 2 The Extraction Algorithm

**Inputs:** A stego image

**Outputs:** Red channel pixel values

**Step-1:** First taking the stego image, then, flip and transform the image so that it can be separated into red, green, and blue (RGB) channel.

**Step-2:** The blue channel is partitioned and rearranged using magic matrix which is divided into four equivalent blocks in encrypted process.

**Step-3:** To the end of embedded information; taking the LSB of two pixels is removed from each block in a cyclic way.

**Step-4:** The decoded message is then decrypted using the proposed MLEA technique (for increasing its security, different encryption, replacing, XOR, and combination measures are used) and a while later every eight-bit combination is changed over into decimal.

**Step-5:** In the end, different values between the secret message extracted values and resultant red channel pixel values are calculated.

**Return** red channel pixel values

- Concealing various measures of information in different images of similar dimensions.
- Encoding same size of information in various images of a similar size.
- Encrypting similar amount of message in the same image of diverse sizes.
- Encoding different size (6kb, 8kb, 10kb, 14kb, 16kb) of data in the different size, dimensions’, and different Gray-scale, Texture and Aerial images.

In perspective 1, concealing 5 distinct sizes of a text (for example 4KB, 6KB, 8KB, 10KB, 16KB) in different images of the same dimension (256 × 256). Furthermore, in perspective 2, a text of 12 Kilobytes is inserted in different color images having size 256 × 256. This investigation is led on 100 pictures. This investigation is led on four or five standards RGB Image. Comparable images of perspective 1 and 3 with different resolutions of (128 × 128, 256 × 256, 512 × 512, and 1024 × 1024) are used and the size of inserting secret text will be 8 Kilobytes. In Perspective 4 the data embedded in different size, dimensions, and different format of images.

Now for the consisting of the suggested model and technique with other associated and existing methods the datasets of different images are used to analyze the edge of the suggested technique which shown in below Figure 9.

**A. PERSPECTIVE 1: DIFFERENT SIZES OF MESSAGE ON DIFFERENT IMAGES OF SAME DIMENSIONS**

Table 3 and Table 4 elaborate the perspective 1 which is the different sizes of information embedded in same dimension of different images. Comparisons based on the PSNR proves the edge of the suggested approach over the state-of-the-art and other existing approaches. Table 1 and 2 elaborate
the perspective 1 which is the different sizes of information embedded in same dimension of different images. The proposed technique and the reference techniques both use a different size of secret message on different and same dimension images in analysis fashion. For a fair comparison, first we collected the resulted percent values (PSNR) of the existing methods from the papers and verified. That resulted values of the reference methods is on which type of inputs (size of message and selection of cover image). Then we took for proposed method; different size of secret messages i.e 4, 6, 8, 10, 14, 16 KB’s and tested on different and same dimensions of the image. First we test by taking same dimension images (512 × 512) and then tested by 4 kb and check the result in terms of PSNR which are dominant as compared with existing methods. After apply same procedures for different size of secret message on 512 × 512 image the results outperforms. The reference methods used only exact size of message, testing the whole method either 10 kb message size and same images. The Means testing is based on only on perspective but the proposed method critically tested on different perspectives.

Comparisons based on the PSNR proves the edge of the proposed method with other existing methods. However, in embedding algorithm of the proposed method, embedding
algorithm used the embedding process bit per pixel (BPP) in a manner; after calculating the differencing values between the red channel and secret data then converting into bits of 1D array and applied MLEA to make cipher. After that, selecting 8 bits from 1D array and set the control and check for every 1st 2nd bits into 1st block of the Blue channel (which are divided into 4 blocks), every 3rd and 4th bits into 2nd block, every 5th and 6th bits into 3rd block, and every 7th and 8th bits into 4th block of the blue channel. After that if all bits are embedded into 4 divided blocks of the blue channel respectively, then control goes to re-arrange the pixels of the dividend block of the blue channel and combine red, green, and blue channels and then proceed for the next step to make the stego image. So 4 equals divided blocks of the blue channel is used for every 1st two bits into block 1, and every 3rd and 4th bits into 2nd block, respectively. The whole process of the embedding are presents in embedding and extraction algorithm section above.

B. PERSPECTIVE 2: ENCODING SAME SIZE OF INFORMATION IN VARIOUS IMAGES OF SIMILAR SIZES

Table 5 elaborates the perspective 2 while taking same size of secret data (16 kb’s) and, when embedded in different images of same dimensions (512 × 512). The obtained results are shown in Figure 10.

C. PERSPECTIVE 3: ENCRYPTING SIMILAR AMOUNT OF MESSAGE IN THE SAME IMAGE OF DIVERSE SIZES

Table 6 and Table 7 prove the dominance of the suggested approach over the current state-of-the-art techniques based on perspective 3 which is the same amount of information while embedded within different images of different dimensions from Image [1], [2], [3], [4], [5], [6]. The same scenario is used over more than 150 different images of different dimensions that prove the edge of the proposed method.

D. PERSPECTIVE 4: ENCODING DIFFERENT SIZES (6kb, 8kb, 10kb, 14kb, 16kb) OF DATA IN DIFFERENT SIZES, DIMENSIONS, AND DIFFERENT IMAGES I.e. GRAY-SCALE, TEXTURE, AND AERIAL

In perspective 4, many different Gray-scale images are used for embedding different size of secret message that indicates the importance of the suggested model and approach which are shown in Table 8. Figure 11 shows datasets of different gray-scale images. Now in perspective 4 the suggested approach is also analyzed founded on texture images which is given below.

In Figure 12, a dataset of many texture images is used for analyzing the proposed method based on the PSNR metric and the obtained outcomes are shown in Table 9. The evaluation and assessment outcome proves the edge of the suggested approach with a high PSNR metric values. In next discussion, we are analyzing the proposed method using aerial images. To do so, we are taking a data set of some aerial images as shown in Figure 13.

In Figure 13, a dataset of many Aerial images is used for analyzing the importance and edge of the proposed method.
| Name and image | Size of Message to be embedded | Md. LSB RGB | Improved LSB for RGB | LSB Replacement through XOR | Mul. Stego for G-Scale | VD using adjacent pixel LSB | GL Mod & MLE | Proposed method (NLST-S) |
|----------------|--------------------------------|--------------|----------------------|----------------------------|------------------------|-----------------------------|--------------|--------------------------|
| Image [1]      | 16 KB’s                       | 128 × 128    | 77.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 89.243                  |
|                |                                | 256 × 256    | 77.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 83.033                  |
|                |                                | 512 × 512    | 77.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 78.223                  |
|                |                                | 1024 × 1024  | 77.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 77.143                  |
|                | Average                        | 77.934       | 66.787               | 69.764                     | 67.098                 | 66.897                      | 66.897       | 80.9105                |
| Image [2]      | 16 KB’s                       | 128 × 128    | 68.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 77.223                  |
|                |                                | 256 × 256    | 68.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 89.113                  |
|                |                                | 512 × 512    | 68.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 87.544                  |
|                |                                | 1024 × 1024  | 68.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 89.043                  |
|                | Average                        | 68.934       | 66.787               | 69.764                     | 67.098                 | 66.897                      | 66.897       | 86.481                  |
| Image [3]      | 16 KB’s                       | 128 × 128    | 75.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 78.022                  |
|                |                                | 256 × 256    | 75.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 80.042                  |
|                |                                | 512 × 512    | 75.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 85.043                  |
|                |                                | 1024 × 1024  | 75.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 89.013                  |
|                | Average                        | 75.934       | 66.787               | 69.764                     | 67.098                 | 66.897                      | 66.897       | 86.030                  |
| Image [4]      | 16 KB’s                       | 128 × 128    | 75.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 80.223                  |
|                |                                | 256 × 256    | 75.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 80.223                  |
|                |                                | 512 × 512    | 75.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 80.223                  |
|                |                                | 1024 × 1024  | 75.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 80.223                  |
|                | Average                        | 75.934       | 66.787               | 69.764                     | 67.098                 | 66.897                      | 66.897       | 80.223                  |
| Image [5]      | 16 KB’s                       | 128 × 128    | 75.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 80.223                  |
|                |                                | 256 × 256    | 75.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 80.223                  |
|                |                                | 512 × 512    | 75.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 80.223                  |
|                |                                | 1024 × 1024  | 75.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 80.223                  |
|                | Average                        | 75.934       | 66.787               | 69.764                     | 67.098                 | 66.897                      | 66.897       | 80.223                  |
| Image [6]      | 16 KB’s                       | 128 × 128    | 75.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 80.223                  |
|                |                                | 256 × 256    | 75.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 80.223                  |
|                |                                | 512 × 512    | 75.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 80.223                  |
|                |                                | 1024 × 1024  | 75.934               | 66.787                     | 69.764                 | 67.098                      | 66.897       | 80.223                  |
|                | Average                        | 75.934       | 66.787               | 69.764                     | 67.098                 | 66.897                      | 66.897       | 80.223                  |

Average of 150 images of different dimensions 75.934 66.787 69.764 67.098 66.897 80.223

| Name and image | Image | Dimension of the image | PSNR value of the Proposed Method |
|----------------|-------|------------------------|-----------------------------------|
| Image [1]      |       | 128 × 128 256 × 256 512 × 512 1024 × 1024 | 89.243 83.033 78.223 73.143 |
| Image [2]      |       | 128 × 128 256 × 256 512 × 512 1024 × 1024 | 80.022 79.043 75.043 70.013 |
| Image [3]      |       | 128 × 128 256 × 256 512 × 512 1024 × 1024 | 87.033 85.941 80.412 77.643 |
| Image [4]      |       | 128 × 128 256 × 256 512 × 512 1024 × 1024 | 87.033 85.941 80.412 77.643 |
| Image [5]      |       | 128 × 128 256 × 256 512 × 512 1024 × 1024 | 87.033 85.941 80.412 77.643 |
| Image [6]      |       | 128 × 128 256 × 256 512 × 512 1024 × 1024 | 87.033 85.941 80.412 77.643 |
which is based on the PSNR metric and the attained results are shown in Table 10. The experimental results prove the improvement of the proposed method with a high PSNR metric values, which are displayed in Table 10.

The suggested approach is critically analyzed based on different perspectives which is discussed one by one in details. In perspective 4, the proposed method is critically analyzed on three different types of images such as Gray-scale, texture,
and aerial images. However, the experimental results prove the improvement and edge of the proposed method which is verified through high PSNR values. In addition, the results also prove the strengthening of the proposed method. Therefore, based on image quality assessment metrics (such as MSE, RMSE, SSIM, NCC, Histogram analysis, explanation is given in Table 10 and Table 11) the experimental influences of the proposed method according to the different perspectives (1, 2, 3, 4 as discussed above) are shown in Tables 12 – 15, correspondingly. Based on different

### Table 9. Different Texture Images are used for Embedding Different Sizes of the Secret Message.

| Name and Image | Image | Secret Message size | PSNR Value of the Proposed Method |
|----------------|-------|---------------------|-----------------------------------|
| TexImg-[1]      | [Image 1] | 6KB                 | 79.209                            |
|                 |        | 8KB                 | 77.033                            |
|                 |        | 10KB                | 73.223                            |
|                 |        | 14KB                | 71.199                            |
|                 |        | 16KB                | 69.143                            |
| TexImg-[2]      | [Image 2] | 6KB                 | 89.223                            |
|                 |        | 8KB                 | 87.113                            |
|                 |        | 10KB                | 86.544                            |
|                 |        | 14KB                | 80.043                            |
|                 |        | 16KB                | 76.908                            |
| TexImg-[3]      | [Image 3] | 6KB                 | 80.112                            |
|                 |        | 8KB                 | 75.042                            |
|                 |        | 10KB                | 72.043                            |
|                 |        | 14KB                | 70.013                            |
|                 |        | 16KB                | 69.098                            |
| TexImg-[4]      | [Image 4] | 6KB                 | 89.033                            |
|                 |        | 8KB                 | 80.961                            |
|                 |        | 10KB                | 79.812                            |
|                 |        | 14KB                | 79.643                            |
|                 |        | 16KB                | 77.890                            |
| TexImg-[6]      | [Image 6] | 6KB                 | 90.314                            |
|                 |        | 8KB                 | 84.941                            |
|                 |        | 10KB                | 80.123                            |
|                 |        | 14KB                | 79.85                             |
|                 |        | 16KB                | 77.678                            |
| TexImg-[9]      | [Image 9] | 6KB                 | 88.033                            |
|                 |        | 8KB                 | 85.941                            |
|                 |        | 10KB                | 82.412                            |
|                 |        | 14KB                | 79.622                            |
|                 |        | 16KB                | 77.0875                           |
perspectives using quality assessment metrics the investigatory and assessment findings and outcomes indicate the importance, dominance, and significance of the suggested method.

In next discussion, the proposed method is critically analyzed based on histogram analysis for perspective 4 such as RGB, Gray-scale, Texture, and Aerial Images which are given below in Figures 14 – 17, respectively. In summary, the whole results and experimental discussion show the superiority of the proposed method. Moreover, the proposed method is used for the LSB substitution, MLEA, Magic Matrix, and some flipping etc., concepts for embedding the secret message within the image. For the motivation and importance of the proposed method, the approach was critically analyzed with...
TABLE 11. PSNR metric values for the proposed method according to perspective 1.

| Size of secret message in KB's | Name and Dimension 512 x 512 |
|-------------------------------|--------------------------------|
| Image [1] | Image [2] | Image [3] | Image [4] | Image [5] | Image [6] | Image [7] | Image [8] | Image [9] |
| 4 | 90.243 | 94.223 | 86.022 | 88.033 | 87.033 | 86.033 | 87.033 | 87.033 | 87.033 |
| 6 | 84.033 | 90.113 | 79.042 | 84.941 | 84.941 | 85.941 | 85.941 | 85.941 | 85.941 |
| 8 | 79.223 | 88.043 | 75.043 | 80.412 | 80.412 | 81.412 | 81.412 | 81.412 | 81.412 |
| 10 | 73.143 | 80.043 | 70.013 | 76.643 | 77.643 | 76.643 | 77.643 | 77.643 | 77.643 |
| 12 | 70.023 | 79.323 | 67.041 | 75.143 | 87.033 | 86.033 | 87.033 | 87.033 | 87.033 |
| 14 | 66.023 | 76.023 | 63.013 | 70.043 | 84.941 | 85.941 | 84.941 | 84.941 | 84.941 |

Average of 165 images of same dimension of the proposed method: 81.865

PSNR: Peak Signal to Noise Ratio is a basic parameter for determining the quality of the both stego and cover images.
If the value of PSNR is greater than 30dB consider as a quality image.

$$PSNR = 10 \log_{10} \left( \frac{C_{max}^2}{MSE} \right)$$

TABLE 12. IQAM results and analysis of the proposed method according to perspective 2.

| IQAM | Name, Dimension, and Secret message size: 512 x 512 and 16 KB |
|------|------------------------------------------------------------|
|     | Image [1] | Image [2] | Image [3] | Image [4] | Image [5] | Image [6] | Image [7] | Image [8] | Image [9] |
| RMSE | 0.025 | 0.021 | 0.125 | 0.022 | 0.012 | 0.022 | 0.112 | 0.012 | 0.023 |
| MSE  | 0.021 | 0.111 | 0.021 | 0.111 | 0.122 | 0.022 | 0.011 | 0.111 | 0.001 |
| NCC  | 0.989 | 0.999 | 0.999 | 0.999 | 0.988 | 0.999 | 0.989 | 0.999 | 0.999 |
| SSIM | 1 | 0.999 | 0.999 | 0.999 | 1 | 0.999 | 1 | 1 | 1 |

Average of 165 images of same dimension of the proposed method: RMSE=0.086, MSE=0.057, NCC=0.985, SSIM=0.999

The quality assessment metrics:

- Peak Signal to Noise Ratio (PSNR) is the basic parameter for determining the quality of both stego and cover images.
- If the PSNR value is greater than 30dB then the image is considered as a quality image. The given formula used for finding PSNR values.
- Mean Square Error (MSE) is the contrast between cover and stego images and both are said to be equal if the MSE is equal to zero.
- So MSE should be least possible to obtain a quality and robust image.
- Root Mean Square Error (RMSE) is a peculiar disparity between cover and stego images.
- It gives an improved a little bit inspection error in metric utilized as needed as a small numerical value.
- Another IQAM which is used to examine how both cover and stego media is identical is Normalized Cross Correlation (NCC).
- Both cover and stego images are said to be same if the value of the NCC is equal to 1, whereas if this value becomes 0, then it shows the absolute difference between both images.
- Another important quality metric is used to decide the quality of both cover and stego images is Structural Similarity Index (SSIM).
- It is used in three parts and these parts decide the quality of the image if the value equals to 1.
- If the value of all segments is less than 1 then it shows the difference between both images.
- The three parts of SSIM are Luminance, Contrast, and Structural. Formulas for each is given.

$$MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (S_{xy} - C_{xy})^2$$

$$RMSE = \sqrt{\frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (S_{xy} - C_{xy})^2}$$

$$NCC = \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} (S(x, y) - \mu_S)(C(x, y) - \mu_C)}{\sqrt{\sum_{x=1}^{M} \sum_{y=1}^{N} (S(x, y) - \mu_S)^2 \sum_{x=1}^{M} \sum_{y=1}^{N} (C(x, y) - \mu_C)^2}}$$

$$SSIM(X, Y) = \frac{\left(2\mu_X\mu_Y + C_1\right)\left(2\sigma_{xy} + C_2\right)}{\left(\mu_X^2 + \mu_Y^2 + C_1\right)\left(\sigma_X^2 + \sigma_Y^2 + C_2\right)}$$

Comparisons of Aerial Cover and Stego Images Histograms

**FIGURE 14. Aerial, Cover, and Stego Images and their Histograms.**
### TABLE 13. IQAM results and analysis of the proposed method according to perspective 3.

| Name and image | Size of Message to be embedded | Different dimension images | MSE   | RMSE  | SSIM  | NCC  |
|----------------|--------------------------------|---------------------------|-------|-------|-------|------|
| Image [1]      | 16 KB’s                        | 128 x 128                 | 0.111 | 0.225 | 1     | 1    |
|                |                                 | 256 x 256                 | 0     | 0     | 1     | 1    |
|                |                                 | 512 x 512                 | 0.111 | 0.212 | 0.999 | 0.999|
|                |                                 | 1024 x 1024               | 0.041 | 0.43  | 1     | 1    |
| Average        |                                |                           | 0.121 | 0.115 | 1     | 0.999|
| Image [2]      | 16 KB’s                        | 128 x 128                 | 0.112 | 0.025 | 1     | 0.999|
|                |                                 | 256 x 256                 | 0.001 | 0.021 | 0.999 | 0.999|
|                |                                 | 512 x 512                 | 0.012 | 0.032 | 0.999 | 0.999|
|                |                                 | 1024 x 1024               | 0.999 | 0.999 | 1     | 1    |
| Average        |                                |                           | 0.121 | 0.025 | 1     | 0.999|
| Image [3]      | 16 KB’s                        | 128 x 128                 | 0.011 | 0.025 | 1     | 0.999|
|                |                                 | 256 x 256                 | 0.112 | 0.021 | 1     | 0.999|
|                |                                 | 512 x 512                 | 0.011 | 0.012 | 0.999 | 0.999|
|                |                                 | 1024 x 1024               | 0.009 | 0.001 | 1     | 1    |
| Average        |                                |                           | 0.011 | 0.021 | 1     | 0.999|
| Image [4]      | 16 KB’s                        | 128 x 128                 | 0.021 | 0.001 | 0.999 | 0.999|
|                |                                 | 256 x 256                 | 0.011 | 0.001 | 0.999 | 0.999|
|                |                                 | 512 x 512                 | 0.011 | 0.012 | 1     | 1    |
|                |                                 | 1024 x 1024               | 0.999 | 0.999 | 1     | 1    |
| Average        |                                |                           | 0.021 | 0.001 | 0.999 | 0.999|
| Image [5]      | 16 KB’s                        | 128 x 128                 | 0     | 0     | 1     | 0.999|
|                |                                 | 256 x 256                 | 0     | 0.100 | 1     | 0.999|
| Average        |                                |                           | 0     | 0.100 | 1     | 1    |

### TABLE 14. IQAM results and analysis of the proposed method according to perspective 3 for Texture Images.

| Name and image | Size of Message to be embedded | Different dimension images | MSE   | RMSE  | SSIM  | NCC  |
|----------------|--------------------------------|---------------------------|-------|-------|-------|------|
| Image [1]      | 16 KB’s                        | 128 x 128                 | 0.111 | 0.223 | 0.999 | 0.999|
|                |                                 | 256 x 256                 | 0     | 0     | 1     | 1    |
|                |                                 | 512 x 512                 | 0.111 | 0.212 | 1     | 1    |
| Average        |                                |                           | 0.121 | 0.115 | 1     | 0.999|
| Image [2]      | 16 KB’s                        | 128 x 128                 | 0.011 | 0.025 | 0.999 | 0.999|
|                |                                 | 256 x 256                 | 0.011 | 0.021 | 0.999 | 0.999|
|                |                                 | 512 x 512                 | 0.011 | 0.012 | 0.999 | 0.999|
|                |                                 | 1024 x 1024               | 0.009 | 0.001 | 0.999 | 0.999|
| Average        |                                |                           | 0.021 | 0.025 | 1     | 0.999|
| Image [3]      | 16 KB’s                        | 128 x 128                 | 0.011 | 0.021 | 0.999 | 0.999|
|                |                                 | 256 x 256                 | 0.011 | 0.012 | 0.999 | 0.999|
|                |                                 | 512 x 512                 | 0.011 | 0.011 | 0.999 | 0.999|
|                |                                 | 1024 x 1024               | 0.002 | 0.003 | 0.999 | 0.999|
| Average        |                                |                           | 0.021 | 0.025 | 1     | 0.999|

### TABLE 15. IQAM results and analysis of the proposed method according to perspective 3 for Aerial Images.

| Name and image | Size of Message to be embedded | Different dimension images | MSE   | RMSE  | SSIM  | NCC  |
|----------------|--------------------------------|---------------------------|-------|-------|-------|------|
| Image [1]      | 16 KB’s                        | 128 x 128                 | 0.111 | 0.223 | 0.999 | 0.999|
|                |                                 | 256 x 256                 | 0     | 0     | 1     | 1    |
|                |                                 | 512 x 512                 | 0.111 | 0.212 | 1     | 1    |
| Average        |                                |                           | 0.121 | 0.115 | 1     | 0.999|
| Image [2]      | 16 KB’s                        | 128 x 128                 | 0.011 | 0.025 | 0.999 | 0.999|
|                |                                 | 256 x 256                 | 0.011 | 0.021 | 0.999 | 0.999|
|                |                                 | 512 x 512                 | 0.011 | 0.012 | 0.999 | 0.999|
|                |                                 | 1024 x 1024               | 0.002 | 0.003 | 0.999 | 0.999|
| Average        |                                |                           | 0.021 | 0.025 | 1     | 0.999|
| Image [3]      | 16 KB’s                        | 128 x 128                 | 0.011 | 0.021 | 0.999 | 0.999|
|                |                                 | 256 x 256                 | 0.011 | 0.012 | 0.999 | 0.999|
|                |                                 | 512 x 512                 | 0.011 | 0.011 | 0.999 | 0.999|
| Average        |                                |                           | 0.021 | 0.021 | 0.999 | 0.999|

Average of 150 images of different dimensions

0.001 0.000 1 0.999
different perspectives by selecting either: (i) different dimension’s images with same size message; or (ii) either different size of messages with same dimension of the same image in terms of payload, imperceptibility, robustness etc. In addition, the proposed method also used different datasets of different types images such as texture, gray-scale, and aerial images for showing the dominance of the research work. The proposed method also used different quality assessment metrics for

| Name of image | Size of Message to be embedded | Different dimension images | MSE | RMSE | SSIM | NCC |
|---------------|--------------------------------|----------------------------|-----|------|------|-----|
| Image [1]     | 16 KB’s                        | 128 x 128                  | 0   | 0    | 1    | 1   |
|               |                                | 256 x 256                  | 0.011 | 0.010 | 0.999 | 0.999 |
|               |                                | 512 x 512                  | 0.021 | 0.001 | 1.000 | 1    |
|               |                                | 1024 x 1024                | 0    | 0    | 0    | 1   |
| Image [2]     | 16 KB’s                        | 128 x 128                  | 0.001 | 0.011 | 0.999 | 0.999 |
|               |                                | 256 x 256                  | 0.021 | 0.11  | 1.000 | 1    |
|               |                                | 512 x 512                  | 0    | 0    | 0.999 | 1    |
|               |                                | 1024 x 1024                | 0.001 | 0    | 0.999 | 1    |
| Image [3]     | 16 KB’s                        | 128 x 128                  | 0.001 | 0.011 | 0.999 | 0.999 |
|               |                                | 256 x 256                  | 0    | 0    | 1    | 1   |
|               |                                | 512 x 512                  | 0    | 0    | 0.999 | 1    |
|               |                                | 1024 x 1024                | 0.001 | 0    | 0.999 | 1    |
| Average of 150 images of different dimensions | | | 0.001 | 0.011 | 0.999 | 0.999 |

**FIGURE 15.** Texture, Cover, and Stego Images and their Histograms.

**FIGURE 16.** Gray-scale, Cover, and Stego Images and their Histograms.
V. CONCLUSION AND FUTURE WORK

The Novel Least Significant Bit Technique (NLSBT) is a novel, enhanced, and improved algorithm that gives a superior security using the Magic Matrix and MLEA and, furthermore, expels the reiteration of the most normal letters. As, the proposed method is better than other approaches which was experimentally assessed by different perspectives and the results prove the importance and significance of the suggested technique. In fact, the suggested approach allows for some morally conscious people to safely negotiate the internal actions. This procedure gives some exceptionally helpful and commercially significant capacities in this advanced era. In this procedure, to insert a secret message in a file, responsibility for property can later be attested and/or to guarantee the reliability of the element. It is similarly relevant to private correspondence and confidential information storing,
assurance of information alteration, access control framework for advanced digital content distribution, and media data set frameworks. The proposed method also gives us an expected ability to conceal the presence of private information, and therefore hardness of identifying the secret message and information.

The uses of steganography is that it clearly needs to be used to send secret messages to an interlocutor, or co-schemer. It can also be used to move delicate information from sender to receiver to such an extent that the exchange of the information is obscure. Furthermore, the method can also be used in network topologies and related scenarios. This is generally helpful for the mysterious messages of botnets and different frameworks under a software engineer’s impact. Because of some procedural packets being essentially exceptionally normal, it could likewise be utilized in more dark and to the start and endpoint of information, and regularly undetected. Finally, it could have the option to withstand more noteworthy everyday hardship. In the future, we will consider these issues and will implement the suggested method in these areas. We will also use other methods to improve the applicability of the proposed method. We also intend to develop some Machine Learning (ML, unsupervised learning) and deep learning architectures for selecting appropriate message size for suitable image types.

ACKNOWLEDGMENT
The implementation code of the proposed method will be provided for a research purpose if requested from the principal author through email.

REFERENCES
[1] U. A. 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. 7, no. 3, pp. 24–31, 2021. [Online]. Available: http://www.mecs-press.org/jmsc/jmsc-v7-n3/JMSC-V7-N3-3.pdf, doi: 10.5815/jmsc.2021.03.03.
[2] L. Alnazzazy, “Secure RGB image steganography based on modified LSB substitution,” Int. J. Embedded Syst., vol. 12, no. 4, pp. 453–457, 2020.
[3] F. Q. A. Alyousuf, R. Din, and A. J. Qasim, “Analysis review on spatial and transform domain technique in digital steganography,” Bull. Electr. Eng. Inform., vol. 9, no. 2, pp. 573–581, Apr. 2020.
[4] R. J. Anderson and F. A. P. Petcoulas, “On the limits of steganography,” IEEE J. Sel. Areas Commun., vol. 16, no. 4, pp. 474–481, May 1998.
[5] A. S. Ansari, M. S. Mohammadi, and M. T. Parvez, “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.
[6] E. Z. Astutri, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and M. K. Sarker, “LSB-based bit flipping methods for color image steganography,” J. Phys. Conf. Ser., vol. 1501, no. 1, Mar. 2020, Art. no. 012019.
[7] M. Bachrach and F. Y. Shih, “Survey of image steganography and steganalysis,” in Multimedia Security, 1st ed., F. Y. Shih, Ed. CRC Press, 2017, pp. 201–214, doi: 10.1201/b16297-11.
[8] M. M. Bartere and H. R. Deshmukh, “Study of data hiding mechanism using virtual key replacement method,” in Proc. Int. Conf. Inventive Comput. Inform. (ICICI), Nov. 2017, pp. 1006–1010.
[9] R. Chandramouli and N. Memon, “Analysis of LSB based image steganography techniques,” in Proc. Int. Conf. Image Process., vol. 3, 2001, pp. 1019–1022.
[10] X. Chen, H. Che, M.-F. Leung, and Y. Wang, “An improved superpixel-based fuzzy C-means method for complex picture segmentation tasks,” in Proc. 14th Int. Conf. Adv. Comput. Intell. (ICACI), Jul. 2022, pp. 231–238.
S. Rahman et al.: Novel Steganography Technique for Digital Images Using the LSB Substitution Method

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 Information 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 was born in Mardan, Khyber Pakhtunkhwa, Pakistan. He received the M.Sc. degree from the University of Peshawar, Pakistan, in 2005, the M.Phil. degree from HITEC University, 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 was with the teaching profession at various national (HITEC Taxila, Gandahara Institute of Technology Peshawar, and Professional College of Commerce Peshawar) and foreign institutions (PSS Sana’a Pakistan Embassy Yemen, UTM Johor Malaysia), from 2008 to 2017. He has been working as an Assistant Professor and the Director ORIC of the Qurtuba University of Science and IT, Peshawar, Pakistan, since September 2017. He has published in reputed computer science journal articles, book chapters, and conference proceedings, and he is also a reviewer of different research journals. Total 19 of his M.S. students are graduated and he is also 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 also an Assistant Editor of HEC Category Y Science Journal The ScienceTech.

HABIB ULLAH KHAN received the Ph.D. degree in management information system area from Leeds Beckett University, U.K. He is currently working as a Professor of information systems with the Department of Accounting and Information Systems, College of Business and Economics, Qatar University. Academic experience-wise, he was associated with many leading universities of Gulf, USA, and Europe. Overall he has more than 21 years of working and research experience in different multinational companies (on different managerial positions), and reputed educational institutions in U.K., USA, Oman, United Arab Emirates, Saudi Arabia, and Qatar. During his past experience, he was an excellent team player and leader; his diversified experience helped him to manage multicultural students and the workforce in educational institutions. He has a strong skill set in managing undergraduate and graduate-level teaching of MIS and general management courses at the university level. The ability to analyze complex management procedures and extensive knowledge in information systems helped him to meet the challenge of remaining current with new and developing technology, and its applications in the management functions. He successfully demonstrated his skills in information management, client relations, training, and communication in a high-pressure environment with a successful management experience in the Gulf Region.

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 an Active Researcher. He is the author of several international publications. 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 Larki Marwat, Pakistan. 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. His research interests include cloud computing, mobile edge clouds, the Internet of Things (IoT), performance, energy efficiency, algorithms, and resource management.

MUHAMMAD ZAKARYA (Senior Member, IEEE) received the Ph.D. degree in computer science from the University of Surrey, Guildford, U.K. He is currently a Lecturer with the Department of Computer Science, Abdul Wali Khan University Mardan (AWKUM), Pakistan. He is the Program Director of the iFuture: a leading research group at AWKUM which has research collaboration with the CLOUDS Laboratory, The University of Melbourne, Australia; and the IoT Laboratory, Cardiff University, U.K. 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. His research interests include cloud computing, mobile edge clouds, the Internet of Things (IoT), performance, energy efficiency, algorithms, and resource management. 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 of Cloud Computing (Springer), and Cluster Computing (Springer). He is also a Guest Editor of Cluster Computing (Springer). He has been listed in the world’s top 2% scientists list for 2020 and 2021.