Hiding Images in the Spatial Domain

Sahera A. S. Almola
sahera.sead@uobasrah.edu.iq
College of Computer Science and Information Technology, University of Basra, Iraq.

Keywords: Image; Steganography; Security; Hiding; LSB; MSB; Spatial Domain; Embedded Data.

Received: June 19, 2022

Currently, information hiding has become an effective technique and has increased interest due to the rapid growth of Internet use. Many techniques can hide and transmit private information. The science of hiding information within the carrier's body ensures secure communication over the Internet so that it can only be recognized and detected by the sender and recipient. Thus, we can use many forms of a carrier, such as images, video, protocol, and audio. However, digital images are most commonly used because of their frequency on the Internet. There are many techniques for hiding information, each with advantages and disadvantages. In this study, we reviewed the techniques used to investigate the term "hiding" by reviewing and collecting various studies related to this field published between 2015 and 2021. This study assessed several ways of addressing this problem. Four measures - image quality, message capacity, and security – were used to assess the additional computational complexity of each method. Finally, the results presented and summarized as performance, security, and hidden image quality are essential for evaluating the approach.

Povzetek: Pregledni članek opisuje metode skrivanja informacij v slikah, objavljene med leti 2015 in 2021.

1 Introduction

The Internet revolution provides easy digital connectivity while also becoming a challenge to secure available web information. To process information security, many methods have been proposed in the area of security systems [1]. Many secure paths like the Internet or phone to transmit and share Information are unsafe in specific conditions and levels. Two techniques can be used for sharing Information in a hidden way: encryption and Information hiding. The message is changed and encrypted using an encryption key known only to the sender and the recipient. Access to a message is more accessible by using the encryption key. Sending a communication using encryption may raise suspicions of the attacker, allowing the message to intercept, attacked, or deciphered. Hiding information techniques have been developed to fix deficiencies in encryption techniques. Steganography is the art and science of communicating in a manner that conceals its presence. Thus, the concealment of Information hides the presence of data such that it cannot be detected. In the science of concealing data, hiding Information within any content of multiple media, such as images, audio, and video, is referred to as "inclusion." Both methods can be combined, i.e., encryption and Hiding, to increase the confidentiality of data delivery [2].

Hiding secret data in the middle of the cover, whether it is a photo, a video, or a text file, will make the observer on this medium or the intruder not know that there is a hidden message in this medium, as the data is included in the image (it is held in the image embedding data) [3]. The image used for the Hiding must give a clearly defined image and, at the same time, retrieve the original image after taking the embedded message and also obtaining the entire message included, so an invisible connection is required without anyone noticing that the connection will occur in some cases. That is why the information hide mechanism is needed. Some hiding methods use space, in which the secret message is included directly in the image points, including the most common methods (LSB) and histogram-base. Several research papers on the science of Hiding have recently been published. In the present work, the research has been reviewed and studied. The audit focused on reviewing the basic concepts of Hiding, assessing the security aspect of the audited research, and comparing them in terms of the selection of the hiding medium and the ability to include it, as well as the maximum amount of a confidential message that can be included in a covered image without affecting image quality.

These new publications need to be collected and reviewed again and briefly to identify all proposed techniques, weaknesses, and strengths, as well as their negatives and pros. Researchers will help design techniques for incorporating advanced spatial areas.

The remainder of the research is organized as follows: after presenting the introduction in section 1, confidential Information is presented in section 2. A Review of the latest techniques for hiding Information in the spatial domain is explained in section 3, Evaluation of Steganography is explained in section 4. Lastly, the last section contains the conclusion.

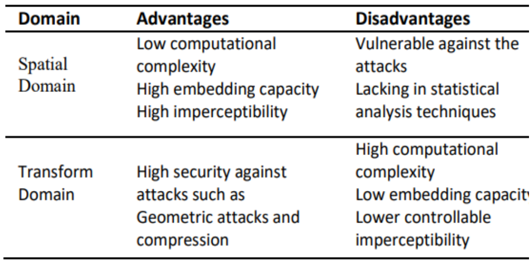
2 Hiding information

Hiding is also known as the art of embedding the data to be sent (maybe text messages or images) within sent data (may be images, audio, or video files) because it contains a sufficient amount of data that enables the user to hide the data inside [4]. There are two ways to hide Information, which are as follows:

A. Spatial Domain Methods: In this method, the secret data is directly embedded in the pixel density, which means that some pixel values in the image are changed directly while the data is hidden.

B. Transformation field methods: The image is transformed into frequency distribution in the frequency domain. Unlike the spatial domain, the changes are done directly on the pixel values in the frequency domain. The spatial domain deals with the rate at which pixel values change. Whatever processing has been done in the frequency domain, the resulting image undergoes inverse transformation to get the desired image. Discrete cosines transform (DCT), discrete Fourier transforms (DFT), and discrete wavelet transform (DWT) are represented examples of the frequency domain. Table 1 shows the advantages and disadvantages of both methods of image masking in spatial and transformational domains.

Table 1: Pros and cons of masking images in the spatial and transformational domains.



Domain	Advantages	Disadvantages
Spatial Domain	Low computational complexity High embedding capacity High imperceptibility	Vulnerable against the attacks Lacking in statistical analysis techniques
Transform Domain	High security against attacks such as Geometric attacks and compression	High computational complexity Low embedding capacit Lower controllable imperceptibility

Spatial domain hiding techniques can be classified as the following [5]:

1. Least significant bit (LSB).
2. Pixel value differencing (PVD).
3. Edges-based data embedding method (EBE).
4. Random pixel embedding method (RPE).
5. Histogram shifting methods (HS)
6. Spread Spectrum Method (SS).
7. Texture-based method (Texture).

The LSB method with the least significant bit is the most commonly used method to hide data. The embedding in this method is done by replacing the less effective pixels of the image with confidential data. After embedding image is almost the same as the original. The LSB of the pixel brings little difference [6]. The public benefits of the LSB spatial domain are as follows:

1. Less chance of deterioration of the original image.
2. Ability to store more Information in an image.

The drawbacks of LSB are:

1. More powerful and hidden data can be recovered.
2. Simple attacks can destroy hidden data [7].

Table 2 shows the advantages and disadvantages of the spatial domain methods [8].

Table 2: Advantages and disadvantages of spatial domain methods.

Disadvantages	Advantages	Technology
*Got hacked by a third party (unauthorized user) *Increasing the embedding capacity negatively can affect the cover file quality	*It is easy to understand *Ease of implementation Good load capacity *The resulting mask file will be similar to the cover file after including confidential Information	LSB
*The level of complexity is very high *Weak defense against geometric attacks, pressure, and stats	*Image quality is preserved *High embedding ability	PVD
*Data gets lost sometimes	*The level of complexity is lower than PVD	GLM
*Low data storage	*A simple mechanism of even and odd equivalence is used. One per pair, zero per person. *It can import message bits from all locations	PCM
*Data storage capacity is larger than PCM	*Strict security measures for the transmission of confidential messages.	ED
*This editing process introduces additional distortion to the hidden image	*high capacity	Diamond Encoding (DE)

3 Review of the latest techniques for hiding Information in the spatial domain

Stealth is intended to protect critical data in the transmission process. The amount of confidential data that can be included, the quality of the image used to hide, and the security of the data are all essential factors in finding a suitable hiding method. The current research presents a detailed study of the modern hiding techniques proposed in the spatial field by researchers, as this was done by collecting different techniques related to this field published from 2015 to 2021. This study was evaluated through the following factors:

1. Image quality

The human visual system (HVS) uses the organ that allows a human being to sense and compare the differences properly between objects. When hidden data in the image changes the image's shape with greater differences between the original and hidden images, reflecting the steganography method's less security. The image with hiding message and without will be placed contiguously to show if there is any difference in appearance just by HVS. Figure 1 shows two images, one before and the other after hiding the message.

Figure 1: Original and hidden message Images.

2. Message capacity

Steganography is a method that can handle a larger message more effectively. Steganography methods that can handle only 15 bytes of the message are considered low capacity. The 20 to 30 bytes are considered medium capacity, while 40 bytes and above are high capacities. The following is a presentation of the most critical methods that have been studied in the current research:

The method in [9] proposed a method for hiding messages in a spatial domain. Two bits of the message are embedded and allowed to be manipulated; the least significant bit of pixel, the second and fourth-bit plane. Interestingly, in each embedding process, only one alternation in a one-bit plane is allowed to happen. According to this method, only 2 bits are changed for each cover image character, one bit from the blue and one from the green layer. The input consists of the cover image and the secret message, and each byte of the secret message is encoded as a binary using [LSBraille]. Where only 6 bits represent the byte of the secret message. The comparing results with LSB-Matching show that it has a sufficient capacity for embedding data and is hard to detect for the steganalysis algorithm Figure 2.

After converting the cover image into (red, green, and blue) layers, each pixel in these layers is converted by ASCII binary format. For a complete secret message, it started with the blue, then the green layer of the same pixel, etc. The two bits of a pixel are included in the blue layer. The message comprises the first and second least significant bits (LSB). Additionally, the third least significant bit may be altered. In each operation, the blue layer bit may be altered by putting the final three bits of the blue layer pixel into the XOR gate and using the following equations:

$$B1 \; XOR \; B2 = N2 \qquad (1)$$

$$B2 \; XOR \; B3 = N3 \qquad (2)$$

Where B1, B3, and B2 are the first, second, and third least significant bit in the blue layer, respectively. Figure 2 shows the proposed method with the spatial domain of the cover image.

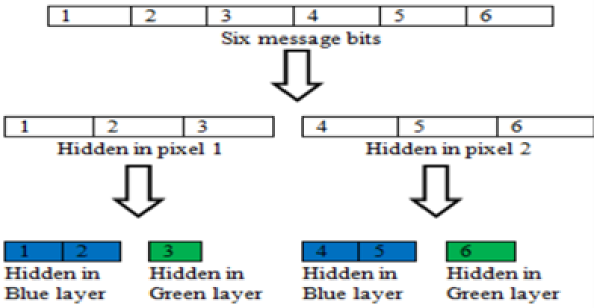


Figure 2: Suggested Method for Cover Image Spatial Domain

There are no changes to the pixel If N2 and N3 outputs are the same as the secret message bits. In contrast, If N2 and N3 outputs are different, only one bit of the original pixel must have changed so that it outputs equations (1) and (2) equal to the embedded bits. The goal is to change only one bit in the blue layer pixel. The only one bit changed in the message bits may be one of the first three bits.

The method in [10] is suggested to deploy a novel Steganography approach based on the LSB matrix. The arrays (LSB0, LSB1, LSB2, and LSB3) are formed by taking significant at least from at least one, two, three, and four pixels, respectively. One of these arrays will be selected to insert different words in the secret message. The LSB3 group can be selected for a better match if our message is more extended.

The different secret message words are plotted on the selected matrix, where the whole match and the low starting indices are noted. If one word occupies a part of the group, this part will be unavailable for the following words. The RSA algorithm encoded the start pointers of each word and its length. The encryption acquired by compression is embedded as text in a restricted area of the image. This reserved position was not used in the formation of the LSB matrix.

The sender embedding algorithm is described in the following steps in Figure 3.

1. Insert the image (Enter the message)
2. Do not change the pixels from 1 to 3000, as the image properties may be distorted. Keep the pixels from 3001 to 34999 to include identical word lengths and pointers.
3. The 35,000 to 95,000 pixels (even the last pixel) are used to formulate the various matrices.

Figure 3: (a), (c), (e), (g) embedded data in the original image, and (b), (d), (f), (h) hidden with different data amounts

4. The operation will be repeated with every secret message word. Hover the binary word over the selected binary array. The max identical Steganography is there, and note below the starting index. All word indications, in this way, are codified, and the indices are index1, index2, and index n.
5. Calculate each word length, length1, length2, length3... length n. Where length1, index1, length2, index2... length n, index n are in the E array.
6. Encrypt E by RSA algorithm, and then compress it with zip. Let us say it is E1. Find the length of E1.
7. Include E1 in at least two significant pixel positions in the reserved area, i.e., from 3001 to 34999 pixels. We will have a stego image.

The stages of the extraction method at the sender are as follows:

1. Receive an image.
2. Format the selected set (LSB0, LSB1, LSB2, or LSB3) from 35,000 pixels to 95,000 pixels (or even the last pixels) of the image.
3. E1 retrieves the matrix of the two least significant segments for locations from 3001 to 34999 pixels.
4. Decode it, then decompress, and thus we get E.
5. Calculate length 1, index 1, length 2, index 2, ..., length n, index n from E.
6. Retrieve words from the selected group with the help of these pointers and different word lengths to format the message.

The method in [11] is based on LSB substitution by reversing the value of secret bits. It divided the image into two parts. The first part includes the secret message. Using the simplest version of the LSB substitution approach, the modification is made to those bit values that include the discovered secret bit. The second part indicates any modification made to each pixel in the first segment. It consists of two stages, the embedding stage and the extraction stage. Let us say I = *p1, p2, .., pn* is the original cover image made up of an array of pixels:-

|pi|= 8bits, pi= (b1, b2,……,b8), bj ∈ (0,1) (3)

The size of the image is calculated as N = H × W (4)

where H and W are the height and width of the image. Assume that M is the secret data bits of length n,

M = m1, m2, · · · · ·, mn where mi ∈ (0, 1) (5)

: The maximum hiding amplitude h in an image I in terms of bits is

(N x 8) ≤h ≤ 1 (6)

The embedding process assumed that the cover image's pixels consist of 256 gray values. The number of secret message bits in each Pi pixel will be included with a gray value yi in the cover image I fixed on all pixels.

-Divide the secret message into k blocks.

-In the first part, directly replace each block k.

LSB of yet, this produced y′i, then picked the value closest to the original value of yi and replaced them together. Then return 0 or 1 as an indicator to show the selected change. In the second part, we start from the end. Note that each LSB bit in this segment represents the change applied to one pixel in the first part. Embed the pointer into the LSB of the pixel. Then apply the optimized LSBs style to each pixel. Determining applied change is essential to restore the original confidential data. Key sequences must be followed at the receiving end.

The method in [12] introduced a new masking technique using the pattern-based, bit-mixing method and Magic LSB for grayscale images. The proposed method provides a convenient block diagram and easy-to-understand examples. PBSA (Pattern-based Bits Shuffling Algorithm), M-LSB embedding method, and extraction algorithms are also shown.

A complete overview of the steganography framework is presented in Figure 4.

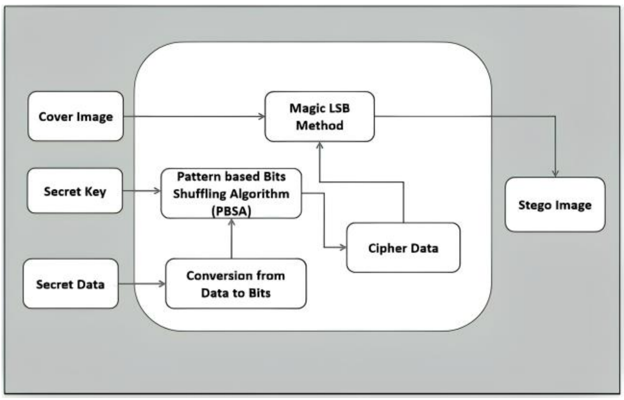
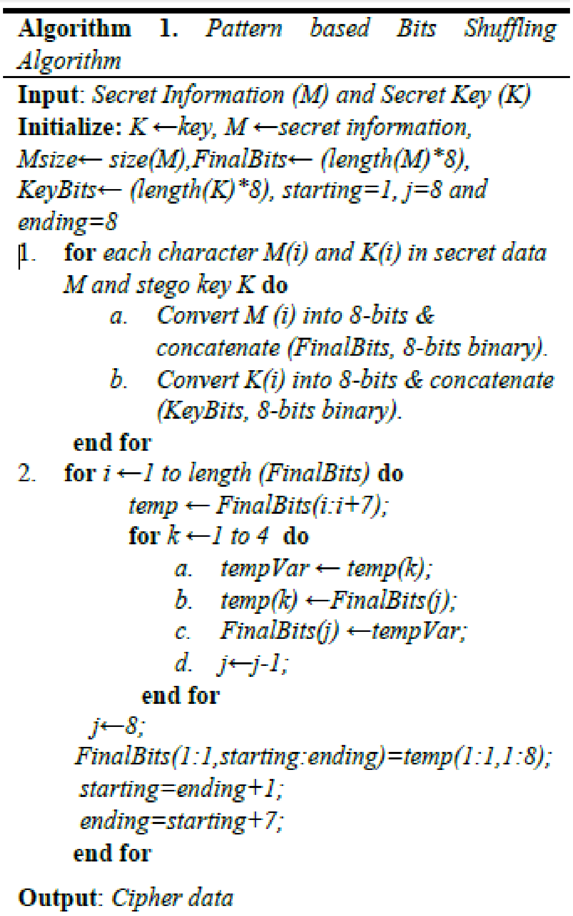

Cover Image
Secret Key
Secret Data
Magic LSB Method
Pattern based Bits Shuffling Algorithm (PBSA)
Conversion from Data to Bits
Cipher Data
Stego Image

Figure 4: Pattern-based bit-shuffle algorithm

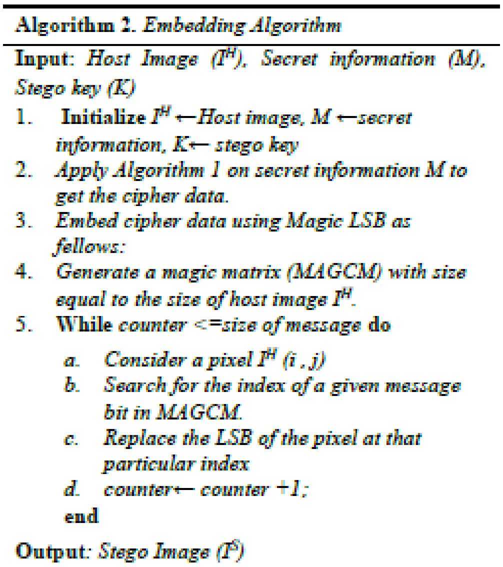
The PBSA algorithm is essential in converting and shuffling the secret data to bits based on a certain pattern and stego key. Using PBSA makes it difficult for attackers to extract the original hidden data. The bit-shuffle algorithm based on the input pattern is as follows:



Algorithm 1. *Pattern based Bits Shuffling Algorithm*

```
Input: Secret Information (M) and Secret Key (K)
Initialize: K ←key, M ←secret information,
Msize← size(M),FinalBits← (length(M)*8),
KeyBits← (length(K)*8), starting=1, j=8 and
ending=8
1. for each character M(i) and K(i) in secret data
   M and stego key K do
      a. Convert M (i) into 8-bits &
         concatenate (FinalBits, 8-bits binary).
      b. Convert K(i) into 8-bits & concatenate
         (KeyBits, 8-bits binary).
   end for
2. for i ←1 to length (FinalBits) do
         temp ← FinalBits(i:i+7);
         for k ←1 to 4  do
               a. tempVar ← temp(k);
               b. temp(k) ←FinalBits(j);
               c. FinalBits(j) ←tempVar;
               d. j←j-1;
          end for
     j←8;
     FinalBits(1:1,starting:ending)=temp(1:1,1:8);
     starting=ending+1;
     ending=starting+7;
   end for
Output: Cipher data
```

In the embedding algorithm, secret data encoded at image densities are based on the embedding method (M-LSB substitution). The role of M-LSB substitution by breaking the confidential data into the entire cover image and increasing the proposed method's security. The embedding algorithm is as follows:



Algorithm 2. *Embedding Algorithm*

```
Input: Host Image ($I^H$), Secret information (M),
Stego key (K)
1.  Initialize $I^H$ ←Host image, M ←secret
    information, K← stego key
2.  Apply Algorithm 1 on secret information M to
    get the cipher data.
3.  Embed cipher data using Magic LSB as
    fellows:
4.  Generate a magic matrix (MAGCM) with size
    equal to the size of host image $I^H$.
5.  While counter <=size of message do
      a. Consider a pixel $I^H$ (i , j)
      b. Search for the index of a given message
         bit in MAGCM.
      c. Replace the LSB of the pixel at that
         particular index
      d. counter← counter +1;
    end
Output: Stego Image ($I^S$)
```

A simple example is given to illustrate the magical LSB method's idea fully. Suppose an IH host image has nine (9) pixels {30, 46, 31, 65, 75, 22, 34, 98, 59} and secret message bits M =$(01101011)_2$. A magic matrix is created to include this bit stream. A size equal to the size of the host image (3 x 3 in this case) is shown in Figure 5.

$$IH = \begin{vmatrix} 30 & 46 & 31 \\ 65 & 75 & 22 \\ 35 & 98 & 59 \end{vmatrix} \quad MAGCM = \begin{vmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{vmatrix}$$

After hiding:

$$IS = \begin{vmatrix} 31 & 46 & 330 \\ 65 & 75 & 23 \\ 34 & 78 & 59 \end{vmatrix}$$

Figure 5: Creating a Magic Array with a Size

Equal to that in the Host Image (3 x 3)

The secret bits are included in the example given based on MAGCM indexes. The first, second, and third secret bit M is hidden in the pixel value (46, 59, and 65), respectively. Continuously, in the same way, Include the 4th, 5th, 6th, 7th, and 8th bit in (35, 75, 31, 22, and 30), respectively. For example, only pixels that appear in bold are changed. In the case of image dimensions 256 x 256, MAGCM will have dimensions of 256 x 256. On the receiver side, hidden bits are extracted according to the magic matrix indices and apply the inverse operations of PBSA.

The method in [13] introduced the Private Domains Approach (PDA) technique, which relies on MSB and hides the data in the essential part of the image. Private domains are randomly available based on image size. Each area is made up of RGB pixels from the cover image. Once we randomly get the domains we need, we can perform the hiding process. See Figure 6, which represents the embedding process.

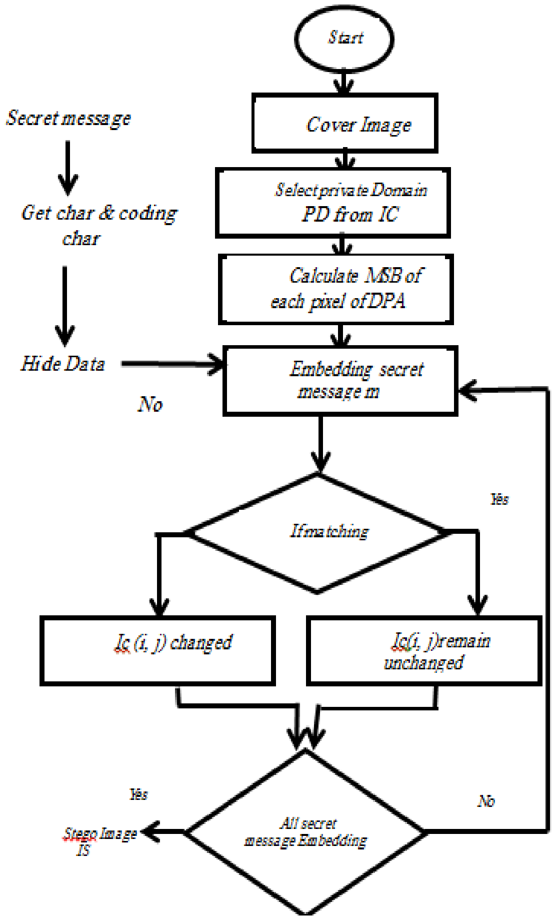
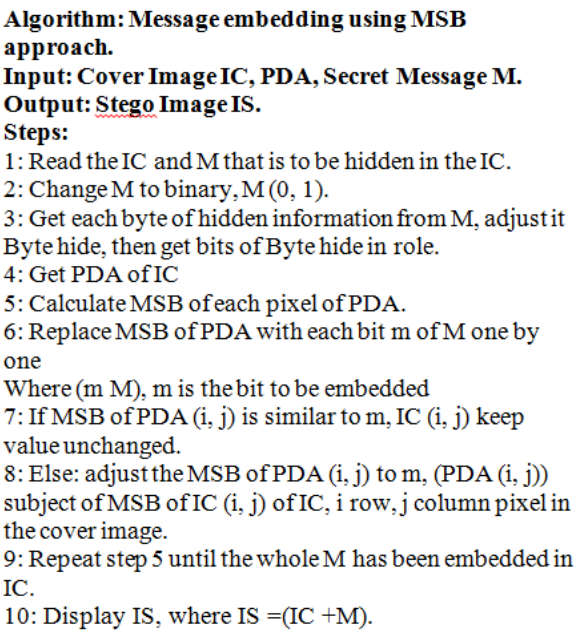


Figure 6: shows the embedding process

However, the embedding process works by taking one of the Private Domains Policy (PDA) parts. Masking will be in bits 5, 6, 7, or 8. To insert the entire secret text, it may mask the pixel's field (red, green, blue). The higher bit rate steganography has the lowest probability of error rate being used to mask bits of confidential Information. According to the presented approach, the secret text bytes of entries under pre-processing photo cover and secret message are represented by binary. Each character is given an encoding where the data is hidden in the most significant bit.



Algorithm: Message embedding using MSB approach.
Input: Cover Image IC, PDA, Secret Message M.
Output: Stego Image IS.
Steps:
1: Read the IC and M that is to be hidden in the IC.
2: Change M to binary, M (0, 1).
3: Get each byte of hidden information from M, adjust it Byte hide, then get bits of Byte hide in role.
4: Get PDA of IC
5: Calculate MSB of each pixel of PDA.
6: Replace MSB of PDA with each bit m of M one by one
Where (m M), m is the bit to be embedded
7: If MSB of PDA (i, j) is similar to m, IC (i, j) keep value unchanged.
8: Else: adjust the MSB of PDA (i, j) to m, (PDA (i, j)) subject of MSB of IC (i, j) of IC, i row, j column pixel in the cover image.
9: Repeat step 5 until the whole M has been embedded in IC.
10: Display IS, where IS =(IC +M).

The method in [14] used edge detection instead of a smooth area for the cover image to hide a secret message either in the spatial domain or wavelet transform-dependent transformation field. They can estimate the exact intensity of the edge before and after embedding the message of the cover images, which is essential when extracting the message. On the other hand, the limited sensitivity of the human visual system cannot detect sharp contrast areas compared to other hiding methods. The method provided a good level of security.

The method in [15] According to density, the method separates the image into three zones (low, medium, and high, labeled L, M, and H, respectively) and exploits pixels up to LSB3. Three image areas are separated by the threshold values t1 and t2. Across images, the size of each alters dynamically. In the low-density (first) zone, up to three less significant bits are used per pixel. Confidential data in the third LSB were combined with the first and second LSB tuning, while the medium-density region (second) with the second LSB worked with the first LSB tuning. In the high-density region (the third), only the first LSB is used to include the data. These three gray-level ranges are used to insert confidential data. The embedding algorithm reads the random grayscale values first with the pixel pointer; if the first region has a value, then the third LSB is modified, preserving the image quality with two optimizations and 1 LSB. The second LSB is used with 1 LSB set in the second region case. Only the first LSB is turned on if the pixel density value is in the third region. Before the embedding and extracting processes, the secret key for determining the pixel index value is generated at random. The value of the secret key may be computed using values between 2 and 9. If the LSB's media containing the steganographic image is intercepted, the interceptors will be unable to delete the secret Information. Figure 7 depicts the method's block diagram.

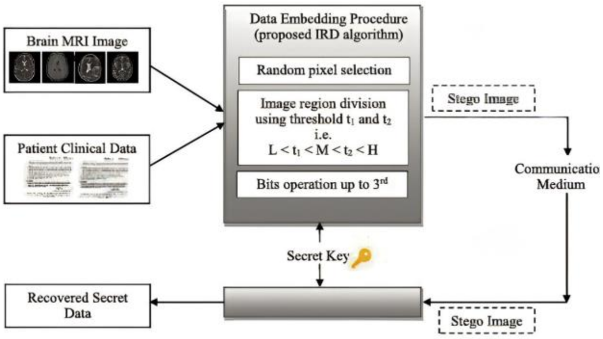


Figure 7: is a block diagram of the method

The method in [16] is Sharing secret image systems using data loss, proposed compression, and conversion system for grayscale images. Securing secret images is done by blocking depending on lossless compression technology. It is applied to each sub-image to obtain a noisy one to increase the security level, and then the secret image is returned. The secret image-sharing system creates a Threshold (t, n) so that any or more shared images can be used to recreate the secret photo. The study introduced a cryptic image-sharing scheme in which the secret image is encrypted firstly by a block-based lossy compression technique and sub-image identification. Image compression technology gives a good-quality image. Arnold transforms the sub-images, and then the posts are created to improve security. Finally, the image steganography concept (i.e., Steganography) was adopted to hide posts within cover images. The proposed method gives good stego image quality.

The method in [17] is for multiple hiding secret images in one 24-bit cover image using replacement-based image masking. Before hiding in the cover image with Arnold Transform, each secret image is encrypted. The results show that this method secures the success of high-capacity data preservation. We get the multi-image technology hiding inside a single 24-bit color image using the Arnold transformation with three secret 8-bit images. The proposed technique gives high power and less computational complexity than the method that gives a satisfactory optical quality of the transmitted image.

The nimble edge detector uses **the method in [18]** new technology based on Edge detector to detect the edge of a cover image where only the edges are included. The method uses Huffman cipher to encrypt confidential data before embedding and random edge-sorting methods to increase the method's security.

The method in [19], the EMD (Exploit Modification Direction) method by Zhang and Wang, uses the - ary() a notation to achieve the embedding of a secret message in the cover image. However, the maximum amplitude of this method is for the shell pixel number. Its embedding capacity rapidly decreases with the increase in selected pixels. To improve this deficiency, a new scheme has been proposed with two main contributions to make the system more efficient maintains. For best concealment of the secret message, the cover image is split into non-overlapping pieces by scanning each pixel line from left to right and top to bottom.

The method in [20] presents two new ways to increase the limits of image-hiding performance under distortion reduction criteria. Similar images are used in the embed stage, and smooth areas are also avoided. Then, a parallel approach is used to insert images, which improves the results. The method relied on calculating the modulation costs for each pixel to increase the safety of the method.

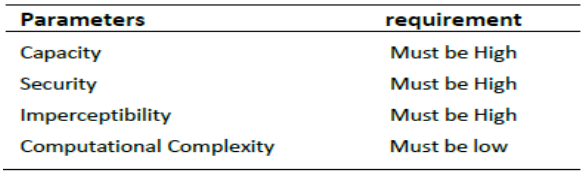
The method in [21] aims at an algorithm that relies on the use of a symmetric key to hide the images, and the least significant bit method was used for Hiding, and the pixel position was randomly chosen to hide the secret bits. The main problem of the proposed system is the random selection of pixel position from a cover image using the chaotic map to increase efficiency and security. The result analysis shows that the algorithm provides an adequate level of security.

The method in [22] offers a new way to increase the security of Information across the network by using information steganography so that the secret message sent is not identifiable .Hiding Information for comparison with LSB and DKL, a comparison has been made to show how the proposed algorithm is better than the long-time LSB algorithm for sending hidden messages. Algorithms are evaluated using baseline evaluation MSE and PSNR to avoid opportunities for attackers to use hidden analysis to retrieve data.

4 Evaluation of steganography

This study aims to conduct a review of the latest publications and related steganography techniques related to image hiding in the spatial domain, some of which are more complex than others and include weaknesses. Table 3 shows the most important measures required in the excellent hiding technique.

Table 3: Standards required in the good hiding technique.



Parameters	requirement
Capacity	Must be High
Security	Must be High
Imperceptibility	Must be High
Computational Complexity	Must be low

Table 3 indicates the maximum capacity of a secret message that can be included in a cover photo without degrading the image quality represented by bits per pixel. The second criterion works to keep the secret image from being exposed by hackers, i.e., how to make the Information resistant to steganography attacks. The third insensitivity criterion means transparency and image quality after the secret message is hidden in the cover image. The image should appear as large as possible, like the original image file. This is a criterion for the noise component, which may be derived by subtracting the image distortion between the cover and the original. Its definition is:

$$PSNR = 10Log10(\frac{C2_{max}}{MSE})$$

Where MSE stands for mean squared error Defined as:

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

Where x and y are the values of the pixel locations for the cover image M and N are the size of the cover image. The fourth criterion is the computational complexity and the cost of the computational complexity to embed and extract a secret hidden message. Many proposed techniques for hiding image information in the spatial domain, and few of them focused on preserving the quality of the image, and others focused on the amount of data that we can hide inside the cover image or another.

This research aims to define specifications for the concealment technique proposed by researchers in this field by revealing weaknesses and defects through powerful new techniques. It is an open topic and motivates researchers to propose an effective solution to this issue. The main features and disadvantages of the essential current image-hiding techniques in the spatial domain are summarized. This is shown in tables 4 and 5.

Table 4: The most important characteristics of existing technologies.

References	Capacity	security	Peak signal-to-noise ratio (PSNR)	Computational Complexity
[9]	Moderate	Low	Moderate	High
[10]	High	High	Moderate	Moderate
[11]	High	Moderate	Low	High
[12]	Low	High	High	Moderate
[13]	Moderate	Moderate	High	Low
[14]	Moderate	Moderate	High	Low
[15]	High	Moderate	High	Low
[16]	Moderate	High	Low	Moderate
[17]	High	High	Low	High
[18]	Low	High	High	Moderate
[19]	Moderate	High	Moderate	Low
[20]	Moderate	Moderate	Low	Low
[21]	High	High	Low	Moderate
[22]	Low	High	High	High

Table 5: The disadvantages of image steganography techniques in spatial domain.

Ref.	Algorithm	Disadvantages
[9]	LSB Technique	No development And security is low
[10]	LSB matrix	No development Low image quality (no distortion caused by embedding can be apparent)
[11]	LSB Changing	The original image must be available for him to return the images
[12]	Shuffling Bits and Magic LSB for grayscale images	A Small amount of data No development
[13]	improved MSB	No development
[14]	Edge finding and encoding XOR	does not discriminate
[15]	Dynamic Programming	Not using all kinds of images
[16]	based image coding	Calculations are not easy
[17]	LSB and At the algorithm	Replay requires the original image Calculations are not easy
[18]	Finding Edge and Link	Capacity
[19]	LSB and EMD	Computationally Complex
[20]	LSB	Limited to certain Information
[21]	Random methods with the least significant bits	does not discriminate
[22]	DKL	Computationally Complex

5 Conclusions

Recently, several studies were performed and published on steganography; some of them focused on reviewing basic concepts. Various assessment measures include the security aspect of the image-hiding system. However, in this review, we considered them outdated since there are many new contributing publications, and it is necessary to group them under a new field in the review paper. We discuss the definition of image hiding and its domains in the present work. In addition, the techniques are in summary form, as explained in the current review. The difference between image-hiding techniques in the spatial domain analyzed various problems and drawbacks of each method devised in the past few years. The primary criteria adopted in this comparison review are based on the discussion of studies. According to the chosen pixel in Hiding and the ability of the algorithm to include pixel identification to achieve the goal of security, adaptation, and image segmentation. In addition, the standard Random Secret Post shows the maximum number of secret messages included in a cover image without degrading the image quality. This will enable important research problems to be addressed in the future. We also intended to enhance the security of more powerful hiding technologists' paper presents the literature review of the hidden spatial domain approach. Existing spatial domain embedding approaches have been objective, and we discuss the methodologies. Depending on the proposed algorithms, all the above methods had advantages and limitations. The image steganography approach should be top implant payload, high quality, and secure. However, no steganography approach has these features.

References

[1] Fabien, A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding-a survey. Proceedings of the IEEE, 87(7), 1062-1078. https://doi:10.1109/5.771065

[2] Yang, C., Liu, F., Luo, X., & Zeng, Y. (2012). Pixel group trace model-based quantitative steganalysis for multiple least-significant bits Steganography. IEEE transactions on information forensics and security, 8(1), 216-228. https://doi:10.1109/TIFS.2012.2229987

[3] Chang, C. C., Lin, M. H., & Hu, Y. C. (2002). A fast and secure image-hiding scheme based on LSB substitution. International journal of pattern recognition and artificial intelligence, 16(04), 399-416. https://doi.org/10.1142/S0218001402001770

[4] Ditta, A., Yongquan, C., Azeem, M., Rana, K. G., Yu, H., & Memon, M. Q. (2018). Information hiding: Arabic text steganography by using Unicode characters to hide secret data. International Journal of Electronic Security and Digital Forensics, 10(1), 61-78. https://doi.org/10.1504/IJESDF.2018.089214

[5] Lakshmi Sirisha, B., & Chandra Mohan, B. (2021). Review on spatial domain image steganography techniques. Journal of Discrete Mathematical Sciences and Cryptography, 24(6), 1873-1883. https://doi.org/10.1080/09720529.2021.1962025

[6] Gahan, A. V., & Devanagavi, G. D. (2020, December). A Secure Steganography Model Using Random-Bit Select Algorithm. In 2020 Third International Conference on Advances in Electronics, Computers, and Communications (ICAECC) (pp. 1-5). IEEE. https://doi.org/10.1109/ICAECC50550.2020.9339474

[7] Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. Signal Processing: Image Communication, pp. 65, 46–66. https://doi.org/10.1016/j.image.2018.03.012

[8] Nilizadeh, A., & Nilchi, A. R. N. (2016, March). A novel steganography method based on matrix pattern and LSB algorithms in RGB images. In 2016 1st Conference on Swarm Intelligence and Evolutionary Computation (CSIEC) (pp. 154-159). IEEE. https://doi.org/10.1109/CSIEC.2016.7482107

[9] Lakshmi Sirisha, B., & Chandra Mohan, B. (2021). Review on spatial domain image steganography techniques. Journal of Discrete Mathematical Sciences and Cryptography, 24(6), 1873-1883. https://doi.org/10.1080/09720529.2021.1962025

[10] Swain, G., & Lenka, S. K. (2015). A novel steganography technique by mapping words with an LSB array. International Journal of Signal and Imaging Systems Engineering, 8(1-2), 115-122. https://dol:10.1504/IJSISE.2015.067052

[11] Mohamed, M. H., & Mohamed, L. M. (2016). High capacity image steganography technique based on LSB substitution method. Applied Mathematics & Information Sciences, 10(1), 259. https://dol:10.18576/AMIS/100126

Muhammad, K., Ahmad, J., Farman, H., & Jan, Z. (2016). A new image steganographic Technique using pattern-based bits shuffling and magic LSB for grayscale images. arXiv preprint arXiv:1601.01386. https://doi.org/10.48550/arXiv.1601.01386

[12] Ali, S. I. M., Ali, M. G., & Qudr, L. A. Z. (2019). PDA: A private domains approach for improved

[13] MSB steganography image. Periodicals of Engineering and Natural Sciences (PEN), 7(3), 1405-1411. http://dx.doi.org/10.21533/pen.v7i3.776

[14] Al-Dmour, H., & Al-Ani, A. (2016). A Steganography embedding method based on edge identification and XOR coding. Expert systems with Applications, 46, 293-306. https://doi.org/10.1016/j.eswa.2015.10.024

[15] Siddiqui, G. F., Iqbal, M. Z., Saleem, K., Saeed, Z., Ahmed, A., Hameed, I. A., & Khan, M. F. (2020). A dynamic three-bit image steganography algorithm for medical and e-healthcare systems. IEEE Access, 8, 181893-181903. https://dol:10.1109/ACCESS.2020.3028315

[16] Das, S. K., & Dhara, B. C. (2015, April). An image secret-sharing technique with block-based image coding. In 2015 Fifth International Conference on Communication Systems and Network Technologies (pp. 648-652). IEEE. 0. https://doi.org/10.1109/CSNT.2015.37

[17] Das, P., Kushwaha, S. C., & Chakraborty, M. (2015, February). Multiple embedding secret key image steganography using LSB substitution and Arnold Transform. In 2015 2nd International Conference on Electronics and Communication Systems (ICECS) (pp. 845–849). IEEE.https://doi.org/10.1109/ECS.2015.7125033

[18] Sun, S. (2016). Novel edge-based image steganography with 2k correction and Huffman encoding. Information Processing Letters, 116(2), 93-99. https://doi.org/10.1016/j.ipl.2015.09.016

[19] Kuo, W. C., Wang, C. C., & Hou, H. C. (2016). Signed digit data hiding scheme. Information Processing Letters, 116(2), 183–191. https://doi.org/10.1016/j.ipl.2015.08.003

[20] Sharifzadeh, M., Agarwal, C., Salarian, M., & Schonfeld, D. (2017). A new parallel message-distribution technique for cost-based Steganography. arXiv preprint arXiv:1705.08616.https://doi.org/10.48550/arXiv.1705.08616

[21] Rajendran, S., & Doraipandian, M. (2017). Chaotic map-based random image steganography using the LSB technique. Int. J. Netw. Secure., 19(4), 593-598. DOI: 10.6633/IJNS.201707.19(4).12) 593

[22] Udhayavene, S., Dev, A. T., & Chandrasekaran, K. (2015). New data hiding technique in the encrypted image: DKL Algorithm (Differing Key Length). Procedia Computer Science, 54, 790-798.https://doi.org/10.1016/j.procs.2015.06.093