**Image Steganography: A comprehensive study on steganography techniques**

 Bishakha Gope1, Sakshi Deo2, Tanishka Chavan3, Sakshi Nawale4, Prof. K.P. Mohalkar5

JSPM’s Rajarshi Shahu College of Engineering, Pune-411033, Maharashtra, India

bishakhagope03@gmail.com1, deosakshi29@gmail.com2, tanishkachavan02@gmail.com3, sakshics108@gmail.com4, komohalkar\_comp@jspmrscoe.edu.in5

**ABSTRACT:** Steganography is a technique used to hide secret messages in images, sounds, or videos. This method allows users to hide and send sensitive information to the receiver in order to prevent it from being hacked. A survey is performed and different data security methods are discussed. Different encoding steganography methods are studied. Also, some encryption algorithms are addressed. Different image formats are analysed for image steganography. The ease with which data is transferred stealthily and efficiently has developed this approach from traditional techniques to new areas of deep learning. The main motive of this paper is to provide a comparative study of the techniques involved in steganography. A few ideas which will be beneficial as a reference for future studies are also discussed.

**KEYWORDS:** *Steganography, encryption, decryption.*

**INTRODUCTION:** Cybersecurity concerns today make it difficult to protect sensitive information over the internet. Attackers may be able to access sensitive information, share it, disclose it, update it, or change its accessibility. Information sent over an insecure connection can be easily modified. The simplicity of steganography has led to its popularity among researchers. As the number of cyber threats increases, it is essential to be able to protect critical information transmitted over the Internet from enemies. Security personnel who are trained and prepared in the use of secure steganography algorithms will be more effective in combating organised cybercrime. Steganalysis & Steganography plays hide-and-seek. Due to the advancement of the deep learning algorithms of cryptographic analysis, the task of designing a more reliable and robust cryptographic analysis framework becomes more and more urgent. Image cryptography and cryptographic analysis have received much attention from law enforcement agencies and social media due to the ease of multimedia communication through the internet. Image cryptographic printing is the most popular medium due to the speed and ease of sending confidential information. Generally, image recording frames can be divided into two categories: spatial domain frames and transformation domain frames**.** When dealing with spatial frameworks, we deal with picture pixel values.

Earlier organisations used a variety of cryptographic and steganographic methods to send sensitive information, reducing the number of changes embedded in images and increasing invisibility. However, because natural images have strong interrelationships, it is not enough to secure this sensitive information. There was further development of steganography algorithms to achieve higher reliability and integrity. In the world of today's steganographic algorithms, images such as BMP, PNG, TIFF and irreversible JPEG may be used for the purpose of hiding confidential information.

This paper presents an overview of the most used steganographic techniques. In this study, we explored the tactical foundations of the technique, as well as their strengths and weaknesses. Moreover, we provided both steganography and steganography analysis studies and a comparison of embedded algorithms to demonstrate how these challenges can be turned into valuable research tools in the future. These observations inform our understanding of the current state of research.

The organisation of the paper is as follows: Section 1 shows the events from history. An overview of various data security technologies is provided in section 2. Section 3 consists of some related work specifications. Section 4 outlines the use of various steganography imaging techniques and the algorithms used. Section 5 describes future applications of image steganography. Section 6 describes open issues/challenges.

**1.** **INCIDENTS FROM HISTORY**

Steganography has been with us for years, whether it's a Revolutionary War spy writing in invisible ink or Da Vinci embedding a secret meaning in his paintings. Steganography has its roots in 500 BC. return. The first physical example of steganography is in the history of Herodotus, which talks about the actions of the Greek leader Histiaeus. Herodotus explains how the news of Xerses' hostile intent was conveyed to the Greeks under the wax of a writing tablet, a technique that involves a dotted pattern of secret inks over the contiguous text. The legend of the pirates is related to the practice of tattooing confidential information, such as maps, on someone's head and having their hair hide it.

 Khan talks about the trick used in China to embed code ideographs in place on the broadcast. A similar idea led to the trellis system used in mediaeval Europe. There, a wooden stencil was placed on top of the seemingly innocuous text to emphasise the embedded secret message. During World War II, grid methods or several variants of espionage were used. At the same time, the Germans developed microdot technology. It prints crisp, high-quality photos reduced to dot size. In the 1980s, then British Prime Minister Margaret Thatcher was very frustrated by the media leaks of cabinet documents and was programmed to code the author's identity into word spacing to detect dishonest ministers. There are rumours that he had a word processor. During the "Cold War, "The US and the Soviet Union wanted to conceal their sensors in hostile installations. These devices had to send data to their country without being detected.

 Steganography is being studied today for both legal and illegal reasons. Some of the first are wartime communications that use spread-spectrum or meteor scatter radios to disguise both the message and its source. With the advent of digital communications and storage in the industrial market, watermarking technology is being developed to limit the use of copyrighted data, as one of the most important issues in the exercise of copyright. Another important use is to embed data related to medical images. This ensures no problem collating the patient's records with the images. Illegal ones include the practice of hiding highly encrypted data to circumvent the restrictions imposed by encrypted export laws.

**2. DATA SECURITY METHODS**

****

 ***Figure 1:*** *Scheme for classifying data security techniques*

**2.1 Cryptography**

The study of communication systems that ensure only the sender and the intended recipient of a message can view its contents is known as Cryptography. The word ‘Kryptos’ comes from the Greek word kryptos, which means to conceal. This is associated with encryption, the wherein regular textual content is encrypted into what's referred to as ciphertext and re-encrypted on arrival. Ancient Egyptians are regarded to have used those strategies in complicated hieroglyphs, and Roman emperor Julius Caesar is assumed to have used one of the first contemporary-day cyphers. When sending digital data, encryption is typically used to encrypt and decrypt electronic mail and different plaintext messages. The simplest manner is to apply an uneven or ‘non-public key’ system. Data encryption is done using a non-public key, and each encrypted message and the non-public key are delivered to the recipient for decryption.

A third party has everything it needs to decrypt and read a message if it is impeded. Cryptographers have devised asymmetric or ‘public key’ solutions to alleviate this problem. Each user has two keys in this situation. The public key is one, while the other one is the private key. The sender encrypts the message and resends it after requesting the intended recipient’s public key. Therefore, theft is useless without the corresponding private key.



  ***Figure 2:*** *A schematic representation of a cryptographic communication process*

**2.2 Steganography**

Steganography is the use of different methods to hide information from unwanted eyes. Steganography has both constructive and harmful applications. Steganography is used by educational institutions, businesses, intelligence agencies, the military, and certified ethics criminals to hide private messages and information to make themselves visible to everyone. Cybercriminals, on the other hand, employ steganography to damage data files or hide harmful malware in seemingly harmless papers. By embedding text into a Word and Excel document, an attacker can start automated attacks using *BASH* and *PowerShell* scripts. When an unknowing person opens one of these scripts, the encrypted secret script runs which is confusing. This process is the recommended ransomware delivery method. Steganography has significant advantages over traditional cryptography. When someone uses encryption, they just notice that the sensitive information is present in the medium in question. Thus, in the presence of encrypted data only, the attacker will be: Here is some sensitive information! However, steganography hides sensitive information in otherwise harmless documents. Therefore, potential hackers are completely unaware that there is something secret and fascinating.

Steganography breaks down into the following types: 1] *Text steganography* uses spaces, uppercase letters, tabs, and other characters. 2] *Audio Steganography* is used in digital audio formats such as WAVE, MIDI, and AVI MPEG, with echo concealment, parity coding, LSB coding, and more. 3] *Video Steganography* handles video formats such as Mp4, MPEG, and AVI, H.264. 4] Additionally, it uses images to transfer hidden data. 5] In *image steganography*, pixel strength is used to obscure information. 6] *Network Steganography* is a network protocol that uses UDP, TCP, and IP as bearers. Researchers preferred such images because of the innocence of digital images as the carrier signal to hide confidential information. It is also better suited for embedding confidential information due to the presence of redundant pixels in the image. Hiding sensitive information in an image is called image steganography.

The algorithms used to process digital images differ significantly due to the wide availability of formats. The common types are: Insert the LSB, Masking and filtering, unnecessary pattern encoding, encrypting and distributing Algorithms and conversions.



 ***Figure 3:*** *A schematic representation of a steganographic communication process*

**2.3 Digital Watermarking**

A Digital Watermark is data embedded in digital intellectual property (IP) that allows the investor or owner of the IP to be identified. Watermarks track and prevent the unauthorized use and access of digital media on the web. DRM technology helps watermarks prevent unauthorized use and access. Digital watermarks are also recognized as forensic watermarks, information hiding, and data embedding. The Watermark provides copyright protection for digital intellectual property such as programs, images, recordings, and videos. The watermark is invisible to the naked eye, but it acts as a signal when downloading or copying copyrighted material.

The powerful watermarks disseminate bit information over included copyrighted material in a random manner. Watermarks are non-convertible for best results and must withstand changes such as reduction in algorithm and reformatting of file. Organizations are evolving new types of digital watermarks in the form of noise. Noise is random digital file data in IT jargon. This type of watermark, in other words, assigns random records to current watermark data. Watermarks look like random electronic data, making it difficult to identify such digital watermarks.

****

 ***Figure 4:*** *Representation of watermark system*

**3. RELATED WORK**

In 2022, Jialiang Xie, Honghui Wang et al. [1] proposed adaptive techniques based on image edges and complicated texture areas which have been widely proposed for image steganography. When creating image steganography, three rules should be kept in mind. The embedded area, for starters, is made up of boundaries and complexes. The image's textured region follows the first complexity rule. Fuzzy enhancements are used to detect edges. The Gray Wolf Optimizer has improved the features (GWO). Second, the bare minimum categorization error rate is utilised to decide which Complex texture area to use. Third, the embedded area cost function is designed using two different averaging filters and KB (KerBohme) filters according to the diffusion rule. Finally, STC embeds sensitive data in an adaptable way (Syndrome trellis code). The proposed approach outperforms the seven traditional algorithms.

In 2022, Fengyong Li, Yishu Zeng et al. [2] present an improved steganographic scheme based on random generation and ensemble stego selection in this research. Unlike conventional steganography, which focuses solely on distortion function design, our technique takes into account both the distortion model and optimum stego-generation. The proposed ensemble selection process can be used to significantly increase the undetectability of any existing safe steganographic scheme. The findings of the experiments suggest that using an ensemble technique can improve steganography security. This system outperforms previous steganographic techniques in terms of detection error rate under various steganalysis, resulting in increased anti-steganalysis capabilities.

In 2022, Xinghong Qin, Bin Li et al. [3] proposed this paper to describe GEAP in detail for colour image steganography in order to overcome the limitations of CNN-based steganography analyzers. GEAP is created by breaking one image down into numerous non-overlapping sub-images. Then the colour pixel vector is iteratively altered. Update costs in stages depending on the relationship coefficient between correction pattern and sign graduation vector. In this way, more change patterns will appear to participate in cost adjustment of vector unit embedding relative cost fluctuations are minimised concerning `∞ distortion will arrive at the same time.

In 2021, U. Sivaramakrishnan, N. Panga et al. [4] studied this concept of visualising steganography via the “Fractional Random Wavelet Transform “(FrRnWT). They compared this method to another technique known as the "Discrete wavelet transform" (DWT), which is frequently used in picture steganography for transforming images. Various sorts of threats such as B. Crop, RST, and compression are investigated by embedding strategies to safeguard the data.

In 2020, X. Duan, Liu Nao et al. [5]introduced steganography technology, which is not the same as the standard STC coding scheme. Artificial intelligence is used to build the cost function instead of manually writing STC code. Full-size images will be blank and end-to-end training methods will be used to minimise image distortion. This method provides improved visual effects and excellent steganography capabilities, according to experimental results, and the model has strong generalisation capabilities that allow steganography and extraction of different datasets.

In 2020, A. Thakur, G.S. Gill et al. [6] compared multiple images created using different bits of the cover images and then MSE and PSNR were calculated. The difference between the stego-image formed with the first LSB and the stego-image created with the second LSB is relatively minor, demonstrating that the second LSB can also hide the data. The same technique can be used in future work on RGB photos to compare different images.

In 2020, T. Kalaichelvi and P. Apuroop et al. [7] proposed a new technique that is introduced where CAPTCHA codes ensure that the end receiver is the intended one and not any robot. For providing protection when interacting with the authenticated user, a random CAPTCHA code is constructed, and Image Steganography is employed to achieve confidentiality. Encryption and decryption mechanisms are used to achieve secret and reliable communication; as a result, a machine cannot decode it using any predetermined technique.Following the establishment of a secure connection with the intended recipient, the original message is transferred with the LSB method, which hides image data using the RGB colour spectrum, ensuring additional encryption. In the future, hybrid cryptography could be utilised for communication.

In 2020, O. Elharrouss, N. Almaadeed et al. [8] suggested a method which starts with a combination of the cover image and the hidden image. A region detection method is specified that uses a local entropy filter to detect regions containing latent images.The image quality improvement procedure was utilised to improve the corrupted images during the hidden process after extracting the concealed images. According to the test results and metrics, the suggested method can hide and extract images with the least amount of information distortion and loss.

In 2020, A. S. Ansari, M. S. Mohammadi et al. [9] proposed this study. This study proposes a paper algorithm for embedding secret messages in a cover image and then comparing the result with the “BLIND HIDE” steganography algorithm using various parameters such as accuracy and accuracy.It can be concluded that the suggested algorithm outperforms BLIND HIDE in terms of accuracy, recall, and precision. The output image produced by our method is around the same size as the source image. The suggested method generates a steganographic image in PNG that is superior to JPEG (Portable Network Graphics). Because it is compressed, BMP (bitmap) is used. These are designed to ensure that your data is processed quickly and securely in the future.

In 2020, R. Sulaiman, C. Kirana et al. [10] proposed this research. Types of research were performed on JPEG and BITMAP images, and it was found that encryption and decryption of the RC4 algorithm paired with LSB take less time in BITMAP images than in JPEG format. As a result, the pixels and bytes scattered in the image have fewer bits when distributed in BITMAP format. Future work, a new approach to steganography with embedded cryptographic algorithms that encrypt text files while creating an image file.

In 2020, Nandhini Subramanian et al. [11] proposed this method.Traditional approaches, CNN based methods, and GAN-based methods are all described in this article, along with their benefits and weaknesses. In addition, detailed tabular summaries of the datasets used, experimental designs considered, commonly used metrics, current trends, and current challenges are provided.

In 2020, Md. Sagar Hossen et al. [12] proposed this study. The proposed system involves the use of AES and RC5 algorithm cryptosystems. Using a hybrid algorithm system along with encryption and decryption, the proposed architecture uses a block size of 128 bits. It also includes a watermarking technique used to ensure the legitimacy of individual digital media owners. DCT, a discrete cosine transform, for the security of image data. Here, the quality of the cover image is excellent and it is difficult to doubt the existence of a secure transformation. Here further work can be done on enhancing the quality of the cover image. An increase in payload leads to an increase in MSE value, this aspect needs to be modified.

In 2020, J. R. Jayapandiyan, C. Kavitha and K. Sakthivel et al. [13] proposed this study presenting an improved LSB embedding method in steganography that improves the visual quality of the cover image in comparison to the traditional LSB algorithm used in steganography. This method works in the spatial area while performing the task. Message coding is a two-step process. The metadata is created in the first phase, and the header data is inserted in the first few bytes of cover images. The next task is to encode the confidential message and save it inside cover images in the most effective and determinable manner possible. The proposed work is made possible by analysing ciphertext strings, which saves space for the ciphertext provided in the cover picture and improves the Stego image quality. Future work on the proposed methodology may uncover more similar spatial domain optimizations, leading to improved image visual quality.

In 2019, J. Horng, C. Lee et al. [14] introduced contrast enhancement technology that allows secret data to be inserted using the enhancement methodology. The cover image is broken into little blocks, each of which is then labelled as a smooth block or a high contrast block. The secret message is placed in a high contrast block so that the contrast of the block is emphasized.Only half of the secret data is included in a smooth-surfaced block..2.31 is the average embedding capacity The embedding strategy has been tailored to the unique properties of the cover images to ensure the better visual quality of the stego-image.

In 2019, Ahmed Hambouz, Yousef Shaheen et al. [15] presented a technique that ensures data secrecy and integrity. Data secrecy is obtained by secretly embedding a bit of data in the stego-image. Decode and encode variables are hashed using the SHA 256 hashing technique to ensure consistency. The proposed model achieved a high PSNR score with an average PSNR of 82.933 per cent when using datasets with different image sizes.Other image kinds, such as.tiff,.bmp, and.gif, will be added to the selectable image type in the future.

In 2019, Weixuan Tang et al. [16] proposed this method. In particular, the cost of pixels is adjusted by ADV-EMB based on the gradient transmitted from the target CNN ridge analyzer.

Therefore, the direction of correction is likely to be the same as the inverse sign of the gradient. In this way, stego images are generated. The proposed steganography scheme increases the false positive rate of the unprotected steganographic analyzer of the target enemy, thus demonstrating better security against the unprotected steganographic analyzer. Additionally, it produces a new class of modern steganography schemes that can overpower CNN-based steganography and reduce its performance.

In 2019, Hope Mogale, M. Esiefarienrhe et al. [17] proposed this paper where they have described an authentication system which is web-based.This system has employed image steganography with the 128-bit encryption algorithm.This system encrypts users' password and takes trillions of years to decrypt and pairs it with a stego image to mask the encrypted password for enhanced security.This security systems outperform strong steganalysis assaults like the chi-squared attack and the neighbourhood histogram when put to the test. This level of protection is suggested for future web apps that handle sensitive user data. Future work is required in the area of explicit passwords, as the attacker can guess the length of the password and hack it.

In 2018, Christy Atika Sari, Giovani Ardiansyah et al. [18] proposed this study. Based on the DWT issue, Huffman suggested code to decrease the total number of message bits leading to an increase in the capacity. In this process of implementation, the message is processed using AES, compressed using “Huffman coding” and then enveloped using DWT. After some experiments with 128 x 128-pixel news images and 512 x 512-pixel cover photos, they obtained an average value of MSE and PSNR as 1.5676 and 40 dB, or 46.1878. Huffman coding is slower than other methods because it uses two paths: building a statistical model and coding.

In 2018, Priya Paresh Bandekar and Sugana G C et al. [19] proposed the research where with the help of PSNR and MSE the efficiency of the algorithm is determined. Image quality will directly depend on PSNR value. They analysed PSNR and MSE of various images and generated graphs on the basis of this method in the MATLAB environment. They found that PSNR and MSE were inversely correlated when they drew the graph. The smaller MSE value will lead to smaller differences between the original image and the scrambled image, and vice versa. The pictures are excellent. The PSNR ratio is 45-50. MSE is near 01.70 dB and MSE is between 0 and 1. The future scope of this paper is the potential for improvements in audio steganography systems in relation to each technique for hiding audio data. Then apply a mixed approach to improve the procedure and combine different techniques to hide the data in the audio signal, making the system more secure to detection.

**Evaluation of image steganography for multiple image formats:**

The primary goal of this analysis is to see how different image formats i.e bitmap, png and jpeg work with different image steganography approaches.



It is observed that:

* The PNG image format has lower capacity and security.
* JPEG has the biggest payload capacity, but
* The BMP image format has a large storage capacity and is more secure.

**4. PROPOSED METHODS:**

**4.1 IMAGE STEGANOGRAPHY TECHNIQUES:**

To embed the confidential data into cover images following techniques are used:

**4.1.1 LSB:**

In the Least Significant Bit (LSB) system, secret messages are hidden in a cover bitmap image. Each character in the secret message and each pixel in the cover image are encoded to binary values. As a security measure, the user must enter the stego key. The resultant stego image is delivered to the recipient over the appropriate communication channel after the secret message is inserted into the cover image file. The stego key is first obtained from the user before defining a starting point for embedding the LSB. The stego key calculates the total of the ASCII values for each character and then the average character value is calculated. The initial LSB position is chosen based on the estimated mean of the entered stego key characters while data is inserted in the LSB of the cover image. The replacement process then continues until the secret message ends. To understand this, Think of a digital image as a 2D array of pixels. Each pixel contains a value depending on its type and depth. Consider the most commonly used modes — *RGB* and *RGBA*. The range of these values ​​is 0 to 255 (8-bit values).



 ***Figure 5:***  *Representation of Image as a 2D Array of RGB Pixels*

 We can use an ASCII table to convert a message to a decimal value and then to a binary value. The pixel values are then repeated one at a time, converted to binary, and each LSB is replaced with the message bit in the sequence. To decode the encoded image, just reverse the process. Collect and save the last bit of each pixel, divide them into 8 groups and convert them to ASCII characters to get the hidden message.



  ***Figure 6****: Working on LSB algorithm*

Assume we need to hide the "hello" message for a 4 x 4 image with the below pixel values:

"[(225, 12, 99),(155, 2, 50),(99, 51, 15),(15, 55, 22),(155, 61, 87),(63, 30, 17),(1, 55, 19),(99, 81, 66),(219, 77, 91),(69, 39, 50),(18, 200, 33),(25, 54, 190) ]"

You can use an ASCII table to convert a secret message to a decimal value and then to a binary value: 0110100 0110101. Now, we iterate through the pixel values one by one, converting them to binary and replacing each least significant bit with the message bits in order (for example, if 225 is 11100001, we replace the last bit with the first data bit (0), and so on). This increases or decreases the pixel value by +1 or 1, however it is entirely unnoticeable. The pixel values ​​obtained after running LSBS are:

[ (224, 13, 99), (154, 3, 50), (98, 50, 15), (15, 54, 23), (154, 61, 87),(63, 30, 17), (1, 55, 19), (99, 81, 66), (219, 77, 91), (69, 39, 50), (18, 200, 33), (25, 54, 190) ]

The hiding algorithm for the LSB system is -

**The embedding Algorithm for the sender:**

**1)** Receive input captions and secret messages.

**2)** Ask the user to enter the stego key and calculate its average value.

**3)** From the average stego key position, convert each character in the secret message and each LSB bit in the title image.

**4)** Cover image LSB bits are replaced with the secret message's binary value associated with the secret message's start and endpoints.

**5)** At the last of the secret message, the value of the end character is added.

**6)** *PSNR* and *SNR* value of original and the resulting image is evaluated

**7)** Stego image is to be delivered to the receiver.

**Extraction algorithm for Receiver:**

**1)** Ask for a stego key as input and then calculate its average value..

**2)** Stego image sent by the sender is loaded.

**3)** Each LSB bit is extracted from the stego image till the end bits are identified.

**4)** Reassemble the least significant bits obtained from the stego image,

**5)** Convert the LSB bit to the corresponding character.

**4.1.2 Masking and Filtering method:**

Masking and filtering are one of known encoding techniques. It is usually performed on 24-bit grayscale images. This process of masking images involves changing the luminance of the masked area. The smaller the variation in luminance the less likely it is to be detected.

The luminance of the masked area is enhanced by 15% to accomplish steganography within an image. To be undetectable by human sight, the luminance must be adjusted by a smaller percentage. Image is used to conceal plaintext or encoded data. In terms of compression, cropping, as well as some image processing, masking outperforms LSB insertion. Masking techniques encode data in key regions of the cover image, making the concealed message more integral to it rather than concealing it in the noise level.

**4.1.3 PVDS:**

Pixel Value Differencing Steganography (PVDS) is a technique that divides an image into several blocks, each of which consists of two consecutive pixels. The difference between two pixels is transferred to a specific range table to determine the number of bits to hide in the block. To decide the number of bits to hide in the block, the difference between the two pixels is mapped to a specific range table. PVDs that are both horizontally and vertically adaptable have been proposed. There are two different techniques in this. The image is divided into 2x2 pixel blocks in the first approach, and 3x3 pixel blocks in the second method. Each block's data is contained in both horizontal and vertical directions..



  ***Figure 7:*** *Embedding scheme of PVD*

**Embedding Algorithm for the sender:**

**1)** Sx and Sx+1 are the non-overlapping blocks’ two consecutive pixels.

**2)** The difference between two consecutive pixels has the value, d= |Sx+1 - Sx|. The small d value implies the pixel is in a smooth area, while a large value for d indicates that it is in an edge area. The value “d” belongs to the range Rn from the table where n varies from 1 to 6.

**3)** The number of bits to embed in the blocks is computed using the formula, b = log2(Un - Ln + 1) where Ln is the lower limit and Un is the upper limit of the Rn range. The secret binary data stream’s b bits of data are calculated as well as its decimal value bd is calculated.

**4)** After hiding this data in the block, d\* = bd + Ln is used to determine the new difference value.

**5)** Difference value m = |d\*- d|.

**6)** The equation below is used to determine the stego-pixel values ​​S'x and S'x+1. The ceiling value in this case is [m / 2] and the floor value of m /2 is [m / 2].

 

**Extraction algorithm for Receiver:**

**1)** S’x and S’x+1 are the two pixels of a block.

**2)** Calculate the difference value d\* = |Sx - S’x+1|, where d\* belongs to a range Rn, whose upper limit is Un and the lower limit is Ln. The range’s hiding capacity, b = log2 (Un – Ln + 1).

**3)** The data that is hidden is acquired by transforming the |d\* – Ln| to b binary bits.

| **Range (Rn)**  | **R1** | **R2** | **R3** | **R4** | **R5** | **R6** |
| --- | --- | --- | --- | --- | --- | --- |
| **(Ln,Un)** |  [0, 7] |  [8, 15]  | [16, 31] | [32, 63] | [64, 127]  | [128, 255] |
| **Capacity (b)**  | 3 | 3 | 4 | 5 | 6 | 7 |

***Table 1:*** *Range table*

**4.1.4 Edge-Based Steganography:**

Data is embedded in edge regions using this technique. Significant alterations in boundaries or texture areas can be noticeable by the human visual system. As a result, embedding a secret bit in the margin is more productive. To effectively identify edge regions, many edge detection methods such as Sobel, Fuzzy, Prewitt, Canny, Laplace, and Hybrid have been developed. The best edge is also determined by a number of additional factors, including the Gaussian kernel, the steepest descent, and threshold selection. In addition, the use of Huffman coding has significantly improved HC. In order to randomise the edge pixels and enhance ARA(attack resistance), a sorting table has been included.



 ***Figure 8:*** *Edge-based steganography architecture*

**4.2 ENCRYPTION ALGORITHMS:**

**4.2.1 AES:**

The *Advanced Encryption Standard* algorithm is a Symmetric Key Block Cipher used for providing security for sensitive data operation in 128-bit plain text. The key size is determined by the number of loops. For 128 bit keys 10 loops, 12 for 192-bit keys and 14 for 256-bit keys. This system’s operations are all byte-oriented. Here 16-byte 4x4 matrix is used to store the 128-bit plaintext. Sub Bytes, Row Shifts, Add keys, and Mix Columns are the most common operations used to encrypt data and produce ciphertext as output. Inverse Subbyte, InverseMix Column, InverseShift Rows, and Inverse S-box are used to decrypt data.



 ***Figure 9:*** *Encryption and decryption using AES*



***Figure 10:*** *AES Encryption*

The algorithm for the AES system is -

**The embedding Algorithm for the sender:**

**Step 1:** Conversion of sub-bytes

The Sub Byte is a replacement byte, which replaces each byte of the ciphertext in the standard lookup table of the s-box with 256 elements. The first hexadecimal value in bytes indicates the row index. The column index is indicated by the second hexadecimal value.

**Step 2:** Shifting of row transformations

Here, the matrix's rows are shifted to the left cyclically. Row 0 is not changed. Row 1 has been relocated to the left by one byte. Shifting in second and third rows is done by 2 and 3 bytes respectively.

**Step 3:** Mix Column Transformations

Multiplication of every column in the newly generated matrix with the columns present in the predefined matrix.

**Step 4:** Adding of Round Key

Xor-ed operation is performed on the resultant matrix and the extended keys that are generated from the first key.

**Extraction algorithm for Receiver:**

**Step 1:** Inverse Sub Bytes Conversion

To create a new matrix, each byte of the matrix is replaced with an inverse s-box table.

**Step 2:** InverseShift Row Transformation

Matrix’s rows are shifted to the right in a cyclic pattern.

**Step 3:** Inverse Mix Column Transformation

The opposite function to Mix Column Transformation.

**Step 4:** Add an Inverse Round-Key Conversion

The round keys should be chosen backwards in the state matrix and xored.

**4.2.2 RC5:**

RC5 is a Symmetric-key block algorithm used for encryption. Cypher text is generated here by execution of encryption to plain text.RC5 can be described by 3 integer values-”w”,”b” and “r” where w: Length of the word (in bits) b: Secret key’s length in bytes r: Total number of rounds

Allowable values ​​for w include 16-bit, 32-bit, and 64-bit, and b and r use values ​​from 1 to 255. It suits hardware and software and is fast and safe to run due to the different sizes of lock (32-bit, 64-bit, 128-bit).



***Figure 11:*** *Operation of the RC5 algorithm*

The algorithm for the RC5 system is -

**Embedding Algorithm for the sender:**

**Step 1:** Two words P and Q are retrieved by splitting the plaintext block in half. The first part of the plaintext block is X and the second part is Y.

**Step 2:** P = P + K[0]

**Step 3:** Q = Q + K[1]

" K[0], K[1],…,K[n] –> keys used in the rounds for encryption "

For n = 1 to p

**Step 4:** P = ((P xor Q) <<< Q) + K[2\*n]

**Step 5:** Q = ((Q xor P) <<< P) + K[2\*n + 1]

The final values of A and B after completing all the rounds is considered as the ciphertext block.

**Extraction algorithm for Receiver:**

For n = p to 1

**Step 1:** Q = (( Q - K[2\*n + 1]) >>>P)xor P

**Step 2:** P = ((P - K[2\*n]) >>> Q)xor Q

**Step 3:** Q = Q - K [1]

**Step 4:** P = P - K [0]

**Step 5:** After all rounds are completed, the plaintext is obtained by combining the values ​​with P and Q

**5. FUTURE SCOPE**

1. Enhancing the security and capacity of an image**:** Security and capacity sharing are fascinating issues in steganography. Increasing the limits has been shown to sacrifice some security. There have been few hypothetical studies to scientifically relate safety to limit parameters. A scientific model that combines the two key requirements of the steganography framework will improve the execution of future insertion computations, as well as computational improvements that provide both high security and constraints despite better steganography analysis. You can use it. It can provide numerical assumptions for advancing existing calculations for dynamic enthusiasm and execution. In any case, the hassle of displaying the de facto highlights of an image can hinder research productivity.
2. Development of algorithms that depend on objects in images**:** As steganography techniques become more sophisticated and most steganography calculations ultimately value their money, certain patterns create calculations that target specific parts of images for installation. These calculations are called steganography and are placed on the object. The main idea of ​​these calculations is to identify the zones (also known as regions of interest (ROI)) in the image. In this zone, the installation minimises distortion.
3. Most image steganography methods use both text or grayscale images as confidential information Further investigation is needed to hide the image Photo and video photos.
4. With experiments to optimise the parameters we can use different datasets to further reduce our storage capacity.
5. More attempts to designs on quantum pictures can be explored in the era of quantum computing approaches.
6. Efforts can be made in order to create a dataset that Contains images from various source cameras, and images format. Compiling all possible algorithms is also done to create a steganographic image.
7. Capacity, Security and robustness are considered in many ways, as performance benchmarks. However, Man-in-the-middle has an opportunity to Attack when the transmission is not a trusted channel Stay manipulation may also occur in transfer.Some of the designed algorithms can counter these attacks Along with other metrics for evaluation.

**6. CHALLENGES**

* Data Availability -There is no appropriate standard dataset for image steganography, despite the fact that it is an unsupervised learning job with the primary goal of image reconstruction.The majority of the techniques involve hiding RGB pictures within RGB cover images. It can be difficult to locate a sufficient dataset. The photos are relatively small, measuring 64 x 64 pixels.
* Other methods are compared - Because the evaluation metrics employed by different methods differ, comparing the suggested method to state-of-the-art methods is difficult.
* Steganography in real-time - Large datasets, such as the 45000 training photographs used, are used to train steganography models. When it comes to real-time steganography, difficulty increases. The trained model necessary for steganography and steganalysis requires the receiving end to provide the stego picture across an untrusted channel.The trained model's capacity to deal with real-time live images containing sounds, skewing, and blurring has yet to be verified.

**7. CONCLUSION**

Steganography is an addition to cryptography, not a replacement. Using steganography to encrypt and hide messages adds an extra degree of security and makes hidden messages less likely to be discovered. For the general public, steganography is still a relatively new notion, but not in the realm of secrecy and espionage. Copyright and ownership of digital content are now tracked via digital watermarking technologies. To ensure that watermarks and embedded information are safe from watermark assaults, efforts must be taken to strengthen the resilience of watermarks.With continuous advances in technology, more efficient and advanced web analytics technology is expected to emerge soon, which may help law enforcement agencies better detection of illegal material transmitted over the Internet.This paper describes some of the steganography techniques. Steganography is used to conceal more than just textual information in images. Steganography can be used with audio files, communication channels, and other text and binary files in addition to digital photographs.

The majority of classic steganography employs LSB replacements and variants. PVD, DCT, and EMD are typically employed in addition to the LSB. Limited ability to hide in traditional ways Overloading the cover image with more pixels to hide the secret message can cause distortion. Photo steganography is a type of image reconstruction that contains both cover images and secret data as input for producing a steganographic image that looks like the title image.

**8. REFERENCES**

[1] Xie, Jialiang, Honghui Wang, and Dongrui Wu. "Adaptive Image Steganography Using Fuzzy Enhancement and Grey Wolf Optimizer." *IEEE Transactions on Fuzzy Systems* (2022).

[2] Li, Fengyong, et al. "Ensemble Stego Selection for Enhancing Image Steganography." *IEEE Signal Processing Letters* 29 (2022): 702-706.

[3] Qin, Xinghong, et al. "Gradually Enhanced Adversarial Perturbations on Color Pixel Vectors for Image Steganography." *IEEE Transactions on Circuits and Systems for Video Technology* (2022).

[4] Sivaramakrishnan, Upasana, Namrata Panga, and G. K. Rajini. "Image Steganography based on Fractional Random Wavelet Transform and Arnold Transform with cryptanalysis." *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*. IEEE, 2021.

[5] Duan, Xintao, et al. "High-capacity image steganography based on improved FC-DenseNet." *IEEE Access* 8 (2020): 170174-170182.

[6] Thakur, A., G. S. Gill, and S. Saxena. "Analysis of Image Steganography Performance Check Using Bit Selection." *2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)*. IEEE, 2020.

[7] Kalaichelvi, T., and P. Apuroop. "Image Steganography Method to Achieve Confidentiality Using CAPTCHA for Authentication." *2020 5th International Conference on Communication and Electronics Systems (ICCES)*. IEEE, 2020.

[8] Elharrouss, Omar, Noor Almaadeed, and Somaya Al-Maadeed. "An image steganography approach based on k-least significant bits (k-LSB)." *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. IEEE, 2020.

[9] Ansari, Arshiya S., Mohammad S. Mohammadi, and Mohammad Tanvir Parvez. "A multiple-format steganography algorithm for color images." *IEEE Access* 8 (2020): 83926-83939.

[10] Sulaiman, Rahmat, et al. "RC4 Algorithm and Steganography to Double Secure Messages in Digital Image." *2020 8th International Conference on Cyber and IT Service Management (CITSM)*. IEEE, 2020.

[11] Subramanian, Nandhini, et al. "Image steganography: A review of the recent advances." *IEEE Access* (2021).

[12] Hossen, Md Sagar, et al. "A New Approach to Hiding Data in the Images Using Steganography Techniques Based on AES and RC5 Algorithm Cryptosystem." *2020 International Conference on Smart Electronics and Communication (ICOSEC)*. IEEE, 2020.

[13] Jayapandiyan, Jagan Raj, C. Kavitha, and K. Sakthivel. "Enhanced least significant bit replacement algorithm in spatial domain of steganography using character sequence optimization." *IEEE Access* 8 (2020): 136537-136545.

[14] Horng, Ji-hwei, Chih-Hung Lee, and Shan-Cheng Yang. "Image Steganography Using Contrast Enhancement Technique." *2019 8th International Conference on Innovation, Communication and Engineering (ICICE)*. IEEE, 2019.

[15] Hambouz, Ahmed, et al. "Achieving data integrity and confidentiality using image steganography and hashing techniques." *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)*. IEEE, 2019.

[16] Tang, Weixuan, et al. "CNN-based adversarial embedding for image steganography." *IEEE Transactions on Information Forensics and Security* 14.8 (2019): 2074-2087.

[17] Mogale, Hope, Michael Esiefarienrhe, and Lucia Letlonkane. "Web Authentication Security Using Image Steganography and AES Encryption." *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*. IEEE, 2018.

[18] Rachmawanto, Eko Hari. "An improved security and message capacity using AES and Huffman coding on image steganography." *TELKOMNIKA Telecommunication Computing Electronics and Control* 17.5 (2019): 2400-2409.

[19] Bandekar, Priya Paresh, and G. C. Suguna. "LSB Based Text and Image Steganography Using AES Algorithm." *2018 3rd International Conference on Communication and Electronics Systems (ICCES)*. IEEE, 2018.