



---

# Refining Medical Image Steganography Scheme Based on Pixels Disparity Value and Huffman Coding

---

Mohammed Ibrahim Mahdi\*

*\*Department of Computer Science, College of Computer Science and Information Technology, Wasit University, Al-Kut City, Wasit Governorate, Iraq.*

*Corresponding Email: \*mmahdi@uowasit.edu.iq*

**Received:** 18 May 2022

**Accepted:** 09 August 2022

**Published:** 24 September 2022

**Abstract:** *The steganography is a new and challenging method for transmitting confidential information over the internet utilizing a hidden cover object. Developing an efficient picture steganography system is currently fraught with difficulties because of the limited capacity, weak resilience, and imperceptibility of current steganography systems under development. This problem can only be solved by increasing the picture steganography's capability and security levels. Methods: Based on these variables, this work aims to present the state-of-the-art approach known as the Pixels Disparity Value (PDV) that hides patient information reports in the distinct medical photos for the second party. It's recommended that the procedure be broken down into three primary phases, each with its own set of instructions. Results: The statistical and economic evaluations of the suggested approach.*

**Keywords:** *Medical Images, Image Steganography, Huffman Coding, Security, Imperceptibility, Pixel Value.*

## 1. INTRODUCTION

Information dissemination is greatly facilitated by recent developments in computer technology. There has been such an exponential increase in the speed and ease with which material can be delivered, received, and disseminated over the internet. Non-secure networks have made it difficult to safeguard these digital files. (Hashim et al., 2020). Information encryption and information concealing have been suggested in the realm of security systems to solve the issue of information security. It is a procedure known as cryptography that scrambles secret messages to make them unreadable (encrypted) (Su et al., 2020). However, eavesdroppers may be drawn to an encrypted secret communication, which isn't necessarily a good thing. To avoid attracting the attention of a third party, invisible communication must be used instead. An information masking technique is required for this same reason.



Information hiding can be divided into two broad types, including steganography and watermarking (Taha *et al.*, 2021); both are used to hide secret Messages, Both approaches are related, but each has a different goal in mind. Watermarking is primarily intended to preserve the integrity of private data from eavesdroppers, with or without disguising the communication's existence. However, steganography hides the data that is to be sent and protects the material that is to be hidden (Hassaballah, Hameed and Alkinani, 2020).

Secret data or ordinary data may be hidden via steganography in non-secure medium, such as a picture. Dedicated research efforts over the past many decades have resulted in the development of reliable and secure Image Steganography Systems (Kadhim *et al.*, 2019). When it comes to image steganography, it's gaining in popularity since it's easy to send multimedia material via low-cost devices like smartphones and IP digital cameras and popular social networking apps like WhatsApp (Hussain *et al.*, 2018). Picture security and secret message concealment remain unresolved difficulties, as does comprehending the hidden data included in an image, among others (Hussain and Hussain, 2011).

Depending on the cover medium, many forms of information concealment techniques exist. To put it another way, sensitive information may be hidden in a variety of media, including images, audio, text, video, DNA, and even protocol. There are benefits and disadvantages to using each of these types of cover material (Karthikeyan *et al.*, 2019). Since of this, images are often employed as a cover material because they are simple to utilise, have a huge storage capacity, and are difficult to detect by an attacker (Qin *et al.*, 2019). Computer applications that employ networking channels and steganography are the most common use cases (Hashim, Mohsin and Rahim, 2019). Media that may be used to transmit data or text is known as an image, and this study focuses on medical equipment such as MRI and CT scanners, which employ this kind of media extensively (Zhang *et al.*, 2019).

For steganography systems to be successful, there are three elements that must be taken into consideration by developers. Existing steganography methods are likewise confronted with these three concerns. The hosting medium must be able to hold a significant amount of data in order to transport sensitive information, which brings us to the first point of contention: payload capacity. The second problem is one of security, in which the technique utilised must be capable of securely securing sensitive data. As a last consideration, steganography schemes' success is determined by their ability to remain undetected (embedded method). (Abd EL-Latif, Abd-El-Atty and Venegas-Andraca, 2019).

Keeping the image's imperceptibility as high as feasible poses the majority of the challenges for researchers in this area, which calls for the image holding secrets to be innocent while handling and mobility. The purpose of this study is to demonstrate that psychotherapy is just as important as traditional treatment and that keeping medical records hidden from patients and their companions is critical to protecting the treating physician's privacy. Because the globe has become a small village, international medical care is now commonplace, and it is necessary to provide the patient report in advance of making any decisions (Hashim, Mohsin and Rahim, 2019). Then, with the suggested study, you can send simply one specific image



that is included with all the details about the patient's situation. Numerous techniques already in use and those recommended in literature each have advantages and disadvantages. Finding a fresh approach that overcomes the drawbacks of existing approaches while gaining advantages is the challenge at hand. (Qin *et al.*, 2019).

Given the importance of medical images nowadays in a way that brought attention make handle this scope is necessary, the direction of the world now is to make an intelligent environment in terms of Artificial intelligence (AI) (Georges and Magdi, 2020), such as machine learning (Zou, Zhang and Liu, 2019). Same as Artificial Neural Network (ANN), which took much attention in the medical images, especially in MRI images (Liu *et al.*, 2020). Any field of science security is considered because it is essential to give life more confidence. Some areas get more attention insecurity in biometric, which is based 100% on security like fingerprint and face recognition. In our system, security is needed less than these fields (mentioned before). However, the proposed system is based on the data retrieval problem, a critical issue here (Reshma *et al.*, 2020).

This research makes use of a variety of medical imagery. A large number of datasets based on these photos may be found on the internet. The bulk of research in the literature has focused on cancer illness diagnosis and detection (Chatterjee *et al.*, 2020). There are two ways to think about security and privacy when it comes to the medical image: first, concealing information (Stoyanov and Stoyanov, 2020), and second, monitoring and recording (Abd-El-Atty *et al.*, 2020). To be successful, it must be taken into account that the findings must be kept online, which necessitates an extremely complex procedure.

The Pixels Disparity Value (PDV) is a state-of-the-art technology that hides patient information reports in the distinct medical photographs for the second party to access. We've devised a three-stage procedure for this project (data preprocessing, embedding, and extracting processes). Each level comprises a series of distinct actions that must be completed. According to the statistical and non-structural criteria, the suggested technique was assessed on a standard dataset of normal and medical photos for comparison. For the purpose of enhancing the system's resilience, the researchers looked at three primary factors: security, capacity, and imperceptibility. Proposed schemes were successfully thwarted by all known assaults on picture steganography systems. The results were better than prior efforts that were considered to be state-of-the art. The mathematical aspects of steganography will be explained in detail in the next sections.

## **Two Preliminaries**

### **Information hiding History**

The notion of masking information is older than the idea of communication and the internet itself (Abd EL-Latif, Abd-El-Atty and Venegas-Andraca, 2019). Watermarking is a second broad word for the first steganography discussed in this proposal. First, the message had to be delivered on foot, and then it had to be sent via mail, phone, and horse. In order to conceal a message, the messenger has two options: remember or hide the message (Sajedi and Yaghobi, 2020). Invisible ink was frequently utilized during World War II, although the extraction process was unique and difficult. Using fake ant devices, ultraviolet light is now used to read the invisible ink. Monk The modern founder's cryptography was used by Johannes Trithemius. This is regarded as the first effort to obfuscate sensitive information in the text

(Shah, Choudhari and Sivaraman, 2008). A stranger's secret message is hidden in the text as a pattern of characters using the Trithemius system, which also uses invocations of the names of angles. Think of this illustration:

(Padiel-aporsy-mesarpon-omeuas-peludyn-malpreaxo) able to elicit the word (Prymus-apex.) Germany utilized a specific method known as null cipher, which is considered an unencrypted transmission, during World War II to conceal sensitive information. Utilizing this method seemed very innocent from the outside. Due to the rapid advancement of the internet and communication, steganography developed quickly. One goal of such a suggestion is to maintain the rate of advancement in this field and conceal secret messages within a reliable system. (Hussain and Hussain, 2013).

### Terminologies in Steganography

Simmons (1984) recounted a narrative to help people grasp the fundamental concept of steganography (Simmons, 1984). Two convicts, Alice and Bob, attempted to communicate with each other in secret while their warden, Wendy, was looking on. Alice and Bob's connection was quickly cut off as soon as she became aware of it. To demonstrate the need of cryptography in the uncontrolled nations, the whereabouts of these two inmates was often used. By using steganographic processes in their ordinary talks, two countries may avoid any suspicion by relaying information without interference from a third party (such as the "warden").

An information theory framework for steganography based on the above-mentioned scenario is shown in Figure 1. (Manohar and Kumar, 2020). E and E are two processes that make up the mentioned framework (D). Right of the illustration shows the issuer who inserts a secret message (M) into an image file that appears on the cover (C). Sender and recipient are in the centre of Wendy's figure, where she seeks to intercept communications. Every so often, she manages to get a glimpse of the information being sent back and forth between the two of them. Only the intended recipient would be able to decipher the message since the distributed secret was shared by both the relay and the receiver. As a "key," this widely disseminated secret may be a method for acquiring the program's extraordinary variables."

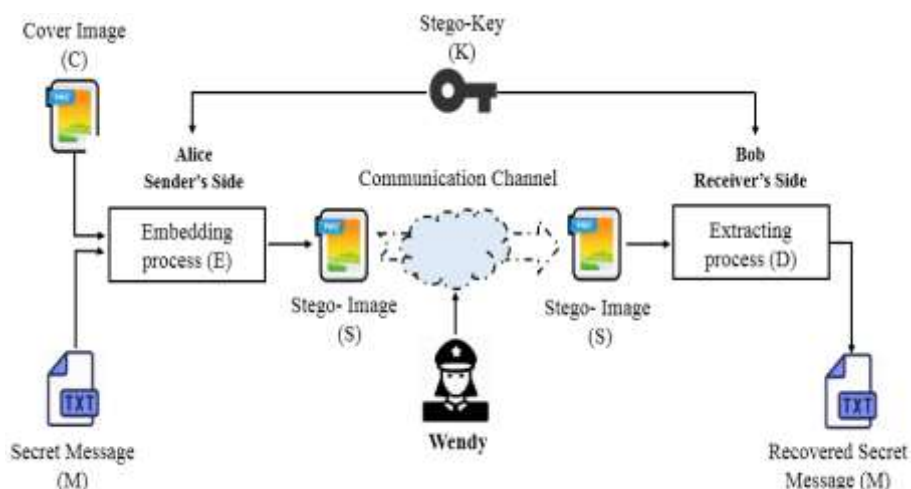


Figure 1. The basic concept of the steganography arrangement in its entirety



Mathematically, steganography can be represented as a quintuple (C, M; K, DK; E K), where C represents the set of cover media used during communication, M represents the set of all concealed messages that must be sent using the covers, and K represents a key selected from a collection of keys. Using a two-function steganography technique as an illustration, consider E K, which is responsible for embedding data and extracting it from the data, and D K, which is responsible for recovering data from the data embedded in the data (Das et al., 2021) [25]. Since the sensitive information was enclosed in a secret message (M), it was necessary to hide it explicitly. COVER MEDIA: These are the media that physically hide their message from the audience. It is a process for creating a secret file that is encrypted using a stego key (S), hence the name "operation" (E) (K). The cover media into which the hidden message is encoded and the hidden message itself are combined to form a S (stego file). Operation refers to the procedure of extracting the embedded data from the stego file (D). The step connecting the stages for attaching the message to the cover's interior and extracting the same message from the stego file is identified by the stego key (K). In its entirety, steganography is the act of concealing sensitive data within different types of media (C) in order to produce a stego file (S) via a stego key (K) when the transmission is complete. Using steganography, the recipient can also access the hidden message (M).

### **Embedding Domains of Image Steganography**

The embedding domains in the steganography systems can be categorized into three classes depending on the hosting places and nature of the embedding process. These include the spatial, frequency, and adaptive domains. The adaptive domain is essentially interlinked to the spatial and transform domain, where each of these categories has its advantages and disadvantages. The main differences between these domains are listed in Table 1. (Kadhim *et al.*, 2019) (Hussain *et al.*, 2018) [6,5]. The sections that follow provide a brief explanation of these domain-based embedding procedures' main features.

Table 1. The spatial, transform, and adaptive domain-based embedding techniques are compared.

Characteristics	Properties	Domains		
		Spatial	Frequency	Adaptive
System type	Complexity	Simple	Complex	It depends on the adaptive algorithm
Pixel Manipulation	Embedding	Direct	Indirect (transformed coefficient)	It depends on adaptive technique
Embedding Capacity	Payload	High payload	Limited payload	Varied payload
Visual Quality	Imperceptibility	High	Less controllable	Highly controllable
Robustness	Compression, Noise, Cropping,	Highly prone	Less prone	It depends on the adaptive algorithm

	Rotating, Filtering			
Security	Attacks	Vulnerable to attacks	Resistant to attacks	Hard to attacks
Statistical detection Attacks/ analysis	RS, Histogram	Easy detect	Hard to expose/unsuccessful	Hard to expose/unsuccessful

### Dataset

The system was trained using the USC-SIPI dataset, which contains the digital photographs (SIPI Image Database, no date). The selection of this dataset is intended to support research in image processing, image analysis, and vision analysis (SIPI Image Database, no date). Depending on the primary characteristic of its image, this dataset has already been divided into volumes. The proposed research for color images used the Lena, Tiffany, Baboon, and Peppers with a dimension of 512 by 512, as shown in Figure 2. These photographs were also utilized to compare the experimental result to the previous one in order to evaluate it. These pictures were chosen from the previously employed USC-SIPI dataset (SIPI Image Database, no date).

Data from a separate medical imaging dataset was used to evaluate the method's performance (Retrieve, no date). Specialist physicians can decipher a wealth of information included in the medical photos. Even from other specialists, a doctor may need to keep certain information private for a specific reason. All of the necessary information may be hidden inside the picture using our approach, and the stego key is all that is needed to extract it.

Typically, the medical picture is scanned and converted into a two-dimensional or three-dimensional image. 3D photographs provide the impression of depth, but 2D images don't. Figure 3 shows medical pictures utilised to test the system, as opposed to the 2D image.



Tiffany



Baboon



Lena



Peppers

Figure 2: The standard SIPI dataset used in the proposed framework

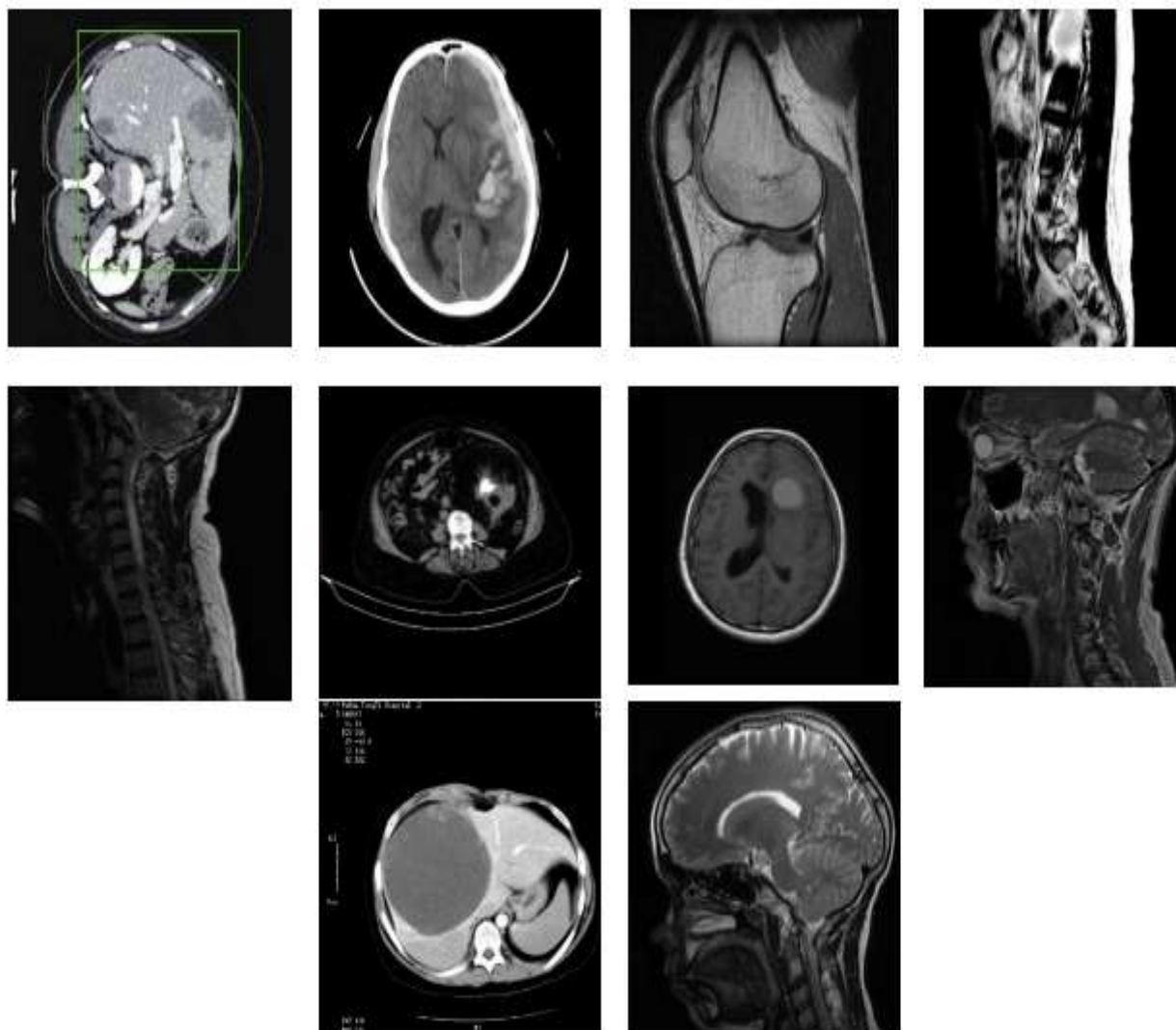


Figure 3. Medical images used in the system performance evaluation



## 2.5 Related Methods of Image Steganography

This section provides a quick summary of the various classic image steganography techniques that have been developed over the years for secure data transfer via the WWW. Additionally, the key characteristics of all image steganography frameworks are provided. Table 2 lists a number of current studies on steganography in terms of capacity and matching PSNR..

Table 2. Different studies in image steganography in terms of capacity and PSNR.

References	Method	Performance
(Muhammad et al., 2016)	LSB - MLEA: Multi-level encryption is applied on stego-key as well as secret data.	> 45dB 1BPP
(Rajendran and Doraipandian, 2017)	LSB: CM LSB approach that makes use of an ISS based on a chaotic map. The hidden bits embedding is based on the created chaotic sequence, which is constructed using a 1-D logistic map.	44.53 dB 2 BPP
(Nyeem, 2017)	Histogram and bit plane A histogram-shifting-based embedding method is applied to each histogram bin independently, depending on the bitplane values.	40 dB 5.0 BPP (High EP)
(Setiadi and Jumanto, 2018)	LSB is an acronym for the term "edge area." Detectors from Canny and Sobel are coupled in order to boost the payload capacity.	50.21 dB 1.03 BPP
(Swain, 2018)	PVD: PVD method with 1×2-pixel blocks in an overlapped fashion	42.96 dB 2.96 BPP
(Sahu and Swain, 2019)	To improve the peak signal-to-noise ratio (PSNR), the PVD-MF ISS uses modulus function (PVD) and modulus function (PVD) to insert payloads (EP).	42.04 dB 1.5 BPP
(Mukherjee et al., 2020)	PVD: This is a disparity between the pixel values of pixels that are encrypted and randomly selected.	41.59 dB 2.94 BPP
(ALabaichi, Al-Dabbas and Salih, 2020)	LSB: Using 3D chaotic maps, such as 3D Chebyshev and 3D logistic maps, to create the least significant bit-based secret map strategies.	46.15 dB 1.0 BPP
(Seyyedi, Sadau and	Wavelet coefficients and RC4 encryption	65.9 dB





Ivanov, 2016)		0.5 BPP
(Islam, Roy and Laskar, 2018)	The cover image is divided into three levels using LWT, and then randomized into non-overlapping blocks of size 2 x 2. On the LWT coefficient component, binary data are incorporated after being encrypted.	43.8 dB 512 bits
(Jude Hemanth et al., 2018)	A modified version of the genetic algorithm (GA) using frequency-domain methods is used for QR embedding.	60.29 dB 0.5 BPP
(Kadhim et al., 2019)	Edge-based image: An adaptive embedding procedure was employed to optimise the Dual-Tree (DT-CWT) subband coefficients using machine learning-based optimization methods.	53.71 dB 1.9 BPP
(Jude Hemanth et al., 2018)	There are three consecutive steps in the method: image segmentation (IS), pixel complexity identification, and content adaptive steganography (CAS) (PCI).	50.98 dB 1.0 BPP

In the above literature table, various approaches have proposed hiding information within an image to improve the imperceptibility (PSNR), each with advantages and disadvantages. In order to summarise the better methods in terms of imperceptibility, (Muhammad et al., 2016) (Rajendran and Doraipandian, 2017) (Swain, 2018) (Sahu and Swain, 2019) have the current achievement in terms of PSNR as mention before, but this achievement is still an un-optimal result because still there is noising inside the stego image compared to the original image. With 65.25 and 66.23 dB, (Seyyedi, Sadau and Ivanov, 2016) achieved a better PSNR. Payload capacity has been altered (low capacity) to improve PSNR and security. By Jude Hemanth et al. in 2018, frequency domain and Genetic Algorithm (GA) methods have been suggested. However, despite the improved PSNR, this approach has a limited payload capacity of 16384 bytes, making it vulnerable to statistical attacks such as the Chi-square attack. In this case, the PSNR is 60.09 and the SSIM is 0.9876.

In order to hide a secret message in a media file such as an image, video, or audio file, the maximum payload capacity is the maximum size of the secret message. As a result, increasing the payload capacity is a worthwhile objective. Therefore, the goal of an effective picture steganographic system is to communicate as much data as possible with the least amount of cover media, or pixels, possible. The steganography process would fail if this limit was exceeded, resulting in noticeable modifications in the multimedia file (Kadhim et al., 2019). When it comes to steganography, the data hiding ratio (DHR) is used to determine how much data is hidden in the original medium (Su et al., 2020). Payload capacity is measured in terms of Bits Per Pixel (Bpp), bytes, and percentage (percent). Table 5 indicates payload capacities ranging from low (Hussain et al., 2018) to moderate (Kadhim et al., 2019) to high.

## 2. METHODOLOGY

Here is a visual representation of the approach that is put forward in this paper, along with a list of its primary components. This visual depiction of the framework explains the originality of the framework in more detail, allowing readers to have a better understanding of our process. For example, the suggested method-based steganography differs from existing steganography techniques in that it may enable strong security while keeping a high level of quality of picture at a cheap cost and suitable payload. Electronic-Patient-Records (EPR) and other private communications requiring confidentiality may benefit greatly from the work given here, since it can be used to securely transmit those bits (Hussain and Hussain, 2013). Providing a visual representation of the suggested solution.

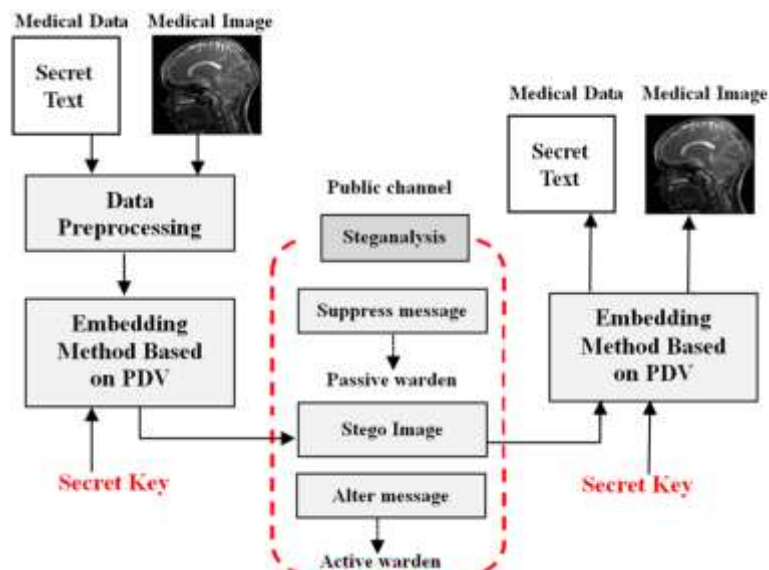


Figure 4. The proposed scheme overall flow

### Data preprocessing

The most crucial step in the suggested stenography system to increase the payload and security of the secret communication is preprocessing. As a result, two crucial steps—including creating the cover image and secret message coincide.

### Enhanced Huffman compression coding

The secret message is preprocessed in two stages: text compression and secret text fragmentation. An additional degree of security is provided by preprocessing the secret message in the proposed approach. This is in addition to increasing the payload space. The three most important qualities of any picture steganography system are: maximal payload storage, excellent imperceptibility (the visual quality of the image after embedding), and resilience (Sahu and Swain, 2019). Consequently, the suggested steganography scheme's increased Huffman compression coding ensured that these elements would be achieved. It is the primary objective of the Huffman coding technique to minimise the text size before embedding it into the picture. Short paths in the Huffman tree are given to frequently

occurring letters in this process using Huffman's algorithm. Using the Huffman coding approach, text repetition (redundancy) may be reduced.

AAAAAAAAAAAAAAAAA BBBBBBBBBBB CCCCCCC	➔	15A,10B,7C
---	---	------------

Figure 5. The text frequency (redundancy) reduction within the Huffman coding

The suggested approach includes a numerical example to help clarify concepts. In this case, five distinct symbols were used, and the result was:

Symbol	S	T	E	G	O
Frequency	22	10	8	6	6

To form the first branch's tree structure, the "G" and "O" frequencies were used, followed by the "E" and "T" frequencies at the same frequency. The frequency of these two parent nodes was 12 and 18, respectively; in the tree, the frequency of each parent node is added together. Finally, both children in one parent were linked by the frequency 22 of the high-frequency letter "S," which was formed at a high level to build the final tree. The standard Huffman coding tree topology is seen in the following figure.

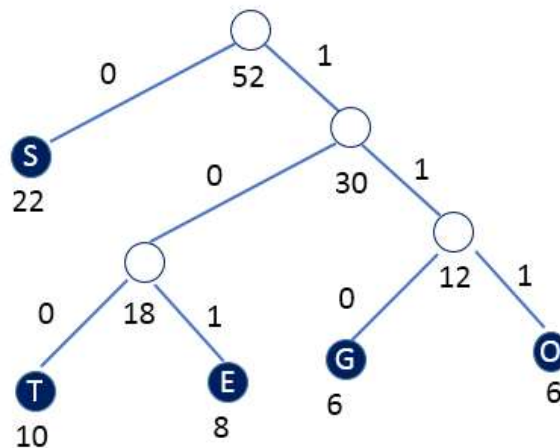


Figure 9. Huffman coding tree

If the same frequency of letters appeared as shown below, it was lowered and the compression deleted 41% from the original text for this example.

Symbol	S	T	E	G	O
Frequency	22	10	8	6	6
Track code	0	100	101	110	111
Length	1	3	3	3	3

Fragmenting the bit stream is an important step in the production of secret messages. Using the Huffman coding method, the resulting text was transformed into binary 0 and 1 numbers.



The embedding stage data length influenced how bits streams were processed at the processing step of the data stream. To protect the integrity of the scheme, these bits were tampered with prior to embedding. To put it another way, the bit stream sample used in the embedding process was compatible with the bit stream sample used in the sampling phase.

### B. Image Pre-processing

Image preparation is a pre-processing step used before the embedding procedure to ensure an effective embedding of the proposed scheme. Image normalisation and image transformation decomposition methods are explained in the following sections.

### Image Normalization Technique

Before performing any action on the picture, this pre-processing step included selecting and analysing it. Before the rest of the processing, the picture was normalised to a certain range (Shah, Choudhari and Sivaraman, 2008). When it came time to design the cover, we decided to stick with the standard steganography format of using images with a maximum resolution of at least 512x512 pixels:

$I_N = (I - \text{Min}) \frac{\text{new Max} - \text{new Min}}{\text{Max} - \text{Min}} + \text{new Min}$	
---	--

where I represents the original picture, I N represents the normalised image, Max represents the image's maximum dynamic range, and Min represents its lowest dynamic range.

### Decomposition Technique for Image Transformation

Using the Fibonacci decomposition approach, the secret data was made more resilient and effective (Abd EL-Latif, Abd-El-Atty and Venegas-Andraca, 2019). To keep things simple, the cover graphic used an 8-bit bitplane. As a result, it was easy to incorporate the stego picture due to the execution of the Fibonacci decomposition, which turned it logically into the 12-bitplanes. Each bitplane of the binary presentation was influenced by  $2^k$ , where k signified the bitplane order (for example, k=3 for the bitplane number 3, k=7 for the bitplane number 7 and so on), and so on. For the binary representation, Table 2 shows how each layer influences the overall result.

Table 2. Impact of each binary bitplane into the whole image

Bitplane No.	1	2	3	4	5	6	7	8
Impact value on image luminance	1	2	4	8	16	32	64	128

Because the LSB in the 12-bitplane embedding was more effective and reliable than the 8-bitplane embedding, there was a significant difference between the (binary representation) 8-bitplane and the (Fibonacci representation) 12-bitplane in the embedding process. Figure 10 illustrates how these two bitplanes differ from one another.

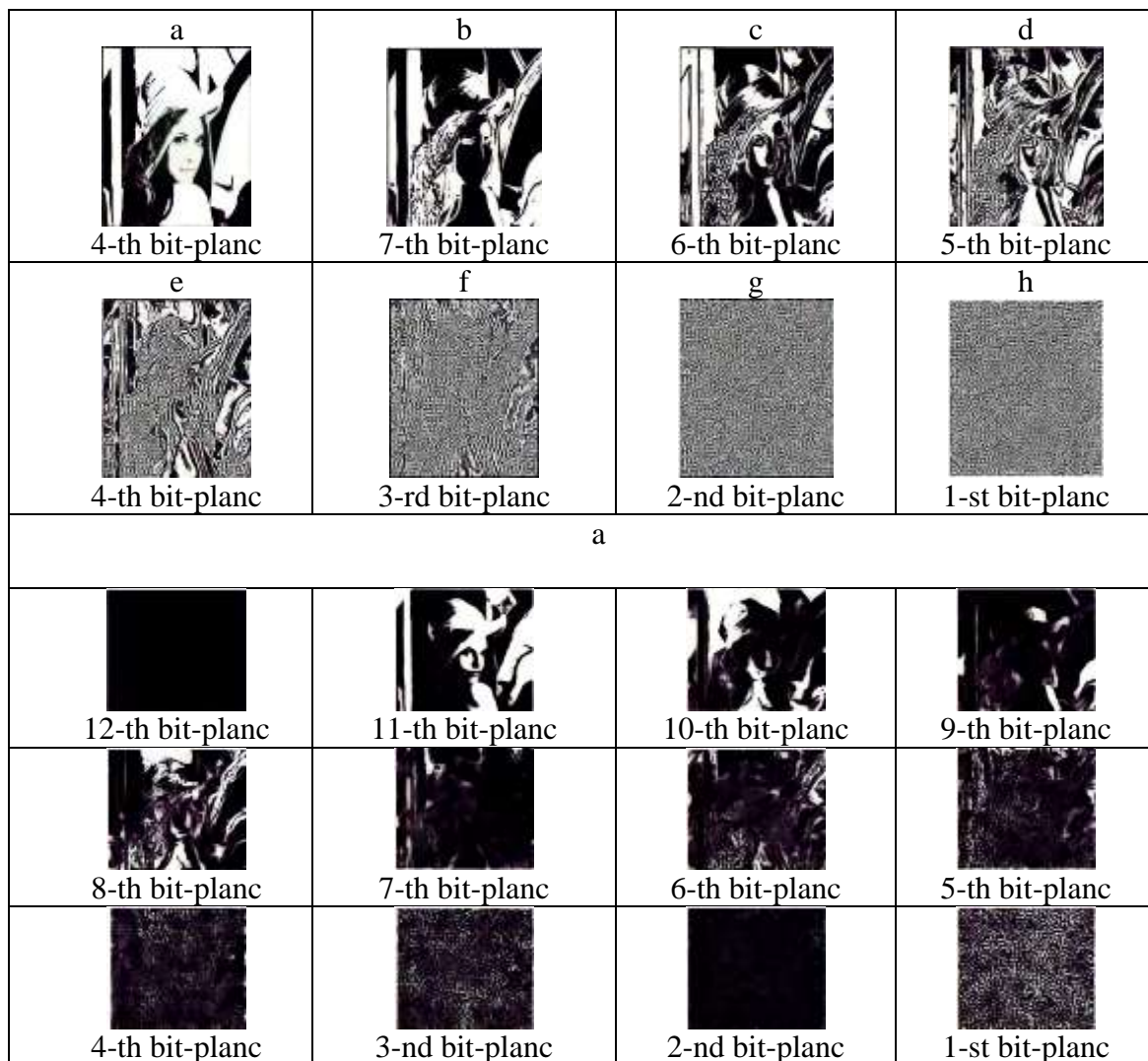


Figure 7. Lena image in the proposed PDV method with the decomposition of (a) 8-bitplane and (b) 12-bitplane.

By employing Zeckendorf's theorem, we were able to demonstrate how to convert any decimal pixel value into its Fibonacci representation using the Fibonacci series (Thomas, 2015):

$$F_1 = 1, F_2 = 1, F_3 = 1 + 1 = 2, F_4 = 2 + 1 = 3, F_5 = 3 + 2 = 5 \dots, F_n = F_{n-1} + F_{n-2}$$

In general, the Fibonacci theory can be summarized as:

$F(n) = \begin{cases} 0 & \text{if } n = 0 \\ 1 & \text{if } n = 1 \\ F(n-1) + F(n-2) & \text{if } n > 1 \end{cases}$	
---	--

The algorithm below is shown the steps for achieving the Fibonacci number sequence.

**Input:** An integer n for n-th Fibonacci number.

**Output:** n-th Fibonacci number.

FN[0]←0







FN[1]←1

**for** i←2 to n-1 **do**

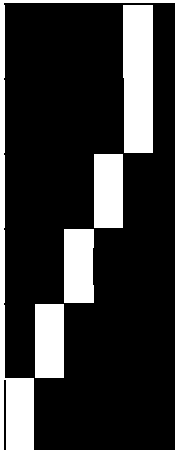





The Fibonacci decomposition was used mainly for three important reasons:  
The Fibonacci decomposition improvement led to better security because it was more difficult for an attacker to estimate the secret data.  
Due to the usage of 12 bit-planes, the system's robustness was strengthened.  
Due to the varied data, it was challenging to identify using the visual attack.

### 3.2 Embedding Method Based on Pixel Disparity Value (PDV)






Using random pixel selection using two settings, the secret message may be buried in the cover photo. Techniques for hiding hidden messages in images and transmitting them undetected to the intended receiver are a key purpose of steganography, which is described in this paper.

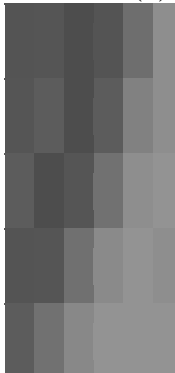




	5 7	57	57	61	87	12 0
	5 7	57	59	72	10 6	12 3
	5 9	59	64	90	12 2	12 4
	6 1	64	89	11 7	12 4	12 4
	6 8	89	11 4	12 5	12 4	12 4
	8 9	11 4	12 8	12 5	12 5	12 5

(a) Local image and pixel value

	0	0	0	0	25 5	0
	0	0	0	0	25 5	0
	0	0	0	25 5	0	0
	0	0	25 5	0	0	0
	0	25 5	0	0	0	0
	25 5	0	0	0	0	0

(b) Edge image and pixel value

	0	0	0	61	87	12 0
	0	0	0	72	10 6	12 3
	0	0	64	90	12 2	0
	0	64	89	11 7	0	0
	6 8	89	11 4	0	0	0

	63	65	57	61	87	12 0
	64	68	59	72	10 6	12 3
	68	59	64	90	12 2	12 4
	61	64	89	11 7	12 4	12 1
	68	89	11 4	12 5	12 4	12 4

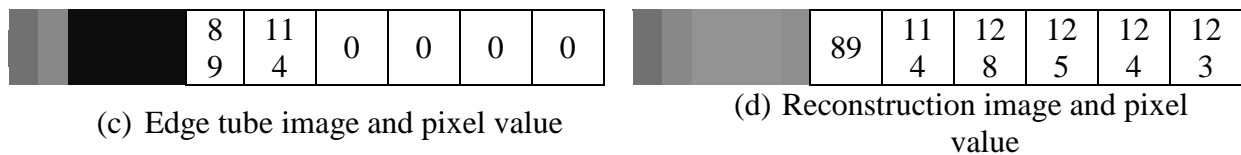


Figure 8. Location of the contrast value with the corresponding pixel value

The contrast or lighting of a pixel is represented by decimal values in a colour or grayscale picture. The grayscale image contains a single decimal value between 0 and 255 (expressed in binary as 28 occupies 8 bits), where 0 represents a black pixel and 255 represents a white pixel. The grayscale picture starts off white and ends up black.. Even when switching between images with lower and higher contrast, it's easy to see distinctions at the object's borders and bounds. Using decimal representations, Figure 8 depicts the contrast area. Figure 8 (a) shows the transition from low contrast at the top left corner to high contrast at the bottom right corner in a gradual transition. Figure 8 shows the optimum spot to hide the hidden message due to the little differences between each pair (d). Around 30-pixel contrast differences are easily discernible by the human eye. Insertion in such a region, on the other hand, often varies as widely as two-pixel values.

Each pixel in the colour picture has three values: Red, Green, and Blue (RGB). Each colour channel is represented by a single byte in the 24-bit (3-byte) representation of these pixels. Because of the ability to leap across these three bytes, the embedment in such a region is versatile. Consequently, comparing three-pixel values in a colour picture is more difficult than in a grey image, since three channels must be verified for embedment. To conceal the secret, the system must meet the pixel embedment criterion. To alter the colour image's contrast, check three values per pixel until you locate the one that has the secret key for the effect you want. It is difficult to place a fraction in one of the three channels because of the numerous requirements it must meet. Thresholding becomes vital when the critical condition calls for a strong embedding strategy to handle it.

During the embedding step, both the block selection and data embedding procedures were carried out concurrently in order to insert or conceal text into a chosen cover picture (grey or RGB colour). Two steps of image division will be used to accomplish security; the first will split the cover picture into 64 sub-images called blocks. Figure 9 illustrates a potential approach for selecting blocks and pixels for a stego picture; these methods for selecting blocks and pixels are depicted in Figure 9. To provide security, the random function is used. It's possible to discover these numbers with a chance of 250 by using a single random parameter on a regular basis; the beginning condition for this function (single). Henon's map function receives 1030 attempts, resulting in roughly 2100, which is sufficient to protect the image's text.

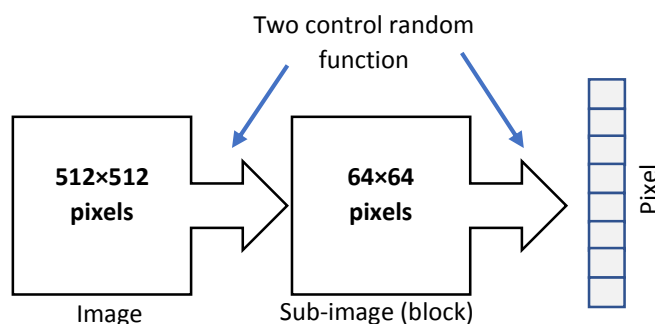


Figure 9. Selection blocks and pixels with the proposed method

Two control settings are used to select the pixels for two stages of the randomization procedure to increase the difficulty (block and pixel selection). Hackers are prevented from interpreting our message from a stego picture by security in the steganography procedure. This makes it almost tough to find a concealed message.

An example of a dynamic function system whose behavior is shown to be chaotic is the Henon map function. The two control parameters for the classical function are  $A=1.4$  and  $A=0.3$ , which make it chaotic. The main variables that control this function are  $A$  and  $b$ , and it can be graphically represented as the coordinate point  $(X_n, Y_n)$  in the plane. Additionally, this equation provides some novel results:

$$\begin{cases} x_{n+1} = 1 - a x_n^2 + y_n \\ y_{n+1} = b x_n \end{cases}$$

Any embedding approach utilises a two-pixel selection and pixel insertion mechanism, as previously indicated. For the system's improved security and imperceptibility, the pixel selection is responsible. Maintaining these two criteria was the primary goal of the current investigation. Two phases of pixel selection were required.

$P(x-1, y+1)$ <b>5</b>	$P(x, y+1)$ <b>6</b>	$P(x+1, y+1)$ <b>7</b>
$P(x-1, y)$ <b>4</b>	<b><math>P(x, y)</math></b>	$P(x+1, y)$ <b>0</b>
<b>3</b> $P(x-1, y-1)$	<b>2</b> $P(x, y-1)$	<b>1</b> $P(x+1, y-1)$

Figure10. The eight neighbors' pixel movement strategy

Movement around the picture was done using a single movement method in the first step. The second step was to ensure that the system was ready to be embedded. Once one step was





complete, the other could begin. A vector was created by adding all of the chosen pixels together. After the selection process was complete, the pixels were randomly rearranged using the new random approach, but the index for each pixel remained intact throughout. The method of the eight neighbours was based on a single requirement relating to the contrast value of the picture. Figure 10 depicts the movement of these eight neighbours across the picture in all three planes (vertical, horizontal, and diagonal).

If you increase or decrease one of these pixels' x- and/or-y coordinates, you may move the pixel to any other place in the picture matrix in any direction. Center and surrounding pixels (x,y) were used to compare in the suggested method. When the threshold was exceeded, the location of a pixel was recorded in vector form and subsequently moved. Alternatively, it was shifted to the next available pixel location. A four-decimal-point difference between two pixels, for example, would place the hidden bit in two adjacent pixels next to the original pixel, as would a three-decimal-point difference. That's why we had to place our pixel somewhere between an area with a high and low level contrast, so that our secret bit could be embedded in that region. As seen in Figure 11, for example, if the secret bit was 0, the secret bit was either embedded with the high value or otherwise (secret bit 1) with the low contrast value. Using the pixel-by-pixel contrast level checks, we were able to scan the whole picture and choose the best place (pixel) to conceal the hidden bit. The suggested steganography strategy proved to be a success when this technology achieved great invisibility and high security. Additionally, the pixel replacement method must be used in conjunction with the pixel selection strategy in order to improve the data concealing algorithm's imperceptibility and security even further.

### **Extracting method based on Pixel Disparity Value (PDV)**

For both security and concealment, the embedding and removing steps were successful. When extracting LSB pixels, the primary goal is to recover the embedded data (secret bits) and concurrently follow the technique specified for embedding pixels. The agreement between the sender and recipient is responsible for the vast majority of information connected to extraction. The remainder of the information is dependent on image nature and surroundings and is deemed changeable information by the implicit stego key. Only a small portion of the secret message is represented in the picture and block partitioning of variable information. A portion of this information is deemed public knowledge, whereas the embedding process itself is considered private knowledge in this context. Figure 12 shows the planned ISS's embedding and extraction procedures.

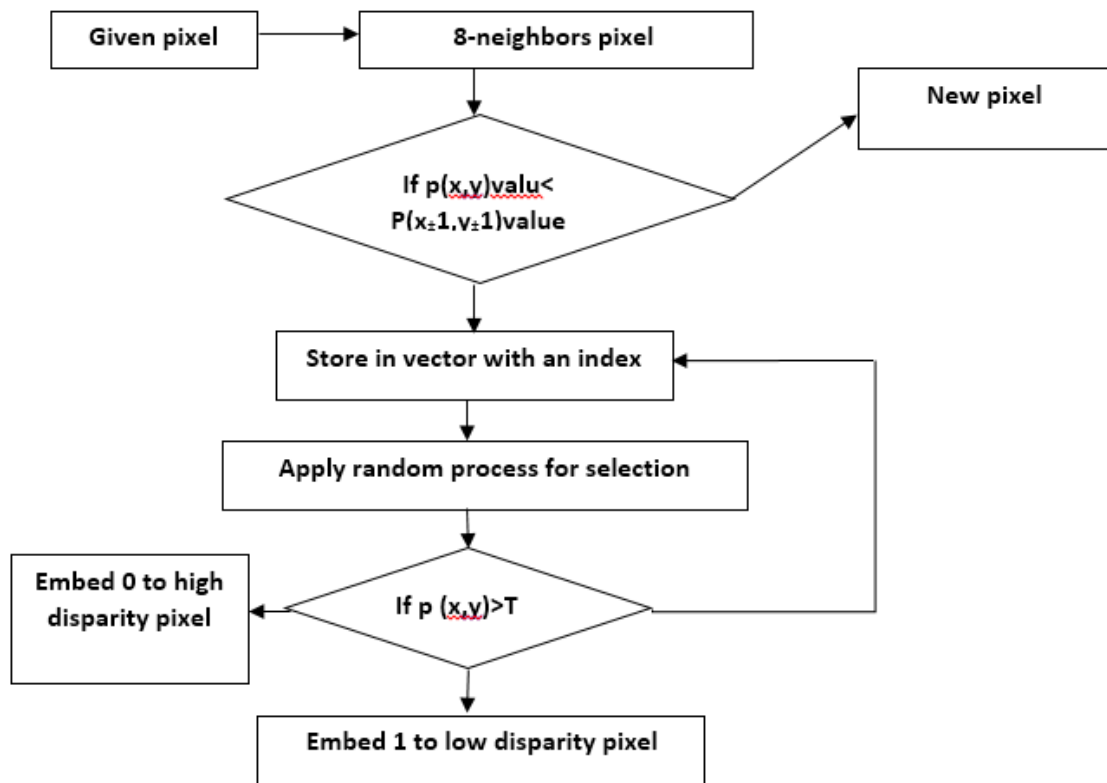


Figure 11. The proposed embedding strategy

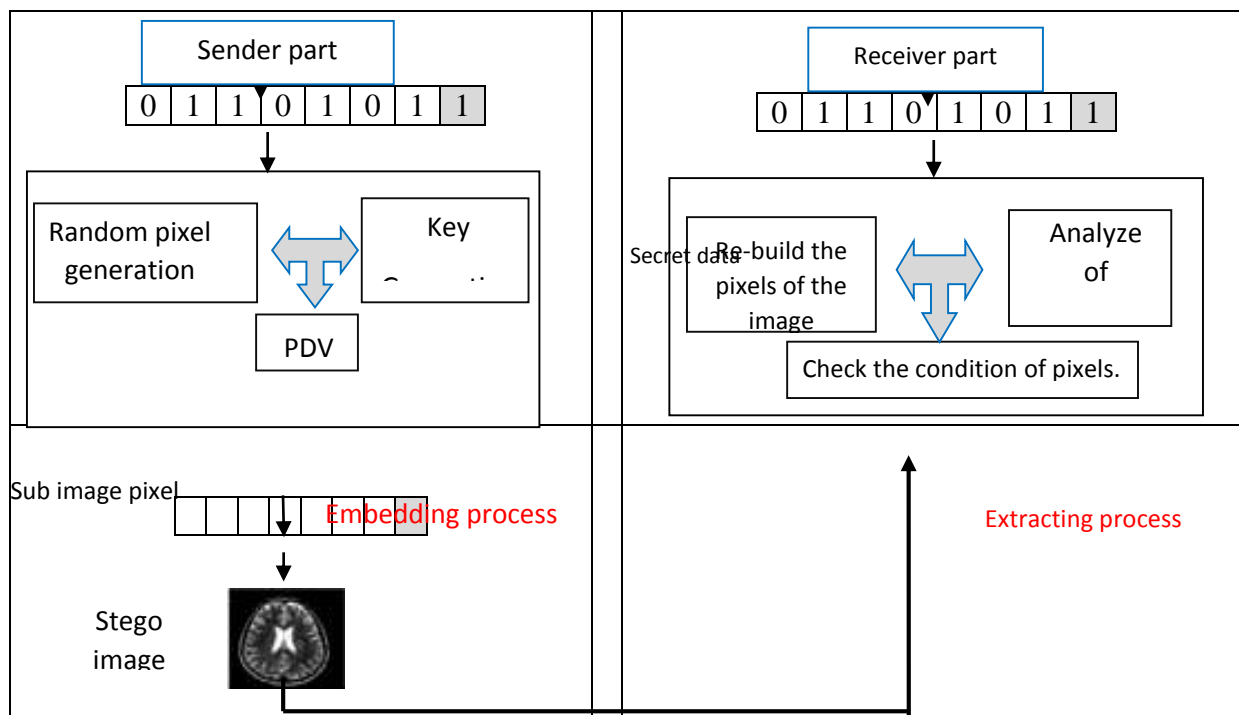


Figure 12. The imperceptibility and security design of the proposed scheme



Images were kept as clear and imperceptible as feasible by embedding and extracting steps. Moreover, the proposed scheme's security was reflected in the joint work of two processes, such as picture partitioning and randomization in block and pixels selection.

### Performance Analysis

If you're looking for an information-hiding system, you'll want one that doesn't raise any suspicions about what's going on within. A pre-sent review of the stego picture is necessary, as well as a comparison with current approaches. For our system, the University of Southern California used a SIPI-dataset made up of grey pictures (SIPI Image Database, no date) and other medical image data from the U.S. National Library of Medicine. It's possible for a specialised doctor to explain medical photos, but for a specific goal, it's necessary for the doctor to conceal certain facts. Here, we play an important role since we can hide all the necessary information in a picture and then extract it effortlessly if the stego key is present. As shown in Figure 3, a scanning device may provide a 2D or 3D picture, depending on how the image is processed.

Among the objective techniques utilized to evaluate the suggested ISS were the embedding capacity (EC), peak signal to noise ratio (PSNR), and structural similarity index (SI). The suggested system's EC value is directly proportional to the amount of pixels used, which can be thought of as the ratio of message bits to cover pixels. (Kadhim and others, 2019) Each pixel included an array of message bits, and the EC is shown as follows (Stoyanov & Stoyanov, 2020)

$$EC = \frac{\text{The number of message bits}}{\text{The number of cover images' pixels}}$$

The following parameters were used in the simulation:

16384 bytes amount to 6.25 percent of a 512x512 pixel picture, which means that every second pixel represents 16 bits. Hence,  $1/16 = 6.25$  percent when a single pixel from two pixels was integrated.

A comparison of the original and stego picture quality was conducted using PSNR following the embedding procedure. In the case of a 512x512 pixel picture, 12.5 percent of 32768 bytes corresponded to the assumption that each pixel was equivalent to 8 bits, meaning that  $1/8 = 12.5$  percent of 32768 bytes was embedded. When 1.5 bits of one pixel are encoded, 49152 bytes represent 18.75 percent of a 512x512-pixel picture. This means that every second pixel was allocated to 16 bits, therefore  $3/16 = 18.75$  percent. HVS judged data embedding to be undetectable when the PSNR was less than 30 decibels) (Hussain et al., 2018). When determining PSNR, the following formula was used: (Abd-El-Atty et al., 2020):

$$PSNR = 10 \cdot \log_{10} \left( \frac{255^2}{MSE} \right) \quad (4.5)$$

with

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2 \quad (4.6)$$

In this equation, MAX represents the image's greatest pixel value, while I and K represent the image's original and noisy pixels, respectively.



Thus, the value of SSIM was utilised to quantify the similarity between the original picture and the stego image (Kadhim et al., 2019). To get at the SSIM value (which varied from -1 to 1, with 1 indicating that there was no difference between the original and stego images) (Hussain and Hussain, 2013):

$$SSIM = \frac{(2P_O Q_S + C_1)(2\sigma_{OS} + C_2)}{(P_O^2 + Q_S^2 + C_1)(\sigma_O^2 + \sigma_S^2 + C_2)} \quad (4.7)$$

Assume that P (O), P O<sup>2</sup>, and "O"<sup>2</sup> represent the mean pixel value, variance, and standard deviation of the original picture, and that Q S represents the stego image. An picture's covariance with a stego image is represented mathematically by the symbol \_OS. Assuming the grayscale picture has a colour depth of 25, the constants C 1 and C 2 are C 1 = L1L and C 2 k1L.

the three embedding types (simple LSB and PDV) utilised to test the performance of the proposed technique with varied EP for the colour standard SIPI pictures (Lena, Baboon (512512)) are shown in tables 4, 5, and 6 respectively) show the acquired PSNR values

Table 4 shows the results.

Color Baboon picture PSNR values were measured using three distinct embedding methods with varying EPs.

Embedding %	PSNR (dB)	
	Simple LSB	Proposed scheme
6.26 %	59.911	70.081
12.6 %	57.819	68.408
18.85 %	55.998	67.846

Table 5. The values of PSNR for the color Lena image were obtained using three types of embedding with different EP.

Embedding %	PSNR (dB)	
	Simple LSB	Proposed scheme
6.26 %	57.011	67.435
12.6 %	54.988	65.530
18.85 %	54.898	64.221

Table 6. The values of PSNR for the color Tiffany image were obtained using three types of embedding with different EP.

Embedding %	PSNR (dB)	
	Simple LSB	Proposed scheme
6.26 %	57.989	69.286
12.6 %	56.988	67.454

18.85 %	54.349	65.919
---------	--------	--------

PSNR values for colour pictures are often lower than those for grayscale images because colour pixels are represented with 24-bits for one pixel instead of 8-bits for the grayscale pixels.


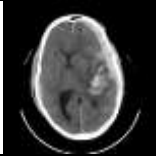

Different amounts of Embedding Percentage (EP) have been used to test the imperceptibility and efficiency of the diverse stego images, as shown in Figures 3,4, and 5. Table 7. displays the results for the standard color (Lina, Baboon, and Tiffany(512×512)) images.








Table 7 : Different evaluation tools with different amounts of EP for color images.

Lina	6.22%	13.5%	18.85%
	SSIM	SSIM	SSIM
	1	1	0.9899
Baboon	6.13%	12.5%	18.85%
	SSIM	SSIM	SSIM
	1	0.9899	0.9898
Tiffany	6.13%	12.6%	18.85%
	SSIM	SSIM	SSIM
	1	1	0.9899

Additionally, medical photos were gathered to assess how well the suggested technique worked with the SIPI standard image collection. Table 8 shows the evaluation settings used to assess the system's performance in the test images.

Table 8 Test medical images used to evaluate the performance of the system

Medical image	EP %	PSNR (dB)	SSIM
	6.26%	66.31	0.9899
	6.26%	65.21	0.9899
	6.26%	67.23	1

	6.26%	66.43	0.9899
	6.26%	66.97	1
	6.26%	64.54	0.9899
	6.26%	65.52	0.9899
	6.26%	63.55	0.9899
	6.26%	66.10	0.9899
	6.26%	66.62	0.9899

### 3. CONCLUSIONS

Researchers in this research have developed a picture steganography approach based on the Pixels Disparity Value (PDV) to keep private patient data hidden from a third party. This novel strategy was shown to increase the security level and payload capacity to tackle the current difficulties. Data was compressed before embedding using the upgraded Huffman coding method. Before it was hidden, modified secret data was utilised to promote the improvement of security and capability. According to the findings of other investigations, different payload capacities were used in this investigation. With the use of PSNR measurements, the plan aimed for greater imperceptibility in order to fend off the onslaught. The results reveal improved PSNR values, proving the validity of the strategy presented.



There will be enhanced security and strong imperceptibility due to the higher complications of pixels allocation and the replacement of bits.

#### **4. REFERENCES**

1. Abd-El-Atty, B. et al. (2020) ‘A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based E-healthcare platforms’, *Sensors*, 20(11), p. 3108.
2. Abd EL-Latif, A. A., Abd-El-Atty, B. and Venegas-Andraca, S. E. (2019) ‘A novel image steganography technique based on quantum substitution boxes’, *Optics & Laser Technology*, 116, pp. 92–102.
3. ALabaichi, A., Al-Dabbas, M. A. A. and Salih, A. (2020) ‘Image steganography using least significant bit and secret map techniques.’, *International Journal of Electrical & Computer Engineering* (2088-8708), 10.
4. Chatterjee, S. et al. (2020) ‘Logarithm similarity measure based automatic esophageal cancer detection using discrete wavelet transform’, in *Recent Trends and Advances in Artificial Intelligence and Internet of Things*. Springer, pp. 427–453.
5. Das, A. et al. (2021) ‘Multi-Image Steganography Using Deep Neural Networks’, arXiv preprint arXiv:2101.00350.
6. Georges, J. and Magdi, D. A. (2020) ‘Using Artificial Intelligence Approaches for Image Steganography: A Review’, in *Internet of Things—Applications and Future*. Springer, pp. 239–247.
7. Hashim, M. M. et al. (2020) ‘Based on IoT Healthcare Application for Medical Data Authentication: Towards A New Secure Framework Using Steganography’, in *IOP Conference Series: Materials Science and Engineering*. IOP Publishing, p. 012120. doi: 10.1088/1757-899X/881/1/012120.
8. Hashim, M. M., Mohsin, A. K. and Rahim, M. S. M. (2019) ‘All-encompassing Review of Biometric Information Protection in Fingerprints Based Steganography’, in *Proceedings of the 2019 3rd International Symposium on Computer Science and Intelligent Control*, pp. 1–8.
9. Hassaballah, M., Hameed, M. A. and Alkinani, M. H. (2020) ‘Introduction to digital image steganography’, in *Digital Media Steganography*. Elsevier, pp. 1–15.
10. Hussain, M. et al. (2018) ‘Image steganography in spatial domain: A survey’, *Signal Processing: Image Communication*, 65, pp. 46–66.
11. Hussain, Mehdi and Hussain, M (2011) ‘Embedding data in edge boundaries with high PSNR’, in *2011 7th International Conference on Emerging Technologies*. IEEE, pp. 1–6.
12. Hussain, Mehdi and Hussain, Mureed (2013) ‘A survey of image steganography techniques’.
13. Islam, M., Roy, A. and Laskar, R. H. (2018) ‘Neural network based robust image watermarking technique in LWT domain’, *Journal of Intelligent & Fuzzy Systems*, 34(3), pp. 1691–1700.
14. Jude Hemanth, D. et al. (2018) ‘A modified genetic algorithm for performance improvement of transform based image steganography systems’, *Journal of Intelligent*



- and Fuzzy Systems, 35(1), pp. 197–209. doi: 10.3233/JIFS-169580.
15. Kadhim, I. J. et al. (2019) ‘Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research’, *Neurocomputing*, 335, pp. 299–326.
  16. Karthikeyan, B. et al. (2019) ‘Authentication of Secret Message using Rabin-Karp in Image Steganography’, in 2019 International Conference on Intelligent Computing and Control Systems (ICCS). IEEE, pp. 388–391.
  17. Liu, J. et al. (2020) ‘Recent advances of image steganography with generative adversarial networks’, *IEEE Access*, 8, pp. 60575–60597.
  18. Manohar, N. and Kumar, P. V. (2020) ‘Data Encryption & Decryption Using Steganography’, in 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE, pp. 697–702.
  19. Muhammad, K. et al. (2016) ‘A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image’, *Multimedia Tools and Applications*, 75(22), pp. 14867–14893.
  20. Mukherjee, N. et al. (2020) ‘A PVD based high capacity steganography algorithm with embedding in non-sequential position’, *Multimedia Tools and Applications*, pp. 1–31.
  21. Nyeem, H. (2017) ‘Reversible data hiding with image bit-plane slicing’, in 2017 20th International Conference of Computer and Information Technology (ICCIT). IEEE, pp. 1–6.
  22. Qin, J. et al. (2019) ‘Coverless image steganography: a survey’, *IEEE Access*, 7, pp. 171372–171394.
  23. Rajendran, S. and Doraipandian, M. (2017) ‘Chaotic map based random image steganography using LSB technique’, *International Journal of Network Security*, 19(4), pp. 593–598. doi: 10.6633/IJNS.201707.19(4).12.
  24. Reshma, V. K. et al. (2020) ‘Optimized support vector neural network and contourlet transform for image steganography’, *Evolutionary Intelligence*, pp. 1–17.
  25. Retrieve (no date). Available at: <https://www.nlm.nih.gov/>.
  26. Sahu, A. K. and Swain, G. (2019) ‘An Optimal Information Hiding Approach Based on Pixel Value Differencing and Modulus Function’, *Wireless Personal Communications*, 108(1), pp. 159–174. doi: 10.1007/s11277-019-06393-z.
  27. Sajedi, H. and Yaghobi, S. R. (2020) ‘Information hiding methods for E-Healthcare’, *Smart health*, 15, p. 100104.
  28. Setiadi, D. R. I. M. and Jumanto, J. (2018) ‘An enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel edge detection’, *Cybernetics and Information Technologies*, 18(2), pp. 74–88. doi: 10.2478/cait-2018-0029.
  29. Seyyedi, S. A., Sadau, V. and Ivanov, N. (2016) ‘A secure steganography method based on integer lifting wavelet transform’, *International Journal of Network Security*, 18(1), pp. 124–132.
  30. Shah, P., Choudhari, P. and Sivaraman, S. (2008) ‘Adaptive wavelet packet based audio steganography using data history’, in 2008 IEEE Region 10 and the Third international Conference on Industrial and Information Systems. IEEE, pp. 1–5.
  31. Simmons, G. J. (1984) ‘The Prisoners’ Problem and the Subliminal Channel’, *Advances in Cryptology*, Springer-Verlag, pp. 51–67.
  32. SIPI Image Database (no date). Available at: <https://sipi.usc.edu/database/database.php>.





33. Stoyanov, Bozhidar and Stoyanov, Borislav (2020) 'BOOST: Medical image steganography using nuclear spin generator', *Entropy*, 22(5), p. 501.
34. Su, W. et al. (2020) 'Image steganography with symmetric embedding using Gaussian Markov random field model', *IEEE Transactions on Circuits and Systems for Video Technology*, 31(3), pp. 1001–1015.
35. Swain, G. (2018) 'Adaptive and non-adaptive PVD steganography using overlapped pixel blocks', *Arabian Journal for Science and Engineering*, 43(12), pp. 7549–7562.
36. Taha, M. S. et al. (2021) 'A Steganography Embedding Method Based on P single/P double and Huffman Coding', in 2021 3rd International Cyber Resilience Conference (CRC). IEEE, pp. 1–6.
37. Thomas, E. (2015) 'The Fibonacci Sequence Through a Different Lens'.
38. Zhang, J. et al. (2019) 'Binary image steganography based on joint distortion measurement', *Journal of Visual Communication and Image Representation*, 58, pp. 600–605.
39. Zou, Y., Zhang, G. and Liu, L. (2019) 'Research on image steganography analysis based on deep learning', *Journal of Visual Communication and Image Representation*, 60, pp. 266–275.