International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Efficient Data Security through Visual Security and Stegnography Schemes

Narendrababu Thumati[1,*], Kavitha Chaduvula[2]

Submitted: 10/09/2022 **Accepted:** 20/12/2022

Abstract: In this paper an information preservation upgrade framework is proposed for secure correspondence depending on reversible information covering through encoded pictures with reserve room method. This was actualized on real RGB picture under hold room method for multi scale disintegration. The Blue color was selected for concealing secure content information. The picture is diffused into local blocks and discrete wavelet is utilized to identify the estimation of gritty coefficients. The estimation part is scrambled by utilizing chaos based encryption technique. The suggested encryption system uses keys for image encoding in addition to improving the security of data bearer confidentiality by making the data challenging to access for any gatecrasher with an arbitrary technique. After encrypting the image, the information hider will disguise a mystery data into an itemized coefficient which are held prior to encryption. Despite encryption accomplishes certain safety impacts, it makes the mystery informations muddled and insignificant. The framework is as further improved with encoded messages by utilizing a symmetrical key technique. That is why our safety method is also known as reverse information covering. The art of secret correspondence involves hiding the current information in another medium. The method of information concealment uses flexible LSB calculations to hide a secret data bits in jumbled image. The mysterious data is removed in an information recovery setup by using the appropriate key to select the encoded pixel and separate the information. By utilizing the decoding key, the picture and extricated content info will be removed from encryption to get a first data. At last the effectiveness of the proposed encryption and information concealing method is examined dependent on picture and information recuperation.

Keywords: *Lifting wavelet transform, Reversible data hiding, Adaptive LSB replacement, Chaos encryption*.

1. Introduction

Reverse information stowing away is a procedure where real picture can be recouped with no misfortune after the implanted messages are recuperated. This strategy is broadly utilized in communicating confidential information in army, investigate organization, Medical data insurance. Here information and the first spread picture will be recuperated with no misfortune.

In [1] Kalker and Willems presented a recursive code to overcome the disadvantages of Reversible Data Hiding that does not arrive at the normal limits. In [2] Zhang improved recursive code development by planning an information implanting for every one of the zero-covers and a progressively productive compression method to arrives at the normal limit. In [3] Tian's contrast development procedure is a famous reverse technique for information inserting. In this strategy the repetition in computerized pictures is enhanced so as to accomplish high inserting limit, and keeps the twisting low.

The above technique experiences some unwanted contortion at low inserting limit. To defeat the above issue, in [4] Thodi presented a strategy called Prediction-mistake enhancement. This new system utilizes the connection inalienable in the near area pixel than the distinction enhancement method. To overcome the downsides of PEE [5] Zeng and Yang examined the PEE and two new methodologies called, versatile inserting and pixel development. In contrast to conventional PEE, which included consistent information, they are committed to converting 1 or 2 bits into extensible pixels in accordance with the local complexity. By lowering the greatest adjustment of pixel values, this reduces embed

[1] Research Scholar, JNTUK, Kakinada, Andhra Pradesh, India.
[2] Professor and Head, Department of IT, GEC, Gudlavalleru, Andhra Pradesh, India. Email: kavithachaduvula12@gmail.com
[*] *Corresponding Author Email*: tnarendrababuthumati.com

effect by removing growing pixels with significant forecast errors.

In [6], Zeng developed a dynamic compressed resolution method which packs the scrambled picture logically in resolutions, with the end goal that decoder can watch a low-goals adaptation of picture. This makes it possible to speculatively and hesitantly recognize good exhibition. A sizable percentage of pre-characterized pixels in Zhang's research had their three LSBs inverted. [7] Separated an encoded picture into blocks, each of which carries one component. Analyzing the square smoothness can help with information extraction and picture recovery. The spatial connection in the decoded image can be used to recognize this process. Chen and Hong [8] in determining the smoothness of each square, Zhang's technique did not totally abuse pixels, nor did it take into account the pixel associations on the edges of nearby squares. These two issues could make information extraction less accurate, but this approach uses a side coordinate plan to additional lower rate of improperly eliminated bits and provides a better method for determining the smoothing of squares. The test results show that the suggested method outperforms Zhang's approach in terms of execution. The information extraction in the previous two procedures relies on the picture being decoded, however Zhang suggested a strategy in [9] where the picture is encrypted to use a key by the content owner. Using an information concealing key, an information hider enshroud the information in an encoded image to obtain a space needed to conceal an information. Decoding a photograph at the beneficiary's end, information can be recovered using the information-concealing key.

Two techniques are utilized to clear the room after scrambling. Since entropy of scrambled pictures has been boosted, [8]-[9] to create stamped picture with low quality for huge payload. But the encryption key decodes the unaltered encoded image. A collector who possesses both an encryption and data concealment keys can access an installed information as seen in first image. In [10], Zhang and Kede Ma scramble a picture after inserting some bits' LSB into other bits using the conventional RDH approach to free up space. Information may then be installed in the positions of these LSB in an encoded picture. This rest of a paper is sorted out as below. The past strategies proposed in [8]–[9] are introduced in section II. An epic technique is explained in Section III pursued by conclusion part in Section IV.

2. Previous Works

Strategies presented in [8]-[9] is condensed as the system. In [8] by determining the smoothness of each block, Zhang's approach did not entirely abuse pixels, and it showed little consideration for the pixels connected to the edges of neighboring blocks. Even these two problems would diminish a genuineness of information extraction this strategy embraces a superior plan for estimating the block smoothness, and uses the side-matching plan to further diminish the mistake pace of extricated pixels. Trial results uncover that presented technique offers best execution over Zhang's work. Within the two strategies, information extraction relies upon picture unscrambling yet in [9], Zhang adopted a strategy, in that picture is encoded via substance proprietor thru utilizing scrambling key. Information hider can conceal information in the scrambled picture to acquire the space to shroud the information by utilizing information concealing key. By decoding a picture, data on the given the fact can be recovered using a key that conceals information. Over two strategies are utilized to "clear the room after encryption. Be that as it may, since an entropy of scrambled pictures has been augmented, [8]-[9] or produce a checked image with a low quality for a heavy payload. Using an encryption key, a photograph that has been encoded but left unaltered can be decoded. A beneficiary who has both an information and encryption covering up keys can get to an information inserted just as a first picture. In [10], Using a conventional RDH method, Kede Ma and Zhang first generate space by implanting the LSBs of particular pixels into various pixels. When inserting information into an encoded picture, they then mix the image locations of these LSBs.

3. Proposed Method

Task suggests improvement of insurance framework for mystery information correspondence over scrambled information covering in encoded pictures with save room method. A safeguard of a picture quality during picture recuperation, holding room approach is utilized to save space for implanting the security instant messages. Here, turmoil encryption is utilized to scramble a picture aside from saved space to make insurance of picture subtleties during transmission. After an encryption, an information hider will cover a scrambled mystery information into saved coefficients utilizing versatile LSB substitution calculation. At long last, picture and shrouded content will be recuperated with no misfortune based same strategies which are utilized at inserting stage.

3.1. Introduction to Wavelet

Within the past couple of years, wavelet change has reached greater than before, acknowledgment in sign preparing by and large and in picture pressure inquire about specifically. In applications like still photo compression, discrete wavelets change (DWT) [11] based plans outperform others like ones dependent on DCT. Since the information picture might have various lengths and there is no compelling reason to divide it into non-covering 2-D squares, wavelet coding schemes at larger pressure proportions avoid blocking artefacts. Wavelet coding schemes are particularly well suited for applications where adaptability and allowed debasement

are crucial due to their inherent multi goal nature. A new picture coding standard called JPEG-2000, which is based on DWT, was just released by the JPEG board of trustees.

Since Fourier Transform (FT) is inappropriate for such signals, we mostly employ Wavelet Transform (WT) to examine non stationary signals, or signals whose recurrent reaction changes over time. Short Time Fourier Transform (STFT) was proposed in order to circumvent the limitations of FT. Between STFT and FT, there is barely any difference. In STFT, the sign is broken up into tiny pieces, which can be thought of as stationary "parcels" of the sign. Because of this, a window work "w" is selected. This window of time should be as wide as the area of the sign that can still be seen as stationary. By using STFT, one can obtain a sign's simultaneous time-recurrence reaction, which is not possible with FT.

For a real continuous signal in time domain, the Fourier transform is distinct as:

$$X(f, t) = \int_{-\infty}^{\infty}[x(t)w(t-\tau)*]e^{-2j\pi ft}dt \qquad (1)$$

We receive various recurrence reactions of the sign sections when the window's length is (t- τ) in time, to the extent that can move a window by altering the estimation of t and by shifting a value of. The problem with STFT is made clear by the Heisenberg vulnerability rule. This guideline states that it is impossible to determine the precise time-recurrence representation of a sign, i.e., to understand what horrifying portions are present at what time. Goals issues are this specific category of problem. The width of the window work being used, sometimes referred to as the help of the window, is the issue at hand. If the window capacity is restricted, the window is said to as minimally bolster. The time objectives are better, the suspicion that the sign is stationary is better, and the recurrence goals are more unfortunate the smaller the window is:

- Thin window ===> great time goals, poor recurrence goals
- Wide window ===> great recurrence goals, poor time goals

The wavelet transformation (WT) was advanced as an alternative to STFT in order to solve the goals problem. When performing a wavelet analysis, it is done until the point where a sign is enhanced by wavelet work, much as how the window work in a STFT increases a sign. Change is calculated individually for various time-space signal components at various frequencies. This method is known as Multi-goals Analysis (MRA) [4] because it analyses a sign at different frequencies with altered goals.

At high frequencies, MRA is designed to provide great time objectives but poor recurrence goals, while at low frequencies, great recurrence goals but bad time goals. This strategy works especially well for signs like photographs and video summaries that include high recurrence segments for short times and low recurrence segments for long terms. The wavelet Ψ (t) change involves projecting a symbol onto all of a mother wavelet's decrypted and extended variations. In order to examine the nature of the wavelet change first, the precise meaning of a mother wavelet will be handled future. Expect the free necessity that t has limited, ethereal assistance up until this point (restricted by the vulnerability rule clearly), at which point a collection of important capacities can be identified. To insert messages in a pixel coefficients of the various sub bands, LWT degrades the image into LL, LH, HL, and HH pictures, namely. Use the lifting plan procedure to change DWT coefficients to Integer coefficients without erasing data. The major component of the spatial space image is included in the LL sub bands.

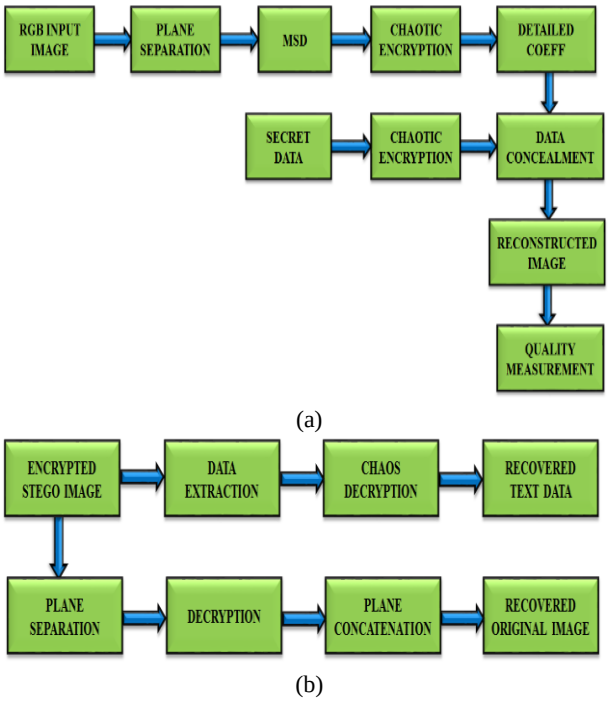


Fig. 1: (a) Framework: "Reserving the room for embedding and the image is encrypted" **(b)** Framework: "Decryption for recovering the original image and data extraction".

The edge data of the picture is contained in high-recurrence sub bands. The proposed framework for encryption and decryption is depicted in Figure 1. These coefficients were selected as the holding area for the content information. Given that the mystery content information is not sensitive to the human visual system, it is incorporated into a wavelet coefficients of high recurrence sub bands. The following are examples of how the mother wavelet, or essential wavelet, is formed from a set of wavelets:

$$\Psi_{ab}(t)=\frac{1}{\sqrt{a}}\Psi\left(\frac{t-b}{a}\right) \qquad (2)$$

In order for the variable "a" (frequency inversion) to produce high frequency and low frequency, respectively, it mirrors the width of a particular premises capacity. The x-interpretation axis's in time is determined by the variable "b." For standardization, the phrase 1/a is used.

3.2. 2-D Transform

1 dimensional DWT can be stretched out to 2 dimensional transformations by utilizing distinguishable wavelet channels. With detachable channels, applying a 1 dimensional transformation to every row of the input and rehashing on the column to estimate the 2 dimensional transformations. Four transformation coefficient sets are created when a level 2 DWT is coupled to the input. The four sets are shown in Figure 2(c) as LL, HL, LH, and HH, where first letter indicates whether a row or column had a low pass or high pass channel applied, and second letter indicates whether a channels had been applied.

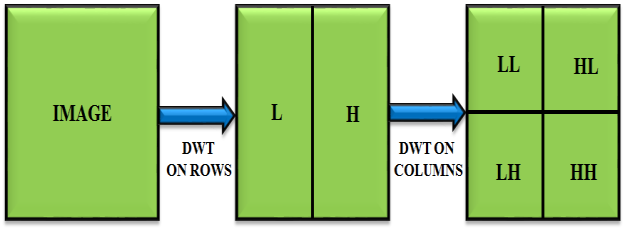


Fig. 2: Block Diagram of DWT **(a)** Original Image **(b)** Output image following the application of a 1-D to a row of input **(c)** Output image following the application of a second 1-D to a row of input.

Images are transformed from spatial space to frequency domain using two dimensions DWT. Each image column is initially converted using a 1D vertical investigation channel bank at each wavelet deterioration level. Each row of the channeled and sub inspected information is connected to a similar channel on a level plane. The four channeled and sub tested images produced by one level of wavelet decay are referred to as sub groups. The LP and HP coefficients following vertical 1 Dimensional DWT and sub inspection are discussed in detail in the top and lower sections of Figure 2(b), correspondingly. Figure 2 displays the results of the flat 1D DWT and sub testing to produce a 2D DWT yield image (c). The various wavelet transform degrees can be utilized to pack information vitality in the groupings that have been least studied. In specifically, a two-level wavelet change can be delivered by modifying the LL sub band in Figure. 3(c) to form the LL2, HL2, LH2, and HH2 sub groups. The R goals levels 0 and (R-1) correspond to the coarsest and best goals, respectively, and the (R-1) level wavelet decay is related to these levels.

More memory and extremely complicated calculations are required for the direct convolutional execution of 1dimensional DWT. An optional use of the one-dimensional DWT, known as the lifting plan, results in a notable reduction in memory usage and calculation unpredictability. Additionally, lifting enables the initial calculation of the wavelet coefficients.

3.2.1. 2-D transforms hierarchy

By using a secondary wavelet filter, 1-D wavelet change can be stretched to a 2-D wavelet change, as shown in Figure 3. By first applying a 1dimensional change to each row of data and then rehashing the majority of the column, one may estimate the 2dimensional change with separate filter.

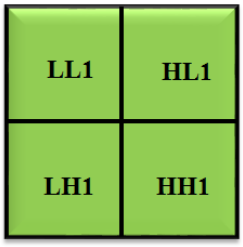


Fig. 3: A 2-D Wavelet Transform with one level and a Sub bands Labeling Scheme

3.3. Lifting wavelet computation

It is crucial to get rid of any superfluous calculations in order to complete a wavelet computation successfully. A careful analysis of the forward and reverse transformations reveals that a significant number of the jobs either cause information to be lost or are invalid tasks. (as multiplied by 0). The 1-D wavelet transformation is approximated by separately employing two inquiry channels at alternating even and odd places. A reverse procedure repeats the length of each sign by embedding zero in each spot before applying the appropriate amalgamation channel to each flag and adding the sifting sign to produce the final turn around transformation.

3.3.1. Forward Transform

$$H= (Co-Ce); L= (Ce+H/2) \quad (3)$$

The odd column and even column pixel values are designated as Co and Ce, respectively.

Step 1: Processing each column separately to produce H and L

Step 2: Processing row by row to obtain LL, LH, HL, and HH, Separate rows of H and L that are odd and even. Specifically, Hodd is an odd row of H, Lodd is an odd row of L, Leven is an even row of L and Heven is an even row of H.

LH = Lodd-Leven; LL = Leven + (LH / 2)

HH = Hodd – Heven; HL = Heven + (HH /2)

3.3.2. Reverse Lifting method

The reverse lifting method is used to generate the opposite integer wavelet transformation. Similar to forward lifting, the procedure.

3.4. Image Encryption

One of the encryption schemes that has been advocated for use in image encryption for safe transmission. It uses an encryption key made from a turbulent grouping and edge work by bit XOR activity to encrypt the input picture's pixel values. For creating turbulent guide

succession, a computed guide is used. It is advantageous to send the mysterious image through an unbound channel in a secure manner to prevent data stealing. A limited nonstop space, also known as a real or unexpected number space, serves as the definition of a chaotic framework. The asymptotic movements of the iterative movement are intended to be perceived by the disarray hypothesis.

3.4.1. Chaotic Encryption Scheme

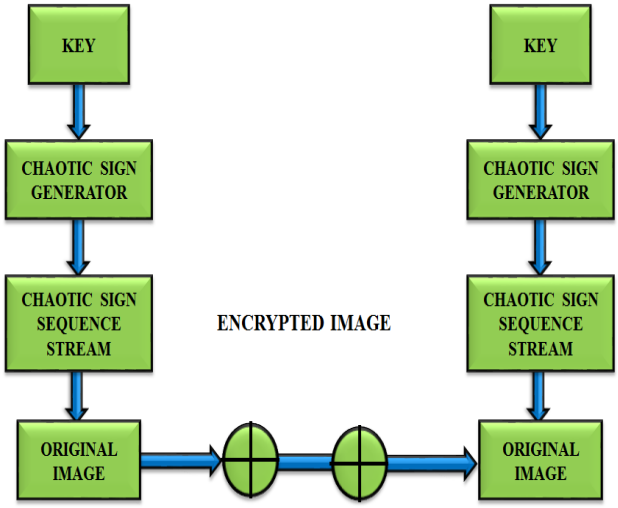


Fig 4: Block diagram of chaotic encryption scheme

A quick way to encrypt video data or messages using turbulence is to use the wide chaotic encryption scheme, as depicted in Figure 4. This method facilitates the discovery of some important information and establishes the crucial security phase. Loud encryption offers high degree security as an advantage. Although the requirement of huge figure storing and a delay in speed are seen as the major obstacles, encryption is nevertheless accomplished by emphasis.

The tumult's characteristics are only slightly altering the field of cryptography. Its characteristics include topological transitivity and starting stage sensitivity. Tumultuous starts by being very delicate. It will then give a slight direction contrast. It offers quite unexpected direction sectional value. Similar features can be delivered through indistinguishable direction. The topology transitivity identifies the state's emphasis on methods and a confined space state. The turbulent encryption method is suggested by (Baptista, 1998). By all accounts, this encryption computation is much better than the one that was done before using conventional techniques. In order to pick the underlying state and parameters for key, we first distinguish between mapping method and direction to encode the message.

We anticipate the primary issue to continue in its current form (direction). Repeat the noisy condition until the route reaches the destination, and then record the repeated action as a code for each message symbol. Replicate a recent trajectories to encode the following message. Using this information, create the subsequent figure.

3.4.2. Data concealing using LSB

Image embedding Method

The three data concealing strategies are

- Inserting the Least Significant Bit.
- Data Hiding With Reversible.
- Utilizing Difference Expansion, reversible data embedding

Maintaining the privacy of binary data when being imparted over the web is a challenging issue. With the limited measure of calculation and with certain known restrictions of the encryption techniques it is easy to launching assaults on figure content. A perfect steganography strategy inserts message data into a transporter picture with virtual subtle changes in the picture. Versatile steganography reaches nearer to this ideality since it uses a regular changes in pixel forces of a spread picture to conceal the mystery message.

In this paper, a new method for LSB detection in binary signals—such as images and sounds—is presented. It is shown that it is possible to estimate the length of disguised messages with a reasonably high degree of accuracy when they are placed into signals as at least significant bits. The cutting edge steganolytic approach depends on test materials that are factually sensitive to LSB insertion operations. Following identification process is rapid and simple. Limits on estimation blunders are established in order to gauge the strength of the suggested steganalytic technique.

Further, defenselessness of new method in dealing with potential assaults is too evaluated, and counter actions are recommended. The strategy is discussed along with the outcome of its application on some example pictures.

The encoding and decoding of the hidden data are discussed below:

3.4.3. To Encode the Hidden Data

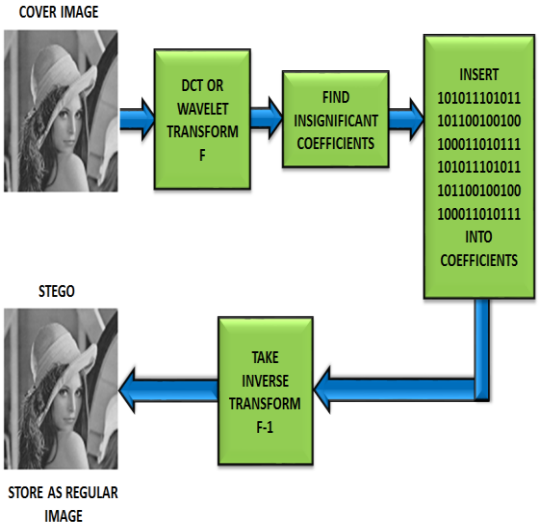


Fig 5: Encoding scheme

The schematic representation of encoding scheme is illustrated in Figure 5. The steps involved in the process of encoding as follows.

1. Convert a cover image using DCT or wavelet transform
2. Identify the coefficient near to the threshold
3. Use hidden bits (LSB Insertion) to replace these bits
4. Find an inverse transform
5. Save as ordinary image

3.4.4. To Decode the Hidden Data

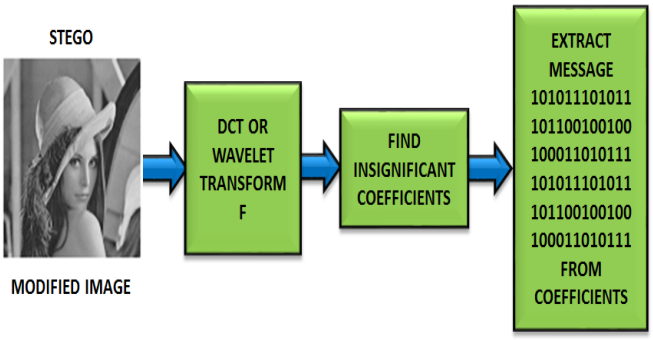


Fig 6: Decoding scheme

Figure 6 illustrates the schematic representation of decoding process. The corresponding steps are as follows,

1. Find the transformation of the hidden image.
2. Chosen are the coefficients that drop below a particular threshold.
3. Obtain the data bits from the coefficients
4. Synthesis these bits into original message

3.4.5. Least significant bit insertion

The bits of a mystery message are randomly distributed and hidden in least significant bits (LSB) of pixels inside a transporter picture, known as the spread picture, in arbitrary LSB inclusion algorithms. The arbitrary interim approach is a well-known method for doing this. Both correspondences share a stegokey, k, which serves as the generator's seed. An idea behind the calculation of the least significant bits is to incorporate the bits secret message into a LSB pixels. Typically, two complementary techniques are used to cultivate this:

- Encryption of the message, so that who has obtain it, should unscramble it before applying it.
- Position of the bits must be randomized by utilizing a cryptographic arbitrary capacity (dispersing), so it becomes practically difficult to reconstruct a message without knowing a seed for irregular capacity.

Along these lines, the message is ensured by two distinctive keys, thus getting significant more security than previous case. This methodology secures the uprightness of the message, being considerably more troublesome (we could state in any event computationally infeasible) to create falseness of the message.

Simple Example with a 24 bit pixel:

1 pixel:

(00100110 10101001 11001100)

Insert 101: (00100110 10101000 11001100)

(Red - Green - Blue)

Simplified Example with an 8 bit pixel:

1 pixel:

(00 01 10 11)

{White- red- green –blue}

Insert 0011: (00 00 11 11)

{White-white-blue- blue}

3.4.6. Benefits of LSB Insertion

The simple and quick method of the LSB computation is a notable area of flexibility. Additionally, a steganography tool has been developed that uses palette control to get around LSB shading changes. With dark scale images, LSB inclusion performs excellently.

3.4.7. LSB substitution

The LSB substitution technique is the steganography technique that is most frequently used. Each pixel in a dark level image contains 8 bits. Therefore, one pixel can display 28=256 different variations. Figure 7 depicts weighting pattern for an 8 bit integer.

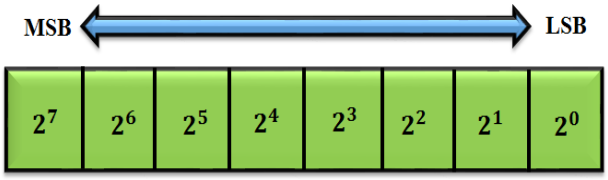


Fig. 7: weighting of an 8-bit pixel

An essential idea of LSB substitution is to insert secret information at privilege most bit (bits with the littlest weighting) thus installing methodology have no influence on real pixel esteem enormously. Scientific portrayal for LSB strategy is: let x indicates to the i^{th} pixel estimation of stego-picture, i x indicates real spread picture, and i m indicates decimal estimation of i^{th} segment in secret information. Quantity of LSBs to be substituted is assumed to be k. Extraction procedure is to duplicate k-furthest right bits legitimately. Henceforth, straightforward arrangement of extricated i m gives real private information. The mentioned strategy is simple and direct. But when limit is extraordinarily expanded, picture quality gets worst and thus suspected stego-picture results. Moreover, secret information may be effectively steeled by removing the k-furthest right bits straight forwardly.

3.5. Quality Measures for Image

Peak signals to mean square error (MSE) and noise ratio are used to gauge the quality of reproduced images (PSNR). The MSE is also called as reconstructed error variance σ_q^2. MSE between first picture f and remade picture g at decoder is considered in the given ways:

$$MSE= \sigma_q^2= \frac{1}{N} \sum_{j,k}(f[j,k] - g[j,k])^2 \quad (4)$$

Where k indicates aggregate of all pixels in images, entirety over j and N is quantity of pixel in every image. The relationship between the change in signal and the change in remaking error is known as the peak signal to clamour proportion. PSNR (decibel) between two images with 8 bits per pixel is:

$$\text{PSNR} = 10\ log_{10}\left(\frac{255^2}{MSE}\right) \quad (5)$$

Generally speaking, actual and recreated images are nearly indistinguishable to the human eye if PSNR is 40 dB or above.

3.6. Keys used in encryption and decryption

3.6.1. Cryptography

Data thumbing is thought to be one of the earliest applications of private key cryptography; in this instance, the mastering technique is "key" (security through lack of clarity). Books on steganography are replete with examples of these techniques being used from the very beginning. Cryptography is the study of encrypting and decrypting data using mathematical operations. By using cryptography, we may keep sensitive data or send it over a shaky network (the internet) without anyone other than the intended recipient being able to read it.

Cryptanalysis is science of deciphering and breaking secure correspondence, whereas cryptography is the study of verifying information. Traditional cryptanalysis combines logical reasoning, the use of scientific tools, design that is isolated from persistence, assurance, and karma in an exciting way. Attackers are frequently referred to as cryptoanalysts. Cryptology encompasses both cryptanalysis and cryptography.

The management of data in an ambiguous (scrambled) structure for secure transmission is referred to as cryptography. The beneficiary can recover the original message by unwrapping the jumbled message using a "key." Stenography improves this by hiding the manner in which a correspondence took place. The spread item is characterized as the harmless message c that contains the message m. The message is then installed into c using a key k known as the Stego-key.

3.6.2. Steganography

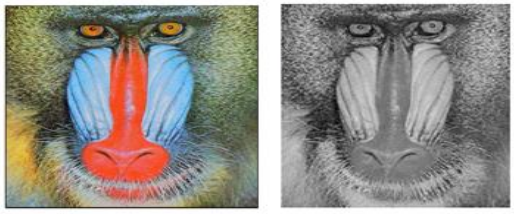
Steganography aims to blend innocent information with secret data. Binary images are ideal for obscuring secret data. Cover images are pictures with an ambiguous message. To begin with, there shouldn't be any visible difference between the cover and stego photos. Embed should not draw any additional attention to the Stego pictures in order to prevent programmers from trying to incorrectly extract the hidden message. The next step is to use a reliable message concealing mechanism. If a person doesn't have a unique separating method and the right mystery key, it is impossible for them to decipher the hidden messages. Third, maximum duration of secret communications that may be kept a secret should be such that this is practicable. "Steganography is the craft of concealing data in a manner that avoids the leakage of shrouded message".

3.6.3. Cryptography VS Steganography

While steganography involves imagining the presence of information to make it impossible to detect, cryptography is the science of encoding information so that no one can decipher the jumbled message. The information that has to be concealed is added to the spread article, which can be a piece of text, a photograph, a sound file, or a video, in order for the spread item's presence to remain unchanged even after the information has been concealed. To create a stego object, data must be concealed and a spread item must be used. The information that has to be concealed is first scrambled with a key to increase security. One should own the key in order to retrieve the locked data. A stego item is one that has data that is obscured and has the exact same appearance as a spread article.

4. Simulated result

(a) Lena Original and B-Plane Image



(b) Baboon Original and B-Plane Image

(c) Pepper Original and B-Plane Image

Fig.8: Original Image and its B Plane

In Figure 8, several original images that are accompanied by their corresponding images in the B Plane is shown.

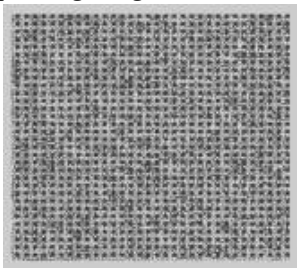


Fig. 9: Reserved Spaces (Dark Region) using LWT

The decomposed image using Lifting Wavelet Transform is illustrated in Figure 9.

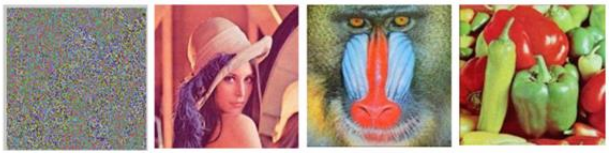


Fig. 10: Encrypted Image and its Recovery

In contrast to the existing method, the proposed stegno-analysis technique is found to work well for images taken (jpeg). The Figure 10 shows the encrypted and recovered images using the suggested method and achieves improved performance in producing error-free stego pictures.

MATLAB R2013a simulates the proposed approaches of chaotic encryption, LSB methodology, and reserve room approach. To create the stego image, a 256*256 sized 8-bit image is used as the cover image (.jpg). Table 1 shows the comparison between PSNR and other techniques.

Table 1: Comparison of PSNR with different techniques

Methods	**LENA**	**BABOON**	**PEPPERS**
FMM [12]	46.06	50.27	45.67
CST [13]	48.48	48.36	50.04
SHSI [14]	57.62	43.67	85.67
Ref [15]	49.59	42.24	50.08
MLSB-SM [16]	57.14	44.78	46.75
DCT & OTP[17]	50.93	46.21	51.40
Ref [18]	49.02	49.26	43.59
PVD & MF [19]	43.28	41.83	41.65
LSB& Data mapping [20]	48.45	48.34	48.13
Proposed Method	**60.47**	**51.11**	**87.21**

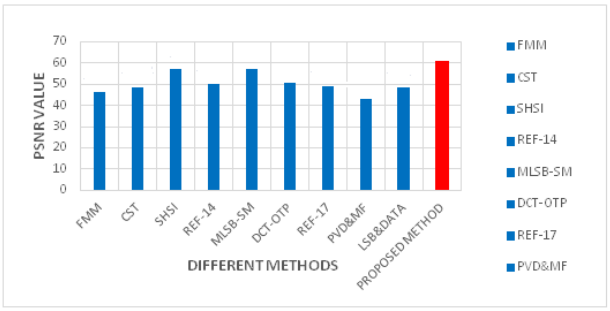


Fig. 11: Comparison of PSNR with Different Techniques

The Table 1 demonstrates the comparison performed between PSNR and other different techniques, showing improved results of PSNR with its corresponding graph illustrated in Figure 11.

Table 2: Comparison of MSE with Existing Approaches

Methods	**LENA**	**BABOON**	**PEPPERS**
FMM [12]	0.9863	0.792	0.890
CST [13]	0.0674	0.783	2.073
SHSI [14]	0.0742	0.962	1.921
Ref [15]	0.0762	0.835	0.739
MLSB-SM [16]	0.0543	0.749	0.998
DCT & OTP [17]	0.5732	1.444	1.435
Ref [18]	1.0041	1.008	2.357
PVD & MF [19]	3.0008	4.127	4.452
LSB& Data mapping [20]	0.0938	0.925	0.965
Proposed Method	**0.0010**	**0.520**	**0.517**

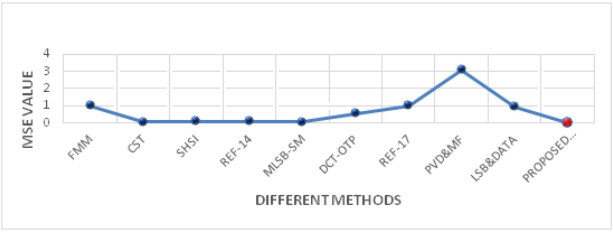


Fig. 12: Comparison Graph for MSE with Existing Approaches

The quality of reconstructed image for existing and proposed system is evaluated and represented in Table 2 following this, the corresponding values are plotted in graph format and displayed in Figure 12.

5 Conclusion

The assurance of picture quality and shrouded information during transmission dependent on reserve room strategy and disordered crypto framework with LSB based information covering is discussed in this paper. Lifting wavelet modification was utilized to successfully conceal information in this case and tumult encryption was employed to ensure an accuracy of an images. This framework creates stego images with minimum error under most extreme information concealing the limit. At last, the system performance was measured with quality measurements like blunder and SNR factor. This methodology has better adaptability with productivity somewhat over earlier strategy.

6. References

[1] J. Zhou, W. Sun, L. Dong, X. Liu, O.C. Au and Y.Y. Tang, "Secure reversible image data hiding over encrypted domain via key modulation", IEEE transactions on circuits and systems for video technology. Vol. 26, No. 3, pp. 441–452, 2015.

[2] W. Zhang, H. Wang, D. Hou and N. Yu, "Reversible data hiding in encrypted images by reversible image transformation", IEEE Transactions on multimedia, Vol. 18, No. 8, pp.1469-1479, 2016.

[3] X. Zhang, “Reversible data hiding in encrypted image”, IEEE signal processing letters. Vol. 18, No. 4, pp.255-258, 2011.

[4] X. Zhang, J. Long, Z. Wang and H. Cheng, “Lossless and reversible data hiding in encrypted images with public-key cryptography”, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 26, No. 9, pp.1622–1631, 2015.

[5] M. J. Traum, J. Fiorentine. (2021). Rapid Evaluation On-Line Assessment of Student Learning Gains for Just-In-Time Course Modification. Journal of Online Engineering Education, 12(1), 06–13. Retrieved from http://onlineengineeringeducation.com/index.php/joee/article/view/45

[6] Z. Qian, X. Zhang and S. Wang, “Reversible data hiding in encrypted JPEG bit stream”, IEEE transactions on multimedia, Vol. 16, No. 5, p.1486-1491, 2014.

[7] Z. Qian and X. Zhang, “Reversible data hiding in encrypted images with distributed source encoding”, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 26, No. 4, pp.636-646, 2015.

[8] F. Peng, Z.X. Lin, X. Zhang and M. Long, “Reversible data hiding in encrypted 2D vector graphics based on reversible mapping model for real numbers”, IEEE transactions on information forensics and security, Vol. 14, No. 9, pp.2400-2411, 2019.

[9] Chauhan, T., and S. Sonawane. “The Contemplation of Explainable Artificial Intelligence Techniques: Model Interpretation Using Explainable AI”. International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 4, Apr. 2022, pp. 65-71, doi:10.17762/ijritcc.v10i4.5538.

[10] Z. Qian, H. Xu, X. Luo and X. Zhang, “New framework of reversible data hiding in encrypted JPEG bit streams”, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 29, No. 2, pp.351-362, 2018.

[11] Y.C. Chen, T.H. Hung, S.H. Hsieh and C.W. Shiu, “A new reversible data hiding in encrypted image based on multi-secret sharing and lightweight cryptographic algorithms”, IEEE Transactions on Information Forensics and Security, Vol. 14, No. 12, pp.3332-3343, 2019.

[12] H. Ge, Y. Chen, Z. Qian and J. Wang, “A high capacity multi-level approach for reversible data hiding in encrypted images”, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 29, No. 8, pp.2285-2295, 2018.

[13] F. Ernawan, D. Ariatmanto and A. Firdaus, "An improved image watermarking by modifying selected DWT-DCT coefficients”, in IEEE Access, Vol. 9, pp. 45474-45485, 2021.

[14] F. A. Jassim, “A novel steganography algorithm for hiding text in image using five modulus methods”, arXiv preprint, 2013.

[15] K. Muhammad, J. Ahmad, N.U. Rehman, Z. Jan, R.J. Qereshi “A secure cyclic steganographic technique for color images using randomization”, Tech J Univ Eng Technol Taxila Pakistan Vol. 19, pp. 57–64, 2014.

[16] Joy, P., Thanka, R., & Edwin, B. (2022). Smart Self-Pollination for Future Agricultural-A Computational Structure for Micro Air Vehicles with Man-Made and Artificial Intelligence. International Journal of Intelligent Systems and Applications in Engineering, 10(2), 170–174. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/1743

[17] K. Muhammad, J. Ahmad, H. Farman, M. Zubair, “A novel image steganographic approach for hiding text in color images using HSI color model”, Middle-East J Sci Res, 2014.

[18] M. Karim “A new approach for LSB based image steganogra-phy using secret key”, 14th International Conference on Computer and Information Technology, pp 286–291, 2011

[19] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho and S. W. Baik, “A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image”, Multimedia Tools and Applications, Vol. 75, No. 22, pp. 14867-14893, 2016.

[20] E. H. Rachmawanto and C. A. Sari, “Secure image steganography algorithm based on DCT with OTP encryption”, Journal of Applied Intelligent System, Vol. 2, No. 1, pp.1-11, 2017

[21] D. Bandyopadhyay, K. Dasgupta, J. K. Mandal and P. Dutta, “A novel secure image steganography method based on Chaos theory in spatial domain”, International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 3, No. 1, pp.11-22, 2014.

[22] Garg, D. K. . (2022). Understanding the Purpose of Object Detection, Models to Detect Objects, Application Use and Benefits. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 01–04. https://doi.org/10.17762/ijfrcsce.v8i2.2066

[23] P. K. Dhar, A. Kaium and T. Shimamura, “Image steganography based on modified LSB substitution method and data mapping”, International Journal of Computer Science and Network Security, Vol. 18, No. 3, pp. 155-160, 2018.

[24] M. Juneja and P. S. Sandhu, “A new approach for information security using an improved steganography technique”, Journal of Information Processing Systems, Vol. 9. No. 3, pp.405-424, 2013.