[1*]Abhrendu Bhattacharya

[2*]Manoj Eknath Patil

Enhancing Video Data Security: A Bch Code-Based Steganographic Method for Robust Message Concealment in DCT Coefficients

Journal of Electrical Systems

Abstract: - This manuscript proposes a novel method for enhancing security in video data by utilizing BCH codes for the encryption and decryption of secret messages, which are then embedded into the Discrete Cosine Transform (DCT) coefficients of the video's edges. The hidden messages are stored in the Y, U, and V planes, excluding the DC coefficients, to ensure minimal impact on video quality. The method is tested on slow and fast-paced videos to evaluate its robustness and performance under different conditions. By incorporating steganography, the technique hides additional information (the "payload") within a cover image or video without noticeable visual changes. The method's effectiveness is demonstrated through comparisons with three alternative calculation approaches, and results indicate that the proposed method outperforms the others in terms of data concealment and preserving visual quality. The method achieved a concealed proportion of 27.53% of the data while maintaining the appearance of the cover video, making it an advantageous solution for secure covert communication in multimedia.

Keywords: Cryptography, Steganography, algorithm, Discrete Cosine Transform Technique, Image Based Steganography.

I. INTRODUCTION

The rapid development of web utilization over high transmission capacity and low cost PC equipment has moved the unstable development of steganography (Krenn J. , January 2004). In the current year, secure and stowed away correspondence is the first prerequisite individuals. Accordingly steganography is acquiring fascination by indi- viduals due to the security issues over web. Steganography implies clandestine com- posing (Beenish Mehboob R. A., 2008). Steganography has developed into a comput- erized procedure of stowing away a document in some type of mixed media, for ex- ample, a picture, a sound record or A video recording, on the other hand, is also fine.

Steganography's purpose is to conceal information, known as a "payload," in a "cover picture" so that it is not visible to the naked eye. The most prevalent methods of steganography (DWT) include the Least Significant Bit (LSB) method, the Discrete Cosine Transform (DCT), and the Discrete Wavelet Transform.

Steganography is a method that can be used in two very different settings: one that is spatial and the other that is repetitive (Chen Ming, 2006). In spatial space, processing is done right on the image's pixel values, but in recurrence space, the pixel values are changed first, and then processing is done on the changed coefficients. Both cases show the same thing. The LSB technique[47] is used in the spatial region, while the DCT and DWT techniques are used in the recurrence region. When the Least Signifi- cant Bit (LSB) algorithm is used, the value of each image pixel is changed so that it matches the value of the pixel next to it. The sensitive information is then hidden in the image's least significant bit, which is the second digit of each pixel's paired value. Even though this algorithm protects the cover image, it can be attacked in ways like editing, pressure, and other ways that photos can be changed. The Discrete Cosine Transform (DCT) and the Discrete Wavelet Convert (DWT) are two mathematical functions[48] that can turn the spatial information of a digital image into the recur- rence area (DWT). Images are changed in the recurrence region, data is added to all the important parts of the medium recurrence sections in DCT, and lossy pressure is calculated along the way. The Discrete Wavelet Transform[49] can make high recur- rence coefficients that can be used to hide information. With these coefficients, you can get to the highest level of strength.

[1]Ph.D, Assistant Professor, Department of Computer Science and Engineering, JIS University, Kolkata, West Bengal, India.

Email: abhrendu.bhattacharya@jisuniversity.ac.in

2 Associate professor, Department of Computer Science & Engineering, SSBT's College of Engineering and Technology, Bambhori, Maharashtra.

Email: mepatil@gmail.com

Copyright © JES 2024 on-line : journal.esrgroups.org

II. REVIEW OF LITERATURE

Krenn,et al.(2004) what steganography was and how to accomplish it.With no hope, Neeta 2004 et al. People claim that the information can be placed in all of the crucial portions of the cover image, and that a typical person will not be able to notice any weird images in the cover image.

Sharma,et al.(2012) fostered another steganography technique in view of sensible tasks for 8bit (dark scale) or 24bit (variety picture) to guarantee protection from steganalysis assaults.

Chen,et al.(2006)and partners proposed another steganography innovation in which mystery messages are encoded in the recurrence space. The recommended calculation is isolated into two modes and five circumstances in view of the necessities of various clients as far as implanting limit and picture quality. Chen Ming et al. focused on the calculations for steganography apparatuses. Different apparatuses are ordered into five gatherings in light of calculation examinations: Tools for steganography in the spatial domain; Other classes, for example, video pack encoding and spread range technique based incorporate change space based steganography devices, report based steganography instruments, and document structure based steganography instruments. Aneesh Jain et al. proposed a procedure for concealing information in bitmap pictures so that there is practically no recognizable distinction between the first and the new picture, and that it is likewise impervious to JPEG pressure.

Beenish Mehboob,et.al(2008) discover the workmanship and research of steganography while in doubt, and suggest a foxy method for hiding statistics in a adorable photo- graph the usage of the maximum un-enormous piece. Hassan Mathkour, et al. created a number of concepts to observe and survey the traits and imperfections of the frameworks gave, and a greater strong steganography method turned into organized that takes gain of the traits even as keeping off the disadvantages.

Nageswara Rao Thota and his coworkers used important MATLAB constraints to make simple JPEG pressure. Mamta Juneja and her colleagues did research on the LSB (Least Significant Bit) expansion and the RSA encryption algorithm to figure out how to make a secure photo steganography system. Using a steganograph to send private correspondence through a public channel is an important topic for K.B.Shiva Kumar and his colleagues to study.

III. STEGANOGRAPHY ALGORITHM BASES ON MLSB STRATEGY

The unique steganography algorithm proposed includes many phases for creating a stego picture Stg, which is created by enclosing a secret image S inside a cover image C. Each of us has an extraction rule that we can use to duplicate the unknown image S. The proposed steganography calculation (on the shipper's side) is composed of two elements, which are depicted in Figure 1 as the major components used for hiding and revealing. This is due to the fact that the shipper's side of the steganography computation requires two distinct pieces. The primary purpose of this initial phase of the project is to create DSIS from the cover image so that restricted data can be delivered whenever it is required. The purpose of the second half of the project is to devise an effective method for incorporating a mystery image into a cover image while maintaining a high level of obscurity to guard against attacks and carry a large payload.

3.1. Algorithm of Image Steganography

The "image division" interaction's purpose is to divide a given cover picture into multiple smaller images based on the outcomes of other hypotheses. Scientists devised and applied a variety of approaches to successfully divide a picture into its constituent components based on the values of force, comparability, and change between nearby bytes. The proposed approach produces an estimate based on a code key, which requires three independent actions. This keeps an attacker from easily figuring out where the edges of the parts are. This is done so that nosy people can't see the information. In Figure 1, we try to make sense of the proposed picture split by looking at it as if it were a cover photo that was cut into many different-sized pieces.

The red, green, and blue layers make up the cover art. Each layer has a two-level display (WC H C), where WC and H C represent the width and height of a cover image, respectively. The image on this cover is composed of red, green, and blue layers.

To calculate the size of fragment (s), apply the following equation: where (Xs, R) is the length of fragment (swidth) and (Ys, R) is the length of fragment (slevel.) (1- 2). It was agreed that the Xs, R and Ys, R for each subchapter would be created using the code key K. We believe that picture division is an excellent method for preventing neutralisation assaults since it allows you to hide secret messages in a more random manner while simultaneously making it more difficult to find out what they are by a factor of 1/(SS), where SS is the sum of the number of divided portions in the cover picture.

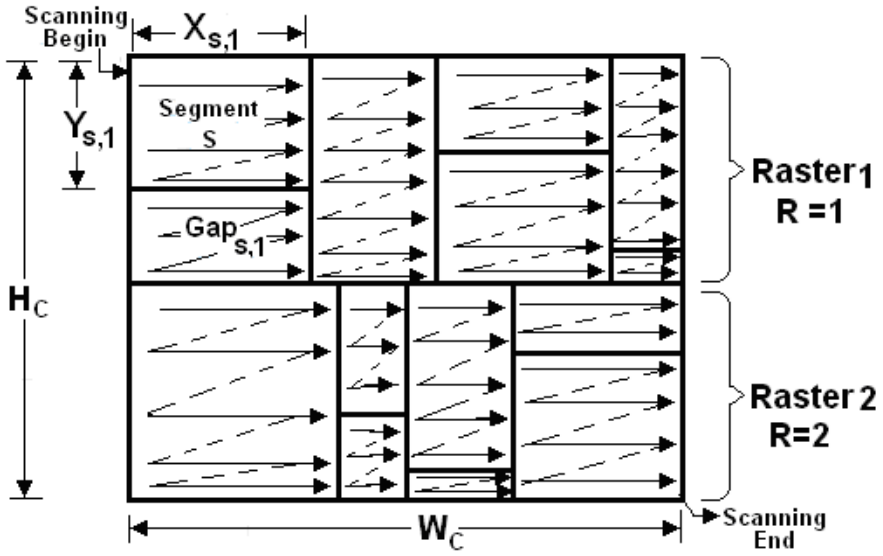

Figure 1: Using a method that isn't the norm to divide images with DSIS Source: (M.Al-Shatanawi, 2015) (M.Al-Shatanawi, 2015) (M.Al-Shatanawi, 2015)

If you have a set of rasters, R, the equation X,s R Y,s R tells you how big each segment is at that raster, where X,s R and Y,s R are the results of other equations (1-2).

$$X_{s,R} = \left\lceil \sqrt{\frac{Wc}{h}} \right\rceil_{+} h$$

$$Ys, R = \left\lceil \sqrt{\frac{Hc+A+B}{\lambda}} \right\rceil_{+} \lambda \quad (1)$$

Val(Str(A) + Str(B)) is equal to D, which is the decimal value of the combined A and B strings. Val(Str(B)+Str(C)) is equal to h, which is the numeric value of the combined B and C strings.

You can turn a decimal number into a string in Excel by using the Str(.) function, and you can turn a string into a decimal number by using the Val(.) function.

3.2. Algorithm 1: DSIS for segmentation of Images

Stage 1: Type in K, Covering Image C, and;

Stage 2: For each of the colours in C, type // color,R,G,B.

Stage 3: For each raster R in the C,;

Stage 3.1: For every single raster segment s,

$$Ms = Val\,(Ks)^{\forall = 1,,,,,,,|\,SS\,|} \quad (2)$$

Stage 3.1.1: MS should be determined using Equation (7)

Stage 3.1.2: Use Equation (6) to calculate F.

$$F = ¢ - \text{Val (Str (Ms))} \quad (3)$$

Stage 3.1.3: Perform A and Equation (3).

$$A = \left\lceil \frac{F}{100} \right\rceil \quad (4)$$

Stage 3.1.4: Using Equation., calculate B. (4).

$$B = \left\lceil \frac{F - A*100}{10} \right\rceil \quad (5)$$

Stage 3.1.5: Equation (5) is used to calculate C.

$$C = (F-(A*100)-(B*10)) \quad (6)$$

Stage 3.1.6: Using Equation (1), calculate Xs,R.

$$X\ s\ ,\ R = \left\lceil \sqrt{\frac{Wc}{h}} \right\rceil_{+} h \quad (7)$$

Stage 3.1.7: Using Equation (2), calculate Ys,R.

$$Ys,\ R = \left\lceil \sqrt{\frac{Hc + A + B}{\lambda}} \right\rceil_{+} \lambda \quad (8)$$

Stage 3.1.8: Using Equation., calculate Gaps,R (8).

$$Gaps,\ R = Xs,\ R * (\max(Yj,\ R) - Ys,\ R)$$

End of each segment s. Finish; / every single R raster

The temporal complexity of DSIS is stated in "Big-O" notation, with the time needed for all segments stated in Equation (9):

Time Seg T (Ms) T(F) T(A) T(B) T(C) T(X) T(Y) O(7) s = + + + + + s + s ≈ (9)

Furthermore, Equation. defines the total time necessary for every single segment for every colors (10):

T(Time Seg SS ,) O(Time Seg 3 SS) O(7 3 SS) O(21 SS) s = s × × ≈ × × ≈ × (10)

3.3. Discrete Cosine Transform (DCT)

DCT is a prominent tension technique that is used in a variety of usages, including picture and video pressure. The DCT isolates the sign into three repeat gatherings: low, focus, and high. The discrete Fourier change is immovably connected with the DCT (DFT). It is a recognizable straight change, suggesting that the 2DDCT is like 1DDCT in one respect, followed by 1DDCT in the other (Chin-Chen, 2008). The modified Edge B DCT repeat factor and the inverted DCT factor of the replayed frame are designed to include the conditions for data video frame A with an MxN destination.

$$B_{pq} = \alpha_p \alpha_q \sum_{M=0}^{p-1} \sum_{N=0}^{q-1} A_{mn} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N} \quad \ldots\ldots\ldots (1)$$

$$A_{mn} = \sum_{M=0}^{p-1} \sum_{N=0}^{q-1} \alpha_p \alpha_q B_{pq} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N} \quad \ldots\ldots\ldots (2)$$

Where

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \frac{\sqrt{2}}{\sqrt{M}}, & 1 \le p \le M-1 \end{cases}$$

And

$$\alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \frac{\sqrt{2}}{\sqrt{N}}, & 1 \le q \le N-1 \end{cases}$$

B (p, q) is the coefficient of the 2DDCT frame for row p and region q, and A (m, y) is the pixel information for edge A and section y. (m, n). Low-secret messages were sent, but they couldn't be found because cover data, limited attention, and high itera- tion factors were used (L. Guangjie, 2011).

3.4. Strategies for Concealing Data in Digital Image

Steganography is a baffling correspondence technique. The stego picture is made by intro- ducing the secret picture that is given to the evenhanded inside the cover picture. This part inspects evaluation limits too as could be anticipated introducing and recuperation moves close (W. Jyun-Jie, 2012).

A. LSB: The Technique of Least-Significant-Bit-Substitution

In LSB steganography, a message is hidden by using only the most basic parts of the high-level data recorded on the cover media. It's called LSB substitution, and it's the most important part of LSB steganography. LSB surrogate steganography is used to encrypt the last part of each data review so that it accurately represents the hidden message. When an 8-bit grayscale bitmap is turned into bytes, the grayscale is taken into account (R. J. Mstafa and K. M. Elleithy, 2015). If you look at the image's infor- mation, you can see that the four pixels below the main image may have a low scale gain.

11010010

01001010

10010111

10001100

To make C darker, change the LSB of the pixels that make up C to a new dim-scale value. This letter's pair value is 10000011.

10000011.

The primary component of the LSBs should be modified generally. The contrast between the cover (special) image with the stego image will be evident to the independent eye. One of its major drawbacks is the small amount of data that can be combined in such images utilising essentially LSB. LSB attacks are nothing out of the usual. LSB approaches performed in 24 bit plans are more consistently recognised than 8 cycle plans (R. Zhang, 2009). Another application of the LSB approach is: Consider a three-pixel cross section of a 24-cycle image in which the number 300 is to be incorporated using the LSB approach. According to all reports, the final cross section is as follows:

B. DCT: Discrete Cosine Transform-Transformations Technique

DCT coefficients are utilised for JPEG pressure. It divides the image into sections of varying importance. It alters the spatial space of a sign or image in relation to the recurring district.

It may divide the image into three distinct sections: high, concentration, and low.

A significant portion of the sign energy in the low recurrent sub-band is at low rehash, containing the most focal visual bits of the image, while high recurrent parts of the image are regularly avoided through strain and disturbance assaults in the high recurrent sub-band (R. Zhang V. S., 2012). The mystery message is encoded as

needed by adjusting the coefficients that are part of the centre recurrent sub-band, ensuring that the image's recognisable quality remains unchanged. The going with condition depicts the general condition for a 1D (N information things) DCT: Figure 2

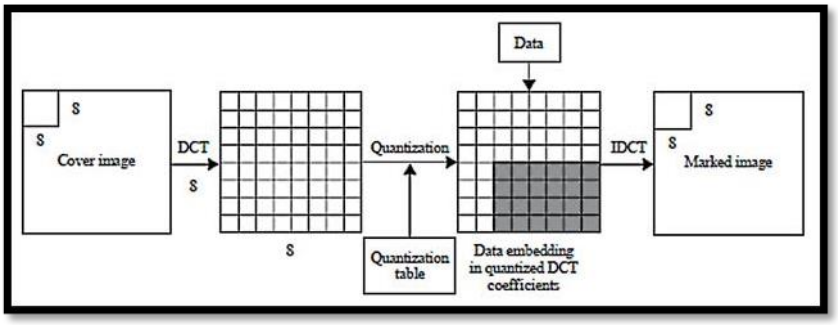

Figure 2. Discrete cosine transform of images

(Image Source: Zheng Guangglou, 2019, Security Research Institute)

$$C(u) = a(u) \sum_{i=0}^{N-1} x_i \cos \frac{(2i+1)u\pi}{2N}$$

N-1, where u=0, 1, 2,The following formula defines a general formula for the 2D DCT (N x M image).

$$C(u.v) = a(v) \sum_{i=0}^{N-1} [a(u) \sum_{i=0}^{N-1} x_i \cos \frac{(2i+1)u\pi}{2N}] \times \cos(\frac{(2i+1)u\pi}{2N})$$

Where u and v are the numbers from 0 to N-1, including N-1. The size of the picture as a whole is NXM pixels. The letter C stands for the DCT coefficient for the uth row and the vth fraction of the DCT organisation (u, v). The power of the pixels in row I and segment j is shown by c I j). (Y. Liu, 2013) DCT is used in the process of steganography. The width of the picture has been decreased by 808 pixels. We start with the column on the far left and move clockwise around the room as we apply the DCT to the blocks. After the message has been processed, the DCT factors are scaled by compressing each block with a quantization table .

C. Discrete Wavelet Transform Method(DWT)

Here, we changed the repeat area by using Haar-DWT [18, 19], which is the DWT iteration with the fewest steps. A 2-layer Haar DWT is made up of the following er- rors: The first step is called the "extend motion," and the second is called the "vertical motion." The factor-by-factor methods for a two-dimensional Haar-DWT look like this:

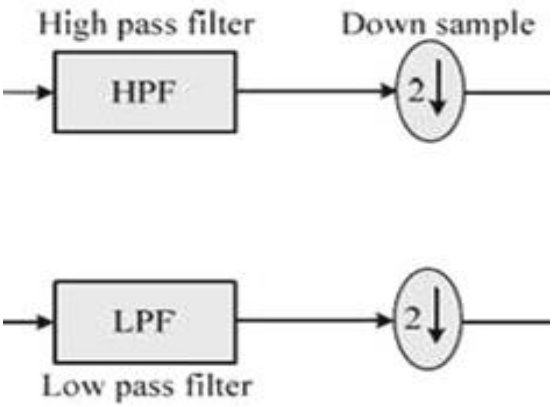

Figure 3: The Horizontal operation on first row picture

Stage 1: All along,channel the pixels from left to proper in bearing. Then,play out the improvement and allowance approach on connecting pixels. Store absolutely the at the left and the qualification at the proper as

displayed in figure 3. Go over this motion till all the strains are take care of. The pixel totals deals with the low repeat part(implied as photograph L)even as the pixel differentiations deal with the excessive repeat a chunk of the predominant photograph(implied as photograph H).

Stage 2: Secondly, channel the pixels absolutely in vertical bearing. Play out the extension and allowance method on bordering pixels and sooner or later save the all out at the pinnacle and the qualification on the bottom as displayed in figure 4. four. Go over this motion till all the frag- ments are dealt with. Finally we can procure four sub-bunches verified as LL, HL, LH, and HH independently. The LL sub-band is the low repeat fragment and on this manner appears essen- tially equal to the number one picture. The entire machine illustrated is known as the first-call for 2-D Haar-DWT. (Diop, 2014).

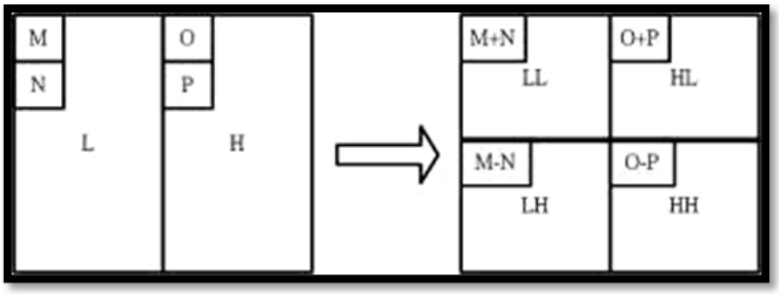

Figure 4. The Vertical Operation

(Image Source: Archana Vaidya, 2013, IOSR journal of Computer Engineering)

D. The DCT-Based Robust-Image-Steganography

Steganography must meet four needs: versatility, imperceptibility, simplicity of percep- tion, and security. According to documented study, the LSB-based method outperforms the iterative spatial method for a wide range of images, including grayscale and variety images (Krenn, 2004). In contrast to LSB-based steganography, DCT-based steganography works flawlessly with only minor image quality distortion. The limited amount of information that can be obscured by this technique does not exactly match LSB-based steganography, but we suggest this technique because there is little change in image quality. The LSB extension is the most harmless and powerless for normal adjust- ments, but DWT-based steganography can be used to keep the low repeat sub-band coeffi- cients unchanged and further improve image quality. This is because the DWT factor has changed the properties of various sub collections. PSNR warns when a secret message is embedded in a repetitive sub-cluster connecting some edges of the main image, taking into account that there are no errors in the basic part (less repetitive part) (Chin-Chen, 2008).

3.5. Algorithm for Steganography

3.5.1. Steganography with LSB

Instant message installing calculation:

Stage 1: See the cover image and the immediate message contained within it.

Stage 2: Binaryize the instant message.

Stage 3: Obtain the LSB for each of the pixels within the cover image.

Stage 4: Alter the LSB of the cover image with each piece of the mystery message.

Stage 5: Create a stego picture.

Stage 6: Find Mean Square Error (MSE), which is the ratio of the image's strongest signal to its weakest signal (PSNR).

Instant message recovery calculation:

To begin with, read the stego realistic.

Stage 7: Determine the LSB of every pixel in the stego picture.

Stage 8: Get the pieces and transform every 8-bit esteem into a person.

3.5.2. DCT Based Steganography

Calculation for implanting instant message: - r.

Stage 1: Examine the cover picture.

Stage 2: Read the mystery message and convert it to paired design.

Stage 3: The cover picture is separated into 88 pixels blocks.

Stage 4: Working from left to right and through and through, take away 128 from every pixel block.

Stage 5: Every block is exposed to DCT.

Stage 6: The quantization table packs every block.

Stage 7: Calculate the LSB of each DC coefficient and replace it with a hint of the mystery message.

Stage 8: Create the stego picture.

Stage 9: Determine the Mean Square Error (MSE).

The stego picture's pinnacle sign to clamor proportion (PSNR). Instant message recovery calculation:

Stage 1: Examine the stego picture.

Stage 2: The Stego picture is partitioned into 88 pixels blocks.

Stage 3: Working from left to right and through and through, take away 128 from every pixel block.

Stage 4: Every block is exposed to DCT.

Stage 5: The quantization table is utilized to pack every block.

Stage 6: Calculate the LSB of each DC coefficient.

Stage 7: Obtain and change over every 8-digit character.

3.5.3. DWT Based Steganography

(Das, 2012) Instant message implanting calculation: -

Stage 1: Read the cover image and the instant message depicted in the cover image.

Stage 2: is to change over the instant message to parallel. On the cover picture, apply the 2D-Haar change.

Stage 3: Determine the flat and vertical separation coefficients of the cover image. The cover image is combined with the DWT coefficient information bits.

Stage 4: Get the stego picture.

Stage 5: Determine the stego picture's Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).

Instant message recovery calculation:

Stage 1: To begin with, read the stego realistic.

Stage 2: Determine the cover picture's flat and vertical separating coefficients. Piece by bit, remove the message and reassemble the cover picture.

Stage 3: Obtain the stego image.

Stage 4: Create a message vector by doing the right thing with the data. Considering what was said before,

3.5.4. Robust Image-Based Steganography Proposal

(Khan, 2014) Calculation to implant instant message:-

Stage 1: See the cover picture and the instant message that will be held inside it.

Stage 2: Binaryize the instant message.

Stage 3: Choose an area to look at and see if either the block Num Bit or the block Tot Bit has a bit value of 1.

Stage 4: In the fourth and final stage, the phase is done if the block with the identifier Num is more important than the value of zero and the block with the identifier Tot Bit is more important than the value of one. The DCT of an 8x8 block is stored in bits 0 and 1.

Stage 5: Choose two arbitrary factors of changing power, K1 and K2. Contingent upon the information bits, increase the worth of the significant askew of the DCT's AC co-productive by K1 or K2.

Stage 6: Read the following information nibbled and recover the following picture block.

Stage 7: If either Block Num or Tot Bit equals M*N/8*8, the message has been successfully implanted.

Stage 8: Download the Stego picture.

Stage 9: Find out the error in the CER-related information that was recovered, as well as the Stego image's Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).

Stage 10: Determine the impact of clamor (like Gaussian commotion) on the recuper- ated information with regards to CER by adjusting the difference.

3.5.5. Instant message recovery calculation:

Stage 1: Obtain the Stego Image as well as the arbitrary factors K1 and K2.

Stage 2: Extract a 8*8 DCT from a block in the Stego Image. Compute the relation- ship between's the off-primary corner to corner DCTs utilizing K1 and K2.

Stage 3: If the message bit is 1 or 0 if the correlation (off-head topseater bay DCT, block K1) is more important than the correlation (off-essential descending DCT, block K2). All 8 * 8 blocks of a Stay Gold image Safe data bits Convert data bits to the message vector "M". Compare with the first message vector "M". This approach is more noteworthy than spatial and iterative steganography.

IV. STEGANOGRAPHY METHODOLOGY PROPOSAL

We supplied a DCT-primarily based totally sturdy video steganographic method thinking about BCH codes on this part. From the beginning, the video path of move- ment is split into outlines; every bundling is completely exceptional over completely to YCbCr range area. The avocation at the back of buying and selling completely to YCbCr collection area is to wreck the affiliation among red, green, and blue tones. The concept approach consists of stages: statistics basis and statistics segment (Horng, 2014).

A. Data Embedding Stage

For security reasons, mysterious messages are shuffled using the private key and code is added to create an encrypted message. Encrypted messages are converted from 2 digits to 8 base digits. Each video sequence is then relocated to a different enclosure. Each package closes with a YUV tone space. Then, at that point in each pass, 2DDCT is freely applied. Therefore, the setup technique hides all Base8 digits of a coded mes- sage made by repeating the DCT except for the DC coefficients for the Y, U, and V planes. Then, the inverse of the two-dimensional discrete cosine transform (DCT) is done on the three Stegobits in each pack to make a Stegoframe. (Mstafa, 2015).

B. Data Extracting Stage

Data extraction is a technique for recovering encrypted messages from your Stego account. This is achieved by separating the stego account into outlines. Each edge is separated by three planes, Y, U and V. Before and after that, 2DDCT is applied un- conditionally to each plane. Except for the DC factor, the most common way to get the encoded information is to get the numbers from all Y, U, and VDCTs. coefficients independently The BCH (7, 4, 1) decoder translates the outcomes data, which is then disentangled by the unwinding framework to extricate[45] the real introduced message. The reasoning for utilizing endlessly encoding techniques prior to

introducing the framework is to build the security and energy of the proposed computation (R.J. Mstafa and K. M. Elleithy, 2015).

4.1. RGB image representation is required as a prerequisite.

A three-dimensional matrix is one way to show how a colour picture is made. However, our analysis showed that only the red channel should be used to show an image[46]. First, the rows are set, then the columns, and finally, the colour of each pixel is set. Since we're using the RGB colour model, the third order will have to figure out what the red and green colour values should be. The size of the image determines what the rows and columns mean [47].

V. EXPERIMENTAL RESULTS AND DISCUSSION

The exploratory weather makes use of numerous factors: the duvet[48] statistics com- bine a dataset consisting of six video moves of CIF kind Foreman, Akiyo, Coast- guard, Container, Bus, and Soccer; moreover, the YUV configuration is 4:2:0. Moreover, every video's point is (352 288), and all records are comparative length with 150 edges. As a secret correspondence, an enormous text report is utilized. To test the suggested ascertaining efficiency, the assignment is finished in MATLAB.

5.1. Visual Quality

The Pick Sign to Noise Ratio (PSNR) is a quality metric that lets you compare two videos objectively and see if they meet the criteria for Good or Stay Gold.

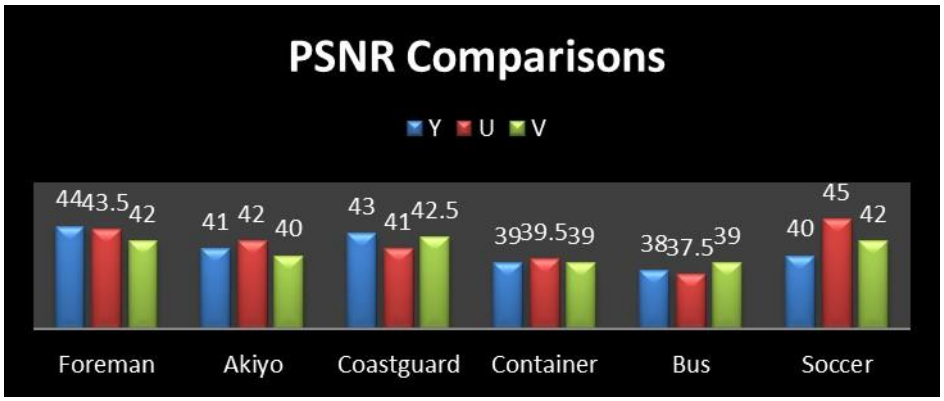

Figure 5. Difficult and Speedy PSNR Of The Y-Components

(Image Source: Khaled Elleithy, 2014, IEEE LISAT)

Table:1. PSNR component of U and V

(Source: Khaled Elleithy, 2014, IEEE LISAT)

Sequence	**Forcman**	**Akiyo**	**Coastguard**	**Container**	**Bus**	**Soccer**
	44	41	43	39	38	40
U	43.5	42	41	39.5	37.5	45
V	42	40	42.5	39	39	42

Table: 2. Combination of PSNR components

(Source: Khaled Elleithy, 2014, IEEE LISAT)

Sequences	PSNRY	PSNRU	PSNRV	PSNR
Foreman	43.25	50.25	48.25	39.51
Allyn	55.25	55.18	40.69	40.32

Coastatutrel	40.45	56.25	45.85	52.69
Container	38.25	49.36	40.58	40.3
Bus	36.99	40.96	30.11	40.85
Soccer	44.52	40.22	42.94	85.25

In Figure. 5, we calculate the slow and fast PSNR of the Y-components for each of the six files. Taking everything into account, the brightness of the Akiyo video is excellent. For each of the six records, there is also a clue at the U component PSNR. The PSNR-U measurements on the Coast Guard footage are the finest of all. In the same way, you can calculate the PSNR of the V-component for each and every one of the fundamentals. PSNR-V was utilised to capture the Coast Guard footage, so it is of the highest quality.

Figure 5 shows the PSNR for each of the 150 edges in each video. Based on the marriage, the final objective first-class outcome for all Foreman, Akiyo, Coastguard, Compartment, Bus, and Soccer bills was between 38.95% and 42.73% dBs. Several pieces of legislation are affected by the PSNR. These include the Foreman, Akiyo, Container, and Bus bills. The ideas behind the Coastguard and Soccer bills are still developing. These things are a direct result of how these bills encourage more competition for resources, which in turn makes things look less nice. The PSNR midpoints for each Y, U, and V segment are shown in Table 1 and 2. At these points, video cuts can always be made in the middle. More than that, each film's visual concept is scored separately by taking the average of all 150 edges. We do this so that each picture can be judged on its own. The type of recording and the rate at which something is changing determine the range of midpoints.

Approach:

Using img read, load the image into variable J. ().

In the r and c variables, you must put the number of rows and the number of columns in image. Create zero matrices Red, of size rXc.

Save the image's associated color plane in the appropriate zero matrix of Red Component.

To see the photos, use the img show() function, but first change their type to uint8.

```
% code in MATLAB to display the red,

% a colour image's colour planes

% image reading

I = imread ('lenna.png');

% number of rows and the columns in the image

 r = size (I, 1);

c = size (I, 2);

% making zero matrices R = zeros (r, c, 3);

% saving the associated colour plane

% red plane

R (:, :, 1) = I (:, :, 1);

% displaying the images figure 6, imshow(uint8(R));
```

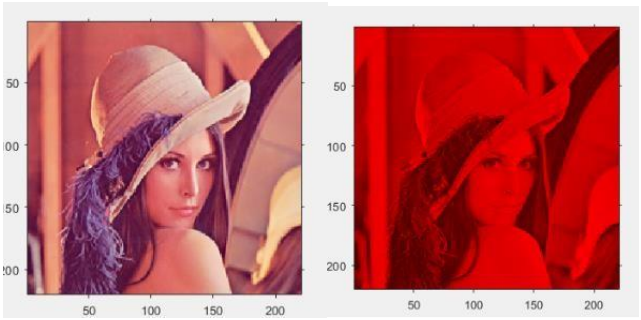

Figure 6: The images figure, im show(uint8(R));

VI. CONCLUSION

This article proposes a DCT-based solid video steganography technique that takes into account BCH bocce helper code. Steganography estimation converts the film into a system, and after a while, separates each edge into parts Y, U, and V. In front of the presentation system, mysterious messages are shuffled and encoded using BCH code. Each YUV section was submitted to 2DDCT. DCT factor regardless of each YUV part. With the exception of the DC coefficient, the DCT coefficient is used to enter the bound information

REFERENCES

[1] M.Al-Shatanawi, Odai & EL-Emam, Nameer. (2015). A New Image Steganography Algorithm Based on MLSB Method with Random Pixels Selection. International Journal of Network Security & Its Applications. 7. 37-53. 10.5121/ijnsa.2015.7203. VL – 7

[2] J.R. Krenn,"Steganography and Steganalysis", January 2004.

[3] Beenish Mehboob, Rashid Aziz Faruqui,"A Steganography Implementation", IEEE 2008

[4] Chen Ming, Zhang Ru, NiuXinxin, Yang Yixian, "Analysis of Current Steganography Tools: Classifications & Features" , International Conference on Intelligent Infor- mation Hiding and Multimedia Signal Processing (IIH-MSP'06), IEEE2006

[5] Jung, K. H." Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane." Journal of Real-Time Image Processing, 14(1), 127-136. 2006

[6] Alturki, F., & Mersereau, R. "Secure blind image steganographic technique using discrete fourier transformation." In Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205) (Vol. 2, pp. 542-545). IEEE.

[7] Ansari, E., Keshtkaran, M., Wallace, R., Mirsadeghi, S. M. H., & Ansari, F. "OOPAP and OPVD: Two Innovative Improvements for Hiding Secret Data Into Images." Iranian Journal of Science and Technology, Transactions of Electrical Engineer- ing, 43(1), 55-65.

[8] Barni, M., Bartolini, F., and Checcacci, N. "Watermarking of MPEG-4 video objects Multimed." IEEE Trans. 7, 23–32. 2005.

[9] Bhattacharyya, S., & Sanyal, G." Hiding Data in Images Using Pixel Mapping Method (PMM)". In security and Management July, 2010, pp. 683-689.

[10] Chin-Chen, T. D. Kieu, and C. Yung-Chen, "A High Payload Steganographic Scheme Based on (7, 4) Hamming Code for Digital Images," in Electronic Commerce and Se- curity, 2008 International Symposium on, 2008, pp. 16-21.

[11] Das, R. and Tuithung, T. "A novel steganography method for image based on Huffman Encoding," in Proceedings of the 2012 3rd National Conference on Emerg- ing Trends and Applications in Computer Science, (Piscataway, NJ: IEEE),2012, pp. 14–18.

[12] Diop, S. M. Farss, K. Tall, P. A. Fall, M. L. Diouf, and A. K. Diop, "Adaptive ste- ganography scheme based on LDPC codes," in 2014 16th International Conference on Advanced Communication Technology (ICACT), 2014, pp. 162-166.

[13] Ghosal, S. K., Mandal, J. K., & Sarkar, R "High payload image steganography based on Laplacian of Gaussian (LoG) edge detector." Multimedia Tools and Applications, 77(23), 2018, pp. 30403-30418.

[14] Hong, W., & Chen, T. S. " A novel data embedding method using adaptive pix- el pair matching." IEEE transactions on information forensics and security, 7(1), 2012, pp.176- 184.

[15] Horng, S.-J., Rosiyadi, D., Fan, P., Wang, X., and Khan, M. K. "An adaptive watermarking scheme for e-government document images." Multimed. Tools Appl. 72, 2014, pp. 3085–3103.

[16] Huang, J., and Shi, Y. Q." Reliable information bit hiding. Circuits Syst. Video Technol." IEEE Trans. 12, 2002, pp. 916–920.

[17] Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H." Image steganography in

[18] spatial domain: A survey." Signal Processing: Image Communication, 65,2018.pp. 46-66.

[19] J. Mstafa and K. M. Elleithy, "A video steganography algorithm based on Kanade- Lucas-Tomasi tracking algorithm and error correcting codes," Multimedia Tools and Applications, 2013, pp. 1-23.
[20] K. Jain, Fundamentals of digital image processing: Prentice-Hall, Inc., 1989.
[21] Kapotas, S. K. and Skodras, A. N. “A new data hiding scheme for scene change detection in H. 264 encoded video sequences,” in Proceedings of the 2008 IEEE International Conference on Multimedia and Expo, Hannover.
[22] Ke, N. and Weidong, Z. “ A video steganography scheme based on H. 264 bit- streams replaced,” in Proceedings of the 4th IEEE International Conference on Soft- ware Engineering and ServiceScience (ICSESS), Beijing, 2013, pp. 447–450.
[23] Khan, A. and Malik, S. A.” A high capacity reversible watermarking approach for authenticating images: exploiting down-sampling, histogram processing, and block selection.” Inform. Sci. 256, 2013, pp. 162–183.
[24] L. Guangjie, L. Weiwei, D. Yuewei, and L. Shiguo, "An Adaptive Matrix Embedding for Image Steganography," in Multimedia Information Networking and Security (MINES), 2011 Third International Conference on, 2011, pp. 642-646.
[25] Liu, T., & Qiu, Z. DA. “DWT-based color image steganography scheme.” In 6th International Conference on Signal Processing, 2002. (Vol. 2, pp. 1568-1571). IEEE.
[26] Luo, W., Huang, F., & Huang, J. “Edge adaptive image steganography based on LSB matching revisited.” IEEE Transactions on information forensics and security, 5(2),2010, pp.201-214.
[27] Maji, G., Mandal, S., Sen, S., & Debnath, N. C. “Dual image based LSB steganography.” In 2018 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom)(pp. 61-66). IEEE.
[28] Mandal, J. K., & Khamrui, A. “A genetic-algorithm-based steganography on colour images (GASCI).” International Journal of Signal and Imaging Systems Engi- neering, 7(1), 2014,59-63.
[29] Li, Z., & He, Y. “Steganography with pixel-value differencing and modulus function based on PSO.” Journal of information security and applications, 43, 2014, pp. 47-52.
[30] Mstafa, R. J. and Elleithy, K. M. “A novel video steganography algorithm in DCT domain based on hamming and BCH codes,” in Proceedings of the 2016 IEEE 37th Sarnoff Symposium, (Newark, NJ: IEEE), 2016, pp. 208–213.
[31] Mstafa, R. J. and Elleithy, K. M.”Compressed and raw video steganography techniques: a comprehensive survey and analysis.” Multimed. Tools Appl. 75, pp. 10311– 10333.
[32] Mstafa, R. J., and Elleithy, K. M. “A new video steganography algorithm based on the multiple object tracking and hamming codes,” in Proceedings of the 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA), (Piscataway, NJ: IEEE), 2015, pp. 335–340.
[33] Muhammad, K., Sajjad, M., Lee, M. Y., and Baik, S. W. “ Efficient visual attention driven framework for key frames extraction from hysteroscopy videos.” Bio- med. Signal Process. Control 33, 2015, pp. 161–168.
[34] Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., and Baik, S. “A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. Multimed. Tools Appl. 2015, pp. 1–27.
[35] R. J. Mstafa and K. M. Elleithy, "A highly secure video steganography using Hamming code (7, 4)," in Systems, Applications and Technology Conference (LISAT), 2014 IEEE Long Island, 2014, pp. 1-6.
[36] R. Zhang, V. Sachnev, and H. Kim, "Fast BCH Syndrome Coding for Steganography," in Information Hiding. vol. 5806, S. Katzenbeisser and A.-R. Sadeghi, Eds., ed: Springer Berlin Heidelberg, 2009, pp. 48-58.
[37] R. Zhang, V. Sachnev, M. B. Botnan, H. J. Kim, and J. Heo, "An efficient embedder for BCH coding for Steganography," Information Theory, IEEE Transactions on, vol. 58, pp. 7272-7279, 2012.
[38] Sajjad, M., Muhammad, K., Baik, S. W., Rho, S., Jan, Z., Yeo, S.-S., et al. “Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices. Multimed. Tools Appl. 2015, pp. 1–18.
[39] Shanableh, T. “Data hiding in MPEG video files using multivariate regression and flexible macroblock ordering.” Inform. For. Secur. IEEE Trans. 7, 2012, pp. 455–464.
[40] Swain, G. “ Very high capacity image steganography technique using quotient value differencing and LSB substitution.” Arabian Journal for Science and Engineer- ing, 44(4), 2019, pp. 2995 3004.
[41] W. Jyun-Jie, C. Houshou, L. Chi-Yuan, and Y. Ting-Ya, "An embedding strategy for large payload using convolutional embedding codes," in ITS Telecommunications (ITST), 2012 12th International Conference on, 2012, pp. 365-369.
[42] R. J. Mstafa and K. M. Elleithy, "A New Video Steganography Algorithm Based on the Multiple Object Tracking and Hamming Codes," in 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA), 2015, pp. 335-340.
[43] Walia, G. S., Makhija, S., Singh, K., & Sharma, K. “ Robust stego-key directed LSB substitution scheme based upon cuckoo search and chaotic map.” Optik, 170, 2018, pp. 106-124.
[44] Wang, H., & Wang, S.” Cyber warfare: steganography vs. steganalysis. Communications of the ACM”, 47(10), 76-82.

[45] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," IEEE Transaction

[46] Xu, C., Ping, X., and Zhang, T. “Steganography in compressed video stream,” in Proceedings of the 1st International Conference on Innovative Computing, Infor- mation and Control, (Beijing: IEEE), 2006, pp. 269–272.

[47] Rajawat, A.S., Rawat, R., Mahor, V., Shaw, R.N., Ghosh, A. “ Suspicious Big Text Data Analysis for Prediction—On Darkweb User Activity Using Computational Intelligence Model. In: Mekhilef, S., Favorskaya, M., Pandey, R.K., Shaw, R.N. (eds) Innovations in Electrical and Electronic Engineering. Lecture Notes in Electrical En- gineering, vol 756. Springer, Singapore. https://doi.org/10.1007/978-981-16-0749- 3_58

[48] Y. Liu, Z. Li, X. Ma, and J. Liu, "A Robust Data Hiding Algorithm for H. 264/AVC Video Streams," Journal of Systems and Software, 2013.

[49] Yang, C. H., Weng, C. Y., Wang, S. J., & Sun, H. M. Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Transactions on Infor- mation Forensics and Security, 3(3),2008, pp. 488-497.

[50] Rajawat, A.S., Rawat, R., Barhanpurkar, K., Shaw, R.N., Ghosh, A. “ Block- chain-Based Model for Expanding IoT Device Data Security. In: Bansal, J.C., Fung, L.C.C., Simic, M., Ghosh, A. (eds) Advances in Applications of Data-Driven Com- puting. Advances in Intelligent Systems and Computing, vol 1319. Springer, Singa- pore. https://doi.org/10.1007/978-981-33-6919-1_5

[51] Ram Kumar, Manoj Eknath Patil ,” Improved the Image Enhancement Using Filtering and Wavelet Transformation Methodologies”, Turkish Journal of Computer and Mathematics Education ,Vol.13 No.3(2022), 987