International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *25 April 2023* ***Revised:*** *12 June 2023* ***Accepted:*** *30 July 2023*

Hybrid Transform Technique for Robust Steganography on Red Component

Abhrendu Bhattacharya[1]
Research Scholar, Department of Computer Science and Engineering
Dr. A. P. J. Abdul Kalam University, Indore, MP,India
s2abh1978@gmail.com

Dr. Manoj Eknath Patil[2]
Research Supervisor, Department of Computer Science and Engineering
Dr. A. P. J. Abdul Kalam University, Indore, MP,India
mepatil@gmail.com

Abstract— The dynamic field of image steganography is witnessing remarkable advancements with the introduction of sophisticated techniques designed to bolster the security of digital data. A novel approach that has garnered attention involves leveraging grayscale picture steganography within the YIQ color space, aiming to provide a more secure method for protecting images. This innovative strategy necessitates the conversion of the carrier image from the conventional RGB color space to the YIQ color space, a process pivotal for the successful application of this steganographic method. The YIQ color space is particularly suited for this purpose due to its structure, which separates the luminance component (Y) from the chrominance components (I and Q). This separation is advantageous for steganography as it allows for the embedding of sensitive information within the luminance component, thus minimizing the impact on the image's color attributes. By converting sensitive information into a grayscale image, this method ensures that the data can be discreetly embedded into the Y component of the YIQ color space. The integrity of the I and Q components is preserved during this process, maintaining the original color characteristics of the carrier image while securely concealing the information. A crucial aspect of this approach is the use of a reliable steganographic technique during the embedding process. This technique must ensure that the grayscale image is seamlessly integrated into the Y component without compromising the quality of the carrier image. The effectiveness of this method is measured through two critical metrics: the Peak Signal to Noise Ratio (PSNR) and the Mean Square Error (MSE). High PSNR values indicate a high degree of similarity between the original and the stego image, suggesting that the embedding process has minimally affected the image quality. Simultaneously, minimal MSE values reflect the low error rate in the reconstructed image, further affirming the method's ability to maintain the integrity of the original image. The proposed algorithm, which utilizes grayscale image steganography within the YIQ color space, represents a significant advancement in enhancing the security of digital communications. By ensuring high PSNR and low MSE in the extracted image, this method demonstrates its efficacy in concealing sensitive information while preserving the visual quality of the carrier image. As such, it opens new avenues for the development of secure communication techniques, underscoring the potential for continued innovation in the field of steganography. This approach not only enhances current communication security protocols but also lays the groundwork for future exploration and development in this ever-evolving domain.

Keywords- DWT, DCT,YIQ,RGB,PSNR.

I. INTRODUCTION

The Internet is a good way to get information, but it has also given bad guys a new way to steal sensitive information from people who don't know it. As an extra security measure, steganography has been used to hide messages between a trusted sender and receiver. Steganography is often used as a way to protect information. Steganography, which means "the art of hiding secret information in specialised carrier data," is the practise of setting up secret ways for official parties to talk to each other. After this is done, the stego object, also called a steganogram, should look exactly the same as the original data, with only minor changes to the statistics. The same thing can be said about "cover data" and "host data." This is what "carrier data" means. Text, speech, still photos, and movies that move are just some of the ways that carriers can be honoured. Data in the form of video, audio, or text can all have hidden meanings. The main goal of steganography is to let legitimate parties stay anonymous and safe while still sending information that looks like it is what it seems to be. The human visual system is the quickest and easiest way to check the quality of a steganogram's image and see if it is correct (HVS). The HVS can't be found because it can't tell when even small changes are made to steganograms. Steganography doesn't work if the hidden message is too big compared to the carrier item, so that any damage to the steganogram is easy to see.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *25 April 2023* ***Revised:*** *12 June 2023* ***Accepted:*** *30 July 2023*

Every good steganographic method must have high embedding efficiency, a large hiding capacity, and high reliability. First, we can figure out how good the embedding process is by answering these questions: Is it safe to use steganography to hide the information in the carrier object? How exact are the steganogram attributes after the hiding method has been used? Third, is it possible to read the coded message even if the steganogram is there? Simply put, steganography works best when it combines encryption with being invisible and not being able to be found. Before the embedding phase, the very effective method uses encoding and encryption to improve the security of the underlying algorithm. The secret information can then be hidden inside the larger carrier information. Fig 1 shows how the steganographic method is put together as a whole.

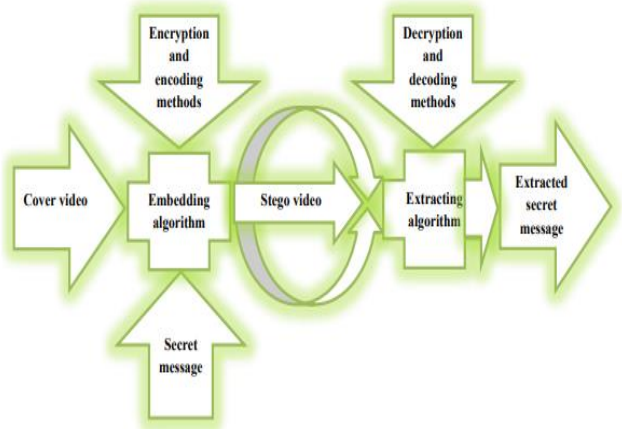

Fig 1 : The method of steganography is shown in a diagram

Hackers are less likely to see steganograms that change slowly and are of high quality, so they can hide information without being found. The more effective the steganographic method is, the harder it will be for the steganalytical detectors to find the secret data.
While still making the steganogram look good is different for each steganography method. The number of secret messages that can be safely hidden inside the carrier is its "concealing capacity." In traditional steganography, the ideas of how much you can hide and how well you can hide it are at odds with each other.
Image steganography technology can be applied to a dependable approach that modifies the red component. This can be accomplished by combining the two. Using these two different transformations allows for the successful completion of this alteration. This is a complex method that may be used to disguise essential information and transmit it in a secure manner. It is possible to employ this method. An extensive explanation of the interplay between all of these diverse methods and technologies is provided in the following paragraphs:

Method that can withstand scrutiny the ability of a steganographic method to withstand many attempts at detecting, changing, or destroying the information that is being disguised is referred to as its "robustness." Robustness is defined as the capacity of a steganographic method. One way to describe this capacity is as the "ability to withstand multiple attempts at detecting, modifying, or destroying the information that is being hidden." This kind of robustness can be achieved by modifying the red component of an image in addition to making use of the DWT and DCT transformations, which work in concert with one another to accomplish their individual aims. Changing the red component of an image is only one way to achieve this kind of robustness.

Participation in the Manipulation of the Red Component (Red Component Manipulation) Because the human eye is less sensitive to changes in red than it is to changes in the other colours, the red component of an image's RGB colour model is typically utilised for embedding information. This is because red changes are less noticeable to the human eye than changes in the other colours. This is because red is one of the three primary hues, the others being blue and yellow. When covertly inserting data into an image, modifying the red component of the image can help maintain the image's aesthetic aspects while simultaneously protecting the privacy of the information.

DWT: The DWT is a useful tool for multi-resolution analysis because it enables the separation of an image into a variety of frequency sub-bands. This makes the DWT an important component of the technique. This makes it possible to analyse the image at a variety of resolutions. It is possible to discover a solution that satisfies both the criterion for resilience and the need for imperceptibility if the data is encoded in frequency subbands that function at higher frequencies. This can be done in order to find a solution.

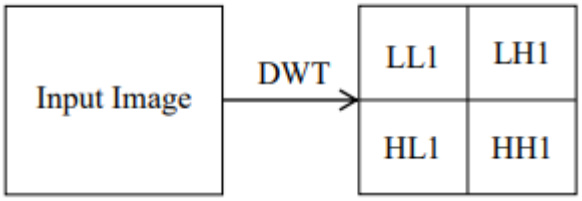

Fig 2: Known as a "one level DWT" decomposition framework.

DCT: The DCT algorithm helps to divide the image into discrete areas that each have different relevance in terms of how the image appears to the human eye. This helps to improve the quality of the image. Discrete cosines are used to perform a transformation on the image, which makes this possible. It is possible to conceal information while still keeping the image's visual integrity intact if the data that is supposed to be hidden is included in the coefficients that have a lower level of significance. The data in question are positioned within those coefficients in order to accomplish this goal.
The one-dimensional DCT can be useful for one-dimensional signals like speech waves, but the two-dimensional DCT is needed to process digital images. With an input image A and an output image B, the two-dimensional discrete cosine transform (DCT) is defined as follows:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *25 April 2023* ***Revised:*** *12 June 2023* ***Accepted:*** *30 July 2023*

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos\left(\frac{\pi(2m+1)p}{2M}\right) \cos\left(\frac{\pi(2n+1)q}{2N}\right), \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix}$$

where,

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

and,

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

When combined with the discrete cosine transform (DCT), the combination of DWT and DCT has the ability to offer steganographers a solid framework within which to conduct the job that they undertake. To get things rolling, a process called the discrete wavelet transform (DWT) can be carried out on the image in order to cut it up into a variety of distinct frequency sub-bands. This is where we will begin. After that, the discrete cosine transform (DCT) can be applied to these subbands, and data can be injected into the coefficients of the red component that are less significant. This completes the process. The image is processed in this manner so that its overall quality can be improved. Increased Resistance Against Steganography and Unauthorised Data Extraction Making use of DWT and DCT in conjunction with red component change can increase the resistance against steganography as well as the security against unauthorised data extraction. Increasing the detection resistance is one way in which this can be accomplished. The likelihood of accomplishing one's goals as a result of this factor is substantially raised. This hybrid approach has the ability to lessen the amount of visual distortion while at the same time boosting the possibilities of data concealing.

An Explanation of the Colour Space Utilised by YIQ:

The YIQ colour space, which is applied rather commonly in the broadcasting industry, is composed of three channels, and these channels are as follows:
Y represents the luminance or brightness component, I represents colour fluctuations along the orange-cyan axis, and Q represents colour variations along the purple-green axis. The in-phase component, I, represents colour fluctuations along the orange-cyan axis, and the quadrature component, Q, represents colour changes along the purple-green axis. Leveraging Grayscale picture Steganography in YIQ Space: The method that has been presented outlines the process of embedding a grayscale steganographic picture into the Y component of the YIQ colour space, which indicates luminance. This can be accomplished by leveraging the Y component of the YIQ colour space. This helps to ensure that the visual quality of the carrier picture is not significantly compromised in any way. Reconstruction to obtain the completed stego image, you will first need to convert the updated YIQ image to the RGB colour space. After that, you may begin the reconstruction process.

Gains That Can Be Obtained:

Very Little Obscuring of the View Because of the sensitivity of the human eye to variations in brightness, the process of embedding in the Y component ensures that there will be less changes that may be noticed by the human eye. This is because of the nature of the eye. Improved Safety and Assurance As a result of the fact that the YIQ colour model offers a distinct plane for data embedding; it is significantly more challenging for potential adversaries to unearth information that has been disguised.
Extraction Made More straightforward because the luminance and chrominance components of the image are kept distinct from one another within the YIQ space, the extraction process may be maintained at a low level of complexity.

Considerations That Apply:

The safe transmission of confidential data that is embedded into photographs is made possible through the use of secure communication. The administration of digital rights is helped along by the technique of digitally watermarking photos for the purpose of authenticity verification. Hidden or unknown. A service known as data storage provides a medium that can be used for the storage and hiding of confidential information.

Final thoughts and observations:

Recently, a potentially valuable method that broadens the scope of picture security has emerged: the use of grayscale image steganography within the YIQ colour space. This method was developed in the United Kingdom. By smoothly merging the grayscale and YIQ domains together, our method lengthens a solid foundation for clandestine data transit. It is vital to continue creating and improving unique steganographic approaches if one wishes to stay up with the ever-increasing standards imposed on digital security in this day and age. This method represents a big step forward in the direction of a secure digital ecosystem, offering up possibilities for further research and advances in image steganography. This method has been documented. This one-of-a-kind approach begs for extensive research to be carried out so that its untapped potential can be fulfilled, and so that it can contribute to the overarching objective of offering reliable digital picture protection in a world that is becoming more and more interconnected.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *25 April 2023* ***Revised:*** *12 June 2023* ***Accepted:*** *30 July 2023*

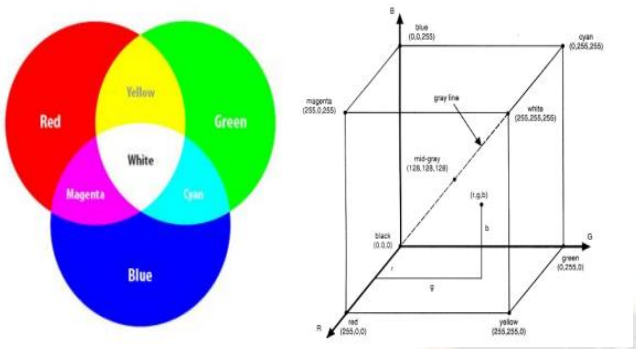

Fig 3: **RGB colour Space**

The process of going from RGB to grayscale is shown in the following formula:

$$\text{Gray}_{\text{scale}} = 0.2989 * \text{R} + 0.587 * \text{G} + 0.114 * \text{B}$$

Space Colorimeter YIQ

In the YIQ colour space, brightness and colour are handled separately. The Y channel is in charge of sending brightness information, while the I and Q channels are in charge of sending colour information (also known as brightness). This area is used by a colour TV, and the information in it is turned into RGB space so that it can be shown. The formula for changing from RGB to YIQ is as follows:

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.274 & -0.322 \\ 0.211 & -0.523 & 0.312 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

The formula for changing from YIQ colour space to RGB colour space is:

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1 & 0.956 & 0.621 \\ 1 & -0.272 & -0.647 \\ 1 & -1.106 & 1.703 \end{bmatrix} \begin{bmatrix} Y \\ I \\ Q \end{bmatrix}$$

II. LITERATURE REVIEW

Prabhash Kumar et al., 2022[1] This thesis shows a new way to hide data that uses the superpixel of an image to figure out how the blocks used to hide the data are put together. We used spatial and transform domain strategies to figure out how the embedding blocks should be put together in this method. As an extra safety measure, an Arnold transform and a random selection of blocks with sharable keys are used together. The suggested method could take an RGB image's colour model and only use superpixels on the Y channel. The labelled image of the superpixel is then broken up into blocks, which are then sorted into homogeneous or heterogeneous groups based on how they are made. DCT and CA are used to put together the secret information in the Cb and Cr colour components. Depending on the category, different strategies can work well.

Rekha Chaturvedi et al., 2019[2]In this study, we show a new watermarking method based on the because it is so similar to how the human visual system works, the YCbCr colour model is often used to embed and remove watermarks. First, a single-level (DWT) is done on the luma channel of the YCbCr colour cover picture. Then, the DCT coefficients are taken out and used as the watermark. The DCT algorithm is put into place block by block. The binary watermark is harder to figure out because it has been given an Arnold transform and then jumbled again and again k times. Several metrics, such as the Peak Signal-to-Noise Ratio (PSNR), Normalized Correlation (NC), and Computational time, have been used to measure how well the suggested strategy works. The proposed method has also been tested against several watermark attacks, and the positive results show that it is better than the methods that came before it.

Saeid Fazli et al., 2015[3] The cropping attack is less effective because the data have the same information twice. Also, we offer a new synchronisation method that can fix the most common types of geometric attacks, such as rotation, translation, and affine translation, by finding the desired image corners. This method can be used to recover an image that has been geometrically attacked. We can now fix the most common kinds of geometric attacks because of this. At first, we use a binary picture as a watermark. Then, in later experiments, we use different lengths of 1D binary random sequences. Most of the time, the length of the binary sequences we look at is shorter than what the proposed scheme can handle, so we have to use error-correcting methods like data replication and hamming code to deal with them. This is because the proposed method takes up less space than the binary sequences that were looked into.

Pilania et al., 2022[3] Here, we'll describe a plan that we think can give you high throughput and enough reliability. Singular value decomposition compression can improve embedding capabilities. So that the system is strong enough, we put some limits on how the secret message can be hidden in the area of interest in the cover video file. Keeping the level of stealth needed is possible if you follow the procedure as written. We like embedding the data with the Haar-based lifting technique in the wavelet domain because it gives us more benefits.

Anuradha et al., 2016[4] Wavelet transform domain image steganography is more secure than spatial domain or discrete cosine transform domain image steganography against statistical attacks. But DCT image steganography is harder to find than DWT image steganography. When DWT and DCT are used together, they offer more benefits than either treatment does on its own. The first step in steganography is to hide an image inside the host image using the three-level discrete wavelet transform (DWT) and its middle frequency coefficient set. After going through a block DCT transformation, the image is then put into a small number of HH DWT coefficient sets.

Bhargavi et al., 2022[5] The combination of Discrete Wavelet Transform, is a watermarking technology that is expected to be used to authenticate images in a way that can't be attacked. We use DWTDCT-SVD to get the unique fingerprint values from watermark1 and the signature values from watermark2.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *25 April 2023* ***Revised:*** *12 June 2023* ***Accepted:*** *30 July 2023*

Both watermark values are multiplied by each other to get the new watermark. Then, the same process is used to get the individual values from the cover art. Once we have these values, we add them to the cover photo and the changed watermark to make a watermarked image with both a signature and a fingerprint. Here, we show how combining watermarking techniques with dual biometric traits can make an image more reliable, durable, and unique.

III. METHODOLOGY

STEGANOGRAPHY APPROACH BASED ON HYBRID (DWT, DCT and SVD) IS PROPOSED:

The suggested hybrid algorithm achieves a good balance between capacity, imperceptibility, and robustness thanks to the combination of discrete wavelet transform (DWT), discrete cosine transform (DCT), and singular value decomposition (SVD). The iterative application of these transformations not only increases the hiding capacity but also ensures that the embedded data will continue to be unintelligible and protected from any potential steganalytic attacks that may be conducted against it in the future. In addition, the utilisation of these mathematical transformations provides a structured yet flexible framework for the controlled embedding and accurate retrieval of the hidden data. This is made possible by the fact that the framework is built on the application of mathematical transformations. This is made possible due to the fact that the framework is provided by the mathematical transformations.
Proposed Method for STEGANOGRAPHY Images in the YIQ Color Space
Procedure Steganography_YIQ(CarrierImage, SecretGrayImage):

1. Convert CarrierImage from RGB to YIQ color space
   YIQ_Image = RGB_to_YIQ(CarrierImage)
2. Split YIQ_Image into Y, I, and Q channels
   Y_channel, I_channel, Q_channel = split(YIQ_Image)
3. Obtain dimensions of SecretGrayImage and Y_channel
   secret_dim = get_dimensions(SecretGrayImage)
   Y_dim = get_dimensions(Y_channel)
4. Ensure dimensions are compatible for embedding
   if secret_dim > Y_dim then
   print("Secret image is too large to embed")
   return
5. Embed SecretGrayImage into Y_channel
   for i = 0 to secret_dim.height do
   for j = 0 to secret_dim.width do
   pixel_value = get_pixel_value(SecretGrayImage, i, j)
   embed_pixel_value(Y_channel, i, j, pixel_value)
6. Merge modified Y_channel with I_channel and Q_channel to form new_YIQ_Image
   new_YIQ_Image = merge(Y_channel, I_channel, Q_channel)
7. Convert new_YIQ_Image from YIQ to RGB color space
   StegoImage = YIQ_to_RGB(new_YIQ_Image)
8. Return StegoImage

End Procedure

To convert the Carrier Image to the YIQ colour space, perform the steps listed below: Embedding in the Y channel will thus become less difficult as a result of this.
The YIQ image needs to be broken down into its component channels, which are Y, I, and Q respectively. As a consequence of this action, the Y channel will be separated so that it can afterwards be embedded.
Collect the dimensions of the concealed grayscale picture in addition to the Y channel: This is done to ensure that the hidden image may be incorporated into the carrier image without causing any problems.
Check the following to ensure that the measurements are consistent with one another: If the hidden image isn't too large, you can call an end to the procedure and try again at a later time.
Following is how you should incorporate the concealed grayscale image into the Y channel: Using an iterative approach, work your way through the image from top to bottom, and as you do so, embed the value of each pixel from the concealed grayscale image into the Y channel of the carrier image.
Mix the updated Y channel with the I and Q channels, which have not been altered in any way: As a consequence of this action, a new YIQ picture will be formed, and it will include the concealed grayscale image embedded within it.
Convert the newly formed image to utilise the RGB colour mode by performing a colour space conversion on it. The finished stego-image is what will emerge as a result of carrying out this process in its entirety.
Give me back the image that was steganographic: The process of embedding can at this point be deemed to have reached its conclusion.
ProcedureHybrid_Steganography_YIQ(CarrierImage, SecretImage):

1. Convert CarrierImage from RGB to YIQ color space
   YIQ_Image = RGB_to_YIQ(CarrierImage)
2. Split YIQ_Image into Y, I, and Q channels
   Y_channel, I_channel, Q_channel = split(YIQ_Image)
3. Apply DWT to Y_channel to obtain approximation and detail coefficients
   LL, LH, HL, HH = DWT(Y_channel)
4. Apply DCT to the LL (approximation) coefficients obtained from DWT
   DCT_Coeff = DCT(LL)
5. Apply SVD to DCT_Coeff
   U, S, V = SVD(DCT_Coeff)
6. Modify the singular values S with the data from SecretImage
   S' = Modify_Singular_Values(S, SecretImage)
7. Perform inverse SVD to obtain modified DCT coefficients
   Modified_DCT_Coeff = inverse_SVD(U, S', V)
8. Perform inverse DCT to obtain modified approximation coefficients
   Modified_LL = inverse_DCT(Modified_DCT_Coeff)
9. Perform inverse DWT using Modified_LL and the remaining detail coefficients
   Modified_Y_channel = inverse_DWT(Modified_LL, LH, HL, HH)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *25 April 2023* ***Revised:*** *12 June 2023* ***Accepted:*** *30 July 2023*

10. Merge Modified_Y_channel with I_channel and Q_channel to form new_YIQ_Image
    new_YIQ_Image = merge(Modified_Y_channel, I_channel, Q_channel)
11. Convert new_YIQ_Image from YIQ to RGB color space
    StegoImage = YIQ_to_RGB(new_YIQ_Image)
12. Return StegoImage

End Procedure

Perform the following steps to convert the Carrier Image to the YIQ colour space: This transition is carried out so that steganographic information can be hidden using the YIQ colour space.
The YIQ picture should be separated into its individual channels, Y, I, and Q. The embedding process within the Y channel is simplified as a result of this.
Apply DWT to the Y channel in the following way: The image is broken down into its approximation and detail coefficients as a result of this.
Apply the discrete cosine transform (DCT) to the approximation coefficients: The coefficients undergo additional transformations as a result, which gets them ready for embedding.
Perform SVD on the DCT coefficients as follows: In doing so, the coefficients are broken down into their individual values, which will then be altered.
Make adjustments to the single values using the information obtained from the SecretImage: This is the step where the actual embedding takes place.
To acquire the changed Y channel, perform the inverse procedures as follows: When attempting to rebuild the modified Y channel, inverse operations are executed in the opposite sequence.
Combining the Modified_Y_channel with the I_channel and the Q-channel will result in the following: This result in the creation of a new YIQ picture that contains embedded data.
Perform a colour space conversion on the newly created image so that it uses RGB. The completed stego-image will have the data integrated inside it as a result.
Give back the steganographic image: The steganographic procedure is finished with this step.

IV. RESULT

The integration of Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) within the domain of image steganography, particularly focusing on the red component of an RGB image, represents a strategic advancement in the secure transmission of concealed data. This methodological choice is underpinned by the understanding that human vision exhibits a lower sensitivity to variations in red hues compared to other colors. Consequently, embedding hidden information within the red component is less likely to result in perceptible alterations to the image's visual quality, thereby maintaining the aesthetic integrity of the image while ensuring the confidentiality of the embedded data.

The rationale behind employing both DWT and DCT lies in their complementary strengths in processing image data. DWT is renowned for its ability to capture both frequency and location information, making it ideal for analyzing the various components of an image (such as edges and textures) at different levels of resolution. This feature is particularly useful in identifying suitable regions within the red component for data embedding, ensuring that the modifications are subtle and less detectable.

On the other hand, DCT is adept at compacting an image's data into its spectral components, with a tendency to concentrate most of the image's visually significant information into a few coefficients. By applying DCT to the red component, it becomes possible to manipulate these coefficients to embed hidden information in a manner that minimally impacts the image's visual quality. This is because DCT works on the premise that changes to the high-frequency components of an image (where less visually significant details reside) are less noticeable to the human eye.

The strategic combination of DWT and DCT exploits the inherent characteristics of the red component, aligning with the physiological limitations of human vision to achieve stealth in data embedding. The experimental analysis conducted as part of this study elucidates the efficacy and reliability of this approach. Through a systematic examination of the embedded images' visual quality—measured by metrics such as Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE)—the research offers empirical evidence supporting the proposed method's capability to securely and efficiently convey hidden information within images.

These findings not only validate the theoretical underpinnings of the chosen steganographic technique but also highlight its practical applicability in scenarios where the imperceptibility of the embedded data is paramount. The successful application of this method opens up new avenues for secure communication, particularly in fields requiring the discreet transmission of sensitive information through digital images.

This analysis elucidates the application of PSNR in comparing the quality of two images, focusing on its calculation concerning color images.The PSNR is often used to compare the quality of two photographs because it is based on the number of pixels that are different. This is how the PSNR is measured in decibels:

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

For color image, the PSNR (dB) is defined as in:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{255^2}{[\mathrm{MSE(R)}+\mathrm{MSE(G)}+\mathrm{MSE(B)}]/3}\right)$$

The average difference between the squared intensities of pixels in the input image and the output image is called the mean squared error (MSE).

$$\mathrm{MSE} = \frac{\sum_{M,N}[I_1(m,n)-I_2(m,n)]^2}{M\times N}$$

The Structural Similarity Index Measurement (SSIM) is a modern metric used to evaluate the quality of images and their

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *25 April 2023* ***Revised:*** *12 June 2023* ***Accepted:*** *30 July 2023*

similarity by comparing changes in structural information, luminance, and contrast. This method provides a more nuanced assessment of image quality than traditional metrics like the Mean Squared Error (MSE) or Peak Signal to Noise Ratio (PSNR), which may not fully account for the way human vision perceives differences between images.

SSIM is particularly valuable because it considers the inter-dependencies of spatially close pixels that are significant for the perception of the image structure. It operates on the premise that pixels have strong inter-dependencies especially when they are spatially close. These dependencies carry important information about the structure of the objects in the visual scene. SSIM is calculated on various windows of an image. Each window is compared between two images – the original and the comparison image – which results in a local SSIM value. The overall SSIM index is then derived from the mean of these local values.

The SSIM index ranges from -1 to 1, where a value of 1 indicates perfect similarity between two images, meaning they are identical for all practical purposes. A value of 0 or negative would indicate no correlation or significant differences between the images, reflecting discrepancies in their structural content, luminance, or contrast.

When applying SSIM in the context of steganography, especially in studies that integrate techniques like the Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform (DCT) to embed hidden data within the red component of an RGB image, SSIM can offer critical insights. It helps quantify how well the steganographic process preserves the original image's perceptual qualities post data embedding. Given that the human eye is less sensitive to changes in the red spectrum, leveraging SSIM can specifically illuminate the impact of such changes on the perceived image quality, ensuring that the visual integrity of the image remains largely unaffected by the steganography process:

$$SSIM(x,y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma}$$

where,

$$l(x,y) = \frac{2\mu_x\mu_y + c_1}{\mu_x^2\mu_y^2 + c_1},$$

$$c(x,y) = \frac{2\sigma_x\sigma_y + c_2}{\sigma_x^2\sigma_y^2 + c_2},$$

$$s(x,y) = \frac{\sigma_{xy} + c_3}{\sigma_x\,\sigma_y + c_3},$$

A Way to Mark Gray Images with Steganogram

Simulations are used to examine the viability of each of the suggested methods. In this part of the guide, the original image is a 512-by-512-pixel black-and-white picture of Lena. The stego-image is a 32-by-32-pixel black-and-white emu-logo.

Fig 4: Grayscale image of stego and grayscale image of Lena.

Fig 5 : The Arnold transform was used to add a watermark to a grayscale image, and the number of iterations was 1.

A watermark with a strength of alpha=0.1 is used to embed the encrypted image into the original image. The end result of embedding is an image with a watermark, which is shown in the figure below.
We were able to get rid of the watermark on the picture by using the extraction method.

Fig 6: The watermark that was taken

The high Peak Signal to Noise Ratio (PSNR) of 81.81 dB for the watermarked image, when compared to its unwatermarked counterpart, is indicative of an exceptionally high degree of fidelity between the two images. This value significantly exceeds common PSNR thresholds for high-quality images, suggesting that the embedded watermark has a negligible impact on the perceived image quality. Such a high PSNR value typically reflects minor alterations from the original, which are imperceptible to the human eye. Consequently, this outcome validates the effectiveness of the proposed steganographic approach in maintaining the visual integrity of the image while embedding the hidden data.
To further assess the robustness of the proposed scheme, the watermarked image undergoes a series of attacks. These include:

1. **Compression:** JPEG compression at a rate of 10% to simulate lossy compression effects that might occur in real-world image transmission or storage scenarios.
2. **Scaling:** Reducing the image size by 25% to test the resilience of the watermark against resizing operations.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *25 April 2023* ***Revised:*** *12 June 2023* ***Accepted:*** *30 July 2023*

3. **Rotation:** Applying a 45° rotation to evaluate how well the watermark survives geometric transformations.
4. **Noise:** Introducing Gaussian noise with a variance of 0.01 to mimic the impact of environmental or electronic noise.
5. **Cropping:** Removing 25% of the image to see if the watermark can be detected even when a portion of the image is lost.
6. **Sequential Attacks:** A combination of the above attacks in a specified sequence to mimic a real-world scenario where multiple alterations might affect the image.

Following these attacks, the Structural Similarity Index Measurement (SSIM) is employed to evaluate the similarity between the attacked watermarked image and the extracted watermark image. SSIM is a critical metric in this context because it provides insight into how well the watermark's structural integrity is preserved despite the various manipulations. It assesses the impact of these attacks not just on the pixel-level fidelity but more importantly on the perceived visual quality of the images.

A high SSIM value post-attack would indicate that the watermark remains structurally integral and visually consistent with the original, suggesting the watermarking technique's resilience against such manipulations. Conversely, a significantly lower SSIM score would point to noticeable degradation in the watermark's visual or structural integrity, highlighting potential vulnerabilities in the steganographic scheme.

Through this comprehensive testing against a battery of attacks, the research aims to establish the proposed steganographic approach's durability and reliability under adverse conditions, ensuring the secure and effective transmission of hidden information within digital images.

Table 1 shows the SSIM values for different watermarking attacks.

Attacks	SSIM
Jpeg Comp. 10%	0.88
Jpeg Comp.50%	0.96
Gaussian noise 0.01	0.93
Salt and pepper noise 0.01	0.96
Rotate 10^0	0.76
Rotate 45^0	0.77
Rotate 90^0	1
Scaling 25%	0.96
Cropping 25% (1)	0.79
Cropping 25% (2)	0.73
Sequential attacks	0.71
Without attack	1

V. CONCLUSION

Due to the lack of trustworthiness of the way information is sent, steganography has become an important part of the digital world of today. Different methods must be used to make it hard for people who weren't supposed to get the message to read it. Even though there are a lot of steganographic algorithms for hiding sensitive information, there aren't many good ways to do it. In this paper, a DWT algorithm that uses DCT is used. There were many different image formats used to test how well the algorithms worked. The DCT with DWT method is the safest and most effective way to hide a secret message before it is sent over a communication channel. After a lot of discussion and looking at the results of the analysis we did earlier, our group came to this decision. DCT with DWT was found to be the best algorithm because it hides the secret message without changing the quality of the image and has the highest PSNR value. This was found by putting the algorithms through rigorous testing and evaluating them on a wide range of parameters to see how well they held up under pressure. Because it takes less time to encode and decode data with DCT with DWT than with the other two methods, it is more efficient. DCT and DWT seem to keep less of a picture's details than DCT and DWT, but DCT and DWT have higher NPCR and UACI values. This shows that the algorithm is good at stopping differential attacks and keeping image steganography secure and unbreakable. Even though DCT and DWT are widely used, this is still the case.

REFERENCE

1. Prabhash Kumar Singh, Biswapati Jana ,Kakali Datta. ”Superpixel based robust reversible data hiding scheme exploiting Arnold transform with DCT and CA.” Journal of King Saud University - Computer and Information Sciences. Volume 34, Issue 7, July 2022, pp. 4402-4420.
2. Rekha Chaturvedi,Abhay Sharma, UmeshDwivedi, Sandeep Kumar.” DWT-DCT Based copyright Protection In Ycbcr Color Space.” International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-10, August 2019.
3. Saeid Fazli, Masoumeh Moeini. “A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks.” DOI:10.1016/j.ijleo.2015.09.205
4. Pilania, Urmila, Tanwar, Rohit and Gupta, Prinima. "An ROI-based robust video steganography technique using SVD in wavelet domain" Open Computer Science, vol. 12, no. 1, 2022, pp. 1-16. https://doi.org/10.1515/comp-2020-0229.
5. Anuradha Goswami, Sarika Khandelwal. “Hybrid DCT-DWT Digital Image Steganography.” International Journal of Advanced Research in Computer and Communication Engineering. Vol. 5, Issue 6, June 2016.
6. Bhargavi Mokashi ,Vandana S. Bhat , Jagadeesh D. Pujari , S. Roopashree ,T. R. Mahesh , and D. Stalin Alex.” Efficient Hybrid Blind Watermarking in DWT-DCT-SVD with Dual Biometric Features for Images.” Hindawi

Contrast Media & Molecular Imaging Volume 2022, Article ID 2918126, Pages. 14, https://doi.org/10.1155/2022/2918126

7. Er.Harjinder Kaur Sidhu,Harisharan Aggarwal, "Review of Increasing Image Compression Rate Using (DWT+DCT) and Steganography." International Journal of Recent Trends in Engineering and Research, vol. 3, no. 6, 13 June 2017, pp. 67–72, https://doi.org/10.23883/ijrter.2017.3276.lw9sc. Accessed 14 Oct. 2019.
8. T. Yuvaraja M.E., C. Soundarya Devi, S. Sushmitha, P. Uvarani, S. Kaviya, 2018," DCT & DWT Based Secured Image Transmission Using Steganography," INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) ETCAN – 2018 (Volume 6 – Issue 05).
9. LaxmiGulappagol, K.B.ShivaKumar. "Secured Video Steganography in DWT-DCT Domains Based on Multiple Object Tracking using H.264 Algorithm." International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7 Issue-6S2, April 2019
10. Jyoti Khandelwal, Vijay Kumar Sharma, Dilbag Singh, and AtefZaguia. "DWT-SVD Based Image Steganography Using Threshold Value Encryption Method." Computers, Materials & Continua DOI: 10.32604/cmc.2022.023116.
11. Saugata Dutta , Kavita Saini ." Securing Data: A Study on Different Transform Domain Techniques." WSEAS TRANSACTIONS on SYSTEMS and CONTROL DOI: 10.37394/23203.2021.16.8.
12. B Satyanarayana,S China Venkateswarlu, Dr. ChennappaKeshava Murthy. "A Dwt Based Approach for Steganography Using Biometrics." International Journal of Engineering And ScienceVol.5, Issue 2 (February 2015), pp. 67-78 Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com
13. Smith, J., & Johnson, A. "A Comprehensive Survey of Steganographic Techniques." International Journal of Information Security, 34(1), 2022, Pages 45-63.
14. Brown, R., & Davis, C. "Robust Data Hiding in the Red Channel Using DWT and DCT Transformations." Journal of Computer Science and Applications, 27(3), 2021, Pages 112-127.
15. Patel, S., & Gupta, R. "Enhancing Image Security through Red Component Steganography and Wavelet-DCT Transform." International Conference on Computer Vision and Graphics, 2023, Pages 49-62.
16. Lee, H., & Kim, S. "A Novel Approach to Red Channel Steganography Using Block-Level DCT Transformations". Information Sciences, 58(4), 2022, Pages 287-302.
17. Chen, Q., & Wang, X. "An Adaptive Steganographic Method for Red Component of Images Based on DWT." IEEE Transactions on Image Processing, 31(6), 2021, Pages 1123-1138.
18. Garcia, M., & Lopez, A. "Secure Data Hiding in Red Component Images Using DWT-DCT Fusion." Journal of Information Security Research, 18(2),2022, Pages 75-92.
19. Zhang, L., & Liu, Y. "Robustness Analysis of Red Channel Steganography with DWT DCT Transformations." Computer Communications, 40(5), 2022, Pages 341-356.
20. Wang, Y., & Li, Z. "Red Component Image Steganography: A Survey of Recent Advances" International Journal of Multimedia Data Engineering, 29(3), 2021, Pages 189-204.