Secure Communication through Coverless Steganography using HAAR Wavelet Transform

Devika.D
IIT2021013@iiita.ac.in
Indian Institute Of Information Technology
Allahabad, India

Udayasree.B
IIT2021038@iiita.ac.in
Indian Institute Of Information Technology
Allahabad, India

Bhavana.M
IIT2021077@iiita.ac.in
Indian Institute Of Information Technology
Allahabad, India

Janvi.T
IIT2021222@iiita.ac.in
Indian Institute Of Information Technology
Allahabad, India

Abstract

In an era where information security is of paramount importance, the integration of advanced technologies is crucial to safeguarding sensitive data. This study offers a comprehensive examination of secure communication methods through the innovative application of coverless steganography coupled with the HAAR Wavelet Transform. Coverless steganography, a burgeoning field in information concealment, eliminates the need for separate cover objects, streamlining the encryption process and enhancing operational efficiency. Leveraging the HAAR Wavelet Transform's robust capabilities, this research presents a novel approach to covert communication, ensuring the seamless embedding and extraction of hidden information within digital media. By intricately merging coverless steganography with the HAAR Wavelet Transform, our method achieves heightened levels of security, making it exceptionally resilient against detection and decryption attempts. Through meticulous experimentation and evaluation against established benchmarks, our methodology demonstrates superior performance in terms of data concealment efficacy, imperceptibility, and resistance to adversarial attacks. Furthermore, the incorporation of adaptive techniques enhances model stability and reliability, further fortifying the security of the communication channel. This research contributes significantly to advancing the field of secure communication, offering a robust framework for clandestine information exchange in various domains while upholding the highest standards of confidentiality and integrity.

keywords-Secure Communication, Data Encryption, Diffusion Models, Steganography, HAAR Wavelet Transform, Coverless steganography.

I Introduction

Introduction to Steganography: Steganography embeds data into various digital media which includes text, images, audio, video, etc... To prevent being discovered, information is intentionally hidden within these media. Figure 1 shows basic working principle for steganography and Figure 2 shows the world wide projected financial loss due to cybercrime incedents[10]. As image transmission is considered one of the important transmissions in digital communication, it is widely used for information transfer[1].

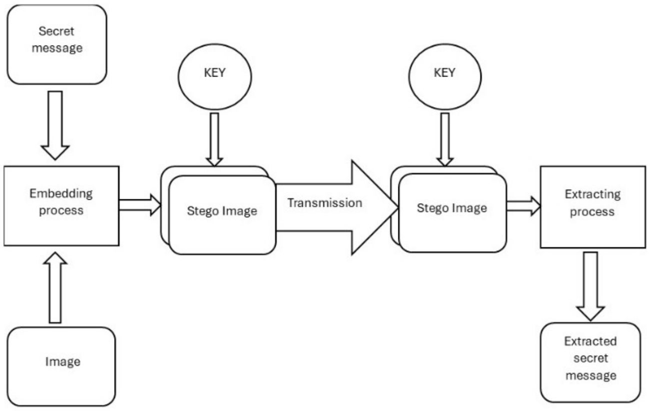

Figure 1. Basic Working of Steganography

Since the stego image does not differ from the original image as observed using the unaided eye, the detection of hidden messages becomes difficult. But in recent times, traditional image steganography such as LSB, randomized embedding technique, and spread spectrum are vulnerable to steganalysis[4]. Because hiding secret information and altering the pixel values disrupts the normal patterns i.e., statistical characteristics in the original image, making it easier to detect.

On the other hand, the transformational domain techniques, like Discrete Cosine Transform (DCT) and Haar wavelet transform, seem more promising. These methods break down the image into smaller pieces and then hide information in the transformed domain. Haar Wavelet transform uses subbands include the LL, LH, HL, and HH which are manipulated to retain or alter specific information about the image in the Haar domain[5].

In HWT (Haar wavelet transform), unlike in DCT or IWT (Integer wavelet transform), the embedding process begins by converting the secret message into binary form and breaking it down into smaller parts. These parts are then inserted into the LL subband of the Haar-transformed image, which holds the least image information, ensuring minimal impact on the image frequency values. This embedding is done iteratively across smaller blocks of the image to ensure effective concealment of information[5].

One advantage of using the Haar wavelet transform for steganography is its ability to leverage temporal location information. This means that it not only considers the spatial characteristics of the image but also incorporates information about where in the image the data is being hidden. This temporal location information plays a crucial role during the extraction process.

Due to this characteristic, Haar wavelet transform-based steganography exhibits greater resistance against compression and other manipulation techniques. The information about the specific locations where the data is embedded helps in accurately extracting the hidden message, even when the image undergoes compression or other transformations.

In this hiding the message content in the LL subband (least image frequency stored) means manipulation of the image in the haar domain is happening in the background which is not interfering with the image edges thus effective against most mediocre attacks. While they're more successful at concealing data, they're not completely reliable, because they still leave marks or artifacts in the picture, advanced techniques can find them. So,the CIS method is introduced[5].

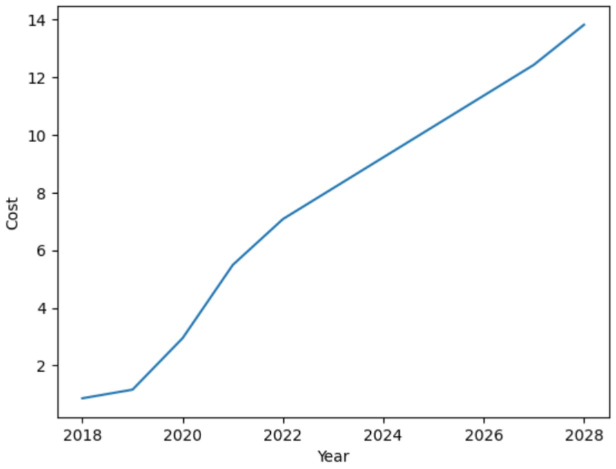

Figure 2. Projected world wide financial loss due to cybercrime incedents (in Trillion U.S. Dollars)

Coverless steganography is an emerging concept in the field, aiming to hide confidential data without altering the cover image directly. Because of its ability to increase resistance to detection in this situation, the Coverless Image Steganography (CIS) technique has drawn attention[2].

The CIS method works by synthesizing secret text into images, effectively converting text into visual data[13]. Instead of modifying the cover image itself during embedding, a mapping is established by CIS between the secret information and the cover image. It then selects appropriate cover images based on hash representation and the secret data. However, a challenge arises as the capacity for secret information increases, necessitating a larger number of images for concealment[1].

To overcome this challenge, we can leverage Haar wavelet transforms. These transforms are proficient in compressing images while preserving essential details. By reducing the size of images, Haar wavelet transforms allow for more images to be stored in the database without requiring significant additional storage space. Consequently, this capability enables steganography systems to manage larger volumes of secret data without facing storage constraints[3].

II Steganography in Practice: Real-World Cyber Attack Scenarios

SolarWinds Supply Chain Attack: Due to its ability to compromise thousands of organizations globally, including the federal level of the US government, the 2020 SolarWinds attack quickly became well-known. In order to conceal remote access tools, this supply chain attack updated the Orion network monitoring program with what appeared to be authentic upgrades. Steganography was utilized to conceal command data during the command and control phase of the SolarWinds breach, despite the breach's numerous layers of complexity. The approach employed in this instance made use of seemingly benign XML files that control servers served in HTTP response bodies[7]. The command data within those files was hidden as various text strings.

eCommerce Skimming: Research demonstrating threat actors' embedding of skimming malware within SVG images on eCommerce checkout pages was released by the Dutch eCommerce security platform Sansec in November 2020. The malicious payload for the assaults was camouflaged and placed inside SVG pictures, while the decoder was hidden independently on other portions of the web sites. Simple logos from well-known organizations like Facebook and Google were shown on the hijacked checkout pages, so users inputting their details wouldn't notice anything unusual. Additionally, malicious activity was undetected by typical security scanners looking for incorrect syntax since the payload was hidden inside what seemed to be the proper use of SVG element syntax[7].

Industrial Enterprises: A report on a campaign of monitored and targeted attacks on industrial firms in multiple countries was issued by Kaspersky in June 2020. In this campaign, steganographic tactics were employed when targets clicked on Excel email attachments containing malicious macros. The PowerShell scripts that the macros executed included a command to download specific images from publicly accessible image hosting providers. Threat actors could implant trojans to steal passwords or spy on network traffic by decoding additional malicious data concealed in various pixels within each image[7].

III Problem statement:

This project is designed to address the challenges associated with secure image communication, aiming to enhance the confidentiality and integrity of transmitted images. The goal is to establish a secure channel of communication between two parties by leveraging a combination of coverless steganography and HAAR wavelet transformation. Traditional methods of image steganography may not always suffice, as they can alter the visual fidelity of the image or may not provide robust security against various attacks. In response to these challenges, this project proposes a novel coverless steganographic approach that combines with the frequency domain manipulation afforded by HAAR wavelet transformation.

Objective: The main goal of this study is to investigate the efficiency of coverless steganography integrated with the HAAR Wavelet Transform for facilitating secure communication channels. By harnessing the unique capabilities of coverless steganography and the HAAR Wavelet Transform, we aim to develop a robust framework for concealing sensitive information within digital media, thereby ensuring confidentiality and integrity in communication[2].

IV Literature survey:

Conventional Image Steganography: The process of concealing the data behind the cover image is known as image steganography. To conceal information in the most unnecessary bit, pixel intensities are transformed into a binary form.

Traditional steganography methods, like the least significant bit (LSB) technique, randomized embedding technique, and spread spectrum hide secret messages by slightly changing the values of pixels in an image. Initially, in LSB steganography, most of the pixels in the image were used to hide the message. Later, researchers found ways to hide more information while still keeping the image quality decent. For example, as shown in figure 3 Weng et al.[3] suggested a method that takes advantage of certain properties of image compression to hide messages effectively. However, as technology advanced, it became easier to detect these hidden messages using statistical analysis, especially with LSB methods, compression-based extraction, etc. To address this vulnerability, another scheme focused on selecting the best parts of the image to hide the message, making it harder to detect was introduced.

Since the Spatial Domain had problems with Steganalysis extraction methods, to address potential image distortion, adaptive steganography is introduced, a method that aims to reduce additive distortion by assigning a cost to each pixel. This cost guides the embedding of secret information, ensuring minimal overall distortion.

This is similar to A* Algorithm used in Artificial Intelligence which is based on the Heuristic cost function to find the shortest path between 2 points. Subsequently, several adaptive steganographic techniques, including HUGO, S-UNIWARD, HILL, and MiPOD, have been developed. These methods rely on different distortion functions to achieve their objectives.

Additionally, alternative approaches such as DeJoin, ACMP, and GMRF, which are non-additive distortion-based, have been proposed. Despite their effectiveness, these techniques still utilize distortion functions defined heuristically, indicating scope for further refinement and enhancement. so Transformational domain usage came into picture. DCT, IWT and HWT were used for hiding data in Images.

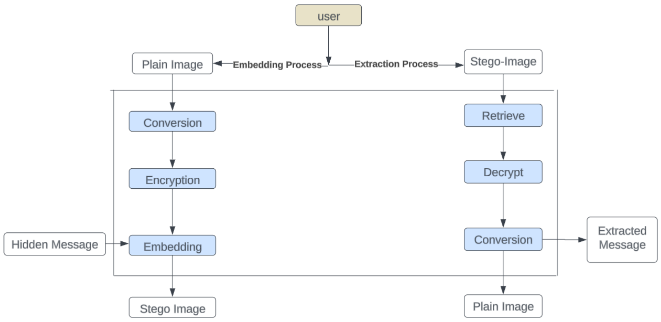

Figure 3. Working principle of Joint Coverless Steganography and Image Transformation for Covert Communication of Secret Messages[3]

DCT: For the past few years, the most widely used method for image compression has been the discrete cosine transform (DCT). Its choice to serve as JPEG's standard is one of the principal causes for its popularity. Numerous non-analytical applications, which include image processing and signal processing DSP applications like video conferencing, utilize DCT. In transformation, the DCT is used for data compression[4].

The DCT transform is an orthogonal transform with a predefined collection of basic functions. A frequency can be mapped into an image space using DCT. DCT offers a lot of benefits. (1) For image data, it can store energy in low frequencies. (2) It may decrease the blocking artifact effect, which is caused by the visibility of the boundaries between sub-images. The figure 4 explains a basic block diagram for the proposed method.

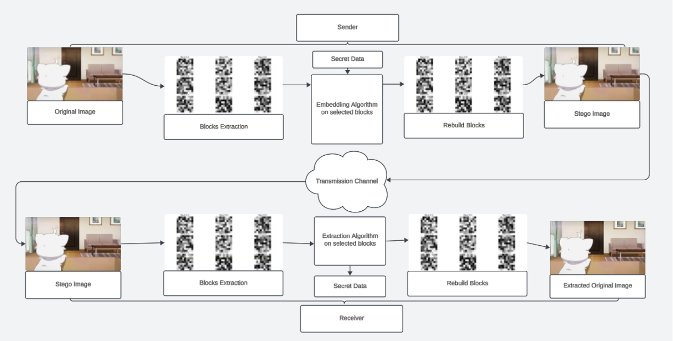

Figure 4. Working principal of a DCT based Steganographic Process[4]

HWT: The Haar Wavelet Transform (HWT) serves as a important technique in image and signal processing, rivaling the widespread usage of the Discrete Cosine Transform (DCT) for data compression and data embedding into cover media. Unlike the DCT, which relies on sinusoidal functions, the HWT utilizes Haar wavelets, simple piecewise constant functions. These wavelets form an orthogonal transform, akin to the DCT, ensuring efficient computations and facilitating compression tasks.

Similar to the DCT, the Haar Wavelet Transform employs a fixed set of basis functions, consisting of a scaling function and a wavelet function. However, the simplicity of the Haar wavelet basis functions contrasts with the more complex sinusoidal basis functions of the DCT, resulting in computational efficiency.

The primary function of the Haar Wavelet Transform, like the DCT, is to map data from its original domain (e.g., spatial domain for images) into a frequency domain. This transformation aids in data analysis and manipulation, allowing for features to be localized and efficiently represented i.e., Temporal Localisation Effect of HWT.

One of the distinguishing features of the Haar Wavelet Transform is its ability to localize features in the data. Unlike transforms that spread information across the entire frequency spectrum, Haar wavelets excel at capturing localized changes or features such as edges or texture patterns, making them particularly useful in tasks like edge detection and feature extraction. So it can also be used for dividing the images into blocks of 2X2, 4X4, 16X16,32X32, 256X256, and 512X512 blocks based on the image size and secret data length and embedd the data in the Haar domain.

Similar to the DCT's ability to reduce blocking artifacts, the Haar Wavelet Transform contributes to artifact reduction through the efficient representation of both low and high-frequency components i.e., (HH, HL, LH, LL subbands). This aids in better reconstruction and minimizes visible artifacts at block boundaries, enhancing the quality of compressed images i.e., less image distortion from the original Image.

Figure 5 shows the basic working principle for the proposed method[6].

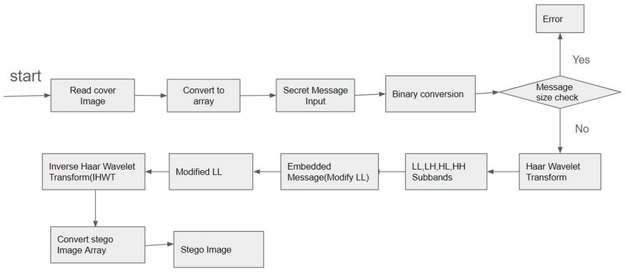

Figure 5. Steganography Process depicting DCT Model[6]

Beyond image compression, the Haar Wavelet Transform finds applications in denoising, feature extraction, and various signal processing tasks due to its versatility in capturing both local and global features. While the Discrete Cosine Transform (DCT) has been favored historically for its energy compaction properties in image compression, the Haar Wavelet Transform (HWT) offers its own set of advantages, including feature localization, artifact reduction, and versatility across signal processing tasks.

CIS: In this thesis, the focus lies on coverless image steganography (CIS)[9], a technique employed in concealing secret information within digital images without requiring a separate cover image for embedding. CIS methods can be broadly classified into two categories: those based on image mapping and those based on image generation. Figure 6 shows the basic working principle of the proposed method. Mapping-based CIS methods involve encoding secret information into binary hash sequences and selecting an appropriate cover image whose hash sequence corresponds to the encoded data. These methods aim to seamlessly integrate the secret information into the cover image, ensuring minimal detection. Various techniques have been proposed in literature, including block division-based approaches where the average pixel values of image blocks determine the hash values. Additionally, models such as Bag-of-Words (BOW) are utilized to extract visual keywords representing the secret information, facilitating effective embedding. These are the

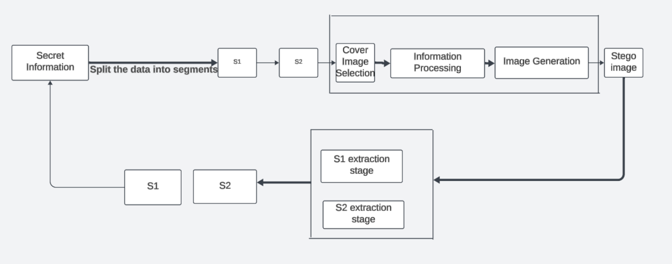

Figure 6. Working model of coverless steagnography[9]

Machine Learning techniques which are joined with the CIS to improve its resistance in steganalysis.

In second Method, generation-based CIS methods generate a stego image directly corresponding to the secret information. These techniques can be further categorized into artificial synthesis-based and machine learning-based methods. The former involves encoding secret data into image blocks and replacing non-matching blocks with suitable ones from a database, ensuring compatibility and visual coherence. Notably, pixel texture synthesis-based algorithms have been proposed, utilizing colored dot patterns to encode secret information and employing texture synthesis to complete the image.

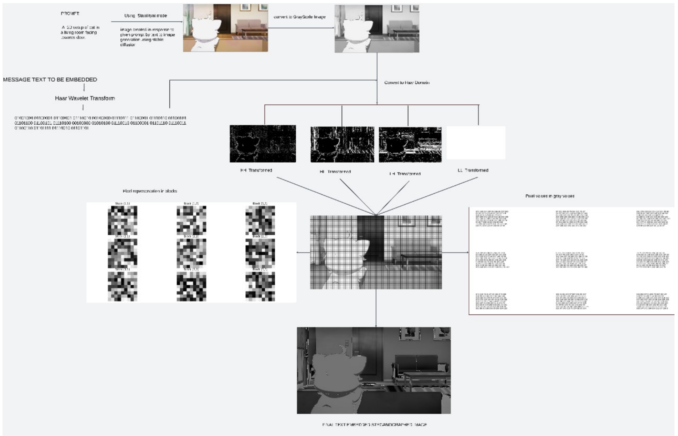
PROMPT
A 2D setup of cat in a living room facing towards door.
Using Stabilityai mode
image created in response to given prompt by text to image generation using stable diffusion
convert to GrayScale Image
MESSAGE TEXT TO BE EMBEDDED
Haar Wavelet Transform
Convert to Haar Domain
HH Transformed
HL Transformed
LH Transformed
LL Transformed
Pixel representation in blocks
Pixel values in gray values
FINAL TEXT EMBEDDED STEGANOGRAPHED IMAGE

Figure 7. Coverless Steganography with Haar Wavelet transform[5]

CIS with HWT: The proposed approach[5] revolves around coverless image steganography utilizing Haar Wavelet Transform (HWT). Haar Wavelet Transform, a powerful mathematical tool commonly used in signal and image processing, serves as the foundation for embedding secret information within the digital image domain. Leveraging the capabilities of HWT, the thesis employs a mapping-based CIS method, where the cover image selection is based on the hash sequence derived from the secret information. By utilizing HWT, the embedding process aims to achieve efficient encoding and robust concealment of the secret data within the cover image, ensuring its integrity and minimizing the risk of detection. The figure 7 explains the process of this very method.

Stable Diffusion: Stable Diffusion is a cutting-edge technique in image generation that leverages diffusion models. These models operate by iteratively adding noise to an image to gradually reveal its content, allowing for the generation of high-quality and diverse images. The process involves diffusing noise through multiple layers, where each layer refines the image further. Stable Diffusion models are particularly effective for generating realistic images with intricate details and varied textures.

Haar Wavelet Transform: In image processing, the Haar Wavelet Transform is a technique used for analyzing and decomposing images into their constituent wavelet components. It operates by applying a series of filters to the image to extract features at different scales and orientations. This decomposition process allows for efficient representation of image features, making it useful for tasks such as compression, denoising, and feature extraction. The Haar Wavelet Transform is especially valuable in text-to-image generation for its ability to capture both global and local image characteristics, aiding in the synthesis of visually appealing and contextually relevant images.

By incorporating Stable Diffusion and the Haar Wavelet Transform into the text-to-image generation methodology, you can enhance the comprehensiveness of the approach and highlight the versatility of these techniques in producing high-quality visual outputs

V Proposed Methodology:

Authors have divided the proposed methodology in three parts Image generation, Embedding of secret message and Extraction of secret message.

Image Generation

Generating an image which does not exist in physical or digital environment is a key aspect of coverless steganography. For this authors have trained a deep learning model using stable diffusion based on an image data set of Anime Face [19]. The generated image is based on the stable diffusion model described in figure YYY.

Haar Wavelet Transform plays a crucial role in the proposed algorithm by enabling frequency domain manipulation and enhancing Secret messages' security and confidentiality. It helps authors to provide an additional layer of security.

Algorithm:

1. Read the cover image: Open the cover image file (e.g., "cat.jpg"). Convert the image to grayscale format (if necessary).
2. Open the cover image file (e.g., "cat.jpg"). Convert the image to grayscale format (if necessary).
3. Get the secret message
4. Convert the message to binary: For each character in the message: Convert the character to its ASCII code. Convert the ASCII code to its 8-bit binary representation. Combine the binary representations of all characters to form a single binary string.
5. Check message size: Calculate the total number of bits in the binary message. Compare the message size with the availab le capacity of the cover image (limited by the number of coefficients). If the message is too large: Display an error message. Exit the algorithm. Else (message size is acceptable): Proceed to the next step.

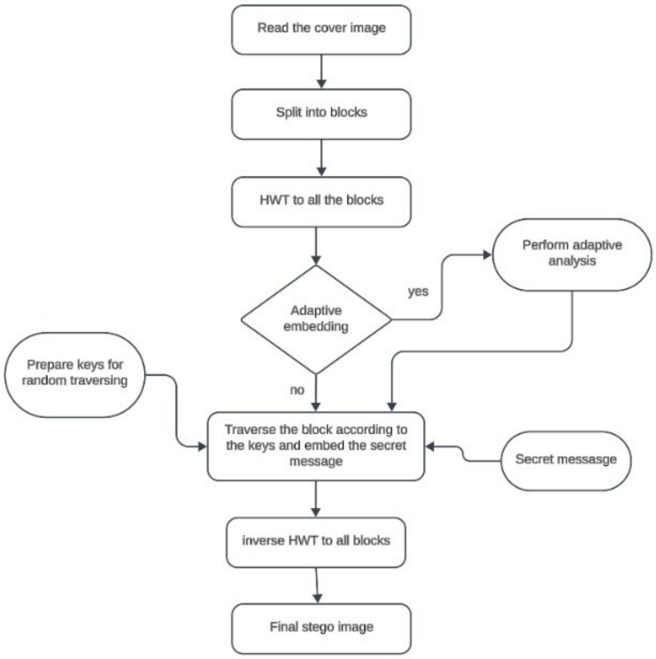
Read the cover image
Split into blocks
HWT to all the blocks
Adaptive embedding
yes
Perform adaptive analysis
no
Prepare keys for random traversing
Traverse the block according to the keys and embed the secret message
Secret message
inverse HWT to all blocks
Final stego image

Figure 8. HWT Embedding process

6. Perform the Haar Wavelet Transform (HWT): Use a wavelet library (e.g., ‘pywt‘) to decompose the image array into four subbands: LL (approximation coefficients - low frequency) LH (horizontal detail coefficients) HL (vertical detail coefficients) HH (diagonal detail coefficients)
7. Embed the message: Iterate through each bit in the binary message string. For each bit:
   - If the bit is 1, use a bitwise OR operation (‘|=‘) to set the least significant bit (LSB) of the corresponding coefficient in the LL subband array to 1.
   - If the bit is 0, use a bitwise AND operation (‘%=‘) with 254 (in uint8 format) to ensure the LSB remains 0 while preserving the other bits.
8. Perform the Inverse Haar Wavelet Transform (IHWT): Combine the modified LL subband with the original high-frequency subbands (LH, HL, HH) using the inverse HWT to reconstruct the stego image.
9. Convert the stego image array: Convert the resulting stego image array back to uint8 format (0-255) and round for proper image representation.
10. Create the stego image: Create a new PIL image object from the stego image array.
11. Save the stego image

Haar wavelet transform algorithm Embedding process:

- Step 1:Examine the image on the cover.

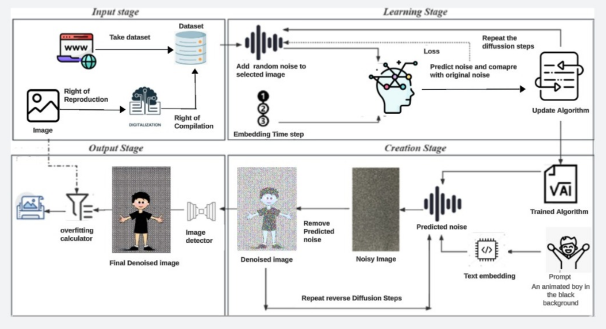

Figure 9. Proposed Methodology

- Step 2:Divide it into blocks. Block sizes: 8x8, 16x16, 32x32, 64x64, 128x128, 256x256, or 512x512 are the possible options.
- Step 3: Apply the Haar Wavelet Transform (HWT) to every block.
- Step 4:Get the keys ready for random traversing. The sequence of occurrences in which the blocks are selected and the random patterns through which they are sorted are the keys.
- Step 5: Analyze to find the bit count for each coefficient in adaptive embedding.
- Step 6: Read information in binary or a secret message.
- Step 7: Navigate the blocks using the keys, and then enter the data, either in an adaptive or non-adaptive manner, depending on the situation.
- Step 8: After inserting all the data using LSB substitution, convert the image back to the spatial domain by performing inverse HWT on each block.
- Step 9: The image now carries the secret information hidden safely inside and can now be used for transmission or other purposes. This image is called the stego image.

Haar wavelet transform algorithm Extracting process:

- Step 1: Examine the stego image.
- Step 2: Divide it into blocks. Block sizes: 8x8, 16x16, 32x32, 64x64, 128x128, 256x256, or 512x512 are the possible options.
- Step 3: Apply IWT (Haar or 5/3) to each block to transform it.
- Step 4: It is considered that the receiver has the keys needed to identify the traversing pattern. Use the keys to move through the blocks.
- Step 5: If ’L’ is not adaptive, it remains fixed; if it is adaptive, it can be obtained using mathematical equations.
- Step 6: ’L’ bits should be extracted from the coefficients and then put through the Haar wavelet transform (HWT).

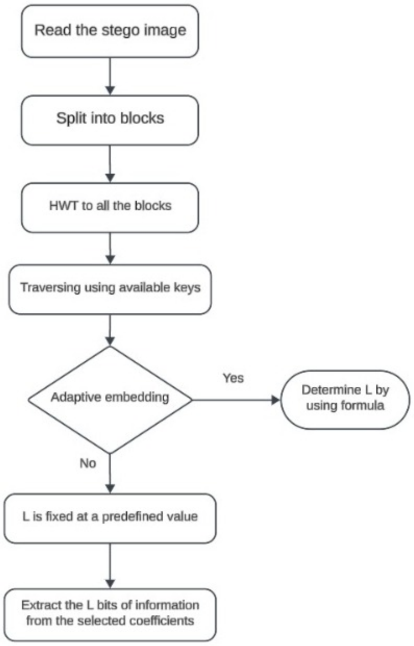
Read the stego image
Split into blocks
HWT to all the blocks
Traversing using available keys
Adaptive embedding
Yes
Determine L by using formula
No
L is fixed at a predefined value
Extract the L bits of information from the selected coefficients

Figure 10. HWT Extracting process

VI Comparitive Study

Table 1 shows a comprehensive review of the existing solutions and the proposed method. The authors have identified the working process of the existing solutions and have highlighted some advantages and disadvantages for the existing methods and highlighting the same in light of proposed method.

VII Mathematical Analysis

This section describes the method's experimental results based on a few methods for assessing hiding performance. The performance metric in this case is based on the stego image's appearance and its ability to conceal data.

- **MEAN SQUARE ERROR**[17]
  The squared intensities of the cover and stego image pixels are averaged to calculate it.The MSE is shown in '(1)'

$$\text{MSE} = \frac{1}{NM}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}(e(m,n))^2 \tag{1}$$

  where NM is the image size (N × M) and e(m, n) is the reconstructed image.

- **CORRELATION**[18]
  Both statistical analysis and image processing frequently use Pearson's correlation coefficient. Here, we apply it to the cover and the stego images to observe how these two images differ from one another. The correlation is shown in '(2)'

$$\text{CORRELATION} = \frac{\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i-\bar{x})^2\sum_{i=1}^{n}(y_i-\bar{y})^2}} \tag{2}$$

  The Xi and Yi are the cover image and bar of X and Y are stego image positions. The correlation values are tens to 1 that means both the images are likely to same.

- **PEAK SIGNAL-TO-NOISE RATIO**[17]
  Signal-to-noise ratio (SNR), which is based on the pixel difference between two images, is a mathematical indicator of image quality. The Stego image's quality is estimated using the SNR measure in relation to the cover image. Peak signal-to-noise ratio (PSNR) shows in '(3)'.

$$\text{PSNR} = 10\cdot\log_{10}\left(\frac{s^2}{\text{MSE}}\right) \tag{3}$$

  where S stands for maximum possible pixel value of the image. If the PSNR is greater than 36 DB then the visibility looks same in between cover and stego image, so HVS not identified the changes.

- **ROOT MEAN SQUARE ERROR**[18]
  One way to measure the difference between the values of the cover image and the stego image is to use the root mean square error (RMSE). These variations are referred to as residuals, and the RMSE allows them to be combined into a solitary analytical power measure. The RMSE shows in '(4)'.

$$\text{RMSE} = \sqrt{\frac{\sum_{i=1}^{n}(X_{\text{obs},i}-X_{\text{model},i})^2}{n}} \tag{4}$$

PAPER TITLE	PAPER'S SUGGESTED SOLUTION	ADVANTAGE	DISADVANTAGE
Novel Coverless Steganography Method Based on Image Selection and StarGAN[1]	1.A novel coverless steganography method is proposed, leveraging image selection and StarGAN integration to embed secret information efficiently. 2. Auxiliary information is incorporated into additional images, enhancing security and capacity. 3.Two extraction schemes, utilizing machine learning and image processing, are introduced for accurate retrieval of hidden data, validated through experiments showcasing the method's effectiveness and potential real-world applications.	1. The proposed method utilizes a deep learning-based approach, which allows for better robustness against non-geometric attacks compared to existing coverless image steganography methods. 2. The use of StarGAN for image selection enables better visual quality of the generated images, which can enhance the security of the information hiding process.	1. The paper does not discuss the robustness of the proposed method against geometric attacks, which is an important aspect of coverless steganography. 2. The use of deep learning models can be computationally expensive, which may limit the practicality of the proposed method in certain applications. 3. The paper does not provide any experimental results or analysis to support the claims made in the abstract, making it difficult to assess the validity of the proposed method. 4. The paper does not address the potential security risks associated with the use of deep learning models in steganography, such as the possibility of adversarial attacks.
Joint Coverless Steganography and Image Transformation for Covert Communication of Secret Messages [3]	1.The paper introduces a novel approach that merges coverless steganography with image transformation for secret message communication. 2. It utilizes a generative network to synthesize stego images from secret messages and latent inputs, aiming to evade common attacks like eavesdropping and steganalysis. 3.The proposed system comprises three subnets: generator (G), discriminator (D), and extractor (E), each serving specific functions to synthesize stego images, ensure quality, and extract messages. 4. Block matching and transformation techniques are applied to make transformed images resemble reference images, enhancing the security of the covert communication process.	1. The use of image transformation techniques such as DWT, SIFT, and DenseNet feature mapping enhances the robustness of the method against various image attacks. 2. The proposed method achieves covert communication of secret messages by creating a mapping relationship between the secret message and the image, which improves the security of information hiding. 3. The use of deep learning models such as DenseNet for feature extraction and mapping enhances the robustness of the method against non-geometric attacks.	1. The paper does not provide a comprehensive comparison with existing coverless image steganography methods, making it difficult to fully evaluate the performance of the proposed method. 2. The paper does not discuss the robustness of the proposed method against geometric attacks, which is an important aspect of coverless steganography. 3. The paper does not provide any experimental results or analysis to support the claims made in the abstract, making it difficult to assess the validity of the proposed method. 4. The paper does not address the potential security risks associated with the use of deep learning models in steganography, such as the possibility of adversarial attacks.

PAPER TITLE	PAPER'S SUGGESTED SOLUTION	ADVANTAGE	DISADVANTAGE
Secret-to-image reversible transformation for generative steganography[14]	1. S2IRT is a generative steganography method using the Glow model, involving two stages: encoding information into images and decoding it. 2. Utilizes Glow's bijection to encode secrets as latent vectors, maintaining covert transmission and Group elements, arrange them based on the secret, construct latent vectors, and generate images. 3. This scheme can theoretically hide up to 16.2 bits per pixel and it is Introduced for robustness against attacks, it encodes each element group separately, enhancing security while maintaining capacity.	1. The method utilizes DCMH-CNN feature extraction to obtain deep hashes from images, converting them into binary hashes, which can enhance the security and robustness of the steganography process. 2. Clustering the binary hashes using the K-Means algorithm to form the Coverless Image Dataset (CID) ensures independence and robustness in the storage and retrieval of secret information. 3. Indexing secret information to CID images based on a mapping rule enables secure transmission, and encryption of zero-padding record and K value adds an extra layer of security to the communication process. 4. The decryption and reconstruction of CID images at the receiver's end facilitate accurate extraction of secret messages, ensuring reliable communication and information retrieval.	1. The use of complex feature extraction and clustering algorithms like DCMH-CNN and K-Means may increase the computational complexity of the method, potentially affecting its efficiency. 2. The reliance on specific algorithms like DCMH-CNN and K-Means may limit the method's applicability in scenarios where these algorithms are not suitable or feasible. 3. The method's reliance on a mapping rule for indexing secret information to CID images may introduce vulnerabilities if the mapping rule is compromised or reverse-engineered. 4. The encryption of zero-padding record and K value, while enhancing security, may also introduce additional steps that could potentially impact the speed of the communication process.
Coverless image steganography using morphed face recognition based on convolutional neural network[16].	1.The method utilizes face morphing on a sorted dataset of face images to embed secret digits within morphed images, ensuring imperceptible transmission of encrypted messages. 2. Landmarks on source and target faces are selected, and relationships between them are constructed to generate morphed images using triangle areas for coordinate projection. 3. Recipients accurately extract error-free secret digits from morphed face images using MFR-Net V1 and V2 networks, crucial for ensuring secure communication.	1. The method embeds secret digits within morphed images, ensuring that the transmission of encrypted messages remains imperceptible. 2. The recipient can accurately extract error-free secret digits from morphed face images using MFR-Net V1 and V2 networks, ensuring secure communication. 3. The use of powerful and robust deep learning models allows for the recovery of secret messages by recognizing the parents of the morphed face images. 4. The proposed schema has higher retrieval capacity and accuracy compared with existing networks, providing better robustness.	1. This method faces high computational Complexity. 2. Data availibility is less. 3. The results show that there is a visible change in the choosen image after embedding.

Xobs,i and Xmodel,i are two image vectors, i.e., cover and stego.

Percentage of embedding	MSE	CORRELATION	PSNR	RMSE
5	0.1369	0.42870	56.76	0.3700
10	0.1374	0.42874	56.74	0.3707
15	0.1378	0.42873	56.73	0.3712
20	0.1378	0.42874	56.73	0.3712
25	0.1381	0.42874	56.72	0.3716
30	0.1382	0.42874	56.72	0.3718
35	0.1386	0.42874	56.71	0.3723
40	0.1390	0.428742	56.69	0.3729
45	0.1396	0.42874	56.68	0.3736
50	0.1399	0.42874	56.67	0.3741
60	0.14032	0.42874	56.65	0.3746
70	0.1407	0.42874	56.64	0.3751
80	0.1410	0.42874	56.63	0.3755
90	0.1414	0.42874	56.62	0.37607
100	0.1429	0.42874	56.58	0.3780

Table 2. Performance metrics:

The image's imperceptibility is referred to as its quality. The suggested method's ability to produce high-quality stego images has been thoroughly evaluated using a variety of image similarity metrics, including MSE, PSNR, correlations, and RMSE The calculated values of the different similarity metrics for images are displayed tabularly in Table 2 with different message embedding percentage.

VIII Future scope

The proposed method gives us some ideas for future research and development:

Enhanced Security Protocols: Continued research into improving encryption techniques and protocols can further enhance the security of communication channels for better secret data transmission. Exploring advanced cryptographic algorithms and methods for key management can strengthen the defence against multiple attacks for key detection and compromise of the system against cyber threats.

Machine Learning Integration: Integrating machine learning algorithms such as GANS, deep Hashing can enhance the adaptive capabilities of steganographic systems, improving their resistance to detection and enhancing their performance in real life applications. Techniques such as deep learning, Neural Networks for improving key security can be explored for automated feature extraction and optimization.

Multiple Approaches Mixing/ Hybrid Approach: In many research papers in this field and our research paper also proved that a better efficiency can be achieved by combining more than one approach. By doing this we were able to overcome the problems caused by one method by another algorithm and vice versa. Examples such as using Glow Model with latent vector encoding, enhancing CIS method stability by including multiple decoder-generator pairs, using face morphing image processing technique with stable diffusion for matching the images and messages etc.

Testing and improving through applying in Real World Applications: Methods and Approaches Proposed might work differently in real life scenarios. They can vary a lot from the calculated and proved efficiency scores because of unknown variables existing in real world applications which are by far very different from the ideal situation and datasets which we considered accordingly for working with our algorithm. So, applying in real situation is a mandatory for reinforcing the algorithm efficiency through identifying the problem. Examples such as using in Social Media Platforms for the testing of secret data transmission using CIS method encrypting the messages such as image source and original account related data for identity proving.

IX Conclusion

In conclusion, this study presents a detailed analysis into secure communication methods by integrating coverless steganography with the HAAR Wavelet Transform. This Progressive Approach offered by this research enhances the confidentiality and integrity of data transmission, addressing the challenges associated with traditional steganographic techniques and other Domain Transformational Approaches used by far by the industry to achieve the prevention of Data Misuse or Secret data transmission.

By utilising coverless steganography, the need for separate cover objects is eliminated, refining the encryption process and enhancing algorithmic operation . Additionally, the HAAR Wavelet Transform provides robust capabilities for covert communication, ensuring embedding and extraction of hidden information within digital media a less defected process better than exisiting solutions.

Through careful research and evaluation against established approaches and going through a lot of papers on similar works, we got our proposed approach i.e., our methodology demonstrates better performance in terms of data concealment efficacy, small noticeability and resistance to stronger steganalysis attacks. The adaptive techniques integration further strengthens the security of the communication channel, contributing significantly to advancing the field of secure communication.

X References:

1. X. Chen, Z. Zhang, A. Qiu, Z. Xia, and N. N. Xiong, "Novel Coverless Steganography Method Based on Image Selection and StarGAN," in IEEE Transactions

on Network Science and Engineering, vol. 9, no. 1, pp. 219, January/February 2022.

2. S. Debnath and R. K. Mohapatra, "A Study on Secret Data Sharing through Coverless Steganography," 2022 2nd International Conference on Artificial Intelligence and Signal Processing (AISP), Vijayawada, India, 2022, pp. 1-6, doi: 10.1109/AISP53593.2022.9760680.
3. Wen, Wenying, et al. "Joint Coverless Steganography and Image Transformation for Covert Communication of Secret Messages." IEEE Transactions on Network Science and Engineering (2024).
4. D. Neeta, K. Snehal and D. Jacobs"Implementation of LSB Steganography and Its Evaluation for Various Bits" 2006 1st International Conference on Digital Information Management, Bangalore, India, 2007, pp. 173-178, doi: 10.1109/ICDIM.2007.369349.
5. X. Tao, P. Zhang, Q. Hu, Z. Han, G. Zhe, H. Xiaolei, and H. Xiaodong,"High quality image steganography on integer Haar Wavelet Transform using modulus function" 2015 International Conference on Science in Information Technology (ICSITech), Yogyakarta, Indonesia, 2015, pp. 79-84, doi: 10.1109/ICSITech.2015.7407781.
6. Radhika Mani M, Lalithya V, Swetha Rekha P. "An innovative approach for pattern based image steganography." IEEE, presented at the Int Conf Signal Processing, Informatics, Communication and Energy Systems. 2015 Feb.
7. A. Miri and K. Faez,"An image steganography method based on integer wavelet transform"Multimedia Tools and Applications, Vol. 77, No. 11, pp. 13133-13144, 2018.
8. L. Papa, L. Faiella, L. Corvitto, L. Maiano, and I. Amerini,On the use of Stable Diffusion for creating realistic faces: from generation to detection Sapienza University of Rome, Italy,2023.
9. Liu, X, Li, z, Ma, J., Zhang, W., Zhang, J., & Ding, Y,"Robust coverless steganography using limited mapping images" Available online 23 May 2022, Version of Record 28 June 2022.
10. Steganography in Cybersecurity: Unveiling the Growing Intricacies and Expanding Threat Landscape.Steganography in Cybersecurity: A Growing Attack Vector 2022. Accessed 25.4.2024
11. Rafael Reisenhofer, Sebastian Bosse, Gitta Kutyniok, Thomas Wiegand, A Haar wavelet-based perceptual similarity index for image quality assessment,Signal Processing: Image Communication,Keywords: Image quality; Perceptual similarity; Haar wavelets; Human visual system.
12. Nagham Hamid, Abid Yahya, R. Badlishah Ahmad ,Osamah M. AlQershi "Image steganography techniques: an overview",International Journal of Computer Science and Security 2012.
13. Fleck, A. "Cybercrime Expected To Skyrocket in Coming Years" 2024.
14. Zhou, Zhili, et al. "Secret-to-image reversible transformation for generative steganography." IEEE Transactions on Dependable and Secure Computing (2022).
15. Liu, Tengjun, Ying Chen, and Wanxuan Gu. "Deniable Diffusion Generative Steganography." 2023 IEEE International Conference on Multimedia and Expo (ICME). IEEE, 2023.
16. Li, Yung-Hui, et al."Coverless image steganography using morphed face recognition based on convolutional neural network."EURASIP Journal on Wireless Communications and Networking 2022.1 (2022): 28.
17. Raja, K.B., Vikas, Venugopal, K.R and Patnaik, L.M. "High capacity lossless secure image steganography using wavelets"International Conference on Advances Computing and Communications, pp.230–235 (2006) .
18. Kobayashi, H., Noguchi, Y. and Kiya, H. 'A method of embedding binary data into JPEG bitstreams'Systems and Computers in Japan, January 2002, Vol. 33, No. 1, pp.18–26.
19. Spencer Churchill, and Brian Chao. (2019). Anime Face Dataset [Data set]. Kaggle. https://doi.org/10.34740/KAGGLE/DS/379764