Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

IMAGE STEGANOGRAPHY : METHODS TO INCREASE ROBUSTNESS AND IMPERCEPTIBILITY

Dr.Ch.Babi ,Ph.D, Associate Professor, *dept of cse, Raghu engineering college,dakamarri(V),Bheemunipatnam visakhapatnam Dist. pin code:531162*

B.Eswar Jagannadh Raja, Ch.Sai Sri Harsha, B.Jessica *students,dept of cse, Raghu engineering college, dakamarri(V),Bheemunipatnam visakhapatnam*

***Abstract*—** Image Steganography could be a method for concealing private data inside a cover picture, empowering secure communication through unreliable channels. This paper investigates different picture steganography strategies, analyzing their qualities and shortcomings. We categorize these strategies based on the space (spatial or recurrence) utilized for implanting the secret information. We research about the key perspectives of picture steganography, counting imperceptibility, embedding capacity, and vigor. This paper points to supply researchers with a comprehensive understanding of distinctive steganographic strategies to select the foremost reasonable strategy for their particular information covering up applications.

***Index Terms*—Image Steganography, Spatial Domain, Frequency Domain, Embedding Capacity, Robustness**

I. INTRODUCTION

The far reaching utilization of the web has encouraged communication but raised concerns exclusively with information security. Steganography offers a arrangement by covering up delicate data inside apparently harmless cover media like pictures. This paper centers on picture steganography, a vital viewpoint of Information hiding.

1.1. Image Steganography's Goals

Conceal secret data: The main goal is to incorporate private information into a cover image so that unauthorized viewers are unable to recognize it is there.

Preserve image quality: To avoid suspicion and maintain the cover image's aesthetic appeal, the steganographic method should make only minor changes to it.

Optimize embedding capacity: The method should effectively embed a sizable quantity of sensitive information into the cover photo.

Assure robustness: To guarantee a successful retrieval, the buried data must be resilient to a variety of attacks, including compression, filtering, and noise addition.

1.2. Comparing Watermarking and Cryptography

Unlike watermarking and cryptography, image steganography

Data is encrypted by cryptography, making it illegible without a decryption key. The changed format of the encrypted data itself draws attention to it.

Adding a watermark to the cover picture for content authentication or copyright protection is known as watermarking. Under some conditions, the watermark is detectable.

2.Image Steganography Techniques

2.1 Least Significant Bit (LSB) Substitution:

LSB replacement is widely used, but despite its simplicity and popularity, it has several inherent drawbacks that warrant more investigation. Below is an explanation of its workings and things to think about:

Embedding Process: After loading the cover image, every pixel value (24 bits for RGB, 8 bits for grayscale) is transformed to binary format.

Each pixel value's least significant bit (LSB) is extracted, or a fixed amount of LSBs are extracted.

A binary stream is also created from the secret data.

Subsequently, every data bit is embedded by substituting the matching data bit for the retrieved LSB(s) of the cover picture pixel.

After that, the altered pixel values are transformed back into decimal format and utilized to recreate the stego-image (an image with concealed data.

Visual Impact:Changes in the lower-left corner pixels' LSBs are less noticeable to the human eye. When the LSB is changed, there is usually less visual distortion and the stego-image looks almost exactly like the original cover image.

Variations of LSB substitutions:

Although the fundamental LSB substitution technique is straightforward, researchers have suggested modifications to improve security or embedding capacity:

Random LSB: With this method, the LSB is modified by randomly choosing a portion of the cover image's pixels in an effort to increase security. Because of this unpredictability, it is more difficult for attackers to use statistical patterns in the stego-image to identify the existence of hidden data. Random selection, however, may result in a dispersed distribution of embedded data, which could lower the total embedding capacity.

Predictable LSB: In this version, speed comes before security. The pixels to be modified by the LSB are chosen according to a preset pattern or sequence. Attackers that are aware of the particular steganographic technique could take advantage of the predictable pattern, even though it is faster than random selection.

Quantization-oriented LSB: This method concentrates on maintaining picture quality while embedding. To account for the hidden data, the pixel values are modified within a predetermined range rather than simply changing the LSBs. This method achieves some degree of data embedding while reducing the

amount of obvious artifacts introduced.

LSB Substitution's Restrictions:

Though widely used, LSB replacement has some intrinsic drawbacks that should be taken into account:

Low Embedding Capacity: The LSB substitution has a comparatively low embedding capacity. The amount of data that can be hidden within the cover image is limited to changing only one LSB per pixel. For situations when there needs to be a significant payload of hidden data, this might not be enough.

Insufficient Robustness: The embedded data in LSB replacement can be destroyed by a variety of picture alteration techniques. LSBs can be changed by methods such as noise addition, filtering, and compression, which can contaminate the hidden data while it is being retrieved.

2.2. Other Techniques in the Spatial Domain:

In addition to LSB replacement, a few more spatial domain steganography methods take advantage of the inherent redundancies in digital images:

Taking Advantage of Redundancies: This technique finds regions in the picture with comparable textures or color values. With little loss in visual quality, secret data can be embedded in these superfluous regions. To incorporate data bits, methods such as Pixel Value Differencing (PVD) modify the variations between neighboring pixel values.

Embedding with Vacant Space: Certain picture file types, including BMP, have comments or extra header data. A little quantity of data can be hidden by taking use of this vacant space. Nevertheless, steganographic instruments acquainted with these formats may be able to identify such concealed data.

Security Factors in Techniques for the Spatial Domain:

Although spatial domain techniques are simpler to deploy than frequency domain approaches, their security is typically weaker. Some security factors for spatial domain steganography are as follows:

Steganalysis: This is the process of figuring out if a stego-image contains any hidden data. Anomalies in the LSBs or other features of the stego-image that can point to the existence of hidden data might be found using statistical analysis methods.

Stego-key:

Security can be improved by adding a secret key to the steganographic procedure.

2.3. Comprehensive Frequency Domain Techniques:

When compared to spatial domain methods, these methods have the following advantages:

Greater Embedding Capacity: More data can be embedded inside the coefficients that represent higher frequencies, which are less noticeable to the human eye, by converting the image to the frequency domain (DCT or DWT).

Enhanced Robustness: Changes in the frequency domain are frequently less obvious in the spatial domain, increasing the buried data's defense against intrusions.

Typical Methods in the Frequency Domain:

Discrete Cosine Transform is used in DCT-based steganography to split an image into different frequency bands. The middle-frequency coefficients have secret data hidden in them to strike a balance between capacity and imperceptibility.

DWT-based Steganography: Divides the image into subbands with different spatial and frequency resolutions by using the Discrete Wavelet Transform. Certain subbands can have data embedded in them based on the intended balance between robustness and imperceptibility.

Although frequency domain approaches are more robust by nature than spatial methods, security considerations should not be overlooked:

Steganalysis in the Frequency Domain: To find hidden data, sophisticated steganalysis approaches can focus on frequency domain anomalies. The goal of methods such as spectral analysis is to find statistical irregularities in the changed coefficients.

Countermeasures:

Spread Spectrum: Within the selected frequency domain, secret data is dispersed over a larger range of coefficients. This lessens the payload in each coefficient but makes it more difficult to identify the encoded information statistically.

Adaptive embedding modifies the embedding strategy dynamically according on the image's local properties. This aids in preventing the introduction of statistical patterns that could be used in steganalysis.

Robustness Error Correction:

Maintaining the integrity of the concealed data during transmission or storage is a critical component of strong steganography. Error correcting techniques can be incorporated to achieve this:

Error Correcting Codes (ECCs): Mistakes that may happen during transmission or storage can be corrected by including ECCs with the secret data. The expected amount of channel noise or potential assaults determines the ECC strength to use.

Joint Embedding and Error Correction: Methods that integrate error correction and data embedding into a single procedure are being investigated. By doing this, the frequency domain's available space for data and ECC information can be used as efficiently as possible.

Advanced Steganography Methods for the Frequency Domain:

Frequency domain steganography research is always changing, with advances being made in the following areas:

Adaptively choosing embedding spots for maximum capacity and robustness can be achieved by the analysis of image attributes using machine learning and deep learning techniques. They can also be used to create more complex error correcting systems that are customized to the particular content of the image.

Psychovisual Models: You can increase imperceptibility even further by using psychovisual models into the steganographic process. These models can direct the embedding technique to reduce the introduction of visually observable artifacts by taking into account the sensitivity of the human visual system to various spatial frequencies.

II. LITERATURE REVIEW

LSB Substitution: Fridrich et al.'s groundbreaking study [1] introduced LSB substitution as a simple yet useful method. Mie et al.'s subsequent investigation [2] looked into better embedding techniques that used LSB matching for increased imperceptibility. Nevertheless, as Chen et al. [3] pointed out, LSB techniques have poor robustness and capacity.

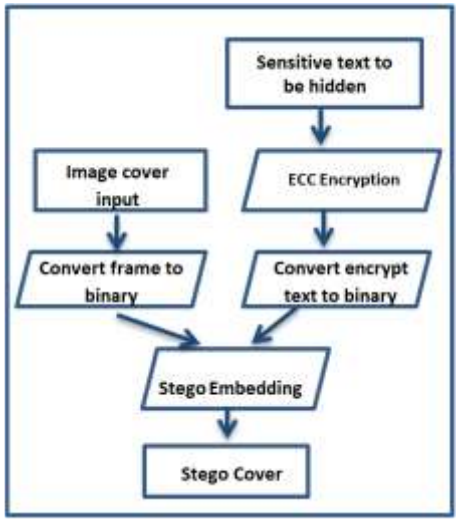
Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

Other Spatial Techniques: Li et al. [5] examined vacant space embedding and emphasized its capacity constraints, whereas Provos [4] suggested using redundant portions in images for steganography.

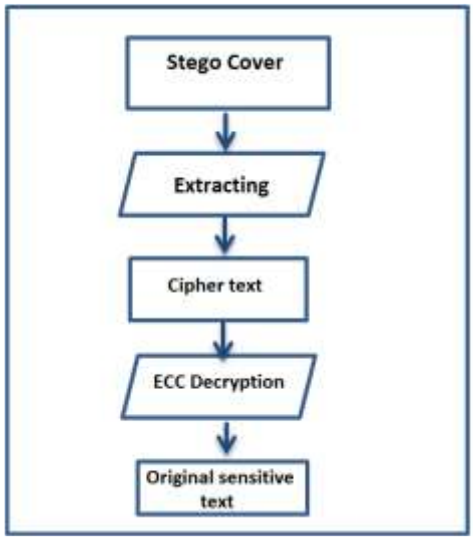
In the frequency domain:

DCT-based Steganography: DCT has been a widely used steganographic technique. Middle-frequency embedding was investigated by Langelaar et al. [6] to strike a balance between imperceptibility and capacity. But as Luo et al. [7] noted, this strategy might not be resilient against various attacks.

DWT-based Steganography: In contrast to spatial approaches, Wu et al.'s steganographic scheme [8] showed enhanced robustness. For optimal performance, Tian [9] looked at selective embedding in particular DWT subbands.



(a) Encrypting and hiding data



(b) Retrieving Data Process

Assessment of Performance:

Imperceptibility: SSIM, a more thorough metric than PSNR, was introduced by Wang et al. [10] for the assessment of image quality. Liu et al.'s more recent studies [11] investigate sophisticated measures that take into account elements like human visual perception.

resilience: A system for assessing steganographic resilience against different attacks was developed by Fridrich et al. [12]. Methods for enhancing robustness against certain assaults, such as JPEG compression, were examined by Barni et al. [13].

III.METHODS

Substitution of the Least Significant Bit (LSB): This is an easy-to-use and popular approach. We can investigate these modifications in further detail for enhanced capacity or security:

Optimized Replacement: Using the incoming data and surrounding pixel values, move the LSB a few locations to the right rather than replacing it exactly. By doing this, visual artifacts can be reduced and embedded data security can be strengthened.

PVD (Pixel Value Differencing) involves calculating the difference between adjacent pixels and then manipulating this difference value to incorporate data instead of directly changing pixel values. As changes are dispersed over pixels, this may increase imperceptibility.
Making Use of Redundancies

Quantization Index Modulation (QIM): Quantize a given color channel into a finite number of levels (for example, the least important portions of the blue channel). Integrate by modifying the color values in visually comparable locations by gradually changing the quantization limits.

Vacant Space Embedding: Though its use is restricted, methods such as taking use of vacant space in headers or comments inside particular image formats (like BMP) can be applied. Tools for steganography that are familiar with these formats may be able to find such buried data.

DCT-oriented Cryptography:

Adaptive Embedding: Examine the content of the image and modify the degree of embedding across various frequency ranges. In regions where visual complexity is higher, this can enhance imperceptibility.
DWT-oriented Cryptography:

Human Visual System (HVS)-based Selective Embedding: Luminance changes are more noticeable to the human eye than chrominance variations. Use this feature to your advantage by aggressively embedding data in higher-frequency chrominance subbands for increased imperceptibility.

Error Correction Codes: To increase the reliability of the

secret data during extraction, particularly following manipulations like compression, apply error correction codes along with it.

Steganographic Key Management: Handle the secret key used for extraction and embedding securely. Techniques like secure key derivation functions and key exchange protocols may be used in this.

IV.PROPOSED MODEL

The Technique of Imperceptibility: Copying the Original
The degree of resemblance between the original cover image and the stego-image with the hidden data is referred to as imperceptibility. The final objective is to produce a stego-picture that, to the naked eye, looks exactly like the cover image.
Assessment of Imperceptibility:
Measuring imperceptibility is crucial to evaluating steganographic techniques' efficacy. These are a few frequently used metrics:

Peak Signal-to-Noise Ratio (PSNR): This conventional measure contrasts the cover and stego pictures' pixel values. Greater similarity is indicated by a higher PSNR. But PSNR has its limitations. Its correlation with human visual perception is not always exact. For example, even if the stego-image adds small but discernible artifacts in visually significant locations, PSNR may still be high.

Structural Similarity Index Measure (SSIM): This sophisticated metric offers a more precise evaluation of how similar the two images' structures seem to the naked eye. Beyond just pixel values, SSIM takes texture, brightness, and contrast into account. This increases its dependability as a steganographic imperceptibility indication.
Models for Visual Quality Assessment (VQA): VQA models trained on human perception data can be used for ever more intricate analyses. These models are able to assess the cover image and forecast the potential effects of different embedding techniques on visual quality. This enables the choice of embedding locations and parameter adjustments to reduce the introduction of human-perceivable artifacts.
The Search for Sturdiness: Robustness

The term "robustness" describes the embedded data's resistance to several types of alteration that the image may experience during storage or transmission. Frequently inadvertent, these manipulations can consist of:
Noise addition: During transmission, electronic noise may contaminate the image data.

Compression: To minimize file size, image compression algorithms might change the values of individual pixels.
Filtering: The embedded data may be impacted by the use of filters to improve or sharpen the image.
These are the models proposed which are some essential methods used to produce reliable steganography:

Error-correcting Steganography Using Adaptive DWT:
The Discrete Wavelet Transform (DWT) is used in this method to embed data in particular subbands. The image is divided into subbands using DWT, each of which has unique spatial and frequency properties.
The method minimizes the impact on visually significant regions by choosing embedding data in subbands with higher redundancy based on analysis of the image content.
It is also possible to incorporate mistake correcting codes with the secret data. These codes assist in identifying and fixing mistakes made during attacks such as compression or noise addition.
In order to determine the best embedding locations within the selected domain (spatial or frequency), this method makes use of optimization methods. The objective is to minimize the effect on imperceptibility while optimizing the embedding capacity (amount of hidden info).
One can use methods such as particle swarm optimization or evolutionary algorithms to find the optimal embedding strategies inside a given search space.

Integration of Visual Quality Assessment (VQA):

The steganographic procedure can incorporate VQA models that have been trained on data related to human perception. During data concealing, these models can dynamically modify the embedding strength by analyzing the cover image.
The VQA model might suggest embedding locations or strengths that are less likely to create visually noticeable artifacts by examining the content of the image.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

Randomly selected pair of cover (left) and steganographic (right) image

V.CONCLUSION

Selecting the Appropriate Instrument: Aligning Steganography Methods with Use Cases:

The choice of the best method for a given application determines how effective image steganography will be. Different approaches are appropriate in different situations since they have different benefits and drawbacks. This is a summary of how to select the most appropriate steganographic technique for your needs as an application.

Hide Tiny Amounts of Information That Are Highly Imperceptible:

Scenario: Let's say you wish to obtrusively identify ownership of a photograph by adding a copyright watermark to it.

Optimal Method: A straightforward spatial domain method like LSB substitution would be adequate in this situation. Because of its extreme imperceptibility, the stego-image will resemble the original almost exactly. It can only hide a tiny amount of data, though, because of its constrained embedding capacity, which is ideal for a copyright watermark.

Hiding Bigger Payloads or Giving Robustness First Priority:

Scenario: Now imagine a scenario in which you need to conceal more secret information inside of an image, such a brief message or authentication key. Furthermore, resilience to possible manipulations during transmission becomes essential.

Optimal Method: Frequency domain methods such as DCT or DWT-based steganography are better options in this situation. These techniques use the characteristics of the image's frequency bands to incorporate data. When compared to spatial approaches, they have a far higher embedding capacity, which lets you hide a bigger payload. Additionally, changes made in the frequency domain frequently have less of an impact on the spatial domain—that is, the actual image—making the embedded data more resilient to manipulations like noise addition or compression.

Things to Take Into Account While Selecting a Technique:

The following are important variables to take into account when choosing an image steganographic method:

The size of the data payload that needs to be hidden. While spatial techniques have limitations, frequency techniques have more potential.

Un perceivability Conditions: How important is it that the stego-picture and the cover image have the exact same visual appearance?

Strongness Requirements: Does the image have to be resistant to changes made to it while it's being stored or transmitted?

Complexity of Computation: Certain methods, especially those in the frequency domain, need more intricate calculations than more straightforward spatial approaches. Think about the processing power that can be used for retrieval and embedding.

Security Points to Remember: The required level of security for the data that is hidden. For low-security applications, spatial approaches might be enough,

VI.BIBILOGRAPHY

https://ieeexplore.ieee.org/document/9335027

https://www.researchgate.net/publication/281693039

https://www.geeksforgeeks.org/image-steganography-in-cryptography/

Bartolini, F., Fontana, V., Barni, M., and Fragouli, A. (2001). strong watermarking for electronic photos. IEEE transactions on visual technology circuits and systems, 11(6), 748-765. (Looks on ways to increase robustness)

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024