DFT and FFT in Image Steganography (and PV fault detection)

# Introduction

* Introduction to Fourier Transform and its Applications

The Fourier Transform (FT) is one of the most significant mathematical tools in modern science and engineering. It provides the foundation for important algorithms like the Discrete Fourier Transform (DFT) and its computationally efficient implementation, the Fast Fourier Transform (FFT). These techniques are pivotal in a wide range of applications, from signal processing to image analysis and even in the construction of the Gaussian function, which is a cornerstone in probability and data analysis.

* Motivation for the Project

This project explores the applications of DFT and FFT in two domains:

* Image Steganography:

Inspired by the increasing demand for data security on the internet, image steganography leverages FFT to encode hidden messages within images. The focus is to understand and apply these Fourier-based techniques to securely embed and extract hidden messages, contributing to the field of secure communication.

* PV Fault Detection Analysis (Side Project):

As an additional objective, this project aims to apply Fourier-based methods to analyze fault signals in photovoltaic (PV) systems. By leveraging DFT/FFT for signal adjustment and fault analysis, this project explores their potential in improving the reliability of PV systems.

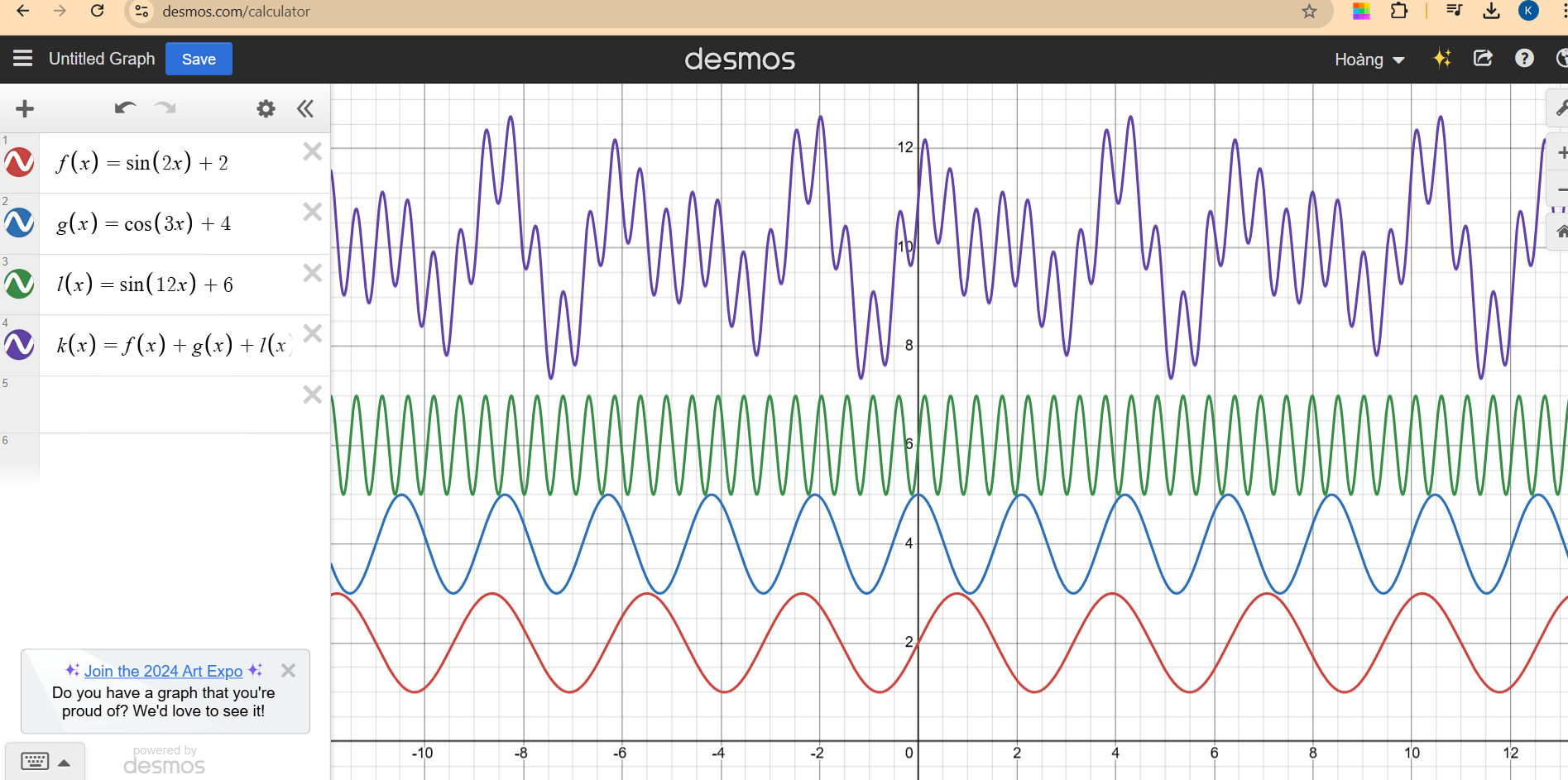
* Why Image Steganography?

The inspiration for choosing image steganography stems from the growing need for secure methods of data transmission in today's digital world. Among the many approaches researched, using FFT for hiding images offers a robust and efficient solution for encoding messages. This project demonstrates how FFT can be employed to meet these demands by securely embedding and extracting data from digital images.

# Theory background

## FT

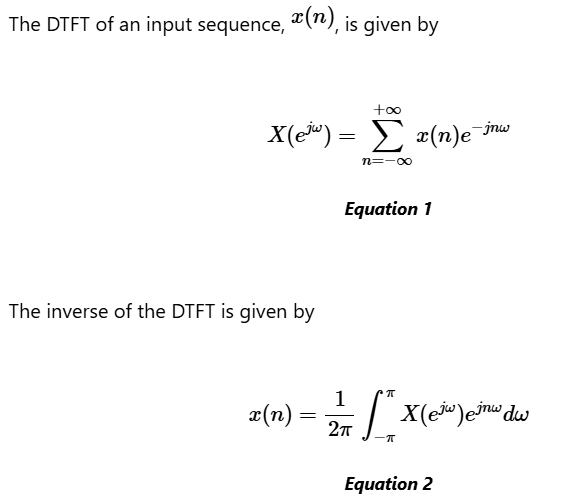
Fourier transform is an interesting function. And it is the answer for the question how can we unmix a complicated signal we record from the real life. Why? Take an example the microphone can measure the air pressure and then give us a signal like this:



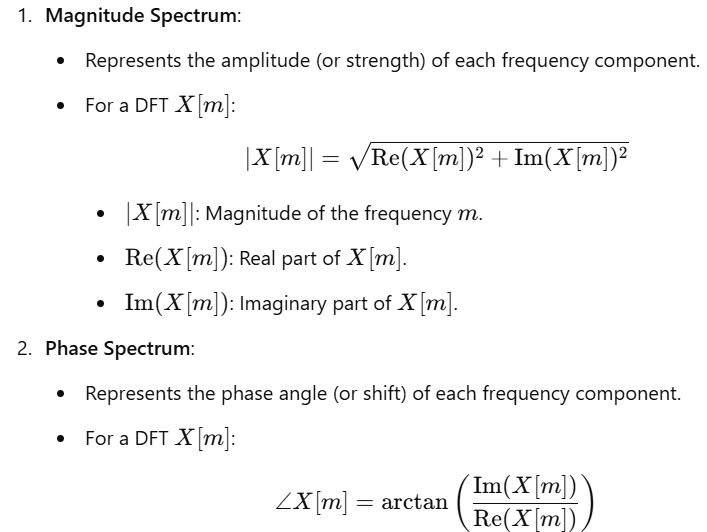
<https://prajwalsouza.github.io/Experiments/Fourier-Transform-Visualization.html>

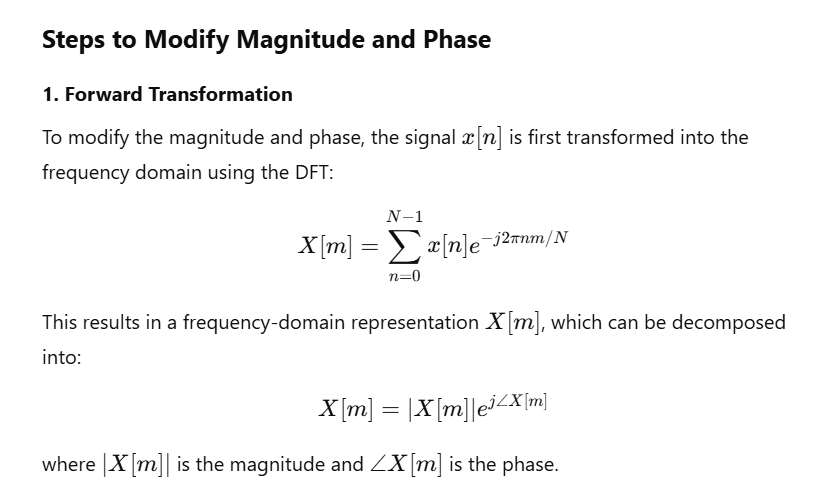
## DFT

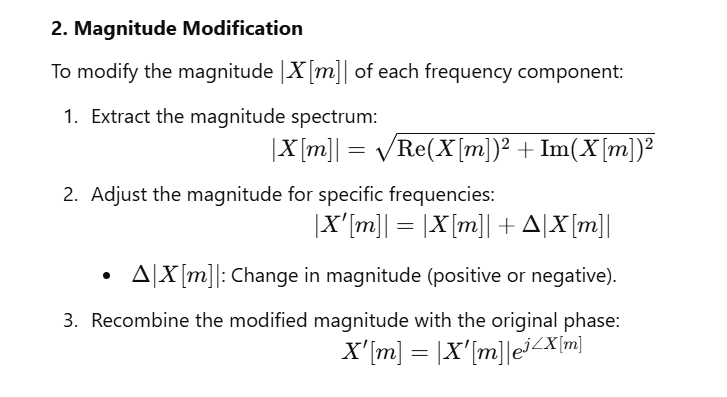
The DFT is one of the most powerful tools in digital signal processing which enables us to find the spectrum of a finite-duration signal. The fourier analysis provides several mathematical tools for determining the frequency content of a time-domain signal, especially the DFT is good for analyzing the discrete sequence x(n). There are only two techniques from the Fourier analysis family which target discrete-time signals: the discrete-time Fourier transform (DTFT) and the discrete Fourier transform (DFT).

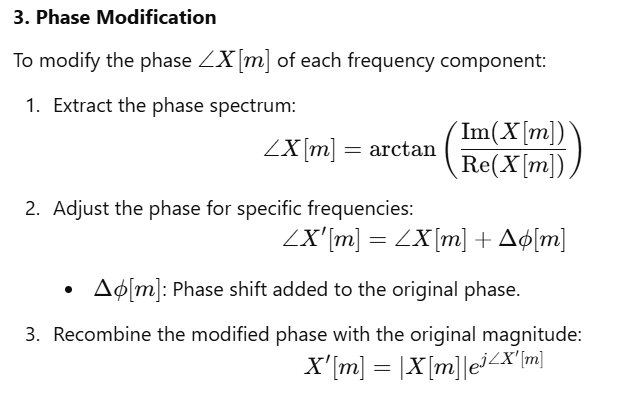


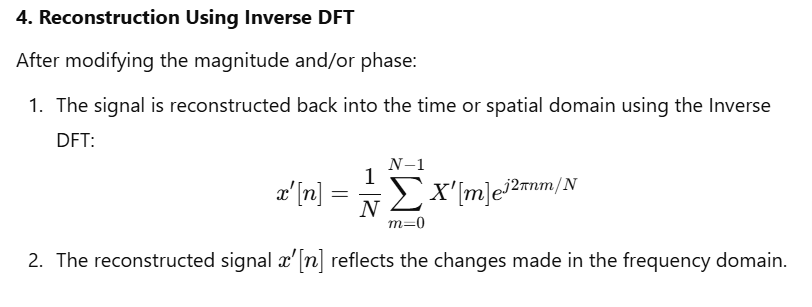
* While the DTFT has the continuous frequency domain which is used in analyzing the theoretical behavior of systems, the DFT has the discrete frequency domain which is applicable to real-world problems like spectral analysis, filtering, and signal compression.
* We can use the DTFT to find the spectrum of a finite-duration signal ; however, given by the above equation is a continuous function of . The DFT can be computed based on the theory of the DTFT.
* The DFT have some properties: Circular/ cyclic time shift, Cyclic/circular convolution, Linear convolution with cyclic convolution. However, just three properties which relates to the applitions of DFT in Image steganography and PV fault detection can be present:
* **Magnitude Spectrum Modifications and Phase Modifications in the DFT:** can be implemented by representing a signal in the frequency domain and allowing specific adjustments to its spectral components before reconstructing it back to the time or spatial domain.

****

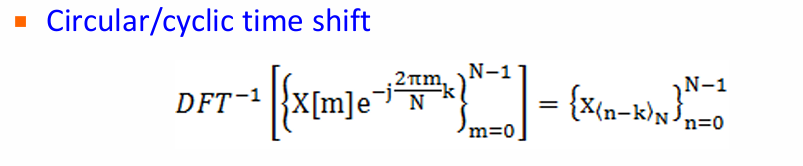
****

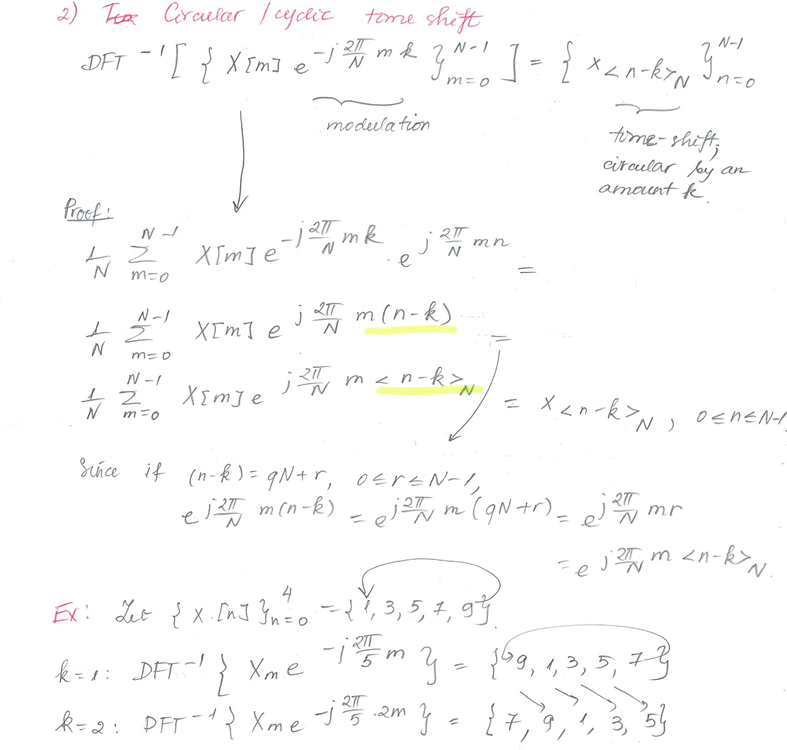
****

****

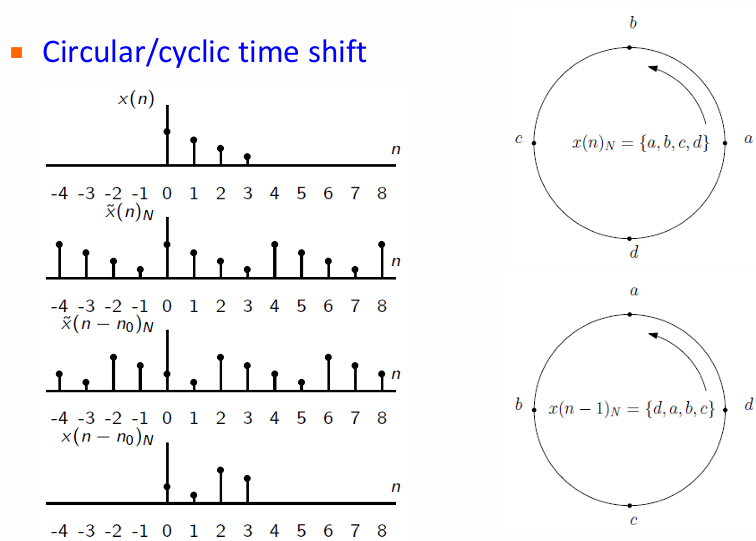
****

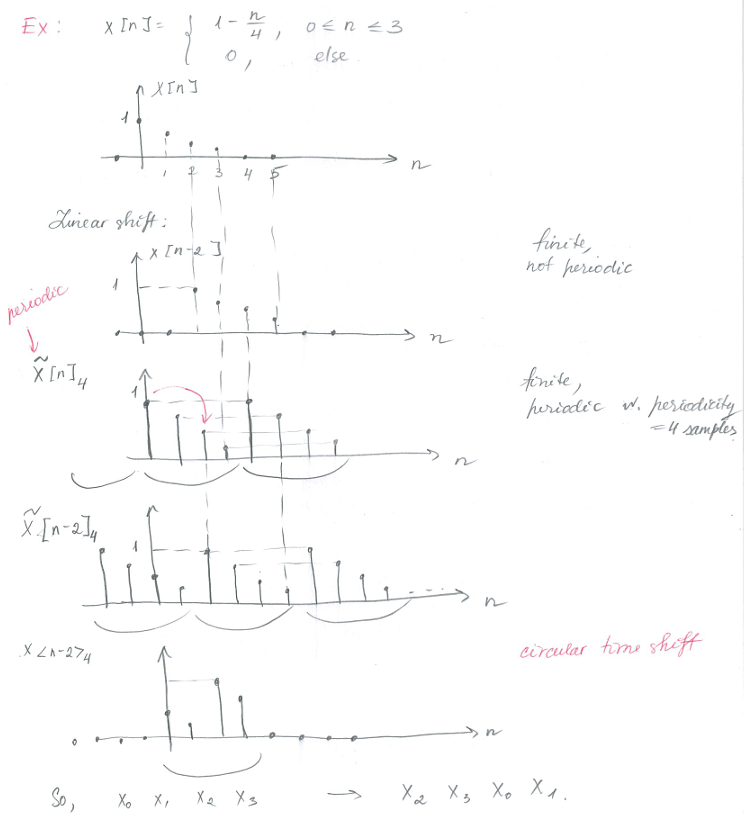
* **The circular/cyclic time shift** property of the DFT decribes how a shift in the time domain affects the frequency domain representation of a signal. In **steganography**, circular time shift is useful for designing robust data encoding schemes against small modifications or cropping. This periodicity ensures resilience in steganography methods. In **PV Fault Detection,** time shifts in PV signal processing (e.g. sudden waveform phase shifts) can identifies using cyclic properties, indicating a transient fault or delay in energy delivery.

****

****

**Explaination:** When a signal is circularly shifted by k positions, the resulting sequence is denoted as , where N is the length of the sequence.

****

****

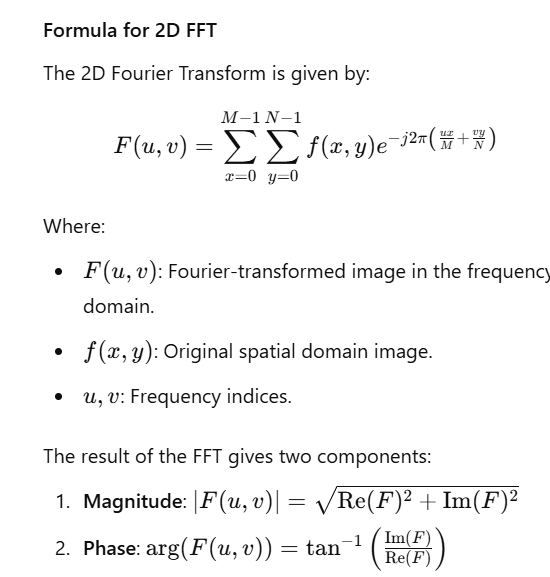
**Explaination:** a circular shift like the elements of a ring. The values “wrap around” when they move past the edge of the sequence. The frequency domain modification/phase modulation reflects this time-domain rotation, enabling efficient cyclic transformations. The above diagram illustrates a non-periodic signal and its periodic extension using a circular time shift. For instance, the first sample is the original finite sequence defined from 0 to 3. The second sample is the sequence wrapped around by a circular shift by -2, creating a periodic version

## FFT

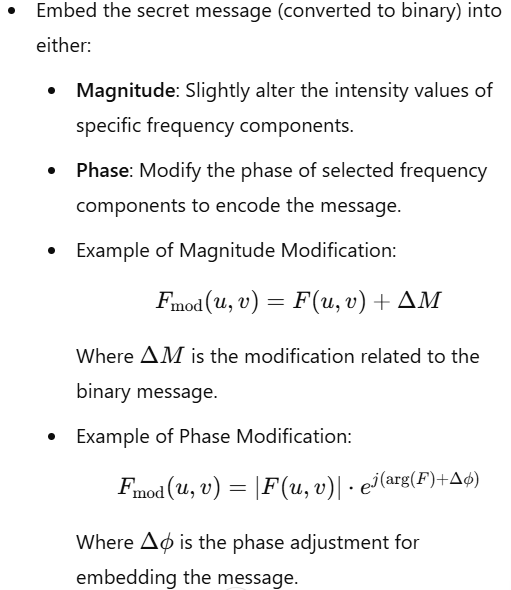
## Image processing

* **Pixel:** A pixel is the smallest unit of a digital image, representing a single point in the image grid. **In grayscale images**, each pixel has an intensity value. **In color images**, each pixel contains color information, typically represented as combinations of Red, Green, and Blue values. Regarding to **Pixel Intensity Analysis**, Pixel values are brightness, contrast, and color distribution. Besides, patterns or features (e.g. edges, textures) are detected based on variations in pixel intensities. Pixels are also a segment grouped or classified into meaningful regions based on intensity, color, or other attributes. In Steganography, pixel values are modified slightly to hide secret data by altering the least significant bit of pixel intensity. On the contrary, in the extraction process, hidden information is retrieved by analyzing specific pixel values or their patterns.
* **Scale-gray:** Grayscales images have a single intensity channel, as opposed to color images which have three channels (e.g. RGB). This reduces the complexity of image processing tasks. It requires less memory and storage compared to color images and facilitates for the faster computations and the more complex algorithms in image processing such as Fourier Transform (DFT). **In image steganography**, LSB Significant bit of a pixel’s intensity value is modified to encode binary data (0 or 1). The change in LSB and the grayscale modification are not noticeable to human eye. Scale-gray is simple to transform the grayscale image into frequency domain using DFT, FFT, DCT or DWT; to modify the magnitude or phase of frequency components to embed data and transform the modified frequency back to the spatial domain to generate the stego image.
* **Aliasing:**
* **What is Aliasing?** Aliasing occurs when a signal is sampled at a rate lower than the **Nyquist rate**, which is twice the highest frequency component of the signal. As a result, higher frequency components of the signal are “misinterpreted” as lower frequencies, causing overlapping or distortion in the sampled signal.
* **In image processing, Nyquist rate** is a value equal to twice the highest frequency (bandwidth) of a given function or signal. It has units of samples per unit time, expressed as samples per second. When the signal is sampled at a higher sample rate, the resulting discrete-time sequence is said to be free of the distortion known as aliasing.
* **Aliasing in Image Steganography:** in spatial domain, changes the pixel intensity may not align with the original sampling resolution of the image. In frequency domain, aliasing can occur when the resolution of the frequency representation is too slow.
* **How Aliasing affects message extraction:** In the frequency domain, if aliasing occurs, the frequency components are misrepresented. => the hidden message embedded in specific high-frequency or low frequency regions may become indistinguishable from aliasing noise, leading to errors during extraction. Besides, it can cause the pixel overlapping. This leads to the mismatch with the original representation.
* **FFT 2D -> Magnitude & Phase**

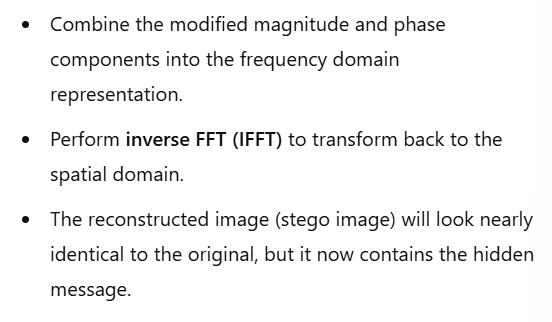
**Step 1:**

****

**Step 2: Modify magnitude or Phase**

****

**Step 3: Reconstruct Image:**

****

## Moving average filter (optional)

# Image steganography

## LSB – Least significant bit

## FFT method in Steganography:

## Result \_ Methodology

## Conclusion

# PV fault detection

## Threshold based method

## Mean and variation method

# Conclusion

# Reference