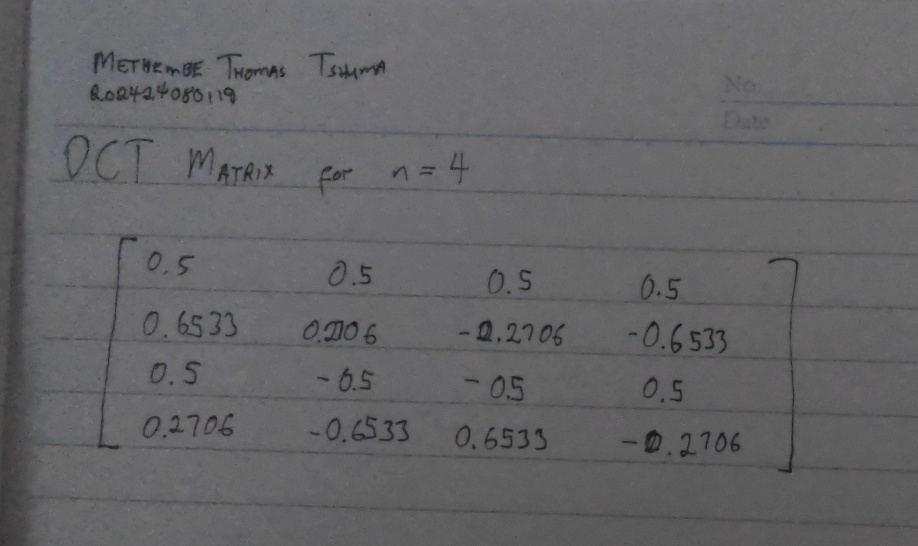
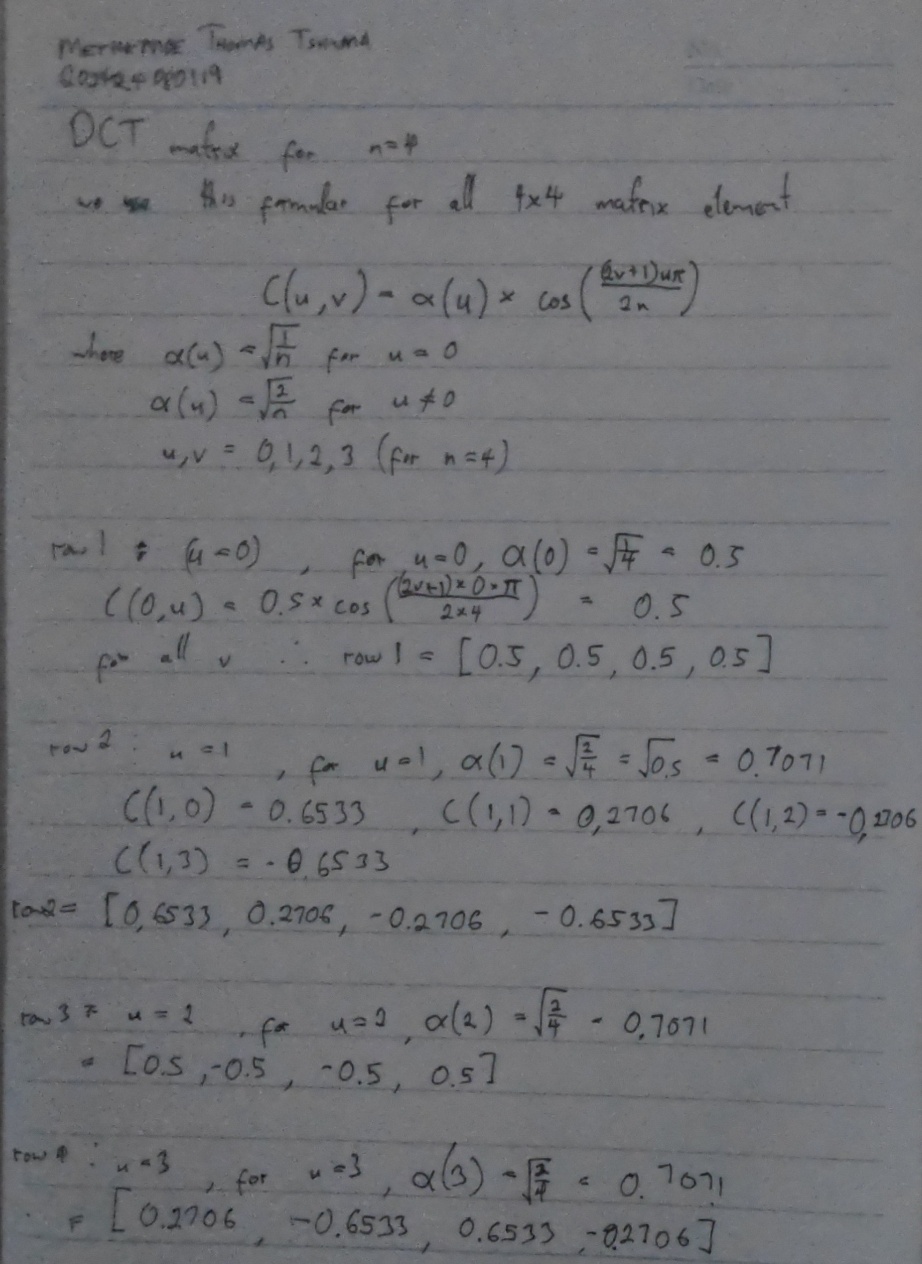
**Assignment 3**

Methembe Thomas Tshuma

202424080119

1. **Sampling** isthe process of selecting discrete points from a continuous image signal, the sampling rate determines the spatial resolution of the digital image and higher sampling rates lead to better image quality but larger file sizes. While **quantization** isthe process of assigning a discrete amplitude level to each sampled value, where the number of quantization levels determines the color depth of the image. Higher quantization levels lead to better color accuracy but larger file sizes.
2. 
3. **Active Image Forgery Detection** is a proactive approach that involves embedding additional information, such as digital watermarks or signatures, into the image during creation. This hidden information acts as a fingerprint, uniquely identifying the image. If the image is altered or tampered with, the embedded information can be used to detect the forgery.

**Passive-blind Image Forgery Detection** is a reactive approach that analyzes the image itself for inconsistencies or anomalies that may indicate tampering. This method does not rely on any additional information embedded in the image. Instead, it examines the image's internal characteristics, such as texture, color, and edge information, to identify potential forgeries.

1. **Copy-Move Forgery** involves duplicating a region within an image and pasting it elsewhere. This creates identical or nearly identical regions within the image. Think of it like copying and pasting a section of a document.

**Image-Splicing Forgery** is a more complex technique that involves taking a region from one image and inserting it into another. This can create inconsistencies in lighting, color, texture, or perspective. Imagine cutting out a piece of one puzzle and trying to fit it into a different puzzle; the pieces won't match perfectly.

1. **Extract Keypoints:** Detect keypoints (distinctive points) within the image using feature detectors like SIFT or SURF.

**Compute Descriptors:** Calculate feature descriptors for each keypoint, representing the local characteristics of the image around the keypoint.

**Match Keypoints:** Compare the descriptors of keypoints from different regions of the image to find matching pairs.

**Verify Matches:** Filter out false matches using geometric constraints or other criteria.

**Detect Forgery:** If a significant number of matching keypoints are found in non-overlapping regions, it indicates a copy-move forgery.

1. (d) None of the above
2. **Preprocessing:** Convert the image to a suitable format (e.g., grayscale) and enhance it if necessary.

**Feature Extraction:** Extract features from the image, such as texture, color, or edge information.

**Forgery Detection:** Apply forgery detection algorithms to analyze the extracted features for inconsistencies or anomalies that may indicate forgery.

**Decision Making:** Based on the analysis, classify the image as genuine or forged.

1. (b) integrity