Beneath the Binary: A Journey into Covert Communication

The City University of New York

CUNY Research Scholars Program

Student: David Liao

Mentor: Dr. Sos S. Agaian

ASAP ACCELERATED STUDY IN ASSOCIATE PROGRAMS

THE CITY UNIVERSITY OF NEW YORK College of Staten Island

ABSTRACT

In an era where digital advancements continue to transform the landscape of secure communication, the need for discreet information transmission methods has never been more crucial. Amidst this, steganography emerges as an arcane technique; adept at embedding information within digital images to avoid unauthorized detection perfectly. This study introduces a steganographic method that harnesses the technique of bit plane slicing. By decomposing digital images into their constituent bit planes, this approach facilitates the nuanced alteration of pixel bits, targeting the least significant bits (LSBs) for the inclusion of hidden messages. This modification is ingeniously designed to remain below the threshold of human perception, thus preserving the visual identity of the original image. A critical examination of this method reveals a careful equilibrium between the imperatives of data concealment and the integrity of image quality, underscoring its resilience to steganalysis; efforts aimed at uncovering such clandestine information. Through a series of experiments, our investigation corroborates the method's proficiency in embedding and retrieving data with negligible impact on visual quality, thereby underscoring its utility in secure and inconspicuous communication. The outcomes of this exploration not only contribute significantly to the burgeoning domain of digital image processing but also pave new pathways for research into sophisticated steganographic methodologies to meet rising concerns.

METHODOLOGY

We adopt a multifaceted approach to produce more results and better analyze these results afterward. In our research, we meticulously explore multiple arrangements of bits to visualize the algorithm's effectiveness with varying bit combinations. Specifically, we focus on strategically manipulating the Most Significant Bits and the Least Significant Bits in parallel. By experimenting with these different ratios we aim to uncover the most effective encryption method that offers the perfect balance between visibility and security.

To quantify the results obtained from this we use a simple model identified as the Structural Similarity Index(SSIM), we compare the original image with the newly created encrypted one and see how similar they are. This metric allows us to compare the original image with the newly created encrypted one to evaluate how similar they appear. SSIM is particularly valuable because it measures the perceptual quality of images. Unlike traditional metrics that simply calculate pixel differences, SSIM considers changes in structural information, luminance, and contrast, which are crucial for human visual perception.

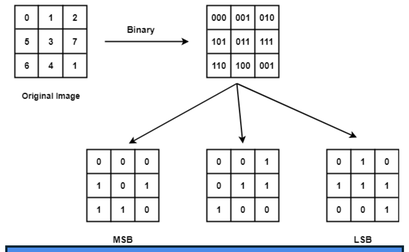
INTRODUCTION

Bitplane slicing decomposes an image into eight binary layers, each corresponding to a different bit in the pixel's binary representation, ranging from 0 to 255. This technique effectively separates the image into multiple layers, allowing for a detailed examination of its visual components at each bit level. While showcasing the structural elements of an image, bitplane slicing also introduces a method known as Bit Plane Compression. This approach prioritizes the most significant bits for encoding and decoding, enabling efficient data compression that maintains the integrity of crucial image details. In simpler terms let's imagine the image as a cake with an intricate design. The most significant bit plane is the top layer where the design is, the least significant is usually just pure cake with little to no design. Now knowing this we are introduced to the idea of Most Significant Bit encryption. This core principle of this is breaking down two images into their eight bit planes. We are attempting to store the first image inside the second image. The first image's most significant bit plane replaces the second images least significant bit plane. After this is done the image should look almost identical to the original image. This is where our research is focused in on; we aim to hide as much of the hidden image into the original image as possible.

Bitplane 1 Bitplane 2 Bitplane 3 Bitplane 4
Bitplane 5 Bitplane 6 Bitplane 7 Bitplane 8

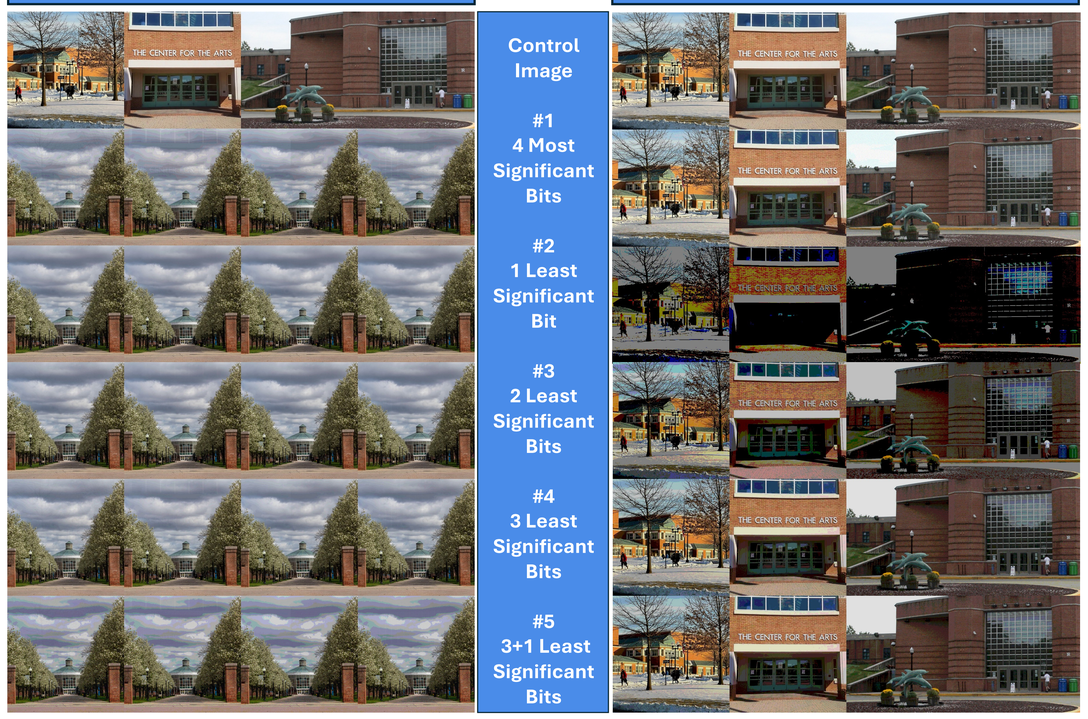
Decomposed Bitplane of Example Image #1

Example Image #1



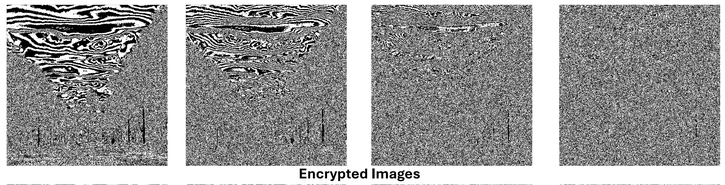
Bitplane Decomposition Visualization

RESULTS

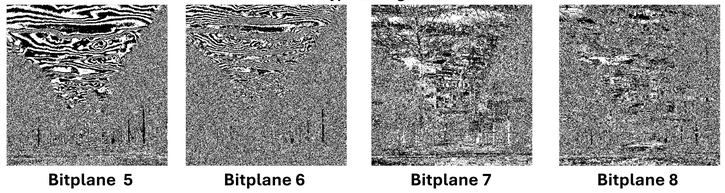


The left side is the results from encrypting with various bit combinations, the left is the resulting decrypted image that comes from it. As you can surmise from looking at the results there are combinations that preserve encrypted image quality and there are others that preserve decrypted image quality. The labeling is how many bits are replaced each time the encryption occurs. The best result here #3 or #4, which result in an almost perfect encrypted image and a high-quality decrypted image.

Control Images



Encrypted Images



Bitplane 5 Bitplane 6 Bitplane 7 Bitplane 8

This visualization is between the control images and encrypted images across their lowest bitplanes, 5-8. When examining the bitplanes it is evident that Control Image #1 is shown in the 7th bitplane of the encrypted image. The main tell here is that the control image should be just sky in the middle yet you can see something tree-like with branches. This visualization is the only way for a human to identify what changes happen as we primarily aim to avoid human detection. The juxtaposition of the control and encrypted images at different bit levels provides an insightful look into the steganographic process, illustrating how data can be concealed within an image's most granular details without compromising the integrity of its overall appearance.

Encrypted	Result 1	Result 2	Result 3	Result 4	Result 5
Image1	93.61%	99.80%	99.35%	97.93%	90.01%
Image2	94.52%	99.82%	99.43%	98.20%	90.12%
Image3	95.93%	99.86%	99.54%	98.60%	90.97%
Image4	95.63%	99.84%	99.51%	98.50%	90.99%
Average Similarity	94.92%	99.83%	99.46%	98.31%	90.52%

The Structural Similarity Index (SSIM) is a metric used to measure the similarity between two images. It is crucial in our study as it quantifies how much the encrypted image retains the appearance of the original, despite the embedded hidden data. The values range from 0 to 100%, where 0 indicates no similarity and 100% means the images are identical.

In the table presented, we observe SSIM values for various encrypted images compared to their original counterparts. The values closely approach 100%, implying that our encryption process preserves the original image's visual structure to a high degree. This is significant as it suggests that the hidden data does not overtly disrupt the perceptual features of the image.

- **Result 1** represents a scenario with higher MSB embedding, offering more security at a slight visual cost.
- **Results 2-4** show increased fidelity to the original image, as fewer MSBs are altered.
- **Result 5** demonstrates the impact when combining MSB with LSB, showing a slight decrease in similarity, indicating a trade-off between encryption strength and image similarity.

An average similarity above 90% across different images suggests that the encryption is generally imperceptible, ensuring the steganographic goal of hiding data in plain sight without significant detection risk.