



StegoChat

Rutvik Dumre	B031
Shiv Avashia	B009
Bux Khurana	B012
Samar Bansod	B044

Image Steganography

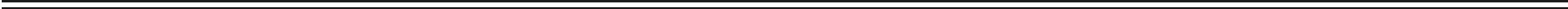
Image steganography refers to hiding information i.e. text, images or audio files in another image or video files.

Why image Steganography?

- Hard to detect
- Original Image is very similar to altered Image
- Embedded data resembles gaussian noise



Steps Involved



Encoding

We firstly compressed the image to a width of 256 without changing the aspect ratio of the image (only the resolution).

Operations performed on the image include:

1. Reshaping
2. Bit plane slicing
3. converting it to

an array of numbers then to a list

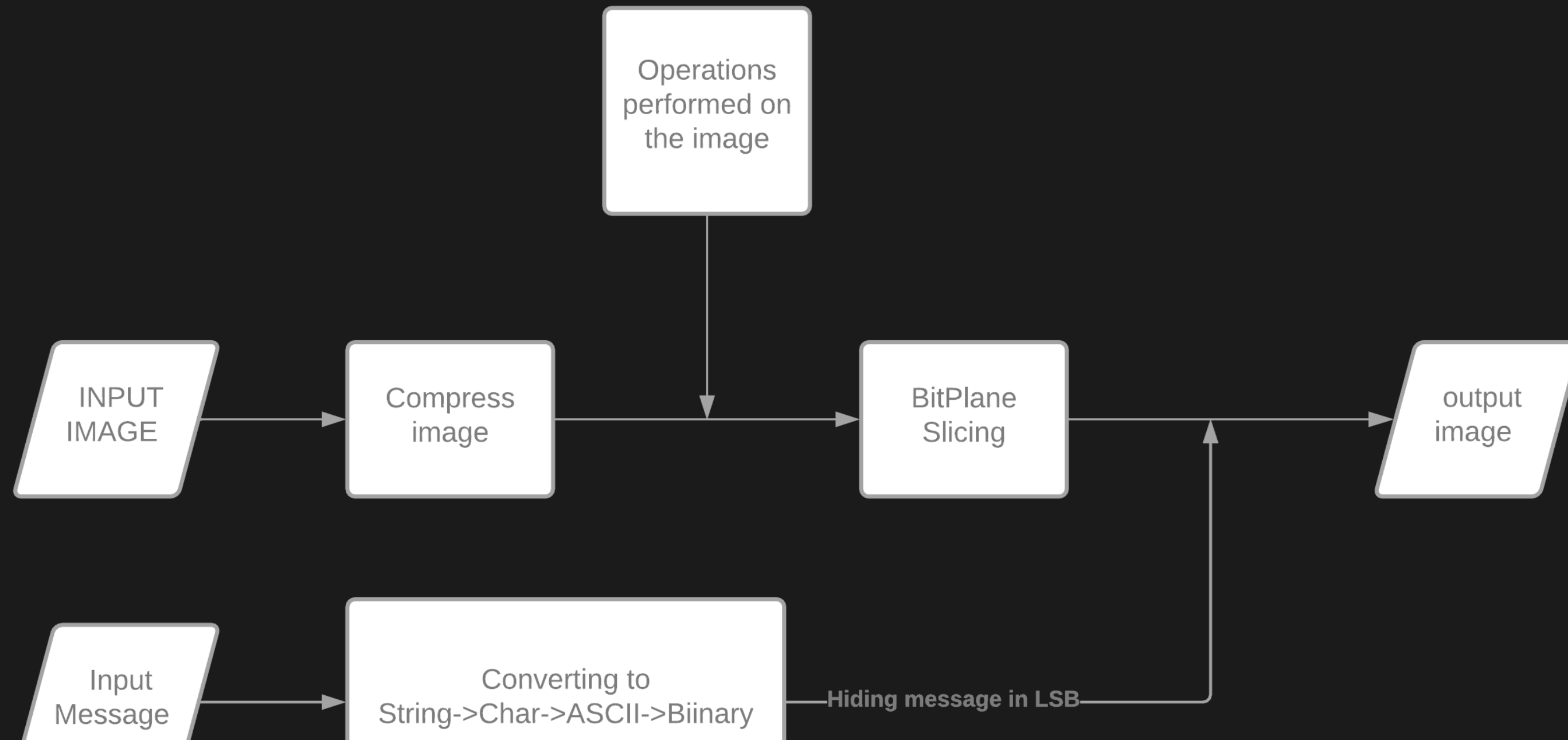
Then we convert the message into a format by appending our digital signature and key at the beginning and end, respectively.

Then we perform bit-plane Slicing to hide the message into our image using the algorithm devised which traverses through a plane and replaces the LSB of the 8- bit binary number of each value of pixels in that plane to our binary values from the ASCII of the Characters in our message.

Then we save the final image after hiding the message.

Block Diagram

ENCODING



Decoding

We take the input of the image to be decoded
After taking the input, we check for the key present in output image.

If no key is present that means the image is not modified or encrypted with a message according to our algorithm.

If the key is present, it marks a flag = 'encrypted' and then checks for the digital signature and mark it as a starting point for message retrieval.

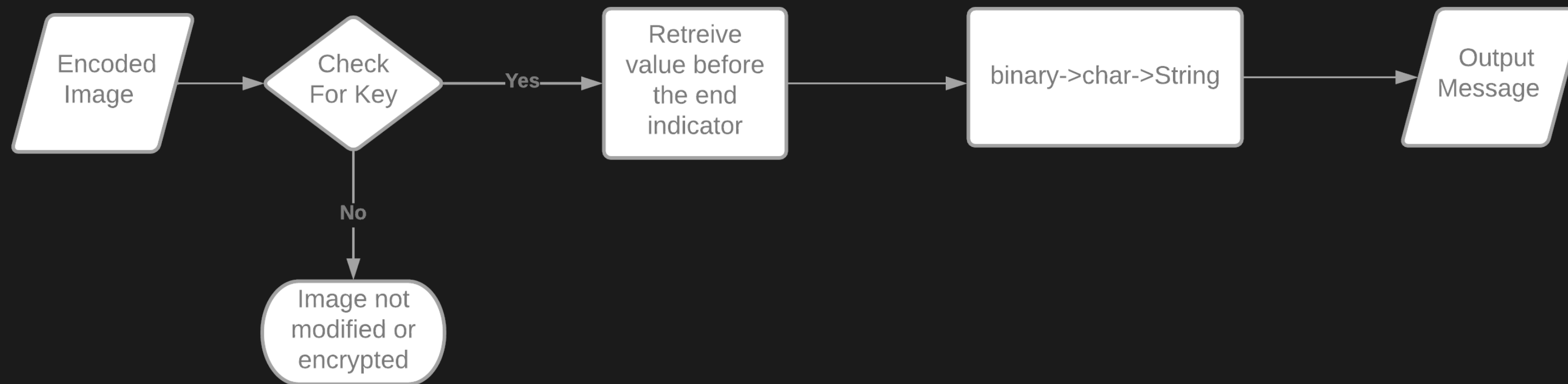
Then the flag is checked for encrypted, if not it displays the image has been modified.

Then we go for un hiding the data using the unhide function

It takes the 8-bit value and then loops in [i:i+8] format as the numbers are 8 -bit binary and then convert it into ASCII values (decimal values) and then to their according Characters to form a String which is our inputted message.

Block Diagram

DECODING

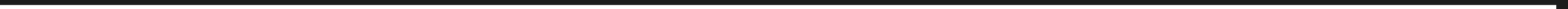


Future Scope

A password can be added to the algorithm which can authenticate the user trying to access the hidden data in the image.

Encryption to the hidden message can be added e.g. 256-bit encryption using protocols like AES and SSL.

The image compression used in the project can be lossless. The steganography capacity can be increased



THANK YOU

