**Abstract**

In this project we will aim to layer several different image encryption techniques that have been proposed in the literature around bit-plane slicing, to create a novel algorithm that is even less susceptible to brute force techniques.

One layer of the many transforms will also feature a novel plane reversal technique to further enhance the security of the encryption.

**Introduction**

With the worlds’ rapid movement towards digitalisation of communication, security and privacy of information are becoming more and more important, leading to large amounts of research going into the study of data encryption techniques in this domain. Optical encryption techniques gather a lot of interest as they provide the ability to process large images very quickly to produce results that are very difficult to brute force as they allow hiding of information along different transforms.

Steganography is the umbrella term used for techniques that use transforms on images to hide the original data. Steganography is several applications in various fields such as image copyright protection, fraud detection, copy control etc.

Steganography is also used on medical records and aadhar cards to conceal private information to protect the identities of individuals.

The term “cover image” describes the medium in which secret information is embedded. Modern image data hiding uses two basic principles for concealing data, namely the embedding and extraction algorithms. The essential components of the embedding algorithm are a cover image, secret data, and a secret key. Stego-image is obtained by concealing the secret data into the cover image using the embedding algorithm. The stego image is then used as an input object to extract the secret data.

Image steganography uses image processing techniques for embedding.

The embedding process in data hiding uses a few basic schemes and plays an important role in any stego-image. The commonly used techniques in steganography are based on the spatial domain, but for this project we will be combining transforms on the intensity domain as well.

**Methodology**

For this project, we will start by selecting a greyscale image for simplicity, but this process can very easily be carried out on a 3 or 4 channel image by applying the same transforms across each channel individually.

The procedure for the project will be the following.

1. Break the image into its individual bit planes (8 planes for an 8-bit image).
2. Apply various transforms on the spatial domain on each bit plane separately. For this project we will apply the same transforms on all the bit planes, but different transforms can be applied on different planes.
3. Apply different transforms on the intensity domain on each bit plane separately. For this project we will apply the same transforms on all the bit planes, but different transforms can be applied on different planes.
4. Apply bit-plane reversal randomisation (Novel)
5. Apply all steps in reverse order to obtain the original image from the encrypted image (decryption).

**Results**

Since the bit-plane reversal technique used here is an independent process and is applied at the end, it does not affect the outcome of any previous step. This results in the addition of an extra layer of security that has possibly 8! Or 40,320 combinations, resulting in an encrypted image that is a lot harder to brute force. Since bit-plane slicing has already been carried out in order to perform transformations on different planes as per literature, this additional step has very little overhead for a very high increase in efficiency.

**Conclusion**

Although this novel technique may not be the single most promising technique, no technique can claim to fit this position either. What matters is that the combinations of such small techniques provide several different layers of encryption, which makes the image share dependencies across several different secret keys instead of just 1, making it close to impossible to decrypt without all the original keys.

Furthermore, this novel method definitely provides a very high increase in security for very low overhead and computational cost, making it an extremely easy to implement step for a much secure encryption.

**Novelty**

The bit-plane reversal technique used in this project is a novel algorithm that uses different combinations of bit planes to create a transform on the intensity domain, promising high performance for a low overhead on encryption architectures that already use bit-plane slicing to perform spatial transforms on individual planes.

**Benefit To Society**

As right to intellectual property, security and privacy grows more important by the day, encryption algorithms become more and more important. Even techniques that offer very little performance are important as they add another layer of dependency, making it that much harder to brute-force when used in combination with other existing techniques.

This technique provides a very high boost in performance, and is therefore an extremely powerful technique to boost the security of encryption architectures that use bit-plane slicing as their base.