CSE 539 Final project: SecureShare

Soham Suresh Jagtap , FNU Raisa Arief
School of Computing and Augmented Intelligence, Arizona State University

With the widespread use of digital technologies, information has become more vulnerable to security breaches and cyber-attacks. To address this issue, new methods of data security are needed. This paper proposes a novel approach to data security by utilizing image steganography and Shamir's secret sharing to embed data into images and divide the image into shares, making it difficult to detect and decrypt by adding two layers of obfuscation.

Keywords: Data security | Image steganography | Shamir Secret Sharing | Information protection

Introduction

Stegastamp [1] is a proven novel deep learning-based architecture that is used for implementing image steganography on colored images. It is a UNet-based architecture that takes some text and a cover image input. The text is encoded in the image during the AutoEncoder's Encoder processing and from the encoder, a Stego-Image is given as the output which has the text encoded in it. The Stego-image is then passed through the decoder for giving the encoded text as the output.

Shamir's Secret Sharing [2] describes a method to divide a given data D into n pieces in such a way that D is easily reconstructable from any k pieces, but even complete knowledge of k - 1 pieces reveals absolutely no information about D [1-Shamir paper]. This provides a way to distribute a secret, divided into n parts, among a group of people. The original secret, however, can only be reconstructed when a minimum number of shares, k, are combined together.

Typically, Shamir's secret sharing is applied to alphanumeric data. SecureShare, however, extends this implementation to embed secrets within images using steganography, and applies Shamir Secret Sharing to divide the image into shares.

Implementation

The primary goal of this project is to utilize steganography and Shamir's secret sharing to securely embed a secret message within an image and divide the image into shares, respectively. The steganography technique employed in this project is StegaStamp.

El-Tigani et al. [3] proposed a (k,n) secret sharing scheme for grayscale images, which involves converting the image to grayscale and then applying Shamir's Secret Sharing on the RGB values of the image. However, this approach may not be optimal for certain applications, as it requires converting the image to grayscale and may not retain the original color information. Additionally, this method utilizes individual RGB pixel values, which may result in slower processing times

To address these limitations, SecureShare proposes a new approach where the image is processed using hex codes of the pixels instead of individual RGB values. This approach allows for more efficient processing and avoids the need for grayscale conversion. By utilizing Lagrange interpolation on the hexcode values, SecureShare is able to generate the necessary x, y values for secret sharing, improving the efficiency of the process.

StegaStamp is built with the TensorFlow library which is Python-based. As the first step of the project, we encode the text using the StegaStamp module in an image. The image is then saved with the name encoded_image.png which is then further passed to the Shamir Secret Sharing algorithm for generating shares and reconstructing the secret image. The image is resized to a 224*224 dimension and hence, preferable use an image with a resolution of more than or equal to 224*224. The output hidden image has a resolution of 400*400 on which the Secret Sharing Algorithm is run.

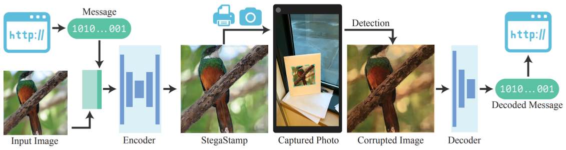


Figure 1: Architecture and workflow for StegaStamp

The PIL library is then used to read in an image and create a numpy array with the hex values of individual pixels. After the creation of the 2D array of hex values, Shamir's secret sharing is applied on the integer values of individual hex codes. The shares are now stored in the 3D shares array, which stores the share value pertaining to the image[i][j] pixel in its shares[i][j][k] element.

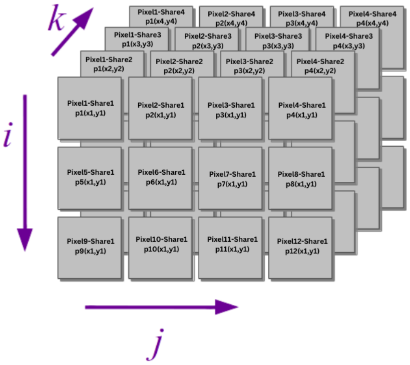


Figure 2:Array for storing generated Shamir's secret shares

For reconstruction, the shares are selected randomly from the set of n shares, which are processed in the reconstruction algorithm to obtain the original hex code.Once the image is reconstructed, it is then passed through the decoder of the StegaStamp module and it gives out the original hidden/encoded text. The text can be seen as a print statement on the terminal.

Results

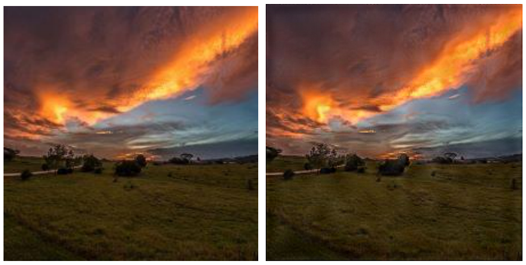
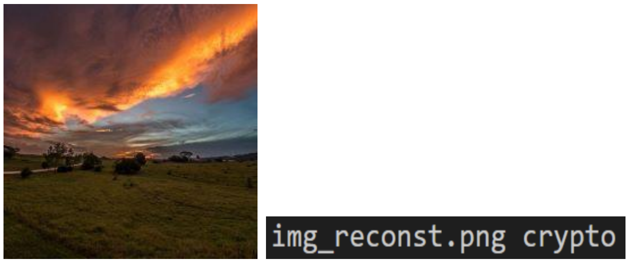


Figure 3: Original Image (left) and encoded image (right)



```
img_reconst.png crypto
```

Figure 4: Reconstructed Image (left) and decoded secret (right)

Conclusion

In conclusion, we successfully implemented the SecureShare project to embed the secret message "crypto" in a 400x400 image. The image was divided into 5 parts with a k value of 3, and the reconstruction algorithm was applied to obtain the original secret message.

Our experiments showed that there was no loss of data during the reconstruction process, and the reconstructed image size remained the same as the original image, which was 209 KB. However, we note that at higher image resolutions, there may be some pixel loss during the conversion process, and in such cases, the field size may need to be increased to ensure that the secret message remains intact.

Overall, the SecureShare project provides a reliable and efficient method for securely sharing secrets by utilizing steganography and Shamir secret sharing techniques. The successful implementation of this project demonstrates its potential for use in various applications, including secure communication and data sharing.

References

[1] Tancik, M., Mildenhall, B. and Ng, R., 2020. Stegastamp: Invisible hyperlinks in physical photographs. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 2117-2126).

[2] Adi Shamir. 1979. How to share a secret. Commun. ACM 22, 11 (Nov. 1979), 612–613. https://doi.org/10.1145/359168.359176

[3] Abdelsatir, El-Tigani & Alhesseen, Sahar & Ali, Hyam & Hashim, Afra. (2014). A Novel (K,N) Secret Sharing Scheme from Quadratic Residues for Grayscale Images. International Journal of Network Security & Its Applications. 10.5121/ijnsa.2014.6406.