Android-Based Digital Image Steganography and Steganalysis

Dominique Piens and Nathan Staffa
Department of Electrical Engineering, Stanford University

Background

Steganography is the discipline concerned with achieving confidential communication by hiding information in plain sight. Steganalysis is the detection of steganography.[1] Through it, users have freedom to operate covertly while performing entirely normal tasks.

Modern steganography typically focuses on utilizing common media, such as images, video, or audio. In addition to being ubiquitous in the modern day, these media have many information redundancies in which a steganographic method can operate.

A basic example of steganography in digital images is modifying the least-significant bits of pixels to conceal a bitwise code, but most modern methods operate in the frequency domain, modifying an image's discrete cosine transform (DCT) coefficients. Our chosen scheme, OutGuess, is such a method.

Motivation

Privacy has never been as large of a concern to the average individual as it is today. With a deluge of high-profile hacks, leaks, and other security breaches in addition to revelations of widespread surveillance, users have increasingly turned to services offering encrypted communications. Yet the very act of using such a service causes suspicion and can lead to increased surveillance. Steganography presents an alternative that draws no extra attention from an observer.

For steganographic tools to be useful, they must be readily available. To that end, several mobile applications have been developed, with varying results. We present the first such application utilizing the OutGuess algorithm for encoding and decoding with a secure key,[2] as well as a detector to give a probabilistic estimate of whether or not an arbitrary image possesses a message hidden with the algorithm.[3]

References

[1] Fridrich, Jessica. "Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes." *International Workshop on Information Hiding*. Springer Berlin Heidelberg, 2004.

[2] Provos, Niels, and Peter Honeyman. "Hide and seek: An introduction to steganography." *IEEE Security & Privacy* 1.3 (2003): 32-44.

[3] Farid, Hany. "Detecting hidden messages using higher-order statistical models." *Image Processing. 2002. Proceedings. 2002 International Conference on*, vol. 2, pp. II-905. IEEE, 2002.

Steganography

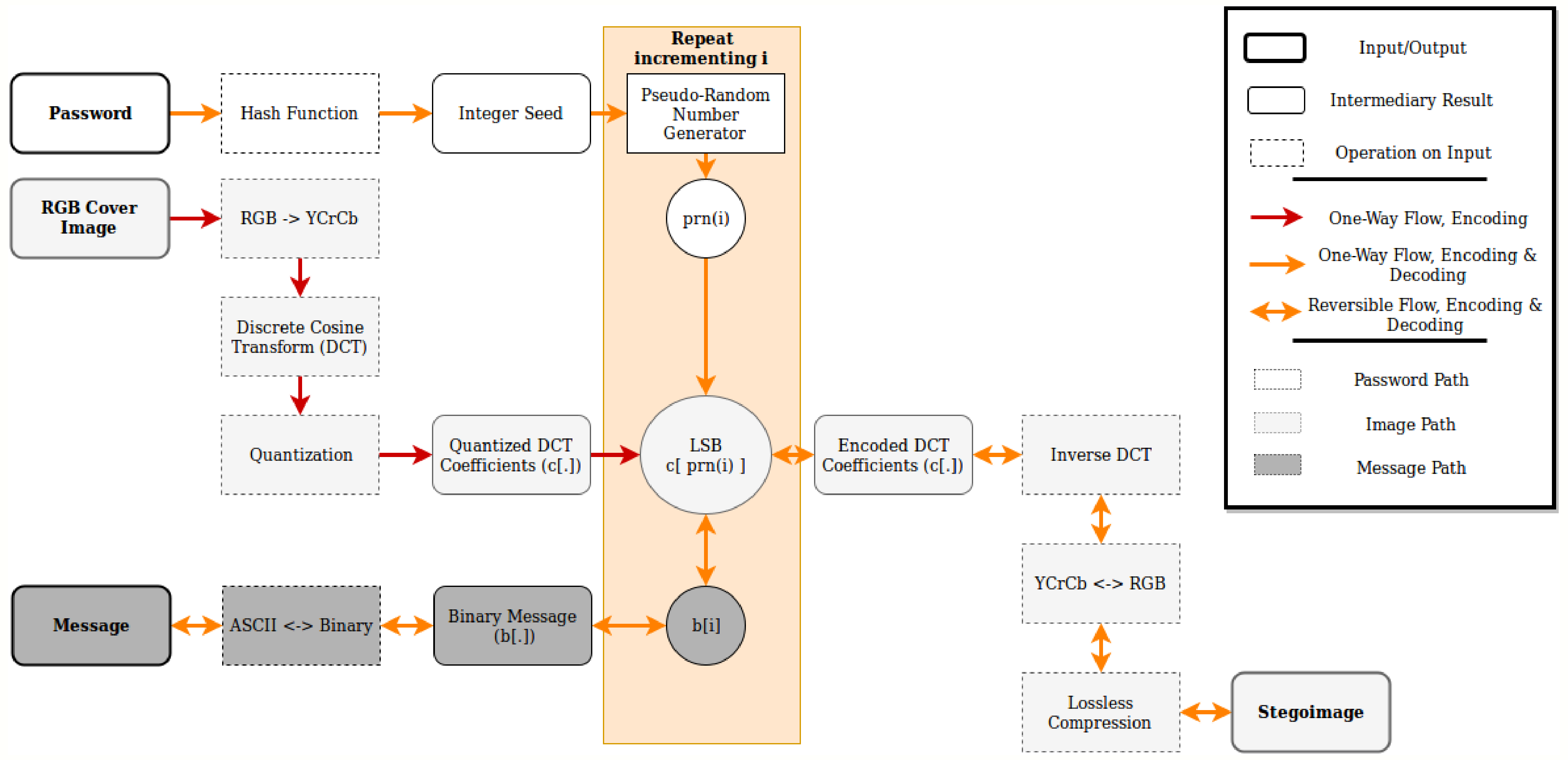

Fig. 1. Block Diagram of Outguess Encoding and Decoding

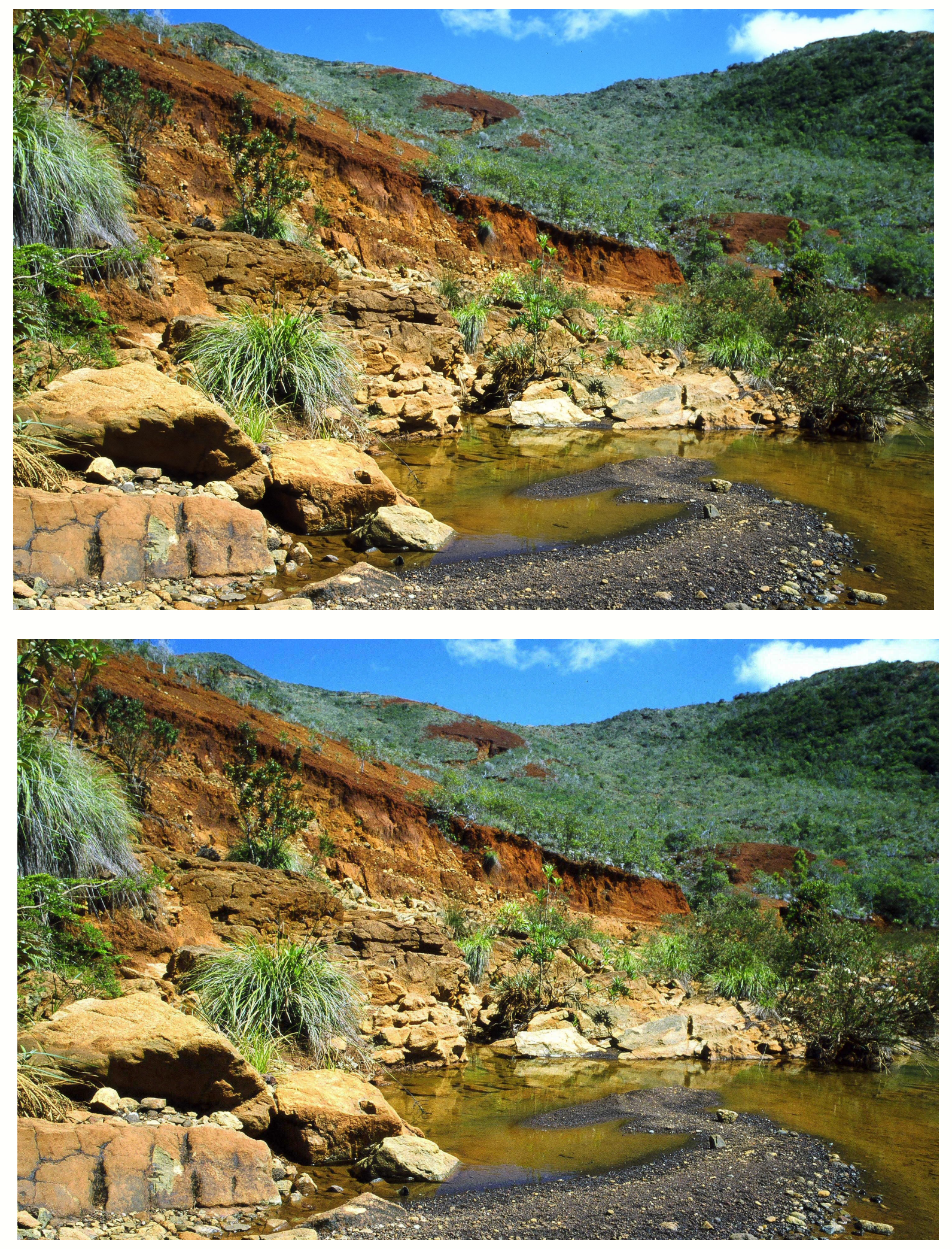

Fig. 2. Top: Cover Image (credit Bananaflo). Bottom: Stegoimage with Mary Shelley's Frankenstein.

Steganalysis

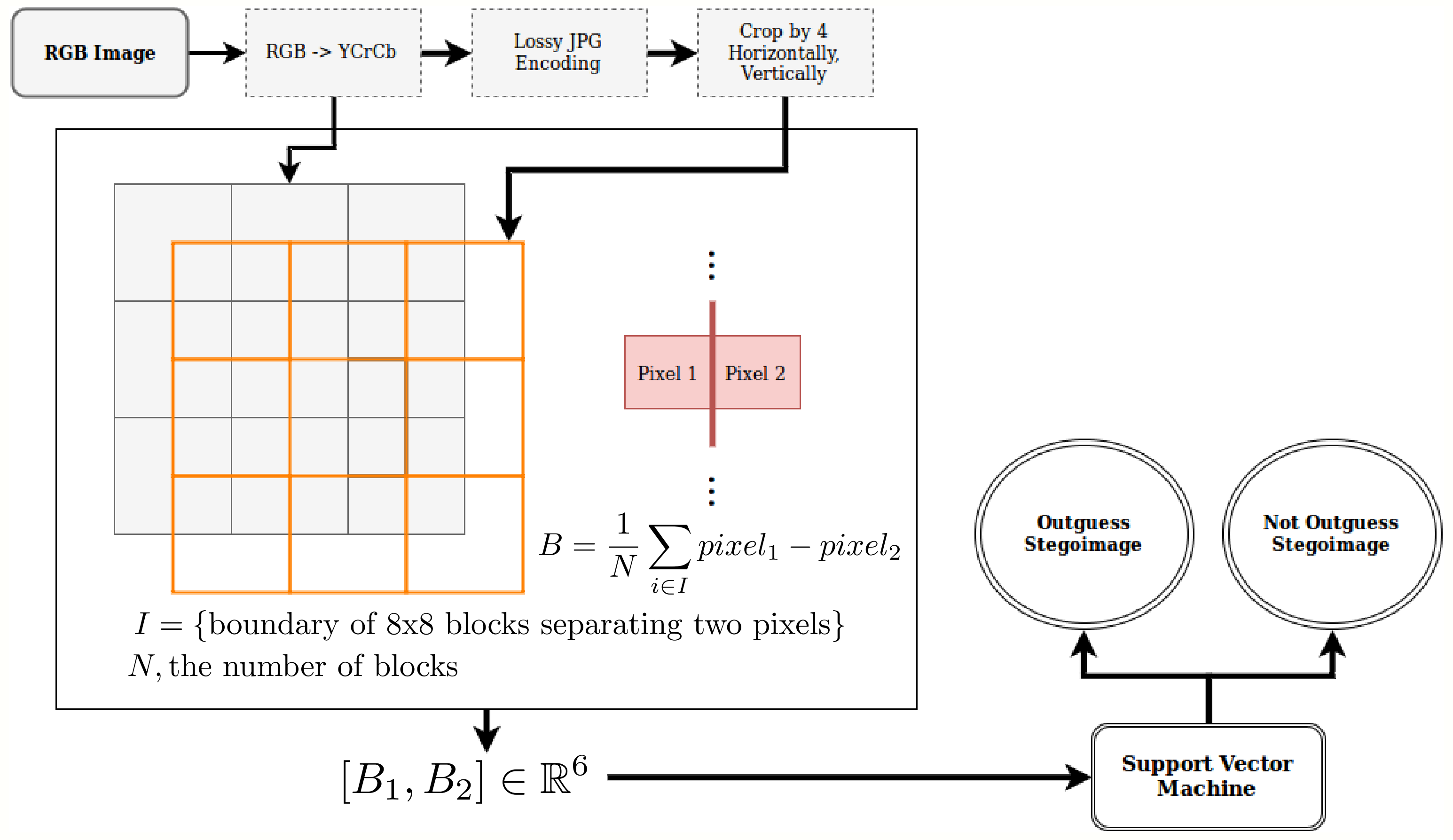
RGB Image
RGB -> YCrCb
Lossy JPG Encoding
Crop by 4 Horizontally, Vertically
Pixel 1
Pixel 2
$B = \frac{1}{N} \sum_{i \in I} pixel_1 - pixel_2$
$I = \{\text{boundary of 8x8 blocks separating two pixels}\}$
N, the number of blocks
$[B_1, B_2] \in \mathbb{R}^6$
Support Vector Machine
Outguess Stegoimage
Not Outguess Stegoimage

Fig. 3. Block Diagram of Outguess Steganalysis

SVM Training

- *Generated training set* of 8572 images (~2kB – 2MB), half are stegoimages with random message lengths up to 256 characters.
- Using OpenCV's built-in cross-validation for hyperparameter tuning, a *radial basis function kernel* yielded best results (lowest false-negative rate for highest accuracy).
- Performed *non-parametric Bootstrap* to estimate upper bound of classification error.
- Fit logistic functions to accuracy vs. distance from the SVM boundary to obtain *steganalysis confidence*.
- **Accuracy: > 68.5% False Negative Rate < 16.3 %**