Android-Based Digital Image Steganography and Steganalysis

Dominique Piens (dpiens@stanford.edu), Nathan Staffa (staffa@stanford.edu)

Steganography is the discipline concerned with achieving confidential communication by hiding information in plain sight. Media for hiding this information include images, video, audio and markup languages (Papapanagiotou et al. 2005). Steganographic schemes typically exploit information redundancies which are not easily perceptible. Digital images tend to exhibit such redundancy, and thus are a popular medium for steganography. Throughout the years, many different methodologies have been proposed in the literature, of which steganographic schemes like F5, OutGuess or Yet Another Steganographic Scheme (YASS) are a sample. While some steganographic techniques operate in the primal domain, the majority of newer techniques utilize the frequency domain to conceal information. F5, OutGuess and YASS occupy this group, embedding the information to hide in the image's discrete cosine transform (DCT) coefficients and extending the range of encodable images to compressed JPEGs (Hamid et al. 2012). The inverse problem of detecting information hidden in plain sight, steganalysis, is similarly developed for digital images. For instance, Fridrich (2004) used linear discriminant analysis to achieve a detection accuracy upwards of 87% on stego-images encoded with OutGuess. Steganography has reached consumers with multiple options present in iOS and Android app stores. Typical app features are encoding and decoding of images with a private key. PixelKnot and SSE for example, use the F5 algorithm to hide text in images. However, one of the challenges of mobile platforms is limited memory and computation. The range of techniques from steganography and steganalysis that can be used reliably on mobile devices is restricted.

We will design Android software to encode and decode stego-images with OutGuess, and detect whether a digital image is a stego-image encoded with OutGuess. The decoding and encoding functions will be implemented with an emphasis on reliability in a mobile setting. Then, we will use machine learning techniques on the DCT of stego-images encoded with OutGuess to train a detector which will indicate a probability that an image is a stego-image. To our knowledge, this work would add two novel features to consumer mobile apps: an OutGuess encoder/decoder, and a stego-image detector.

REFERENCES

Fridrich, Jessica. "Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes." In *International Workshop on Information Hiding*, pp. 67-81. Springer Berlin Heidelberg, 2004.

Hamid, Nagham, Abid Yahya, R. Badlishah Ahmad, and Osamah M. Al-Qershi. "Image steganography techniques: an overview." *International Journal of Computer Science and Security (IJCSS)* 6, no. 3 (2012): 168-187.

Papapanagiotou, Konstantinos, Emmanouel Kellinis, Giannis F. Marias, and Panagiotis Georgiadis. "Alternatives for multimedia messaging system steganography." In *International Conference on Computational and Information Science*, pp. 589-596. Springer Berlin Heidelberg, 2005.