On The Limits of Steganography

R.J. Anderson, F.A.P. Petitcolas

IEEE Journal on Selected Areas in Communication
16:4, pp 474-481, May 1998
DOI: 10.1109/49.668971

Liam Fearnley

Summary

- Steganography – the art of obscuring the presence of a secret message.
- Steganography is a useful tool, but there are numerous theoretical and practical limitations placed on its utility, and no ‘gold standard’ analogous to the one-time pad for cryptography.

Appreciative Comment

- One of the threads that the paper picks up on and works with is the concept that steganography and compression are heavily interlinked fields.

Steganography and Compression

- Steganographic messages must, by definition, be hidden in redundant data.
  - If they weren't, they'd be perceptible, and not secret…
- Compression algorithms work by stripping out redundant data.
  - For instance, MPEG-3, which truncates masked noise, inaudible frequencies, etc.

Degradation

- In many ways, compression can be viewed as degradation of a file in a way that conserves space.
- The paper assesses the impact of attacks based on degradation – for instance, the introduction of imperceptible ‘jitter’ into audio files by deletion/duplication of samples.

Appreciative Comment

- The paper recognises the problems associated with embedding into purely redundant data (for example, the least significant digits of image pixels) and the weakness of these methods to DoS type attack, and then provides a rigorous theoretical treatment of the subject.

Critical Comment

- The paper does recognise that it is trivial to defeat more integrated, time-dependent steganographic systems by degradation imperceptible to the user.
- However, it mentions the possibility of overcoming these attacks by using a slightly more complex time-dependent system dependent on echoes detectable by statistical transform, without justifying how it resists this kind of attack.

Critical Comment

- "*This is a serious concern with copyright, that may subsist for a long time (typically 70 years after the author's death for text and 50 years for audio). Even where we are concerned only with the immediate future, the industry experience is that it is a "wrong idea that high technology serves as a barrier to piracy or copyright theft; one should never underestimate the technical capability of copyright thieves."* "

Open Question

- The paper discusses the need to have systems that will last in timeframes of the order of 70+ years. Is it reasonable to assume that any system which has a significant weakness to standard compression algorithms will last that long? How can you model this kind of vulnerability?