Steganography for Radio Amateurs— A DSSS Based Approach for Slow Scan Television

Andreas Westfeld*

Technische Universität Dresden
Institute for System Architecture
01062 Dresden, Germany
mailto:dl1dsx@inf.tu-dresden.de

Abstract. In 2005, Germany introduced a new Amateur Radio Ordinance prohibiting encrypted radio traffic at home. Crypto-bans can be circumvented using steganography. However, present steganographic methods are not eligible because the embedded message will not survive the usual distortions in a radio transmission. Robust as current watermarking methods are, they leave clearly detectable traces and have a smaller capacity.

This paper presents measures that improve the robustness of steganographic communication with respect to non-intentional, random channel errors and validates their effectiveness by simulation. For the scenario of a radio communication, we determine practicable parameters for least detectability under six different short wave conditions. The resulting method embeds messages with a length of up to 118 bytes in a narrow-band Slow Scan Television connection in Martin-M1 mode.

1 Requirements for Robust Steganography

Steganography is the art and science of invisible communication. Its aim is the transmission of information embedded invisibly into carrier data. Secure watermarking methods embed short messages protected against modifying attackers (robustness, watermarking security) while the existence of steganographically embedded information cannot be proven by a third party (indiscernibility, steganographic security).

The existence of steganographic methods is one of the main arguments against a crypto-ban, since steganography facilitates the confidential exchange of information like cryptography, but goes unnoticed and consequently cannot be effectively persecuted. Nevertheless, Germany expanded the regulation that international amateur communications should be "in plain language" [1] to domestic ones in its Amateur Radio Ordinance in 1998. The new German Amateur Radio Ordinance from 2005 [2] explicitly prohibits encrypted amateur communications

* DL1DSX

J. Camenisch et al. (Eds.): IH 2006, LNCS 4437, pp. 201–215, 2007.

in the operational framework: (§ 16) Amateur radio communication must not be encrypted to obscure the meaning thereof.[1]

In general, steganographic communication uses an error-free channel and messages are received unmodified. Digitised images reach the recipient virtually without errors when sent, e. g., as an e-mail attachment. The data link layer ensures a safe, i. e. mostly error-free, transmission. If every bit of the carrier medium is received straight from the source, then the recipient can extract a possibly embedded message without any problem. However, some modes (e. g., analogue voice radio, television) do without the data link layer, because the emerging errors have little influence on the quality and can be tolerated.

Without error correction, distortions are acceptable only in irrelevant places where they have the least influence on the carrier. However, typical steganographic methods prefer these locations for hiding payload. The hidden message would be most interfered with in error-prone channels. Therefore, robust embedding functions have to add redundancy and change only locations that are carefully selected regarding the proportion between unobtrusiveness and probability of error. This increases the risk of detection and permits a small payload only.

This paper presents measures that improve steganography in terms of robustness with respect to non-intentional, random channel errors as they occur in radio communications. Some watermarking methods are also robust against distortions in the time and frequency domains. Tachibana et al. introduced an algorithm that embeds a watermark by changing the power difference between the consecutive DFT frames [3]. It embeds 64 bits in a 30-second music sample. Compared to the proposed steganographic method this is a quarter of the payload in a host signal (carrier) occupying 50 times the bandwith. It is robust against radio transmission. However, it was not designed to be steganographically secure and the presence of a watermark is likely to be detected by calculating the statistics of the power difference without knowing the pseudo random pattern. Van der Veen et al. published an audio watermarking technology that survives air transmission on an acoustical path and many other robustness tests while being perceptionally transparent [4]. The algorithm of Kirovski and Malvar [5] embeds about 1 bit per second (half as much as the one in [3]) and is even more robust (against the Stirmark Benchmark [6]). In brief, there are watermarking methods that survive radio transmission, offer small capacities and achieve perceptual transparency, however, they are not steganographically secure.

Marvel et al. [7] developed a robust steganographic method for images based on spread spectrum modulation [8]. This technique enables the transmission of information below the noise or carrier signal level (signal to noise ratio below 0 dB). Likewise it is difficult to jam, as long as transmitter and receiver are synchronised. Therefore, successful attacks de-synchronise the modulated signal [9]. Messages embedded using the algorithm of Marvel et al. will not survive the time and frequency dispersion of the channel considered here.

[1] "Amateurfunkverkehr darf nicht zur Verschleierung des Inhalts verschlüsselt werden; ...".