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; ...".

Since it is almost impossible for an attacker to control the distortions in the time and frequency domains that a radio communication is exposed to we can allow for the additional requirement of steganography (undetectability) without restricting the typical capacity of watermarking.

The following Section 2 describes the model and simulation of high frequency (HF) propagation. Section 3 extends a known steganographic spread spectrum method stepwise by modules that decrease the error rate of the steganographic signal for radio communications. Sensible parameters are determined by simulation, which allow an error-free transmission. Some security concepts are discussed in Section 4, where the paper is also summarised.

2 HF Channel Simulation

Simulating the variable behaviour of the ionosphere not only allows faster bench testing in the lab during the development stage, but also the comparison under reproducible, standardised conditions. In this research a software implementation was employed, based on source codes of Johan Forrer, KC7WW[2]. We implemented it as an R package [10] named `chansim` that accommodates a wide range of simulated conditions, including those given in the Recommendation 520-1 of the CCIR[3] (good, moderate, poor, flutter-fading, see Table 1) [11]. The simulation model is an implementation of the Watterson Gaussian-scatter HF ionospheric channel model [12], which is the de facto standard for this kind of work [13].

Table 1. Preset parameters for channel simulation

HF channel condition	Delay time	Doppler spread
Noise	0 ms	0 Hz
Flat 1	0 ms	0.2 Hz
Flat 2	0 ms	1 Hz
CCIR good	0.5 ms	0.1 Hz
CCIR moderate	1 ms	0.5 Hz
CCIR poor	2 ms	1 Hz
CCIR flutter fading	0.5 ms	10 Hz
Extreme	2 ms	5 Hz

From a physical point of view, the HF channel is characterised as a multi-path time-varying environment that produces time and frequency dispersion [14]. The reason for the multitude of paths lies in the reflections of radio signals from

[2] These alphanumeric strings behind names are call signs of radio amateurs.

[3] Comité consultatif international pour la radio, which became the ITU-R (Radiocommunication Sector of the International Telecommunication Union) in 1992.

different layers in the ionosphere. In addition, multiple reflections can occur between the earth's surface and the ionosphere, giving rise to multi-hop propagation. Thus, the received signal can contain several echoes, separated in time by a matter of milliseconds (delay time). Doppler spread (frequency spread) occurs if the particular path lengths change due to a movement of the ionosphere with its specular nature.

For mid-latitude HF circuits, the amount of multi-path (delay time τ_i) can range up to 6 ms and the fading rate (Doppler spread) can be as high as 5 Hz [15]. However, more typical values are 2 ms and 1 Hz, respectively, which are the basic parameters of the standardised CCIR "poor" HF channel.

One of the key contributions to HF channel modelling was a paper by Watterson et al. [12] in 1970. In this paper, a stationary model for the HF channel was proposed and experimentally validated with on-air measurements. Although HF channels are generally non-stationary, this model has been shown to be valid for sufficiently short times ($\approx$ 10 minutes) and for band-limited channels ($\approx$ 10 kHz). The Watterson Model views the HF channel as a transversal filter where the taps are complex and vary with time (see Figure 1). It produces phase and amplitude distortions in the signal.

The time-varying taps (h_i) are generated by filtering complex white Gaussian noise through filters whose frequency-domain power spectra have a Gaussian shape. The desired Doppler spread is controlled by the standard deviation of these power spectra.

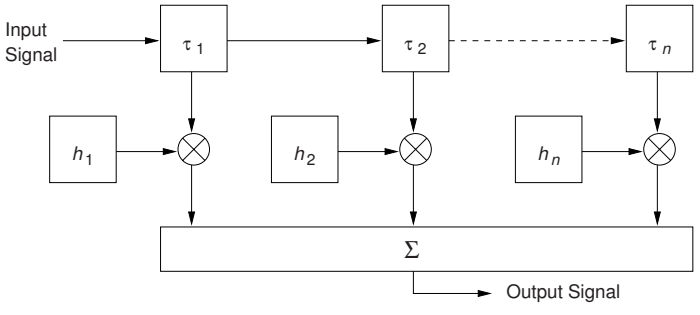

Fig. 1. Watterson HF channel model [12]

3 Design of the System

3.1 Slow Scan Television

Slow Scan Television (SSTV) has a relatively long transmission phase compared with voice radio. This increases the chance of a reasonable steganographic capacity despite the small bandwith of 3 kHz. SSTV is widespread among radio amateurs.

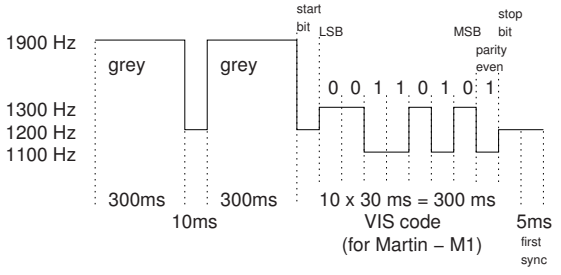

Fig. 2. VIS code to signal SSTV mode and start of an image[16]

An SSTV signal starts with a VIS[4] code that announces an image transmission and its mode. Its time–frequency diagram is shown in Figure 2. There exist about 30 different SSTV modes. Martin-M1 was developed by Martin H. Emmerson, G3OQD, and is one of the most commonly used.

The Martin-M1 mode encodes colour images with a resolution of 320×256 pixels. The image is sent row by row from top to bottom. For each row there is a synchronisation impulse followed by the intensity information for the green, blue, and red colour channel. These intensities are encoded as tones with frequencies in the range of $1400 \ldots 2400$ Hz (see Figure 3). A 1200 Hz tone serves as sync pulse. Altogether the SSTV signal lasts 1 minute and 55 seconds, possibly extended by the call sign of the sender in CW[5] (Morse code).

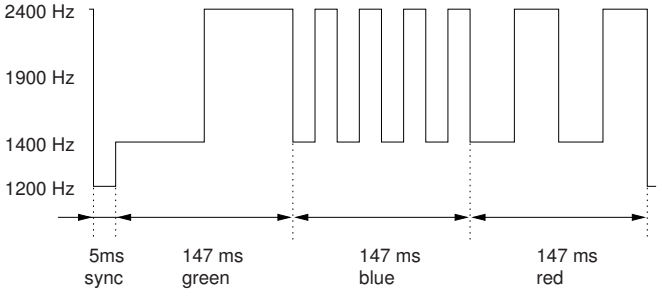

Fig. 3. One of 256 rows in Martin-M1 mode

We selected QSSTV [17] by Johan Maes, ON4QZ, as the most suitable open source SSTV software to base the implementation of our steganographic system on. Since most of the SSTV programs are closed source or obsolete implementations, there are no real alternatives.

[4] This name is inherited from weather fax: VIS=visible, IR=infrared.
[5] continuous wave.

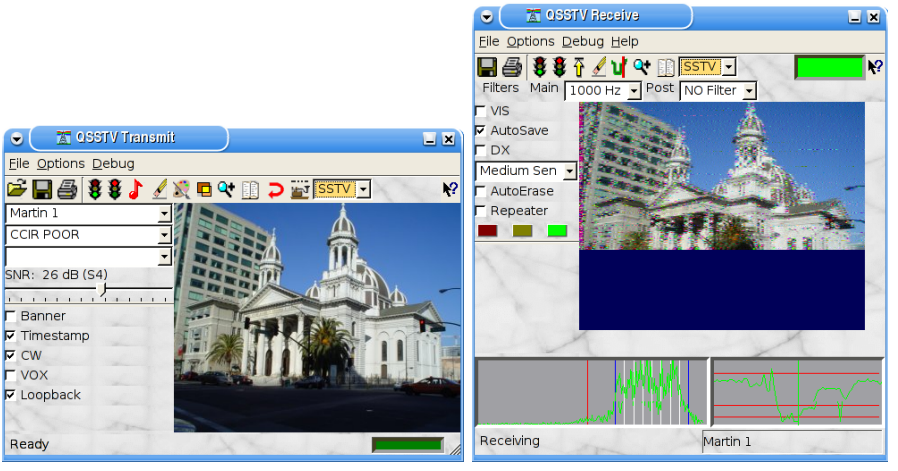

Fig. 4. Modified QSSTV with loopback HF channel simulator

We extended QSSTV with the already mentioned channel simulator by Johan Forrer, KC7WW. Figure 4 shows the graphical user interface with extra loopback option and settings for SNR (signal to noise ratio) and HF conditions. A simulated transmission lasts only a few seconds and is much faster than the 2 minutes for a real transmission. The Receive window in the figure is reconstructing the image from a simulated signal transmission (CCIR poor, SNR 26 dB).

The SSTV signal generated by QSSTV has a sampling rate of 8000 samples per second, offering sufficient resolution for the transmitted signal range 200 . . . 3000 Hz.

3.2 Steganographic SSTV System

This section describes the overall steganographic SSTV system (see Figure 5). Its components have three main goals: embedding, phase correction, and error correction.

First the message is made fault-tolerant by an error correcting code (ECC). The redundancy is added to compensate for the loss due to fading and atmospherics that cannot be prevented otherwise. However, an opponent cannot search for this redundancy because it is masked by the key derived spreading sequence, which acts like a stream cipher. The interleaver, which permutes the encoded message, prevents burst errors. The differential encoder enables a correct demodulation also for signals received with the wrong sign due to phase distortion. The resulting symbols are spread and their energy is distributed over a longer period of time. Pulse shaping with an RRC filter (root raised cosine) limits the bandwith of the spread signal, which is added with relatively low level to the SSTV signal ($-27 \ldots -11$ dB) and therefore difficult to detect. The sum of both signals is transmitted to the receiver. In our experimental environment the conditions of the HF channel are simulated in a reproducible way. For real use,

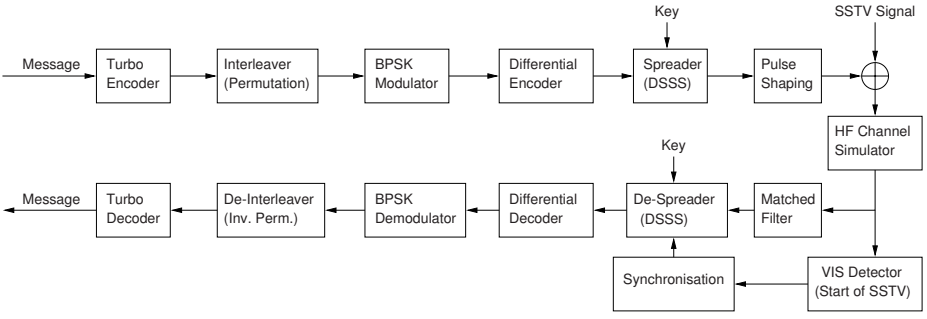

Fig. 5. Path of the steganographic signal in the steganographic SSTV system

the signal with its 8000 samples per second would be converted into an analogue audio signal by the sound card of the computer and then broadcast with an single side band (SSB) HF transmitter. The short-wave receiver of the remote station is connected to another sound card of a computer, which digitises the analogue signal and processes it further. The digitised signal can also be tapped from the output of the channel simulator of the experimental environment. It is an ordinary SSTV signal and therefore the image content can be demodulated as usual. The synchronisation information of the SSTV signal guarantees that the receiver also recognises the start of the steganographic signal. Before the steganographic signal is demodulated at the receiver side, a matched RRC filter must be applied to reduce the interference between the elements of the spreading sequence (chips). The de-spreader retrieves the energy of the particular binary symbols from the steganographic signal. It needs the same key that was used by the sender. The differential decoding corrects the signal in times when the signal was inverted due to phase distortions, and the de-interleaver coupled with the turbo decoder tries to correct the remaining errors in the signal. This allows the level of the received symbols act as a measure of reliability (soft decision decoding, see Section 3.7).

3.3 Pure Direct Sequence Spread Spectrum (DSSS)

DSSS converts the message to embed m into an embedding sequence $s = mn$ by multiplication with a spreading sequence n (see Figure 6). We use a long spreading sequence n, which is pseudo-randomly derived from the key. The elements of the spreading sequence are called *chips* and have a duration T_c. The symbol duration T_s is a multiple of T_c. The embedding sequence s is scaled by a gain factor g (modulation degree) before it is added to the carrier signal c, resulting in the steganogram $c_\mathrm{s} = c + gs$. The receiver extracts the message from the distorted signal c'_s by integrating $c'_\mathrm{s} n$ piecewise over the symbol duration T_s.[6]

[6] Figure 6 is simplified for clarity and the extraction is based on the distorted embedding sequence.

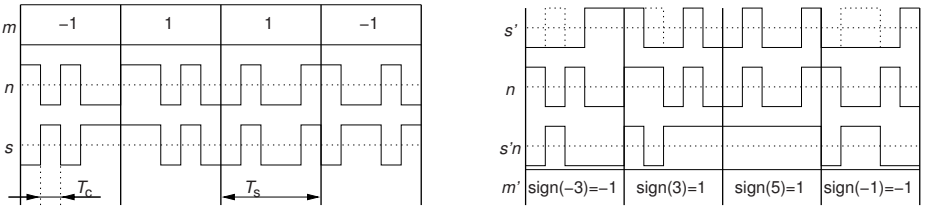

Fig. 6. DSSS modulation (left) and demodulation after distortion (right)

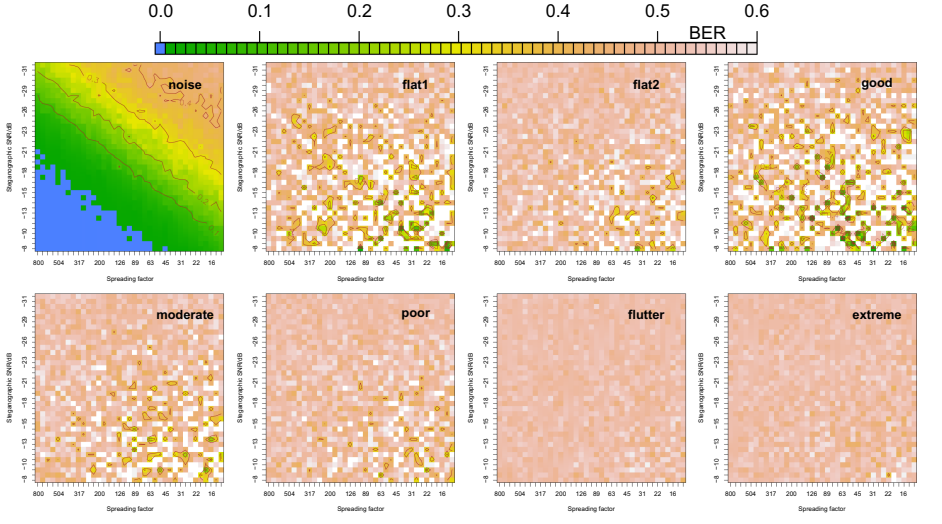

Fig. 7. Direct sequence spread spectrum (DSSS)

In the following first experiment, we tried different spreading factors with several steganographic SNR's and measured the resulting bit error rates (BER). This experiment was repeated for the eight HF conditions defined by the parameters of Table 1. Figure 7 shows the BER as a physical map. It plots the (logarithmically falling) spreading factor on one axis and the steganographic noise ratio (in decibel) on the other axis. The largest capacity is rightmost and the lowest detectability is upmost in the diagrams. Error-dominated regions (BER $\approx 50\,\%$) are white, high error rates are brown, low error rates are green, and error-free areas are plotted in blue.

As expected, pure DSSS survives only the additive white Gaussian noise (AWGN) channel [7] (HF condition "noise"), which is a rather unlikely condition for a short wave transmission. The channel's SNR was set to 26 dB (S4). All other simulated conditions produce BERs around the mean 0.5 with varying standard deviations. This is due to the phase shift caused by a fading multi-path channel.

3.4 Differential Encoding of the Secret Message

The transmitted signal is complexly distorted, i. e., its phase is moving and its amplitude is Rayleigh distributed [18]. Since the radio amateur technology only receives the real part of the signal and therefore is not able to estimate the phase difference, the channel cannot be equalised. We use binary phase shift keying (BPSK), because other modulations like quadrature phase shift keying (QPSK) and quadrature amplitude modulation (n-QAM) assume a complex signal. The phase can adopt arbitrary values from 0 to 360°. This results in a bit error rate around 0.5. However, the relative change of the phase per symbol is small. The key to a successful transmission over a channel with (slowly) changing phase displacement is differential demodulation [19]. Figure 8 shows the demodulated sequence of 4000 impulses, which have been transmitted under "CCIR poor" conditions (correct reception has positive sign, erroneous reception negative sign). The grey curve represents the analogue signal intensity, the black one its sign.

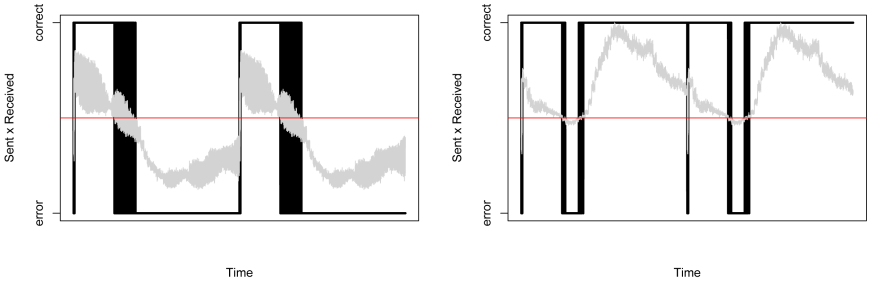

Fig. 8. Burst errors due to phase distortion (left) and improvement by differential demodulation (right)

One can convert the constantly wrong passages into a correct signal by differential encoding. This encoding ensures that the signal is not independently interpreted at a certain point in time, but based on its predecessor. Hence, the decoded signal is correct apart from the samples at destructive interference. A sequence of Boolean values $\boldsymbol{a}$ (*true* encoded as -1 and *false* as 1) is converted into a differential encoded sequence $\boldsymbol{b}$ and decoded again by the following rules:

$$b_k = \prod_{i=1}^{k} a_i = \begin{cases} k = 1\colon a_1 \\ k > 1\colon a_k \cdot b_{k-1} \end{cases} \qquad a_k = \begin{cases} k = 1\colon b_1 \\ k > 1\colon b_k \cdot b_{k-1} \end{cases}$$

Differential encoding results in a significantly lower error rate for all conditions with Doppler spread (see Figure 9). Only in the pure AWGN channel it increases the BER, because single errors have double effect after decoding. Error-free areas are not affected by differential encoding.

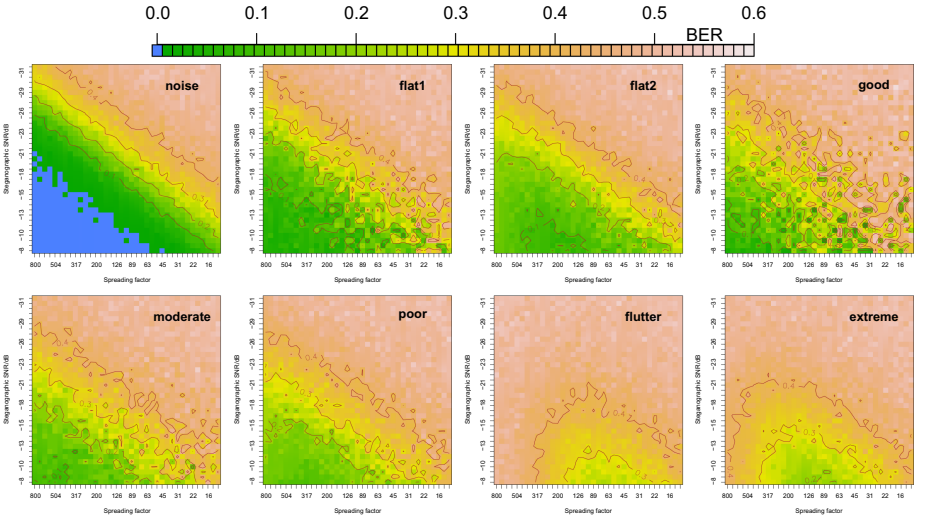

Fig. 9. Direct sequence spread spectrum (DSSS) with differential encoding

3.5 Error-Correcting Code for the Secret Message

To correct the loss due to fading, an error-correcting code (ECC) is used, which is based on an implementation of turbo codes for an OFDM sound modem (orthogonal frequency division multiplexing) [20]. This implementation permits code rates[7] in the range $\frac{1}{3} \ldots 1$. In the following experiments we worked with the smallest possible code rate of $\frac{1}{3}$. Unfortunately, no configuration was found that results in an error-free transmission for the conditions "flutter" and "extreme." One could try to reduce the code rate, however, most SSTV systems cannot even decode the image under such extreme conditions.

We estimated useful parameters for the least detectability from Figure 10. Table 2 shows parameters with best steganographic SNR for simulations that faultlessly transmitted three consecutive messages at the first go. These parameters are dependent on the channel conditions. Sensible parameters will be derived in measurements over the air that are currently prepared. The transmission with parameters off the table under a specific condition works the more reliably the less indented the northern shoreline of the error-free lake in the respective landscape appears. The steganographic SNR in the table is determined based on the undistorted signal, to which the attacker has no access.

We can see that the lowest error rate is not always expected for the largest spreading factor. The reason for this is the increased probability for a change of sign due to phase distortion in longer symbols. On the other hand, the gain from de-spreading is diminishing with shorter sequences (smaller spreading factors) and thus the interference between the embedded and the carrier signal is increasing.

[7] Ratio of the number of information bits to the number of bits in the code word.

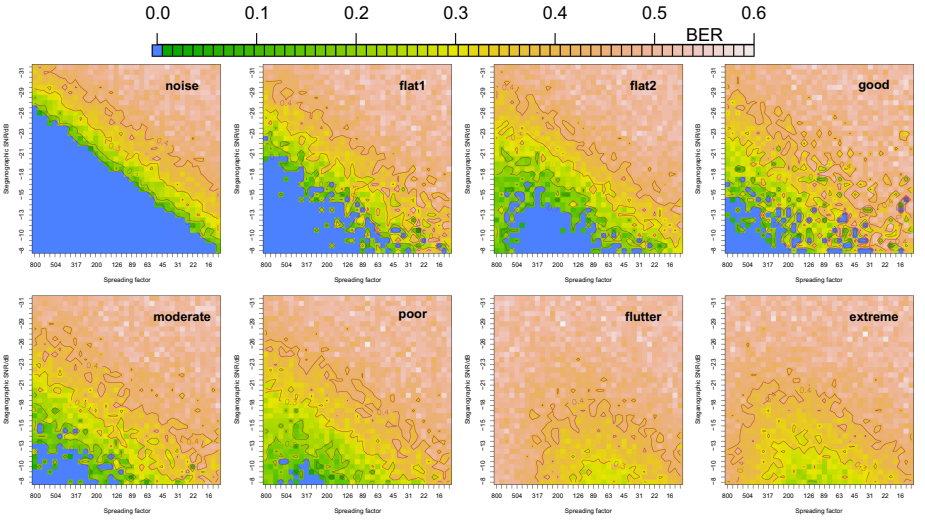

Fig. 10. Direct sequence spread spectrum (DSSS) with differential encoding and turbo code

3.6 Sender-Side Pulse Shaping and Matched Receive Filter

The spreading sequence consists of a sequence of square pulses with vertical transitions that occupy infinite bandwith. The Nyquist Criterion tells us that we cannot transmit square pulse shapes over a bandlimited channel [21]. An SSTV signal is limited to the frequency range 200 Hz ... 3000 Hz. To reduce the loss, the signal is formed and restricted to the required spectrum by a pulse shaping root raised cosine (RRC) filter [22]. The impulse response $g(t)$ of the filter is defined as follows:

$$g(t) = \frac{4\alpha}{\pi\sqrt{T_\mathrm{c}}} \frac{\cos\left(\frac{(1+\alpha)\pi t}{T_\mathrm{c}}\right) + \frac{T_\mathrm{c}}{4\alpha t}\sin\left(\frac{(1-\alpha)\pi t}{T_\mathrm{c}}\right)}{1 - \left(\frac{4\alpha t}{T_\mathrm{c}}\right)^2}$$

$$\lim_{t\to 0} g(t) = \frac{4\alpha + \pi(1-\alpha)}{\pi\sqrt{T_\mathrm{c}}}$$

The RRC has a parameter $\alpha = 2f_\mathrm{u}T_\mathrm{c} - 1$ called roll-off factor. This can shift the upper cutoff frequency f_u for the chip duration T_c in certain limits. Since the amplitude of the RRC is decreasing on both sides it can be truncated below a certain threshold ε and limited to a finite duration.

The spectrum for an RRC filter (roll-off factor $\alpha = \frac{1}{2}$, chip duration $T_\mathrm{c} = 2$ sample points, 8000 Hz sampling rate) is shown in Figure 11 (left). The filter forms the signal before transmission and its upper cutoff frequency $f_\mathrm{u} = 3000$ Hz adopts the signal bandwith to the channel.

Table 2. Parameters for SSTV steganography with least detectability

HF channel condition	Spreading factor	Steganographic SNR	Capacity
Noise	800	−27 dB	46 bytes
Flat 1	800	−21 dB	46 bytes
Flat 2	320	−16 dB	118 bytes
CCIR good	640	−15 dB	58 bytes
CCIR moderate	450	−13 dB	83 bytes
CCIR poor	320	−11 dB	118 bytes
CCIR flutter fading	—	—	0
Extreme	—	—	0

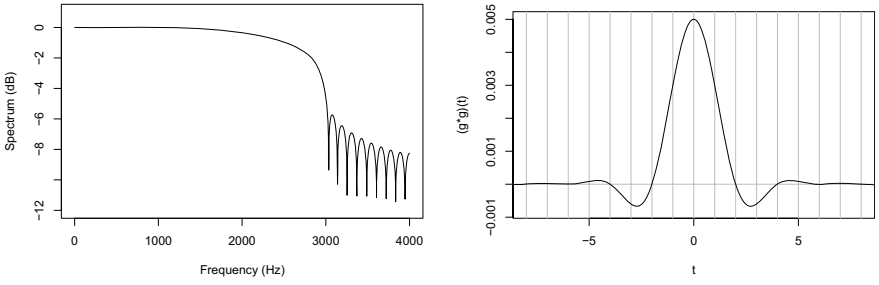

Fig. 11. Spectrum of a truncated RRC filter with $\alpha = \frac{1}{2}$ und $T_c = 2$ (left) and impulse response of a matched pair of RRC filters (right)

To fulfil the first Nyquist condition (zero inter-symbol interference), T_c has to be the first root of the filter's impulse response. At the same time, the signal to noise ratio has to be maximised, which requires identical (matched) send and receive filters for real signals. The combination of two root raised cosine filters forms a raised cosine filter, which complies with this first Nyquist condition. Figure 11 (right) shows that for nonzero integers k the impulse response of the combination fulfils $(g * g)(kT_c) = 0$. Consequently the signal does not interfere with neighbour chips at their sample points.

3.7 Soft Decision Decoding

Figure 12 shows the gain of pulse shaping (middle) compared with the modulation of square pulse shapes (left). We noticed a small increase from 18 to 22 error-free transmissions under CCIR poor conditions in our experiments. If not only the sign is considered in the decoding (=hard decision), but also the level of the received signal as a measure for its reliability (=soft decision), the number of error-free transmissions slightly increases again from 22 to 27.

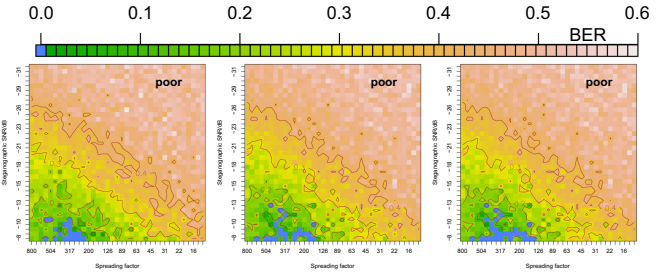

Fig. 12. Direct sequence spread spectrum (DSSS) with differential encoding and turbo code under CCIR-poor HF conditions with hard decision decoding (left), plus pulse shaping and matched filter (middle), and soft decision decoding (right)

4 Security Considerations and Conclusion

The simulations have shown that narrow-band radio links, as they are used by radio amateurs on short wave, can be used for the transmission of spread spectrum modulated embedded messages despite dynamic phase and frequency distortions on the channel. The physical limits of this scenario have been determined experimentally. Some ten thousand simulated radio communications have been compared to each other with different values for the parameters steganographic SNR and capacity under reproducible, standardised propagation conditions and in different system increments.

An attacker is facing the task to prove the existence of a steganographic message, i. e., to distinguish between messages with and without steganographic content. This distinction has to be made on the basis of the steganographic noise, which is either present or not. This noise ought to be separated from other available sources of noise: the noise that is already in the carrier-pattern, the noise of the transmitter, the ambient atmospheric noise, and the channel noise, i. e., the distortions, which the signal is exposed to on its way to the receiver.

An attacker can improve his or her situation by choosing a favourable geographical position, a more sensitive receiver, or an antenna with increased gain and a better directional receiving pattern. To decide the question of security we have to see if the advantage of the recipient, who knows the secret key used to spread the symbol energy over a longer period of time, is sufficient to protect from attackers under possibly better physical circumstances, who have to do without this knowledge. As the measurements have shown (cf. Section 3.5), there is an optimum for the spreading factor. This means that we cannot automatically decrease the capacity in favour of the steganographic SNR (by means of a larger spreading factor). The key advantage of using SSTV is its saving effect by providing synchronisation pulses. There is no need to add redundancy to the steganographic signal in order to synchronise sender and receiver. The existing synchronisation pulses are sufficient for this purpose. The time before

the first row synchronisation pulse and after the end of the embedded message should be used for a smooth fade of the steganographic noise level since abrupt changes can be detected more easily.

One could try to derive a steganalytic method from the Twin Peaks attack on digital watermarks [23]. This attack relies on the duplication of peaks in the histogram when a spreading sequence $\{-d, +d\}^n$ is added. The success of this attack very much depends on the particular image, because the effect only appears in histograms with distinct peaks. In the SSTV scenario, an attacker cannot access the undistorted steganogram. We cannot preclude peaks in the histogram of SSTV signals, though they are polished on their way to the receiver. As the SSTV signal interferes with the steganographic signal, the attack becomes more difficult and therefore pure spreading sequences with exactly two peaks at $-d$ and d have been analysed. After a simulated transmission, the distribution was—apart from the AWGN channel—always unimodal. A transmission with line of sight is similar to an AWGN channel but is still subject to fading (Rice fading) [18]. To what extent a line of sight attack is successful has to be researched in practice.

The security of the proposed system is hard to compare since robust steganography for radio links is a new territory and the absence of attacks impedes benchmarking the security within the simulation environment. The validation of the simulated results in practice is subject to future research.

Acknowledgements

The author is grateful to Oliver Prätor for beneficial impulses and fruitful discussions as well as to the anonymous reviewers for their comments. The work on this paper was supported by the Air Force Office of Scientific Research, Air Force Material Command, USAF, under the research grant number FA8655-04-1-3036. The U. S. Government is authorised to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation there on.

References

1. International Telephone and Telegraph Consultative Committee (CCITT): Implementing order for the radio regulations (German designation: VO Funk) (1982)
2. German Federal Ministry of Economics and Labour: Ordinance concerning the Amateur Radio Act (German designation: AFuV) (2005) Online available at `http://bundesrecht.juris.de/bundesrecht/afuv_2005/gesamt.pdf`
3. Tachibana, R., Shimizu, S., Nakamura, T., Kobayashi, S.: An audio watermarking method robust against time- and frequency-fluctuation. In: Delp, E.J., Wong, P.W. (eds.) Security, Steganography and Watermarking of Multimedia Contents III (Proc. of SPIE), pp. 104–115. San Jose, CA (2001)
4. van der Veen, M., Bruekers, F., Haitsma, J., Klaker, T., Lemma, A.N., Oomen, W.: Robust multi-functional and high-quality audio watermarking technology. In: 110th Audio Engineering Society Convention. Volume Convention Paper 5345 (2001)

5. Kirovski, D., Malvar, H.S.: Spread-spectrum watermarking of audio signals. IEEE Trans. on Signal Processing 51, 1020–1033 (2003)
6. Steinebach, M., Petitcolas, F., Raynal, F., Dittmann, J., Fontaine, C., Seibel, S., Fates, N., Ferri, L.: StirMark benchmark: audio watermarking attacks. In: International Conference on Information Technology: Coding and Computing, pp.49–54 (2001)
7. Marvel, L.M., Boncelet, C.G., Retter, C.T.: Spread spectrum image steganography. IEEE Transactions on Image Processing 8, 1075–1083 (1999)
8. Pickholtz, R.L., Schilling, D.L., Milstein, L.B.: Theory of spread-spectrum communications—a tutorial. IEEE Transactions on Communications 30, 855–884 (1982)
9. Petitcolas, F.A.P., Anderson, R.J., Kuhn, M.G.: Attacks on copyright marking systems. In: Aucsmith, D. (ed.) IH 1998. LNCS, vol. 1525, pp. 219–239. Springer, Heidelberg (1998)
10. R Development Core Team: R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria (2005) ISBN 3-900051-07-0. Online available at `http://www.R-project.org`
11. CCIR: Recommendation 520-1, Use of high frequency ionospheric channel simulators. Recommendations of the CCIR III, pp. 57–58 (1990)
12. Watterson, C.C., Juroshek, J.R., Bensema, W.D.: Experimental confirmation of an HF channel model. IEEE Transactions on Communication Technology 18, 792–803 (1970)
13. Forrer, J.B.: A low-cost HF channel simulator for testing and evaluating HF digital systems. In: Proceedings of the 18th ARRL and TAPR. Digital Communications Conference, Phoenix, Arizona (1999) `http://www.tapr.org/pub_dcc18.html`
14. Eleftheriou, E., Falconer, D.D.: Adaptive equalization techniques for HF channels. IEEE Journal on Selected Areas in Communications 5, 238–247 (1987)
15. Furman, W.N., Nieto, J.W.: Understanding HF channel simulator requirements in order to reduce HF modem performance measurement variability. In: Proceedings of HF01, the Nordic HF Conference, Fårö, Sweden (2001) Online available at `http://www.nordichf.org/index.htm?forms/cdrom.htm\&2`
16. Wumpus: Einige SSTV-Modi (1997) Online available at `http://home.snafu.de/wumpus/sstvmod.htm`
17. Maes, J.: QSSTV (2005) Online available at `http://users.telenet.be/on4qz/qsstv/`
18. Rappaport, T.S.: Wireless Communications: Principles and Practice. IEEE Press, Piscataway, NJ, USA (1996)
19. Couch II, L.W.: Digital and Analog Communication Systems. Prentice Hall, Upper Saddle River, NJ (2001)
20. Walma, M.: BCJR turbo code encoder/decoder (1998) Online available at `http://cvs.berlios.de/cgi-bin/viewcvs.cgi/ofdm/soundmodem/newqpsk/turbo.c?rev=HEAD`
21. Saucedo, R., Schiring, E.E.: Introduction to Continuous and Digital Control Systems. Macmillan, New York (1968)
22. Lee, E.A., Messerschmitt, D.G.: Digital Communications. Kluwer Academic Publishers, Boston (1994)
23. Maes, M.: Twin Peaks: The histogram attack to fixed depth image watermarks. In: Aucsmith, D. (ed.) IH 1998. LNCS, vol. 1525, pp. 290–305. Springer, Heidelberg (1998)