

# Asymptotic Behavior of the ZZW Embedding Construction

Jessica Fridrich, *Member IEEE*

**Abstract**—We analyze asymptotic behavior of the embedding construction for steganography proposed by Zhang, Zhang, and Wang (ZZW) at 10th Information Hiding by deriving a closed-form expression for the limit between embedding efficiency of the ZZW construction and the theoretical upper bound as a function of relative payload. This result confirms the experimental observation made in the original publication.

## I. MOTIVATION AND BACKGROUND

Steganography deals with secret communication by hiding messages in innocuous-looking objects, such as digital images, by slightly modifying the colors of their pixels. The goal is to make the stego images, which carry secret messages, statistically indistinguishable from the original unmodified (cover) images [2]. Statistical detectability of most steganographic schemes increases with embedding distortion (see, e.g., [10]). This is why most stegosystems limit the amplitude of embedding changes to the smallest possible value. In this case, the distortion is often measured with the number of embedding changes. The average number of bits embedded per one embedding change is called embedding efficiency and it constitutes an important numerical characteristic of a steganographic scheme.

By mapping the individual pixels of the cover to elements of a finite field, for example, by associating a bit (or  $q$ -ary symbol from finite field  $\mathbb{F}_q$ ) with each pixel value<sup>1</sup>, one can formulate the problem of maximizing embedding efficiency within the framework of coding theory [3], [8]. In particular, it is known that a  $q$ -ary linear code  $\mathcal{C}$  with length  $n$ , dimension  $k$ , parity check matrix  $\mathbf{H}$ , and covering radius  $R$  can be used to communicate  $n - k$   $q$ -ary symbols (or  $(n - k) \lg q$  bits) in a cover consisting of  $n$  elements by making at most  $R$  changes in the following manner. Let  $\mathbf{x} \in \mathbb{F}_q^n$  be the vector of symbols assigned to  $n$  elements of the cover. Then,  $n - k$  message symbols,  $\mathbb{F}_q^{n-k}$ , can be embedded in  $\mathbf{x}$  by modifying the symbols of pixels to  $\mathbf{y} = \mathbf{x} + \mathbf{e}(\mathbf{m} - \mathbf{H}\mathbf{x})$ , where  $\mathbf{e}(\mathbf{s})$  is a coset leader of the coset corresponding to syndrome  $\mathbf{s}$ . The recipient can read the message from the stego object as its syndrome,  $\mathbf{m} = \mathbf{H}\mathbf{y}$ , because  $\mathbf{H}\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{m} - \mathbf{H}\mathbf{x}$ . The

average number of embedding changes of this scheme is equal to the average weight of a coset leader or the average distance to code defined as  $R_a = \frac{1}{q^n} \sum_{\mathbf{x} \in \mathbb{F}_q^n} d(\mathbf{x}, \mathcal{C})$ . Here,  $d(\mathbf{x}, \mathcal{C}) = \min_{\mathbf{c} \in \mathcal{C}} d(\mathbf{x}, \mathbf{c})$ , where  $d(\cdot, \cdot)$  is the Hamming distance. Thus, the embedding efficiency is  $e = \frac{n-k}{R_a} \lg q$ . As shown in [5], for a fixed relative message length,  $\alpha = \frac{n-k}{n} \lg q$ , the embedding efficiency is bounded from above by the rate-distortion bound

$$e(\alpha) \leq \frac{\alpha}{H_q^{-1}(\alpha)}, \quad (1)$$

where  $H_q^{-1}(x)$  is the inverse of the  $q$ -ary entropy function on  $[0, 1 - 1/q]$ ,  $H_q(x) = -x \lg x - (1-x) \lg(1-x) + x \lg(q-1)$ , where  $\lg$  is logarithm at the base 2. Alternatively, the bound can be stated in terms of the change rate  $\beta = R_a/n$ ,  $e \leq \frac{H_q(\beta)}{\beta}$ , because the largest relative payload that can be embedded using change rate  $\beta$  is  $H_q(\beta)$ . As a special case, we point out that the bound on embedding efficiency for ternary codes is by 1 larger than the bound for binary codes because  $\frac{H_3(\beta)}{\beta} = \frac{H_2(\beta)+\beta}{\beta} = \frac{H_2(\beta)}{\beta} + 1$ .

Various embedding methods were proposed based on both linear and non-linear codes (see, e.g., the references in [6]). Arguably, the simplest binary matrix embedding method uses binary Hamming codes,  $\mathcal{H}_l$ , with codimension  $l$ . Such codes can be used to embed  $n - k = l$  bits in  $n = 2^l - 1$  pixels by making on average  $R_a = 1 - 2^{-l}$  embedding changes, which corresponds to embedding efficiency  $\frac{l}{R_a} = \frac{l}{1-2^{-l}}$  at relative payload  $\frac{l}{n} = \frac{l}{2^l-1}$ . The recent construction proposed by Zhang et al. [11] (referred to as the ZZW construction in this paper) allows construction of new families of codes with very high embedding efficiency from existing codes. An interesting and important property of this construction is that the embedding efficiency of the new codes seem to follow the upper bound (1) as  $\alpha$  decreases to zero. In this paper, we prove this experimental observation and derive a closed form expression for the value of the limit. The performance of a steganographic scheme in the zero-payload limit is important, for example, to avoid detection over multiple uses of the stego channel [9].

In the rest of this paper, we constrain ourselves to binary codes. In Section II, we first briefly describe the ZZW construction. The main result is stated, proved, and analyzed in Section III. The correspondence is concluded in Section IV. Caligraphic font will be used for codes and sets, matrices and vectors are boldface. The symbol  $\oplus$  is reserved for bit-wise eXcluded OR (XOR).

## II. THE ZZW EMBEDDING CONSTRUCTION

Let  $\mathcal{C}_0$  be a code (not necessarily linear) of length  $n$  that can embed  $m$  bits in  $n$  pixels using on average  $R_a$  changes. We

The work on this paper was supported by Air Force Office of Scientific Research (AFOSR) under the research grant number FA9550-08-1-0084. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation there on. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of AFOSR or the U. S. Government.

Jessica Fridrich is Professor at the Department of Electrical and Computer Engineering, Binghamton University, NY 13902 USA (607-777-6177; fax: 607-777-4464; e-mail: fridrich@binghamton.edu)

<sup>1</sup>A popular way is to use the least significant bit of the pixel value or, in general, the modulo  $q$  operation.

will say that  $\mathcal{C}_0$  is  $(R_a, n, m)$ . The following construction leads to a family of codes  $\mathcal{C}_p$ ,  $p \geq 1$ , that are  $(R_a, n2^p, m + pR_a)$ .

For a positive integer  $p$ , we describe the construction of the  $p$ th member of the code family  $\mathcal{C}_p$ . Divide the cover into  $L$  disjoint groups of  $n2^p$  pixels. Furthermore, divide each group into  $n$  disjoint subsets, each consisting of  $2^p$  pixels. Denote by  $\mathbf{x}[i, s, g]$ ,  $i = 1, \dots, 2^p$ ,  $s = 1, \dots, n$ ,  $g = 1, \dots, L$ , the  $i$ th element in the  $s$ th subset from the  $g$ th group. First, embed  $m$  bits  $\mathbf{b} \in \{0, 1\}^m$  in each group (this means  $mL$  bits are embedded in the whole image) by applying the embedding code  $\mathcal{C}_0$  to the binary vector  $\mathbf{v}$  obtained by XOR-ing all  $2^p$  bits from each subset

$$\mathbf{v}[s] = \bigoplus_{i=1}^{2^p} \mathbf{x}[i, s, g], \quad s = 1, \dots, n. \quad (2)$$

Mark down the indices of subsets whose XOR needs to be changed to embed the message  $\mathbf{b}$ , say  $j_1, j_2, \dots, j_r \in \{1, \dots, n\}$ . On average, there will be  $R_a$  such subsets in each group, or  $E[r] = R_a$ . To change the XOR in (2), one pixel must be changed in each marked subset. We will let this one change communicate additional  $p$  bits through a binary Hamming code of codimension  $p$ , which will give us the expected payload  $m + pR_a$  per each group (or per  $n2^p$  cover elements) for the code  $\mathcal{C}_p$ . However, because the receiver will not know which subsets communicate this additional payload (the receiver will not know the indices  $j_1, \dots, j_r$ ), the sender must use codes for memory with defective cells (also called wet paper codes [7]), which is the step described next.

Let  $\mathbf{H}$  be the  $p \times (2^p - 1)$  parity check matrix of a binary Hamming code. Compute the syndrome of each subset as  $\mathbf{s}^{(s,g)} = \mathbf{H}\mathbf{x}[:, s, g] \in \{0, 1\}^p$ , where  $\mathbf{x}[:, s, g] = (\mathbf{x}[1, s, g], \dots, \mathbf{x}[2^p - 1, s, g])$  written as a column vector<sup>2</sup>. Concatenate all these syndromes to one column vector of  $np$  bits

$$\mathbf{s}^{(1,g)}, \mathbf{s}^{(2,g)}, \dots, \mathbf{s}^{(n,g)}. \quad (3)$$

Now realize that due to the property of Hamming codes, for each  $j_i$  we can arrange that each syndrome  $\mathbf{s}^{(j_i,g)}$ ,  $i = 1, \dots, r$ , can be changed to an arbitrary syndrome by making at most one change to  $\mathbf{x}[:, j_i, g]$ .

Label all  $p$  bits of syndromes coming from subsets  $j_1, j_2, \dots, j_r$  as dry (which makes total  $pr$  dry elements per group) and all remaining elements in (3) as wet (in the defective memory scenario, wet bits correspond to stuck cells while dry bits correspond to correctly functioning cells). Concatenate the vectors (3) from all groups to form one long vector of  $Ln p$  elements. This vector will have  $p(r_1 + \dots + r_L)$  dry elements or on average  $E[p(r_1 + \dots + r_L)] = LR_a p$  dry elements. Now, form a random sparse matrix  $\mathbf{D}$  with  $Ln p$  columns and  $p(r_1 + \dots + r_L)$  rows so that its columns follow the robust soliton distribution as described in [7]. Thus, using wet paper codes, we can communicate on average  $LpR_a$  message bits. If the wet paper code dictates that a syndrome  $\mathbf{s}$  be changed to  $\mathbf{s}' \neq \mathbf{s}$ , we can arrange for this by modifying exactly one element in the corresponding vector of bits  $\mathbf{x}[:, j_i, g]$ . If no

<sup>2</sup>Note that we are reserving the last element from each subset  $\mathbf{x}[2^p, s, g]$  to be used later.

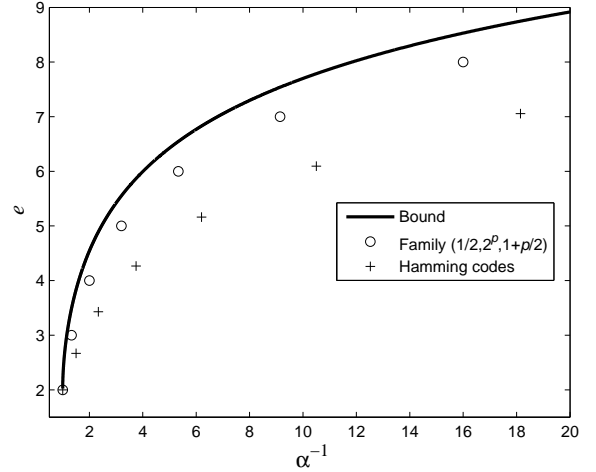


Figure 1. Embedding efficiency of codes from the family  $(\frac{1}{2}, 2^p, 1 + \frac{p}{2})$  for  $p = 0, \dots, 6$ ,  $e(p) = p + 2$ , as a function of relative payload. The bold line is the upper bound (1) for  $q = 2$ . The embedding efficiency,  $\frac{l}{1-2^{-l}}$ , of binary Hamming codes,  $\mathcal{H}_l$ , for  $l = 1, \dots, 7$  is shown for comparison.

change in the syndrome  $\mathbf{s}^{(j_i,g)}$  is needed, all bits  $\mathbf{x}[:, j_i, g]$  must stay unchanged. But because we still need to change the XOR of all elements  $\mathbf{x}[1, j_i, g], \dots, \mathbf{x}[2^p, j_i, g]$  in (2), we simply flip the  $2^p$ th bit  $\mathbf{x}[2^p, j_i, g]$  because this bit was put aside and does not participate in the syndrome calculation.

To summarize, we embed per each group, or per  $n2^p$  elements,  $m + pR_a$  bits using on average  $R_a$  changes. We can also say that the relative payload

$$\alpha(p) = \frac{m + pR_a}{n2^p} \quad (4)$$

can be embedded with embedding efficiency

$$e(p) = \frac{m + pR_a}{R_a} = p + \frac{m}{R_a} = p + e(0). \quad (5)$$

Here, we abbreviate  $e(\alpha(p))$  as simply  $e(p)$ .

By inspecting this construction for the Hamming code  $\mathcal{H}_1$ , which corresponds to the trivial embedding method that embeds one bit in one pixel using on average  $\frac{1}{2}$  change, or the  $(\frac{1}{2}, 1, 1)$  code, we discover something truly remarkable. The ZZW family of codes is  $(\frac{1}{2}, 2^p, 1 + \frac{p}{2})$  and its embedding efficiency for various values of  $p$ ,  $e(p) = \frac{1+p/2}{1/2} = p + 2$ , is shown in Figure 1. This family outperforms all known embedding schemes constructed from structured covering codes (both linear and non-linear [1]) designed to have a small covering radius to bound the worst case of the number of embedding changes. Code families of sparse random constructions [4] follow the bound even closer. This surprisingly good performance is due to the fact that the codes were designed to have small average distance to code,  $R_a$ , even though their covering radius (the worst number of embedding changes) may be quite large.

### III. ASYMPTOTIC BEHAVIOR OF THE ZZW CONSTRUCTION

An observation was made in [11] that the difference between the embedding efficiency (5) of the codes  $\mathcal{C}_p$  and the upper

bound (1) approaches a finite limit as  $p \rightarrow \infty$ . We now prove this fact and derive a closed form expression for the limit as a function of the code parameters.

*Theorem 1:* Under the notation established in Section II,

$$\lim_{p \rightarrow \infty} \frac{\alpha(p)}{H_2^{-1}(\alpha(p))} - e(p) = \frac{1}{\ln 2} - \frac{m}{R_a} + \lg \frac{n}{R_a} = \lambda(R_a, n, m). \quad (6)$$

*Proof:* From (4) and (5), we need the asymptotic behavior of

$$\frac{\alpha(x)}{H_2^{-1}(\alpha(x))} - x - \frac{m}{R_a}, \quad (7)$$

as  $x \rightarrow \infty$ , where  $\alpha(x) = (a + bx)2^{-x}$ ,  $a, b > 0$ ,  $a = \frac{m}{n}$ ,  $b = \frac{R_a}{n}$  (Note that  $\alpha(x) \rightarrow 0$  as  $x \rightarrow \infty$ ). Here, we use  $x$  instead of  $p$  because we allow  $x$  attain real values as opposed to  $p$ , which is an integer. First, we derive an asymptotic expansion of the inverse  $x(\alpha)$  as  $\alpha \rightarrow 0$ . By taking the logarithm,

$$x = -\lg \alpha + \lg(a + bx).$$

The first order approximation to  $x(\alpha)$  is  $x(\alpha) = -\lg \alpha$ . It turns out, we will need the second order approximation

$$x = -\lg \alpha + \lg(a - b \lg \alpha) + r, \quad (8)$$

where  $r$  is the remainder

$$r = \lg(a + bx) - \lg(a - b \lg \alpha). \quad (9)$$

The remainder tends to zero for  $x \rightarrow \infty$ , which can be seen as follows. From the expression for  $\alpha(x)$ , for any  $0 < \epsilon < 1/2$  there exists  $x_0$ , such that  $\forall x \geq x_0$

$$2^{-x} \leq \alpha(x) \leq 2^{-x+\epsilon x}, \quad (10)$$

or

$$-\lg \alpha \leq x \leq \frac{-\lg \alpha}{1 - \epsilon}. \quad (11)$$

Using this bound, we can write for the remainder (9)

$$\begin{aligned} 0 &\leq r \leq \lg \frac{a - b \frac{1}{1-\epsilon} \lg \alpha}{a - b \lg \alpha} = \\ &= \lg \left( 1 + \frac{\epsilon}{1 - \epsilon} \frac{-b \lg \alpha}{a - b \lg \alpha} \right) < \frac{2\epsilon}{\ln 2} \end{aligned} \quad (12)$$

for sufficiently small  $\alpha$  or, equivalently, sufficiently large  $x$ . This is because  $\frac{\epsilon}{1-\epsilon} < 2\epsilon$  for  $\epsilon < 1/2$  and  $\lg(1 + \delta) = \frac{1}{\ln 2} \ln(1 + \delta) < \frac{1}{\ln 2} \delta$  for all  $\delta \neq 0$  (note that  $\frac{-b \lg \alpha}{a - b \lg \alpha}$  tends to one as  $\alpha \rightarrow 0$ ). Thus, we just established that  $r \rightarrow 0$  as  $x \rightarrow \infty$ .

To obtain the asymptotic behavior of (7), we use the variable

$$z = H_2^{-1}(\alpha(x)).$$

Note that  $z \rightarrow 0$  is equivalent with  $x \rightarrow \infty$ . We now rewrite (7) using the variable  $z$  as

$$\frac{H_2(z)}{z} - \alpha^{-1}(H_2(z)) - \frac{m}{R_a}, \quad (13)$$

which can be written using  $A(z) = -\frac{1-z}{z} \lg(1-z)$  and using (8) as

$$\lg \frac{1}{z} + A(z) - [-\lg H_2(z) + \lg(a - b \lg H_2(z)) + r] - \frac{m}{R_a}$$

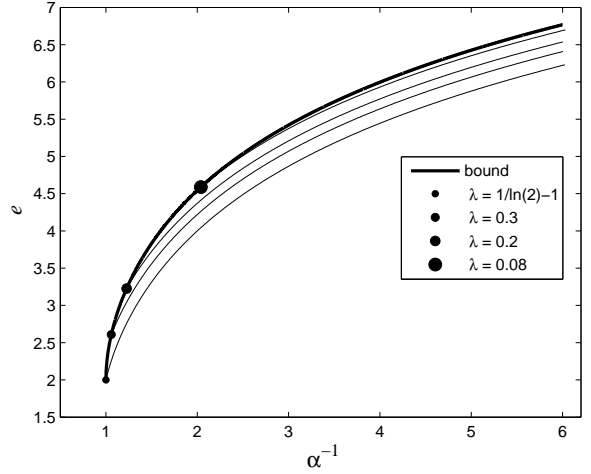


Figure 2. The lines correspond to codes  $(R_a, m, n)$  whose embedding efficiency  $e = m/R_a$  and relative payload  $\alpha = m/n$  satisfy  $\lambda(R_a, m, n) = \text{const}$ . The black dots mark the intersection of the line with the bound on embedding efficiency (1).

$$\begin{aligned} &= A(z) + \lg \frac{H_2(z)}{z(a - b \lg H_2(z))} - r - \frac{m}{R_a} \\ &= A(z) + \lg \frac{\lg \frac{1}{z} + A(z)}{a - b \lg(z \lg \frac{1}{z} + zA(z))} - r - \frac{m}{R_a}. \end{aligned}$$

Note that  $A(z) = \frac{1}{\ln 2} + O(z)$  as  $z \rightarrow 0$ . We continue by rewriting the last expression

$$A(z) + \lg \frac{\lg \frac{1}{z} + A(z)}{a + b \lg \frac{1}{z} - b \lg(\lg \frac{1}{z} + A(z))} - r - \frac{m}{R_a}. \quad (14)$$

The leading term in both the numerator and denominator is the same,  $\lg \frac{1}{z}$ , which means that the  $\lg$  term tends to  $-\lg b = \lg \frac{n}{R_a}$ . Combining this with the fact that  $A(z) \rightarrow \frac{1}{\ln 2}$  and  $r \rightarrow 0$  as  $z \rightarrow 0$ , (14) tends to

$$\frac{1}{\ln 2} + \lg \frac{n}{R_a} - \frac{m}{R_a} = \lambda(R_a, n, m). \quad (15)$$

Another way to represent the asymptotic behavior is to draw the pairs  $(\alpha, e) = \left(\frac{m}{n}, \frac{m}{R_a}\right)$  for all codes with the same limit  $\lambda = \lambda(R_a, n, m)$ . From (15), such pairs must satisfy  $\lambda = \frac{1}{\ln 2} + \lg \frac{e}{\alpha} - e$ , which defines the embedding efficiency  $e$  as a function of  $\alpha$  for each value of  $\lambda$ . A few examples of such curves,  $e(\alpha; \lambda)$ , are shown in Figure 2. Note that the black dots that mark the intersection of  $e(\alpha; \lambda)$  with the bound on embedding efficiency do not correspond to any known codes with the exception of the case  $e = 2$  and  $\alpha = 1$ .

The ZZW construction inherits its asymptotic behavior from Hamming codes, which form the family  $(1 - 2^{-l}, 2^l - 1, l)$ . This means that they can embed relative payload  $\alpha_l = \frac{l}{2^l - 1}$  with embedding efficiency  $e_l = \frac{l}{1 - 2^{-l}}$ . Using an approach similar to the above one can prove that Hamming codes also follow the bound with the following limit

$$\lim_{l \rightarrow \infty} \frac{\alpha_l}{H^{-1}(\alpha_l)} - e_l = \frac{1}{\ln 2}.$$

### A. Comparing codes

The value of the limit  $\lambda(R_{a,n,m}) = \lambda(\mathcal{C})$  could be used for comparing codes in the zero-payload limit. This limit is important for steganography since a necessary condition to avoid being detected by an adversary over multiple use of the steganographic channel is that the embedded payload approaches zero. Thus, it seems natural to define  $\mathcal{C}_1 \prec \mathcal{C}_2$  if and only if  $\lambda(\mathcal{C}_1) \leq \lambda(\mathcal{C}_2)$ .

Under this ordering, it is rather surprising that among all Hamming codes,  $\mathcal{H}_l$ , the code with the smallest value of  $\lambda$  is the trivial  $\mathcal{H}_1$  because

$$\lambda(\mathcal{H}_l) = \frac{1}{\ln 2} - \frac{l}{1-2^{-l}} + \lg \frac{2^l-1}{1-2^{-l}} = \frac{1}{\ln 2} - \frac{l}{2^l-1}$$

and thus for  $l > 1$

$$\lambda(\mathcal{H}_1) = \frac{1}{\ln 2} - 1 < \frac{1}{\ln 2} - \frac{l}{2^l-1} = \lambda(\mathcal{H}_l).$$

This result is perhaps less surprising if we realize that  $\mathcal{H}_1$  is the only Hamming code directly on the bound.

We close this paper with a note that under this ordering, the best known codes today originate from low density generator matrix codes [6].

## IV. CONCLUSIONS

The embedding efficiency of codes from the ZZW embedding construction [11] follows the upper bound on embedding efficiency. The distance to the bound in the zero-payload limit can be expressed in a closed form using the code parameters. The limit could be used to order codes by their asymptotic performance. We note that the embedding construction for  $\pm 1$  embedding also proposed in [11] approaches the bound on embedding efficiency of ternary codes with the same limit (6). This is because the ternary bound increases by 1 compared to the binary bound (as explained in Section I) and, as shown in [11], the embedding efficiency of  $\pm 1$  ZZW code families is also larger by 1.

## REFERENCES

- [1] J. Bierbrauer and J. Fridrich. Constructing good covering codes for applications in steganography. *LNCS Transactions on Data Hiding and Multimedia Security*, 4920:1–22, 2008.
- [2] C. Cachin. An information-theoretic model for steganography. In D. Aucsmith, editor, *Information Hiding, 2nd International Workshop*, volume 1525 of *Lecture Notes in Computer Science*, pages 306–318, Portland, OR, April 14–17, 1998. Springer-Verlag, New York.
- [3] R. Crandall. Some notes on steganography. *Steganography Mailing List*, available from <http://os.inf.tu-dresden.de/westfeld/crandall.pdf>, 1998.
- [4] T. Filler and J. Fridrich. Binary quantization using belief propagation over factor graphs of LDGM codes. In *45th Annual Allerton Conference on Communication, Control, and Computing*, Allerton, IL, September 26–28, 2007.
- [5] J. Fridrich, P. Lisoněk, and D. Soukal. On steganographic embedding efficiency. In J. L. Camenisch, C. S. Collberg, N. F. Johnson, and P. Sallee, editors, *Information Hiding, 8th International Workshop*, volume 4437 of *Lecture Notes in Computer Science*, pages 282–296, Alexandria, VA, July 10–12, 2006. Springer-Verlag, New York.
- [6] J. Fridrich and T. Filler. Practical methods for minimizing embedding impact in steganography. In E. J. Delp and P. W. Wong, editors, *Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX*, volume 6505, pages 02–03, San Jose, CA, January 29 – February 1, 2007.

- [7] J. Fridrich, M. Goljan, and D. Soukal. Efficient wet paper codes. In M. Barni, J. Herrera, S. Katzenbeisser, and F. Pérez-González, editors, *Information Hiding, 7th International Workshop*, Lecture Notes in Computer Science, pages 204–218, Barcelona, Spain, June 6–8, 2005. Springer-Verlag, Berlin.
- [8] F. Galand and G. Kabatiansky. Information hiding by coverings. In *Proceedings IEEE, Information Theory Workshop, ITW 2003*, pages 151–154, Paris, France, March 31 – April 4, 2003.
- [9] A. D. Ker. Batch steganography and pooled steganalysis. In J. L. Camenisch, C. S. Collberg, N. F. Johnson, and P. Sallee, editors, *Information Hiding, 8th International Workshop*, volume 4437 of *Lecture Notes in Computer Science*, pages 265–281, Alexandria, VA, July 10–12, 2006. Springer-Verlag, New York.
- [10] J. Kodovský, J. Fridrich, and T. Pevný. Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities. In J. Dittmann and J. Fridrich, editors, *Proceedings of the 9th ACM Multimedia & Security Workshop*, pages 3–14, Dallas, TX, September 20–21, 2007.
- [11] W. Zhang, X. Zhang, and S. Wang. Maximizing steganographic embedding efficiency by combining Hamming codes and wet paper codes. In K. Solanki, K. Sullivan, and U. Madhow, editors, *Information Hiding, 10th International Workshop*, Lecture Notes in Computer Science, pages 60–71, Santa Barbara, CA, June 19–21, 2008. Springer-Verlag, New York.