Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 186-191*

Sum covers in steganography

Petr Lisoněk[1] plisonek@sfu.ca
Department of Mathematics, Simon Fraser University
Burnaby, BC, CANADA V5A 1S6

Abstract. We extend the study of steganography schemes with pooling to the case when two changes per cell are allowed. We show that such schemes are equivalent to a new, symmetric version of sum covers known in combinatorial design theory. We give a construction that is better in the information versus distortion metric than the schemes with one change per cell. A number of interesting questions concerning the underlying sum cover sets remain open.

1 Steganography background

Steganography is the science of information hiding. The sender starts with a *cover object,* such as for example a digital multimedia file, and (s)he embeds a hidden message into the cover object by slightly distorting it in a way that enables the intended recipient to retrieve the hidden message from the distorted cover object; at the same time the very existence of the hidden message should be impossible to detect by any third party.

Typically the cover object is a sequence of elements of D, where $D = \{0, \ldots, m-1\}$, $m = 2^e$. In current applications we usually have $e \in \{8, 12, 16\}$. For example, $e = 8$ for grayscale digital images and $e = 16$ for CD quality audio.

Let S denote the set of message symbols. A message to be communicated by the sender to the recipient is a string of elements of S. In most steganographic schemes, the sender and the recipient agree on a *symbol-assignment function*

$$s : D \to S. \tag{1}$$

To embed a given message symbol $z \in S$ in a given element $x \in D$, the sender modifies x to x' so that $s(x') = z$ and $|x - x'|$, the *amplitude of the embedding change,* is as small as possible.

One of the goals of Steganography is to design schemes with high embedding efficiency, which can be broadly defined as the ratio between the amount of the communicated information (information rate) and the amount of introduced distortion (distortion rate) [3, 4].

The embedding efficiency can be increased by *applying covering codes,* and we recommend [1] or [5] for an introduction to this topic. In order to achieve a

desired information rate (or a desired distortion rate), one can use direct sums of covering codes.

It has been established in the steganography literature that the impact of embedding becomes statistically detectable rather quickly with the increasing amplitude of embedding changes. Thus, from now on we limit ourselves to so-called *±1 embedding changes* in which the sender modifies each element of D by at most one, which is the smallest possible modification. Hence we will be measuring the total amount of distortion simply by *counting the number of embedding changes.*

We note that a problem will arise in the rare case when the sender is required to apply the $+1$ change to the value $m-1 \in D$ or the -1 change to the value $0 \in D$. Then the sender can choose a different cover object (or the sender can perform a change of a magnitude greater than 1 to achieve the same effect). If we neglect these rare events, then we can assume that $D = \mathbb{Z}$, which makes our algebraic treatment easier.

Let $\mathbb{Z}_n = \mathbb{Z}/(n)$ denote the integers modulo n. A concrete example of a symbol-assignment function (1) that requires only ± 1 embedding changes is given by $S = \mathbb{Z}_3$ and $s(x) = x \bmod 3$. This function has a better embedding efficiency than the notorious "least significant bit embedding" defined by $s(x) = x \bmod 2$.

1.1 Schemes with pooling

In [3] we proved that the embedding efficiency can be increased by *pooling* the elements of D. We partition the cover object into disjoint segments, each of which consists of d elements of D. That is, we partition the cover object into elements of D^d, which we will call *cells.* The details of partitioning into cells are immaterial for our study. For example, the cells can be formed by adjacent elements along some pseudo-random path through the cover object. This pseudo-random path can be generated by the sender and by the recipient from a shared secret seed.

In contrast to (1), the symbol-assignment function will now be a mapping

$$s : D^d \to S. \tag{2}$$

The information rate achieved by s in (2) is $d^{-1} \log_2 |S|$ bits per element of the cover object. Therefore, given the cell dimension d and the maximum number c of changes allowed per cell, we wish to maximize $|S|$. The upper bound on $|S|$ is

$$U_{d,c} := \sum_{i=0}^{c} \binom{d}{i} 2^i$$

since s must be surjective.

One example of a function of the type (2) is given by taking $S = \mathbb{Z}_{2d+1}$ and

$$s(x_1, \ldots, x_d) := \left(\sum_{i=1}^{d} i x_i \right) \bmod (2d+1). \tag{3}$$

In order to embed any symbol $u' \in \mathbb{Z}_{2d+1}$ into any cell $x \in D^d$ using (3), at most one ± 1-change is required. This can be seen as follows: Let (e_i) denote the standard basis of $\mathbb{Z}^d$, and assume $s(x) = u$. Let $\delta = u' - u$. If $\delta = 0$, then no change is performed. Otherwise let $\delta = \varepsilon_k k$ with $\varepsilon_k \in \{-1, 1\}$ and $k \in \{1, 2, \ldots, d\}$. We modify x to $x' = x + \varepsilon_k e_k$; indeed $s(x') = u'$. Note that the embedding defined by (3) is optimal if at most one ± 1-change per cell is allowed, since $|\mathbb{Z}_{2d+1}| = 2d + 1 = U_{d,1}$.

We finish this introductory section by an informal sketch of the main result of [3]. Suppose that $2d + 1$ is a prime power. Let the embedding scheme Σ_1 be defined by the symbol-assignment function (3) and using $(2d + 1)$-ary Hamming codes as covering codes (see the note about covering codes above). Let the embedding scheme Σ_2 be defined by the symbol-assignment function $x \mapsto x \bmod 3$ and using ternary Hamming codes as covering codes to achieve the same distortion rate as Σ_1. Then the information rate of Σ_1 is never worse than the information rate of Σ_2. The precise statement with proofs can be found in [3].

2 Schemes with two changes per cell

The present paper is concerned with the embedding schemes that allow *at most two* ± 1*-changes per cell.* We will continue to use the definitions and notation introduced in Section 1. We start by presenting the mathematical background.

Let R be a ring, $C \subseteq R$, $u \in R$. We define

$$C + C = \{x + y : x, y \in C,\ x \neq y\} \tag{4}$$

and further let $-C = \{-x : x \in C\}$ and $C - u = \{x - u : x \in C\}$. We say that $A, B \subset R$ are *shift equivalent* if there exists a $v \in R$ such that $A = B - v$.

Definition 1. *A subset $S \subseteq \mathbb{Z}_n$ is called a* strict sum cover of $\mathbb{Z}_n$, *abbreviated* SSC(n), *if $S + S = \mathbb{Z}_n$.*

The adjective *strict* emphasizes the condition $x \neq y$ in (4). Many papers (e.g. [6, 7]) consider sumsets both with and without this distinctness condition, hence we feel the need to emphasize the choice made in our definition.

Definition 2. *A subset $S \subseteq \mathbb{Z}_n$ is called* symmetric *if $0 \in S$ and $-S = S$. A subset $S \subseteq \mathbb{Z}_n$ is called a* symmetric strict sum cover of $\mathbb{Z}_n$, *abbreviated* SSSC(n), *if S is symmetric and S is an* SSC(n).

Lemma 3. *If $A = \{0, \pm a_1, \ldots, \pm a_d\}$ is an* SSSC(n), *then*

$$s(x_1, \ldots, x_d) = \left(\sum_{i=1}^{d} a_i x_i \right) \bmod n$$

is a symbol-assignment function that allows the sender to embed any symbol in $\mathbb{Z}_n$ into any cell in $\mathbb{Z}^d$ by at most two ± 1-changes.

The proof is a straightforward extension of the argument for the case of one ± 1-change that was given near the end of Section 1. Note the importance of the condition $x \neq y$ in (4); without imposing this condition it could happen that we require one change of amplitude 2. However, per the discussion in Section 1, two changes of amplitude 1 are preferable to one change of amplitude 2.

Lemma 3 makes our objective fairly obvious: Given d, we wish to maximize n such that an SSSC(n) with $2d + 1$ elements exists.

Definition 4. *For a positive integer k we denote by $n_\gamma(k)$ the largest n such that an* SSC(n) *of cardinality k exists. For an odd positive integer k we denote by $\hat{n}_\gamma(k)$ the largest n such that an* SSSC(n) *of cardinality k exists.*

The notation $n_\gamma(k)$ was introduced in the influential paper by Graham and Sloane [6]. To the best of our knowledge the SSSC(n) have not been studied in the literature; hence the notation $\hat{n}_\gamma(k)$ is new.

Clearly for all odd k we have $\hat{n}_\gamma(k) \leq n_\gamma(k)$.

Proposition 5. *For $3 \leq k \leq 13$, k odd, we have $\hat{n}_\gamma(k) = n_\gamma(k)$.*

Proof. The values $n_\gamma(k)$ for $k \leq 14$ are determined in [7]; they are tabulated in the last row of Table 1 therein. The corresponding SSC($n_\gamma(k)$) are tabulated in Table 4 of that paper. We will now show that for odd $k \in [3, 13]$, each optimal strict sum cover given in [7] is shift equivalent to a symmetric set:
$k = 3$, $C = \{0, 1, 2\} \subset \mathbb{Z}_3$, $C = \{0, \pm 1\} \subset \mathbb{Z}_3$
$k = 5$, $C = \{0, 1, 2, 3, 6\} \subset \mathbb{Z}_9$, $C - 6 = \{0, \pm 3, \pm 4\} \subset \mathbb{Z}_9$
$k = 7$, $C = \{0, 1, 2, 3, 4, 8, 13\} \subset \mathbb{Z}_{17}$, $C - 2 = \{0, \pm 1, \pm 2, \pm 6\} \subset \mathbb{Z}_{17}$
$k = 9$, $C = \{0, 1, 2, 6, 9, 12, 16, 17, 18\} \subset \mathbb{Z}_{30}$, $C - 9 = \{0, \pm 3, \pm 7, \pm 8, \pm 9\} \subset \mathbb{Z}_{30}$
$k = 11$, $C = \{0, 1, 11, 12, 18, 22, 24, 27, 30, 32, 36\} \subset \mathbb{Z}_{42}$,
$C - 27 = \{0, \pm 3, \pm 5, \pm 9, \pm 15, \pm 16\} \subset \mathbb{Z}_{42}$
$k = 13$, $C = \{0, 1, 2, 3, 4, 7, 13, 21, 29, 36, 44, 52, 58\} \subset \mathbb{Z}_{61}$,
$C - 2 = \{0, \pm 1, \pm 2, \pm 5, \pm 11, \pm 19, \pm 27\} \subset \mathbb{Z}_{61}$ □

A lower bound on $n_\gamma(k)$ is given in [2] by a simple construction that uses the sets

$$T(r,k) = \{0, 1, \ldots, r-1\} \cup \{2r-2, 3r-2, \ldots, kr-2\}.$$

We make the following observation:

Proposition 6. *If r is odd or k is even, then $T(r,k)$ is shift equivalent to a symmetric set.*

Proof. If r is odd, then the set

$$T(r,k) - \frac{r-1}{2}$$

is symmetric. If k is even, then the set

$$T(r,k) - \left(\frac{k+2}{2}r - 2\right)$$

is symmetric. The verification is straightforward; we omit its details. □

Proposition 7. *Let $k = 2d+1$. Then $\hat{n}_\gamma(k) \geq d^2 + 3d - 1$.*

Proof. Proposition 2.3 of [2] and some extra calculations show that, for each d, $T(d+1, d+1)$ is an SSC($d^2 + 3d - 1$) of cardinality $2d+1$. By Proposition 6, $T(d+1, d+1)$ is shift equivalent to a symmetric set for each d. □

Proposition 7 shows that the scheme which uses two changes per cell is superior to the scheme using one change per cell, assuming of course a fair comparison when both schemes have the same overall distortion rate $2/d$. Indeed, if d is even, then using $\mathbb{Z}^d \simeq \mathbb{Z}^{d/2} \times \mathbb{Z}^{d/2}$ and defining the symbol-assignment function by applying (3) to each of the factors produces a symbol set of cardinality $(2d/2+1)(2d/2+1) = d^2 + 2d + 1$. Similarly, if d is odd then using $\mathbb{Z}^d \simeq \mathbb{Z}^{(d-1)/2} \times \mathbb{Z}^{(d+1)/2}$ and defining the symbol-assignment function by applying (3) to each of the factors produces a symbol set of cardinality $(2(d-1)/2+1)(2(d+1)/2+1) = d^2 + 2d$. In either case this is less than the $d^2 + 3d - 1$ symbols guaranteed by Proposition 7 combined with Lemma 3.

By non-exhaustive computer search we have verified that the bound of Proposition 7 is not tight for odd k in the range $9 \leq k \leq 61$. For example, $\{0, \pm 3, \pm 12, \pm 13, \pm 21, \pm 26, \pm 48, \pm 52, \pm 54, \pm 65, \pm 84, \pm 91\}$ is an SSSC(195) of cardinality 23 while Proposition 7 only guarantees $\hat{n}_\gamma(23) \geq 153$. An interesting open problem is to give a systematic construction of examples that improve the bound of Proposition 7.

3 Conclusion

We have extended our previous work on steganography schemes with pooling to the case when two changes per cell are allowed. We have shown that such schemes can be obtained from a specialized, symmetric version of sum covers known in combinatorial design theory. We gave a construction that is better in the information versus distortion metric than the schemes with one change per cell.

A number of interesting questions about the symmetric strict sum covers remain open. We conjecture that the equality $\hat{n}_\gamma(k) = n_\gamma(k)$ holds for a larger set of values k than those established in Proposition 5. A construction of examples that improve the bound of Proposition 7 would have practical value. It appears that the optimal covers achieving the value $\hat{n}_\gamma(k)$ often possess a lot of symmetry; it would be interesting to study this phenomenon theoretically.

References

[1] J. Bierbrauer, Personal communication, Available from http://www.ws.binghamton.edu/fridrich/covcodes.pdf, 1998.

[2] M. Chateauneuf, A. C. H. Ling, D. R. Stinson, Slope packings and coverings, and generic algorithms for the discrete logarithm problem. *J. Combin. Des.* 11, 2003, 36-50.

[3] J. Fridrich, P. Lisoněk, Grid colorings in steganography. *IEEE Trans. Inform. Theory* 53, 2007, 1547-1549.

[4] J. Fridrich, P. Lisoněk, D. Soukal, On steganographic embedding efficiency. *Proc. 8th Inform. Hiding Conf.* (J. Camenisch et al., Eds.), Lect. Notes Comp. Sci. 4437, 2007, 282-296.

[5] F. Galand, G. Kabatiansky, Steganography via covering codes, *IEEE Intern. Symp. Inform. Theory*, Yokohama, Japan, 2003. Slides available at www-rocq.inria.fr/secret/Fabien.Galand/PAPERS/galand_isit03.pdf.

[6] R. L. Graham, N. J. A. Sloane, On additive bases and harmonious graphs, *SIAM J. Algebr. Discr. Math.* 1, 1980, 382-404.

[7] H. Haanpää, Minimum sum and difference covers of abelian groups, *J. Integer Seq.* 7, 2004, Article 04.2.6, 10 pp. Available from http://www.emis.de/journals/JIS/VOL7/Haanpaa/haanpaa.pdf.