

# Information Hiding by Coverings\*

F. Galand

INRIA Rocquencourt, Projet CODES, Le Chesnay, France and  
GREYC, University of Caen, Caen, France.

G. Kabatiansky

Institute for Information Transmission Problems,  
Russian Academy of Sciences,  
Moscow, Russia.

## Abstract

We propose a formal model for embedding information in black-white images and prove the equivalence between existence of embedding schemes and covering codes. An asymptotically tight bound on the performance of embedding schemes is given. We construct efficient embedding schemes via known coverings. In particular, one of those schemes allows to embed up to  $\lfloor \log_2(n+1) \rfloor$  bits in coverwords of  $n$  bits, changing at most one bit, which is twice better than [6]. We rewrite some previous schemes with a look towards their covering structures. Finally, we address the problem of active warden in a similar way, giving a model, establishing the relationship with centered codes and concluding by a construction of schemes resisting to active warden.

## 1 Introduction

The subject of steganography is the dissimulation of messages, it is a different one from cryptography which is concerned with transformations of messages but not hiding their existences.

The success of digital media, transmission, storage, ... has led to a wide work in steganography for the past few years, see [1]. Many methods have been proposed when the data in which information is embedded is a picture (e.g. [3, 8, 15, 11]). A few of them are concerned with two-color images (see [17, 6, 10, 13]).

In the sequel, we are interested in embedding schemes using, as coverdata, binary information in which all bits are equally valuable, e.g. two-color images. N. Boston wants “to develop a theory of watermarking that in some ways parallels coding theory” (see [4]), on the contrary, we develop it on the

---

\*in proceedings of IEEE Information Theory Workshop 2003, IEEE, pp. 151 – 154.

basis of coverings and focus on dissimulation — i.e. we are more dealing with steganography rather than watermarking. The organization of this paper is the following: in section 2, we state our formal framework; in section 3 we recall basic facts about covering codes and prove the equivalence between covering codes and embedding schemes. This equivalence gives us an asymptotically tight bound on the performance of embedding schemes (§4). In §5, we propose an efficient construction of schemes using covering codes and show how some previous schemes dealing with two-color images [17, 6] can be represented through covering codes. Finally (§6), still using covering codes, we address the problem of an active warden, deriving an equivalence with centered error-correcting codes introduced by Bassalygo and Pinsker in [2], a bound on corresponding schemes and giving an effective construction.

## 2 Formal Model

We are concerned with binary information in which all bits are equally valuable. Let  $\mathbf{B}^n$  be the set of all binary words of length  $n$ , and let  $d(x, y) = |\{i : x_i \neq y_i\}|$  be the Hamming distance between two words  $x = (x_1, \dots, x_n)$  and  $y = (y_1, \dots, y_n)$  and  $w(x) = |\{i : x_i \neq 0\}|$  be the Hamming weight of  $x$ .

We consider the following model. Alice wants to embed some information  $x \in \mathbf{X}$  (where  $\mathbf{X}$  is the set of all embeddable messages) in some binary coverword  $v \in \mathbf{V} \subset \mathbf{B}^n$ , but in an invisible way, i.e. the resulting stegoword  $s$  should look like  $v$ . This last property shall mean for us that the words  $s$  and  $v$  almost coincide: the Hamming distance between these two words is small, namely  $d(v, s) \leq T$ , where  $T$  is some threshold value depending on the scheme. Let us denote the corresponding embedding mapping by  $E: \mathbf{V} \times \mathbf{X} \rightarrow \mathbf{S}$ , where  $\mathbf{S} \subset \mathbf{B}^n$  is the set of possible stegowords. “Embedding” means it is possible to extract the embedded information  $x$  from  $s$ , i.e. there exists an extracting function  $f: \mathbf{S} \rightarrow \mathbf{X}$  and  $f(s) = x$  for  $s = E(v, x)$ . One can assume w.l.o.g.  $\mathbf{S}$  to be  $\mathbf{B}^n$ , otherwise we add the message  $*$  to  $\mathbf{X}$ , and define  $f(s) = *$  for all  $s \in \mathbf{B}^n \setminus \mathbf{S}$ . In other words, we regard the absence of embedded information as a particular message from  $\mathbf{X}$ .

**Definition 1** *An embedding scheme with a quality threshold  $T$  is a pair of mappings, an embedding mapping  $E: \mathbf{V} \times \mathbf{X} \rightarrow \mathbf{B}^n$  and an extracting function  $f: \mathbf{B}^n \rightarrow \mathbf{X}$ , such that for any  $x \in \mathbf{X}$  and for any  $v \in \mathbf{V}$ , the stegoword  $s = E(v, x) \in \mathbf{B}^n$  has the following properties:*

1.  $f(s) = x$ ,
2.  $d(s, v) \leq T$ .

This definition means that for any data  $x$  and any coverword  $v$ , we can “embed  $x$  in  $v$ ”, and this embedding needs to change not more than  $T$  bits in the coverword  $v$  to get the stegoword  $s$ . Note we do not require to be able to recover  $v$  from  $s$ , in general it is not a steganographic issue:  $v$  has no interest in itself.

Such a scheme is easily transformed into a hiding one: Let  $\mathbf{X}$  be an abelian group, the key shared by Alice and Bob is an element  $k \in \mathbf{X}$ . To hide  $x$  Alice evaluates  $\hat{x} = x + k$  and forms the stegoword  $s = E(v, \hat{x})$ . Bob can find  $\hat{x}$  from the received (observed)  $s$  and then he recovers  $x$  as  $x = \hat{x} - k$ .

### 3 Covering Codes and Embedding Information

In this section we prove the equivalence between covering codes and embedding schemes: an  $R$ -covering code leads to an embedding scheme of threshold  $R$  and *vice versa*. Let us start from the example of Hamming codes showing how to use coverings for embedding.

Let  $\mathcal{H}$  be a Hamming code of length  $n = 2^m - 1$  with  $m \times n$  parity check matrix  $H$  (see [9]). It is known that for any element  $u \in \mathbf{B}^m$  there is exactly one vector  $z$  of weight 1 or less ( $w(z) \leq 1$ ) such that  $z \cdot H^t = u$ , i.e. a Hamming code is a covering of radius 1. Then for a given coverword  $v$  and information embedded  $x \in \mathbf{B}^m$  we find  $z$  such that  $z \cdot H^t = x - v \cdot H^t$  and set the stegoword:  $s = v + z$ . Hence,  $s \cdot H^t = v \cdot H^t + z \cdot H^t = x$  and  $d(v, s) = w(v - s) = w(z) \leq 1$ . Note, this scheme provides the same amount of information to embed and twice less amount of changes than [6] (we will return to this example later).

**Remark 1** *This scheme is perfectly secure in the sense of [5], namely, assume  $v$  is uniformly distributed over  $\mathbf{B}^m$ , then  $s$  is also uniformly distributed over  $\mathbf{B}^m$ .*

#### 3.1 Covering Codes

We recall some basic facts about covering codes (coverings for short) [7]. An  $(n, M)R$ -covering code  $\mathbf{C} = \{c_1, \dots, c_M\}$  is a subset of  $\mathbf{B}^n$  such that, for any vector  $y \in \mathbf{B}^n$ , there exists a codeword  $c \in \mathbf{C}$  such that  $d(y, c) \leq R$ . The covering  $\mathbf{C}$  is said to be linear if  $\mathbf{C}$  is a vector subspace of  $\mathbf{B}^n$  (over the binary field  $\mathbb{F}_2$ ) and denoted as  $[n, k]R$ -covering, where  $k$  is the dimension of  $\mathbf{C}$ . Let  $H$  be a  $(n - k) \times n$  parity check matrix of  $\mathbf{C}$ . It is known that a  $[n, k]$  code  $\mathbf{C}$  is an  $R$ -covering if and only if for any element  $u \in \mathbf{B}^{n-k}$  there exists a vector  $z \in \mathbf{B}^n$  of weight  $w(z) \leq R$  such that  $u$  is the syndrome of  $z$ , i.e.  $u = z \cdot H^t$ . Denote by  $r_L(n, R)$  the largest possible value of  $r = n - k$  for  $[n, k]R$ -coverings and similarly let  $r(n, R)$  denote the largest possible value of  $r = n - \log M$  over all  $(n, M)R$ -coverings. Let us recall the following result

**Proposition 1**

$$\log \left( \sum_{i=0}^R \binom{n}{i} \right) - \log n \leq r_L(n, R) \leq r(n, R) \leq \log \left( \sum_{i=0}^R \binom{n}{i} \right).$$

#### 3.2 Equivalence of Coverings and Embedding Schemes

The key idea of the following proposition is embedding data in the syndrome of the stegoword, that is change the syndrome of the coverword  $v$  to the word  $x$

we want to embed. This can be done by changing at most  $R$  bits of  $v$  providing we use an  $R$ -covering.

**Proposition 2 (From Covering to Embedding)** *Let  $\mathbf{C}$  be an  $[n, k]R$  linear covering code and  $H$  its parity-check matrix. Define  $f: \mathbf{B}^n \rightarrow \mathbf{B}^{n-k}$  by  $f(s) = s \cdot H^t$  and  $E: \mathbf{B}^n \times \mathbf{B}^{n-k} \rightarrow \mathbf{B}^n$  by  $E(v, x) = v + z$  where  $z \in \mathbf{B}^n$ ,  $w(z) \leq R$  and  $z \cdot H^t = x - v \cdot H^t$ . Then, the couple  $(f, E)$  is an embedding scheme able to embed  $2^{n-k}$  different messages in any binary word of length  $n$  with a quality threshold  $R$ .*

**Remark 2** *Similar ideas for constructing embedding schemes by means of coding theory were used in [12], but schemes proposed in [12] have twice larger (i.e. worst) quality threshold.*

**Proposition 3 (From Embedding to Covering)** *Let  $f$  be the extracting function of a given scheme of threshold  $T$ . For all  $x \in \mathbf{X}$ , the set  $U_x = \{s \in \mathbf{B}^n : f(s) = x\} = f^{-1}(\{x\})$  is a  $T$ -covering and all these sets are pairwise disjoint.*

Finally, Prop. 2 and 3 lead to

**Corollary 1** *Let  $h(n, T)$  be the maximal number of bits embeddable by schemes using binary coverwords of length  $n$  with quality threshold  $T$ . We have*

$$r_L(n, T) \leq h(n, T) \leq r(n, T).$$

Hence, an embedding scheme (with quality threshold  $T$ ) is a slightly stronger condition than  $T$ -covering, because embedding scheme generates not a single, but  $|\mathbf{X}|$  disjoint  $T$ -coverings. But in particular case of linear coverings these two notions coincide. It will lead us in the next section to derive asymptotically tight bound on the performance of embedding schemes.

## 4 Asymptotically Tight Bound on the Performance of Embedding Schemes

Since for any given coverword  $v$  only  $\sum_{i=0}^T \binom{n}{i}$  different (stego)words can be obtained by changing at most  $T$  coordinates of  $v$ , then we have the following

**Proposition 4 (Hamming bound)** *For any embedding scheme of quality threshold  $T$ , using binary words of length  $n$  as coverwords, the number of different messages  $M(n, T)$  that can be embedded is bounded by*

$$M(n, T) \leq \sum_{i=0}^T \binom{n}{i}. \quad (1)$$

Recall that  $h(n, T) = \log M(n, T)$  and hence this bound can also be derived from the established equivalence and Prop. 1. The right hand side of (1) is upper bounded by

$$2^{nH_2(\frac{T}{n})}$$

for  $2T < n$ , where  $H_2(x) = -x \log x - (1-x) \log(1-x)$  is the entropy function (see [9, p. 310]). Therefor, we have

$$h(n, T) \leq nH_2\left(\frac{T}{n}\right) . \quad (2)$$

Note this is a good approximation of (1) when  $T$  grows linearly with  $n$ .

For other important case  $T$  fixed and  $n$  growing to infinity it follows from Prop. 4 (and Stirling formula) that

$$h(n, T) \leq T \log n - \log(T!) \quad , \quad T \text{ fixed.} \quad (3)$$

Fortunately there are known constructions of linear coverings very close to the Hamming bound. In the next section we give constructions showing the upper bounds are asymptotically tight.

## 5 Construction

To illustrate our approach, we construct schemes asymptotically close to the Hamming bound and look to the covering structure of some previous work dealing with two color images [17, 6].

### 5.1 Good Schemes from Coverings

A Hamming code is a  $[2^r - 1, 2^r - 1 - r]$ 1-code whose parity-check matrix  $H_r$  is composed of all column vectors of  $\mathbf{B}^r \setminus \{0\}$ . It is known (and easy to verify) that Hamming codes are 1-coverings.

Recall the direct sum construction. Consider  $[N_i, k_i]R_i$ -coverings  $\mathbf{C}_i$  with parity-check matrices  $H_i$ , where  $i = 1, \dots, T$ . Then their direct sum  $\mathbf{C} = \{(c_1, \dots, c_T) : c_i \in \mathbf{C}_i\}$  is a  $[N_1 + \dots + N_T, k_1 + \dots + k_T]R$ -covering with  $R = R_1 + \dots + R_T$ . Let  $\mathbf{C}$  be the direct sum of  $T$  Hamming codes of the same length  $N = 2^r - 1$ , so  $\mathbf{C}$  is a  $[NT, (N-r)T]T$ -covering. Then by Prop. 2,  $\mathbf{C}$  leads to an embedding scheme of threshold  $T$ , which uses coverwords of length  $n = NT$  and allows to embed  $Tr$  bits of information. For  $T$  fixed and  $N$  (or  $n$ ) growing to infinity it means that the scheme can embed asymptotically  $T(\log n - \log T)$  bits. On the other hand, the maximum number of information bits is upper bounded by  $T \log n - \log T!$  (see (3)) and hence (Stirling formula) the difference between the upper bound and the construction is approximately  $T \log e$ . Thus we have the following

**Proposition 5** *Embedding schemes based on direct sum of Hamming codes are asymptotically close to the upper bound (3) (for  $T$  fixed) and provide approximately  $T \log n$  bits of embedded information with quality threshold  $T$ .*

Recall that random linear coverings asymptotically achieve the Hamming bound (see [7, Th. 12.3.4]) in the form (2). Hence in the case of quality threshold  $T$  grows linearly with length  $n$  of coverwords there exist asymptotically optimal (in number of embedded bits) embedding schemes based on linear coverings.

## 5.2 A Look at the Covering Structure of Previous Schemes

A few works dealing with two-color images have already been done, we review some schemes with a look towards their covering structures. For the sake of simplicity we have slightly simplified those schemes.

The scheme presented in [17] embeds one bit in a block of size  $m \times n$  changing at most one bit. To do so, a key is chosen, namely a  $m \times n$  binary matrix  $K$ . Then, write  $B$  a block and  $B \odot K$  the component wise product of  $B$  and  $K$ . A bit is embedded in the parity of the Hamming weight of  $B \odot K$ : that is a bit of  $B$  is changed to get the right parity. We can do exactly the same with coverings: choose a parity check matrix of size  $1 \times mn$ , composed of a single row  $K$ . The bit is embedded in the syndrome  $(B \odot K) \cdot K^t$  (viewing  $B$  as a column vector of dimension  $mn$ ).

On the other hand, the scheme presented in [6] embeds  $r = \log(mn + 1)$  bits in a block of size  $m \times n$  changing at most 2 bits with  $mn = 2^r - 1$ . In addition to a matrix  $K$ , this scheme uses a  $m \times n$  weight matrix  $W$  which has the property that the set of its entries  $\{W_{i,j}\}$  is exactly  $\{1, 2, \dots, 2^r - 1\}$ . Given a  $m \times n$  binary matrix  $M$ , write  $M \otimes W$  the component wise (rational integer) product and  $w_I(M)$  the (rational integer) sum of the entries of  $M \otimes W$ . For a block  $B$ ,  $r$  bits,  $x_0, \dots, x_{r-1}$ , are embedded in the modular integer  $b = w_I(B \oplus K) \bmod 2^r$ : write  $x = x_0 + 2x_1 + \dots + 2^{r-1}x_{r-1}$ , choose at random two couples  $(i_1, j_1)$  and  $(i_2, j_2)$  such that changing the corresponding entries in  $B$ , namely  $B_{i_1, j_1}$  and  $B_{i_2, j_2}$ , increase  $b$  by  $x - b$  modulo  $2^r$  — the property of the weight matrix ensures the existence of those couples. In fact, this scheme "hides" the use of Varshamov-Tenengolts codes [16]. Recall for two given integers,  $0 \leq a \leq n$ , the Varshamov-Tenengolts code  $VT_a(n)$  is the set of all binary words  $(c_1, \dots, c_n)$  satisfying  $\sum_{i=1}^n ic_i \equiv a \pmod{n+1}$ . Thus, the code used is  $VT_0(2^r - 1)$ .

Note that embedding schemes based on direct sum of Hamming codes allow either to embed the same amount of bits with twice better quality threshold ( $T = 1$  instead of  $T = 2$ ) or to embed roughly twice more number of bits with the same quality threshold.

## 6 Active Warden and Centered Error-Correcting Codes

Above we considered embedding schemes that can be easily transformed into hiding schemes for the case of a passive warden, who can only intercept stegowords sent by Alice to Bob. Now consider the case of an active warden who can change at most  $t$  bits of a stegoword  $s = E(v, x)$ . Then Alice should embed the message  $x$  in such a way that Bob can recover  $x$  from the stegoword  $s$  even in presence of at most  $t$  arbitrary (adversary) errors. Hence, the corresponding embedding mapping  $E: \mathbf{V} \times \mathbf{X} \rightarrow \mathbf{B}^n$  should have an extra property: any  $E(c, x)$  and  $E(c', x')$  corrupted by at most  $t$  binary errors must not be mixed by the extracting function. It leads to the following definition of an embedding scheme resistant to the active warden.

**Definition 2** *An embedding scheme with quality threshold  $T$  resistant to an active warden of strength  $t$  is an embedding scheme with quality threshold  $T$  with the following additional requirement on the embedding mapping  $E$ : for any  $v, v' \in \mathbf{V}$  and any  $x \neq x' \in \mathbf{X}$*

$$d(E(v, x), E(v', x')) \geq 2t + 1 .$$

It is equivalent to require that the distance between coverings  $U_x$  and  $U_{x'}$  is at least  $2t + 1$  (see Prop. 3). This definition is known in coding theory as the definition of centered error-correcting codes [2]. It can be formulated in the following way: to find the maximal number  $M(n, T, t)$  of  $T$ -coverings such that any two of them are separated by a Hamming distance not less than  $2t + 1$ .

Let us show how embedding schemes based on the direct sum of Hamming codes can be adapted for this case. The original embedding scheme (see §5.1) uses the set of all  $2^{Tr}$  possible syndromes. This set can be represented as the set of all  $T$  dimensional vectors over the field  $\mathbb{F}_{2^r}$ . In the following we identify  $\mathbb{F}_{2^r}^T$  and  $\mathbf{B}^{2^{Tr}}$ . To provide an ability to correct warden's errors let us use for embedding of information not all possible syndromes but only from a  $2^r$ -ary code.

The information to embed,  $x$ , is encoded in a codeword  $\psi(x)$ , then  $\psi(x)$  is embedded in the syndrome of the coverword  $v$  by adding to  $v$  a vector  $z \in \mathbf{B}^{2^{Tr}}$  such that  $w(z) \leq T$  and  $z \cdot H^t = \psi(x) - v \cdot H^t$ , where  $H$  is the parity check matrix of the direct sum of  $T$  Hamming codes. To recover  $x$  from  $s = v + z$ , perform a decoding on  $\psi(s \cdot H^t)$ .

**Proposition 6** *Consider a  $2^r$ -ary code of length  $T$ , correcting  $t$  errors (over  $\mathbb{F}_{2^r}$ ). Let  $M$  be its cardinality. Then it is possible to construct an embedding scheme with quality threshold  $T$ , resisting to  $t$  arbitrary errors and embedding  $M$  different messages in (binary) words of length  $n = (2^r - 1)T$ .*

Taking Reed-Solomon code of length  $T$  over  $\mathbb{F}_{2^r}$  ( $T \leq 2^r - 1$ ) and correcting  $t$  errors, we have  $\log(M) = (T - 2t)r$ . Thus, denoting by  $h(n, T, t)$  the maximal number of bits embedded by schemes using binary coverwords of length  $n$  with quality threshold  $T$  resisting to  $t$  arbitrary errors, we have for  $T$  and  $t$  fixed,  $r$  growing to infinity,

$$T - 2t + o(1) \leq \frac{h(n, T, t)}{\log_2 n} .$$

**Remark 3** *One can use Algebraic-Geometric codes (cf. [14]) instead of Reed-Solomon codes to obtain constructive schemes with  $T$  and  $t$  growing linearly with  $n$ .*

On the other hand, an analog of Hamming bound for centered codes derived in [2] states that the cardinality of such a code (equivalently, the number of messages which the corresponding scheme is able to embed) is not more than  $M(n, T, t) \leq \binom{n}{T} / \binom{n}{t}$ . Hence under the same hypothesis for the parameters  $T, t$  and  $r$  we have

$$\frac{h(n, T, t)}{\log_2 n} \leq T - t + o(1) .$$

## 7 Conclusions

Our formal framework for information embedding in binary strings allowed us to establish equivalence between the problem of "binary" embedding schemes and the problem of coverings in binary Hamming space. Known results in theory of coverings lead to derive asymptotically tight bound on the performance of "binary" embedding schemes and present good, practical construction of schemes. Some previous works enter in our framework, showing the generality of this approach. We extend our approach to the case of an active warden and establish equivalence between this problem and the problem of centered error-correcting codes.

## References

- [1] R.J. Anderson, editor. *Information Hiding (IH 1996)*, volume 1174 of *LNCS*, 1996.
- [2] L.A. Bassalygo and M.S. Pinsker. Centered error-correcting codes. *Problems of Information Transmission*, 35:30–37, 1999.
- [3] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. Techniques for data hiding. *IBM System Journal*, 35(3–4):313–336, 1996.
- [4] N. Boston. A mathematical foundation for watermarking. Preprint (<http://www.math.wisc.edu/~boston/bostonpreps.html>).
- [5] C. Cachin. An Information-Theoretic Model for Steganography. In *Information Hiding (IH 1998)*, volume 1525 of *LNCS*, pages 306–318, 1998.
- [6] Y.-Y. Chen, H.-K. Pan, and Y.-C. Tseng. A secure data hiding scheme for two-color images. In *IEEE Symposium on Computers and Communication (ISCC 2000)*, pages 750–755.
- [7] G. Cohen, I. Honkala, S. Listyn, and A. Lobstein. *Covering Codes*. North-Holland, 1997.
- [8] I.J. Cox, J. Killian, T. Leighton, and T. Shamoan. A secure, robust watermark for multimedia. In Anderson [1], pages 183–206.
- [9] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 3 edition, 1996.
- [10] G. Pan, Y. Wu, and Z. Wu. A novel data hiding method for two-color images. In *Inter. Conf. on Information and Communications Security (ICICS 2001)*, volume 2229 in *LNCS*, pages 261–270.
- [11] I. Pitas. A method for signature casting on digital images. In *IEEE International Conference on Image Processing*, volume 3, pages 215–218, 1996.

- [12] V.M. Sidelnikov, A.Yu. Serebriakov, A.G. Dyachkov, and P.A. Vilenkin. Methods of constructing steganographical channel. Manuscript, 2000.
- [13] Y.-C. Tseng and H.-K. Pan. Secure and invisible data hiding scheme for two-color images. In *IEEE Infocom 2001*, April 2001.
- [14] M.A. Tsfasman and S. Vladut. *Algebraic Geometric Codes*. Mathematics and its Applications. Kluwer Academic Publishers, 1991.
- [15] R.G. van Schyndel, A.Z. Trikel, and C.F. Osborne. A digital watermark. In *IEEE International Conference on Image Processing*, volume 2, pages 86–90, 1994.
- [16] R.R. Varshamov and G.M. Tenengolts. Codes which correct single asymmetric errors. *Automation and Remote Control*, 26(2):286–290, 1965.
- [17] M.Y. Wu and J.H. Lee. A novel data embedding method for two-color facsimile images. In *Int. Symposium on Multimedia Information Processing*, Dec. 1998.