Linear Hash Functions as a Means of Distortion–Rate Optimization in Data Embedding

Boris Ryabko
boris@ryabko.net
Institute of Computational Technologies SB RAS
Novosibirsk State University
Novosibirsk, Russia

Andrey Fionov
a.fionov@ieee.org
Siberian St. Univ. of Telecom. and Inform. Sci.
Novosibirsk, Russia

ABSTRACT

Embedding hidden data is usually performed by introducing some distortions (errors) in cover objects. If the distortions exceed a certain bound, steganalysis can detect the presence of hidden data. So the problem is to embed as much data as possible and not exceed a permissible distortion level to ensure indetectability. We describe a general class of stegosystems that solves the problem by employing linear hash functions. The suggested stegosystems allow to transmit hidden information of the amount asymptotically close to the maximum possible under the given distortion.

CCS CONCEPTS

• **Security and privacy → Pseudonymity, anonymity and untraceability**; *Digital rights management*.

KEYWORDS

data hiding, data embedding, embedding rate, linear hash function

ACM Reference Format:
Boris Ryabko and Andrey Fionov. 2019. Linear Hash Functions as a Means of Distortion–Rate Optimization in Data Embedding. In *ACM Information Hiding and Multimedia Security Workshop (IH&MMSec '19), July 3–5, 2019, Paris, France.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/ 3335203.3335740

1 INTRODUCTION

The classical problem of steganography is transmitting messages so that the very fact of transmission be concealed from any observer. To achieve this goal, the messages are embedded in various innocuous objects (digital photos, audio, video, etc.), called cover objects or covertexts, whose transmission cannot raise any suspicion. The observer who examines transmitted objects tries to detect the presence of hidden data, which is the problem of steganalysis.

We assume that there are two communicating parties — the sender and the receiver. The sender embeds a secret message in a cover object and transmits it to the receiver over an open communications channel. The receiver is able to extract the message from the cover object. There is also an eavesdropper who observes all transmissions and carries out steganalysis to detect the fact of transmitting hidden data. We also assume that the secret messages are encrypted prior to their embedding and thus are indistinguishable from uniformly distributed random sequences. While the methods of embedding and extracting data are assumed to be publicly known, the sender and receiver may agree in advance on some secret parameters, collectively referred to as a stego key, which can be used primarily for encryption and decryption of messages but also for determining some other parameters of data hiding algorithms.

Embedding hidden data is usually performed by introducing some distortions (errors) in cover objects. Distortions can be measured in different ways depending on the nature of cover object. In the simplest case, it may be the number of bits changed divided by the total number of bits in least significant bit (LSB) replacement or matching algorithms. For other examples, we may refer to additive distortion [1] and universal distortion for JPEG images [2]. The progress in steganalysis shows that if the distortions exceed a certain bound, the presence of hidden data can be detected, and the bound tends to be smaller and smaller. So the problem to be solved by the sender of hidden messages is to embed in cover object as much data as possible while not exceeding a given (permissible) level of distortion. In that case, the stegosystem is believed to ensure indetectability of hidden data transmission.

At the extreme of embedding without any distortion at all, there is a class of so-called perfect stegosystems introduced in [3] where embedding data does not change the structure and statistical properties of cover objects. In particular, efficient methods of constructing such systems for covertexts generated by information sources with finite memory were suggested in [4]. However, embedding hidden data in digital images, audio and similar "natural" objects that cannot be modeled by finite memory sources has to be based on introducing distortions. These distortions make cover objects "less natural" which is the main hook for steganalysis that permits to detect the presence of hidden data. There are two basic approaches in enhancing stegosystems' security: (i) constructing adequate models, such as a statistical model of DCT coefficients [5] and a content-adaptive model [6] (also used for steganalysis) and (ii) constructing methods of increasing the rate of embedding under a specified distortion constraints [1] which is the subject of the present paper.

To clarify the essence of the problem, let us consider an example. Let the sender be able to transmit innocuous N-bit messages in which she can change no more than n bits. (It is supposed that the eavesdropper can detect the fact of introducing distortion and, hence, the fact of hidden data transmission, if $n+1$ bits or more have been changed). One of the possible strategies for the sender is to select n positions (agreed with the receiver) and replace them with

IH&MMSec '19, July 3–5, 2019, Paris, France

ACM ISBN 978-1-4503-6821-6/19/06…$15.00
https://doi.org/10.1145/3335203.3335740

the bits of a secret message. In this case, the embedding rate as well as the distortion bound is n/N and the size of the set of all possible secret messages is 2^n. On the other hand, if the sender may select any n positions in the covertext to make changes, she has the set of possible messages of a rather greater size $\sum_{i=0}^{n}\binom{N}{i}$ (she may change not exactly n bits but any their number up to n). Consequently, the sender can potentially transmit secret messages of $\log\sum_{i=0}^{n}\binom{N}{i}$ bits which asymptotically, as N gets large, equals $Nh(n/N)\,(1+o(1))$, where $h(x)=-(x\log x+(1-x)\log(1-x))$ is the binary Shannon entropy, see [7]. We can see that even for small embedding rates n/N, the length of embedded message, asymptotically, can be much greater than n. However, the problem at the receiver is how he will know the bit positions that have been changed by the sender.

The idea of introducing distortion not in fixed n positions of covertext but in "variable" positions determined by both the embedded message and cover object, was in one form or another realized in stegosystems utilizing error-correcting codes (covering codes, matrix encoding). Such systems were first suggested in [8] and then developed and generalized in [1, 9–11] and many other works.

We consider another general class of stegosystems that are proved to be asymptotically optimal with respect to the embedding rate under any admissible distortion. Let there be given a stegosystem with the set of covertexts $\hat{C}$ and the set of admissible distortions $\hat{D}$. For instance, $\hat{C}$ may be a set of digital photos in full-color BMP format with resolution 1280×800 pixels where each pixel is encoded by three bytes, representing the intensities of red, green and blue color components (RGB). A set of admissible distortions $\hat{D}$ may be composed of elements represented as three matrices (maps) of zeros and ones, each of size 1280×800, where ones indicate the positions which must be changed by LSB replacement or LSB matching, the share of ones being not greater than some threshold (say, 1%) in each matrix. But what is important, our approach is suitable for more complicated distortion models. An alternative demand may admit distortions of not more than 1% of LSB, as previously, but distortions in adjacent pixels are prohibited. In the third case, the distortions are admitted if in any 10×10 square (or a circle with a diameter of 10 pixels) there is not more than 1 bit changed. And so on. Notice that the latter distortion patterns introduce some dependences in distortions which can hardly be implemented by error-correcting coding techniques.

A natural question is related to estimation of the amount of information which can be covertly transmitted in the system $\hat{C}$, $\hat{D}$. Let us call this value the capacity of the system and denote by γ. Then, evidently,

$$\gamma \le \log|\hat{D}|\,, \tag{1}$$

where, as usually, $|\hat{D}|$ is the number of elements in $\hat{D}$. Indeed, each distortion corresponds to one hidden message, so the number of words of length γ (which is 2^γ) cannot be greater than the number of admissible distortions $|\hat{D}|$, hence $2^\gamma \le |\hat{D}|$.

We suggest a stegosystem construction that allows to transmit secret information of the amount asymptotically close to the maximum possible, i.e. $\log\sum_{i=0}^{n}\binom{N}{i}$. The construction is based on linear hash functions whose definition and properties are given in Sect. 2. In Sect. 3 we suggest a stegosystem construction based on linear hash functions. Finally, in Sect. 4 we study the asymptotic capacity of such stegosystems.

2 LINEAR HASH FUNCTIONS

The notion of hash function is well-known. Hash functions are widely used in various fields. There are many constructions that meet certain requirements, for example, cryptographic hash functions (see, e.g., [12]) and hash functions with special properties, e.g., for watermarking purposes [13]. We need a hash function that possesses two main properties: good mixing capability and linearity. It is worth noting that the required hash function does not need to be cryptographically secure.

First, we clarify the concept of hash function mixing property. Let λ be a function defined over the binary words of length N and taking values in the set of binary words of length m, moreover, $N\ge m\ge1$. We refer to this function as *mixing* if for any $v\in\{0,1\}^m$

$$P\{\lambda(w)=v\}=2^{-m}\,, \tag{2}$$

if different w are picked from the set of words $\{0,1\}^N$ uniformly at random (independently and with equal probabilities).

Second, we assume that the function λ is *linear*, i.e. for any $c,d\in\{0,1\}^N$ the identity is valid

$$\lambda(c\oplus d)=\lambda(c)\oplus\lambda(d)\,. \tag{3}$$

As an example of (a class of) hash functions that are mixing and linear consider hash functions defined over binary fields. Every word

$$w=w_{N-1}w_{N-2}\dots w_1w_0\in\{0,1\}^N$$

may be seen as the polynomial

$$w(x)=w_{N-1}x^{N-1}+w_{N-2}x^{N-2}+\dots+w_1x+w_0\,. \tag{4}$$

Let m be an integer and

$$g(x)=x^m+g_{m-1}x^{m-1}+g_{m-2}x^{m-2}+\dots+g_1x+g_0$$

be a degree m polynomial. We define the hash function $\lambda_G(w)$ as the remainder from devision of $w(x)$ by $g(x)$:

$$\lambda_G(w)=w(x)\bmod g(x)\,, \tag{5}$$

using this notation both for polynomial and the word formed by its coefficients. Note immediately that from elementary properties of polynomials it follows that $\lambda_G(w_1\oplus w_2)=\lambda_G(w_1)\oplus\lambda_G(w_2)$, i.e. λ_G is a linear hash function.

It is known that if $g(x)$ is an irreducible polynomial then the set of all possible polynomials $\lambda_G(w)$ constitutes a binary field $\mathbb{F}_{2^m}$ whose definition and main properties can be found in many textbooks, see, e.g., [12].

3 CONSTRUCTING STEGOSYSTEM USING LINEAR HASH FUNCTION

We could see in the example considered in the introduction that, in many cases, both covertexts and distortions may be represented as binary words of equal length and the process of applying the distortion d to the covertext c may be reduced to bitwise addition modulo 2, i.e. the covertext with introduced distortion may be represented as $w=c\oplus d$. In this section, we describe a stegosystem Λ whose capacity is close to the upper bound (1).

Let λ be a mixing linear hash function defined over the set of words w and taking values in the set of binary words of a certain length γ_λ.

Describe now the sequence of actions of the sender and the receiver defining the system Λ.

Let the sender have a covertext $c \in \hat{C}$ and wish to send it with embedded secret message $s \in \{0,1\}^{\gamma_\lambda}$. To do that the sender computes $u = \lambda(c)$, $v = u \oplus s$, and finds the distortion $d \in \hat{D}$ satisfying the identity $\lambda(d) = v$. The sender forms the stegotext $w = c \oplus d$ and sends it to the receiver.

The receiver extracts the message by computing $s = \lambda(w)$.

More precisely, the following is valid:

Theorem 1. *Let the stegosystem Λ be used. If for every word $v \in \{0,1\}^{\gamma_\lambda}$ there exists $d \in \hat{D}$ for which $\lambda(d) = v$, then $\lambda(w) = s$ and the system capacity equals γ_λ.*

Proof. Indeed, from linearity of λ it follows that $\lambda(w) = \lambda(c \oplus d) = \lambda(c) \oplus \lambda(d)$. Due to the system construction $\lambda(d) = v = u \oplus s$ and $\lambda(c) = u$ hence $\lambda(c \oplus d) = u \oplus (u \oplus s) = s$. The theorem is proved. □

Remark 2. *In order to fulfill the condition that $d \in \hat{D}$ for which $\lambda(d) = v$ exists, it is sufficient to require that the values of hash function λ cover entirely the set of γ_λ-bit words, i.e. the identity must hold $\{\lambda(d) : d \in D\} = \{0,1\}^{\gamma_\lambda}$. Then, evidently, for any $v \in \{0,1\}^{\gamma_\lambda}$ such $d \in \hat{D}$ can be found that $\lambda(d) = v$. Notice also that the system capacity equals γ_λ in this case.*

Consider an implementation of the described protocol using the hash function $\lambda_G(w)$ defined over a binary field $\mathbb{F}_{2^m}$ (Sect. 2). Denote by Λ_G the described above stegosystem Λ in the case when the hash function λ_G is employed.

Let the covertexts be binary words of length $N = 2^m - 1$, $m \geq 1$, and the admissible distortion be 1 bit (in other words, the sender gets an N-bit word w in which she may change not more than 1 bit for hidden data transmission). Formally, the set of admissible distortions $\hat{D}$ may be represented as $\hat{D} = \{s_0, s_1, \ldots, s_N\}$, where s_i is a word having a single 1 at the i-th position and zeros at the remaining positions (s_0 consisting of zeros only).

To construct the stegosystem Λ_G choose a primitive polynomial $g(x)$ of degree m that constitutes a binary field $\mathbb{F}_{2^m}$ and let for a word $w \in \{0,1\}^N$ hash function $\lambda_G(w)$ be defined by identities (4) and (5). (Note that the length of hash values is m bits.)

Proposition 3. *The capacity of the stegosystem Λ_G equals m bits which is the maximum possible value.*

Proof. Recall that $\hat{D} = \{s_0, s_1, \ldots, s_N\}$, hence the capacity of this stegosystem cannot exceed $\log|\hat{D}| = \log(N+1) = m$. Let us show now that the capacity equals m. Indeed, the capacity of stegosystem Λ_G is determined in the remark to Theorem 1. As it follows from the remark, it suffices to show that the values of hash function λ_G are different at all possible distortions $d \in \hat{D}$. We defined the set $\hat{D}$ so that any element s_i contains a single 1 bit in the i-th position (s_0 is all zeros). Consequently, $\lambda_G(s_i) = x^{i-1} \bmod g(x)$ for all $i = 1, 2, \ldots, N$, see (5). By definition, the polynomial $g(x)$ is primitive and the property of binary field dictates that $x^{i-1} \bmod g(x)$ are non-zero and different for all $i = 1, 2, \ldots, N = 2^m - 1$, (they generate $2^m - 1$ different non-zero elements of the field). Hence all $\lambda_G(s_i)$ are different for $i = 1, 2, \ldots, N$ and also differ from $\lambda_G(s_0) = 0$. □

Consider a more specific example. Let $m = 2$ and thus $N = 3$. In this case, the set of admissible distortions $\hat{D} = \{000, 001, 010, 100\}$ (we write the words in big-endian format, i.e. the least significant bit is the rightmost, for ease of association with polynomials). Assume that the primitive polynomial $g(x) = x^2 + x + 1$ is chosen. Then the hash function values for the elements of $\hat{D}$ are:

$$\begin{aligned} \lambda_G(000) &= 00\,, \\ \lambda_G(001) &= 1 \bmod g(x) = 01\,, \\ \lambda_G(010) &= x \bmod g(x) = x = 10\,, \\ \lambda_G(100) &= x^2 \bmod g(x) = x + 1 = 11\,. \end{aligned}$$

Suppose the sender has the covertext $c = 101$ and wishes to transmit the secret message $s = 11$. By the protocol defining stegosystem Λ, she computes $u = \lambda_G(c) = \lambda_G(101) = (x^2+1) \bmod (x^2+x+1) = x = 10$, finds $v = u \oplus s = 10 \oplus 11 = 01$ and determines $d \in \hat{D}$ for which $\lambda_G(d) = 01$: $d = 001$. The sender introduces distortion d in covertext c: $w = 101 \oplus 001 = 100$, and sends it to the receiver. The receiver computes $\lambda_G(w) = \lambda_G(100) = 11$ and gets the secret message $s = 11$.

Remark that with the admissible distortion 1 bit, the considered stegosystem Λ_G has the same capacity as a stegosystem based on Hamming codes, see [11].

4 ASYMPTOTIC CAPACITY OF STEGOSYSTEMS BASED ON HASH FUNCTIONS

In this section, we show that "almost any" stegosystem based on hash function has the capacity asymptotically close to the maximum possible. To do this, we go back to considering the general system Λ. In this system, the sender transmits in one covertext object γ_λ bits of secret information which means, by definition, that the capacity equals γ_λ.

Assume that the sets of covertexts $\hat{C}$ and admissible distortions $\hat{D}$ are given, their elements are represented by binary words of length N, and there is a hash function λ, of which is only known that it possesses the mixing property (2). Let us estimate the capacity γ_λ of this system. First, note that with any $m > 0$ and any hash function λ the situation is possible when the values of hash function $\lambda(d)$, $d \in \hat{D}$, do not completely cover the set $\{0,1\}^m$, i.e.

$$\{v : \lambda(d) = v,\ d \in \hat{D}\} \neq \{0,1\}^m\,.$$

Therefore the described system may have some (non-zero) capacity only with certain probability. Obviously, only those systems are practically interesting which have this probability close to 1, say, $1 - 10^{-8}$.

It occurs that, asymptotically, under any arbitrarily small $\delta > 0$ the capacity γ_λ is close to the maximum possible. More formally, the following holds:

Theorem 4. *Let the stegosystem Λ be defined on the set of covertexts $\hat{C}$, the set of randomly selected admissible distortions $\hat{D}$ and uses a hash function λ which possesses the mixing property (2). Then for large $|\hat{D}|$ and any $\delta > 0$ the inequality*

$$\gamma_\lambda \geq \log|\hat{D}| - \log\ln(|\hat{D}|/\delta) \tag{6}$$

holds with probability $1 - \delta$ (here log *denotes binary and* ln *natural logarithms).*

Proof. The proof is based on known solutions of the problem of distributing balls into boxes. The problem is formulated as follows. There are M boxes into which K balls are to be distributed uniformly at random, besides, each box can stow an arbitrary number of balls. A random variable μ_0 is defined to be the number of boxes that remain empty after finishing the distribution of balls. It is shown in [14] that

$$E(\mu_0) \le M\mathrm{e}^{-K/M} . \tag{7}$$

With respect to the stegosystem Λ, we may consider every word from the set $\{0,1\}^m$ as a box, and the elements of $\hat{D}$ as the balls. Besides, assume that the ball d is placed in the box $v \in \{0,1\}^m$, if $\lambda(d) = v$. Note that the mixing property (2) ensures uniformity of distribution of balls into boxes. So

$$M = 2^m , \ K = |\hat{D}| . \tag{8}$$

Random variable μ_0 being not equal to zero, means that the values of hash function $\lambda(d)$ do not cover entirely the set $\{0,1\}^m$ under the given $\hat{D}$. By the condition of the theorem, it is required that the probability of this event be equal to $1-\delta$, i.e.

$$P\{\mu_0 = 0\} = 1 - \delta . \tag{9}$$

Notice now that, by definition,

$$E(\mu_0) = \sum_{j=1}^{\infty} j \times P\{\mu_0 = j\} .$$

It is plain that

$$E(\mu_0) \ge \sum_{j=1}^{\infty} 1 \times P\{\mu_0 = j\} = 1 - P\{\mu_0 = 0\} .$$

From this inequality and (7) we obtain

$$M\mathrm{e}^{-K/M} \ge 1 - P\{\mu_0 = 0\} ,$$

consequently,

$$P\{\mu_0 = 0\} \ge 1 - M\mathrm{e}^{-K/M} .$$

By substitution of (9) in the last inequality we obtain

$$1 - \delta \ge 1 - M\mathrm{e}^{-K/M} .$$

Hence

$$K/M - \ln M \le \ln(1/\delta) .$$

Taking into account that the number of boxes M is less than the number of balls K (since, according to the theorem condition, we consider large $K = |\hat{D}|$), from the last inequality we obtain

$$K/M - \ln K \le \ln(1/\delta) .$$

By rearranging the last inequality we can see that

$$M \ge K/\ln(K/\delta) .$$

Considering that this inequality holds with probability $1-\delta$ and Eq. (8) is valid, taking logarithms we obtain

$$\gamma_\lambda \ge \log|\hat{D}| - \log\ln(|\hat{D}/\delta)| .$$

This completes the proof. □

5 CONCLUSION

A general class of stegosystems was suggested that solves the problem of maximizing the hidden data embedding rate under a given permissible level of cover object distortion by employing linear hash functions. An advantage of the suggested approach is the ability to utilize complex distortion models including mutually exclusive and dependent distortions.

ACKNOWLEDGMENTS

The work is supported by the Russian Foundation for Basic Research under the grant no. 18-29-03005.

REFERENCES

[1] Tomáš Filler, Jan Judas, and Jessica Fridrich. 2011. Minimizing additive distortion in steganography using syndrome-trellis codes. *IEEE Trans. on Info. Forensics and Security* 6, 1, 920–935. DOI: 10.1109/TIFS.2011.2134094

[2] Vojtěch Holub, Jessica Fridrich, and Tomáš Denemark. 2014. Universal distortion function for steganography in an arbitrary domain. *EURASIP Journal on Information Security* 2014, 1. DOI: 10.1186/1687-417X-2014-1

[3] Christian Cachin. 2004. An information-theoretic model of steganography. *Information and Computation* 192, 1 (July 2004), 41–56. DOI: https://doi.org/10.1016/j.ic.2004.02.003

[4] Boris Ryabko and Daniil Ryabko. 2011. Constructing perfect steganographic systems *Information and Computation* 209, 9 (September 2011), 1223–1230. DOI: https://doi.org/10.1016/j.ic.2011.06.004

[5] Thanh Hai Thai, Rémy Cogranne, and Florent Retraint. 2014. Statistical model of quantized DCT coefficients: application in the steganalysis of Jsteg algorithm. *IEEE Trans. Image Processing* 23, 5 (May 2014), 1980–1993. DOI: 10.1109/TIP.2014.2310126

[6] Vahid Sedighi, Rémy Cogranne, and Jessica Fridrich. 2016. Content-adaptive steganography by minimizing statistical detectability. *IEEE Trans. Inform. Forensics and Security* 11, 2, 221–234. DOI: 10.1109/TIFS.2015.2486744

[7] Thomas M. Cover and Joy A. Thomas. 2006. *Elements of Information Theory* (2nd. ed.). Wiley-Interscience, New York, NY.

[8] Ron Crandall. 1998. Some notes on steganography. (December 1998). Retrieved February 2, 2019 from http://dde.binghamton.edu/download/Crandall_matrix.pdf

[9] Andreas Westfeld. 2001. High capacity despite better steganalysis (F5–A steganographic algorithm). In *Proceedings of the 4th International Workshop on Information Hiding*. LNCS 2137, Springer-Verlag, Berlin, Heidelberg, 289–302. DOI: 10.1007/3-540-45496-9

[10] F. Galand and Grigory Kabatiansky. 2003. Information hiding by coverings. In *Proceedings 2003 IEEE Information Theory Workshop*. 151–154. DOI: 10.1109/ITW.2003.1216717

[11] J'urgen Bierbrauer and Jessica Fridrich. 2008. Constructing good covering codes for applications in steganography. *Transactions on Data Hiding and Multimedia Security III*. LNCS 4920, Springer, Berlin, Heidelberg, 1–22. DOI: https://doi.org/10.1007/978-3-540-69019-1_1

[12] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. 1996. *Handbook of Applied Cryptography*. CRC Press.

[13] Jessica Fridrich and Miroslav Goljan. 2000. Robust hash functions for digital watermarking. In *Proceedings of International Conference on Information Technology: Coding and Computing*. IEEE, 173–178. DOI: 10.1109/ITCC.2000.844203

[14] Valentin F. Kolchin, Boris A. Sevastyanov, and Vladimir P. Chistyakov. 1978. *Random Allocations*. V. H. Winston, Washington, New York, distributed solely by Halsted Press.