E-capacity analysis of data hiding channels with geometrical attacks

E. Topak[a], S. Voloshynovskiy[a], O. Koval[a], M. E. Haroutunian[b], J.E. Vila-Forcén[a], and T. Pun[a]

[a]CUI-University of Geneva, 24 rue du Général-Dufour, CH-1211, Geneva 4, Switzerland;
[b]Institute for Informatics and Automation Problems, National Academy of Science, Armenia

ABSTRACT

In a data hiding communications scenario, geometrical attacks lead to a loss of reliable communications due to synchronization problems when the applied attack is unknown. In our previous work, information-theoretic analysis of this problem was performed for theoretic setups, i.e., when the length of communicated data sequences asymptotically approaches infinity. Assuming that the applied geometrical attack belongs to a set of finite cardinality, it is demonstrated that it does not asymptotically affect the achievable rate in comparison to the scenario without any attack. The main goal of this paper is to investigate the upper and lower bounds on the rate reliability function that can be achieved in the data hiding channel with some geometrical state. In particular, we investigate the random coding and sphere packing bounds in channels with random parameter for the case when the interference (channel state) is not taken into account at the encoder. Furthermore, only those geometrical transformations that preserve the input dimensionality and input type class are considered. For this case we are showing that similar conclusion obtained in the asymptotic case is valid, meaning that within the class of considered geometrical attacks the rate reliability function is bounded in the same way as in the case with no geometrical distortions.

Keywords: data hiding, geometrical attacks, *E*-capacity analysis.

1. INTRODUCTION

Data hiding refers to a near invisible embedding of information into multimedia files in order to provide, depending on the particular application scenario, copyright protection, content authentication or to assist media files processing and management.[1]

The problem of reliable communication of the embedded information via an attacking channel that should be solved on the side of the data-hider has a dual one on the side of the attacker, who is targeting impairing reliable communications. Among the existing classes of aggressive scenarios that the attacker may apply (signal processing, protocol attacks, etc.), geometrical transformations represent such a choice for the attacker that lead to the performance loss via the protocol desynchronization.

Low computational complexity and high efficiency that do not depend on the amount of available side information (SI) about the data hiding method make geometrical attacks very attractive for practice as well as their analysis and countermeasure development an important and challenging research issue for the data hiding community.

Additional complexity of the problem originates from the broad diversity of such transformations that include translation, rotation, cropping, shearing, *etc.* or even their composition. Evidently, under these conditions establishing the reliable communications would not be possible without clear understanding of the main properties of geometrical transformations due to their influence on the codebook design. Therefore, as the first task, one should start with the classification of known geometrical transformations. The main classification feature should reflect particularities of the protocol desynchronization introduced by the geometrical transformation and should

Further author information: (Send correspondence to S. Voloshynovskiy): E-mail: svolos@cui.unige.ch, http://sip.unige.ch

be based on the dimensionality of the channel output, whose state is determined by the applied geometrical transformation.

According to the given classification criterion, i.e. the effect on the dimensionality of input, one can differentiate two types of geometrical transformations: a group of geometrical transformations that modify the dimensionality of their input sequence and a group of geometrical transformations that preserve the dimensionality of their input.

A further classification can be considered based on the effect of geometrical transformations on the empirical distribution of input sequences, i.e., input type: geometrical transformations that change the type of their input and those that does not have an effect on the type. As an example to transformations that change the input type, one can give cropping. Similarly, circular shift and permutation of elements of the input sequence as well as random bending attack are from the group of geometrical attacks that do not modify the input type.

In some communications scenarios, there is a possibility to have a priori or a posteriori knowledge about the applied geometrical transformation. Therefore, depending on the availability of SI about the geometrical transformation, one can give the following classification of communications scenarios:

- SI is available at the encoder,
- SI is available at the decoder,
- SI is available at both the encoder and the decoder,
- No SI is available neither at the encoder nor at the decoder.

While one can recognize a significant progress in development of practical data hiding algorithms robust to geometrical distortions, theoretical analysis of this problem from the positions of information theory has just initiated.

Among the existing results of information theoretic analysis of the data hiding channels with geometrical attacks, one can point out recent results of Merhav[2] and Moulin,[3] who analyzed the problem in detection formulation. These results allow to conclude about the asymptotic independence of the protocol performance from the applied geometrical transformation in the case when the cardinality of the set of possible attacks is finite.

Similar conclusion were made by Topak *et al.*,[4] who analyzed the problem in communications formulation. It was demonstrated that, in the asymptotic case, when the length of communicated data sequences goes to infinity and assuming that the applied attack belongs to the set of typical geometrical transformations with a finite cardinality, achievable rate is not affected by the applied geometrical transformation and it is equal to the rate in case where there is no geometrical attack at all.

Besides capacity analysis in the data hiding protocols with geometrical state, another challenging research issue is the investigation of the achievable random exponent. To our best knowledge, no result exists up to date bounding the performance of the data hiding protocols with geometrical state in this sense.

Motivated by this gap in the theoretical performance limits justification of the data hiding protocols with geometrical attacks, we formulate the main goal of this paper in the development of the upper and lower bounds on the achievable rate-reliability function in such communications setups. The main underlying assumptions of our analysis are:

1. the encoder does not benefit from the availability of the host data (random coding-based scenario);
2. the geometrical state is not available neither to the encoder nor to the decoder;
3. the geometrical attack belongs to the class of geometrical attacking strategies that do not modify the dimensionality and type of the input.

The rest of the paper is organized as follows: In Section 2, a brief review of the method of types is provided. Afterwards, in Section 3, the problem of reliable communications through data hiding channels with geometrical attacks is formulated from the information-theoretic point of view. Section 4 contains the E-capacity analysis for data hiding channels with geometrical attacks in terms of random coding lower bound and sphere packing upper bound on the rate-reliability function. Finally, Section 5 concludes the paper and presents some possible directions for the future research.

We adapt the following notations in this paper: We use capital letters to denote random variables X, small letters x to denote their realizations. The superscript N is used to designate length-N vectors $x^N = [x[1], x[2], ..., x[N]]^T$ with k^{th} element $x[k]$. We use $X \sim p_X(x)$ or simply $X \sim p(x)$ to indicate that a random variable X is distributed according to $p_X(x)$. Calligraphic fonts $\mathcal{X}$ denote sets $X \in \mathcal{X}$ and $|\mathcal{X}|$ denotes the cardinality of $\mathcal{X}$. $(\mathbf{N}(x)|x^N)$ stands for the number of times a particular symbol x occurs in x^N. We use $H(W)$ and $I(W;V)$ to denote the entropy of W and the mutual information between W and V respectively. $D(p||p')$ is used to indicate the divergence between probability distributions p and p'. P is used to denote the empirical distribution (type) of a sequence x^N, $\mathcal{P}_N(X)$ designates the set of all possible types of x^N sequences and $T_P^N(X)$ is reserved to denote the set of x^N sequences that has the type P. Similarly, $T_{P,Q}^N(Y|x^N)$ designates the set of y^N sequences in the Q-shell of x^N and $\mathcal{Q}_N(\mathcal{Y}, P)$ denotes the set of all possible Q-shells for a given $x^N \in T_P^N(X)$.

2. METHOD OF TYPES: BASIC DEFINITIONS & PROPERTIES

Let $w^N = [w[1], w[2], ..., w[N]]$ be a sequence of N symbols such that $w[i] \in \mathcal{W}$. The *type* P of w^N is the empirical distribution of each symbol $w \in \mathcal{W}$ within w^N defined as[5]:

$$P = \frac{(\mathbf{N}(w)|w^N)}{N}. \tag{1}$$

For a sequence of length N with elements coming from the set $\mathcal{W}$, there are at most $(N+1)^{|\mathcal{W}|}$ values that the sequence might have. Therefore, the number of types is upper bounded as:

$$|\mathcal{P}_N(W)| \leq (N+1)^{|\mathcal{W}|}. \tag{2}$$

If the elements of the sequence $w^N = [w[1], w[2], ..., w[N]]$ are independently and identically distributed (i.i.d.) according to $p(w)$, then the probability of w^N will be[6]:

$$p(w^N) = \exp\{-N(H(W) + D(P||p(w)))\}, \tag{3}$$

where the probability of a sequence depends on its type P. Thus, according to (3), sequences with $P = p(w)$ has the highest probability $\exp\{-N(H(W))\}$. Moreover, based on this result it can be concluded that the sequences of the same type also have the same probability. This links the types with strongly typical sequences whose properties are defined according to Shannon-McMillan theorem.[6]

After calculating the probabilities of sequences in a particular type class, one can bound the cardinality of a type class $P \in \mathcal{P}_N(W)$ as:

$$(N+1)^{-|\mathcal{W}|}\exp\{N(H(W))\} \leq |T_P^N(W)| \leq \exp\{N(H(W))\}. \tag{4}$$

Considering the fact that the sequences of the same-type are equiprobable, based on (3) and (4), one can derive the following bounds for the probability of a type class as:

$$(N+1)^{-|\mathcal{W}|}\exp\{-N(D(P||p(w)))\} \leq p(T_P^N(W)) \leq \exp\{-N(D(P||p(w)))\}. \tag{5}$$

There exists a similar definition for joint distribution of multiple sequences. Let $w^N = [w[1], w[2], ..., w[N]]$ and $v^N = [v[1], v[2], ..., v[N]]$ be two sequences of length N such that $w[i] \in \mathcal{W}$ and $v[i] \in \mathcal{V}$. The *joint type* (P, Q) of sequences w^N and v^N is the empirical distribution defined as:

$$(P, Q) = \frac{(\mathbf{N}(w, v)|(w^N, v^N))}{N}. \tag{6}$$

After giving the definition of joint type, it is important to introduce the *conditional type* of v^N given w^N as the empirical distribution Q, if $(\mathbf{N}(w,v)|(w^N,v^N)) = (\mathbf{N}(w)|w^N)Q(v|w)$ for all $w \in \mathcal{W}$ and $v \in \mathcal{V}$. The set of sequences v^N with conditional type Q for a given $w^N \in T_P^N(W)$ is called a *Q-shell* of w^N and is denoted by $T_{P,Q}^N(V|w^N)$. The set of all Q-shells for a given $w^N \in T_P^N(W)$ is designated by $\mathcal{Q}_N(\mathcal{V},P)$.

Similar to (2),(3),(4) and (5), one can obtain the following properties of the conditional type Q[5] :

$$|\mathcal{Q}_N(\mathcal{V},P)| \leq (N+1)^{|\mathcal{W}||\mathcal{V}|} \tag{7}$$

$$p(v^N|w^N) = \exp\{-N(H(V|W) + D(Q||p(v|w)|P))\} \tag{8}$$

$$(N+1)^{-|\mathcal{W}||\mathcal{V}|}\exp\{N(H(V|W))\} \leq |T_{P,Q}^N(V|w^N)| \leq \exp\{N(H(V|W))\} \tag{9}$$

$$(N+1)^{-|\mathcal{W}||\mathcal{V}|}\exp\{-N(D(Q||p(v|w)|P))\} \leq p(T_{P,Q}^N(V|w^N)) \leq \exp\{-N(D(Q||p(v|w)|P))\} \tag{10}$$

3. RELIABLE COMMUNICATIONS THROUGH DATA HIDING CHANNELS WITH GEOMETRICAL ATTACKS

A data hiding communications scenario under the analysis is depicted in Figure 1. In this setup, one assumes the existence of $|\mathcal{K}|$ different users that communicate using a particular codebook defined by a realization of the secret key $K = k$, $K \in \{1, 2, \ldots, |\mathcal{K}|\}$. Codebooks are constructed from codewords W^N that are from a particular type class $T_P^N(W)$. Encoder and decoder, which are common to all users, are informed about codebooks used depending on the particular key. However, they are not informed about the applied geometrical transformation, so, this scenario falls into the last classification category presented in the Introduction.

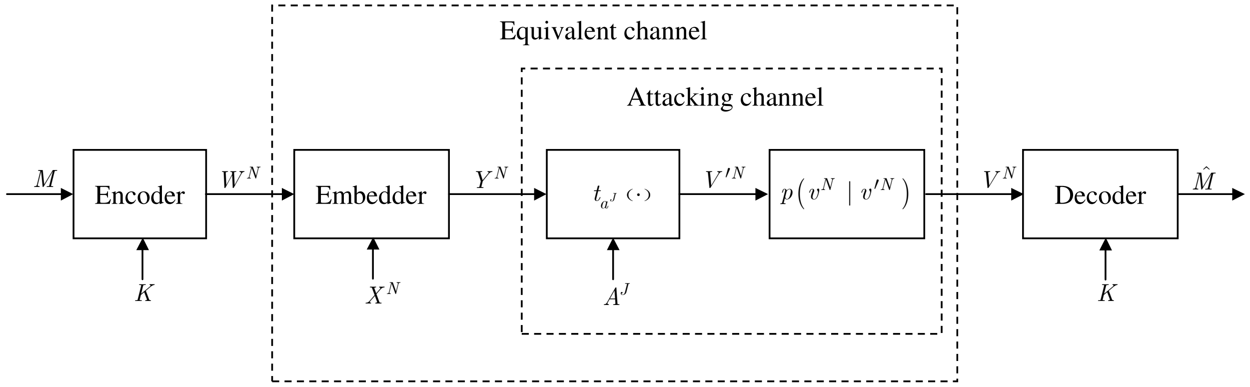

Figure 1. Considered communications setup.

The main stages of the communications in this setup (Figure 1) are as follows:

- Codebook generation: From the type P generate at random $|\mathcal{M}||\mathcal{K}|$ $N-$length codewords and distribute them randomly among $|\mathcal{K}|$ codebooks to guarantee collusion-free communications for a given class of geometrical transformations with cardinality $\left|\mathcal{A}^J\right|$. This is accomplished in the way similar to the bad codewords' expurgating.[6]

- Encoder: The encoder maps the message M, $M \in \{1, 2, \ldots, |\mathcal{M}| = \exp\{NR\}\}$, and the key K into a watermark sequence W^N of length N according to an encoding function $\phi : \{1, 2, \ldots, |\mathcal{M}|\} \times \{1, 2, \ldots, |\mathcal{K}|\} \to \mathcal{W}^N$.

- Equivalent channel:

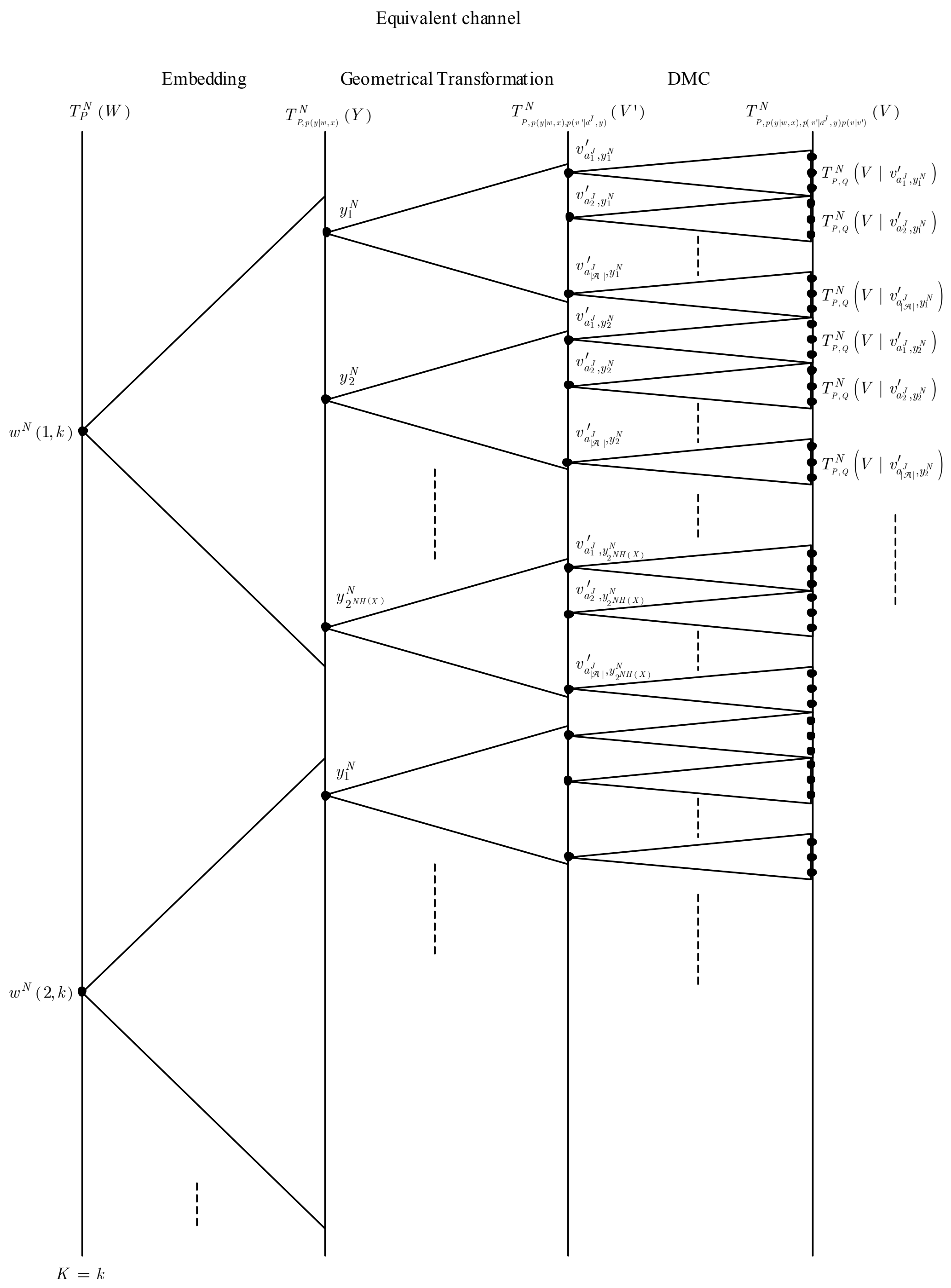

Figure 2. Codewords selection considering the equivalent channel.

– W^N is combined with the host data X^N using an embedding function $\varphi : \mathcal{W}^N \times \mathcal{X}^N \to \mathcal{Y}^N$ according to some mapping $p(y^N|w^N, x^N)$.

– Resulting stego data Y^N is sent to the attacking channel. The attacking channel consists of two parts: geometrical transformation part $t_{a^J}(.)$ and discrete memoryless channel (DMC) part $p(v^N|v'^N) = \prod_{i=1}^N p(v_i|v'_i)$.

First of all, a geometrical transformation t_{a^J} with some random parameters a^J from a set of geometrical transformations with a finite cardinality $|\mathcal{A}^J|$ is applied to the stego data Y^N. As it was already mentioned, it is assumed that this geometrical transformation does not modify the dimensionality N and type of the stego data*. Following the geometrical transformation, the DMC maps the transformed data V'^N to the attacked data V^N according to its channel transition probability $p(v^N|v'^N)$. As an example of such attacking channels, one can give the circular shift operation followed by addition of noise.

The joint probability distribution for the given equivalent channel input and output under the assumed class of geometrical attacks that do not modify the dimensionality of the input can be written as:

$$p(w^N, x^N, a^J, v^N) = p(w^N)p(x^N)p(a^J)p(v^N|w^N, x^N, a^J), \tag{11}$$

where $p(v^N|w^N, x^N, a^J)$ can be expressed either as:

$$p(v^N|w^N, x^N, a^J) = \sum_{y^N} p(y^N|w^N, x^N) \sum_{v'^N} p(v'^N|a^J, y^N)p(v^N|v'^N), \tag{12}$$

or as:

$$p(v^N|w^N, x^N, a^J) = \sum_{y'^N} p(y'^N|a^J, w^N) \sum_{v''^N} p(v''^N|y'^N, x^N)p(v^N|v''^N). \tag{13}$$

Therefore, one can change the order of the embedding and geometrical attack parts in the equivalent channel (Figure 3). However, it should be noticed that this assumption is not generally true for those geometrical channels that do not preserve the dimensionality of the input sequences and their type. Furthermore, assuming that X^N is distributed according to $p(x^N) = \prod_{i=1}^N p(x_i)$ and t_{a^J} and ϕ functions work samplewise, i.e., $p(y'^N|a^J, w^N) = \prod_{i=1}^N p(y'_i|a^J, w_i)$ and $p(v''^N|y'^N, x^N) = \prod_{i=1}^N p(v''_i|y'_i, x_i)$, the equivalent channel from the input W^N to the output V^N can be given as:

$$\begin{aligned} p(v|w) &= \sum_x p(x) \sum_{a^J \in \mathcal{A}^J} p(a^J)p(v|w, x, a^J), \\ &= \sum_x p(x) \sum_{a^J \in \mathcal{A}^J} p(a^J) \sum_{y'} p(y'|a^J, w) \sum_{v''} p(v''|y', x)p(v|v''), \\ &= \sum_{a^J \in \mathcal{A}^J} p(a^J) \sum_{y'} p(y'|a^J, w) \sum_{v''} p(v''|y')p(v|v''), \\ &= \sum_{a^J \in \mathcal{A}^J} p(a^J) \sum_{y'} p(y'|a^J, w)p(v|y'). \end{aligned} \tag{14}$$

Thus, the equivalent channel can be partitioned into the geometrical attack $p(y'|a^J, w)$ and equivalent DMC $p(v|y')$ parts as shown in Figure 3.

- Decoder: At the decoder, the message $\hat{M}$ can be decoded from the attacked data V^N based on the knowledge of the key K according to a decoding function $\psi : \mathcal{V}^N \times \{1, 2, \ldots, |\mathcal{K}|\} \to \{1, 2, \ldots, |\mathcal{M}|\}$. The decoder, which neither has a geometrical synchronization framework for recovery nor a priori knowledge about the applied geometrical transformation will have to consider all elements of the geometrical attack set $\mathcal{A}^J$ as the possibly applied one and to perform an exhaustive decoding for reproductions of codewords $m \in \mathcal{M}$ for each geometrical attack $a^J \in \mathcal{A}^J$.[7]

The performance of the introduced communications scheme can be measured with the probability of error:

$$p_e = p(\mathcal{V}^N - \psi^{-1}(m, k)|w^N(m, k)). \tag{15}$$

*It should be noticed that in the general case, geometrical transformation can modify the length of the input sequence and its type. However, this kind of geometrical transformation is out of the scope of this paper

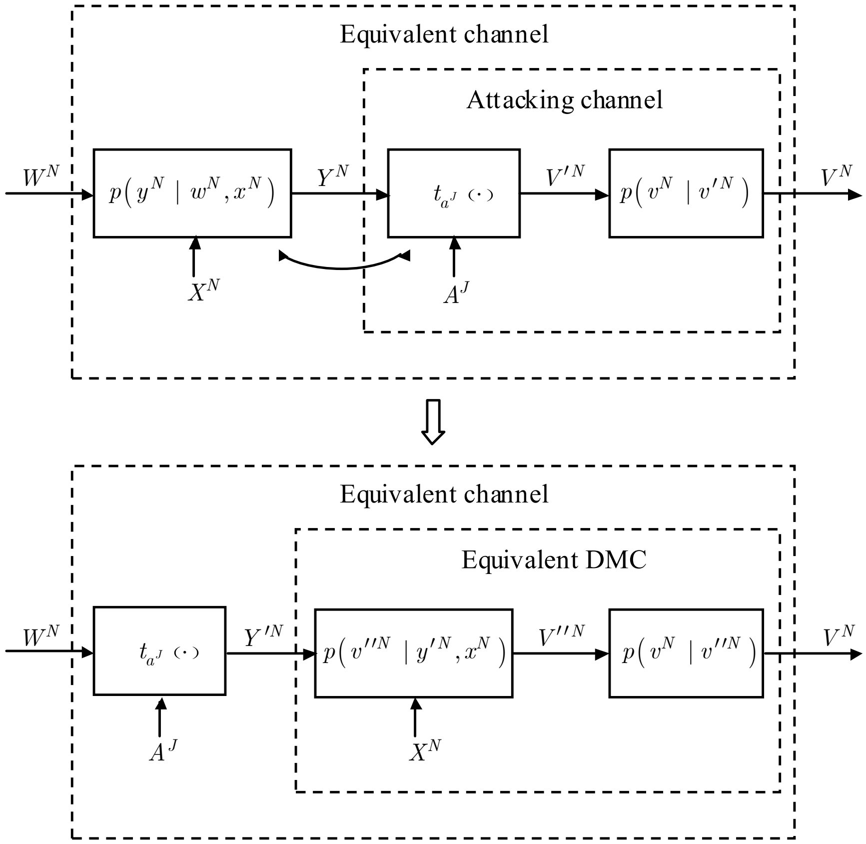

Figure 3. Possible structures of the equivalent channel.

Assuming that for the fixed key $K = k$, messages $m \in \mathcal{M}$ and geometrical attacks $a^J \in \mathcal{A}^J$ are equiprobable, one can define the average probability of error as:

$$\overline{p_e} = \frac{1}{|\mathcal{A}^J|} \sum_{a^J \in \mathcal{A}^J} \frac{1}{2^{NR}} \sum_{m \in \mathcal{M}} p(\psi(V^N(t_{a^J}(w^N(m,k))), k) \neq m | w^N(m,k)), \tag{16}$$

and the maximum probability of error as:

$$p_{e,max} = \max_{m \in \mathcal{M}, a^J \in \mathcal{A}^J} p_e. \tag{17}$$

Consider the data hiding codes with error probabilities exponentially decreasing with a given reliability E in the exponent:

$$p_e \leq \exp\{-N(E-\delta)\}. \tag{18}$$

Denote the best volume of the code of length N for the channel $p(v|w)$ satisfying the above condition on error probability for a given reliability $E > 0$ by $|\mathcal{M}|$. E-capacity is defined as:

$$R(E, p(v|w)) = C(E, p(v|w)) \triangleq \lim_{N \to \infty} \frac{1}{N} \ln |\mathcal{M}|. \tag{19}$$

E**-capacity** is considered **maximal**, $C_{max}(E, p(v|w))$, or **average**, $\overline{C}(E, p(v|w))$, depending on the particular probability of error consideration in the calculation of the above limit. In fact, when $0 < E < \infty$:

$$C_0(p(v|w)) \leq C_{max}(E, p(v|w)) \leq \overline{C}(E, p(v|w)) \leq C(p(v|w)), \tag{20}$$

where $C_0(p(v|w))$ is the zero-error capacity of the channel, which is the smallest upper bound on R for which beginning from some N there exists a code (ϕ, ψ) with $p_e = 0$.

For a given $p(v|w)$ and E, rate-reliability function $R(E, p(v|w))$ can be upper bounded by the sphere packing bound and lower bounded by the random coding bound[8] in terms of the codebook volume $|\mathcal{M}|$.

As complementary to results provided in,[4] it is also demonstrated that as the length N of communicated data sequences asymptotically approaches ∞ and E goes to 0, for a given finite $|\mathcal{A}^J|$, $R(E, p(v|w))$ coincides with the maximum achievable rate R for the case when there is no geometrical attack at all.

4. E-CAPACITY ANALYSIS FOR DATA HIDING CHANNELS WITH GEOMETRICAL ATTACKS

In the following sections, we perform an E-capacity analysis for the communications scenario given in Figure 1 through the data hiding channel with geometrical attacks of finite cardinality by deriving random coding lower bound and sphere packing upper bound on the E-capacity successively.

As it was demonstrated in the previous Section, a given data hiding channel presented by an embedding part $p(y^N | w^N, x^N)$, a geometrical attack $t_{a^J}(w^N)$ and a DMC attacking channel $p(v^N | v'^N)$ can be equivalently represented by sequentially acting geometrical attack, embedding and the DMC. Therefore, the foregoing consideration will be performed with respect to the equivalent channel that consists of the geometrical transform $t_{a^J}(w^N)$ and the equivalent DMC channel $p(v^N | y'^N)$ that combines the embedding and attacking parts. It is also of particular importance to note that since the geometrical transforms $t_{a^J}(w^N)$, $a^J \in \mathcal{A}^J$, that do not modify the type of its input, one has $y'^N \in T_P^N(W)$.

4.1. Random coding bound for E-capacity of data hiding channels with geometrical attacks

The achievable rate in the data hiding communications protocol with geometrical state is lower bounded by the random coding bound $R_r(E, p(v|y'))$ as[8]:

$$R_r(E, p(v|y')) \leq C_{max}(E, p(v|y')) \leq \overline{C}(E, p(v|y')), \tag{21}$$

where

$$\begin{aligned} R_r(P, E, p(v|y')) &\triangleq \min_{Q: D(Q||p(v|y')|P) \leq E} |I(Y'; V) + D(Q||p(v|y')|P) - E|^+, \\ R_r(E, p(v|y')) &\triangleq \max_P R_r(P, E, p(v|y')), \end{aligned} \tag{22}$$

where Q corresponds to the $Q-$shell introduced by Csiszar and Korner.[5] Following lemma is essential in the proof of the random coding bound:

Lemma (packing lemma): For the given $E > 0$, $\delta \geq 0$, type P from the set $\mathcal{P}_N(Y')$:

$$|\mathcal{M}| = \exp\left\{N \min_{Q: D(Q||p(v|y')|P)) \leq E} |I(Y'; V) + D(Q||p(v|y')|P) - E - \delta|^+\right\}, \tag{23}$$

there exists $|\mathcal{M}||\mathcal{K}||\mathcal{A}^J|$ distinct vectors from $T_P^N(Y')$, which includes $|\mathcal{M}||\mathcal{K}|$ codewords used to communicate messages $m \in \mathcal{M}$ for each user $k \in \mathcal{K}$ and their reproductions for each geometrical attack $a^J \in \mathcal{A}^J$, such that for any $m \in \mathcal{M}$, $k \in \mathcal{K}$, $a^J \in \mathcal{A}^J$, for conditional types Q, Q', and N large enough:

$$\begin{aligned} &\left| T_{P,Q}^N(V|t_{a^J}(w^N(m,k))) \bigcap \left(\bigcup_{m' \neq m} T_{P,Q'}^N\left(V|t_{a^J}(w^N(m',k))\right)\right)\right| \leq \\ &\qquad \left|T_{P,Q}^N(V|t_{a^J}(w^N(m,k)))\right| \exp\{-N|E - D(Q'||p(v|y')|P)|^+\}. \end{aligned} \tag{24}$$

One can show[8] the existence of $|\mathcal{M}||\mathcal{K}|$ distinct codewords satisfying (23) and (24).

Proof of the random coding bound: The data-hider possessing the key $K = k$ decodes v^N to such m' that for some a'^J and Q':

$$v^N \in T^N_{P,Q'}(V|t_{a'^J}(w^N(m',k))) \text{ and } D(Q'||p(v|y')|P), \tag{25}$$

is minimal. This type of decoding is known as **minimum divergence decoding** to be a particular case of the maximum likelihood decoding.[8] This requires the knowledge of channel transition probability $p(v|y')$ at the decoder. One can also assume the **maximum mutual information** (MMI) decoding considered by Csiszar and Korner,[5] where the knowledge of $p(v|y')$ is not required. In the case of decoding (25), one tries to find such a $t_{a'^J}(w^N(m',k))$, when the statistics of a dummy channel Q' coincides with $p(v|y')$ for a given P. This also corresponds to the case, when the decoder besides the message decoding can establish the parameters of the applied transformation.

In this case, an error happens if the codeword $w^N(m,k)$ was transmitted and distorted by some geometrical transformation $a^J \in \mathcal{A}^J$ to $t_{a^J}(w^N(m,k))$, but there exists the following situation for some Q' that:

$$v^N \in T^N_{P,Q}(V|t_{a^J}(w^N(m,k))) \bigcap T^N_{P,Q'}(V|t_{a'^J}(w^N(m',k))) \text{ and } D(Q'||p(v|y')|P) \le D(Q||p(v|y')|P). \tag{26}$$

Let $\mathcal{D}$ denote a set of Q and Q' distributions for which (26) is valid. Then, the probability of decoding error for the data-hider is given by:

$$p_e \le p\left(\bigcup_{\mathcal{D}}\left(\left(\bigcup_{a^J\in\mathcal{A}^J} T^N_{P,Q}(V|t_{a^J}(w^N(m,k)))\right)\bigcap\left(\bigcup_{m'\neq m}\bigcup_{a'^J\in\mathcal{A}^J} T^N_{P,Q'}\left(V|t_{a'^J}(w^N(m',k))\right)\right)\right)|w^N(m,k)\right),$$

$$= p\left(\bigcup_{\mathcal{D}}\bigcup_{a^J\in\mathcal{A}^J}\bigcup_{a'^J\in\mathcal{A}^J}\left(T^N_{P,Q}(V|t_{a^J}(w^N(m,k)))\bigcap\left(\bigcup_{m'\neq m} T^N_{P,Q'}\left(V|t_{a'^J}(w^N(m',k))\right)\right)\right)|w^N(m,k)\right). \tag{27}$$

According to the justification presented in the beginning of this Section one has the equivalence of two transition probabilities $p(v^N|y'^N)$ and $p(v^N|w^N)$ and since $p(v^N|y'^N)$ is constant for a fixed P and Q (8), (27) is upper bounded by:

$$\sum_{\mathcal{D}}\sum_{a^J\in\mathcal{A}^J}\sum_{a'^J\in\mathcal{A}^J}\left|T^N_{P,Q}(V|t_{a^J}(w^N(m,k)))\bigcap\left(\bigcup_{m'\neq m} T^N_{P,Q'}(V|t_{a'^J}(w^N(m',k)))\right)\right|p(v^N|y'^N). \tag{28}$$

Then according to (24) from the packing lemma and (28) can be upper bounded as:

$$\begin{aligned}
p_e &\le |\mathcal{A}^J||\mathcal{A}^J|\sum_{\mathcal{D}}\exp\{NH(V|Y')\}\exp\{-N(E-D(Q'||p(v|y')|P))\}\times\\
&\times \exp\{-N(H(V|Y')+D(Q||p(v|y')|P))\},\\
&\le (N+1)^{2|\mathcal{Y}'||\mathcal{V}|}|\mathcal{A}^J||\mathcal{A}^J|\exp\{N(H(V|Y')-E+D(Q'||p(v|y')|P)-H(V|Y')-D(Q||p(v|y')|P))\}\\
&= (N+1)^{2|\mathcal{Y}'||\mathcal{V}|}|\mathcal{A}^J||\mathcal{A}^J|\exp\{N(D(Q'||p(v|y')|P)-D(Q||p(v|y')|P)-E)\}\\
&= \exp\left\{-N\left(E-D(Q'||p(v|y')|P)+D(Q||p(v|y')|P)-2|\mathcal{Y}'||\mathcal{V}|\frac{\ln(N+1)}{N}-\frac{2\ln\left(|\mathcal{A}^J|\right)}{N}\right)\right\}\\
&\le \exp\{-N(E-\delta)\},
\end{aligned} \tag{29}$$

as $N \to \infty$. Result in (29) can be interpreted as follows: In case when the applied geometrical transformation belong to a set of finite cardinality $|\mathcal{A}^J|$ that is not exponential in N and that there are as many distinct codewords as given by (23) from a particular type class $T^N_P(Y')$ satisfying (24), p_e will be asymptotically bounded by (29).

4.2. Sphere packing bound for E-capacity of data hiding channels with geometrical attacks

For a given data hiding channel $p(v^N|w^N)$ with geometrical transformation part $y' = t_{a^J}(w)$, where a^J is from a set of finite cardinality $|\mathcal{A}^J|$, and succeeding DMC equivalent part $p(v|y')$, as $E > 0$, the E-capacity $C(E, p(v|y'))$ is upper bounded by the sphere packing bound $R_{sp}(E, p(v|y'))$ as[8]:

$$C_{max}(E, p(v|y')) \leq \overline{C}(E, p(v|y')) \leq R_{sp}(E, p(v|y')), \tag{30}$$

where

$$\begin{aligned} R_{sp}(P, E, p(v|y')) &\triangleq \min_{Q: D(Q||p(v|y')|P) \leq E} I(Y'; V) \\ R_{sp}(E, p(v|y')) &\triangleq \max_P R_{sp}(P, E, p(v|y')). \end{aligned} \tag{31}$$

Proof of the sphere packing bound: Let $E > \delta > 0$ and a (ϕ, ψ)-code of length N is defined with rate R. We would like to upper bound the average probability of error for the data-hider, who has access to the codebook for the key $K = k$ and performing the decoding considering codewords $m \in \mathcal{M}$ from the codebook for $K = k$ and their reproductions for each geometrical attack $a^J \in \mathcal{A}^J$ by:

$$\overline{p_e} = \frac{1}{|\mathcal{M}|} \frac{1}{|\mathcal{A}^J|} \sum_{m \in \mathcal{M}} \sum_{a^J \in \mathcal{A}^J} p\{\mathcal{V}^N - \psi^{-1}(m, k) | w^N(m, k)\} \leq \exp(-N(E - \delta)). \tag{32}$$

Remembering the fact that all codewords, which are to be partitioned into all codebooks, are generated simultaneously from the same distribution $p(w)$ and the applied geometrical attack does not change the type of its input W^N, total number of codewords in all codebooks and their geometrical reproductions for each $a^J \in \mathcal{A}^J$ can be defined by summing the numbers of codewords from each type as:

$$|\mathcal{M}||\mathcal{A}^J| = \sum_P \left| t_{\mathcal{A}^J}(\phi(\mathcal{M}, k)) \bigcap T_P^N(Y') \right|. \tag{33}$$

Since the number of types is upper bounded by $(N+1)^{|\mathcal{Y}'|}$, there is a "major type" such that:

$$\left| t_{\mathcal{A}^J}(\phi(\mathcal{M}, k)) \bigcap T_{P^*}^N(Y') \right| \geq |\mathcal{M}||\mathcal{A}^J|(N+1)^{-|\mathcal{Y}'|}. \tag{34}$$

Considering only codewords of the "major type", average probability of error for the data-hider will be:

$$\begin{aligned} \sum_{a^J \in \mathcal{A}^J} \sum_{m: t_{a^J}(\phi(m,k)) \in T_{P^*}^N(Y')} & p\left(T_{P^*,Q}^N(V | t_{a^J}(w^N(m,k))) - \psi^{-1}(m,k) | w^N(m,k)\right) \\ & \leq |\mathcal{M}||\mathcal{A}^J| \exp\{-N(E - \delta)\}. \end{aligned} \tag{35}$$

Due to the properties of types[5] and using the same argument as in the proof of the random coding bound, probability of error in the summation term of (35) can be written in terms of the cardinality of the set and the conditional probability as:

$$\begin{aligned} & \sum_{a^J \in \mathcal{A}^J} \sum_{m: t_{a^J}(\phi(m,k)) \in T_{P^*}^N(Y')} \left\{ \left| T_{P^*,Q}^N(V | t_{a^J}(w^N(m,k))) \right| - \right. \\ & \left. - \left| T_{P^*,Q}^N(V | t_{a^J}(w^N(m,k))) \bigcap \psi^{-1}(m,k) \right| \right\} p(v^N | y'^N) \leq |\mathcal{M}||\mathcal{A}^J| \exp\{-N(E - \delta)\}, \\ & \sum_{a^J \in \mathcal{A}^J} \sum_{m: t_{a^J}(\phi(m,k)) \in T_{P^*}^N(Y')} \left| T_{P^*,Q}^N(V | t_{a^J}(w^N(m,k))) \right| - \frac{|\mathcal{M}||\mathcal{A}^J| \exp(-N(E - \delta))}{\exp\{-N(D(Q||p(v|y')|P^*) + H(V|Y'))\}} \leq \\ & \sum_{a^J \in \mathcal{A}^J} \sum_{m: t_{a^J}(\phi(m,k)) \in T_{P^*}^N(Y')} \left| T_{P^*,Q}^N(V | t_{a^J}(w^N(m,k))) \bigcap \psi^{-1}(m,k) \right|. \end{aligned} \tag{36}$$

Since the decoding regions are assumed to be disjoint, the right hand side of the inequality (36) can be upper bounded by $|T^N_{P^*,Q}(V)|$. Thus, (36) becomes:

$$\left|t_{\mathcal{A}^J}(\phi(\mathcal{M},k))\bigcap T^N_{P^*}(Y')\right|(N+1)^{-|\mathcal{Y}'||\mathcal{V}|}\exp\{NH(V|Y')\} - |\mathcal{M}||\mathcal{A}^J|\exp(-N(E-\delta))\times \\ \exp\left\{N\left(D(Q||p(v|y')|P^*)+H(V|Y')\right)\right\} \leq \exp\{NH(V)\}. \quad (37)$$

Putting the inequality $\left|t_{\mathcal{A}^J}(\phi(\mathcal{M},k))\bigcap T^N_{P^*}(Y')\right| \geq |\mathcal{M}||\mathcal{A}^J|(N+1)^{-|\mathcal{Y}'|}$ from (34) into (37), one gets:

$$\begin{aligned} &|\mathcal{M}||\mathcal{A}^J|(N+1)^{-|\mathcal{Y}'|}(N+1)^{-|\mathcal{Y}'||\mathcal{V}|}\exp\{NH(V|Y')\} - |\mathcal{M}||\mathcal{A}^J|\times \\ &\times\exp\left\{N(D(Q||p(v|y')|P^*)+H(V|Y')-E+\delta)\right\} \leq \exp\{NH(V)\} \\ &|\mathcal{M}| \leq \frac{\exp\{NH(V)\}\exp\left\{-N\left(H(V|Y')+\frac{\ln(|\mathcal{A}^J|)}{N}\right)\right\}}{(N+1)^{-|\mathcal{Y}'|(|\mathcal{V}|+1)}-\exp\left(N\left(D(Q||p(v|y')|P^*)-E+\delta\right)\right)} \\ &|\mathcal{M}| \leq \frac{\exp\left\{N\left(I(Y';V)-\frac{\ln(|\mathcal{A}^J|)}{N}\right)\right\}}{(N+1)^{-|\mathcal{Y}'|(|\mathcal{V}|+1)}-\exp\left(N\left(D(Q||p(v|y')|P^*)-E+\delta\right)\right)} \end{aligned} \quad (38)$$

Taking $\frac{1}{N}\ln$ of the right and left parts of (38), one gets the sphere packing bound on the E-capacity as:

$$R \leq I(Y';V) - \frac{\ln(|\mathcal{A}^J|)}{N} - \frac{\ln(B)}{N}, \quad (39)$$

where $B = (N+1)^{-|\mathcal{Y}'|(|\mathcal{V}|+1)} - \exp\left(N\left(D(Q||p(v|y')|P^*)-E+\delta\right)\right)$ and $R = \frac{1}{N}\ln|\mathcal{M}|$. Therefore, provided that $D(Q||p(v|y')|P^*) < E-\delta$, $\frac{\ln(|\mathcal{A}^J|)}{N}$ and $\frac{\ln(B)}{N}$ terms in (39) diminish as $N \to \infty$. Then, the upper bound on R can be minimized by the choice of conditional type Q.

5. CONCLUSIONS AND FUTURE RESEARCH PERSPECTIVES

In this paper, we have provided an E-capacity analysis for data hiding channels with geometrical attacks from the positions of sphere packing upper bound and random coding lower bound on the E-capacity. We considered the group of geometrical attacks that do not change the dimensionality and type of their input and do not require an interpolation.

For the asymptotic case, we have shown that given results for the achievable rate of reliable communications through data hiding channels with geometrical attacks coincide with the previous results for the case when there is no geometrical attack at all applied to the stego data.

A future extension of the current work would be for the data hiding scenarios, where the host state is available at the encoder for the generation of watermark codewords. Moreover, consideration of data hiding channels with geometrical attacks that change the dimension and type of their input would be another future work.

ACKNOWLEDGMENTS

This paper was partially supported by SNF Professeur Boursier grant PP002–68653, by the European Commission through the IST Programme under contract IST-2002-507932-ECRYPT and Swiss IM2 projects.

REFERENCES

1. I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*, Morgan Kaufmann Publishers, Inc., San Francisco, 2001.
2. N. Merhav, "An information-theoretic view of watermark embedding-detection and geometric attacks," June 2005. invited talk, presented at WaCha 2005, Barcelona, Spain.
3. P. Moulin, "A detection-theoretic and computational framework for designing geometrically resilient watermarking systems," June 2005. invited talk, presented at WaCha 2005, Barcelona, Spain.
4. E. Topak, S. Voloshynovskiy, O. Koval, M. Mihcak, and T. Pun, "Towards geometrically robust data-hiding with structured codebooks," *ACM Multimedia Systems Journal, Special Issue on Multimedia and Security* , 2005. published online at http://www.springerlink.com/media/b0cyhc8uyk4jph8ugt33/contributions/f/4/3/9/f4392u5p824845t5.pdf.
5. I. Csiszar and J. Korner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Academic Press, New York, 1981.
6. T. Cover and J. Thomas, *Elements of Information Theory*, Wiley and Sons, New York, 1991.
7. E. Topak, S. Voloshynovskiy, O. Koval, and T. Pun, "Achievable rate analysis of geometrically robust data-hiding codes in asymptotic set-ups," in *EUSIPCO-2005, 13th European Signal Processing Conference*, (Antalya, Turkey), September 4-8 2005.
8. M. Haroutunian and S. A. Tonoyan, "Random coding bound of information hiding E-capacity," in *Transactions of IEEE International Symposium on Information Theory*, (Chicago, USA), 2004.