ACHIEVABLE RATE ANALYSIS OF GEOMETRICALLY ROBUST DATA-HIDING CODES IN ASYMPTOTIC SET-UPS

Emre Topak, Sviatoslav Voloshynovskiy, Oleksiy Koval and Thierry Pun

Centre Universitaire d'Informatique (CUI), Université de Genève
24, rue du Général-Dufour
CH-1211 Genève 4, Switzerland

ABSTRACT

Geometrical transformations bring synchronization problems into the robust digital data-hiding. Previous works on this subject were concentrated on the robustness to particular geometrical transformations. In this paper, the achievable rates of reliable robust data-hiding in channels with geometrical transformations are investigated from an information-theoretic point of view for theoretical set-ups, where lengths of data sequences asymptotically approach infinity.

1. INTRODUCTION

Digital data-hiding is the art of information communication by embedding it into some digital multimedia documents. Being embedded this information should be reliably decodable even some intentional and unintentional attacks were applied to the marked document. Geometrical transformations belong to a class of such attacking strategies that lead to the significant complication or even complete failure of the decoding due to the desynchronization between the encoder and the decoder.

Although geometrical transformations are easily implementable, the decoder in a classical communications set-up without a synchronization framework has to perform decoding by considering all possible geometrical transformations. Low computational complexity of implementation for the attacker in contrast to the high computational complexity of recovery for the data-hider makes the issue of geometrical transformations a fundamental challenge in the design of robust data-hiding systems.

In previous research on the robust data-hiding in channels with geometrical transformations, the main focus was on the robustness to a particular class of geometrical transformations, like general affine transformation [1], [2] and to geometrical transformations on the local level [3]. However, the analysis of achievability of reliable robust data-hiding that is measured in terms of probability of decoding error has not been studied yet. Thus, the aim of this paper is to perform an information-theoretic analysis of the robust data-hiding under geometrical attacks from the point of view of the achievable rate. The analysis is carried out for the *theoretic set-ups*, where the lengths of communicated sequences asymptotically approach infinity.

The rest of the paper is organized as follows. In Section 2, information-theoretic analysis of data-hiding is performed. Afterwards, in Section 3, modeling of geometrical attacks is considered. In Section 4, achievability of data-hiding in channels with geometrical transformations is investigated. Conclusions and future research directions are given in Section 5.

Notations. We use capital letters X to denote scalar random variables, bold capital letters $\mathbf{X}$ to denote vector random variables, corresponding small letters x and $\mathbf{x}$ to designate the realization of scalar and vector random variables, respectively. The superscript N is used to denote length-N vectors $\mathbf{x} = x^N = \{x[1], x[2], \ldots, x[N]\}$ with i^{th} element $x[i]$. 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 $\mathscr{X}$ denote sets $X \in \mathscr{X}$ and $|\mathscr{X}|$ denotes the cardinality of the set $\mathscr{X}$. $\mathbb{Z}$ and $\mathbb{R}$ stand for the sets of integers and real numbers, respectively. $H(X)$ denotes the entropy of a random variable X and $I(X;Y)$ designates the mutual information between random variables X and Y.

2. INFORMATION-THEORETIC ANALYSIS OF DATA-HIDING

Block diagram of a generic data-hiding is presented in Fig. 1.

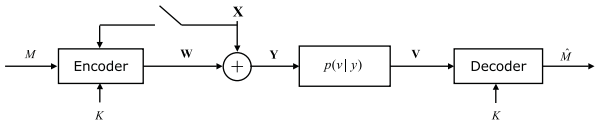

Figure 1: Communication set-up for data-hiding.

A stego data $\mathbf{y} \in \mathscr{Y}^N$ of length N is obtained by adding a watermark sequence $\mathbf{w} \in \mathscr{W}^N$ to a cover data $\mathbf{x} \in \mathscr{X}^N$ according to:

$$\mathbf{Y} = \mathbf{W} + \mathbf{X}. \tag{1}$$

$\mathbf{W}$ is generated by the encoder based on the message index M that is uniformly distributed over the set $\mathscr{M} = \{1, 2, \ldots, |\mathscr{M}|\}$, where $|\mathscr{M}| = 2^{NR}$, the key $K \in \mathscr{K} = \{1, 2, \ldots, |\mathscr{K}|\}$, and, possibly, the cover data $\mathbf{X}$. $R = \frac{1}{N}\log_2|\mathscr{M}|$ is the rate of communications.

The realization of the key determines a particular codebook to be used at both encoder and decoder during communications. The codebooks are generated randomly and revealed to the encoder and the decoder with the knowledge of corresponding keys.

Depending on whether or not non-causal host state information $\mathbf{X}$ is taken into account in the watermark sequence generation, the *random binning* and the *random coding* are used for codebook design, respectively. In the random coding, Fig. 2 [4], the encoder sends the codeword $\mathbf{W}(M,K)$, which corresponds to a particular value of M in the codebook determined by K, as the watermark sequence. In the random binning, Fig. 3 [5], in the codebook defined by K, the encoder looks in the bin determined by M for a codeword $\mathbf{U}$,

which is jointly-typical with $\mathbf{X}$ [5]. After finding the jointly-typical $(\mathbf{U},\mathbf{X})$ pair, the encoder maps them to the watermark sequence $\mathbf{W}(M,\mathbf{X},K)$ according to a probabilistic mapping $p(\mathbf{w}|\mathbf{u},\mathbf{x})$.

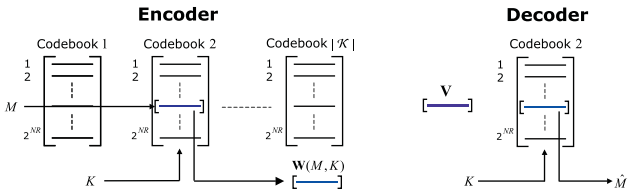

Figure 2: Communications scenario based on random coding.

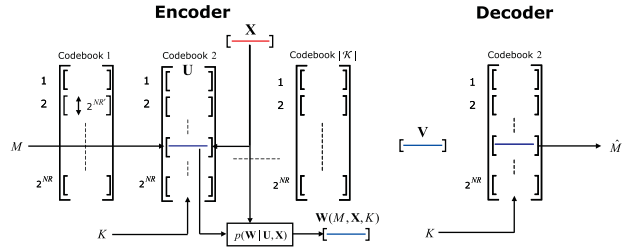

Figure 3: Communications scenario based on random binning.

The watermark sequence combined with the host data is sent to the discrete memoryless channel (DMC) that converts the input $\mathbf{Y}$ to the output $\mathbf{V}$ in a probabilistic manner according to the channel transition probability $p(\mathbf{v}|\mathbf{y}) = \prod_{i=1}^{N} p(v_i|y_i)$.

At the decoder, $\widehat{M}$ is decoded from $\mathbf{V}$ with the knowledge of K. In the random coding, the decoder looks through the codebook defined by K for the codeword $\mathbf{W}(\widehat{M},K)$ which is jointly typical with $\mathbf{V}$. When such a unique codeword $\mathbf{W}(\widehat{M},K)$ is found, the index $\widehat{M}$ is declared as the decoded message. In the random binning, the decoder looks for a codeword $\mathbf{U}$ that is jointly-typical with $\mathbf{V}$ in the $K-$defined codebook. When such a unique codeword $\mathbf{U}$ is found, the index $\widehat{M}$ of the bin that contains $\mathbf{U}$ is considered as the decoded message.

3. MODELING OF GEOMETRICAL ATTACKS

When a geometrical transformation $T_A(.)$ is applied to $\mathbf{Y}$, pixel coordinates of $\mathbf{Y}$ are modified accordingly[1]. The result $\mathbf{V}$ of these operations is called the attacked data:

$$\mathbf{V} = T_A(\mathbf{Y}), \tag{2}$$

where the subscript A represents the type of the geometrical transformation applied to $\mathbf{Y}$. Affine, bilinear and projective transformations are examples of types that A can take.

A can be parameterized by a set of J parameters $\mathbf{a} = (a_1,a_2,\ldots,a_J)$ such that $\mathbf{a} \in \mathbb{Z}^{J}$[2]. For example, when A takes the form of affine transformation, a pixel at the coordinates (n_1,n_2) in $\mathbf{Y}$, i.e. $y[n_1,n_2]$, will be transferred to new coordinates (n_1',n_2') in $\mathbf{V}$, i.e. $v[n_1',n_2']$, according to:

$$\begin{bmatrix} n_1' \\ n_2' \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} n_1 \\ n_2 \end{bmatrix} + \begin{bmatrix} a_5 \\ a_6 \end{bmatrix}. \tag{3}$$

In this case, $\mathbf{a} = (a_1,a_2,a_3,a_4,a_5,a_6)$. If we assume that Fig. 4 represents the space $\mathscr{A}$ of all possible geometrical transformations, then a particular transformation $\mathbf{A} = \mathbf{a}$ will be represented by a dot in this space. Total number of elements in this space is defined by the cardinality $|\mathscr{A}|$.

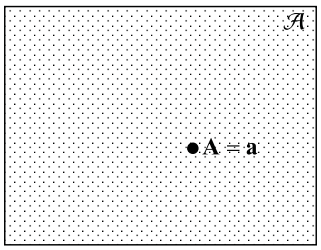

Figure 4: The space $\mathscr{A}$ of possible geometrical tranformations and its element $\mathbf{A} = \mathbf{a}$.

However, in practical data-hiding applications due to the visual acceptability constraint, an intentional geometrical attack space would not include all elements of $\mathscr{A}$ defined above. Nevertheless, to be general, the set of $-$typical geometrical transformations [4], $\mathscr{A}^{(J)}(A)$, will be considered as the space of possibly applied geometrical transformations, with $|\mathscr{A}^{(J)}| < |\mathscr{A}|$. In the case when $\mathbf{a} \in \mathbb{R}^J$, the volume of the set is referred to instead of cardinality.

If the parameters of $\mathbf{a} = (a_1,a_2,\ldots,a_J)$ are distributed independently and identically according to $p(a)$, then, $|\mathscr{A}^{(J)}|$ will be upper bounded as [4]:

$$|\mathscr{A}^{(J)}| \leq 2^{J(H(A)+\ )}, \tag{4}$$

where $H(A) = -\ \ p(a)\log_2 p(a)$ and the summation is performed over the set of values that a can take.

4. ACHIEVABLE RATE OF DATA-HIDING IN CHANNELS WITH GEOMETRICAL TRANSFORMATIONS

Consider a theoretical communications set-up where the length of data sequences goes to infinity, i.e. $N \rightarrow\ \ $, and the decoder neither has a geometrical synchronization framework for recovery nor a priori knowledge about the applied geometrical transformation. It is inevitable for this decoder to regard all elements of $\mathscr{A}^{(J)}$ as a possibly applied one and, thus, to perform an exhaustive decoding for each $\mathbf{a} \in \mathscr{A}^{(J)}$.

In the following Sections, achievability of reliable communications in channels with geometrical transformations is analyzed for the random coding and the random binning strategies starting from a communications scenario without any geometrical transformations. Reliability of the communications is measured by the probability of decoding error, P_e, that is the probability that the decoded message $\widehat{M}$ is not equal to the sent message M, i.e. $Pr\left[\widehat{M} \neq m | M = m\right]$.

[1] It should be noticed here that we did not assume memory effects in the channel due to the intersymbol interference caused by the interpolation.

[2] In general, one can assume $\mathbf{a} \in \mathbb{R}^J$.

4.1 Communication set-ups based on random coding

In the case of random coding, the decoder will make a decoding error in following situations [4]:

- *There is not any codeword* $\mathbf{W}$*, which is jointly-typical with* $\mathbf{V}$ *in the codebook determined by* K: According to the asymptotic equipartition property (AEP) [4], this event is unlikely.
- *Another codeword* $\mathbf{W}'$ *from the codebook such that* $(\mathbf{W}' \neq \mathbf{w}|\mathbf{W} = \mathbf{w})$ *is jointly-typical with* $\mathbf{V}$: According to the AEP, any $\mathbf{W}'$ from the $K-$defined codebook and $\mathbf{V}$ constitutes a jointly typical pair with the probability $2^{-N(I(W;V|K)- \ )}$, where is an arbitrary small positive number, i.e. $\to 0$. Since there are $\left(2^{NR_{RC}}-1\right)$ different $\mathbf{W}'$ apart from $\mathbf{W}' = \mathbf{w}$ in a particular codebook, the probability of decoding error in the random coding case, $P_e^{RC(N)}$, is upper bounded by:

$$P_e^{RC(N)} \leq 2^{NR_{RC}} 2^{-N(I(W;V|K)- \ )}, \tag{5}$$

where R_{RC} is the random coding-based communication rate in channels without geometrical transformations. If R_{RC} satisfies the condition:

$$R_{RC} \leq I(W;V|K) - \ , \tag{6}$$

then, $P_e^{RC(N)} \to 0$, as $N \to$ and $\to 0$.

Furthermore, when the decoding is performed at all elements of the space $\mathscr{A}^{(J)}$, the upper bound in (5) becomes:

$$\begin{aligned} P_e^{RC(N)} &\leq |\mathscr{A}^{(J)}| 2^{NR_{RC}^G} 2^{-N(I(W;V|K)- \ )}, \\ &\leq 2^{N\frac{1}{N}\log_2|\mathscr{A}^{(J)}|} 2^{NR_{RC}^G} 2^{-N(I(W;V|K)- \ )}, \\ &\leq 2^{N(\frac{1}{N}\log_2|\mathscr{A}^{(J)}| + R_{RC}^G - (I(W;V|K)- \ ))}, \end{aligned} \tag{7}$$

where R_{RC}^G is the random coding-based communication rate in channels with geometrical transformations. Therefore, if R_{RC}^G satisfies the condition:

$$R_{RC}^G \leq I(W;V|K) - \ - \frac{1}{N}\log_2|\mathscr{A}^{(J)}|, \tag{8}$$

$P_e^{RC(N)} \to 0$, as $N \to$ and $\to 0$. Moreover, taking (4) into account, (8) can be rewritten in the following form:

$$R_{RC}^G \leq I(W;V|K) - \ - \frac{J(H(A)+ \ )}{N}. \tag{9}$$

As $N \to$ and $\to 0$, $\frac{J(H(A)+ \ )}{N}$ term in (9) vanishes and the upper bound on R_{RC}^G reduces to:

$$R_{RC}^G \leq I(W;V|K) - \ , \tag{10}$$

which coincides with (6) that bounds the rate in channels without geometrical transformations. Consequently, in a theoretical set-up based on random coding scenario, the upper bound on the rate of reliable communications is not affected by applied geometrical transformations[3].

[3] It should be noticed here that we did not assume memory effects in the channel due to the intersymbol interference caused by the interpolation. Obviously, $R_{RC}^G < R_{RC}$ in this case.

4.2 Communication set-ups based on random binning

In the case of random binning, one encounters with a coding error in following situations:

- *There is not any codeword* $\mathbf{U}$ *in the codebook defined by* K *at the encoder, which is jointly-typical with* $\mathbf{X}$: According to the AEP, any codeword $\mathbf{U}$ and $\mathbf{X}$ may form a jointly-typical pair with the probability $2^{-N(I(U;X|K)- \ )}$. Since there are $2^{NR'}$ codewords $\mathbf{U}$ for any M in a particular codebook defined by K, the probability of this event will be bounded by

$$\begin{aligned} P_e^{RB(N)} &\leq (1-2^{-N(I(U;X|K)- \ )})^{2^{NR'}}, \\ &\leq \exp(-2^{N(R'-I(U;X|K)+ \ )}), \end{aligned} \tag{11}$$

where we used the fact that $(1-x)^n \leq e^{-nx}$. If $R' > I(U;X|K) - \ $, $P_e^{RB(N)} \to 0$ as $N \to$ and $\to 0$.
- *There is not any codeword* $\mathbf{U}$ *in the* $K-$*defined codebook, which is jointly-typical with* $\mathbf{V}$: According to the AEP, this event is unlikely.
- *A codeword* $\mathbf{U}$ *from another bin* $\widehat{M}$ *such that* $\left(\widehat{M} \neq m|M = m\right)$ *is jointly-typical with* $\mathbf{V}$: According to the AEP, any codeword $\mathbf{U}$ from the codebook defined by K and $\mathbf{V}$ may form a jointly-typical pair with the probability $2^{-N(I(U;V|K)- \ )}$. Since there are $\left(2^{NR_{RB}}-1\right)$ bins in total with an index $\widehat{M}$ such that $\widehat{M} \neq m$, the probability of decoding error in the random binning case, $P_e^{RB(N)}$, is upper bounded by:

$$P_e^{RB(N)} \leq 2^{N[R_{RB}+R']} 2^{-N(I(U;V|K)- \ )}, \tag{12}$$

where $R' = I(U;X|K) +$ and R_{RB} is the random binning-based communication rate in channels without geometrical transformations. If the data-hider communicates with the following condition on R_{RB}:

$$R_{RB} \leq I(U;V|K) - I(U;X|K) - 2 \ , \tag{13}$$

then, $P_e^{RB(N)} \to 0$, as $N \to$ and $\to 0$.

When the decoder performs the decoding at all elements of the space of typical geometrical transformations, $P_e^{RB(N)}$ will be upper bounded by

$$\begin{aligned} P_e^{RB(N)} &\leq |\mathscr{A}^{(J)}| 2^{N[R_{RB}^G+R']} 2^{-N(I(U;V|K)- \ )}, \\ &\leq 2^{N\frac{1}{N}\log_2|\mathscr{A}^{(J)}|} 2^{N[R_{RB}^G + I(U;X|K)+ \ ]} 2^{-N(I(U;V|K)- \ )}, \\ &\leq 2^{N(\frac{1}{N}\log_2|\mathscr{A}^{(J)}| + R_{RB}^G + I(U;X|K)+ \ - (I(U;V|K)- \ ))}, \end{aligned} \tag{14}$$

where R_{RB}^G is the random binning-based communication rate in channels with geometrical transformations. If R_{RB}^G is such that:

$$R_{RB}^G \leq I(U;V|K) - I(U;X|K) - 2 \ - \frac{1}{N}\log_2|\mathscr{A}^{(J)}|, \tag{15}$$

$P_e^{RB(N)} \to 0$, as $N \to$ and $\to 0$. Furthermore, similar to (9), $\frac{1}{N}\log_2|\mathscr{A}^{(J)}|$ term in (15) is eliminated as $N \to$ and the upper bound for R_{RB}^G becomes

$$R_{RB}^G \leq I(U;V|K) - I(U;X|K) - 2 \ , \tag{16}$$

which is equal to the condition on R_{RB} given in (13) for channels without geometrical transformations. Thus, in theoretical set-ups with random binning, the reliable communications do not suffer from geometrical transformations.

5. CONCLUSION

In this paper, it is demonstrated for theoretical set-ups, where data lengths asymptotically approach infinity, using an information-theoretic argument that reliable digital data-hiding in channels with geometrical transformations is possible. Presented achievable rates for each case in channels with and without geometrical transformations allow to conclude that maximum rate of reliable communications is asymptotically the same.

A future extension of this work will be an information-theoretic analysis for *practical set-ups*, in which the data lengths are finite, to investigate the achievability of reliable digital data-hiding in channels with geometrical transformations.

Acknowledgment

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. The authors are also thankful to the members of SIP group for many helpful discussions during group seminars. Special thanks are to K. Mihcak (Microsoft Research, Redmond, USA) for his comments and contributions.

The information in this document reflects only the authors views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

REFERENCES

[1] J. J. K. O. Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking," in *IEEE Int. Conf. on Image Processing ICIP1997*, Santa Barbara, CA, USA, October 1997, pp. 536–539.

[2] M. Kutter, "Digital image watermarking: hiding information in images," Ph.D. dissertation, EPFL, Lausanne, Switzerland, August 1999.

[3] S. Voloshynovskiy, F. Deguillaume, and T. Pun, "Multibit digital watermarking robust against local nonlinear geometrical distortions," in *IEEE Int. Conf. On Image Processing ICIP2001*, Thessaloniki, Greece, October 2001, pp. 999–1002.

[4] T. Cover and J. Thomas, *Elements of Information Theory*. Wiley and Sons, New York, 1991.

[5] S. Gel'fand and M. Pinsker, "Coding for channel with random parameters," *Probl. Control and Inf. Theory*, vol. 9, no. 1, pp. 19–31, 1980.