Lossy Source Coding with Reconstruction Privacy

Kittipong Kittichokechai, Tobias J. Oechtering, and Mikael Skoglund
School of Electrical Engineering and the ACCESS Linnaeus Center
KTH Royal Institute of Technology, Stockholm, Sweden

Abstract—We consider the problem of lossy source coding with side information under a secrecy constraint that the reconstruction sequence at a decoder should be kept secret to a certain extent from another terminal such as an eavesdropper, a sender, or a helper. We are interested in how the reconstruction privacy constraint at a particular terminal affects the rate-distortion tradeoff. In this work, we allow the decoder to use a random mapping, and give inner and outer bounds to the rate-distortion-equivocation region for different cases. In the special case where each reconstruction symbol depends only on the source description and current side information symbol, the complete rate-distortion-equivocation region is characterized. A binary example illustrating a new tradeoff due to the new secrecy constraint, and a gain from the use of randomized decoder is given.

I. INTRODUCTION

With the emergence of Internet of Things (IoT) and the growing predominance of smart devices, we are transitioning into a future scenario where almost everyone and everything will be connected. Significant amount of data will be exchanged among users and service providers which inevitably leads to a privacy concern. A user in the network could receive different versions of certain information from different sources. Apart from being able to process the information efficiently, the user may also wish to protect the privacy of his/her action which is taken based on the received information. In this work, we address a privacy concern of the final action/decision taken at the end-user in an information theoretic setting. More specifically, we consider the problem of lossy source coding under the privacy constraint of the end-user whose goal is to reconstruct a sequence subject to a distortion criterion. The privacy concern of the end-user may arise due to the presence of an external eavesdropper or a legitimate terminal such as a sender or a helper who is curious about the final reconstruction. We term the privacy criterion as end-user privacy, and use the normalized equivocation of the reconstruction sequence at a particular terminal as a privacy measure.

Let us consider Fig. 1 where there exist several agents collecting information for the central unit. Assuming that the agents communicate efficient representations of the correlated sources to the central unit through the rate-limited noiseless links so that the central unit is able to estimate a value of some function of the sources $F(X^n_1, X^n_2, X^n_3)$ satisfying the distortion criterion. However, there is a privacy concern regarding the reconstruction sequence (final decision/action) at the central unit, that it should be kept secret from the agents. This gives rise to a new tradeoff between the achievable rate-distortion pair and privacy of the reconstruction sequence. Potential applications of the illustrated setting include those in the area of distributed cloud services where the end-user (central unit) can process information received from the cloud service providers (agents), while guaranteeing that his/her final action will be kept private from the providers, at least to a certain extent. From the problem formulation point of view, the end-user privacy constraint can also be considered as a complement to the common reconstruction constraint in lossy source coding problems [1] where the reconstruction sequence is instead required to be reproduced at the sender.

In this work, we study a special case of Fig.1 where there are two sources, one of which is available directly at the decoder. We denote by $X^n$ the source to be encoded, and $Y^n$ the unencoded source available at the decoder. Alternatively, we may view $Y^n$ as correlated side information generated from a helper. The reconstruction sequence $\hat{X}^n$ is an estimate of the value of some component-wise function $F^{(i)}(X^n, Y^n)$, where the $i$th component $F^{(i)}(X^n, Y^n) = F(X_i, Y_i)$ for $i = 1, \ldots, n$. Without the end-user privacy constraint, this corresponds to the problem of source coding with side information at the decoder or the Wyner-Ziv problem [2], [3]. We consider three scenarios where the end-user privacy constraint is imposed at different nodes, namely the eavesdropper, the encoder, and the helper, as shown in Fig. 2, 3, and 4. Since the goal of end-user privacy is to protect the reconstruction sequence generated at the decoder against any unwanted inferences, we allow the decoder mapping to be a random mapping. It can be shown by an example that the randomized decoder can improve the achievable equivocation rate as compared to the one derived for the deterministic decoder.

A. Contribution

We study an implication of the end-user privacy on the rate-distortion tradeoff where the privacy constraint is imposed at
different nodes in the system. A summary of contribution is
given below.

- End-user privacy at eavesdropper (Fig. 2): In Section
  II we characterize inner and outer bounds to the rate-
distortion-equivocation region for the cases where the
side information is available non-causally and causally
at the decoder. In a special case where the decoder has
no memory, that is, each reconstruction symbol depends
only on the source description and current side information
symbol, the complete characterization of the rate-
distortion-equivocation region is given.
- End-user privacy at encoder (Fig. 3): This setting is
  included in Fig. 2 when \( Z^n = X^n \). The results can be
  obtained from those of the setting in Fig. 2.
- End-user privacy at helper (Fig. 4): Inner and outer
  bounds to the rate-distortion-equivocation region are
given in Section III.

B. Related Work

The idea of protecting the reconstruction sequence against
an eavesdropper was first considered as an additional secrecy
constraint in the context of coding for watermarking and
encryption in [4] where the author considered a watermarking
setting using a secret key sequence to protect the (watermark)
encryption in [4] where the author considered a watermarking
constraint in the context of coding for watermarking and
an eavesdropper was first considered as an additional secrecy
constraint in Section III.

II. END-USER PRIVACY AT EAVESDROPPER

A. Problem Formulation

We consider a setting in the presence of an external
eavesdropper, as shown in Fig. 2. Source, side information,
and reconstruction alphabets, \( \mathcal{X}, \mathcal{Y}, \mathcal{Z}, \mathcal{X} \) are assumed to
be finite. Let \( (X^n, Y^n, Z^n) \) be \( n \)-length sequences which are i.i.d.
according to \( P_{X,Y,Z} \). A function \( F_i^{(n)}(X^n, Y^n) \) is assumed to
be a component-wise function, where the \( i \)-th component
\( F_i^{(n)}(X^n, Y^n) = F_i(X_i, Y_i) \) for \( i = 1, \ldots, n \) (cf., e.g., [3]).
The end-user privacy at the eavesdropper who has access to
\( W \) and \( Z^n \) is measured by the normalized conditional entropy
\( H(X^n|W, Z^n)/n \). We are interested in characterizing the
optimal tradeoff between rate, distortion, and equivocation of
the reconstruction sequence in terms of the rate-distortion-
equivocation region.

Definition 1: A \((|\mathcal{W}^{(n)}|, n)\)-code for source coding with
end-user privacy consists of:
- an encoder \( f^{(n)} : \mathcal{X}^n \rightarrow \mathcal{W}^{(n)} \),
- a randomized decoder which maps \( w \in \mathcal{W}^{(n)} \) and \( y^n \in
  \mathcal{Y}^n \) to \( \hat{x}^n \in \mathcal{X}^n \) according to \( p(\hat{x}^n|w, y^n) \),
where \( \mathcal{W}^{(n)} \) is a finite set.

Let \( d : \mathcal{X} \times \mathcal{Y} \times \mathcal{X} \rightarrow [0, \infty) \) be the single-letter distortion
measure. The distortion between the value of the function of
source sequence and side information and its estimate at the
decoder is defined as

\[
d^{(n)}(F^{(n)}(X^n, Y^n), \hat{X}^n) \triangleq \frac{1}{n} \sum_{i=1}^{n} d(F(X_i, Y_i), \hat{X}_i),
\]

where \( d^{(n)}(\cdot) \) is the distortion function.

Definition 2: The rate-distortion-equivocation tuple
\((R, D, \Delta) \in \mathbb{R}_+^3 \) is said to be achievable if for any \( \delta > 0 \) and
all sufficiently large \( n \) there exists a \((|\mathcal{W}^{(n)}|, n)\) code such that

\[
\frac{1}{n} \log |\mathcal{W}^{(n)}| \leq R + \delta,
\]

1In ITA 2014, we have learned that equivocation of the reconstruction
sequence was also considered as a secrecy metric in [13] in their contexts.
where $a$ follows from, conditioned on the codebook, we have the Markov chain $\hat{X} - (T^n, Y^n) - (J, K, Z^n)$, and from Fano’s inequality, $(b)$ follows since $(J, K)$ is a function of $X^n$, and that conditioning reduces entropy, $(c)$ from the codebook generation and from bounding the conditional entropy terms (proofs are given in [15]), and $(d)$ from the Markov chains $T - U - X - (Y, Z)$ and $\hat{X} - (U, Y) - (X, T, Z)$.

In the equivocation bound of $R_{\text{in}}^{(c)}$, the first term corresponds to uncertainty of $\hat{X}$ due to the use of randomized decoder. The difference $I(X; Y | T) - I(\hat{X}; Z | T)$ can be considered as an additional uncertainty due to the fact that the eavesdropper observes $Z^n$, but not $Y^n$ which is used for generating $\hat{X}$. From the proof of the outer bound $R_{\text{out}}^{(c)}$, random variable $V$ is related to certain reconstruction symbols and it reflects the fact that conditioned on the source description, the reconstruction process is not necessarily memoryless.

Remark 1: We can relate our result to those of other settings where $F^{(c)}(X^n, Y^n) = X^n$. For example, the inner bound $R_{\text{in}}^{(c)}$ can resemble the optimal results of the following settings.

- **Lossless reconstruction:** When considering the lossless reconstruction of the source $X^n$, it can be shown that our problem reduces to the secure lossless source coding problem considered in [12]. To obtain the rate-equivocation region, we set $\hat{X} = U = X$.

- **Side information privacy:** We observe from the proof that we can obtain the result for the setting with side information privacy in [7] which considers $Z = \emptyset$ (constant), and the privacy constraint on $\frac{1}{n} H(Y^n | W)$. By setting $\hat{X} = Y$ and $T = \emptyset$ in the equivocation constraint, and considering a deterministic decoder in $P_{\text{in}}^{(c)}$, we obtain the complete rate-distortion-equivocation region for the corresponding side information privacy setting.

### C. Causal Side Information

Next we consider the variant of Fig. 2 where the side information $Y^n$ is available only causally at the decoder. This could be relevant in delay-constrained applications as mentioned in [16] and references therein. We consider the following types of reconstructions.

- **Causal reconstruction:** $\hat{X}_i \sim p(\hat{x}_i | w_i, y^{i-1})$ for $i = 1, \ldots, n$.

- **Memoryless reconstruction:** $\hat{X}_i \sim p(\hat{x}_i | w_i, y_i)$ for $i = 1, \ldots, n$.

---

2For the side information privacy setting, $\frac{1}{n} H(Y^n | W)$ is not affected by the decoding mapping. Therefore, randomized decoders are not helpful.
Definition 4: Let \( R_{\text{in}}^{\text{(eve,causal)}} \) be the set of all tuples \( (R, D, \Delta) \in \mathbb{R}^3_+ \) such that
\[
R \geq I(X; U)
\]
\[
D \geq E[d(F(X, Y), \hat{X})]
\]
\[
\Delta \leq H(X|U, Z)
\]
over joint distributions factorized as
\( P_{X,Y,Z}(x,y,z)P_{U|X}(u|x)P_{X|U,Y}(\hat{x}|u, y) \).

Remark 2: For the special case where \( Y = \emptyset \), the rate-distortion-equivocation region is given by \( R_{\text{in}}^{\text{(eve,causal)}} \) with the corresponding set of distributions such that \( Y = \emptyset \). We can see that if the decoder is a deterministic mapping, the achievable equivocation rate is zero since the eavesdropper observes everything the decoder does. However, for some \( D > 0 \), by using the randomized decoder, we can achieve the equivocation rate of \( H(\hat{X}|U, Z) \) which can be strictly positive.

D. Special Case: End-user privacy at the encoder

Fig. 2 includes the setting of end-user privacy at the encoder in Fig. 3 as a special case by setting \( Z^n = X^n \) since the source description is a deterministic function of \( X^n \). The above results can readily reduce to the corresponding results for the problems in Fig. 3 as follows.

- Inner bound: The inner bound for the setting in Fig. 3 is obtained from \( R_{\text{in}}^{\text{(eve)}} \) by setting \( Z = X \) and \( T = U \).
- Inner and outer bound for causal reconstruction and the rate-distortion-equivocation region for memoryless reconstruction are obtained from \( R_{\text{in}}^{\text{(eve,causal)}} \) and \( R_{\text{out}}^{\text{(eve,causal)}} \) by setting \( Z = X \).

III. END-USER PRIVACY AT HELPER

Next we consider the setting in Fig. 4 where the end-user privacy is imposed at the helper who provides side information \( Y^n \) to the decoder. We are interested in how the decoder should utilize the correlated side information in the reconstruction while keeping the reconstruction sequence secret from the helper. The problem formulation and definition of the code are similar as before, except that the end-user privacy constraint is now at the helper, i.e., \( H(\hat{X}^n|Y^n) \geq \Delta - \delta \).

Definition 5: Let \( R_{\text{in}}^{\text{(helper)}} \) be the set of all tuples \( (R, D, \Delta) \in \mathbb{R}^3_+ \) such that
\[
R \geq I(X; U|Y)
\]
\[
D \geq E[d(F(X, Y), \hat{X})]
\]
\[
\Delta \leq H(\hat{X}|U, Y) + I(X; \hat{X}|Y)
\]
over joint distributions factorized as
\( P_{X,Y,Z}(x,y,z)P_{U|X}(u|x)P_{X|U,Y}(\hat{x}|u, y) \).

Remark 3: One example showing that randomized decoder can enlarge the rate-distortion-equivocation region is when \( Y = X \) in Fig. 4. Since the source is available completely at
the decoder, the zero rate is achievable. In this case, we have that $\mathcal{R}_{\text{help}}$ is given by $\mathcal{R}_{\text{in}}^{(\text{help})}$ where $X = Y$ and $U = \emptyset$. For any positive $D$, the randomized decoder could randomly put out a reconstruction sequence that still satisfies the distortion level $D$, and achieve a positive equivocation rate as opposed to the zero equivocation in the case of deterministic decoder.

IV. Binary Example

In this section, we consider an example illustrating the potential gain from allowing the use of randomized decoder. Specifically, we consider the setting in Fig. 2 under memoryless reconstruction and assumptions that $Z = \emptyset$ and $F(X,Y) = X$. Then, we evaluate the corresponding result in Proposition 3.

Let $\mathcal{X} = \{0,1\}$ be binary source and reconstruction alphabets. We assume that the source symbol $X$ is distributed according to Bernoulli(1/2), and side information $Y \in \{0,1,e\}$ is an erased version of the source with an erasure probability $p_e$. The Hamming distortion measure is assumed, i.e., $d(x,\hat{x}) = 1$ if $x \neq \hat{x}$, and zero otherwise. Inspired by the optimal choice of $U$ in the Wyner-Ziv result [2], we let $U$ be the output of a BSC($p_u$), $p_u \in [0,1/2]$ with input $X$. The reconstruction symbol generated from a randomized decoder is chosen s.t. $\hat{X} = Y$ if $Y \neq e$, otherwise $\hat{X} \sim P_{\hat{X}|U}$, where $P_{\hat{X}|U}$ is modelled as a BSC($p_2$), $p_2 \in [0,1/2]$. With these assumptions at hand, the inner bound to the rate-distortion-equivocation region in Proposition 3 can be specialized as

$$\mathcal{R}_{\text{in},\text{random}} = \{(R, D, \Delta) | R \geq 1 - h(p_u), \quad D \geq p_e(1 - p_2) + (1 - p_e)h, \quad \Delta \leq h(p_u(1 - p_e) + p_2p_e) \}$$

for some $p_u, p_2 \in [0,1/2]$, where $h(\cdot)$ is a binary entropy function and $a \ast b \triangleq a(1-b) + (1-a)b$.

For comparison, we also evaluate the inner bound for the case of the Wyner-Ziv optimal deterministic decoder by setting $p_2 = 0$. We plot the achievable minimum distortion as a function of equivocation rate for a fixed $R = 0.7136$, where $p_e = 0.5$. Fig. 5 shows the tradeoff between achievable minimum distortion and equivocation rate for a fixed rate $R$. We can see that in general the minimum distortion is sacrificed for a higher equivocation. For the same particular structure of $P_{U|X}$ and the given deterministic decoder in this setting, it shows that, for a given rate $R$ and distortion $D$, a higher equivocation rate $\Delta$ can be achieved by using a randomized decoder. As for the low equivocation region, we observe a saturation of distortion because the minimum distortion is limited by the rate. The value $\Delta_{\text{sat}}$ at which the minimum distortion cannot be lowered by decreasing $\Delta$ can be specified as $\Delta_{\text{sat}} = h((1 - p_e)h^{-1}(1 - R))$, and the corresponding $D_{\text{max}}(R, \Delta_{\text{sat}}) = p_e(1 - p_e)h^{-1}(1 - R)$ is the minimum distortion according to the Wyner-Ziv rate-distortion function.

In the special case where $Y = \emptyset$, the gain can be shown as follows (cf. Remark 2). If the decoder is a deterministic mapping, the achievable equivocation rate is always zero since the eavesdropper is as strong as the decoder. The corresponding distortion-rate function for this example is given by $D \geq h^{-1}(1 - R)$. However, by using the randomized decoder as above, we can achieve $D \geq h^{-1}(1 - R) \ast h^{-1}(\Delta)$ (by letting $p_e = 1$ in $\mathcal{R}_{\text{in},\text{random}}$). For $D = h^{-1}(1 - R) \ast c$, where $c \in (0,1/2]$, we can achieve the equivocation rate $h(c)$ which is strictly positive.

References

[1] Y. Steinberg, “Coding and common reconstruction,” IEEE Trans. Inf. Theory, vol. 55, no. 11, 2009.
[2] A. D. Wyner and J. Ziv, “The rate distortion function for source coding with side information at the decoder,” IEEE Trans. Inf. Theory, vol. IT-22, pp. 1-10, Jan. 1976.
[3] H. Yamamoto, “Wyner-Ziv theory for a general function of the correlated sources,” IEEE Trans. Inf. Theory, vol. 28, no. 5, pp. 803-807, Sep 1982.
[4] N. Merhav, “On joint coding for watermarking and encryption,” IEEE Trans. Inf. Theory, vol. 52, pp. 190-205, Jan. 2006.
[5] N. Merhav, “On the Shannon cipher system with a capacity-limited key-distribution channel,” IEEE Trans. Inf. Theory, vol. 52, pp. 1269-1273, Mar. 2006.
[6] E. Ekrem and S. Ulukus, “Secure lossy source coding with side information,” in Proc. Allerton Conf. Commun. Control Comput., 2011.
[7] R. Tandon, L. Sankar, and H. V. Poor, “Discriminatory lossy source coding: Side information privacy,” IEEE Trans. Inf. Theory, vol. 59, pp. 5665-5677, Sep. 2013.
[8] C. Heegard and T. Berger, “Rate distortion when side information may be absent,” IEEE Trans. Inf. Theory, vol. 31, no. 6, pp. 727-734, Nov. 1985.
[9] V. Prabhakaran and K. Ramchandran, “On secure distributed source coding,” in Proc. IEEE Inf. Theory Workshop, 2007, pp. 442-447.
[10] D. Gündüz, E. Erkip and H. V. Poor, “Lossless compression with security constraints,” in Proc. IEEE ISIT, 2008, Toronto, pp. 111-115.
[11] R. Tandon, S. Ulukus and K. Ramchandran, “Secure source coding with a helper,” IEEE Trans. Inf. Theory, vol. 59, pp. 2178-2187, 2013.
[12] J. Villard and P. Piantanida, “Secure multiterminal source coding with side information at the eavesdropper,” IEEE Trans. Inf. Theory, vol. 59, no. 6, June 2013.
[13] C. Schieler and P. Cuff, “Rate-Distortion Theory for Secrecy Systems,” http://arxiv.org/abs/1305.3905, 2013.
[14] A. El Gamal and Y-H. Kim, Network Information Theory, Cambridge University Press, 2011.
[15] K. Kittichokechai, T. J. Oechtering, and M. Skoglund, “Lossy source coding with reconstruction privacy,” 2014 [Online]. Available: people.kth.se/~kki/enduserpri.pdf
[16] T. Weissman and A. El Gamal, “Source coding with limited-look-ahead side information at the decoder,” IEEE Trans. Inf. Theory, vol. 52, no. 12, pp. 5218-5239, 2006.