Information Embedding with Reversible Stegotext

Orna Sumszyk and Yossef Steinberg
Technion—Israel Institute of Technology
[ornad,ysteinbe]@[tx,ee].technion.ac.il

Introduction

Outline

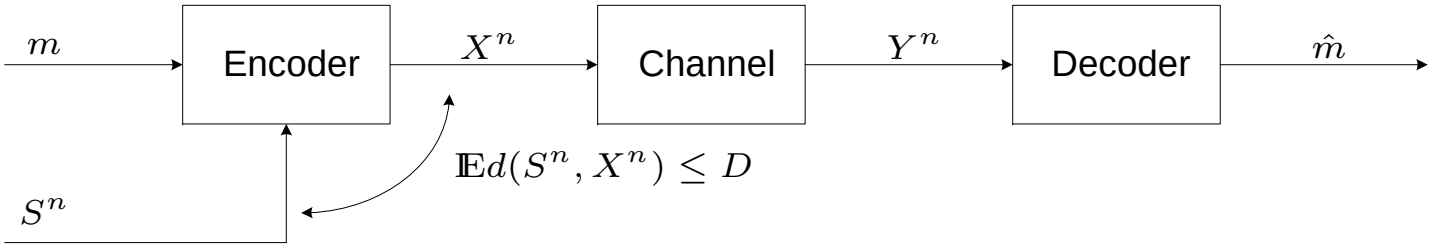
- The general Information Embedding problem
- Reversible Information Embedding
- Stegotext Reversible Information Embedding
- Main result
- Discussion
- Examples
- Iterative algorithm

Introduction
Outline
The Information Embedding (IE) Problem
Reversible IE
Drawbacks of Reversible IE

Stegotext RIE

END

The Information Embedding (IE) Problem



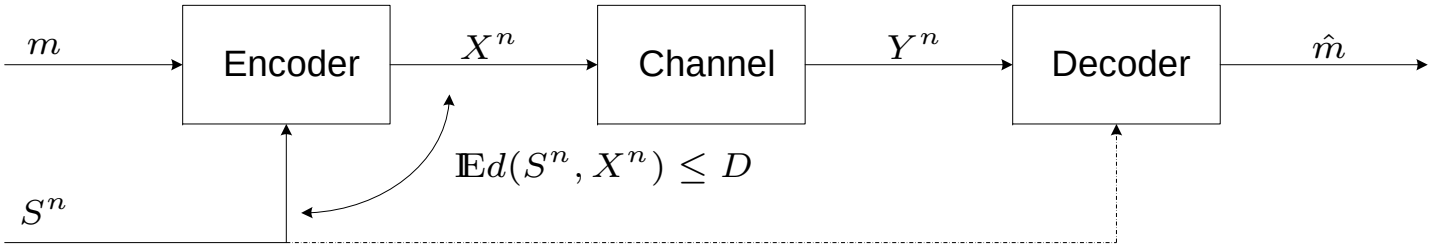
- A message m is embedded into host signal S^n, producing the composite signal or stegotext X^n.
- X^n is transmitted via $P_{Y|X}$ (attack channel) to its destination. (Fixed.)
- At the destination, a noisy version Y^n of the stegotext is received, from which m is decoded.
- In IE, m is embedded into S^n in a manner that is transparent to the unintended observer $\Rightarrow$ a distortion constraint between S^n and X^n.
- Public IE – The host S^n is available only at the encoder.

Introduction
Outline
The Information Embedding (IE) Problem
Reversible IE
Drawbacks of Reversible IE

Stegotext RIE

END

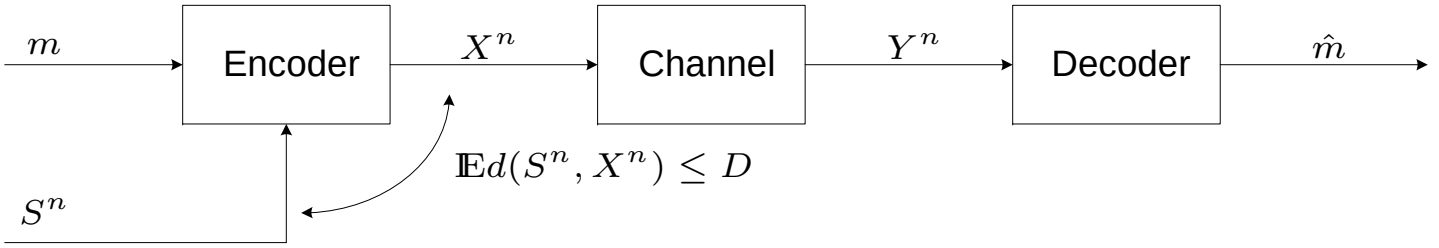
The Information Embedding (IE) Problem



- A message m is embedded into host signal S^n, producing the composite signal or stegotext X^n.
- X^n is transmitted via $P_{Y|X}$ (attack channel) to its destination. (Fixed.)
- At the destination, a noisy version Y^n of the stegotext is received, from which m is decoded.
- In IE, m is embedded into S^n in a manner that is transparent to the unintended observer $\Rightarrow$ a distortion constraint between S^n and X^n.
- Public IE – The host S^n is available only at the encoder.
- Private IE – The host S^n is available at both, encoder and decoder.

Introduction
Outline
The Information Embedding (IE) Problem
Reversible IE
Drawbacks of Reversible IE
Stegotext RIE
END

The IE Problem (cont'd)

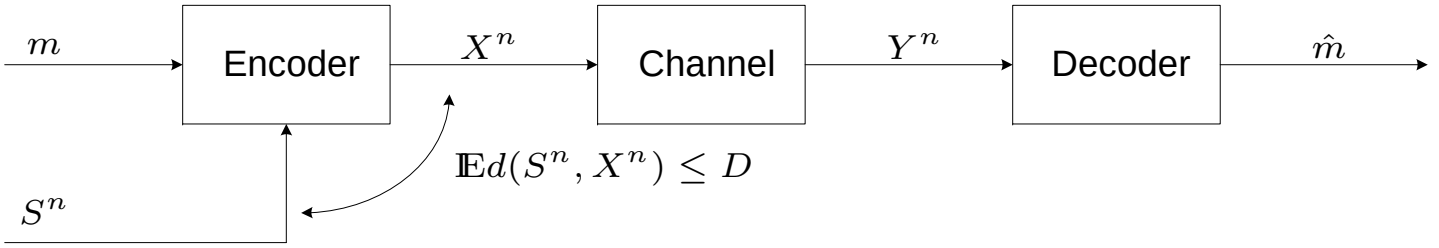


Classical IE – embedding rate vs. input distortion [Moulin & O'Sullivan, 2003]:

$$\mathcal{C}_{ie}(D) = \max_{\mathbb{E}d(S,X) \leq D} [I(U;Y) - I(U;S)]$$

Introduction
Outline
The Information Embedding (IE) Problem
Reversible IE
Drawbacks of Reversible IE
Stegotext RIE
END

The IE Problem (cont'd)



Classical IE – embedding rate vs. input distortion [Moulin & O'Sullivan, 2003]:

$$\mathcal{C}_{ie}(D) = \max_{\mathbb{E}d(S,X)\leq D} [I(U;Y) - I(U;S)]$$

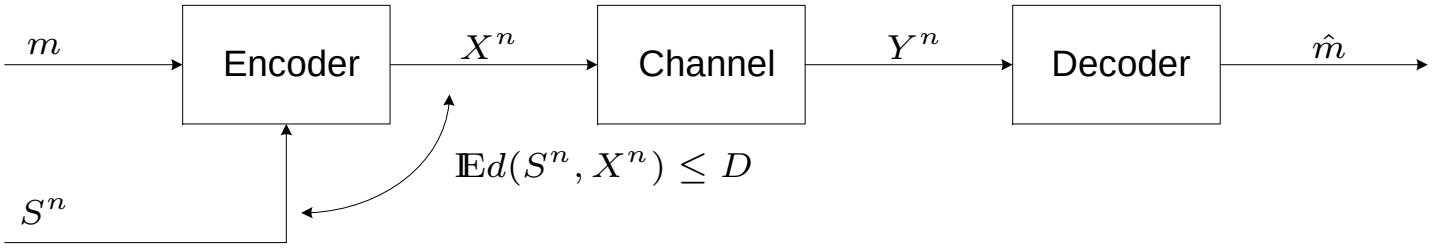
- The host S^n is of value at the destination (the reason for communicating from the first place).
- The destination obtains a noisy version of the stegotext X^n.

Introduction
Outline
The Information Embedding (IE) Problem
Reversible IE
Drawbacks of Reversible IE

Stegotext RIE

END

The IE Problem (cont'd)



Classical IE – embedding rate vs. input distortion [Moulin & O'Sullivan, 2003]:

$$\mathcal{C}_{ie}(D) = \max_{\mathbb{E}d(S,X)\leq D} [I(U;Y) - I(U;S)]$$

- The host S^n is of value at the destination (the reason for communicating from the first place).
- The destination obtains a noisy version of the stegotext X^n.

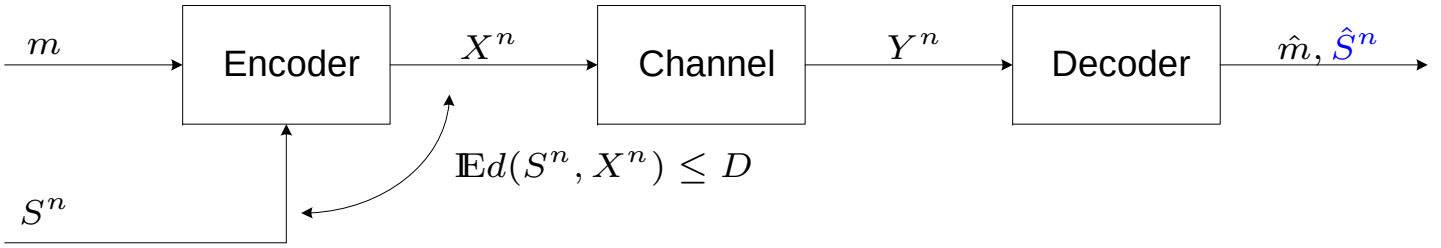
Some applications cannot tolerate high distortion at the destination (e.g., medical imagery).

$\Rightarrow$ Reversible Information Embedding

Introduction
Outline
The Information Embedding (IE) Problem
Reversible IE
Drawbacks of Reversible IE
Stegotext RIE
END

Reversible IE

[Fridrich, Goljan, Du *SPIE* 2002], [Kalker & Willems, Santorini 2002]



In reversible IE (RIE), an additional constraint is imposed, that S^n can be faithfully restored from Y^n. The constraint $\mathbb{E}d(S, X) \leq D$ is still relevant.

$$\mathcal{C} = \sup[H(X) - H(S)]$$ (no attack channel, Kalker & Willems)

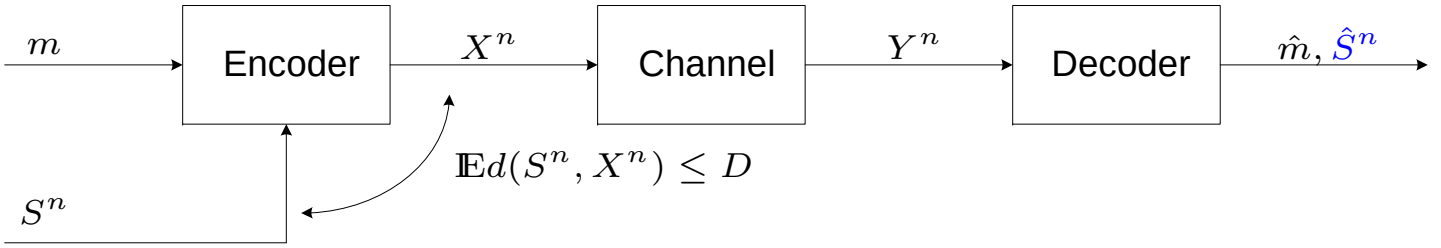
$$\mathcal{C} = \sup[I(X;Y) - H(S)]$$ (with channel, Kalker & Willems, 2002, Willems & Kalker, DIMACS 2003. Kotagiri & Laneman '05)

In both cases, the supremum is taken over all distributions $P_{X|S}$ satisfying $\mathbb{E}d(S, X) \leq D$.

Introduction
Outline
The Information Embedding (IE) Problem
Reversible IE
Drawbacks of Reversible IE
Stegotext RIE
END

Reversible IE

[Fridrich, Goljan, Du *SPIE* 2002], [Kalker & Willems, Santorini 2002]



In reversible IE (RIE), an additional constraint is imposed, that S^n can be faithfully restored from Y^n. The constraint $\mathbb{E}d(S, X) \leq D$ is still relevant.

$$\mathcal{C} = \sup[H(X) - H(S)]$$ (no attack channel, Kalker & Willems)

$$\mathcal{C} = \sup[I(X;Y) - H(S)]$$ (with channel, Kalker & Willems, 2002, Willems & Kalker, DIMACS 2003. Kotagiri & Laneman '05)

In both cases, the supremum is taken over all distributions $P_{X|S}$ satisfying $\mathbb{E}d(S, X) \leq D$.

Introduction
Outline
The Information Embedding (IE) Problem
Reversible IE
Drawbacks of Reversible IE

Stegotext RIE

END

Drawbacks of Reversible IE

- The cost of decoding the host S^n is high especially when the entropy of S is high.
- When the host signal has continuous alphabet, (e.g., the Gaussian case), host reversibility is impossible.
- Willems & Kalker suggested to recover S destination with distortion $\leq D$.
  This problem is still open. Equivalent to *simultaneous transmission of data and state* [Sutivong, Cover, Chiang, & Kim, ISIT 2002. Gaussian case - 2005].

- Some applications need the host at the destination only to embed into it again the decoded message $\hat{m}$, and obtain the stegotext $\hat{X}^n$ (e.g., in order to transmit it further).

Introduction
Outline
The Information Embedding (IE) Problem
Reversible IE
Drawbacks of Reversible IE

Stegotext RIE

END

Drawbacks of Reversible IE

- The cost of decoding the host S^n is high especially when the entropy of S is high.
- When the host signal has continuous alphabet, (e.g., the Gaussian case), host reversibility is impossible.
- Willems & Kalker suggested to recover S destination with distortion $\leq D$.
  This problem is still open. Equivalent to *simultaneous transmission of data and state* [Sutivong, Cover, Chiang, & Kim, ISIT 2002. Gaussian case - 2005].

- Some applications need the host at the destination only to embed into it again the decoded message $\hat{m}$, and obtain the stegotext $\hat{X}^n$ (e.g., in order to transmit it further).

$\Longrightarrow$ *Stegotext Reversible Information Embedding (SRIE)*

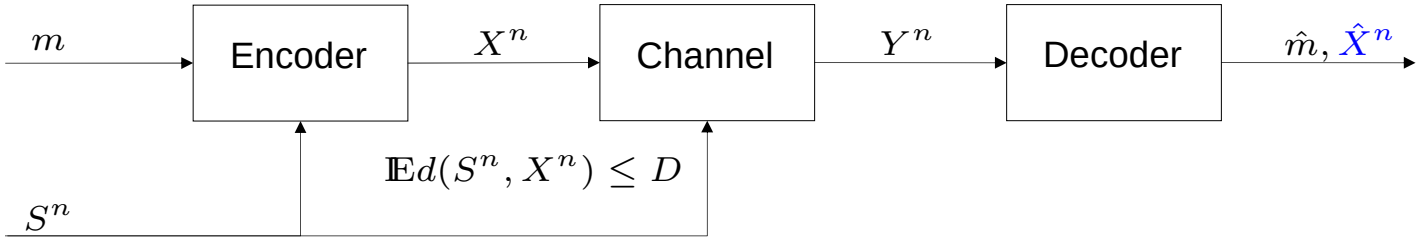
Stegotext Reversible Information Embedding

Problem Formulation

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

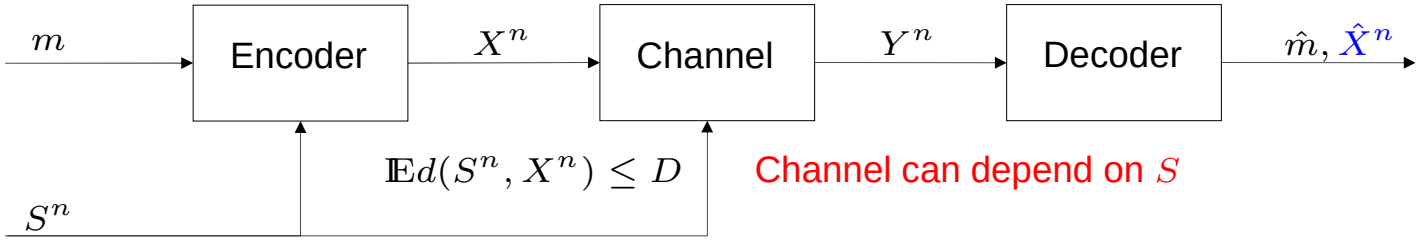


Problem Formulation

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

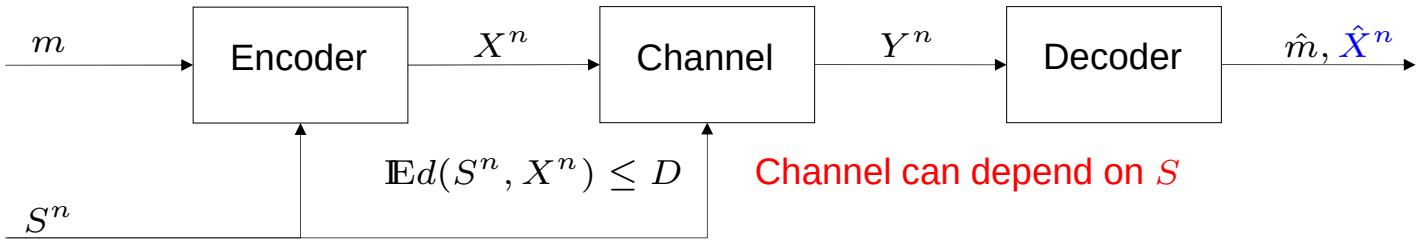


Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Problem Formulation



Definition: Let $\mathcal{M} = \{1, 2, \ldots, 2^{nR}\}$. An $(n, 2^{nR}, D, \epsilon)$ stegotext reversible information embedding (SRIE) code for the model channel $P_{Y|X,S}$, with host distribution P_S consists of

$$f : \mathcal{M} \times \mathcal{S}^n \to \mathcal{X}^n, \qquad \text{encoder map}$$

$$g : \mathcal{Y}^n \to \mathcal{M}, \qquad g_x : \mathcal{Y}^n \to \mathcal{X}^n, \qquad \text{decoding maps}$$

such that

$$P(g(Y^n) \neq m) < \epsilon,$$

$$P(g_x(Y^n) \neq f(m, S^n)) < \epsilon,$$

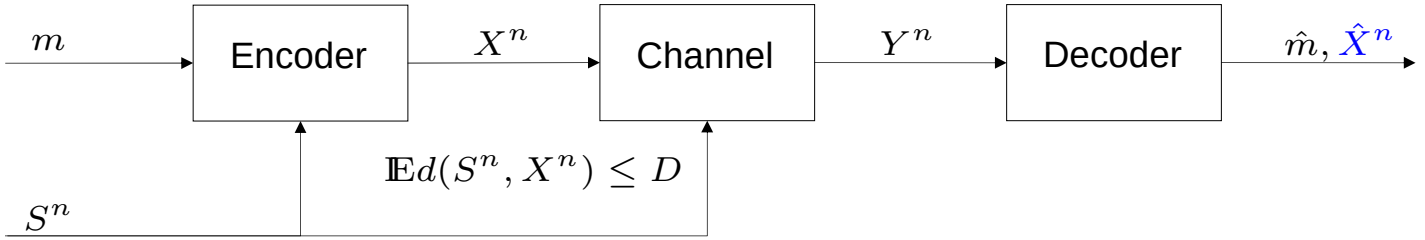
$$\mathbb{E}d(S^n, X^n) \leq D.$$

Problem Formulation *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END



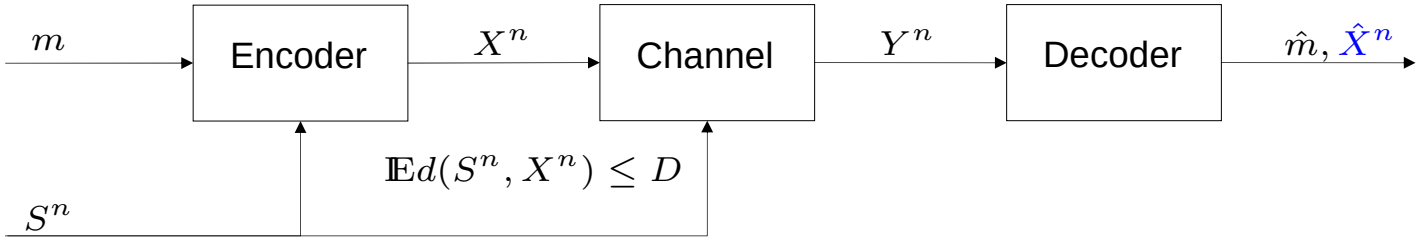
- The SRIE capacity function, $\mathcal{C}_{srie}(D)$, is the supremum on all rates with distortion D, and arbitrarily small ϵ.

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Main Result



Theorem 1 *For any memoryless channel $P_{Y|X,S}$ and host P_S, the SRIE rate–distortion region is given by the convex hull of all pairs (R, D) satisfying*

$$0 \leq R \leq I(X;Y) - I(X;S),$$

$$\mathbb{E}d(S, X) \leq D$$

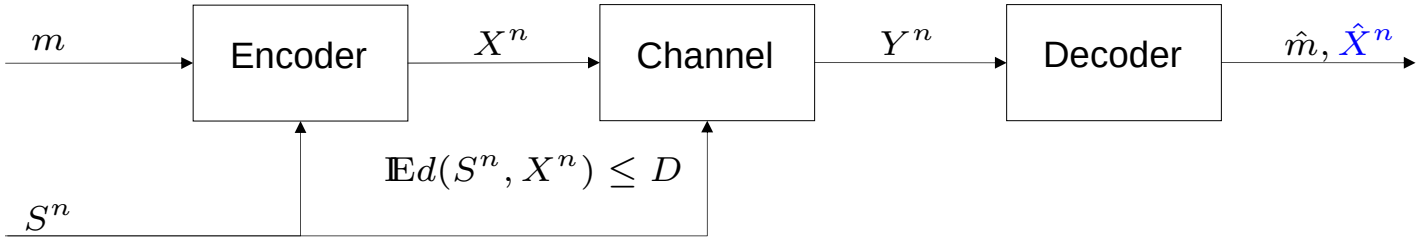
for some joint distribution $P_S P_{X|S} P_{Y|X,S}$.

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Main Result



Theorem 1 *For any memoryless channel $P_{Y|X,S}$ and host P_S, the SRIE rate–distortion region is given by the convex hull of all pairs (R, D) satisfying*

$$0 \leq R \leq I(X;Y) - I(X;S),$$

$$\mathbb{E}d(S, X) \leq D$$

for some joint distribution $P_S P_{X|S} P_{Y|X,S}$.

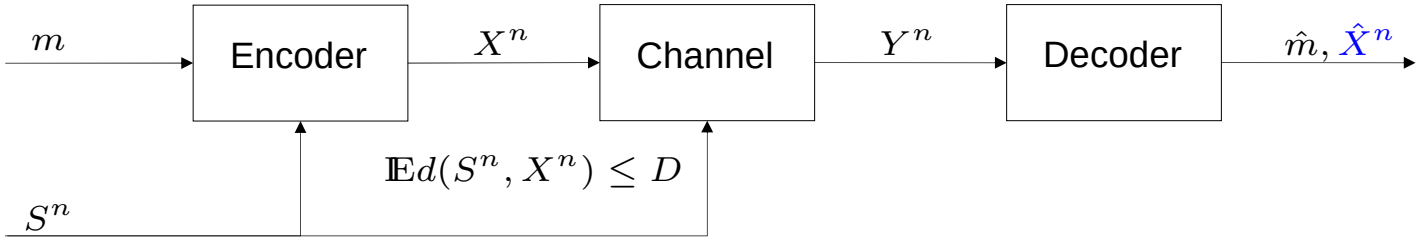
- In some channel models, low values of D may not be achievable, even with rate $R = 0$.
- In general, CH is needed. Not needed when the channel is independent of S.

Main Result *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END



Corollary 1 *For any memoryless channel $P_{Y|X}$ and host P_S, the SRIE rate–distortion function is given by*

$$\mathcal{C}_{srie}(D) = \max[I(X;Y) - I(X;S)] \tag{1}$$

where the max is taken over all distributions $P_{X|S}$ satisfying

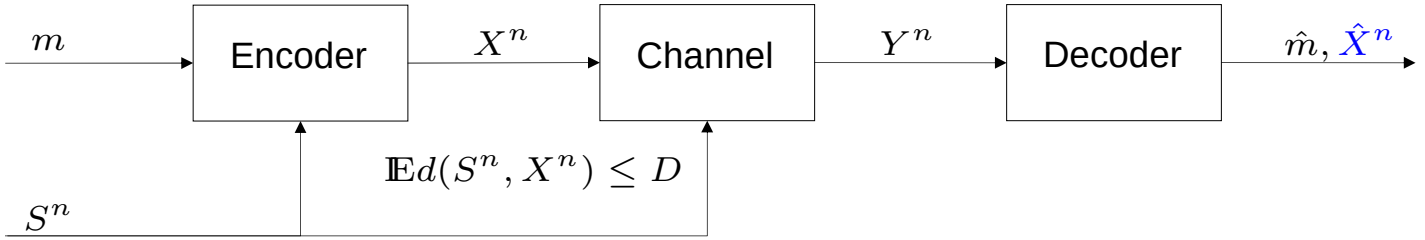
$$\mathbb{E}d(S,X) \leq D. \tag{2}$$

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Main Result *(cont'd)*



Corollary 1 *For any memoryless channel $P_{Y|X}$ and host P_S, the SRIE rate–distortion function is given by*

$$\mathcal{C}_{srie}(D) = \max[I(X;Y) - I(X;S)] \tag{1}$$

where the max is taken over all distributions $P_{X|S}$ satisfying

$$\mathbb{E}d(S,X) \leq D. \tag{2}$$

- If there does not exist $P_{X|S}$ such that the right hand side of (1) is non-negative and (2) is satisfied, then the distortion D is not achievable with any rate.

Main Result *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Comparing the two formulae, given a memoryless channel $P_{Y|X}$ and host P_S, we have

$$\begin{aligned} \mathcal{C}_{rie}(D) &= \sup[I(X;Y) - H(S)] \\ \mathcal{C}_{srie}(D) &= \sup[I(X;Y) - I(X;S)], \end{aligned}$$

therefore

$$\mathcal{C}_{srie}(D) \geq \mathcal{C}_{rie}(D).$$

and the inequality is strict in most cases of interest.

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Main Result *(cont'd)*

Comparing the two formulae, given a memoryless channel $P_{Y|X}$ and host P_S, we have

$$\begin{aligned} \mathcal{C}_{rie}(D) &= \sup[I(X;Y) - H(S)] \\ \mathcal{C}_{srie}(D) &= \sup[I(X;Y) - I(X;S)], \end{aligned}$$

therefore

$$\mathcal{C}_{srie}(D) \geq \mathcal{C}_{rie}(D).$$

and the inequality is strict in most cases of interest.

- Constructing the stegotext X^n at the destination by first decoding the host S^n and encoding it again with the decoded message $\hat{m}$ is suboptimal.
- If the user needs only the stegotext at the destination, he can retrieve it even if the host signal has continuous alphabet.

A Rate-Distortion Dual

The SRIE problem is closely related to the Gel'fand-Pinsker problem:

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

A Rate-Distortion Dual

The SRIE problem is closely related to the Gel'fand-Pinsker problem:

$$C_{GP} = \max[I(U;Y) - I(U;S)]$$

A Rate-Distortion Dual

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

The SRIE problem is closely related to the Gel'fand-Pinsker problem:

$$C_{GP} = \max[I(U;Y) - I(U;S)]$$

$$C_{SRIE} = \max[I(X;Y) - I(X;S)]$$

A Rate-Distortion Dual

The SRIE problem is closely related to the Gel'fand-Pinsker problem:

$$C_{GP} = \max[I(U;Y) - I(U;S)] \qquad R_{WZ} = \min[I(X;U) - I(Y;U)]$$

$$C_{SRIE} = \max[I(X;Y) - I(X;S)]$$

Introduction

Stegotext RIE

- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

A Rate-Distortion Dual

The SRIE problem is closely related to the Gel'fand-Pinsker problem:

$$C_{GP} = \max[I(U;Y) - I(U;S)] \qquad R_{WZ} = \min[I(X;U) - I(Y;U)]$$

$$C_{SRIE} = \max[I(X;Y) - I(X;S)] \qquad ??$$

An RD Dual (cont'd)

A rate-distortion dual problem: source coding with common knowledge (CK) constraint [ITA 2008].

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

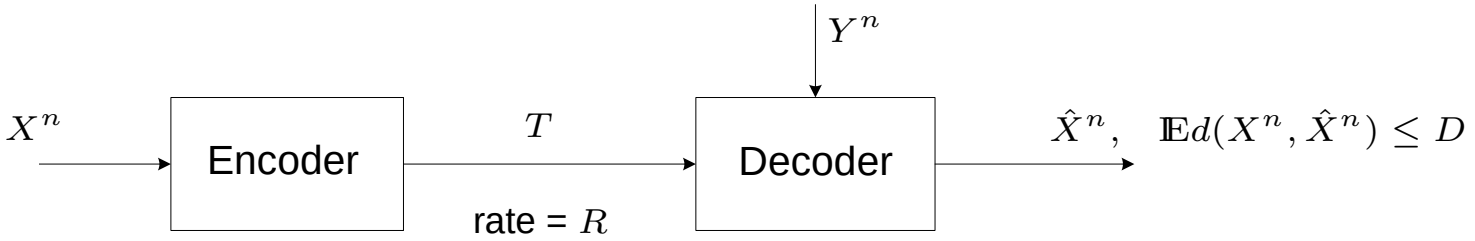
An RD Dual *(cont'd)*

A rate-distortion dual problem: source coding with common knowledge (CK) constraint [ITA 2008].

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END



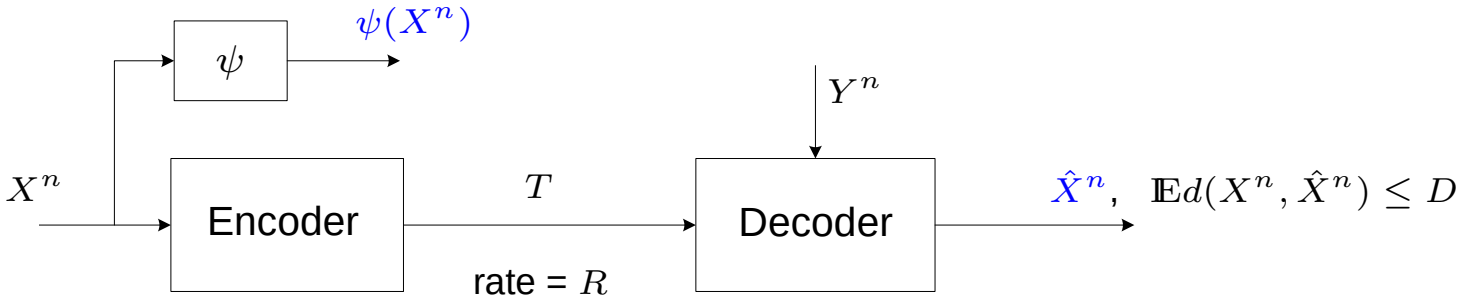
An RD Dual *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

A rate-distortion dual problem: source coding with common knowledge (CK) constraint [ITA 2008].



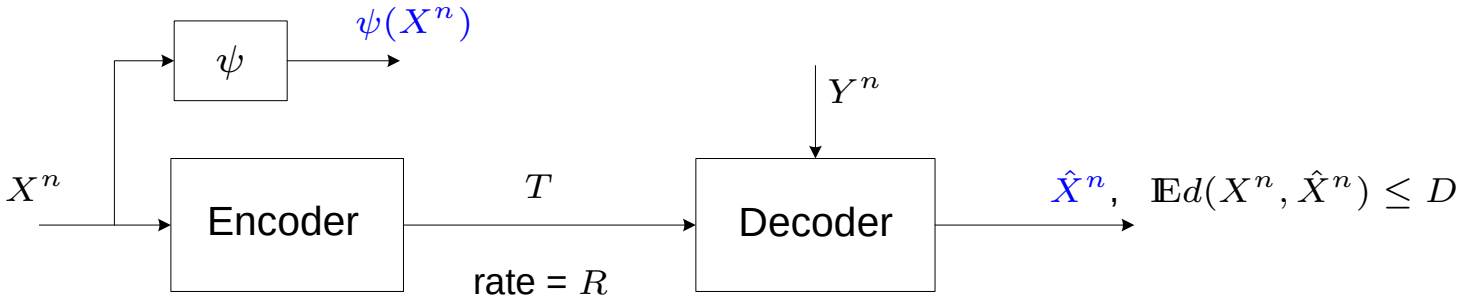
Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

An RD Dual *(cont'd)*

A rate-distortion dual problem: source coding with common knowledge (CK) constraint [ITA 2008].



Definition: Let $\mathcal{T} = \{1, 2, \ldots, 2^{nR}\}$. An $(n, 2^{nR}, D, \epsilon)$ common knowledge (CK) code for the source X with decoder side information Y consists of an encoder-decoder pair

$$f : \mathcal{X}^n \to \mathcal{T}, \qquad g : \mathcal{T} \times \mathcal{Y}^n \to \hat{\mathcal{X}}^n,$$

and a sender reconstruction map

$$\psi : \mathcal{X}^n \to \hat{\mathcal{X}}^n,$$

such that

$$\mathbb{E}d(X^n, g(f(X^n), Y^n)) \leq D,$$

$$P_{XY}\left(\psi(X^n) \neq g(f(X^n), Y^n)\right) \leq \epsilon.$$

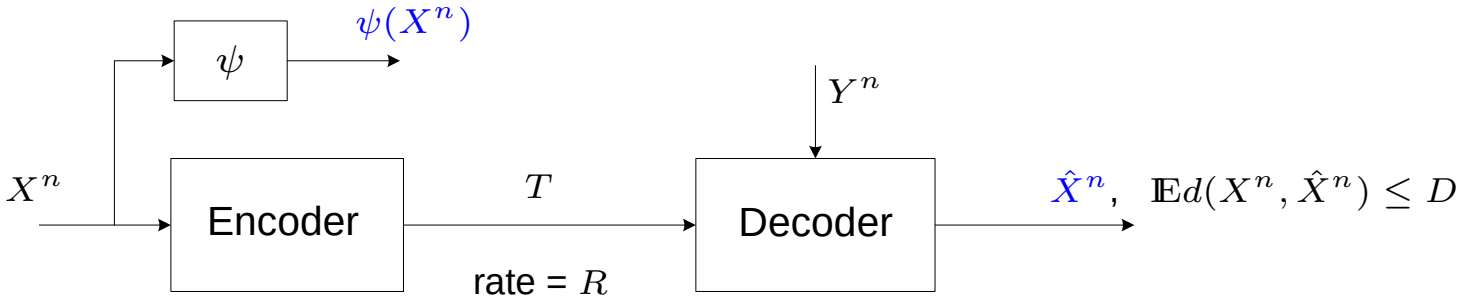
An RD Dual *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

A rate-distortion dual problem: source coding with common knowledge (CK) constraint [ITA 2008].



$$\hat{X}^n = g(f(X^n), Y^n)$$

$$P_{XY}\left(\psi(X^n) \neq \hat{X}^n\right) \leq \epsilon \quad \text{(CK constraint)}.$$

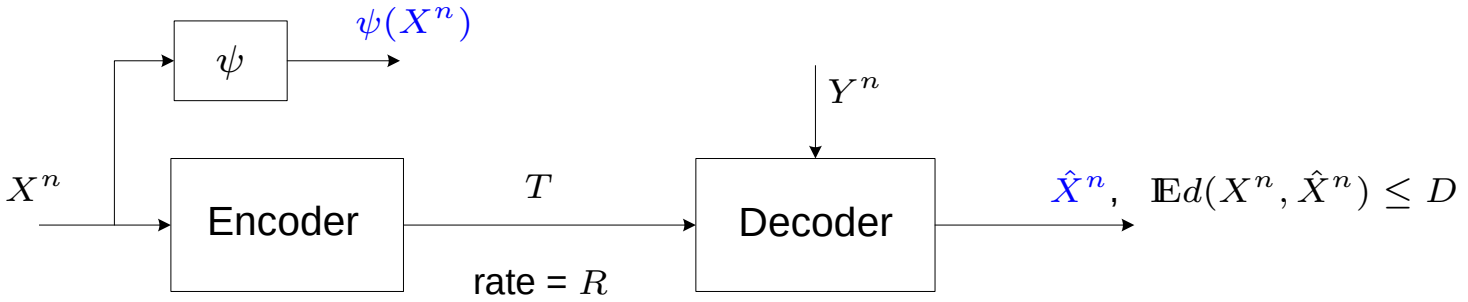
An RD Dual *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

A rate-distortion dual problem: source coding with common knowledge (CK) constraint [ITA 2008].



$$\hat{X}^n = g(f(X^n), Y^n)$$

$$P_{XY}\left(\psi(X^n) \neq \hat{X}^n\right) \leq \epsilon \quad \text{(CK constraint)}.$$

- The CK rate-distortion function, $R_{ck}(D)$, is the minimal achievable CK coding rate, under average distortion D and arbitrarily small ϵ.

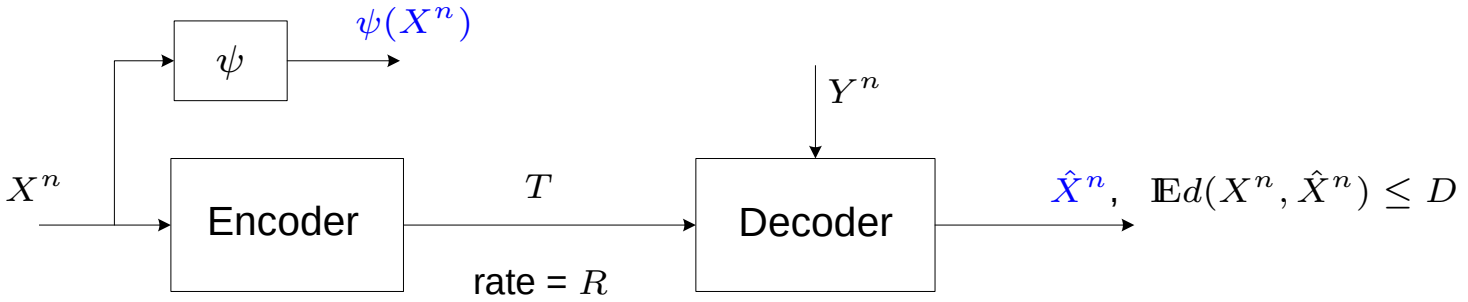
Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

An RD Dual *(cont'd)*

A rate-distortion dual problem: source coding with common knowledge (CK) constraint [ITA 2008].



Theorem 2 *[ITA 2008]*

$$R_{ck}(D) = \min[I(X;\hat{X}) - I(Y;\hat{X})]$$

where the minimum is over all $\hat{X}$ *such that* $\hat{X} \ominus X \ominus Y$ *and*

$$\mathbb{E}d(X,\hat{X}) \leq D.$$

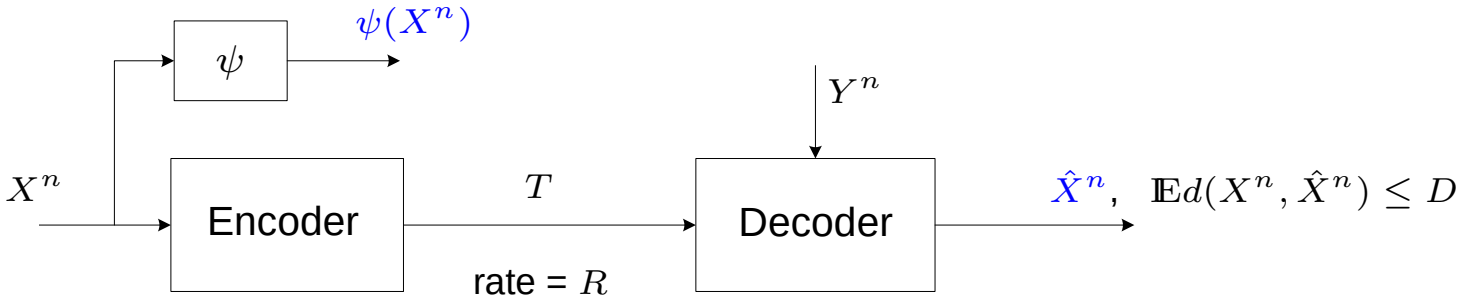
An RD Dual *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

A rate-distortion dual problem: source coding with common knowledge (CK) constraint [ITA 2008].



Theorem 2 *[ITA 2008]*

$$R_{ck}(D) = \min[I(X;\hat{X}) - I(Y;\hat{X})]$$

where the minimum is over all $\hat{X}$ *such that* $\hat{X} \ominus X \ominus Y$ *and*

$$\mathbb{E}d(X,\hat{X}) \leq D.$$

Due to the Markov conditions, $R_{ck}(D) = \min I(X;\hat{X}|Y)$.

An RD Dual *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Remark: The function

$$R = \min[I(X;\hat{X}) - I(Y;\hat{X})]$$

was introduced also by Zheng, He, and Yang [CWIT 2007], in a different perspective.

An RD Dual *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Remark: The function

$$R = \min[I(X;\hat{X}) - I(Y;\hat{X})]$$

was introduced also by Zheng, He, and Yang [CWIT 2007], in a different perspective.

A simple alternative to the Wyner-Ziv rate distortion scheme:

- Use a *conventional* quantizer at the encoder, to encode X^n
- Bin the quantizer output
- Use Y^n at the decoder to resolve the binning. Do not try to further reduce distortion at the decoder with the use of SI Y^n.

An RD Dual *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

An RD Dual *(cont'd)*

$$C_{GP} = \max[I(U;Y) - I(U;S)]$$

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

An RD Dual *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

$$C_{GP} = \max[I(U;Y) - I(U;S)]$$

$$C_{SRIE} = \max[I(X;Y) - I(X;S)]$$

An RD Dual *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

$$C_{GP} = \max[I(U;Y) - I(U;S)] \qquad R_{WZ} = \min[I(X;U) - I(Y;U)]$$

$$C_{SRIE} = \max[I(X;Y) - I(X;S)]$$

An RD Dual *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

$$C_{GP} = \max[I(U;Y) - I(U;S)] \qquad R_{WZ} = \min[I(X;U) - I(Y;U)]$$

$$C_{SRIE} = \max[I(X;Y) - I(X;S)] \qquad ??$$

An RD Dual *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

$$C_{GP} = \max[I(U;Y) - I(U;S)] \qquad R_{WZ} = \min[I(X;U) - I(Y;U)]$$

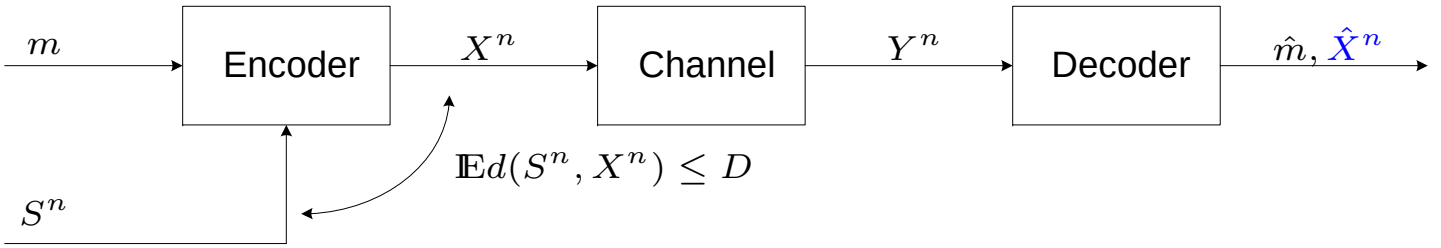
$$C_{SRIE} = \max[I(X;Y) - I(X;S)] \qquad R_{ck} = \min[I(X;\hat{X}) - I(Y;\hat{X})]$$

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Examples



Example 1 *Host independent channel.*

- $\mathcal{S} = \mathcal{X} = \mathcal{Y} = \{0, 1\}$
- $S \sim$ Bernoulli$(\frac{1}{2})$
- $Y = X \oplus Z$
- $Z \sim$ Bernoulli(p_z) independent of S and X
- The distortion measure d is the Hamming distance

Examples *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Define

$$p \triangleq P(X=1|S=0) \quad \text{and} \quad q \triangleq P(X=0|S=1).$$

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Examples *(cont'd)*

Define

$$p \triangleq P(X=1|S=0) \quad \text{and} \quad q \triangleq P(X=0|S=1).$$

The capacity is given by

$$\mathcal{C}_{srie}(D) = h(D) - h(p_z) \qquad \text{with} \qquad p = q = D,$$

where

- h is the binary entropy function

$$h(\alpha) = -\alpha \log \alpha - (1-\alpha)\log(1-\alpha), \alpha \in [0,1],$$

- $\star$ is the cyclic convolution

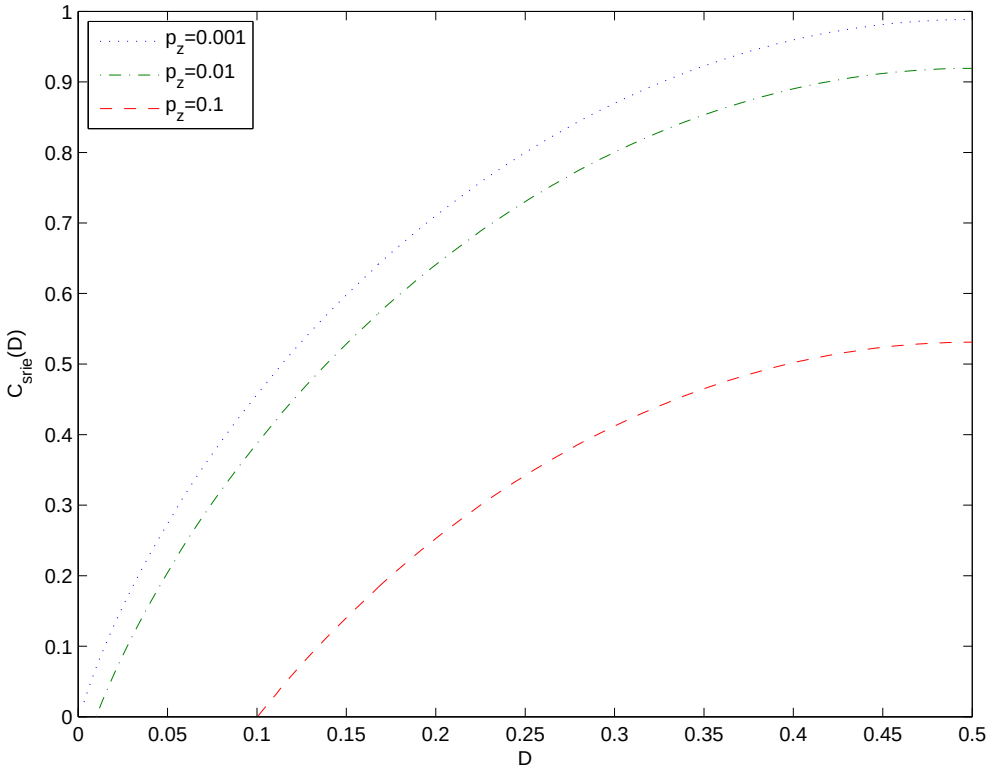
$$a \star b = a(1-b) + (1-a)b.$$

Examples *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

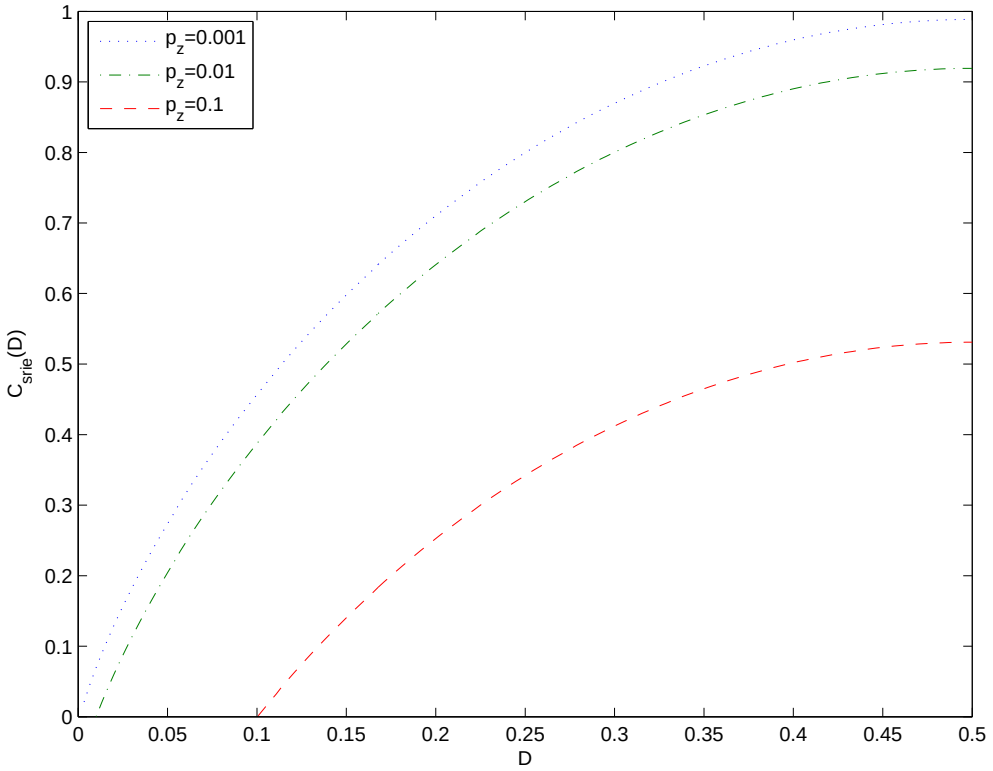


Examples *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END



For $S \sim$ Bernoulli$(\frac{1}{2})$, $I(X;Y) - H(S) < 0$ for any input distribution and any $D < 0.5$ (since due to the channel noise, $I(X;Y) < 1$).

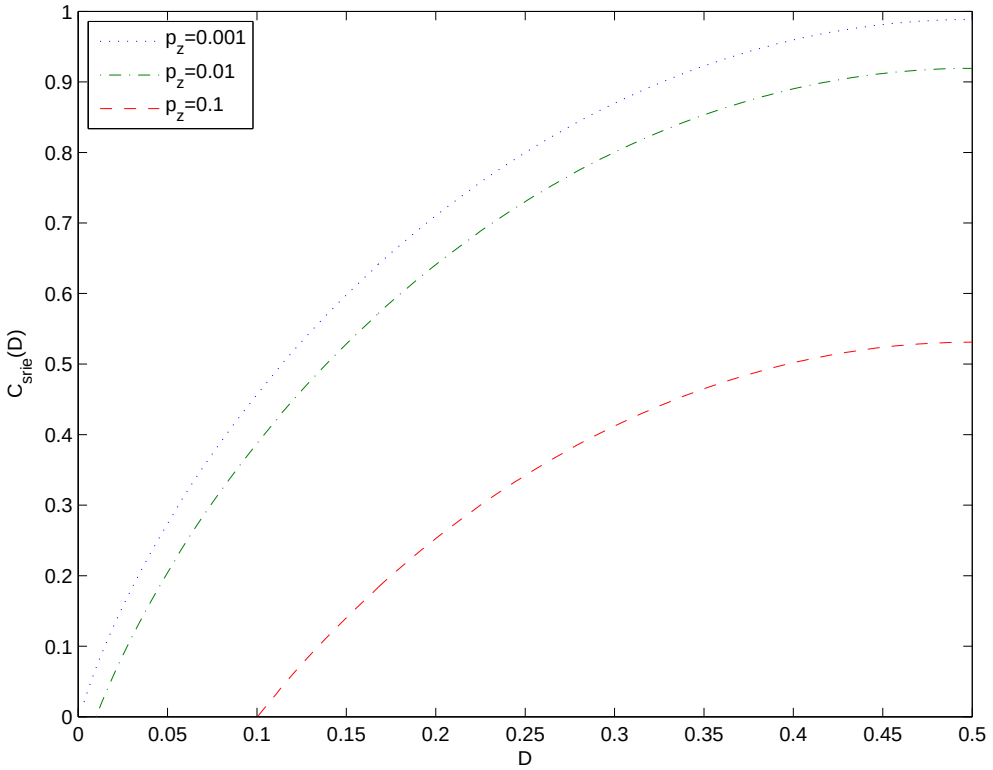
$\Longrightarrow$ Host reversibility cannot be achieved here at all for values of D less than 0.5.

Examples *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END



For $S \sim$ Bernoulli$(\frac{1}{2})$, $I(X;Y) - H(S) < 0$ for any input distribution and any $D < 0.5$ (since due to the channel noise, $I(X;Y) < 1$).

$\Longrightarrow$ Host reversibility cannot be achieved here at all for values of D less than 0.5.

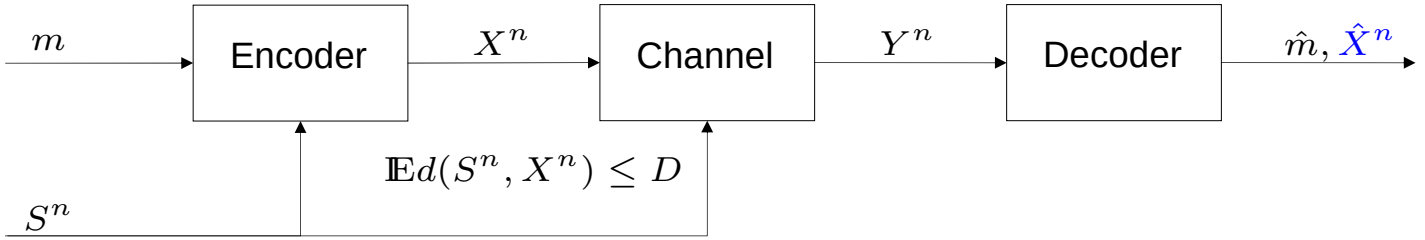
But stegotext can be reconstructed at the destination for moderate values of D as can be seen from the graph.

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Examples *(cont'd)*



Example 2 *Host dependent channel.*

As in example 1 except that

- $S \sim$ Bernoulli(p_s)
- $Y = X \oplus S \oplus Z$

Examples *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

The SRIE rate–distortion region is given by the convex hull of all (R, D) pairs verifying

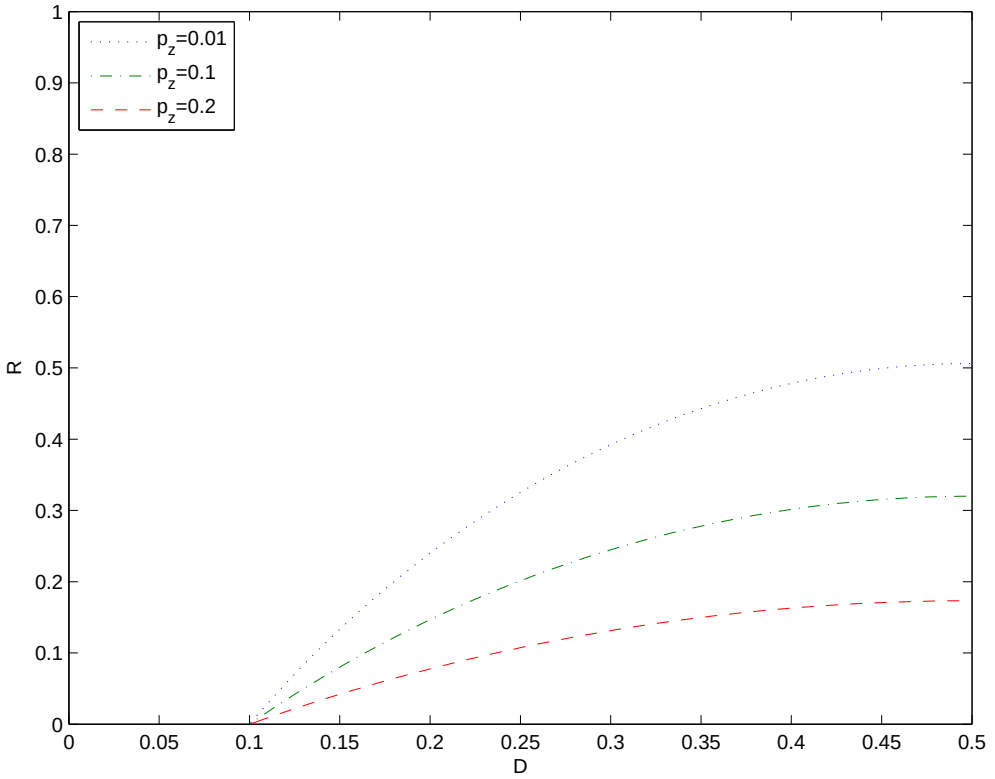
$$
\begin{aligned}
D &\geq (1-p_s)p + p_s q \\
R &\leq (1-p_s)h(p) + p_s h(q) - (1-(p_s \star p_z)) \cdot \\
&\quad h\left(\frac{p(1-p_z)(1-p_s) + (1-q)p_z p_s}{1-(p_s \star p_z)}\right) \\
&\quad - (p_s \star p_z) h\left(\frac{p p_z (1-p_s) + (1-q)(1-p_z)p_s}{p_s \star p_z}\right) \\
&\quad - h(p_s \star p_z) + h(p_z \star ((1-p_s)p + p_s q)).
\end{aligned}
$$

Examples *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END



Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Iterative algorithm

- Computation of the capacity function is a difficult optimization problem.
- Blahut and Arimoto provide efficient numerical computation for memoryless channels.
- An Arimoto–Blahut like algorithm for computing numerically the capacity of the SRIE channel is provided, only in the case where the channel is independent of S given X, i.e. $P_{Y|X,S} = P_{Y|X}$.
- In this case indeed, the capacity is a concave function of D, and this fact is needed for the algorithm to converge.

Iterative algorithm (cont'd)

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Define the functional $J(\mu)$ as

$$J(\mu) \triangleq \sup_{P(x|s)} \{I(X;Y) - I(X;S) - \mu(\mathbb{E}d(S,X) - D)\}.$$

Due to the concavity of $\mathcal{C}_{srie}(D)$, $J(\mu)$ characterizes the capacity curve when running over values of $\mu \geq 0$.

Iterative algorithm *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Define the functional $J(\mu)$ as

$$J(\mu) \triangleq \sup_{P(x|s)} \{I(X;Y) - I(X;S) - \mu(\mathbb{E}d(S,X) - D)\}.$$

Due to the concavity of $\mathcal{C}_{srie}(D)$, $J(\mu)$ characterizes the capacity curve when running over values of $\mu \geq 0$.

After optimization, D can be computed as

$$D = \sum_{s,x} P(s)P^*(x|s)d(s,x),$$

where $P^*(x|s)$ maximizes $J(\mu)$.

Iterative algorithm *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Define the functional

$$F(q,Q) \triangleq \sum_{s,x,y} P(s)q(x|s)P(y|x)\log\frac{Q(x|y)}{q(x|s)} - \mu\sum_{s,x} P(s)q(x|s)d(s,x).$$

Now, $J(\mu)$ can be written as

$$J(\mu) = \sup_{q(x|s)} F(q,Q_0) + \mu D,$$

where Q_0 is defined as

$$Q_0(x|y) \triangleq \frac{\sum_s P(s)q(x|s)P(y|x)}{\sum_{x,s} P(s)q(x|s)P(y|x)}.$$

Iterative algorithm (cont'd)

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

The following lemma is the main key to the iterative algorithm.

Lemma 1

$$J(\mu) = \sup_{q(x|s)} \sup_{Q(x|y)} \{F(q,Q) + \mu D\}.$$

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Iterative algorithm (cont'd)

The following lemma is the main key to the iterative algorithm.

Lemma 1

$$J(\mu) = \sup_{q(x|s)} \sup_{Q(x|y)} \{F(q, Q) + \mu D\}.$$

The algorithm iterates through each one of q and Q increasing F with respect to one argument while leaving the other one fixed.

- F is maximized over Q with q fixed by setting $Q = Q_0$.
- F is maximized over q with Q fixed by setting

$$q^*(x|s) = \frac{\exp(-\mu d(s,x)) \prod_y Q(x|y)^{P(y|x)}}{\sum_x \left[\exp(-\mu d(s,x)) \prod_y Q(x|y)^{P(y|x)}\right]}.$$

Iterative algorithm *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

The following lemma is the main key to the iterative algorithm.

Lemma 1

$$J(\mu) = \sup_{q(x|s)} \sup_{Q(x|y)} \{F(q, Q) + \mu D\}.$$

The algorithm iterates through each one of q and Q increasing F with respect to one argument while leaving the other one fixed.

- F is maximized over Q with q fixed by setting $Q = Q_0$.
- F is maximized over q with Q fixed by setting

$$q^*(x|s) = \frac{\exp(-\mu d(s,x)) \prod_y Q(x|y)^{P(y|x)}}{\sum_x \left[\exp(-\mu d(s,x)) \prod_y Q(x|y)^{P(y|x)}\right]}.$$

The following lemma guarantees that the algorithm converges to the global optimum.

Lemma 2 *$F(q, Q)$ is concave in q and Q.*

Iterative algorithm *(cont'd)*

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

- The value of F for q^* is given by

$$F(q^*, Q) = \sum_s P(s) \max_x \sum_y P(y|x) \left(\log \frac{Q(x|y)}{q^*(x|s)} - \mu d(s,x) \right).$$

- Define $U(q)$ in the following way:

$$U(q) \triangleq \sum_s P(s) \max_x \sum_y P(y|x) \left(\log \frac{Q_0(x|y)}{q(x|s)} - \mu d(s,x) \right).$$

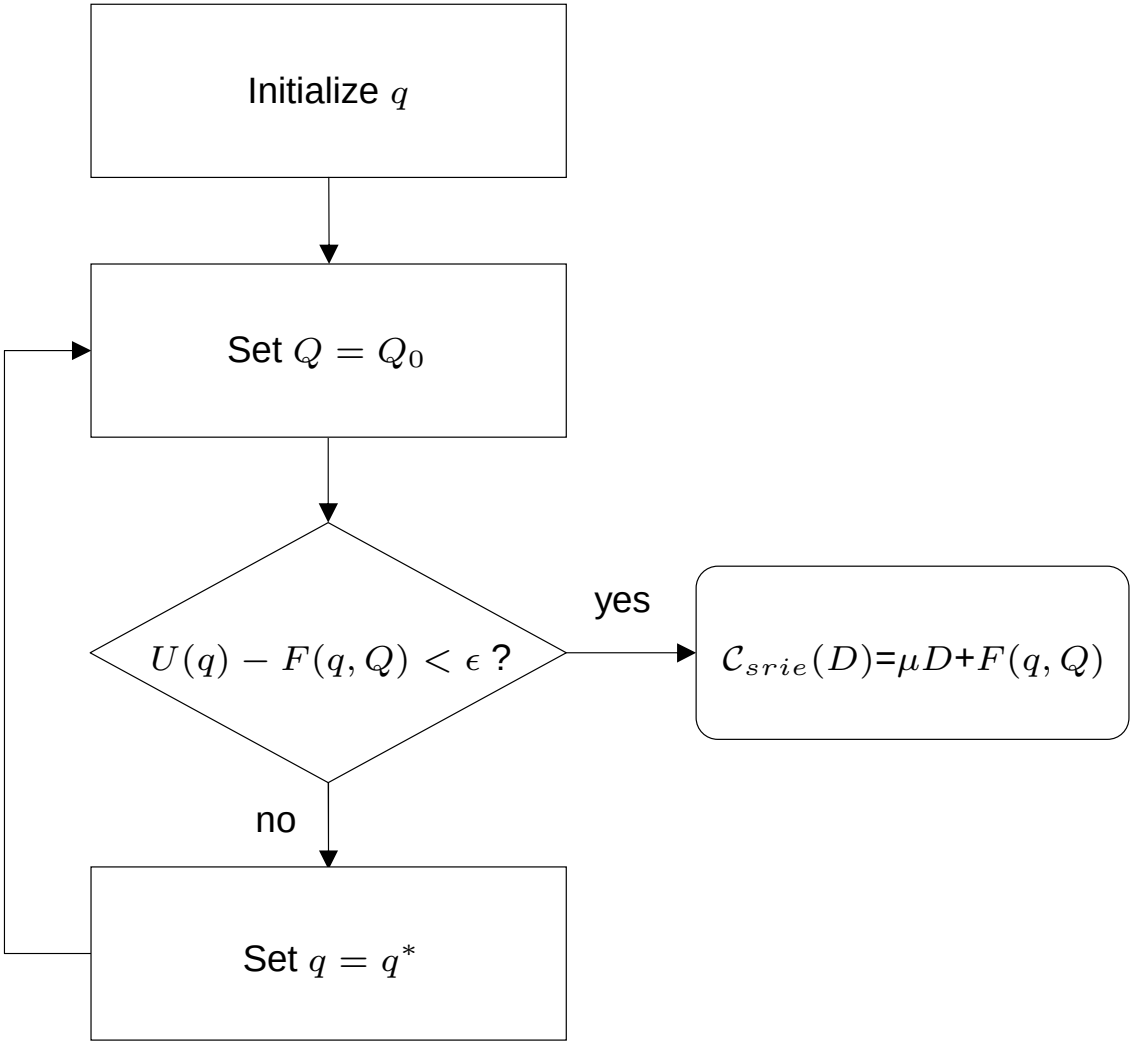
- $U(q)$ forms an upper bound on $F(q, Q)$ which converges to F as F approaches a maximum.
- The algorithm terminates with $|\mathcal{C}_{srie}(D) - F| < \epsilon$, for any desired accuracy $\epsilon > 0$.

Introduction

Stegotext RIE
- Problem Formulation
- Main Result
- A Rate-Distortion Dual
- Examples
- Iterative algorithm

END

Flowchart of the iterative algorithm



Thank You!