On Joint Coding for Watermarking and Encryption

Neri Merhav

Department of Electrical Engineering

Technion—Israel Institute of Technology

Haifa 32000, Israel

The $7^{\rm th}$ Information Hiding Workshop—IH 05:

Barcelona, Spain, June 2005

General Motivation

Encryption and watermarking are related, but different:

Encryption	–	hiding the contents of secret information.
Watermarking	–	hiding the existence of secret information.

In the last few years, there are increasingly more efforts in combining watermarking and encryption, both in the fronts of research and in actual technologies used in commercial products with copyright protection, like the CD and the DVD.

Some Internet content providers post in their websites warning messages, like the following one:

Copyright © 2001 Genealogy Leaves^{TM}

All of the scanned maps are protected by copyright and have an embedded Digimark digitally encrypted watermark. Use of these maps for any other purpose other than personal genealogical research is not permitted.

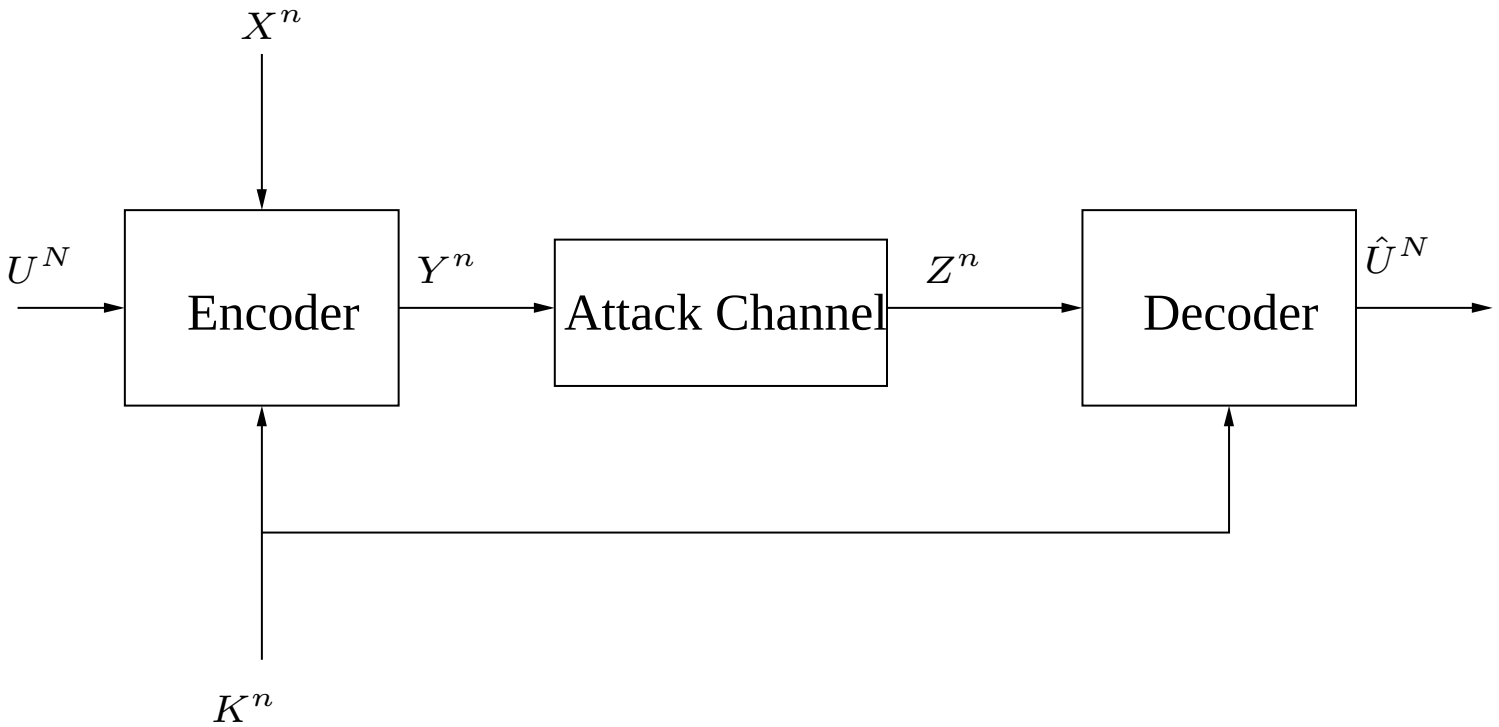
`http://genealogy.lv/1864Lancaster/copyright.htm`

Objectives

Our main objective is to address the problem of joint coding for watermarking and encryption from an information–theoretic point of view.

Specifically: to explore fundamental limits and coding strategies for the best possible tradeoffs between several parameters:

- Reliable WM decoding: small bit/block error probability.
- Reasonably small degradation in quality: small distortion.
- Good security of the watermark: high equivocation.
- Good compressibility of the stegotext: low entropy.


X^n
U^N
Encoder
Y^n
Attack Channel
Z^n
Decoder
$\hat{U}^N$
K^n

The Problem (Without Attack)

For memoryless U^N, X^n, K^n, and $N/n = \lambda$, find an encoder

$$Y^n = f(U^N, X^n, K^n)$$

and decoder

$$\hat{U}^N = g(Y^n, K^n) \text{ with small } P_e = \Pr\{\hat{U}^N \neq U^N\}$$

under the following specifications:

1. Quality: $\frac{1}{n}\sum_{i=1}^{n} Ed(X_i, Y_i) \leq D$.
2. Compressibility: $\frac{1}{n} H(Y^n) \leq R_c$.
3. Security: $\frac{1}{N} H(U^N|Y^n) \geq h$.

What are the conditions on D, R_c and h for which this is possible?

A Solution Strategy

- Compress U^N to $NH(U)$ bits.
- Encrypt Nh compressed bits by $nH(K) = NH(K)/\lambda$ key bits.
- Use the encrypted msg for selecting a R–D codebook for X^n ($\exists\ 2^{nH(Y|X)}$ distinct codebooks).

(D, R_c, h) can be achieved this way if:

- $h \leq H(K)/\lambda$
- $\exists\ P_{Y|X}$ such that: $H(Y|X) \geq \lambda H(U)$, $\lambda H(U) + I(X;Y) \leq R_c$, and $Ed(X,Y) \leq D$.

Q: Is this the best one can do?

Optimality

A: Yes, in the sense that the conditions are also *necessary*.

This gives rise to a separation principle:

Lossless compression $\rightarrow$ encryption $\rightarrow$ R-D embedding.

Lossy Reconstruction

Suppose now that some distortion is allowed

$$\frac{1}{N}\sum_{i=1}^{N} Ed'(U_i, \hat{U}_i) \leq D'$$

and that we would then like to secure also $\hat{U}^N$:

$$\frac{1}{N} H(\hat{U}^N | Y^n) \geq h'.$$

Q: What are the conditions for the achievability of (D, R_c, h, D', h')?

A: A quintuple (D, R_c, h, D', h') is achievable **iff**:

- $h \leq H(K)/\lambda + H(U) - R_U(D'), \;\; h' \leq H(K)/\lambda$.
- $\exists\, P_{Y|X}$ such that: $H(Y|X) \geq \lambda R_U(D')$,

  $\lambda R_U(D') + I(X;Y) \leq R_c$, and $Ed(X,Y) \leq D$.

Achievability – same as before except that lossless compression of U^N is replaced by lossy compression to $R_U(D')$.

The earlier separation principle still applies.

What happens in the Presence of Attack?

The decoder has access to Z^n, instead of Y^n, where

$$P(Z^n|Y^n) = \prod_{i=1}^{n} P(Z_i|Y_i).$$

We can now re–define the equivocation requirements as

$$\frac{1}{N}H(U^N|Y^n, Z^n) \geq h \text{ and } \frac{1}{N}H(\hat{U}^N|Y^n, Z^n) \geq h'.$$

What are now the best tradeoffs?

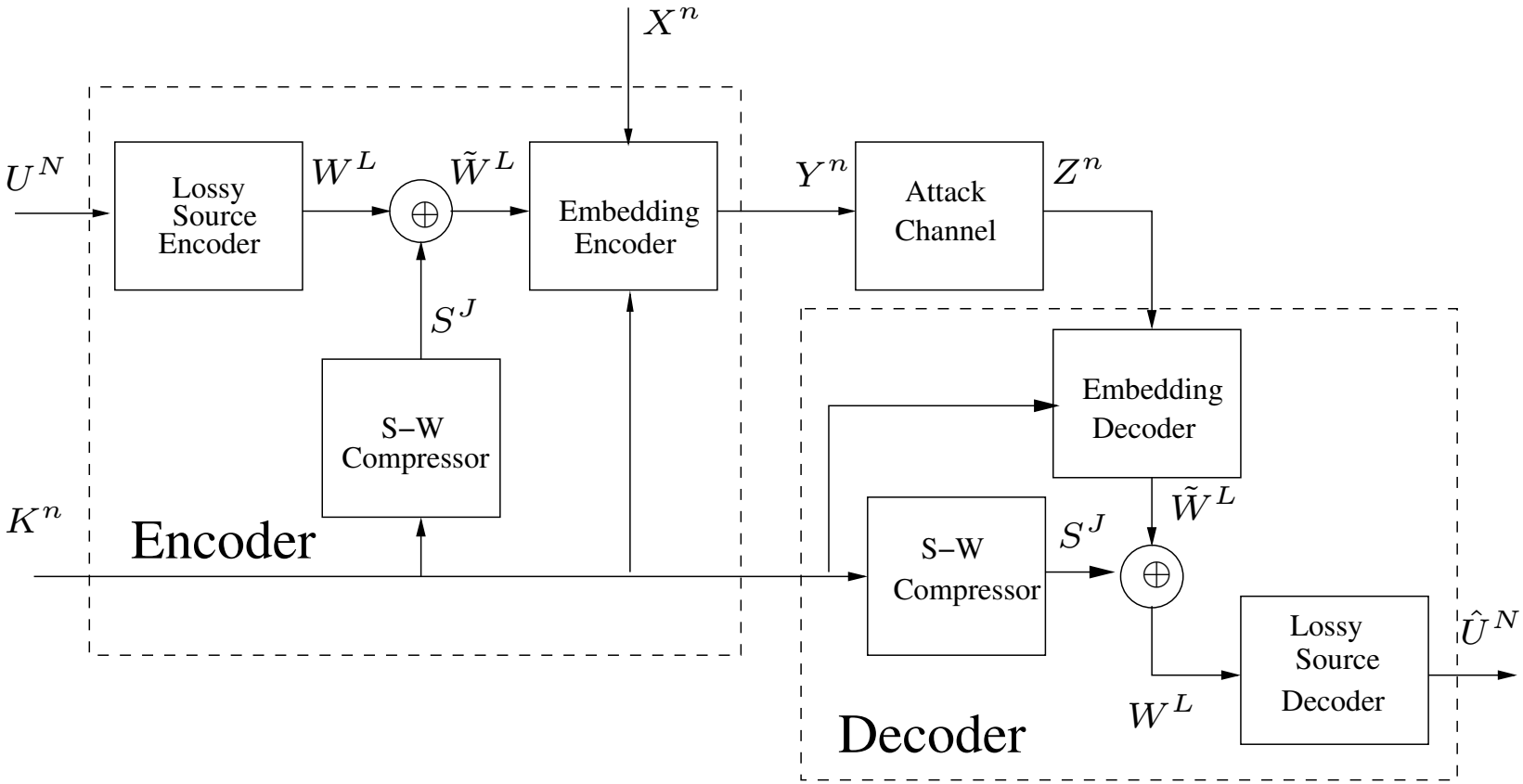
Joint coding under attack

Theorem: A quintuple (D, R_c, h, D', h') is achievable iff there exist RV's V and Y with $P(K, X, V, Y, Z) = P(X)P(K)P(V, Y|K, X)P(Z|Y)$ s.t.

- $h \leq H(K|Y)/\lambda + H(U) - R_U(D'), \quad h' \leq H(K|Y)/\lambda.$
- $\lambda R_U(D') \leq I(V; Z|K) - I(V; X|K).$
- $R_c \geq \lambda R_U(D') + I(X; Y, V|K) + I(K; Y), \quad D \geq Ed(X, Y).$

Comments:

1. No separation between encryption and WM.
2. Channel with SI: X at the encoder, K – at both ends.
3. R-D coding of U^N – still separate.


X^n
U^N
Lossy Source Encoder
W^L
$\tilde{W}^L$
Embedding Encoder
Y^n
Attack Channel
Z^n
S^J
S–W Compressor
K^n
Encoder
Embedding Decoder
$\tilde{W}^L$
S–W Compressor
S^J
Lossy Source Decoder
$\hat{U}^N$
W^L
Decoder

Embedding and Stegotext Compression

- Given K^n, generate $2^{nI(V;Z|K)}$ random codewords $\{V^n\}$ according to $P(V|K)$ and partition them into $2^{NR_U(D')}$ bins, each of size $\geq 2^{nI(V;X|K)}$.
- Given (K^n, V^n), generate $2^{nI(X;Y|V,K)}$ random stegowords $\{Y^n\}$ according to $P(Y|K,V)$.
- For (X^n, K^n), find a typical V^n within the appropriate bin.
- For (X^n, K^n, V^n), find a jointly typical Y^n.
- Compress Y^n to $\log|\{Y^n\}| \approx n[\lambda R_U(D') + I(X;Y,V|K) + I(K;Y)]$.
- The decoder estimates V^n reliably from (Z^n, K^n) and then decodes according to the bin.

Extensions

- Allowing dependence between K and X:

$$P(K^n|X^n) = \prod_{i=1}^{n} P(K_i|X_i).$$

- As K^n plays the role of SI, it makes sense to talk about "private" compression:

$$\frac{1}{n} H(Y^n|K^n) \leq R'_c.$$

What are now the achievable sixtuples $(D, R_c, h, D', R'_c, h')$?

Coding theorem revisited

Theorem: A quintuple $(D, R_c, h, D', R_c', h')$ is achievable iff there exist RV's V and Y with $P(K, X, V, Y, Z) = P(X, K)P(V, Y|K, X)P(Z|Y)$ s.t.

- $h \leq H(K|Y)/\lambda + H(U) - R_U(D'), \quad h' \leq H(K|Y)/\lambda.$
- $\lambda R_U(D') \leq I(V; Z|K) - I(V; X|K).$
- $R_c \geq \lambda R_U(D') + I(X; Y, V|K) + I(K; Y), \quad D \geq Ed(X, Y).$
- $R_c' \geq \lambda R_U(D') + I(X; Y, V|K).$

Comments:

1. K now depends on X.
2. R_c' has a similar lower bound as R_c, just without the last term.

Excess Key Rate

Thus far, we have implicitly assumed that $H(K) \leq \lambda R_U(D')$:

For the purpose of securing U^N, there is no need for more key rate.

For the purpose of further securing $\hat{U}^N$, however, excess key rate can improve secrecy.

If $H(K) > \lambda R_U(D')$, we can make $H(K|Y) > \lambda R_U(D')$, and use the $T = n[H(K|Y) - \lambda R_U(D')]$ extra key bits for selection among 2^T distinct rate–distortion codebooks among the totality of $2^{NH(\hat{U}|U)}$ that exist. Thus, it is possible to improve the security of $\hat{U}^N$ to the level of

$$h' = \min\{H(\hat{U}), H(K|Y)/\lambda\}$$

but not any further.

But once we do that, it is no longer clear that $\hat{U}$ should correspond to the rate–distortion–optimal test channel, that minimizes $I(U;\hat{U})$ subject to the distortion constraint.

Coding theorem re–revisited

Theorem: A quintuple $(D, R_c, h, D', R_c', h')$ is achievable iff there exist a channel $P(\hat{U}|U)$ and RV's V and Y as before s.t.

- $h \leq H(U) - [I(U;\hat{U}) - H(K|Y)/\lambda]_+$.
- $h' \leq \min\{H(\hat{U}), H(K|Y)/\lambda\}$.
- $\lambda I(U;\hat{U}) \leq I(V;Z|K) - I(V;X|K)$.
- $R_c \geq \lambda I(U;\hat{U}) + I(X;Y,V|K) + I(K;Y), \quad D \geq Ed(X,Y)$.
- $R_c' \geq \lambda I(U;\hat{U}) + I(X;Y,V|K)$.
- $D' \geq Ed'(U,\hat{U})$.

Separation fails completely now, as the test channel $U \to \hat{U}$ is affected here by the other ingredients of the system.

Conclusion

- Defining and studying a framework of combined WM, encryption, and compression.
- Substantial differences between the cases with and without attack.
- Cryptographic key may play a role of SI.
- Separation holds in simple special cases, but falls apart with increasing generality.
- Characterizing structures of optimal coding systems.

Future Questions

- The case where the stegotext has to be secured.
- Allowing a non–memoryless channel $P(K^n|X^n)$.
- Key distribution via a capacity–limited channel.
- Devising practical algorithms (linear/lattice, Turbo, LDPC codes).
- Public–key methods.

THANK YOU!!