A Joint Source-Channel Coding Scheme for Image-in-Image Data Hiding

K. Solanki, O. Dabeer, B. S. Manjunath,
U. Madhow, and S. Chandrasekaran

Vision Research Laboratory
Department of Electrical and Computer Engineering
University of California, Santa Barbara CA 93106 USA

http://vision.ece.ucsb.edu

Outline

- Motivation
  - New criterion for hiding: Graceful improvement
- Contribution
  - Hybrid Digital-Analog Hiding Scheme
  - Analog Information Hiding
  - MMSE Decoding for JPEG Attacks
- Implementation Issues
- Examples
- Conclusion and future work

Image-in-Image Hiding

- **Goal**: To hide an image called *signature* image into another image called *host* or *cover* image.
- **Design Criteria, or Requirements**:
  1) Transparency: The degradation to the *host* image should be imperceptible.
  2) Robustness: It should be possible to recover the *hidden*, or *signature* image under a variety of attacks.
  3) Capacity: It should be possible to hide large *signature* images.
- A number of hiding schemes that satisfy these criterion have been proposed, e.g., [Chou et al `00], [Chen & Wornell `01], and [Jacobsen et al `02].

Previously Proposed Scheme: Example

Original 512x512 Host Image

Original 256x256 Signature Image

← Design QF=50

Previously Proposed Scheme: Example

Hidden/Composite Image

Recovered 256x256 Signature Image

Recovered after JPEG attack at QF=50

Another Criterion: Graceful Improvement

- Graceful improvement: The quality of the recovered signature image should be better if the attack is milder.
- Motivation:
  - Attack level is seldom known apriori.
  - Broadcast scenario: There could be multiple receivers with different attack channels.

Graceful Improvement: How?

- Graceful improvement and degradation in signal fidelity requires *joint* source-channel coding.
- Joint source-channel coding has been studied for the Gaussian channel, e.g., [Chen and Wornell `98], [Mittal and Famdo `02], [Skoglund et al `02], [Vaishampayan and Costa `03].
- Such schemes have not been studied for the data hiding channel (to the best of our knowledge).
- Somewhat related work: [Wu and Liu `03] propose *multiple bit hiding*, but for different application and approach.

Joint Source Channel Hiding: Fundamental Limits

- We consider fundamental limits for the Gaussian data hiding channel.
- Formulation:
  - Consider an i.i.d. Gaussian signature source with zero mean and variance σ^2.
  - The hider is at most allowed to introduce a mean squared error of D_1 per host symbol.
  - Gaussian attack introduces an additional distortion of at most D_2 per host symbol.
  - We are interested in recovering the signature image with distortion of D_3 per signature symbol.
  - There are ρ channel uses (or host symbols) per source (or signature) symbol.

Joint Source Channel Hiding: Fundamental Limits (Cont.)

- From the information capacity results [Costa `83],

$$C = \frac{1}{2}\log\left(1+\frac{D_1}{D_2}\right)$$

- From the rate distortion theory,

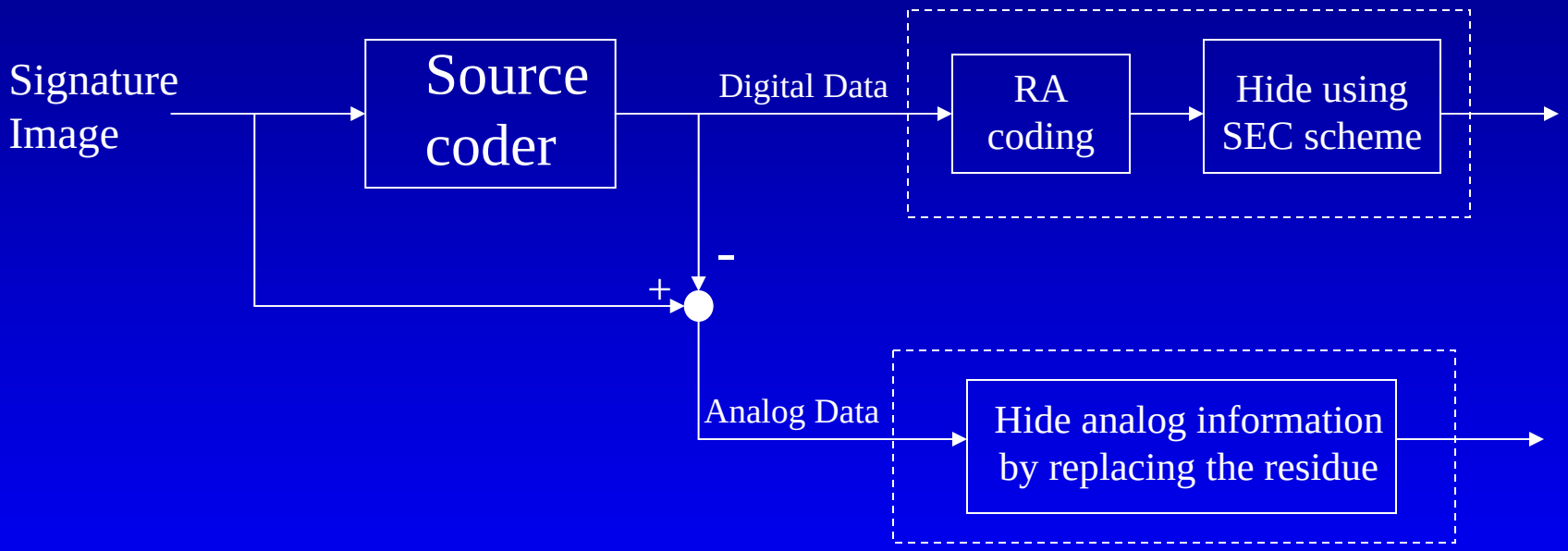
$$R(D_3) = \frac{1}{2}\log\frac{\sigma^2}{D_3}$$

- For hiding ρ symbols per channel use, we have, $R(D_3) \le \rho C$. Thus, we can deduce that,

$$D_3 \ge \frac{\sigma^2}{\left(1+\frac{D_1}{D_2}\right)^{\rho}}$$

Hybrid Digital-Analog Hiding

The signature image is divided into digital data and analog residue.



Hiding Analog Information

- We propose a new strategy to hide an analog number into a host sample.

Hiding using scalar quantization of the host

- To hide an analog number *m* into a host sample *h*:
  - Quantize the host *h* using a quantizer of step size Δ.
  - Scale the source *m* to lie in the interval $(0, \Delta)$.
  - Replace the residue with the scaled source.
- The message *m* is always measured from an even reconstruction point.

Hiding Analog Information: Example

- Let us consider an example $\Delta = 1$, and the host symbol $h = 6.235$
- Say, we want to hide a source symbol $m = 0.729$ (a real number $\in (0, \Delta)$)
- The encoder first determines that the host symbol lies between 6 and 7, then it sends the source symbol directly within that interval, i.e., 6.729.
- Note: if the host symbol is, say, 5.341 (between 5 and 6), then the symbol sent is 5.271 (0.729 measured from 6).

Hiding Analog Information (Cont.)

- The symbol y to be sent for hiding a message m into a host symbol h is given by,

$$y = \Delta\left(\left\lfloor h/\Delta \right\rfloor\right) + m, \qquad \text{if } \left\lfloor h/\Delta \right\rfloor \text{ is even,}$$

$$= \Delta\left(\left\lfloor h/\Delta \right\rfloor + 1\right) - m, \qquad \text{if } \left\lfloor h/\Delta \right\rfloor \text{ is odd.}$$

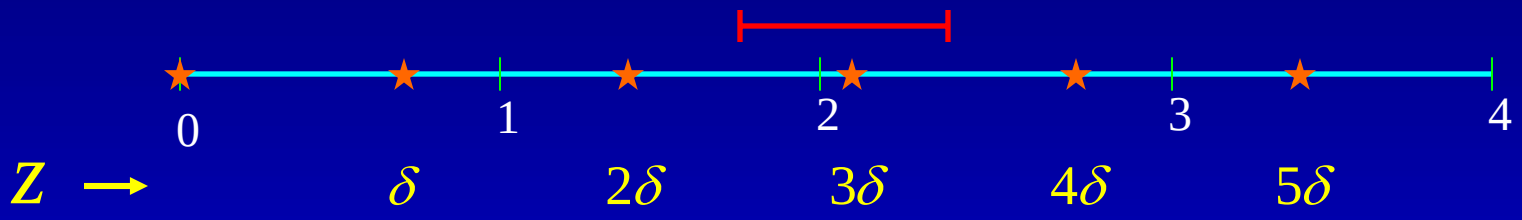
JPEG attacks and MMSE decoding

- Decoding: Varying levels of JPEG compression are considered at the decoder.
- Assumption: The decoder knows the attack level, but the encoder does not.
- We derive the *minimum mean squared error* (MMSE) decoder for the proposed hiding scheme under uniform quantization attack.

MMSE Decoder for JPEG attack

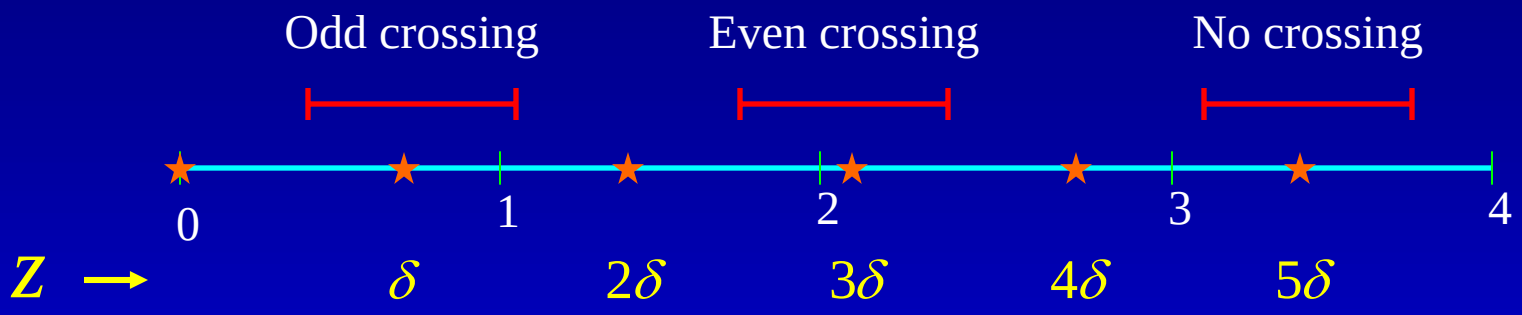
- We consider the case of hiding a uniform random variable $\boldsymbol{m} \sim U[0,1]$ into an independent host coefficient $\boldsymbol{h}$ to obtain $\boldsymbol{y}$.
- Without loss of generality, we assume $\Delta = 1$.
- We restrict our attention only to attacks with quantization interval less than or equal to the design interval.
- Denoting the attack quantization interval $\delta \leq 1$, the received symbol $z = Q(y)$.
- The MMSE decoder is simply the conditional expectation $E[\boldsymbol{m}/\boldsymbol{z}=z]$.

MMSE Decoder for JPEG attack (II)



- Thus, $z \in \{..., -2\delta, -\delta, 0, \delta, 2\delta, ...\}$
- Ambiguity interval: If $z = a\delta$ is received, then y necessarily lies in the interval $[(a-1/2)\delta, (a+1/2)\delta]$, which we call its *ambiguity* interval.

MMSE Decoder for JPEG attack (III)



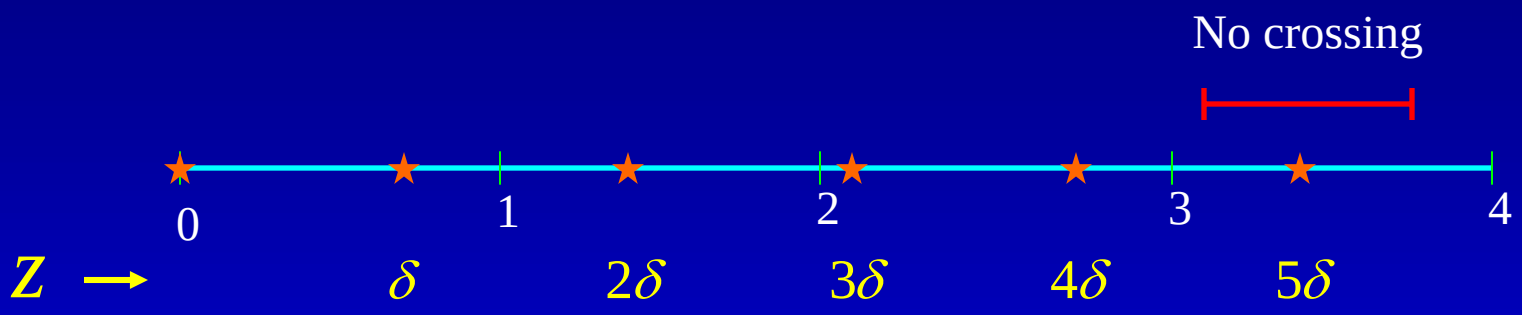
- Consider the integer interval $[n, n+1)$ in which z is received:

(i) No crossing: The ambiguity interval of y does not cross into another integer interval.

(ii) Even crossing: The ambiguity interval crosses an even integer.

(iii) Odd crossing: The ambiguity interval crosses an odd integer.

MMSE Decoder for JPEG attack (IV)



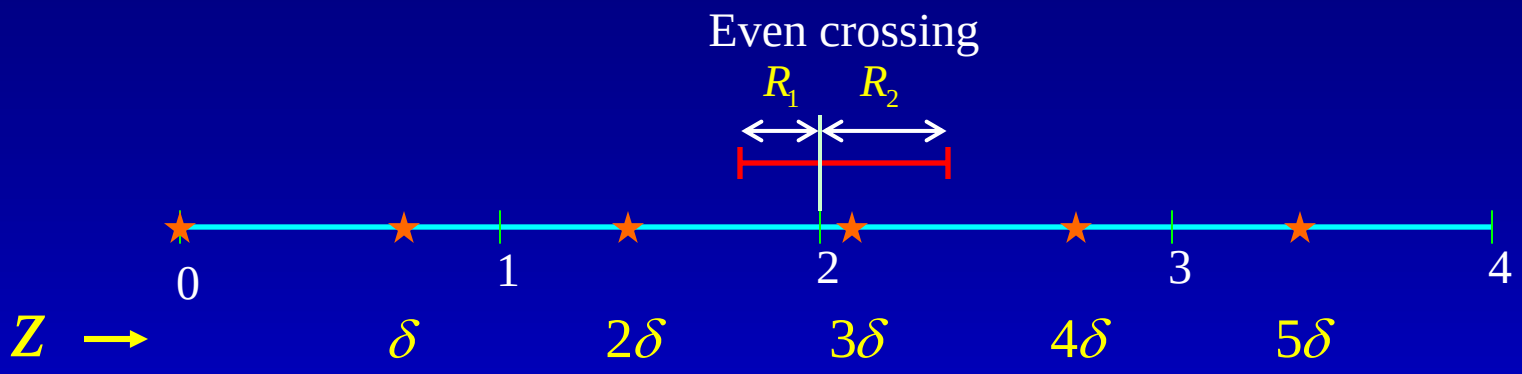
- No crossing: in this case,

$$f_{m/z}(m/z) = U\left[(a-1/2)\delta,(a+1/2)\delta\right]$$

- The corresponding MMSE estimate is,

$$\hat{m} = z - n \quad \text{if n even,}$$
$$= (n+1) - z \quad \text{if } n \text{ odd.}$$

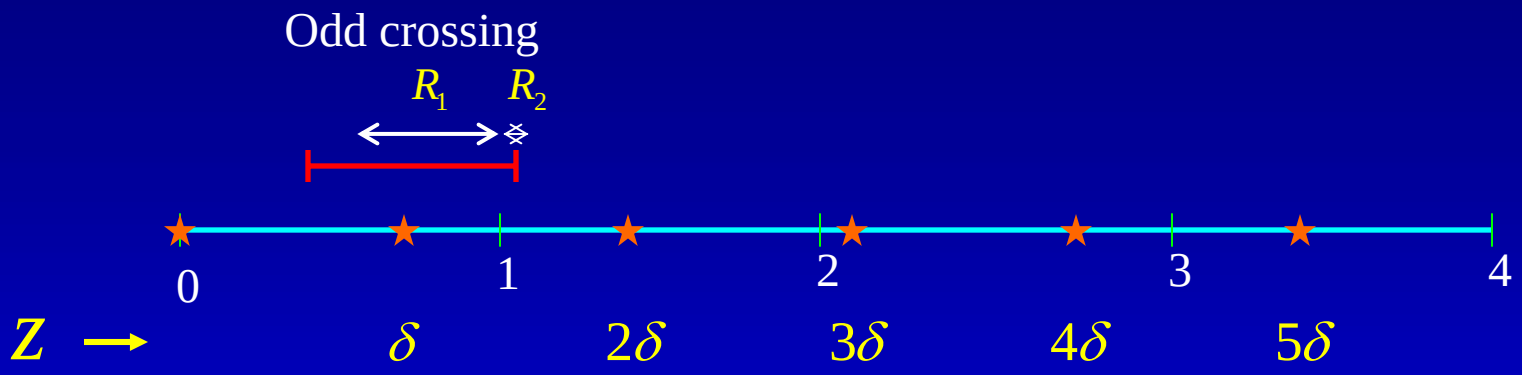
MMSE Decoder for JPEG attack (V)



- Even crossing: Define R_1 and R_2 as shown.
- MMSE estimate: Applying Bayes' rule and after some simplifications, we get the MMSE estimate as,

$$\hat{m} = \frac{\delta}{2} - \frac{R_1 R_2}{\delta}$$

MMSE Decoder for JPEG attack (VI)



- Odd crossing: Analysis similar to the even case.
- MMSE estimate given as,

$$\hat{m} = 1 - \frac{\delta}{2} + \frac{R_1 R_2}{\delta}$$

Image-in-Image Hiding: Implementation

Encoding process:

1. Processing the signature image
   - Separate signature image into analog and digital parts.
   - Digital part: JPEG compressed bitstream.
   - Analog part: Residues of pre-selected DCT coefficients.
2. Allocating the channels
   - Allocate the host coefficients for analog and digital parts.
   - A few low frequency coefficients are reserved for analog channel.
   - Other channels form the candidate band for digital hiding.
3. Hiding the digital part
   - RA coded selectively embedding in coefficient (SEC) scheme is used to hide digital information.
4. Hiding the analog part
   - Analog part is sent using the proposed method.

Example 1

- Hiding 128x128 image into a 512x512 image with design quality factor (QF) of 25.
- Processing the signature image:
  - Image compressed at QF=10, forming the digital part.
  - Residues of 16 low frequency coefficients form the analog part.
- Allocating the channels:
  - One coefficient each from each 8x8 block forms the analog channel.
  - 34 coefficients form the candidate band for the digital channel.

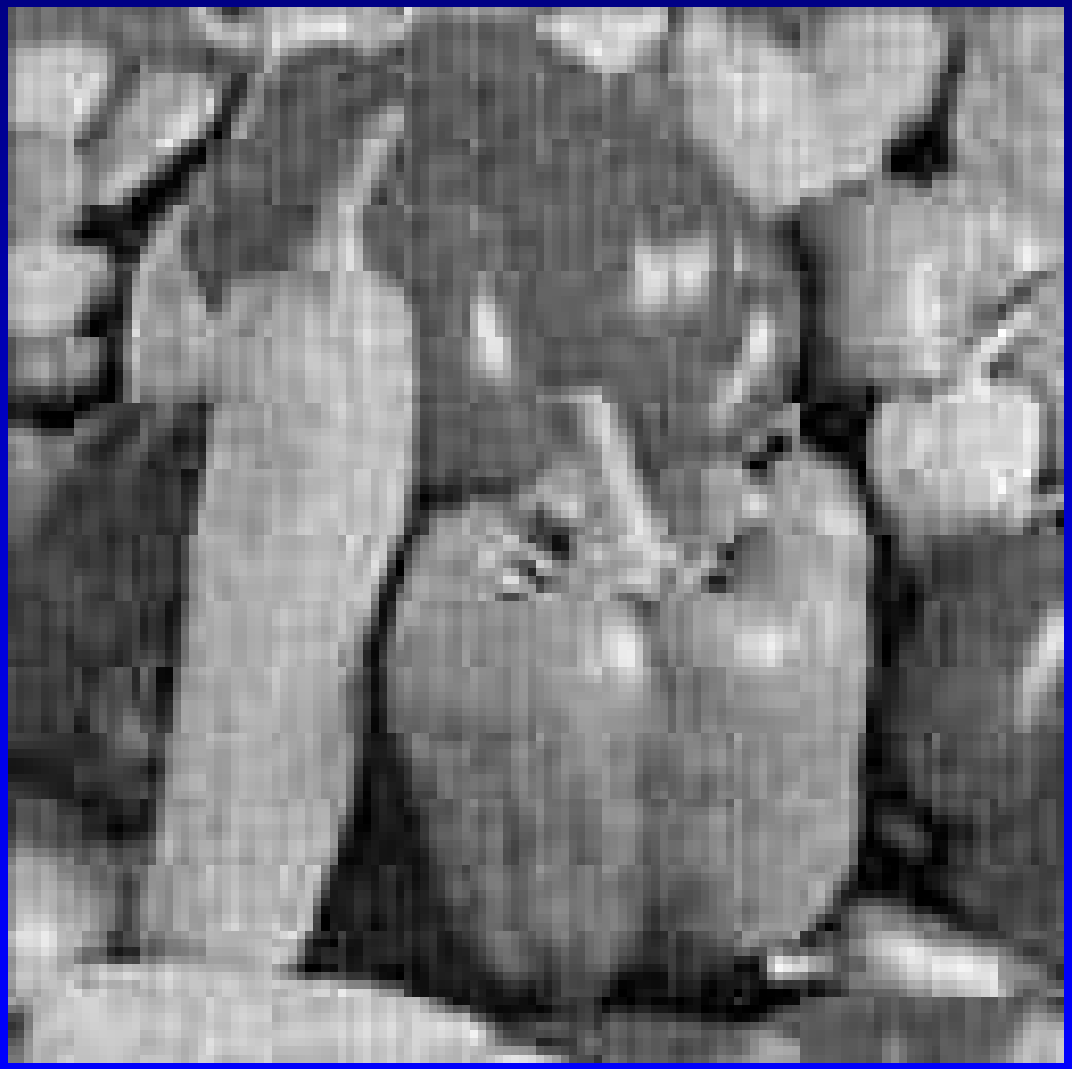
Example 1: Host Image

Original 512x512 Harbor image

Harbor image with
128x128 peppers image hidden

Received Signature Image: Attack QF = 25 (93.5% compr.) MSE = 0.0286

Received Signature Image:
Attack QF = 30 (92.4% compr.) MSE = 0.0373



Received Signature Image:
Attack QF = 35 (90.4% compr.) MSE = 0.0321

Received Signature Image:
Attack QF = 40 (89.6% compr.) MSE = 0.0275

Received Signature Image:
Attack QF = 45 (88.7% compr.) MSE = 0.0193

Received Signature Image:
Attack QF = 50 (88.0% compr.) MSE = 0.0128

Received Signature Image:
Attack QF = 55 (87.2% compr.) MSE = 0.0149

Received Signature Image:
Attack QF = 60 (86.2% compr.) MSE = 0.0145

Received Signature Image:
Attack QF = 65 (85.0% compr.) MSE = 0.0119

Received Signature Image:
Attack QF = 70 (83.6% compr.) MSE = 0.0087

Received Signature Image:
Attack QF = 75 (81.9% compr.) MSE = 0.0060

Received Signature Image:
Attack QF = 80 (79.4% compr.) MSE = 0.0059

Received Signature Image:
Attack QF = 85 (75.8% compr.) MSE = 0.0043

Received Signature Image:
Attack QF = 90 (70.0% compr.) MSE = 0.0029

Received Signature Image:
Attack QF = 95 (57.7% compr.) MSE = 0.0025

Received Signature Image: No Attack

Example 2

- Here, we hide a larger image (a 256x256 image) with a higher design QF of 50.
- Processing the signature image:
  - The signature image is JPEG compressed at QF=18, and residues of 12 low frequency coefficients constitute the analog part.
- Allocating the channels
  - 3 coefficients per block are used for sending analog residue and 32 coefficients per block form the candidate embedding band for the digital data.

Example 2: Host Image

Original 512x512 Bridge image

Bridge image with
256x256 Lena image hidden

Received Image: Attack QF = 50 (84.3% compr.) MSE = 0.0267

Received Image: Attack QF = 55 (83.2% compr.) MSE = 0.0398

Received Image: Attack QF = 60 (81.9% compr.) MSE = 0.0371

Received Image: Attack QF = 65 (80.2% compr.) MSE = 0.0319

Received Image: Attack QF = 70 (78.3% compr.) MSE = 0.0254

Received Image: Attack QF = 75 (76.1% compr.) MSE = 0.0162

Received Image: Attack QF = 80 (72.5% compr.) MSE = 0.0140

Received Image: Attack QF = 85 (67.8% compr.) MSE = 0.0090

Received Image: Attack QF = 90 (60.0% compr.) MSE = 0.0046

Received Image: Attack QF = 95 (45.1% compr.) MSE = 0.0025

Received Image: No Attack

Conclusions and Future Work

- We demonstrated a simple gracefully improving image-in-image hiding method. As the JPEG attack quality factor increases, the signature image is received with better quality.
- A new method to hide analog information was proposed.

Future work:

- Using better and more suited compression mechanisms for signature image compression (such as SPIHT).
- Exploring various other joint source-channel coding strategies for this application.

Thank You

http://vision.ece.ucsb.edu