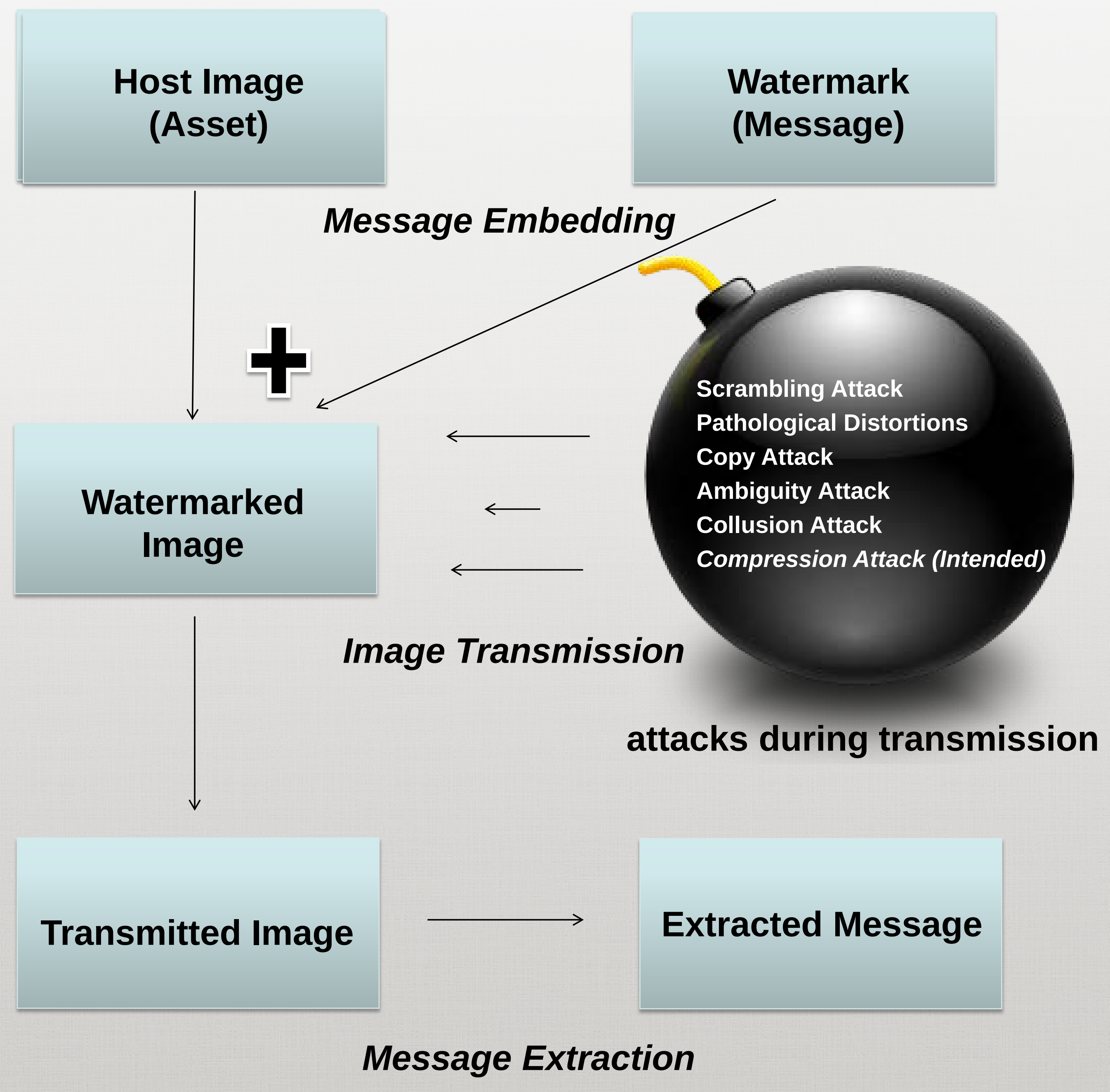
Robustness Analysis on DCT Watermarking Technique Under Compression Attack

Zehua Jin[1], Shengrong Wu[1], William Xie[1], Yize Zhao[1]
1 - Department of Electrical & Computer Engineering, Rice University, Houston, 77005, USA
DGTWTMK@gmail.com

Digital Watermarking Procedure


Host Image (Asset)

Watermark (Message)

Message Embedding

+

Watermarked Image

Scrambling Attack
Pathological Distortions
Copy Attack
Ambiguity Attack
Collusion Attack
Compression Attack (Intended)

Image Transmission

attacks during transmission

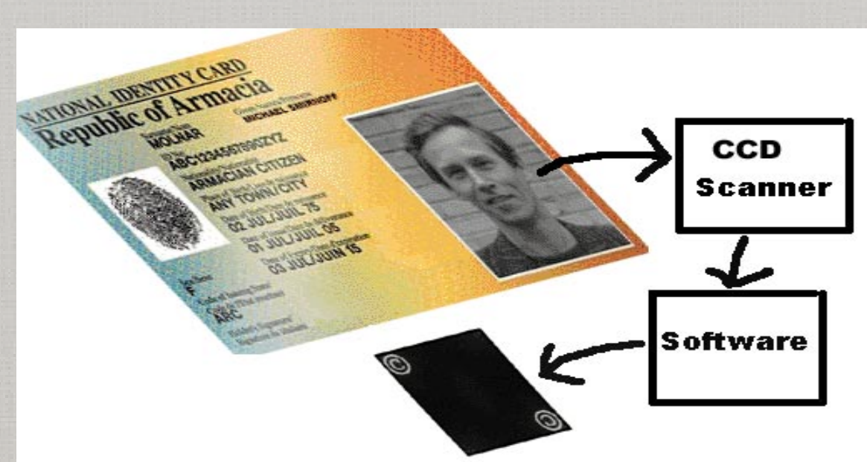
Transmitted Image

Extracted Message

Message Extraction

Digital Watermarking Applications

- Deter *digital counterfeiting bank notes*
- *Copyright protection*
- ID Card security
- Fingerprinting
- Ownership assertion
- Fraud & temper detection



e.g. Hidden watermark on ID , which can be detected by CCD scanner

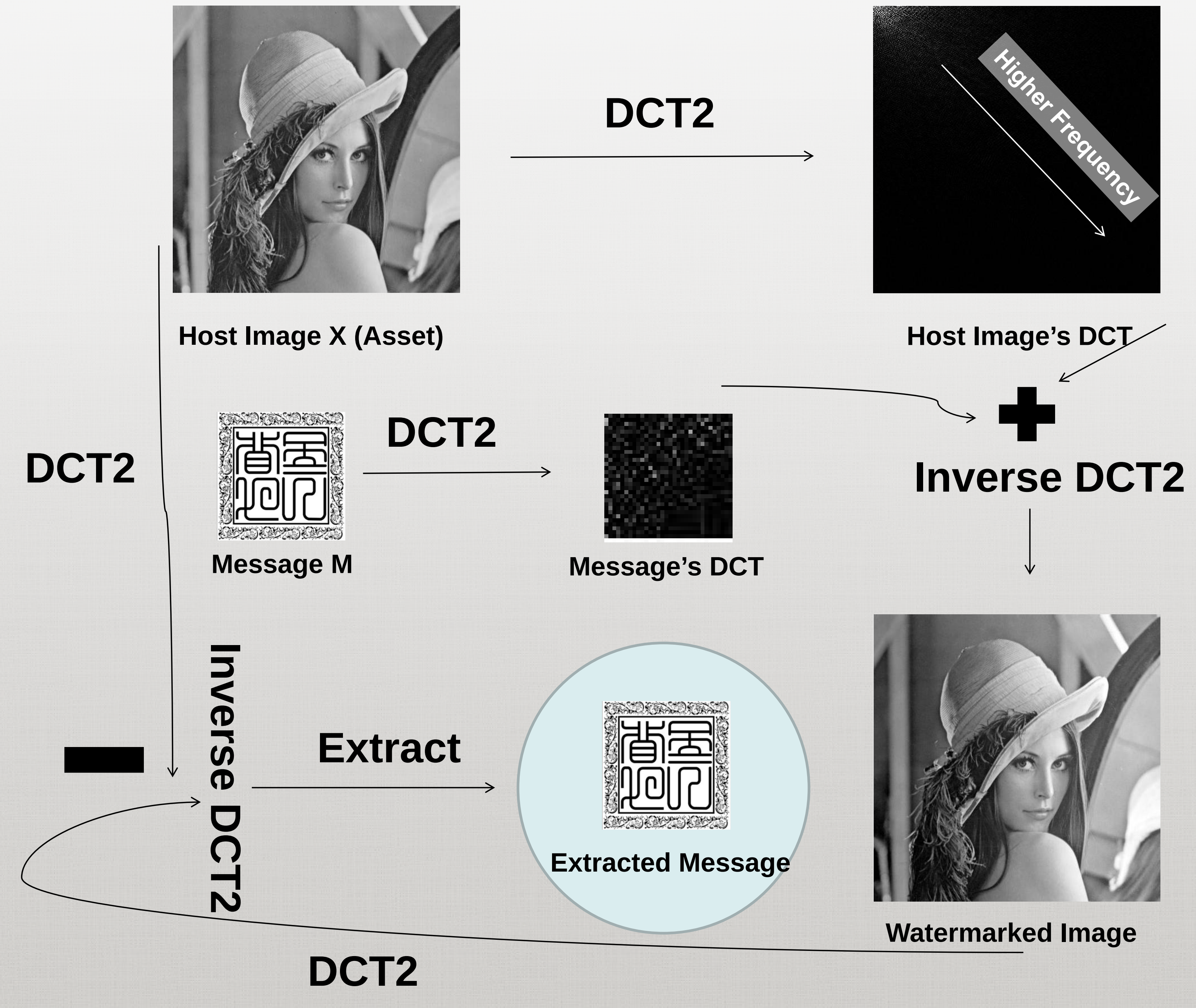
Watermarking in Spectral Domain by Discrete Cosine Transform, an Approach that has been Cited 2837 Times

- More efficient
- *Energy compaction*
- Larger confidents get wiped out

But Where to Apply it?

We need to know its robustness to decide its applications!

DCT Watermarking Algorithm



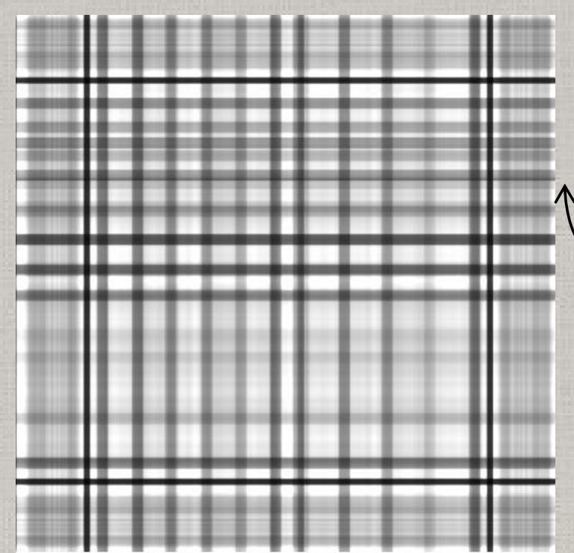
However…with some attacks, such as SVD compressions…

Try some singular value decomposition compressions!

blurry watermarked image at 10 iterations

watermarked image at 50 iterations

extracted image getting blurry at 50 iterations



extracted image barely recognizable at 10 iterations

Robustness Analysis

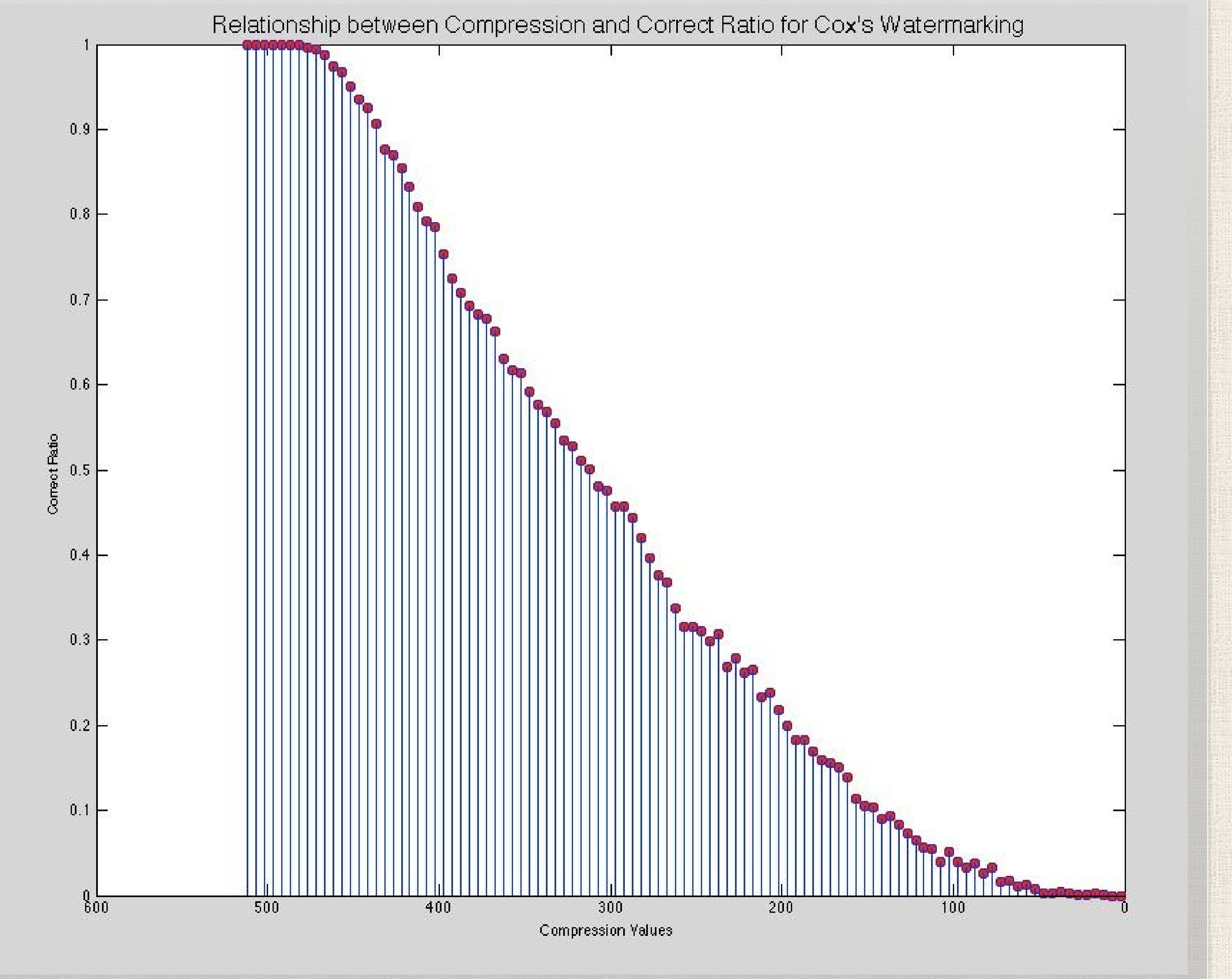
Goal

To compare the extracted message with the original message at different compression ratio

Method

- use a length-1000 randomly generated vector as message
- extract vector x1, the extracted message, represented as a vector (DCT,embedding, summation, singular compression, extraction)
- extract vector x0, the original message ,presented as a vector (reshaped original matrix)
- convert both message into the same length, L
- correct ratio=number of corrected element/L (how much percentage of elements were successfully extracted

Result



Conclusions

- At very large compression iterations and very small compression iterations, correct ratio remain relatively unchanged when compression iterations changes slightly
- Between 100-450 iterations, the correct ratio has a linear behavior

Future Work

- to plot visibility VS compression value
- to include color image watermarking
- to compare the robustness of this algorithm with others

1.Chandramouli, R., Nasir Memon, and Majid Rabbani. "Digital watermarking." *Encyclopedia of Imaging Science and Technology* (2002).
2. Fridrich, Jessica, and Miroslav Goljan. "Comparing robustness of watermarking techniques." *Electronic Imaging'99*. International Society for Optics and Photonics, 1999.
3. Voloshynovsky, S., et al. "Generalized watermarking attack based on watermark estimation and perceptual remodulation." *Proceedings of SPIE: Security and Watermarking of Multimedia Content II, San Jose, CA, USA* (2000).
4. Voloshynovskiy, Sviatolsav, et al. "Attacks on digital watermarks: classification, estimation based attacks, and benchmarks." *Communications Magazine, IEEE* 39.8 (2001): 118-126.
5. Cox, Ingemar J., et al. "Digital watermarking." U.S. Patent No. 5,915,027. 22 Jun. 1999.
6. Cao, Lijie. "Singular value decomposition applied to digital image processing." *Division of Computing Studies, Arizona State University Polytechnic Campus, Mesa, Arizona State University polytechnic Campus* (2006).