Watermark Security via Secret Wavelet Packet Subband Structures

Werner Dietl, Andreas Uhl
{wdietl,uhl}@cosy.sbg.ac.at

Overview

- Introduction
- Tree Decompositions
- Embedding Variations
- Security Assessment
- Quality Assessment
- Conclusions

Introduction

- Digital watermarking for copyright protection and integrity verification
- Invisible digital image watermarking for copyright protection
- Discrete Cosine Transform (DCT) used in JPEG compression standard
- Discrete Wavelet Transform (DWT) an alternative to DCT, many advantages
- DWT used in JPEG2000
- Existing watermarking schemes by Kim, Wang and Xia use the DWT

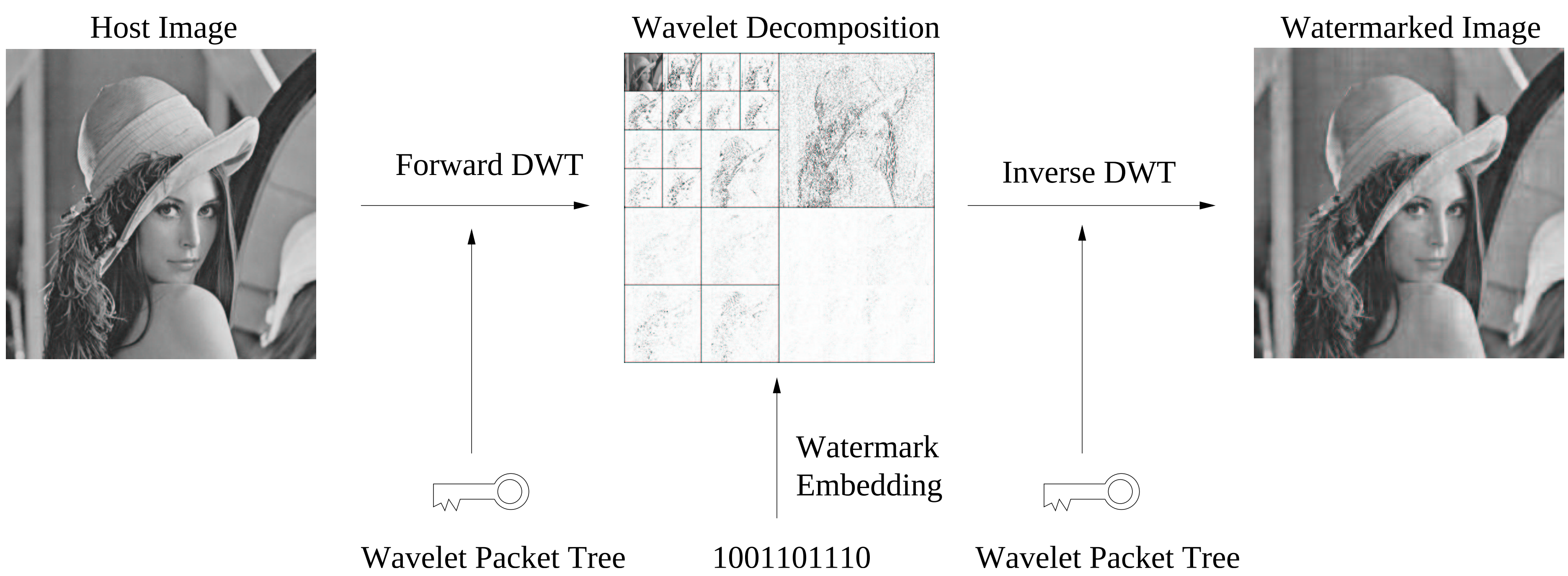
Wavelet Packet Decomposition

- Standard pyramidal decomposition only recursively decomposes the approximation subband LL
- Wavelet Packet decomposition more general and allows to decompose any subband
- Special algorithms for image compression to find good decomposition
- We look at two different Wavelet Packet decompositions
- Both with either 4 or 7 decomposition levels

Previous Work

- Wang uses one non-pyramidal decomposition
- Tsai uses wavelet packets, but no details are given
- Vehel uses the wavelet packet decomposition itself as the watermark
- Pommer uses random wavelet packet decompositions for secure image compression

Watermarking with the Wavelet Packet Decomposition



Watermarking Algorithm

- Implemented the Wang algorithm
- Wang proposed keeping the decomposition structure secret
- But no experimental results shown
- Use the Biorthogonal 7/9 filter for decompositions

Decomposition Strategy 1

- Random decomposition of subbands
- 50% likeliness of decomposition for every subband
- Number of possible trees for n+1 decompositions, A. Pommer ($f(0) = 1$):

$$f(n) = \sum_{i=0}^{4} \binom{4}{i} \cdot (f(n-1))^i$$

- For 4 levels around 2^{65} trees
- For 7 levels around 2^{4185} trees

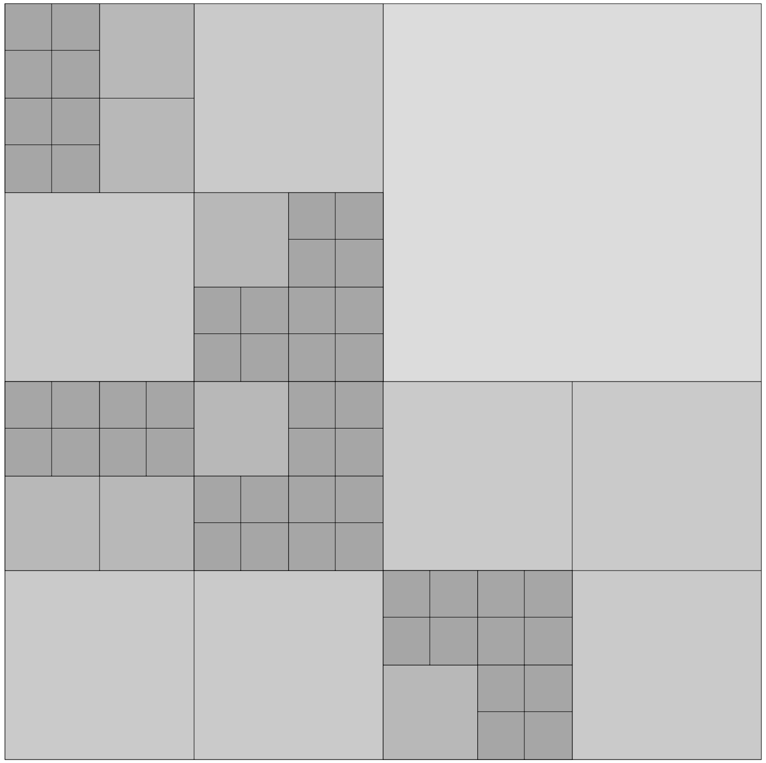
Decomposition Strategy 2

- Random decomposition with emphasis on middle frequencies
- No decomposition of HL_1, LH_1 and HH_1
- More likeliness for decompositions on levels 3 and 4
- Less likeliness to become a pyramidal decomposition
- Number of possible trees: one level fewer than for decomposition 1
- For 4 levels around 83521 trees
- For 7 levels around 2^{1046} trees

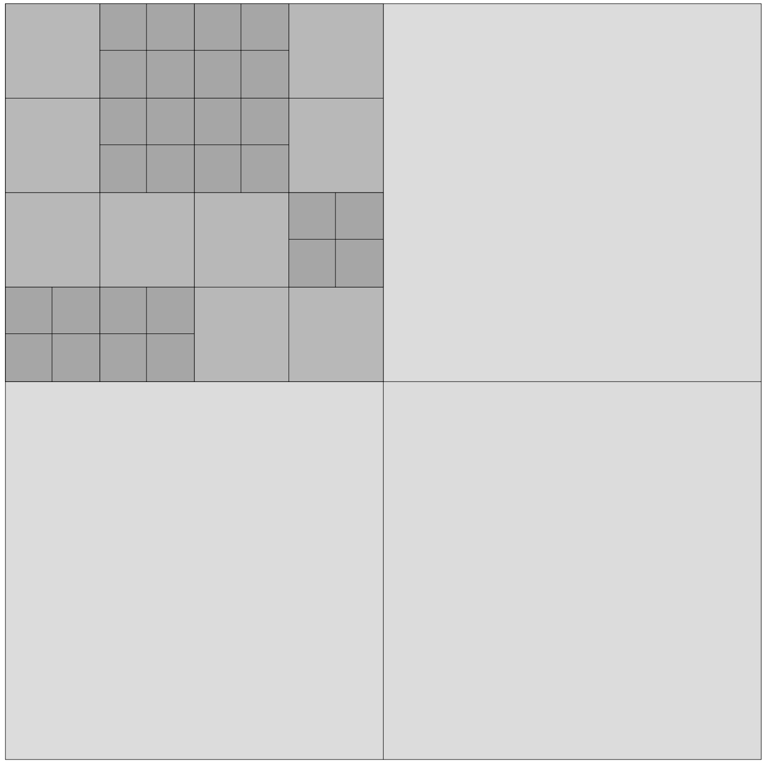
Tree Decomposition

- Use a tree number to initialise a PRNG
- Different tree numbers produce very different trees
- Close-together tree numbers do not produce similar trees

Example for Decomposition 1, 4 Levels

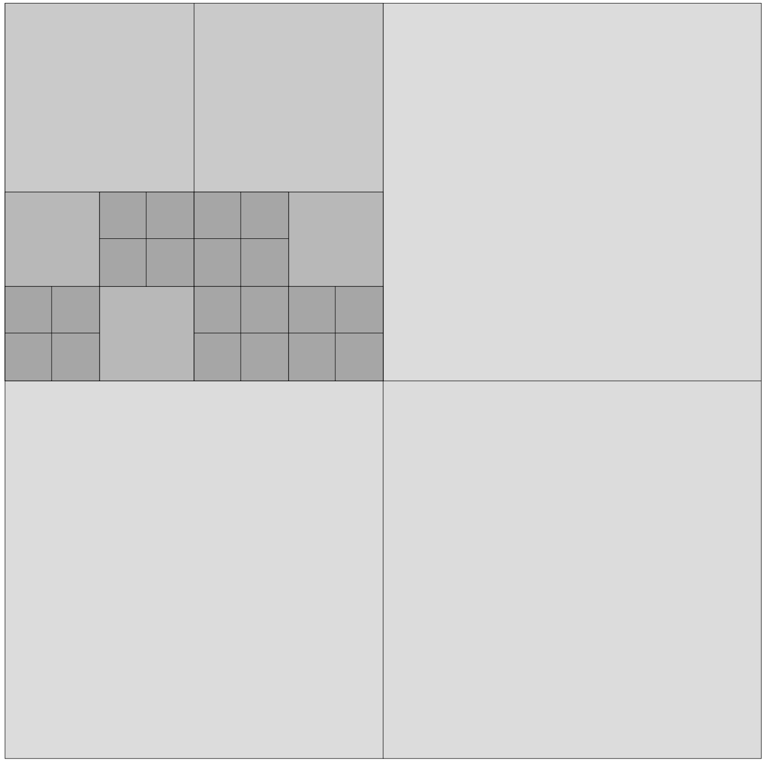


Tree 150000

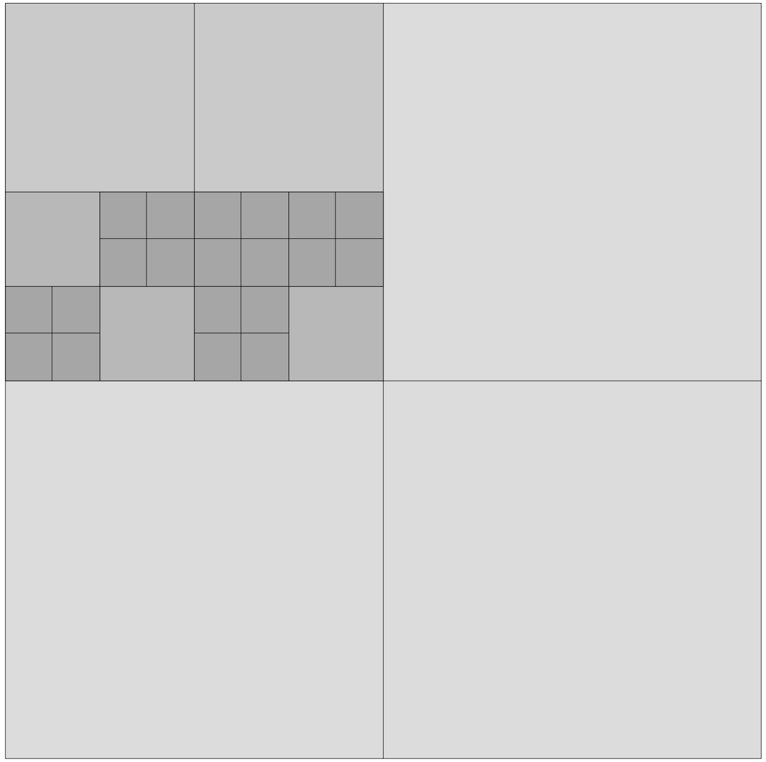


Tree 200000

Example for Decomposition 2, 4 Levels



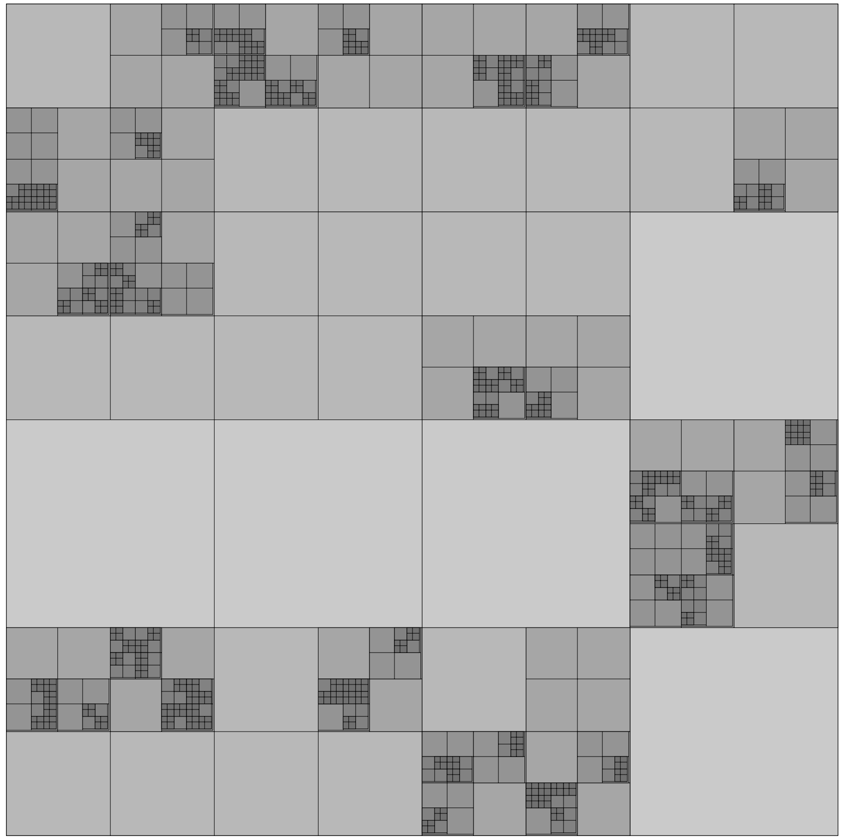
Tree 150000



Tree 200000

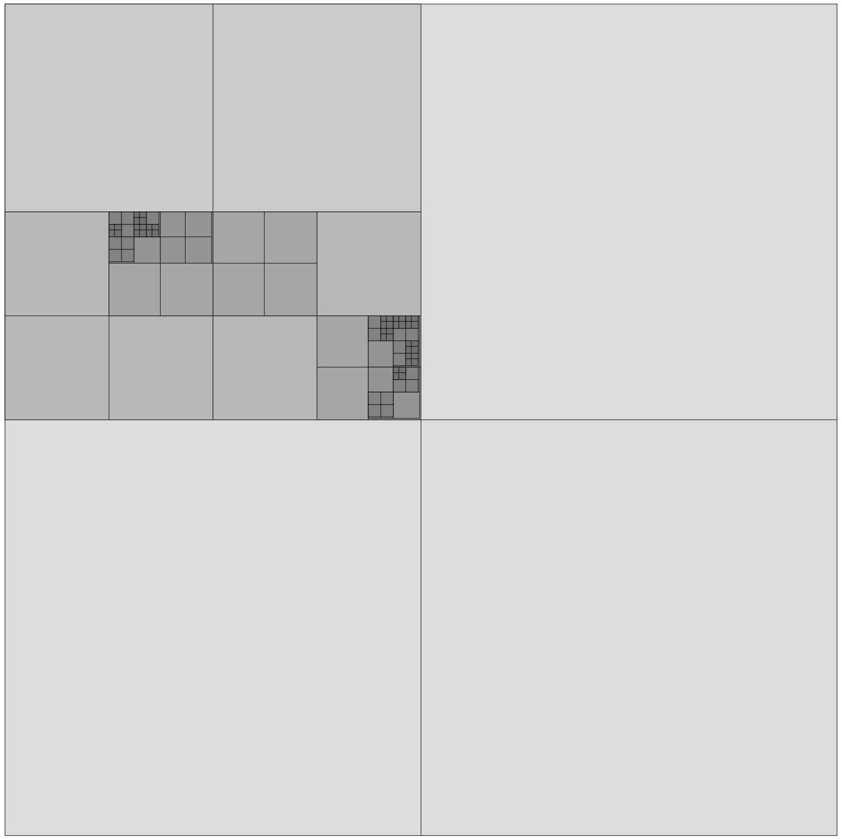
Example for Decomposition 1, 7 Levels

Tree 150000

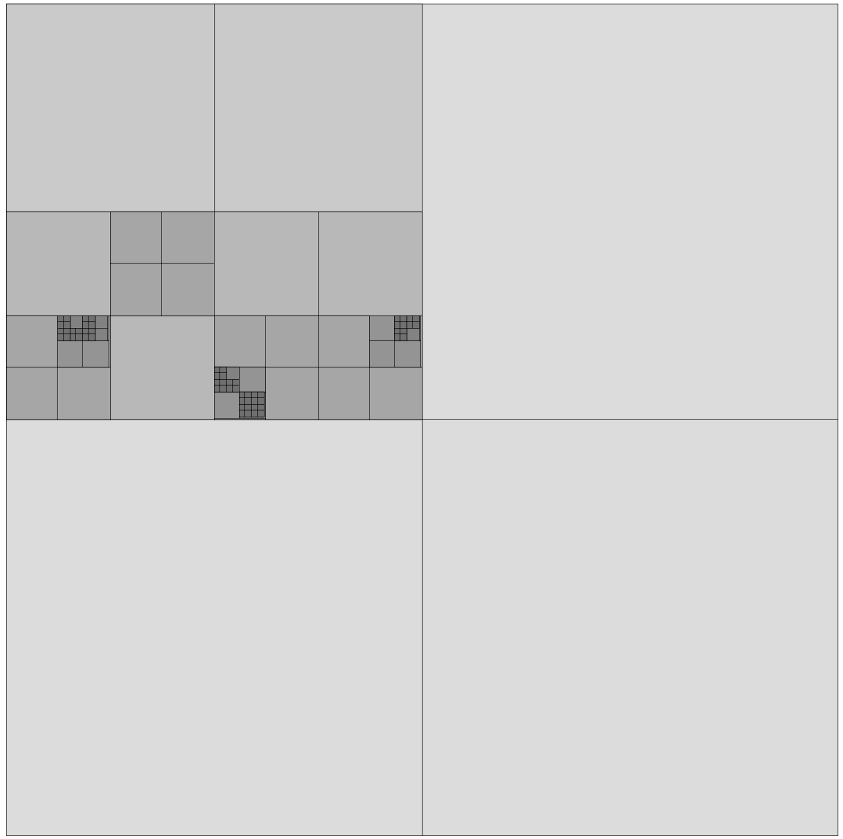


Tree 200000

Example for Decomposition 2, 7 Levels



Tree 150000



Tree 200000

Embedding Variations

- Common subtries are likely to happen, especially for few decomposition levels
- Add an additional element of randomness
- For simplicity we reuse the tree number as seed
- We could use this as second key number

Variation 1 — Tree-dependent Coefficient Skipping

- Only use 95% of the selected coefficients
- Initialise PRNG with the tree number as seed
- For every coefficient that Wang selects test whether $PRNG <= 0.95$
- Coefficient skipping also proposed in Wang paper, but no results shown

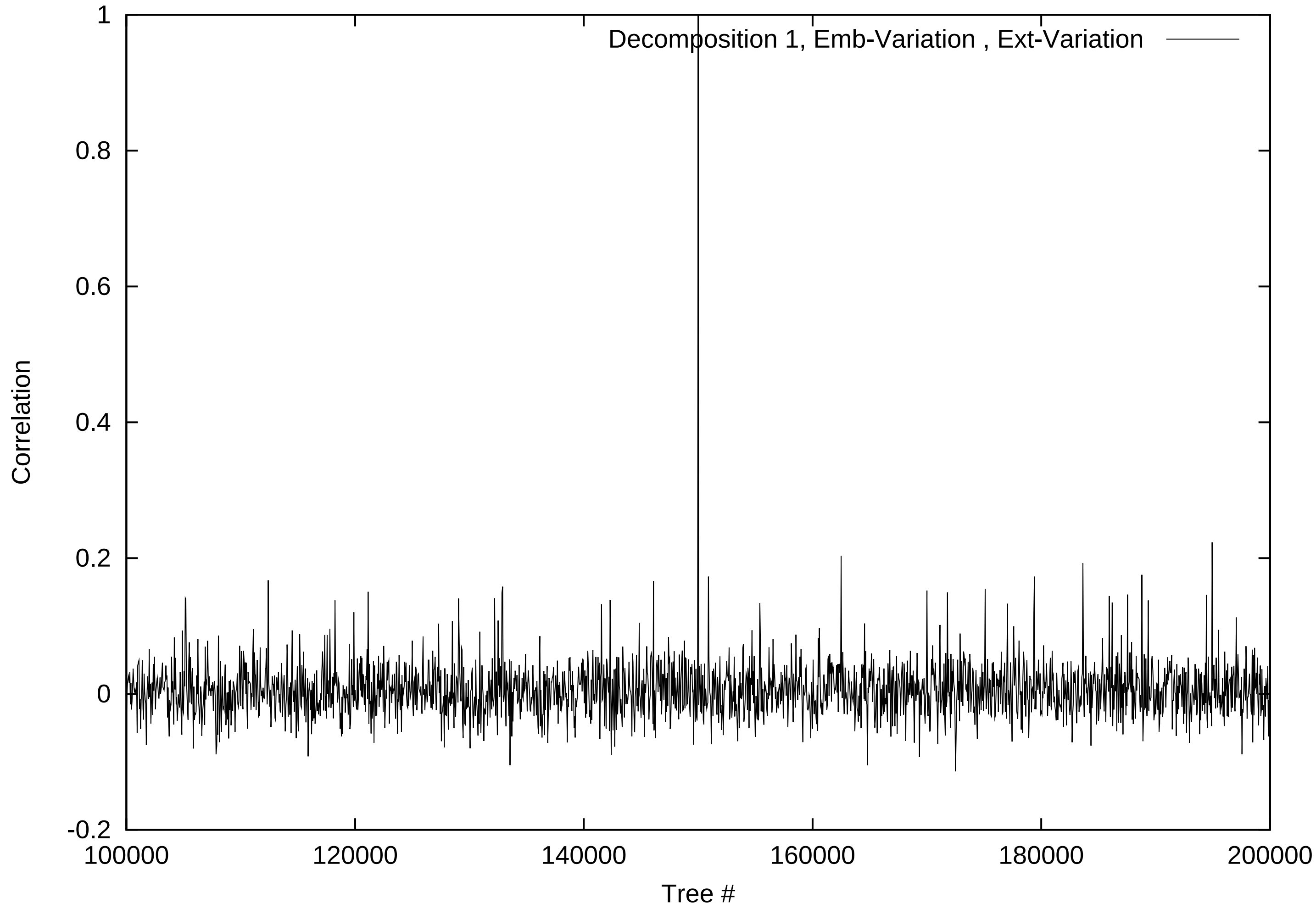
Variation 2 — Tree-dependent Watermark Shuffling

- Create a random permutation of the watermark before embedding it
- Use the tree number to determine the permutation

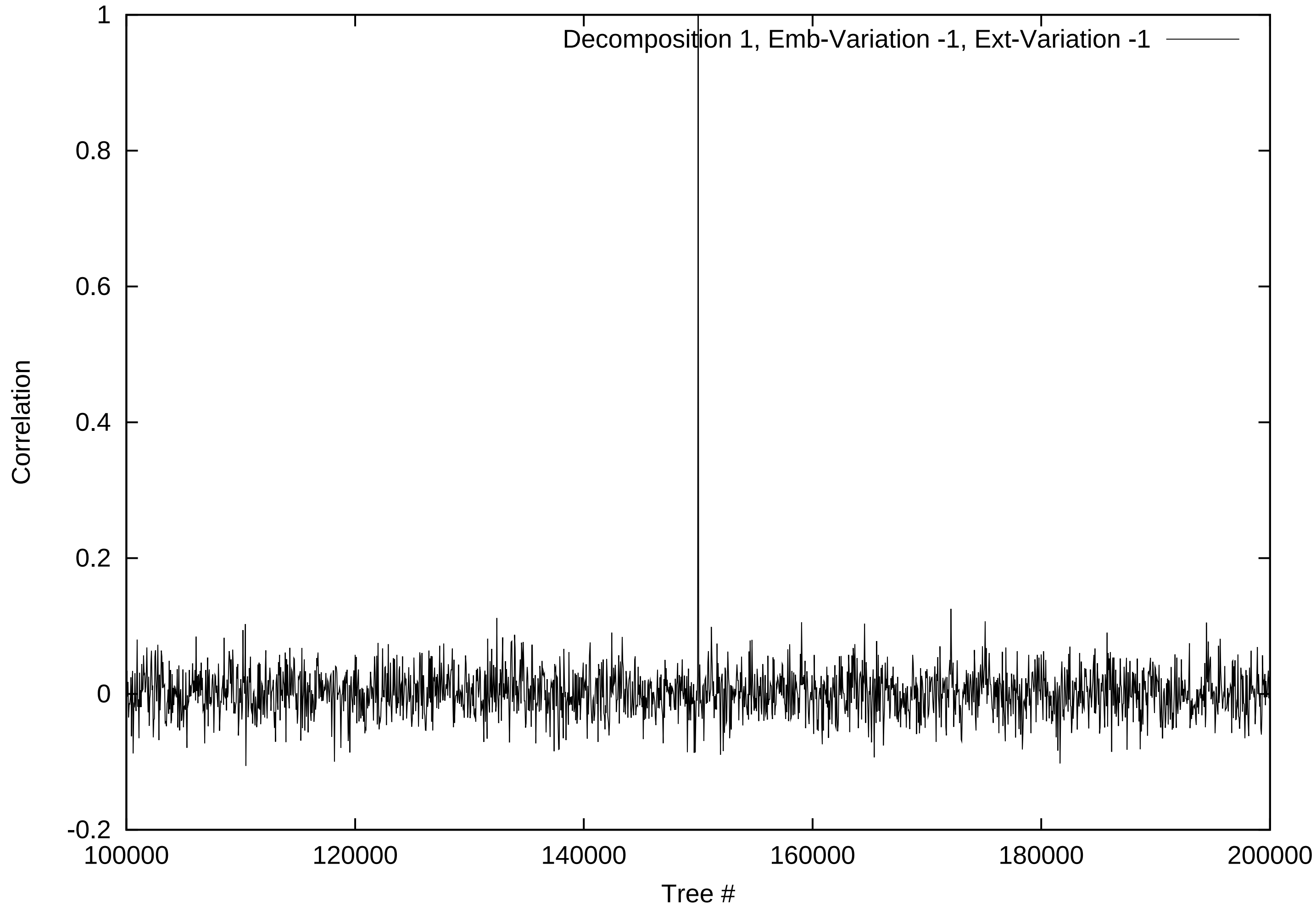
Security Assessment

- Embed watermark into Lena with 40dB PSNR and tree number 150.000
- Extract with numbers 100.000 to 200.000 with step size 50
  $\rightarrow$ 2001 measurements
- Use decompositions 1 and 2, with 4 and 7 levels
- Use watermark length 1000

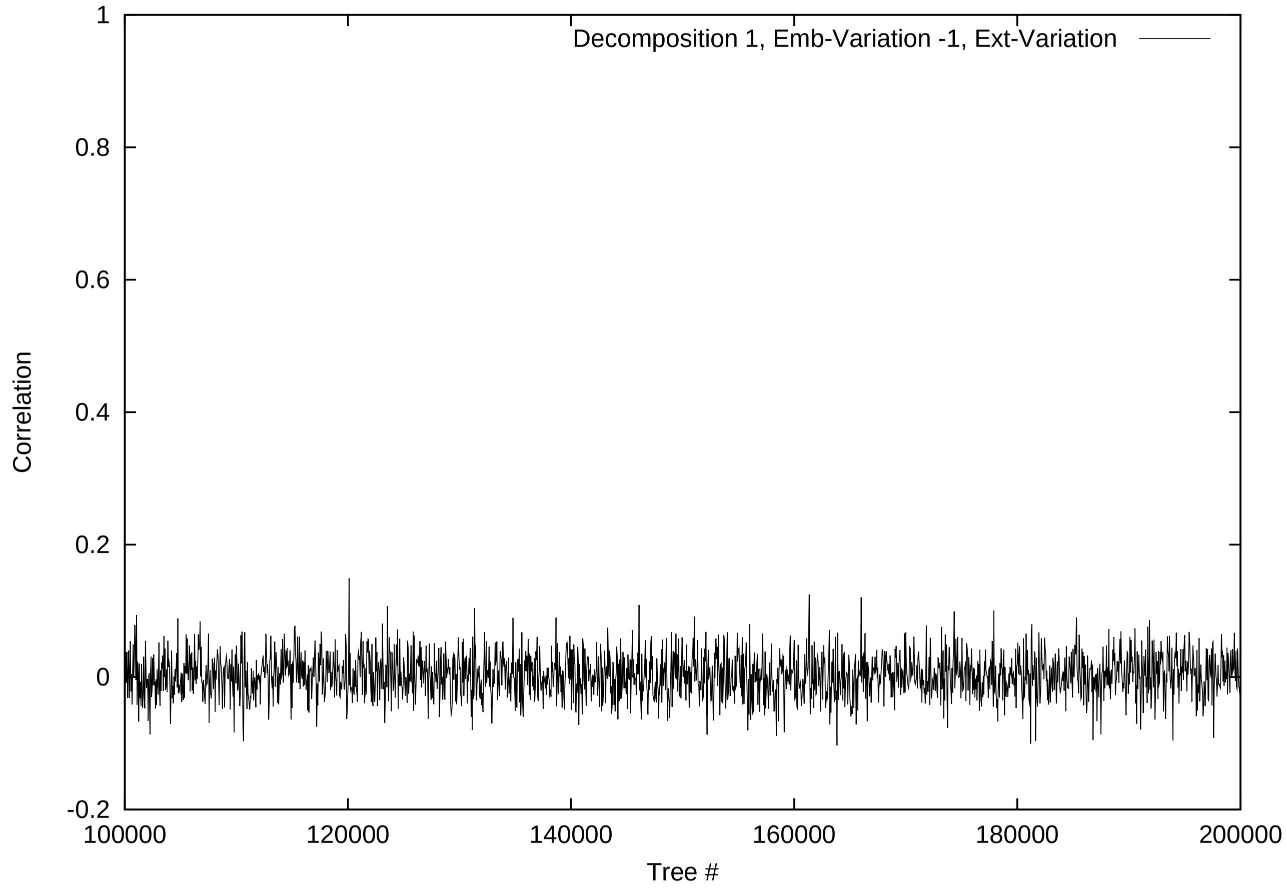
Decomposition 1, 7 Levels, WM Length 1000, No Variation



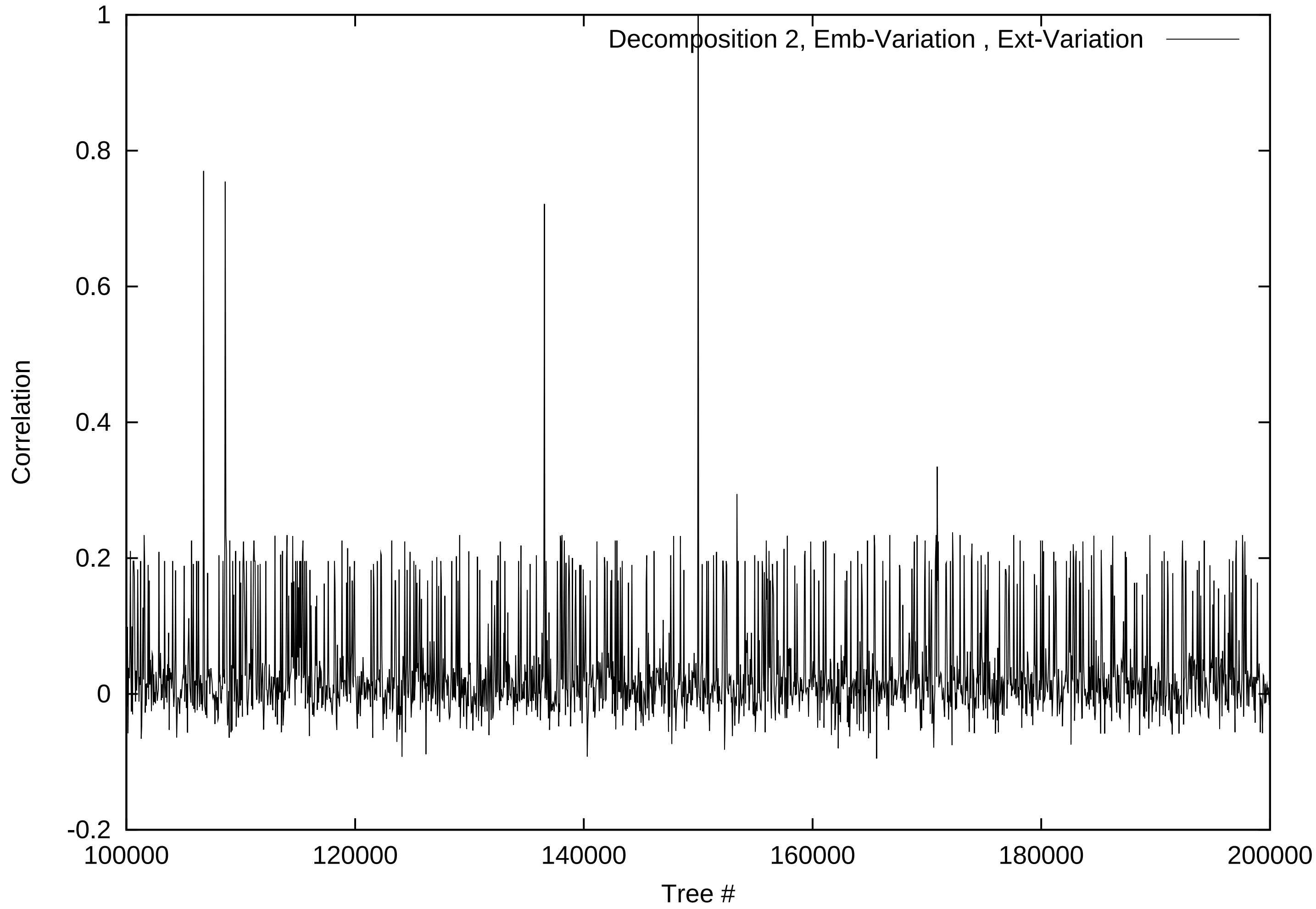
Decomposition 1, 7 Levels, WM Length 1000, Variation 1



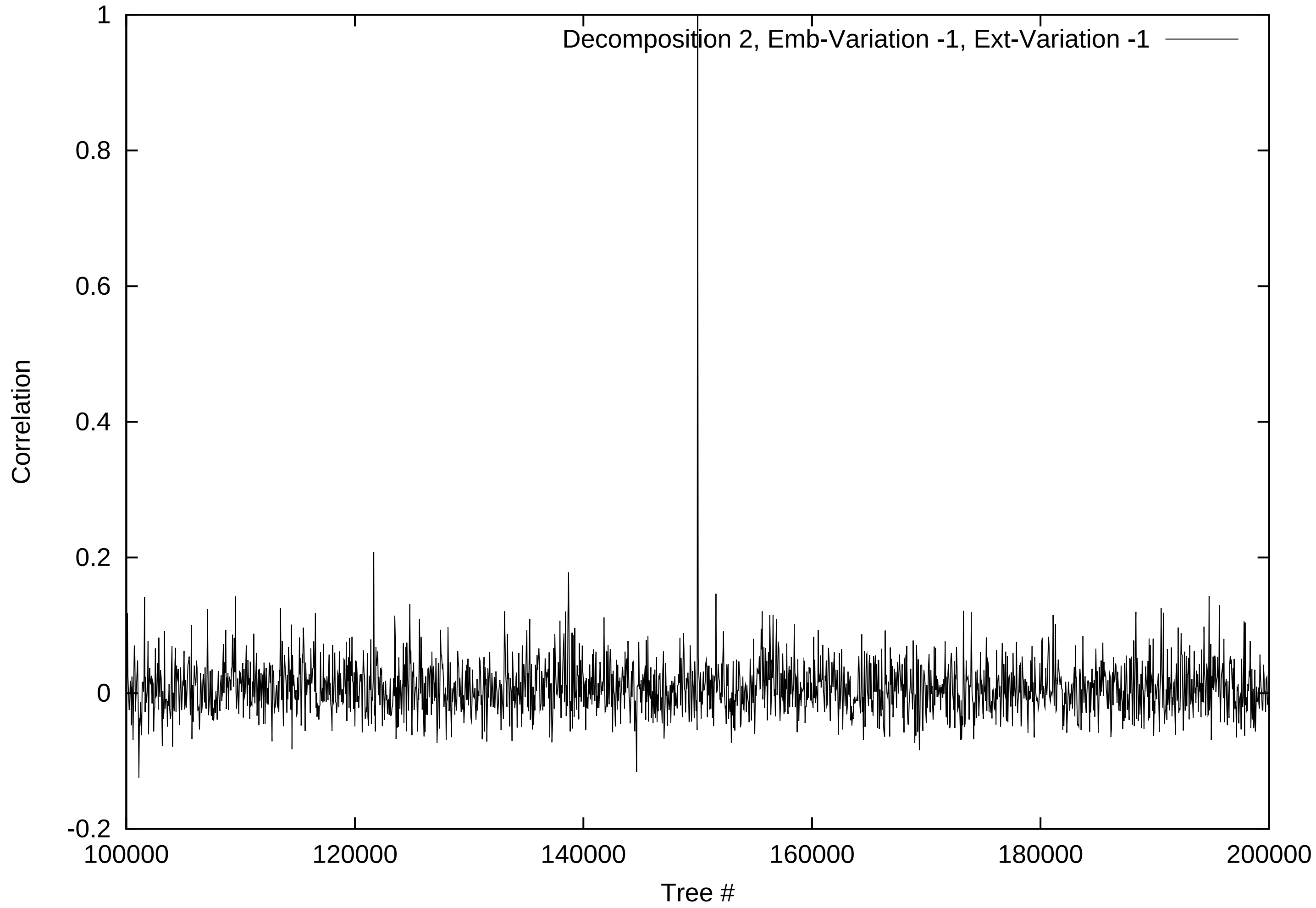
Decomposition 1, 7 Levels, WM Length 1000 Embedding Variation 1, No Extraction Variation



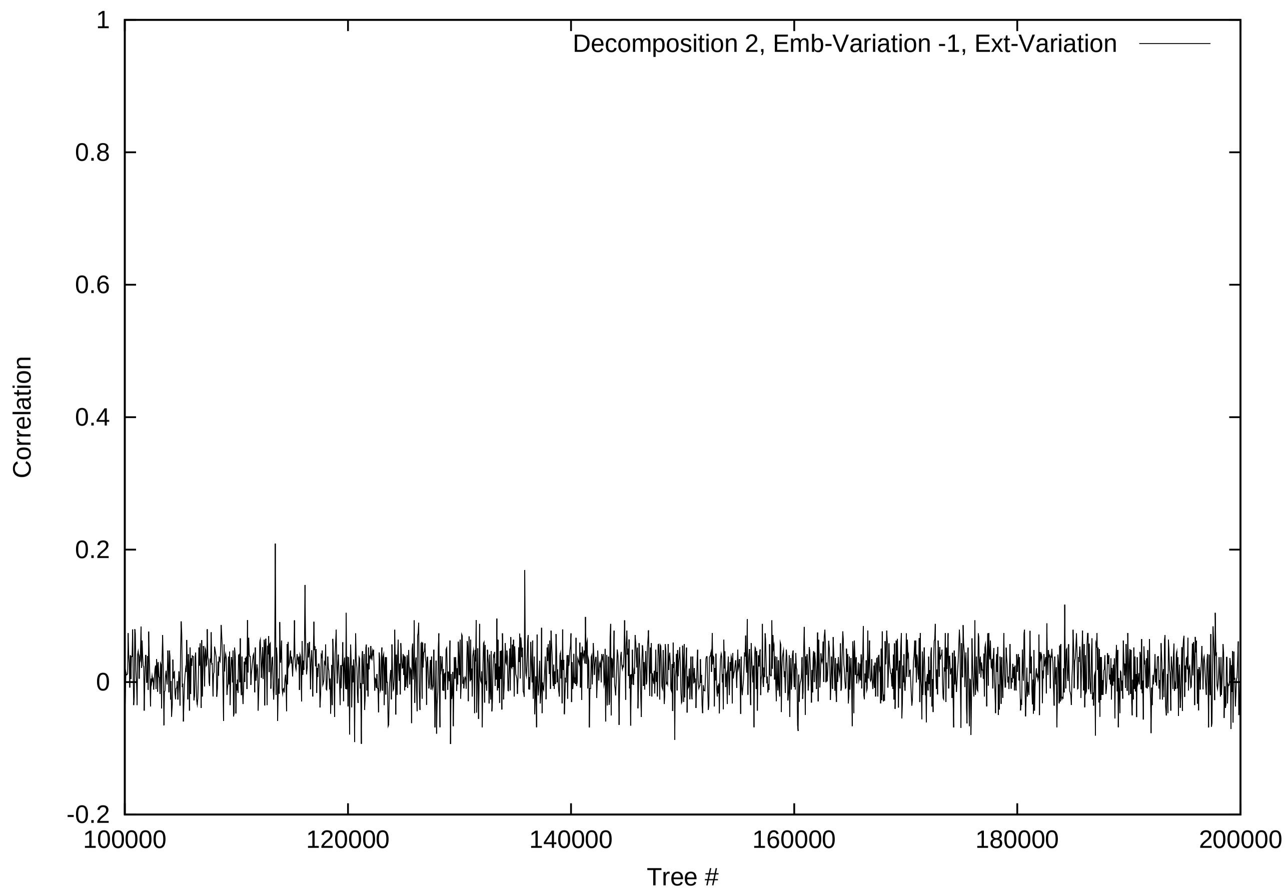
Decomposition 2, 7 Levels, WM Length 1000, No Variation



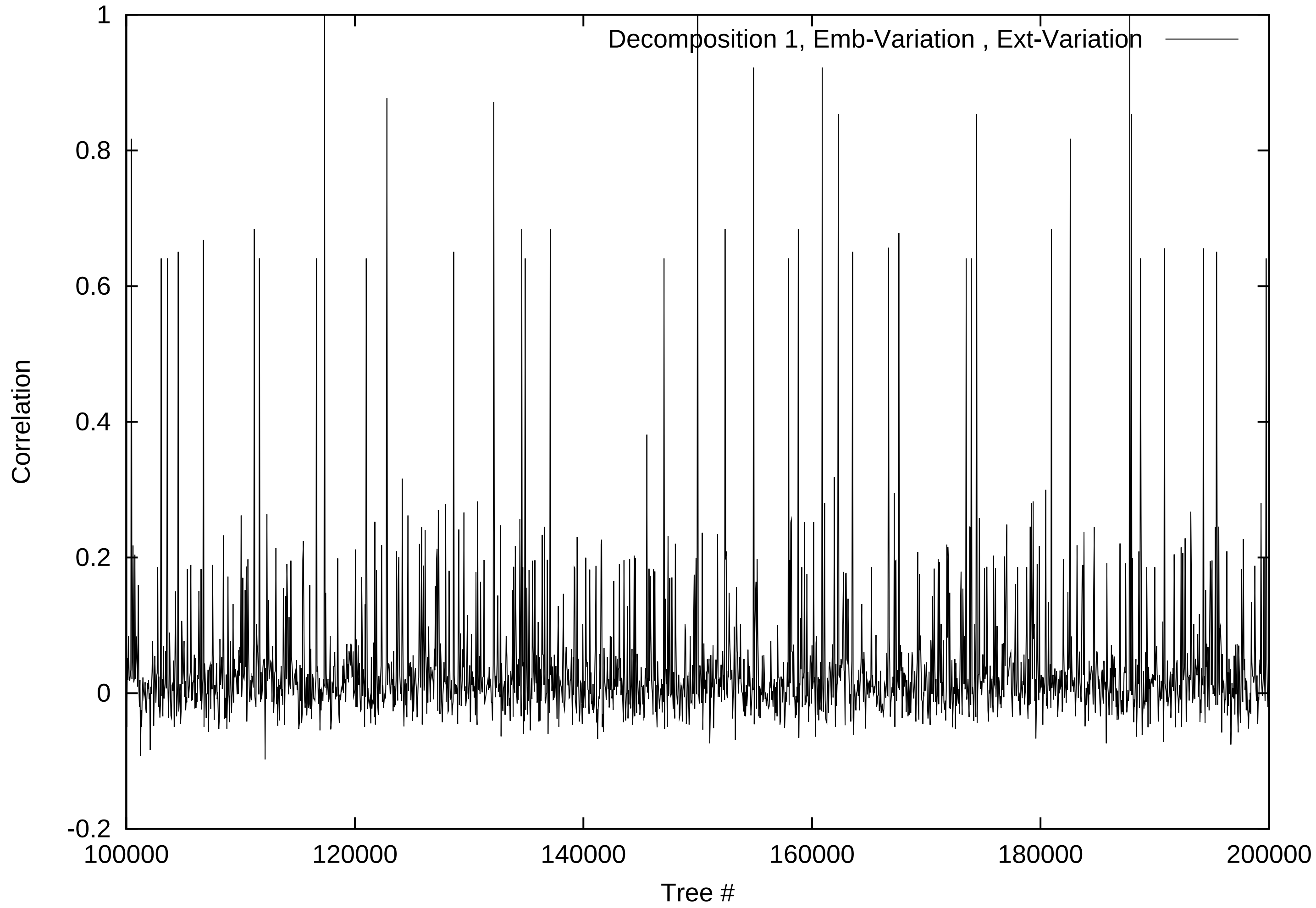
Decomposition 2, 7 Levels, WM Length 1000, Variation 1



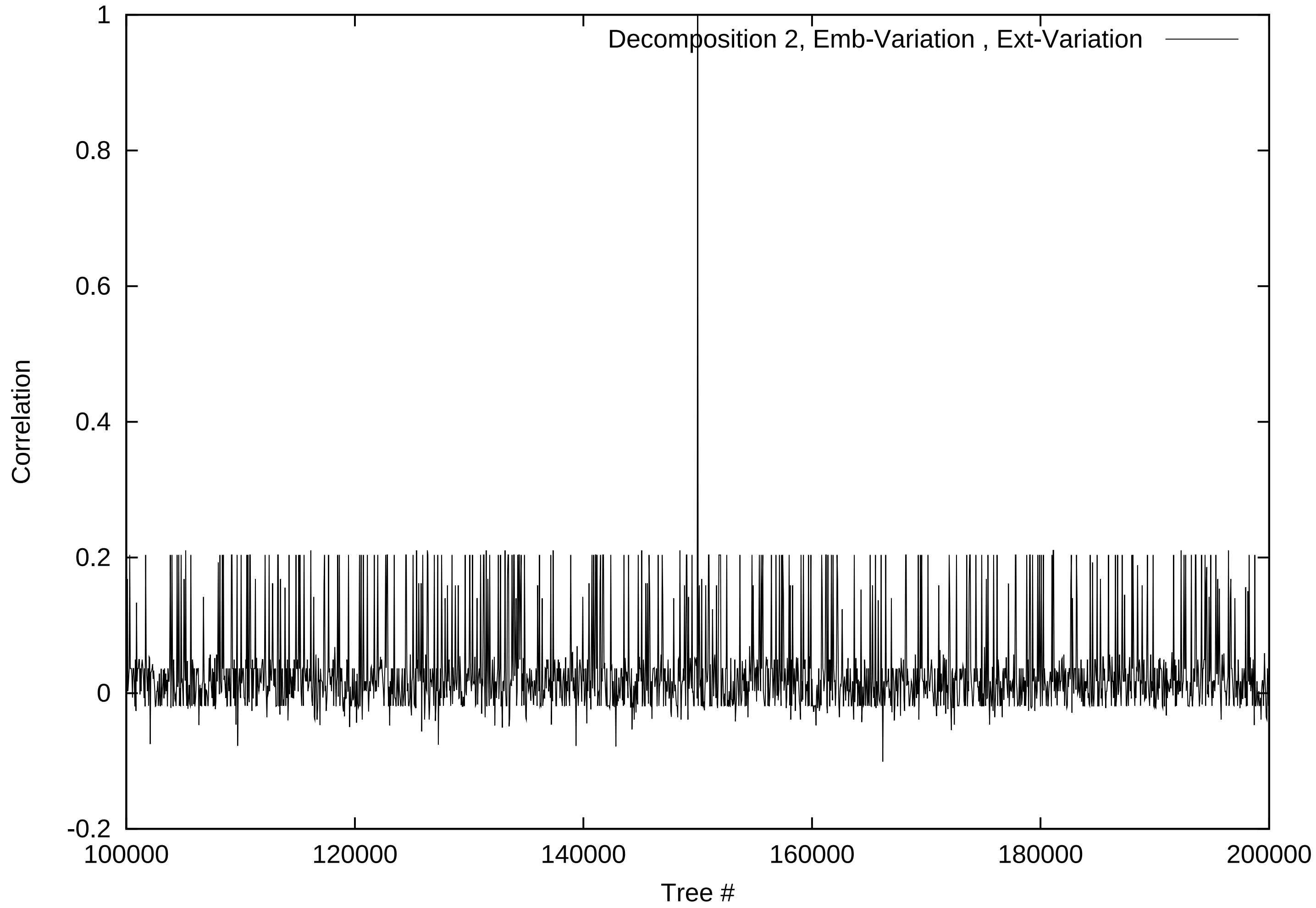
Decomposition 2, 7 Levels, WM Length 1000 Embedding Variation 1, No Extraction Variation



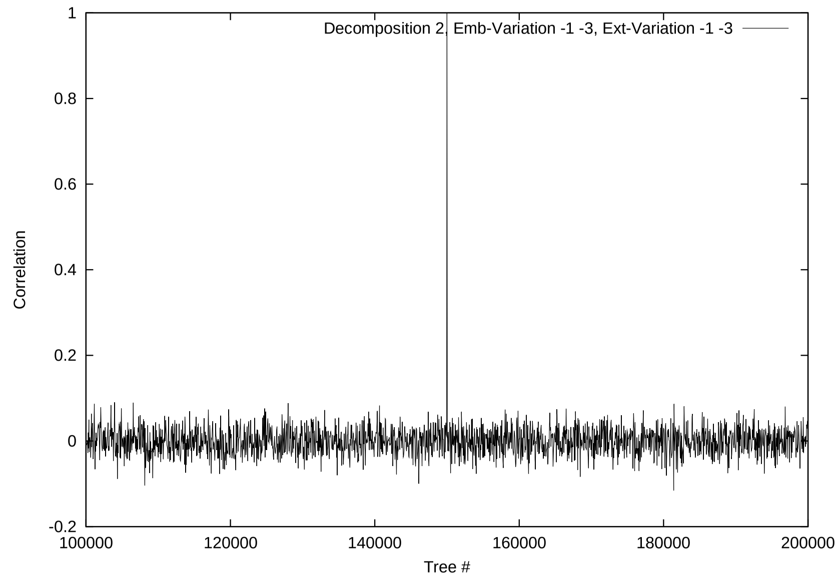
Decomposition 1, 4 Levels, WM Length 1000, No Variation



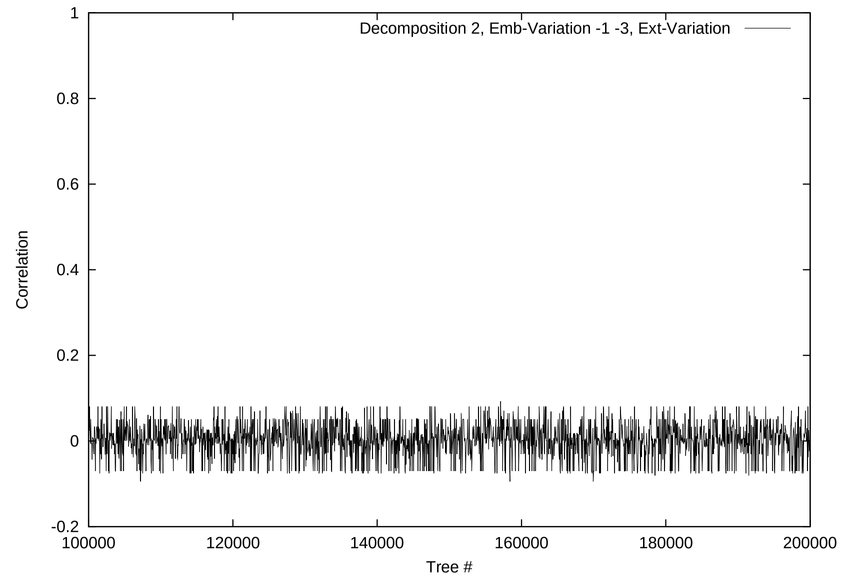
Decomposition 2, 4 Levels, WM Length 1000, No Variation



Decomposition 2, 4 Levels, WM Length 1000, Variation 1 & 2



Correct Extraction



Incorrect Extraction

Conclusions from the Security Assessment

- Different tree numbers can have common sub-trees
- Common sub-trees can result in high correlation
- Additional measures need to be taken to make embedding secure
- Skipping coefficients and shuffling the watermark both increase the security
- Unwanted correlation for wrong tree numbers removed
- No correlation when detecting without a variation

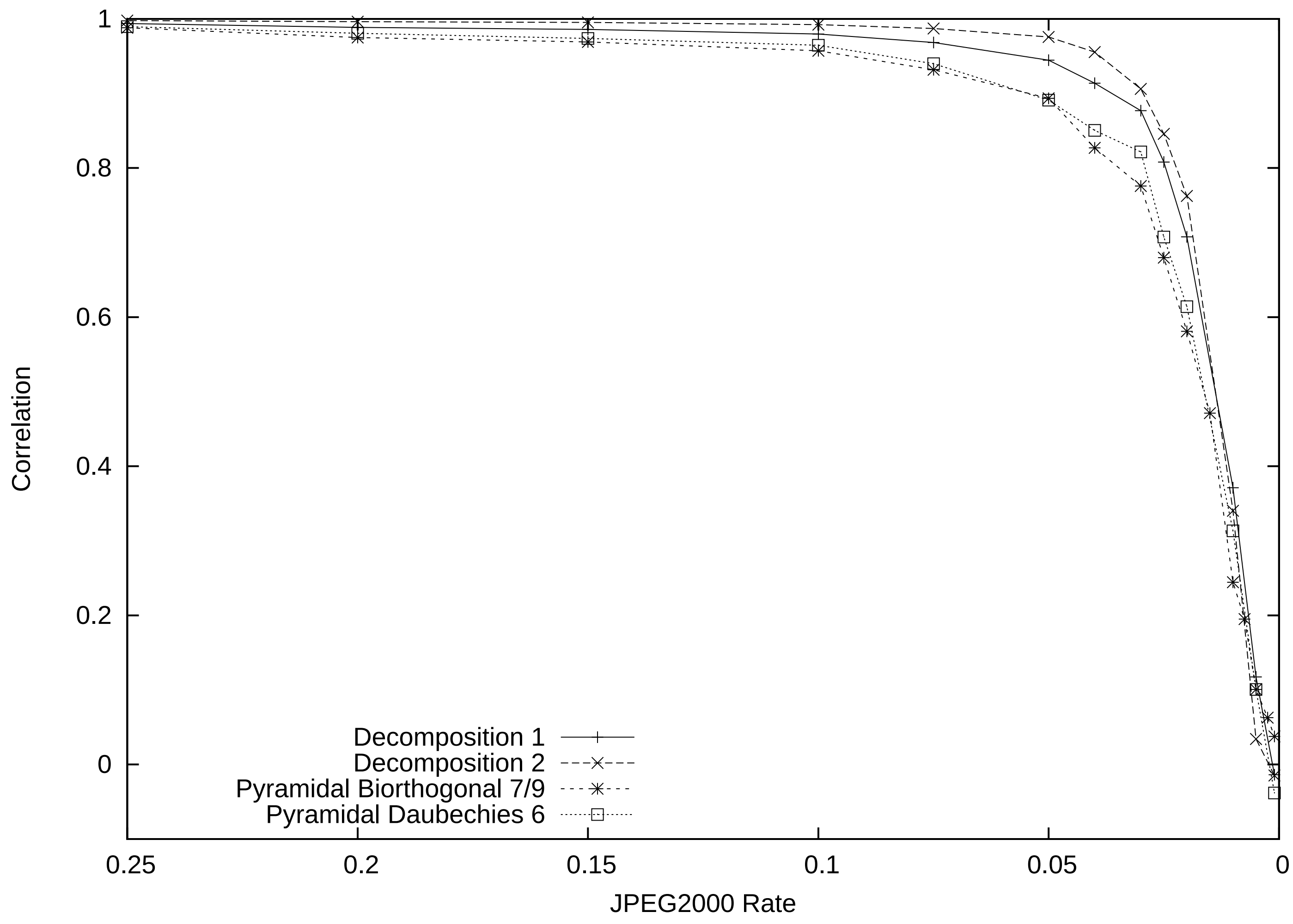
Quality Assessment

- Embed a watermark with 40dB PSNR
- Compress the watermarked image with JPEG and JPEG2000 at different rates
- Extract the watermark from the compressed image and measure the correlation
- WM lengths 1000, 5000 and 20000; 4 or 7 decomposition levels
- Decomposition method 1 or 2 and image Lena

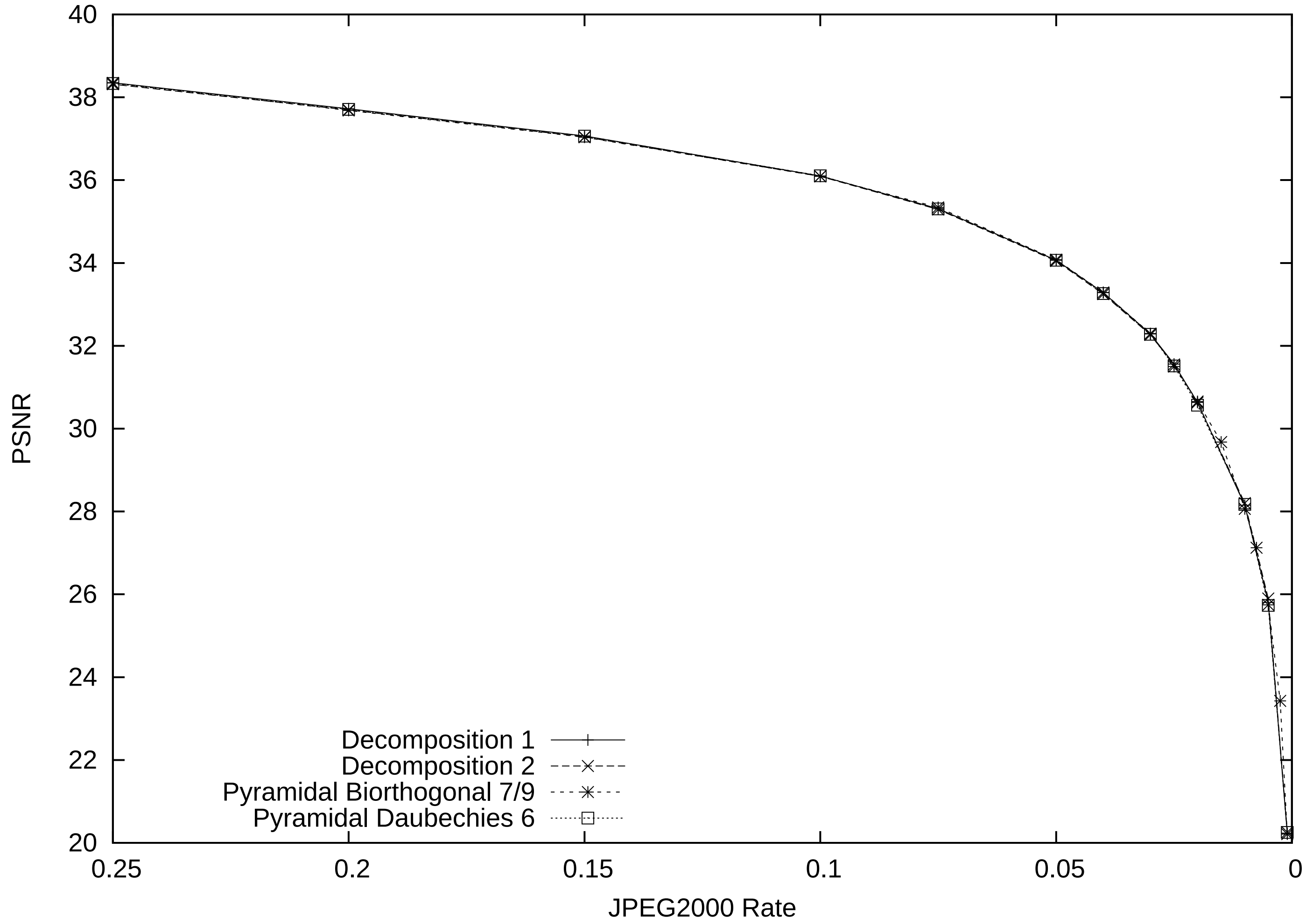
Quality Assessment II

- Tree numbers 100.000 to 200.000 with step size 400
  $\rightarrow$ 251 measurements
- Calculate minimum, maximum and average
- Compare with Daubechies 6 and Biorthogonal 7/9 pyramidal systems

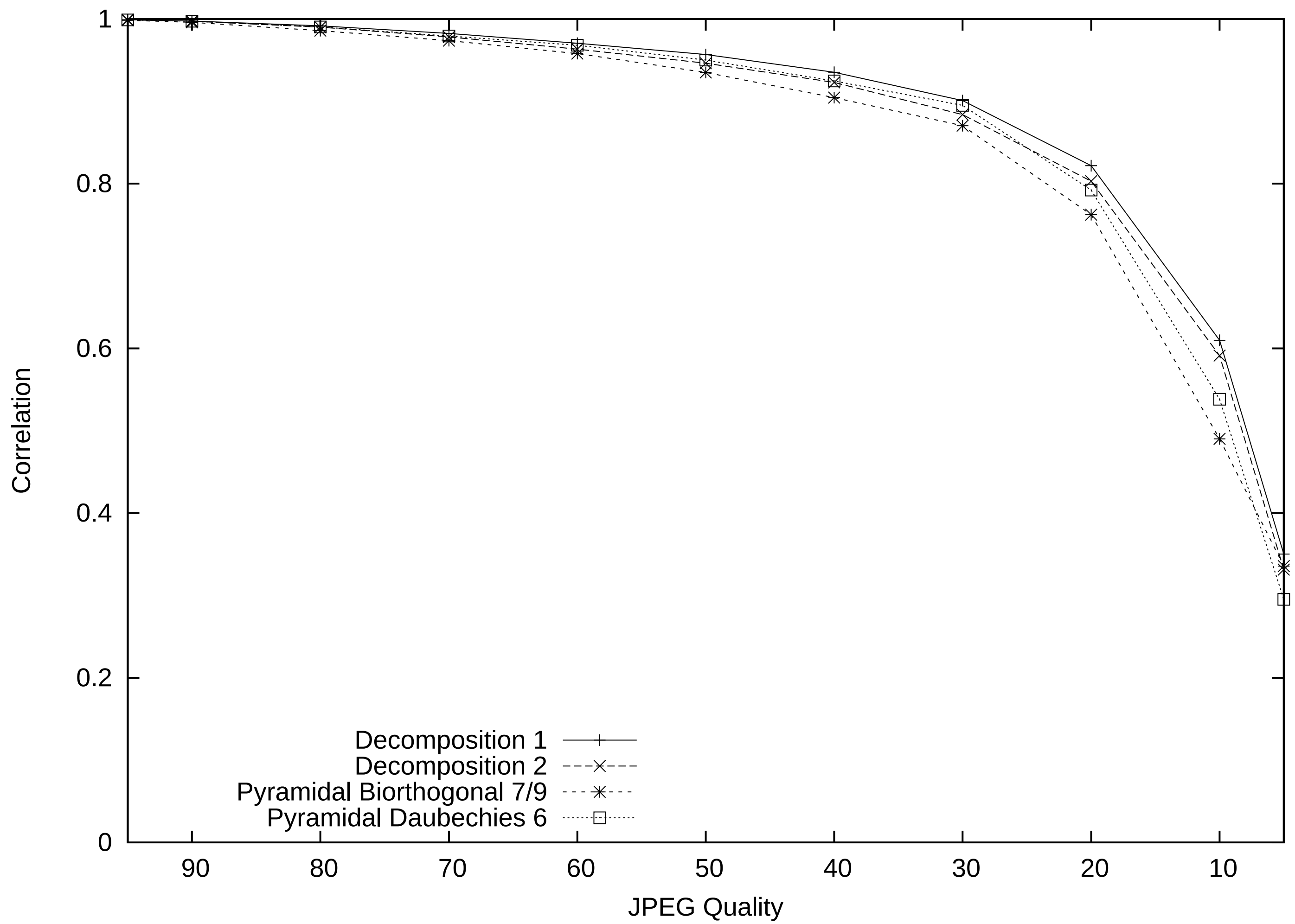
Lena, 7 Levels, WM Length 1000, JPEG2000 Correlation



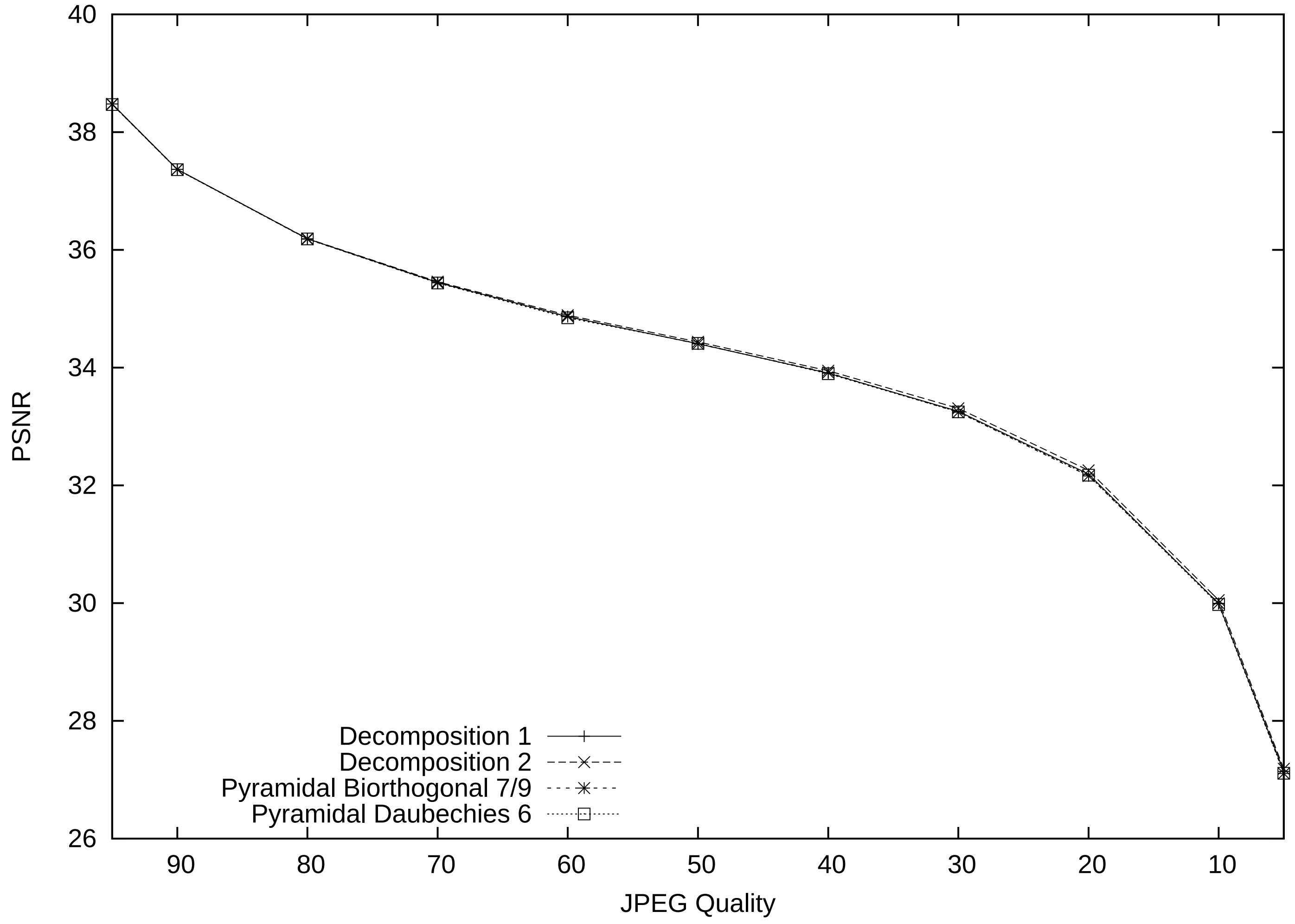
Lena, 7 Levels, WM Length 1000, JPEG2000 PSNR



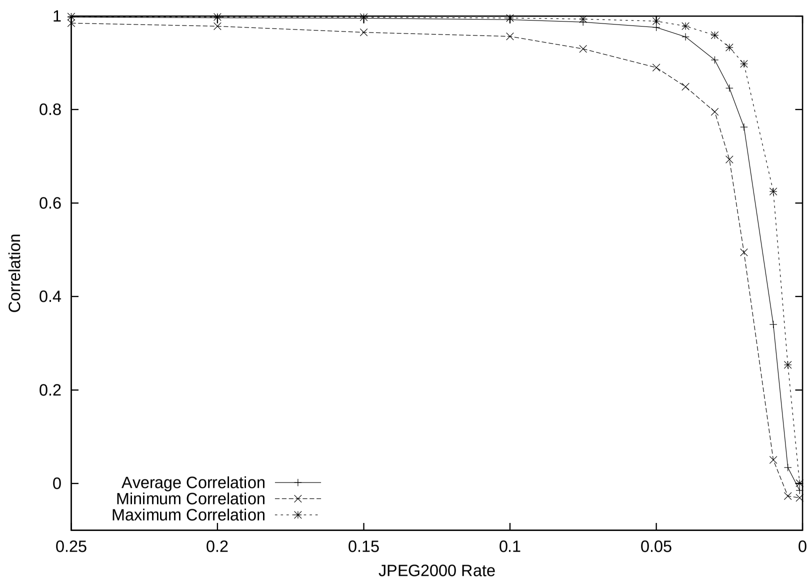
Lena, 7 Levels, WM Length 1000, JPEG Correlation



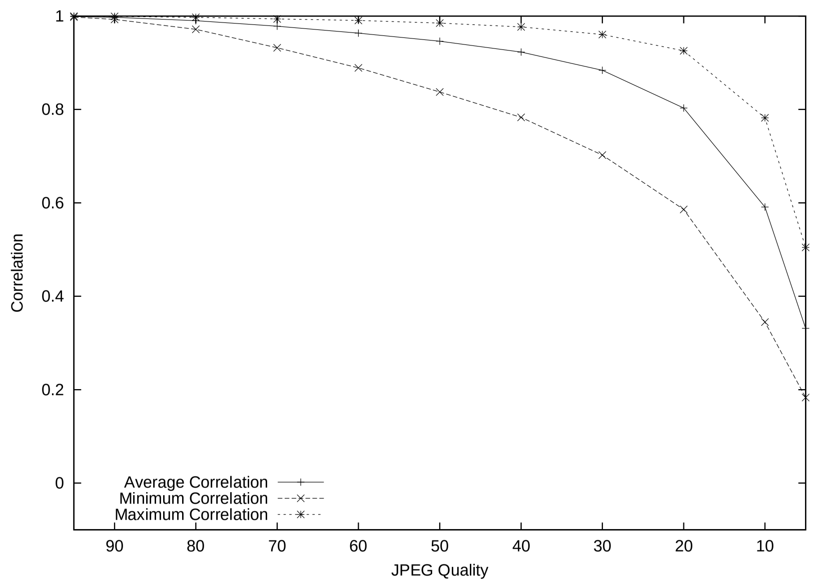
Lena, 7 Levels, WM Length 1000, JPEG PSNR



Lena, Decomposition 2, 7 Levels, WM Length 1000, Details

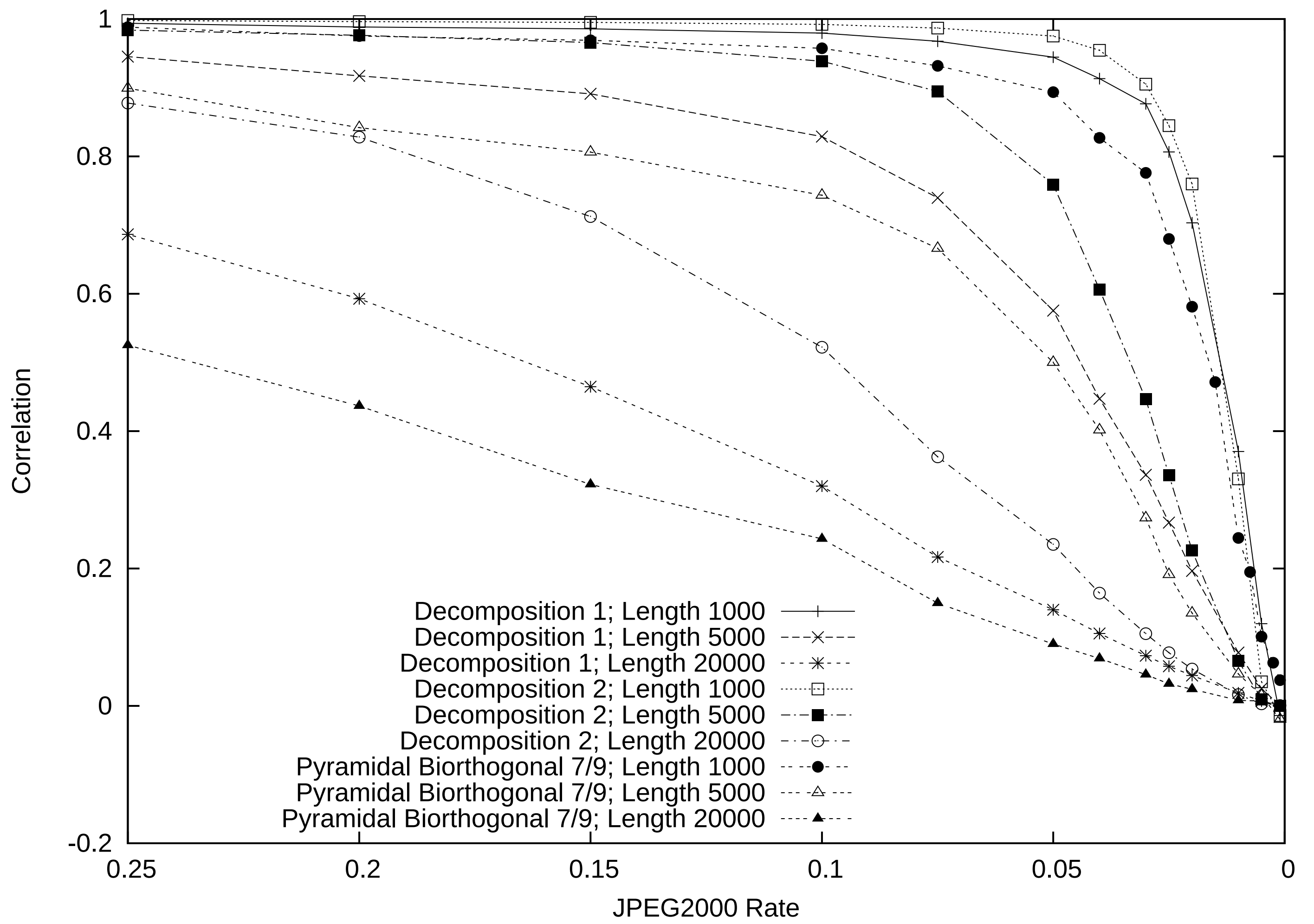


JPEG2000 Correlation

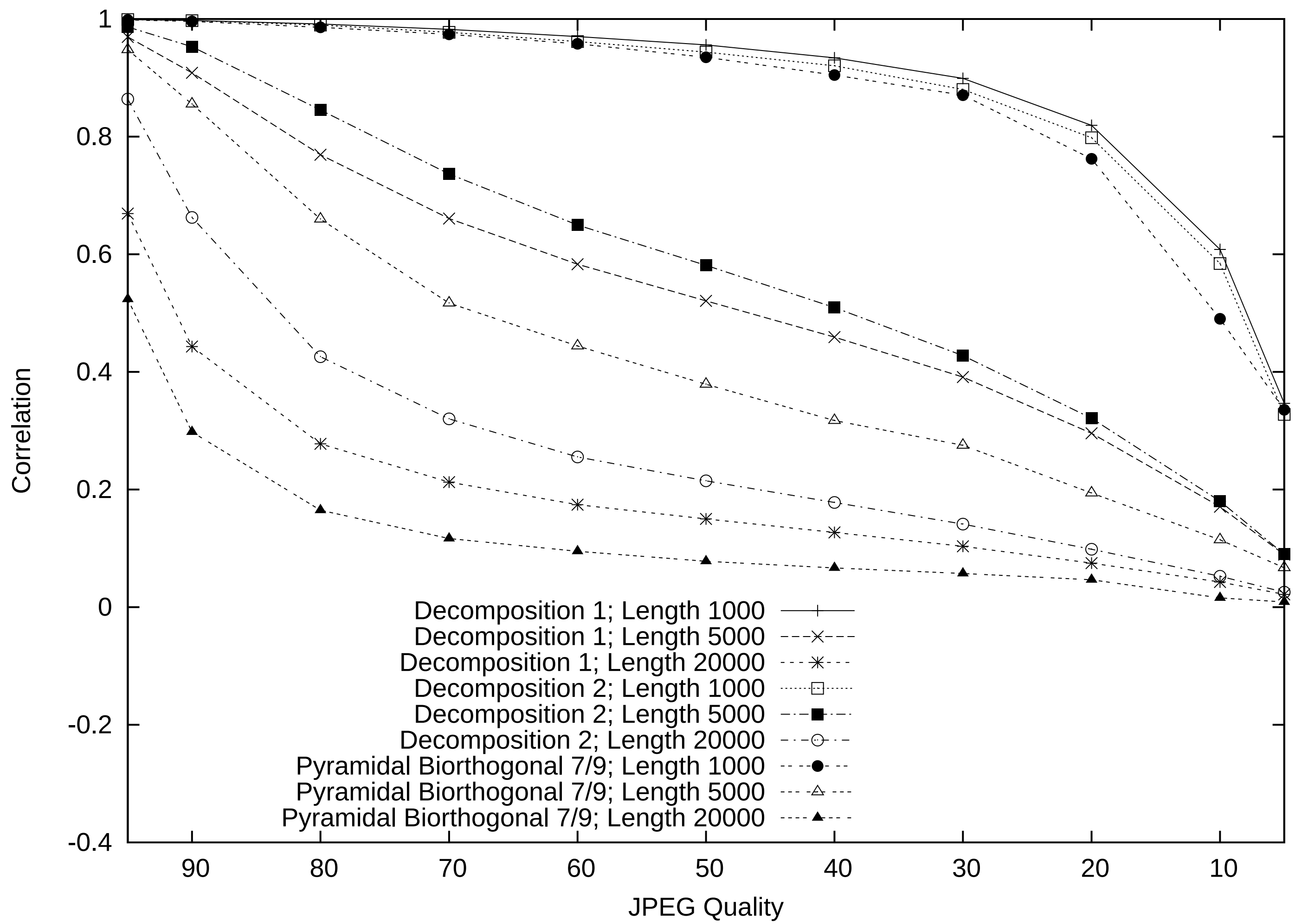


JPEG Correlation

Lena, 7 Levels, Length Comparison, JPEG2000 Correlation



Lena, 7 Levels, Length Comparison, JPEG Correlation



Conclusions from the Quality Assessment

- As expected decomposition 2 shows better compression behavior for longer watermarks
- Both wavelet packet decompositions are better than the standard filters with pyramidal decomposition

Overall Conclusions

- Wavelet packet decomposition can be used to hide the watermark embedding domain
- Coefficient skipping or watermark shuffling must be used to protect against common subtrees
- Decomposition 2 with 7 levels has 2^{1046} possible trees
- Decomposition 2 has superior properties for longer watermarks