



Watermarking During DWT

Ping Hu

University of Central Arkansas



Overview

- Watermarking and JPEG2000 Standard
- Conventional DWT based watermarking methods
- A Secure Watermarking For JPEG2000
- Improvement



What is watermarking?

- Began with Tirkel's paper "A digital watermark" in 1994
- In general, digital watermarking works by embedding information into images, audios and videos.
- Keep the distribution of digital multimedia work both profitable for the document owners and reliable for the customers



Properties:

- Invisibility: the watermark should keep imperceptible to avoid being overwritten.
- Robustness: the watermark must be difficult to be removed by adding noises.



Challenges

- **Common signal processing:** e.g. color alterations for pictures; analog to digital and digital to analog conversions; resampling; requantization; lossy compression; . . .
- **Geometric transforms:** e.g. rotation; scaling; translation; cropping
- **Tamper resistance:** the watermark should be against collusion attacks, which mainly focus on combining copies of the same dataset to remove the mark, or to multiply watermarking.



Watermarking algorithms classification

- **Based on spatial domain:**

 - old algorithm such as LSB

- **Discrete cosine transform:**

 - Besides application in the early image and video coding standards such as JPEG

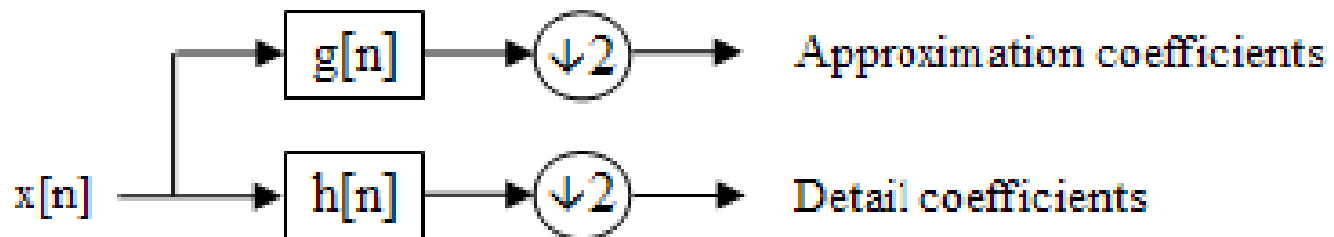
- **Wavelet transform domain:**

 - new standard of image compression such as JPEG2000

- **Other transforms:**

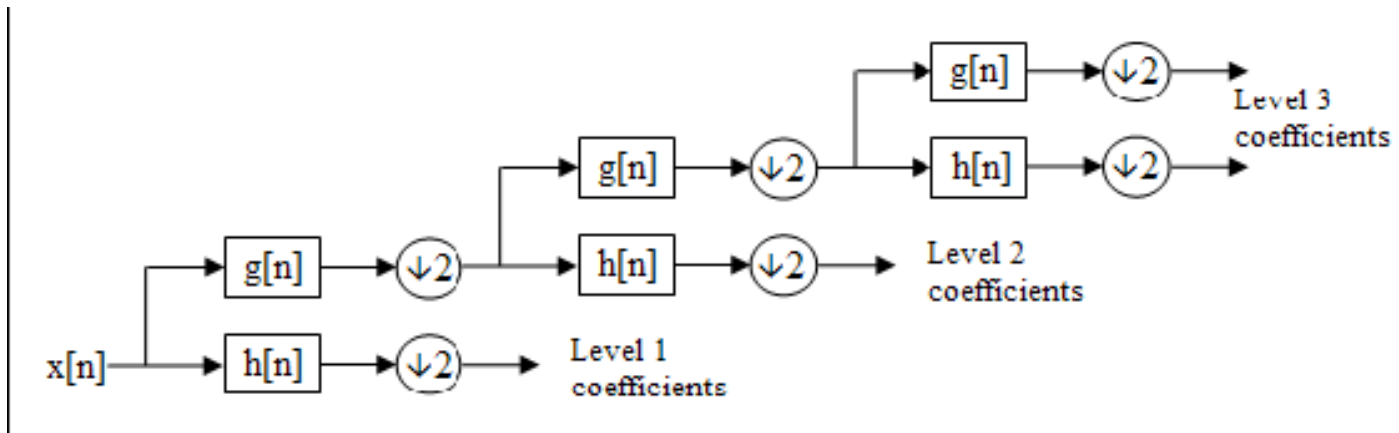
DWT standard

- Formulation based upon the use of recurrence relations to generate progressively finer discrete samplings of an implicit mother wavelet function.



Block diagram of filter analysis

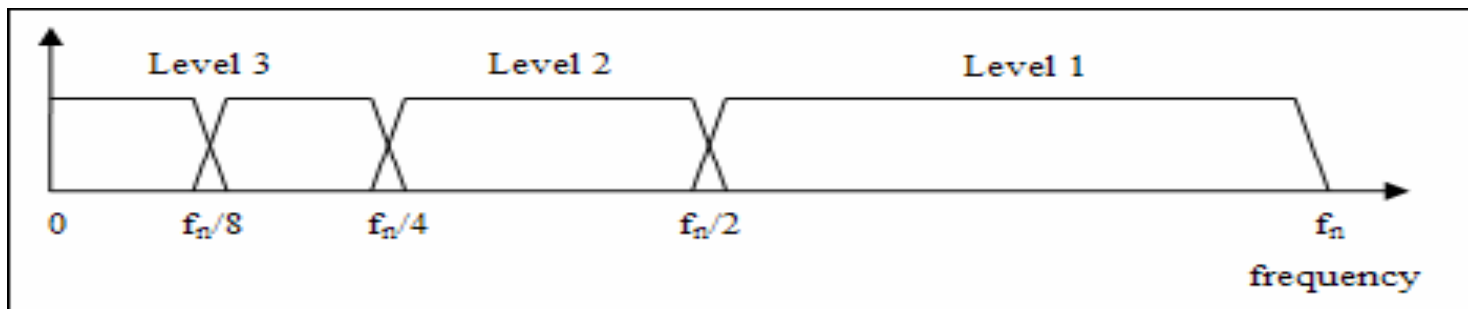
DWT standard (cont'd)



A 3 level filter bank

DWT standard (cont'd)

Level	Frequencies	Samples
3	0 to $f_n/8$	4
	$f_n/8$ to $f_n/4$	4
2	$f_n/4$ to $f_n/2$	4
1	$f_n/2$ to f_n	4



JPEG2000 Standard

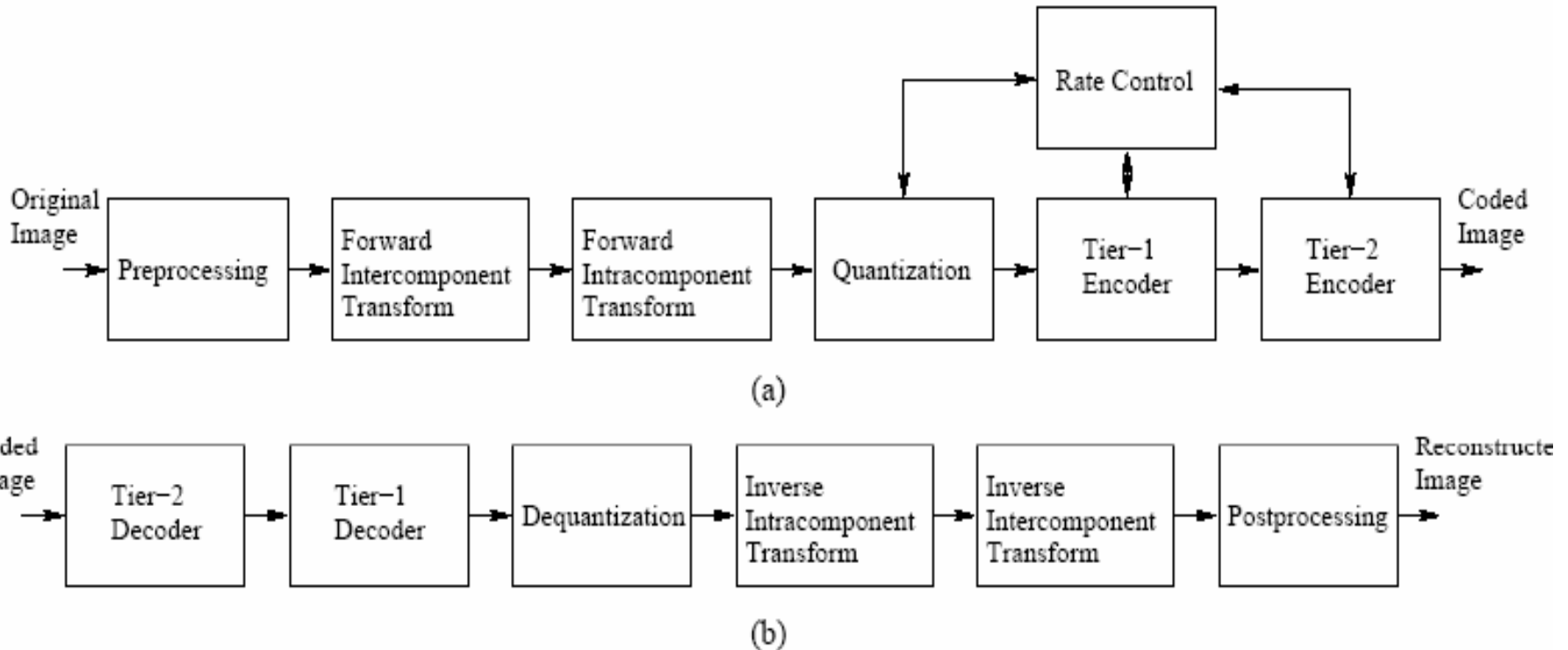
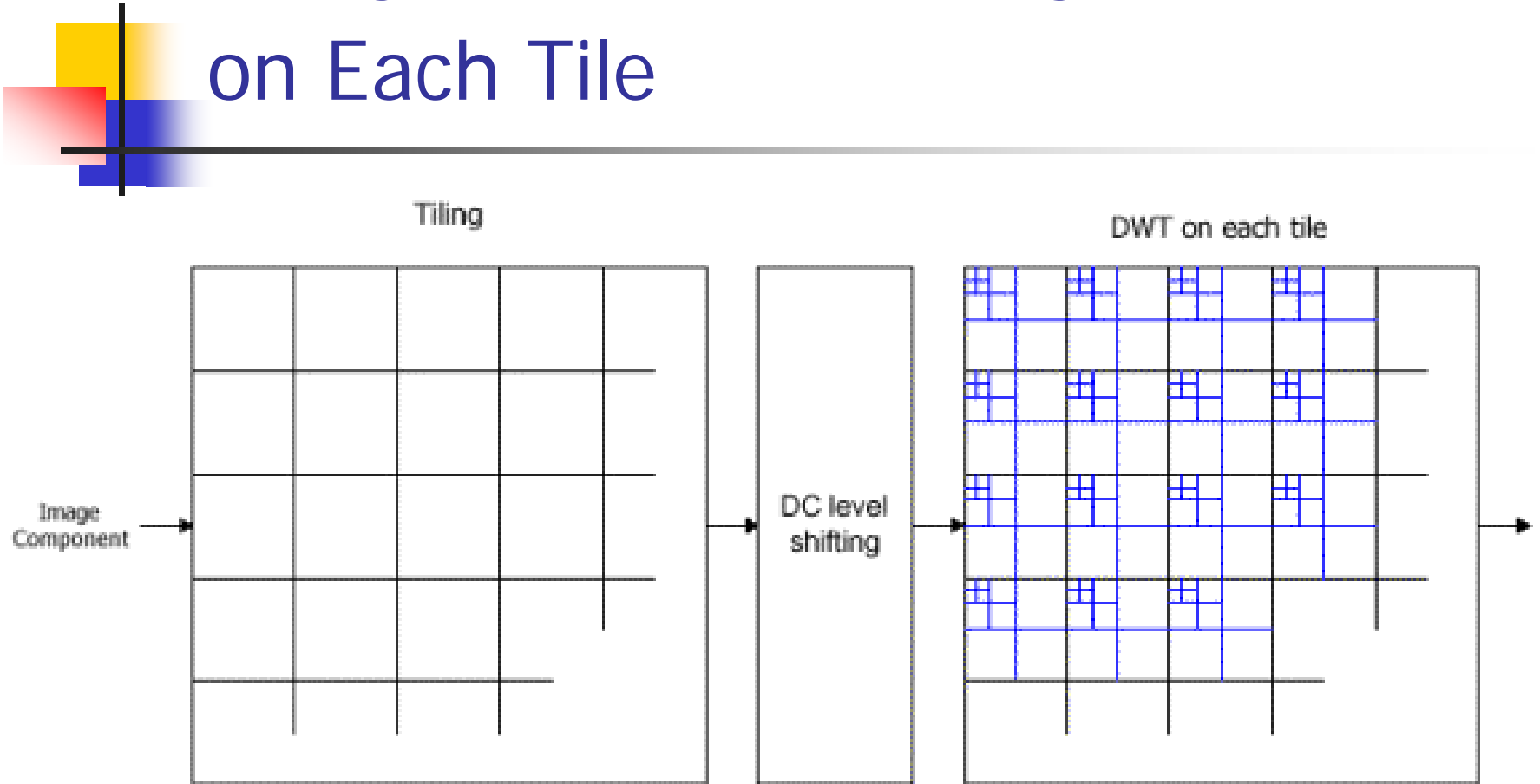


Fig. 5. Codec structure. The structure of the (a) encoder and (b) decoder.

Figure 1: The encoding and decoding pipeline of JPEG2000

Tiling, DC Level Shifting, and DWT on Each Tile





Forward Intracomponent Transform

- For each resolution level of wavelet transform, a component is divided into four frequency bands:
 - 1) horizontally and vertically low-pass (LL)
 - 2) horizontally lowpass and vertically high-pass (LH)
 - 3) horizontally high-pass and vertically low-pass (HL)
 - 4) horizontally and vertically high-pass (HH).
- The input tile-component signal is considered as $LLR-1$. At each resolution level, the LL band is used for further decomposition, until $LL0$ is obtained.

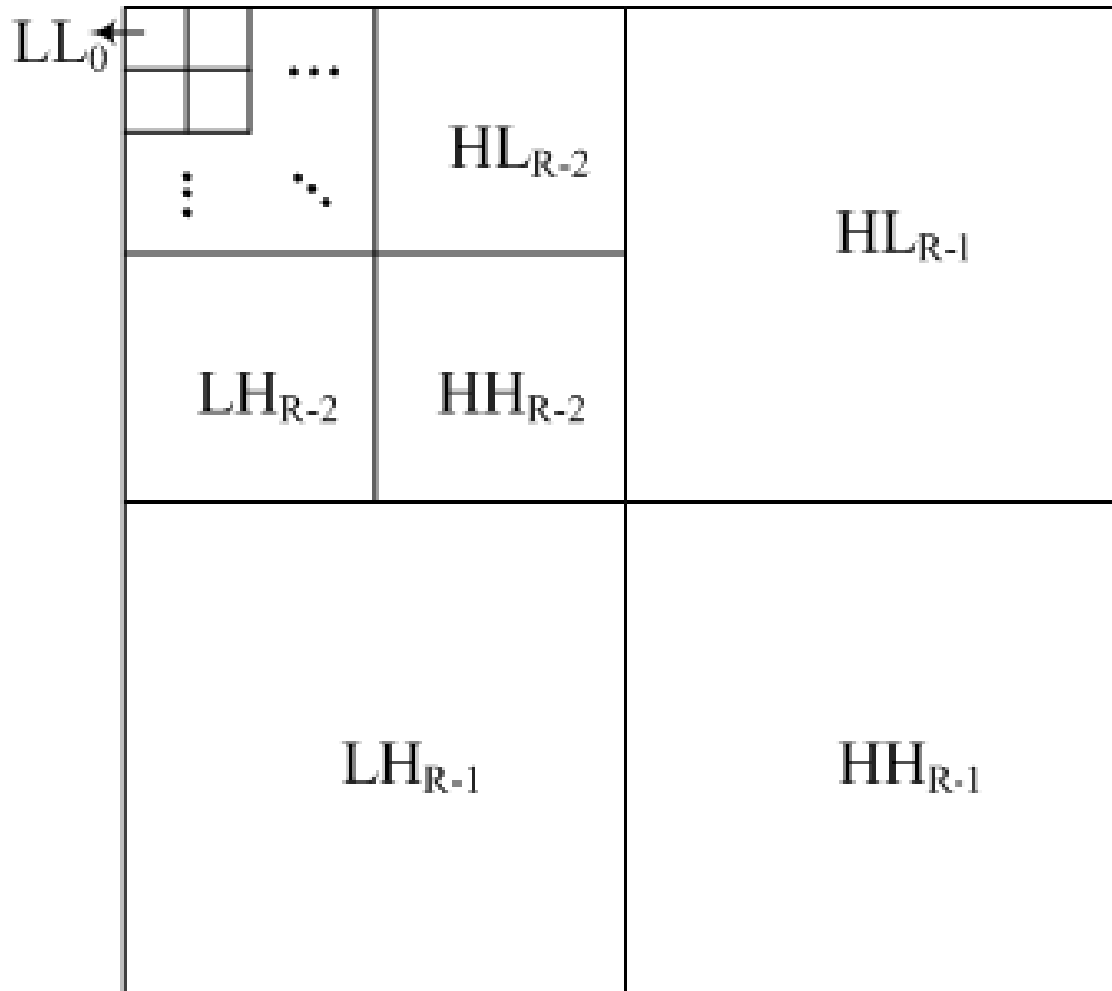
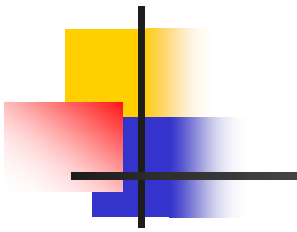


Figure 2: Structure of sub-band Tree

Example of Forward Intracomponent Transform





Watermarking During DWT

- Discrete Wavelet Transform (DWT) is the key stage of the JPEG2000 compression.
- By embedding a watermark in the same domain as the compression scheme used to process the image, we can handle lossy compression because we are able to anticipate which the transformed coefficients will be discarded by the compression scheme



Conventional DWT based watermarking

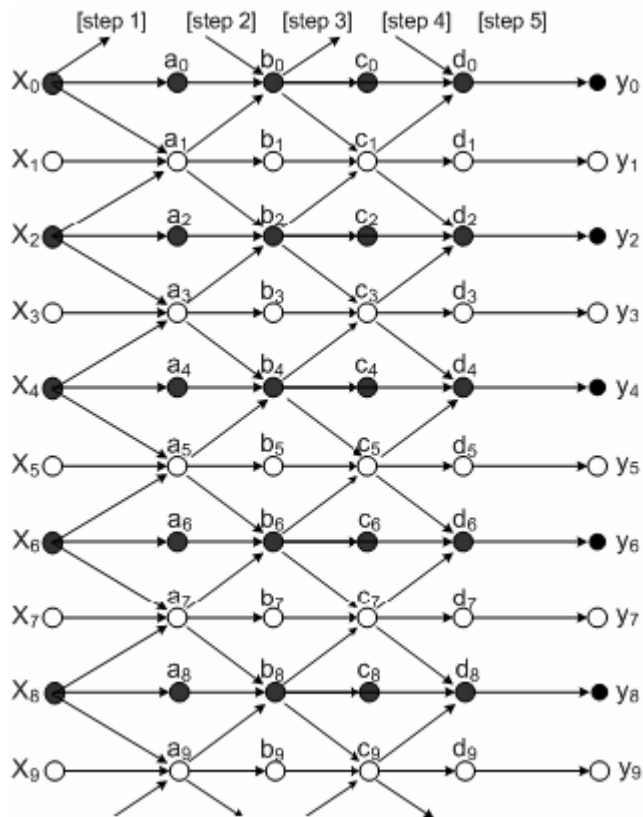
- These techniques insert watermark into transformed coefficients after the transform is completed.
- Advantage: convenient to implement
- Disadvantage: the filter-banks for watermarking is the same as the filter-banks for the compression, it is easy to remove or modify



A Secure Watermarking For JPEG2000

- Proposed by Seo et al. In 2001
- In order to make the filter-banks for watermarking is different from the filter-banks for compression, the watermark is inserted into the coefficients obtained from the on-going process of lifting for DWT.

A Secure Watermarking For JPEG2000(cont'd)



$$a_i = \begin{cases} x_i + \alpha(x_{i-1} + x_{i+1}) & \text{for } i = 2n + 1 \\ x_i & \text{otherwise} \end{cases} \quad (1)$$

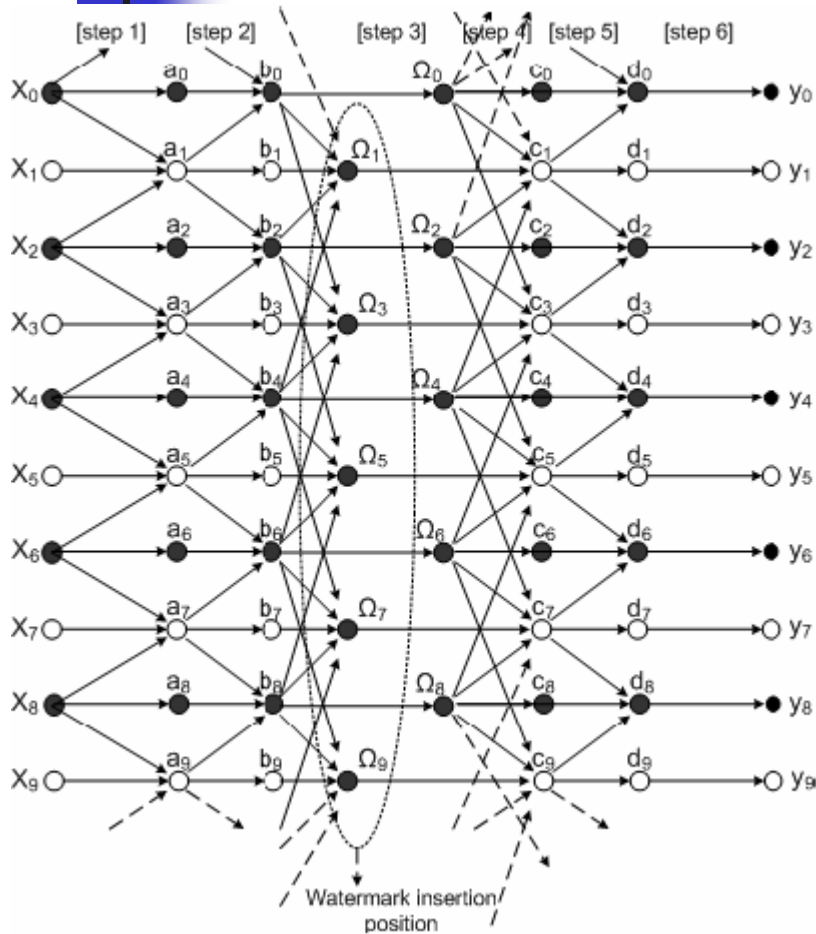
$$b_i = \begin{cases} a_i + \beta(a_{i-1} + a_{i+1}) & \text{for } i = 2n \\ a_i & \text{otherwise} \end{cases} \quad (2)$$

$$c_i = \begin{cases} b_i + \gamma(b_{i-1} + b_{i+1}) & \text{for } i = 2n + 1 \\ b_i & \text{otherwise} \end{cases} \quad (3)$$

$$d_i = \begin{cases} c_i + \delta(c_{i-1} + c_{i+1}) & \text{for } i = 2n \\ c_i & \text{otherwise} \end{cases} \quad (4)$$

$$y_i = \begin{cases} d_i + \delta(d_{i-1} + d_{i+1}) & \text{for } i = 2n + 1 \\ d_i & \text{otherwise} \end{cases} \quad (5)$$

A Secure Watermarking For JPEG2000(cont'd)



$$\Omega_i = \begin{cases} b_i + (\gamma - \omega)(b_{i-1} + b_{i+1}) \\ \quad + \omega(b_{i-3} + b_{i+3}) \\ b_i \end{cases} \quad \begin{array}{l} \text{for } i = 2n + 1 \\ \text{otherwise} \end{array} \quad (6)$$

$$c_i = \begin{cases} \Omega_i + \omega(\Omega_{i-1} + \Omega_{i+1}) \\ \quad - \omega(\Omega_{i-3} + \Omega_{i+3}) \\ \Omega_i \end{cases} \quad \begin{array}{l} \text{for } i = 2n + 1 \\ \text{otherwise} \end{array} \quad (7)$$



Advantage and Disadvantage

- The advantage of this method is, it keep the filter banks used for watermark insertion as a secret, so that the filter banks will not be revealed as a tool to remove or damage the watermark.
- Because the watermark is inserted into high frequency components of the on-going process of lifting for DWT, it is can resist sharpen attack well. However, when facing to blurring attacks, the watermark will be easily removed since blurring is a low-frequency pass filter.



Further Work

- Therefore, I think that if we want the watermark to be robust enough, we can not only insert it into high frequency components only. We should consider some lower frequency components in condition of the invisibility property.
- Based on this foundation, we can extract low-frequency information from the ongoing process of DWT by adding one step between c_i and d_i . The original procedure $c_i \rightarrow d_i$ is changed to $c_i \rightarrow \tau_i \rightarrow d_i$, as shown in the equations below.



Further Work

- The challenge of this algorithm how to keep watermark to be invisible
- We must control the amount of changes of the coefficients caused by the watermark



Conclusion

- Watermarking is playing an important role in computer security, to detect the legitimate owner, to protect copyright, and so on.
- Conventional watermarking method on JPEG2000 images during DWT.
- A secure watermarking method
- Still can improve this algorithm



References

- [1] Tirkel A, Schyndel V. A digital watermark[A]. In: Proceeding ICIP[C], 1994(2): 86—89
- [2] Wolfgang R, Delp E. A watermarking technique for digital imagery: Further studies[A]. In: Proceedings of international conference on imaging science, system and technology[C]. Las Vegas, NV, 1997. 21—23
- [3] Cox I.J., Kilian J., Leighton F.T., Shamoon, T., Secure spread spectrum watermarking for multimedia, Image Processing, IEEE Transactions on Volume 6, Issue 12, Dec. 1997 Page(s):1673 – 1687
- [4] M. Ramkumar, A. N. Akansu, and A. A. Alatan, A robust data hiding scheme for images using DFT, Proceedings of the 6th IEEE International Conference on Image Processing ICIP '99, pp. 211 - 215, (Kobe, Japan), October 1999.
- [5] Yong-Seok Seo, Min-Su Kim, Ha-Joong Park, Ho-Youl Jung, Hyun-Yeol Chung, Young Hug, Jae-Duck Lee, *A Secure Watermarking For JPEG2000*, Image Processing, 2001. Proceedings. 2001 International Conference on Volume 2, 7-10 Oct. 2001 Page(s):530 - 533 vol.



Q&A

Thank you!!