Evaluation of Watermark Robustness to JPEG2000 Based Content Adaptation Attacks

Deepayan Bhowmik, Charith Abhayaratne

Department of Electronic and Electrical Engineering, University of Sheffield
Sheffield, S1 3JD, United Kingdom
{d.bhowmik, c.abhayaratne}@sheffield.ac.uk.

Keywords: Watermarking, content adaptation, JPEG2000.

Abstract

Bit streams of scalable coded media are adapted at various nodes in multimedia usage chains to cater the variations in network bandwidths, display device resolutions and resources and usage preferences. This is achieved by extracting the most relevant segments from the scalable coded bit stream corresponding to the quality-resolution requirements. Such adaptations can affect the watermarking information embedded in the content and can result in errors in extracting and authentication of such watermark data. A framework for evaluating watermarking robustness to JPEG2000 based content adaptation attacks is presented. The proposed framework represents commonly used wavelet based watermarking algorithms as a subset of a general watermarking framework and simulates the content adaptation modes based on JPEG2000 transcoding to provide a general framework for evaluating watermark robustness in such adaptations and the influence of different embedding modes.

1 Introduction

Recently scalable coding such as JPEG2000 and the emerging H.264 scalable video coding (SVC) extension, has received a considerable attention for universal multimedia access (UMA) applications for seamless multimedia delivery from production to end user. UMA facilitates various users to consume multimedia which is independent of application device, network media, network speed, resource limitation and user preferences. The input media is coded in such a way that the main host server keeps the bit stream of full resolution content which can be decoded to produce a maximum quality, spatial and temporal resolution output. The supply of the scaled content, to a less capable display or to transmit through a lower bandwidth, is adapted in different nodes having different scaling parameters. At each node the scaling parameters might be different and a new bit stream is generated. Finally suitable decoded version is produced at the end-user display terminals. The framework for the scalable coding process can be divided in three main modules [2], [10]: Encoder, Extractor and Decoder. Encoder module is responsible to create the full resolution, highest quality compressed bit stream focusing on three main functionalities: quality scalability, resolution scalability and temporal resolution scalability. In a cross media engine the extractor module truncates the generated scalable bit stream depending upon the context and produces the adapted bit-stream which is also scalable and can be re-adapted at following network nodes by using another extractor. Decoder module finally decodes any adapted bitstream to produce the scaled media. During content adaptation (CA) process since irrelevant subbands and bit planes are discarded, some content protection information such as watermarking can also be lost. Therefore it is important to consider content adaptation as watermark attack when evaluating watermarking schemes.

Recent years have seen a plethora of visual media watermarking algorithms being developed with the advancement of visual media technologies. There have been some efforts on on the evaluation of watermarking technologies. For example with a given watermarked image, Stirmark [9] applies different attacks including cropping, filtering, rotation, JPEG compression to generate a number of modified images which are used to verify the existence of the watermark. Checkmark [8] performs the same job as Stirmark does and also evaluate and rate the watermarking schemes using different attacks including wavelet based compression. Watermark Evaluation Testbed [3] implemented a framework which enables different algorithms to test and check the robustness against different attacks. However all these work focused on attack characterisation based on common attacks like rotation, scaling and compression.

With the growing popularity of scalable coded media, there is a necessity for the formal evaluation of the watermark robustness against CA. In this paper we present a formal framework for evaluating different watermarking methods on robustness to scalable coding driven CA present in UMA. The framework, watermark evaluation bench for content adaptation modes (WEBCAM)[1] is a flexible modular formal framework evaluating the effect of various design parameters involved in wavelet-based watermarking robustness against CA attacks. The main objectives of this new framework are

1. To provide tools to emulate scalable coding based content adaptation and to use them on evaluation of watermark robustness.

2. To provide controlled experimental environment for wavelet based watermark evaluation. We achieved the same by disecting commonly used wavelet based watermarking algorithms into basic modules and fitting them into a common watermarking framework.

[1]The latest version of WEBCAM is available for download from http://svc.group.shef.ac.uk/webcam.html

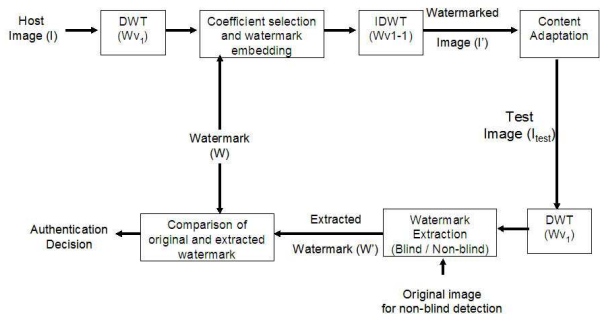

Figure 1: Block diagram of complete WEBCAM system architecture.

3. To identify new watermarking schemes by choosing various modules and parameters from this common framework which also can be be used as a learning tool of wavelet based watermarking.

The rest of the paper is organised with Section 2 which discusses the WEBCAM architecture including watermark embedding and extraction schemes along with content adaptation model. The example results using the framework are shown in Section 3. Finally, we conclude with a brief statement about our framework and some closing remarks in Section 4.

2 WEBCAM System Architecture

A controlled experimental set up is provided in WEBCAM framework as stated in objective 2. A basic block diagram of the complete system is shown in Fig. 1. WEBCAM architecture is designed in a modular approach based on three main functional areas: Watermark Embedding, Content Adaptation and Watermark Extraction and Authentication. The phase-I of WEBCAM focuses on watermarking for scalable coded images especially wavelet based watermarking.

2.1 Watermark Embedding

Watermark embedding process provides a platform to build new wavelet based algorithms using different combinations of parameters. Fig. 2 shows the basic blocks of the embedding procedure. A forward wavelet transform is applied to the target image with a choice to select wavelet kernel from a set of available linear and non-linear wavelet kernels (*e.g.*, orthogonal, biorthogonal, Morphological and spatially adaptive wavelets). Non-linear wavelets are realised using lifting schemes and quincunx method (Median lifting on quincunx sampling) [1, 4]. The wavelet coefficients are then modified according to the selected embedding procedure. A choice of subband and selection of important coefficients enhance the experimental combination. An inverse wavelet transform which is same as the forward wavelet kernel is then applied to produce the watermarked image. Finally the embedding performance is evaluated using PSNR and data hiding capacity information.

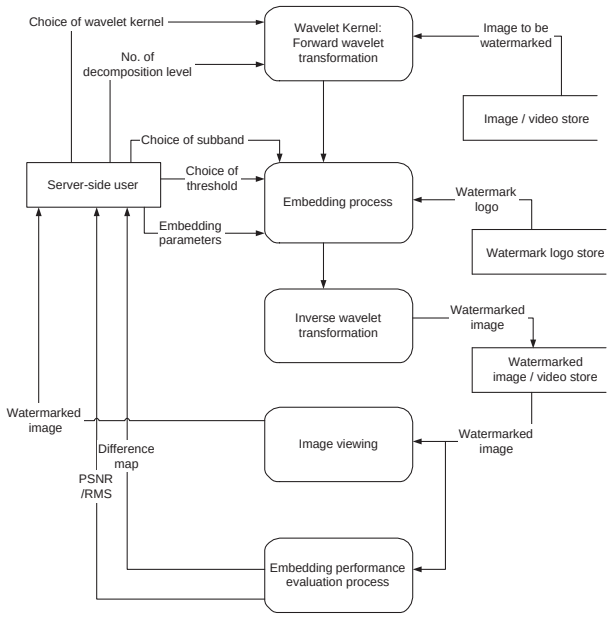

Figure 2: Block diagram of watermark embedding procedure.

WEBCAM framework evaluated various wavelet based embedding techniques discussed in the literatures [5, 7, 12, 13] and generalised under one common platform. It is observed that the basic embedding principle of the algorithms remains same and can be presented with following Equation (1).

$$C'_{m,n} = C_{m,n} + \Delta_{m,n}, \tag{1}$$

where $C'_{m,n}$ is modified coefficient at (m, n) position, $C_{m,n}$ is the coefficient to be modified and $\Delta_{m,n}$ is the modification due to watermark embedding. The embedding procedures are categorised in two main types of embedding algorithms: direct coefficient modification [5, 12] and quantisation based [13, 6].

In direct coefficient modification schemes, selected coefficients are directly modified based on following modification value (refer Equation (2)).

$$\Delta_{m,n} = \alpha.(C_{m,n})^b.W_{m,n}, \tag{2}$$

where $\Delta_{m,n}$ is modification value at (m, n) position, $C_{m,n}$ is the coefficient to be modified, α is the watermark weighting factor, $b = 1, 2...$ is the watermark strength parameter and $W_{m,n}$ is the watermark value. Authors of these schemes suggested different α and b value in their algorithms. In this framework we evaluate the performances using different α and b value separately or using combinations. The selection of the coefficients to be modified are suggested differently in different algorithms. A bit adaptive thresholding is followed in [5] whereas manual thresholding is done in [12]. This framework also includes above mentioned coefficient selection procedures to evaluate its effect on robustness.

A rank order based algorithm has been proposed in quantisation based watermarking schemes. It changes

the median value of a local area based (typically 3x1 coefficient window) on neighboring values as shown in Fig. 3. The selection of 3x1 window of the coefficients are

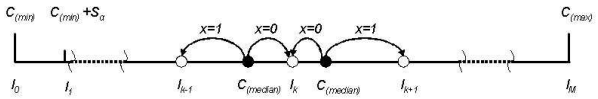

Figure 3: Rank order based quantisation

differently suggested in the literatures. Based on the selection procedures, we have categorised quantisation based method in two sub categories: intra subband quantisation [13] and inter subband quantisation [6]. In intra subband quantisation a non-overlapping 3×1 running window is passed through the selected frequency subband of the wavelet decomposed image as shown in Fig. 4(a). In the case of inter subband quantisation

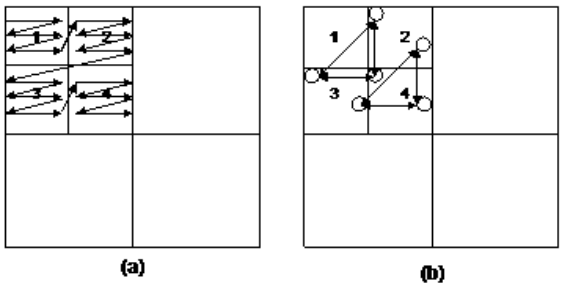

Figure 4: Quantisation embedding algorithm: (a) Raster scanning & (b) Median coefficient modification

a frequency orientation scanning is performed instead of the 3×1 running window (refer Fig. 4(b)). In both the cases once the coefficients are selected, the median value of each 3x1 window is modified according to rank order system. The modification value $\Delta_{m,n}$ is decided based on the quantisation step δ within the range of the selected 3x1 window. Different functions are suggested in the literatures to find the value of δ and the functions normally consists of minimum (C_{min}) and maximum (C_{max}) value of the coefficients in each selected window.

$$\delta = f(\alpha, C_{min}, C_{max}), \tag{3}$$

where α is the weighting factor. The modification of the median coefficient depends upon the position within the region in the quantisation interval (l_k) and the watermark information ($W_{m,n}$). The median value is modified to one of the quantisation step value as shown in Fig. 3. The direction of the modification is defined as a function (refer Equation (4)) of watermark information $W_{m,n}$ and the indices of the region of quantisation interval k.

$$f() = XOR(f(k), W_{m,n}) \tag{4}$$

More information about the quantisation based methods can be found in [6, 13].

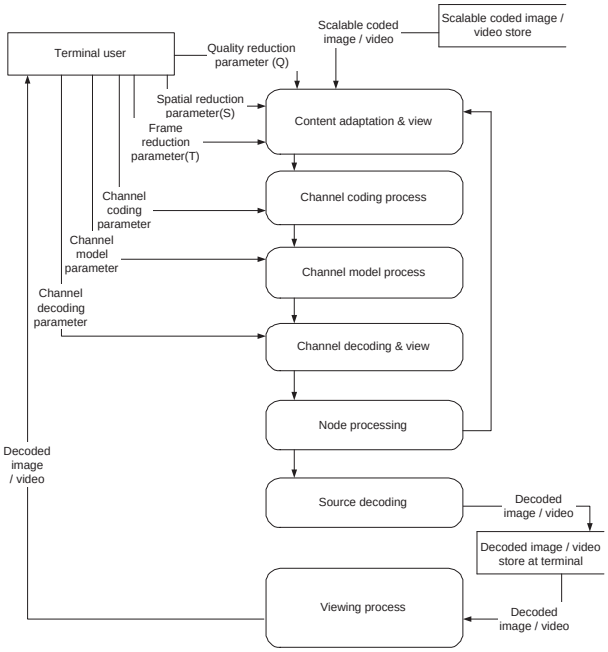

Figure 5: Block diagram of Content Adaptation attacks.

An inverse wavelet transformation of the associated wavelet base is then performed after watermark embedding to get the watermarked image. It also computes the embedding performance metrics such as imperceptibility measure and data hiding capacity.

2.2 Content Adaptation

The first objective to emulate CA is modeled in this module. The content adaptation module has two parts: content adaptation of scalable coded bit stream and simulation of transmission channel properties as shown in Fig. 5. The scalable coded bit stream is adapted at different transmission nodes based on the transmission speed, transmission medium and display devices. For example a full resolution bit stream is kept in the main server. To deliver this content to the end user we need to use transmission channel. The bit stream is adapted according to the channel capacity follwed by channel coding, channel model for transmission. At the receiving node a channel decoding is done to reproduce the bitstream. This bit stream is either readapted and follows the same process to be transmitted to another node or decoded at the same node to be displayed at the user device.

In this framework (Phase-I) we have used JPEG2000 based [11] content adaptation scheme. A quality scalability can compress the bitstream to generate a degraded version whereas a resolution scalability makes the image size smaller. This scaled version of the bitstream is then decoded to generate the content adopted image which is used to extract the watermark.

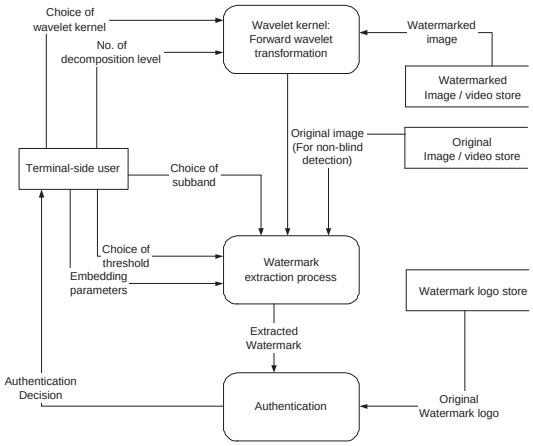

Figure 6: Block diagram of Watermark extraction procedure.

2.3 Watermark Extraction and Authenticity

Watermark extraction procedure can be categorised in two types: non-blind [12, 5] and blind [6, 13]. Original image is required only for a non-blind type of watermarking algorithm. The extraction procedure comprises of three basic modules: forward wavelet transformation, extraction algorithm and authentication decision. A block diagram of the the extraction procedure which is related to embedding algorithms is shown in Fig. 6. The forward wavelet transformation module is similar to the one which is used for embedding. Due to content adaptation attack especially for spatially scaled images a re-scaling scheme has been adopted for watermark extraction. The spatial resolution adaptation makes the image size smaller than the original size and thus it needs to be re-scaled to original size especially for the cases where higher frequency bands are used for embedding. The extraction procedure follows the inverse algorithm of the embedding scheme. The watermark extraction is based on the majority voting rule of the extracted watermarks. Finally the authenticity module decides whether the extracted watermark matches the original one. A similarity correlation [5] or Hamming distance measurement [6] helps to decide the authenticity. In the framework different authentication methods are included to compare the performances.

3 Evaluation Examples using WEBCAM

We have conducted a set of experiments using WEBCAM and evaluate watermarking performance with respect to embedding and robustness. As stated in the objectives, with different combination of parameters it is possible to rebuild the algorithms discussed in the literatures with different combination parameters available in WEBCAM (refer Table 1). We have performed experiments with various combinations of design parameters to create new watermarking schemes and evaluated their performances. The embedding performance (PSNR) is shown in Fig. 7.

Example results are shown to evaluate and compare the robustness of different watermarking schemes in a controlled

Method	Subband Selection	Wavelet Kernel	Decomp Level	Scheme
Direct($b = 2$)	High	Haar	2	[12]
Direct($b = 1$)	All	Biorthogonal	3	[5]
Intra Subband	Low	Any	2	[13]
Inter Subband	High	Haar	1	[6]

Table 1: Realisation of wavelet based algorithms using different combination of WEBCAM parameters

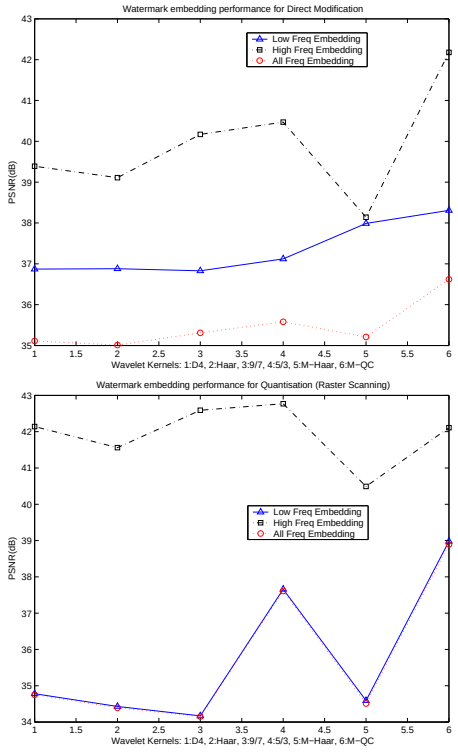

Figure 7: Watermark embedding distortion performance graph. *Row1:* Direct modification. *Row2:* Intra subband scanning

experimental set up. In each cases the content adaptation is simulated for full resolution and half resolution image with different compression ratio. Following are the examples of the experimental set and their results using the framework:

1. Different methods are compared with given set of wavelet kernel, embedding region and no of decomposition level (as shown in Fig. 8).

2. Different embedding region are compared for direct modification method when other parameters are fixed (as shown in Fig. 9).

3. Different embedding region are compared for intra subband quantisation with given wavelet kernel and decomposition level (as shown in Fig. 10).

4. Robustness due to different wavelet kernels have been

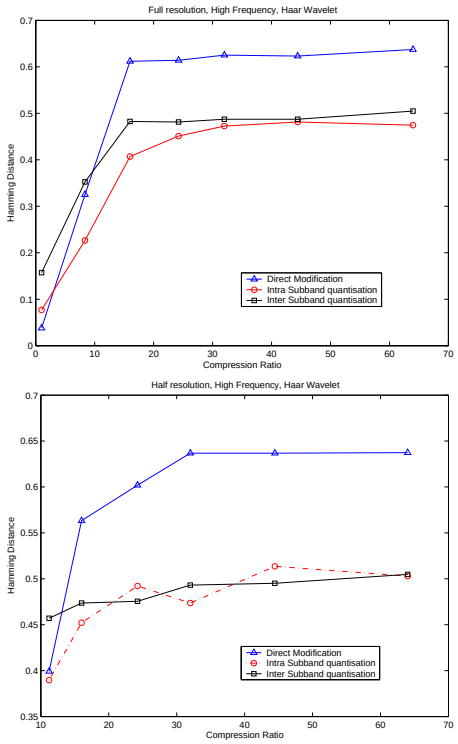

Figure 8: Evaluation of different methods with given wavelet kernel, embedding region and no of decomposition level. Hamming distance is measured for full resolution (*Row 1*) and half resolution (*Row 2*) with various compression ratio.

compared for direct modification (as shown in Fig. 11).

5. Comparison is made due to different wavelet kernels for intra subband quantisation for given embedding region and decomposition level (as shown in Fig. 12).

4 Conclusion

We have dissected commonly used wavelet based watermarking algorithms into basic modules and fit them into a common framework. For formal evaluation of watermarking algorithms on robustness to content adaptation, in this paper we have discussed the inclusion of of JPEG2000 based content adaptation attacks and evaluated the robustness of various wavelet based watermarking algorithms to quality and resolution scalability.

Acknowledgements

This project is funded by BP-EPSRC Dorothy Hodgkin postgraduate award.

References

[1] G. C. K. Abhayaratne and H. Heijmans. A novel morphological subband decomposition scheme for 2D+t wavelet video coding. In *Proc. Int'l Symp. on Image and Signal Processing and Analysis*, volume 1, pages 239–244, 2003.

[2] S. Dogan, S. Eminsoy, A. H. Sadka, and A. M. Kondoz. Video content adaptation using transcoding for enabling uma over umts. In *Proc. 5th International Workshop on Image Analysis for Multimedia Interactive Services (WIAMIS 2004)*, 2004.

[3] O. Guitart, H. C. Kim, and E. J. Delp III. Watermark evaluation testbed. *SPIE Journal of Electronic Imaging*, 15:041106 (13 pages), 2006.

[4] H.J.A.M. Heijmans and J. Goutsias. Nonlinear multiresolution signal decomposition schemes. ii. morphological wavelets. *Image Processing, IEEE Transactions on*, 9(11):1897–1913, Nov 2000.

[5] J. R. Kim and Y. S. Moon. A robust wavelet-based digital watermarking using level-adaptive thresholding. In *Proc. IEEE ICIP*, volume 2, pages 226–230, 1999.

[6] Deepa Kundur and Dimitrios Hatzinakos. Digital watermarking using multiresolution wavelet decomposition. In *Proc. ICASSP*.

[7] P. Meerwald and A. Uhl. A survey of wavelet-domain watermarking algorithms. In *Proc. SPIE Security and Watermarking of Multimedia Contents III*, volume 4314, pages 505–516, 2001.

[8] S. Pereira, S. Voloshynovskiy, M. Madueno, S. Marchand-Maillet, and T. Pun. Second generation benchmarking and application oriented evaluation. In *Proc. 4th Intl. Information Hiding Workshop, Pittsburgh, PA, Lect. Notes Comput. Sci.*, volume 2137, pages 340–353, 2001.

[9] F. A. Petitcolas, M. Steinebach, F. Raynal, J Dittmann, C. Fontaine, and N. Fates. Public automated web-based evaluation service for watermarking schemes: Stirmark benchmark. In *Proc. IEEE ICIP*, volume 4314, pages 575–584, 2001.

[10] N. Sprljan, M. Mrak, G. C. K. Abhayaratne, and E. Izquierdo. A scalable coding framework for efficient video adaptation. In *Proc. 6th International Workshop on Image Analysis for Multimedia Interactive Services (WIAMIS)*, 2005.

[11] D. S. Taubman and M. W. Marcellin. *JPEG2000 Image Compression Fundamentals, Standards and Practice*. Springer, USA, 2002.

[12] X. Xia, C. G. Boncelet, and G. R. Arce. Wavelet transform based watermark for digital images. *Optic Express*, 3(12):497–511, December 1998.

[13] L. Xie and G. R. Arce. Joint wavelet compression and authentication watermarking. In *Proc. IEEE ICIP*, volume 2, pages 427–431, 1998.

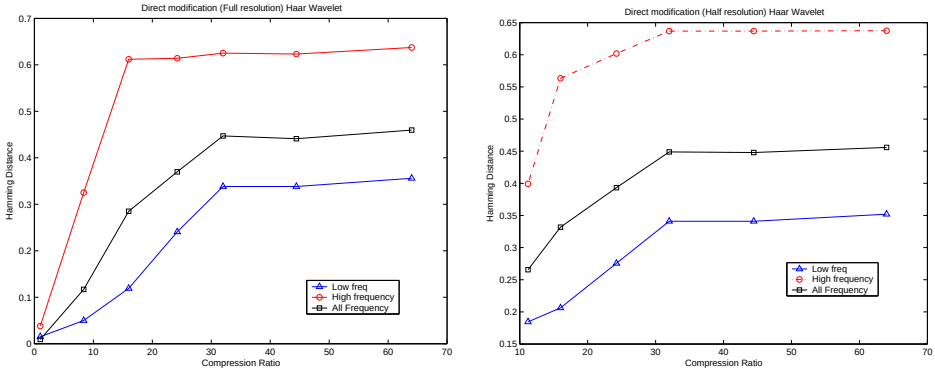

Figure 9: Evaluation of different embedding region with given direct modification algorithm, wavelet kernel and no of decomposition level. Hamming distance is measured for full resolution (*Column 1*) and half resolution (*Column 2*) with various compression ratio.

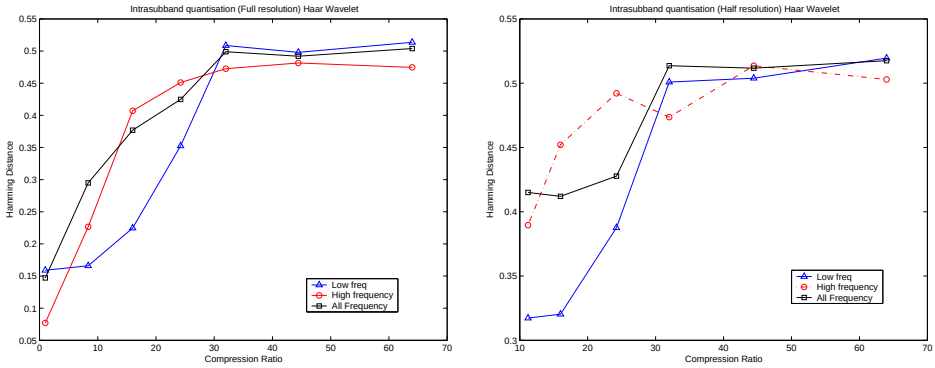

Figure 10: Evaluation of different embedding region with given intra subband quantisation algorithm, wavelet kernel and no of decomposition level. Hamming distance is measured for full resolution (*Column 1*) and half resolution (*Column 2*) with various compression ratio.

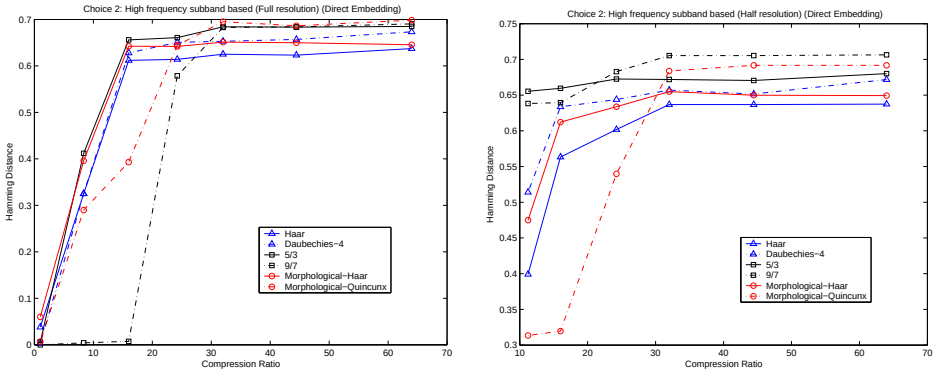

Figure 11: Evaluation of using different wavelet kernel with given direct modification algorithm, selected embedding region and no of decomposition level. Hamming distance is measured for full resolution (*Column 1*) and half resolution (*Column 2*) with various compression ratio.

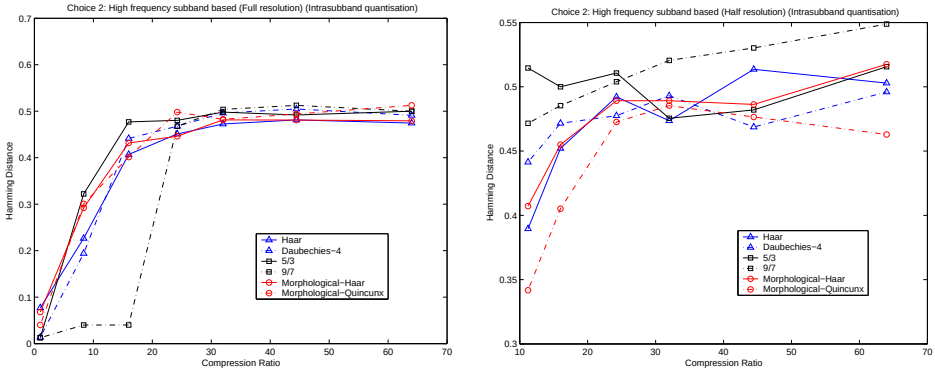

Figure 12: Evaluation of using different wavelet kernel with given intra subband quantisation algorithm, selected embedding region and no of decomposition level. Hamming distance is measured for full resolution (*Column 1*) and half resolution (*Column 2*) with various compression ratio.