

Lifting Based Wavelet Transform for Lossy to Lossless Image Coding

Mr. W.B.Pahurkar¹, Prof.Ms. V. S. Sakharkar², Prof.Ms. A. B. Pahurkar³, Prof. Vivek I. Akolkar⁴

¹Research Scholar, P R Patil College of Engineering, Amravati

^{2,3}Assisitant Professor, PRMIT & R, Badnera,

⁴Assisitant Professor, SLRTCE, Mira Road(E), Thane-401107

¹pahurkarwasudeo@gmail.com, ²vssakharkar@mitra.ac.in, ³abpahurkar@mitra.ac.in, ⁴vivek.akolkar@slrtce.in

Abstract: In current age of information security plays a vibrant role. Information or messages are exchanged over a network out of which enormous data is confidential which increases the demand for advance information security. The different approaches like cryptography and steganography are used for security purpose. But both of them have some gaps and when used discretely does not perform well hence we use the amalgamation of both cryptography and steganography called as metamorphic cryptography. In this paper we mainly focus on providing double layer security for the video using Metamorphic Cryptography. Each frame of the video is first Encrypted using Symmetric Key; each frame of the encrypted video is further concealed with cover image resulting into Steganography image. The proposed system is simple and new and therefore can be used to transfer highly confidential data like military secrets, hospital reports and other data. This proposed method strives for high security to an eavesdropper's inability to detect hidden information.

Keywords: Security, Cryptography, Video Steganography.

1. INTRODUCTION

In Metamorphic Encryption Technique three steps befallen, this are as follows first one is Symmetric Encryption Technique, in that symmetric key encryption AES (Advanced Encryption Standard) Algorithm used because this algorithm is most superior then others algorithms then in second step chaotic rearrangement of encrypted data this is use for, arrange the encrypted data in image randomly and in third step Steganography used in that steganography LSB (Least Significant Bit) Technique is used.

Symmetric Key Encryption

In Symmetric Key Encryption Technique we can use AES (Advanced Encryption Standard) Algorithm. The need for coming up with a new algorithm was actually because of the perceived weakness in DES. The 56-bit key of DES were no longer considered safe against attacks based on exhaustive key searches and the 64-bit blocks were also considered as weak. In October 2000, Rijndael was announced as the final selection for AES. In November 2001 became a US Government standard published as Federal Information Processing Standard 197(FIPS 197). AES was to be based on 128-bit blocks, with 128-bit keys. According to its designers [2]. AES is a block cipher intended to replace DES for commercial applications. It uses a 128-bit block size and a key size of 128, 192, or 256 bits. AES does not use a Feistel structure. Instead, each full round consists of four separate functions: byte substitution, permutation, arithmetic operations over a finite field, and XOR with a key [1].

. Symmetric and parallel structure

This gives the implementers of the algorithm a lot of flexibility. It also stand up well against cryptanalysis attacks.. . Adapted to modern processors

The algorithm works well with modern processors (Pentium, RISC, parallel).

. Suited to smart cards

The algorithm can work well with smart cards.

Rijndael supports key length and plain text block sizes from 128 bits to 256 bits, in the steps of 32 bits. The key length and the length of the plain text blocks need to be selected independently. AES mandates that the plain text block size must be 182 bits and key size should be 128,192 or 256 bits. In general two versions of AES are used: 128-bit plain text block combined with 128-bit key block and 128-bit plain text block with 256-bit key block [2].

Since the 128-bit plain text block and 128-bit key length are likely to pair as a commercial standard, we will examine that case only. Other principles remain the same. Since 128-bit give a possible key range of $2^{128}=3*10^{38}$ keys, Andrew Tanenbaum outlines the strength of this key range in his un-imitable style:

Even if NSA manages to build a machine with 1 billion parallel processors, each being able to evaluate one key per picosecond, it would take such a machine about 10^{10} years to search the key space. By then the sun would have burned out, so the folks then present will have to read the results by candlelight. The basics of Rijndael are in a mathematical concept called as Galois Field theory.

Similar to the way DES function, Rijndael also uses the basic techniques of substitution and transposition (i.e. permutation). The key size and plain text block size decide how many rounds need to be executed. The minimum number of rounds is 10 and maximum number of rounds is 14. One key differentiator between DES and Rijndael is that all the Rijndael operation involve entire byte and not

individual bits of byte. This provides for more optimized hardware and software implementation of the algorithm. Following steps describes the Rijndael at a high level.

Chaotic Rearrangement

Chaotic rearrangement is a time series prediction, chaotic arrange the encrypted data in the image chaotically or randomly. Chaotic rearrangement is also called as randomly, arrange the encrypted data for higher level of security because number of round protect the secure data.

Steganography

Steganography can be defined as the art and science

of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message [12].It is a form of security through insignificance. Simply put, steganography is simply a way of concealing the existence of secret communication.

Steganography is not to be mixed up with cryptography. Cryptography involves the scrambling of communication to make impossible to read to unintended recipient. One may not know the intended meaning of the message, but it is obvious that it exists. Steganography makes an attempt to hide the fact that the secret communication even exists, thereby not drawing attention to it. It replaces bits of unused data into the file-i.e. graphics, sound, text, audio, and video with some other bits that have been obtained secretly and unauthorized manner. [12]

Digital Steganography Techniques

Modern steganography entered the world in 1985 with the coming one of the personal. The advents of new technology make this a seemingly limitless art form. Digital Steganography utilizes digital media (images, audio and video files) as a cover for hidden data [12]. The basic idea involves hiding and stuffing bits or bytes into various forms of media, and then transmitting that media across a network. There are now over 800 known digital steganography tools available at little and no cost.

There are numerous ways to conceal information in digital steganography. The most common are LSB (Least Significant Bit) and injection. Because it's superior as compare to others techniques, below describe the LSB in great detail.

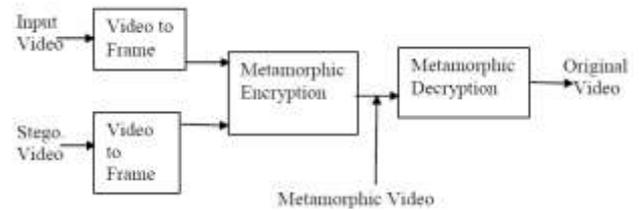
Least Significant Bit (LSB)

The Least Significant Bit (LSB) is a technique used in digital Steganography. The least significant bit term comes from the numeric significance of the bits in a byte. The high-order and most significant bit is the one with the highest arithmetic value (that is, 2⁷=128), whereas the low-order and least significant bit is the one with the lowest arithmetic value (that is, 2⁰=1).

The least significant bits are the open to areas of the file and are the playing ground for Steganography. These bits or bytes can be substituted with the information to be hidden without significantly altering the file.

A simple example of LSB substitution; to conceal the character 'G' across the eight bytes below of a carrier file (the least significant bits are underlined) [12]: **10010101**

**00001101 11001001 10010110 00001111 11001011
 10011111 00010000**



Above figure shows the proposed method of metamorphic approach. Here first of all we take one input video which is to be sent and we take a second steganography video which we want to hide in the input video. Let's call these videos as V1 and V2 respectively. So here we will hide video V2 into V1 and the final encrypted video will look like as V1. Here we will convert both the videos V1 and V2 into frames and will obtain the fused frames by metamorphic encryption as single video which is the final encrypted video which contains information of both the videos but looks like as the input video V1. In order to get the secret stego video back from the encrypted video we have to perform the metamorphic decryption which is the reverse process of encryption technique

II. PERFORMANCE METRICS

To evaluate the performance of image compression systems, a technique to measure compression is needed.

For this , the compression ratio (CR) metric is often employed and is defined as [9]

$$CR = \frac{\text{original image size in bits}}{\text{com pressed image size in bits}} \quad (1)$$

Sometimes compression is instead quantified by stating the *bitrate* (BR) measured by compression in bpp (bits per pixel).The bit rate after compression and compression ratio are related as [9]

$$BR = \frac{\text{bits /pixel for original image}}{CR} \quad (2)$$

In the case of lossy compression, the reconstructed image is nearly equal to the original. The difference between the original and reconstructed signal is defined by approximation error or *distortion*. It is expressed in terms of *mean-squared error* (MSE) or *peak-signal-to-noise ratio* (PSNR). These are defined, respectively as in [9],

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (x[i, j] - \hat{x}[i, j])^2 \quad (3)$$

Where *x* is the original image with dimensions *M*×*N* having *P* bpp, and *x*^ is the reconstructed image. Evidently, smaller

lifting scheme. The lifting scheme is a simple yet powerful tool to construct second generation wavelets. The lifting scheme is an alternative description of the discrete wavelet transform as well as an alternative way to build wavelets. Lifting provides several advantages including:

- In-place calculation of the wavelet coefficients
- Inverse wavelet transform is easily obtained
- Ability to perform integer-to-integer wavelet transform.
- Extension to domains, which are not shift-invariant.
- Extension to irregularly-sampled data

Lifting scheme directs to a faster, in-place calculation of the wavelet transform [22]

IV. DESIGN AND IMPLEMENTATION

4.1 Filter Banks for Image Coding

Filter banks are mainly used to separate the input signal into multiple components and each component carrying a single frequency subband of the original signal [23], [24]. It is desirable to design the filter bank such that these subbands can be recombined to recover the original signal so that we get the original signal.

Ideal filters, inherently, are not feasible and the issue was first addressed using two-channel linear-phase filter banks and a design called quadrature mirror filter bank (QMF). To cancel aliasing resulting from the decimation and interpolation processes quadrature mirror filter bank was introduced [23], [25]. Johnston's filters are a family of QMF designed to cancel aliasing [26].

The QMF solutions do not allow perfect reconstruction (PR) of the signal and later Smith and Barnwell [27] developed the conjugate quadrature filter bank (CQF) in a formulation which does not use linear-phase filters but allows PR of the signal. Both QMF and CQF solutions have a two-channel filter bank which can be hierarchically associated in a binary-tree path in order to create filter banks with more than two channels.

A uniform filter bank is the one where all, let us say, M filters have bandpass width of π/M , thus signals of all Subband are decimated and interpolated by a factor of M [23],[24]. Fig. 1 shows an M -channel critically decimated uniform filter bank. In this figure, M is the number of filters (or number of channels or Subband), $x(n)$ is the input signal, and $\hat{x}(n)$ is the recovered signal after synthesis. The Subband signals are represented by $y_i(m)$ ($0 \leq i \leq M-1$), and the filters with impulse responses $f_i(m)$ and $g_i(m)$ ($0 \leq i \leq M-1$) correspond to analysis and synthesis sections, respectively.

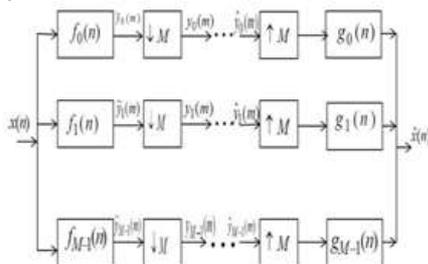


Fig 1: Critically decimated uniform filter bank. Analysis (left) and synthesis (right)].

Filter banks can also be classified into paraunitary or bi-orthogonal [24]. In paraunitary FIR filter banks, each $f_i(m)$ has a one-to-one correspondence to $g_i(m)$ [15], [25], [28], while in bi-orthogonal filter banks the set $f_i(m)$ is found from the entire set of $g_i(m)$ or vice versa [24], [28]. This is similar to the relation between orthogonal and non-orthogonal matrices, and in fact, orthogonal block transforms are a special case of paraunitary filter banks, while non-orthogonal ones belong to the class of bi-orthogonal filter banks.

In numerous applications, especially image processing, it is crucial that all analysis and synthesis filters have linear phase. Such system is called a linear phase filter bank (LPFB). Besides the elimination of the phase distortion which is often disastrous in many image processing applications [30], LP filters preserve the locality of the edges, the key to success of hierarchy image coding algorithms [28], [29], [31], [32].

The latter Polyphase representation in Figure 2 proves to be very useful, both theoretically and practically, in filter bank design and application.

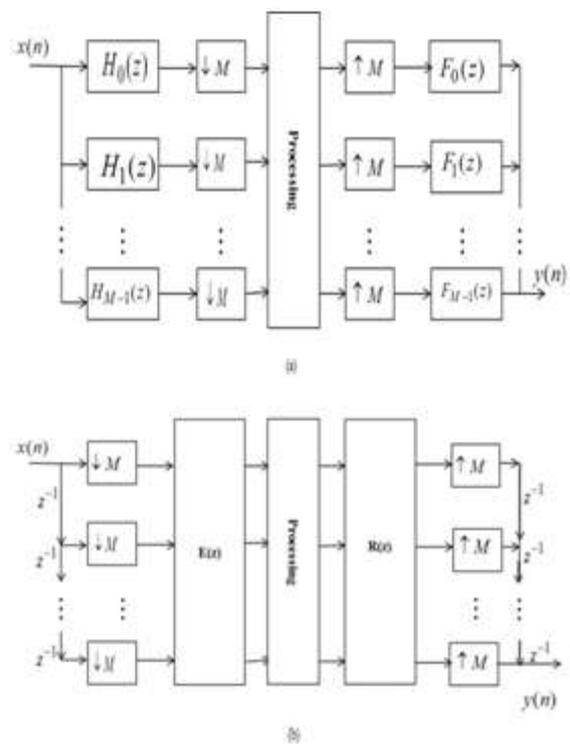


Figure 2: M-channel filter bank a) regular structure b) Polyphase structure

Not only does it allow the processing of signals at lower rates, but it also simplifies filter bank theory dramatically.

4.2 Bi-orthogonal Filter Banks (BOFBs)

PUFBs can be designed easily and also the number of design parameters is smaller than that of BOFBs. The frequency responses of PUFBs are usually worse. Also PUFB's have many restrictions compared to BOFBs. To apply FBs to lossless image coding, the lattice structure should be represented by lifting structures which has unity

diagonal scaling coefficients to avoid quantization errors. Factorization of BOFBs involves non-unity diagonal scaling coefficients. Hence, they have not been applied to lossless coding directly.

In [36], degree-1 BOFBs which have unity diagonal scaling coefficients throughout the lifting structure have been proposed. In [37], order-1 building blocks in BOFBs are taken forward. Though this lifting structure has more design parameters than those of the conventional order-1 PUFBs And degree-1 BOFBs, structure shown in [37] provide reduction in the number of rounding operations since a rounding operation can be regarded as quantization noise; the number of rounding operations affects the subband energy compaction.

The structure shown in [37] has taken into account not only restriction such as paraunitary but also has rounding operation less compared to [30] and [40].

But still the structure in [37] did not consider the restrictions such as number of channels and McMillan degree. The block-lifting structure proposed in [38] covers broader family which gives best solution compared to the conventional methods. This structure is free from the restriction such as Paraunitary, number of channels and McMillan degree while maintaining less rounding operations than [39] and [40]. Compared to conventional FBs, the designed BOFBs give better Lossy-to-lossless image coding performance in both PSNRs and perceptual visual quality for the images containing a lot of high frequency components [38].

V. RESULTS

5.1 Filter coefficient

Consider $M = 4$, $\gamma_k = 2$ and set the initial random parameter for L_k and U_k and optimize it for maximum coding gain which gives the filter impulse response as Figure 3 and frequency response as Figure 4

Image coding results are as follow shown in Figure 5 which shows Original image and Figure 6 shows Reconstructed image:

The PSNR performance is 22.93 dB.

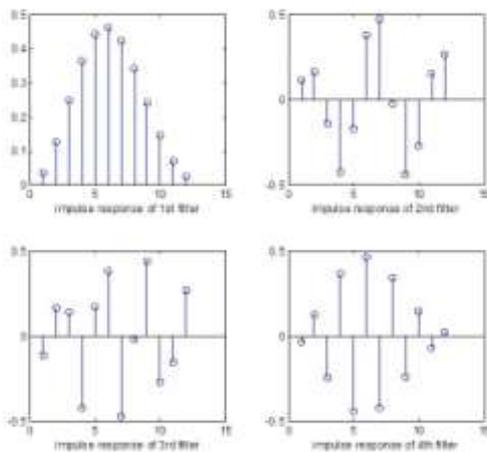


Figure3 :Impulsereponse of filter bank

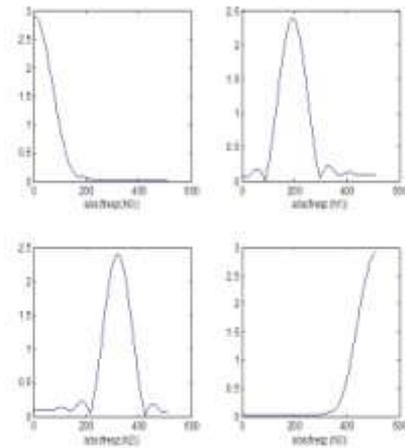


Figure4 : Frequency response of filter banks



Figure 5: Original Barbara Image



Figure 6: Reconstructed Barbara Image

VI. DISCUSSION AND CONCLUSION

This paper focuses on the theory, structure, design, implementation, and application in image compression of linear phase perfect reconstruction filter banks with arbitrary

M channels and arbitrary-length filters. This class of FBs is purposely chosen to have high practical values: linear phase, FIR, real (sometimes even rational and integer) filter coefficients, and exact reconstruction. The approach consistently taken throughout the dissertation is to parameterize the FBs by lattice structures based on the factorization of the analysis and synthesis polyphase transfer matrices. From a slightly different point of view, the factorization allows the construction of a highly complex system from a cascade of identical low-order building blocks, each is carefully designed to propagate structurally the most desired properties, namely linear phase and perfect reconstruction.

In other words, in the lattice representation, both of these crucial properties are retained regardless of the quantization of lattice coefficients to any desired level.

The lattice structure offers a powerful characterization in both FB design and implementation. From a design perspective, the lattice coefficients can be varied independently and arbitrarily without affecting the LP and PR properties. Secondary FB properties such as high coding gain and low stopband attenuation can be further achieved using unconstrained optimization techniques. From an implementation perspective, the cascading construction provides a fast, efficient, robust, and modular structure which leads itself nicely to hardware realization in VLSI.

REFERENCES

- [1] Bahl L. R., Kobayashi H, "Image Data Compression by Predictive Coding I: Prediction Algorithms", IBM Journal of Research & Development, vol. 18, no. 2, 1974.
- [2] Wen-Jun Zhang Song-Yu Yu Hong-Bin Chen, "A new adaptive classified transform coding method [image coding]" International Conference on Acoustics, Speech & Signal Processing, 1989.
- [3] M. Antonini, M. Barlaud, P. Mathieu, and I. Daubchies, "Image coding using wavelet transform," IEEE Trans. Image Process., vol. 1, no. 4, pp. 205–220, Apr. 1992.
- [4] Budge S., Baker R, "Compression of color digital images using vector quantization in product codes", IEEE Trans. Image Process., vol. 10, no. 4, pp. 129–132, Apr. 1985.
- [5] Anderson G., Huang T., "Piecewise Fourier Transformation for Picture Bandwidth Compression", IEEE Trans. Communication Technology, vol. 19, no. 2, pp. 133–140, Apr. 1971
- [6] Ready P, Wintz P, "Information Extraction, SNR Improvement, and Data Compression in Multispectral Imagery", IEEE Trans. Communications, vol. 21, no. 10, pp. 1123–1131, Oct. 1973.
- [7] Feria, Erlan H. Barba, Joseph Scheinberg, Norman, "A Simple Predictive Transform Coder for Images" *IEEE Military Communications Conference - Communications - Computer*, 1986.
- [8] Andrews H., Patterson C., "Singular Value Decomposition (SVD) Image Coding", IEEE Trans. Communications, vol. 24, no. 4, pp. 425–432, Apr. 1976.
- [9] Michael D.A.(2002), "Reversible integer-to-integer transforms for image coding", (Phd thesis), University of British Columbia
- [10] H. S. Malvar and D. H. Staelin, "The LOT: Transform coding without blocking effects," IEEE Trans. Acoust., Speech, Signal Process., vol. 37, no. 4, pp. 553–559, Apr. 1989.
- [11] H. C. Reeve. III. And J. S. Lim. "Reduction of blocking effect in image coding." in Proc. ICASSP 83. Boston.MA. pp. 1212-1215., Apr. 1983.
- [12] D. E. Pearson and M. W. Whybray, "Transform coding of images using interleaved blocks," IEEE Proc., Part F, vol. 131, pp. 466-472, Aug. 1984.
- [13] H. S. Malvar, "A pre- and post-filtering technique for the reduction of blocking effects," presented at the Picture Coding Symp., Stockholm, Sweden, June 1987.
- [14] N. Ahmed and K. R. Rao, "Orthogonal transforms for digital signal processing." New York, NY: Springer, 1975.
- [15] H. S. Malvar, "Signal Processing with Lapped Transforms". Norwood, MA: Artech House, 1992.
- [16] P. Cassereau, "A New Class of Optimal Unitary Transforms for Image Processing", Master's Thesis, Mass. Inst. Tech., Cambridge, MA, May 1985.
- [17] K. R. Rao and P. Yip "Discrete Cosine Transform: Algorithms, Advantages, Applications", San Diego, CA: Academic Press, 1990.
- [18] R. L. de Queiroz, T. Q. Nguyen, and K. R. Rao, "The GenLOT: Generalized linear-phase lapped orthogonal transform," IEEE Trans. Signal Process., vol. 44, no. 3, pp. 497–507, Mar. 1996.
- [19] C. K. Chui (ed.), "Wavelets - A Tutorial in Theory and Applications", San Diego, CA: Academic Press, 1992.
- [20] A. N. Akansu and R. A. Haddad, "Multiresolution Signal Decomposition: Transforms, Subband, Wavelets", San Diego, CA: Academic Press, 1992.
- [21] W. Sweldens "The lifting scheme: A construction of second generation wavelets," SIAM J. Math. Anal., vol. 29, no. 2, pp. 511–546, 1997.
- [22] W. Sweldens, "The lifting scheme: A new philosophy in biorthogonal wavelet constructions," in Proc. of SPIE 2569, 1995.
- [23] R. E. Crochiere and L. R. Rabiner, Multirate Digital Signal Processing. Englewood Clis, NJ: Prentice-Hall, 1983.
- [24] P. P. Vaidyanathan, Multirate Systems and Filter Banks. Englewood Cliffs, NJ: Prentice Hall, 1992.
- [25] D. Esteban and C. Galand, "Applications of quadrature mirror to split band voice coding schemes". Acoustics, Speech, and Signal Processing, IEEE International Conference on ICASSP '77.vol.2,pp.191-195,May 1977.
- [26] J. D. Johnston, A filter family designed for use in quadrature mirror filter banks, "Proc. of Intl. Conf. on Acoust. Speech, Signal Processing, Denver, CO, pp. 291{294, 1980}.
- [27] M. J. Smith and T. P. Barnwell, "Exact reconstruction techniques for tree structured Subband coders", IEEE Trans. Acoust., vol.34,no.3,pp.434-441,Jun 1986.
- [28] M. Vetterli and D. Le Gall, "Perfect reconstruction filter banks: some properties and factorizations", IEEE Trans. Acoust., Speech, Signal Processing, ASSP-37, pp.1057 {1071, July 1989}.
- [29] A. V. Oppenheim and R. W. Schaffer, Digital Signal Processing, Englewood's Cliffs,NJ : Prentice-Hall, 1975.
- [30] D. Le Gall, and A. Tabatabai "Sub-band coding of digital images using symmetric short kernel filters and arithmetic coding techniques" Proc. of Intl. Conf. onAcoust., Speech, Signal Processing, pp. 761 {764, 1988}.
- [31] R.L. de Queiroz and K. R. Rao, "Time-varying lapped transforms and wavelet packets", IEEE Trans. on Signal Processing, vol. 41, pp. 3293{3305, Dec. 1993}.
- [32] R. L. de Queiroz and H. S. Malvar, "On the asymptotic performance of hierarchical transforms", IEEE Trans. on Signal Processing, Vol 40, pp. 2620{2622, Oct. 1992}.
- [33] X. Gao, T. Q. Nguyen, and G. Strang, "On factorization of M channel paraunitary filter banks," IEEE Trans. Signal Process. Vol. 49, no. 7, pp. 1433–1446, Jul. 2001.
- [34] M. Ikehara and Y. Kobayashi, "A novel lattice structure of M channel paraunitary filter banks," in Proc., IEEE Int. Symp. Circuits Syst., pp. 4293–4296, 2005.
- [35] T. Suzuki, Y. Tanaka, and M. Ikehara, "Lifting-based paraunitary filter banks for Lossy/lossless image coding," IEICE Trans. Fundamentals, vol. J89-A, no. 11, pp. 950–959, Nov. 2006.
- [36] Y.-J. Chen, S. Oraintara, and K. S. Amaratunga, "M-channel lifting-based design of paraunitary and biorthogonal filter banks with structural regularity," in Proceedings of ISCAS '03., Bangkok, Thailand, May 2003.
- [37] S. Iwamura, Y. Tanaka, and M. Ikehara, "An efficient lifting structure of biorthogonal filter banks for lossless image coding," in Proc. of ICIP'07, San Antonio, TX, Sep. 2007, pp. 433–436.
- [38] Taizo Suzuki , Masaaki Ikehara, and Truong Q. Nguyen, "Generalized Block-Lifting Factorization of M-Channel Biorthogonal Filter Banks for Lossy-to-Lossless Image Coding" IEEE Transactions on Image process.,vol.21,no.7,pp3220-3228, July2012
- [39] P. Hao and Q. Shi, "Matrix factorizations for reversible integer mapping," IEEE Trans. Signal Process., vol. 49, no. 10, pp. 2314–2324, Oct. 2001.
- [40] Y. She, P. Hao, and Y. Paker, "Matrix factorizations for parallel integer transformation," IEEE Trans. Signal Process. vol. 54, no. 12, pp. 4675–4684, Dec. 2006.