Advances in Mechanics
Volume 11, Issue 2, 2023
Page 186-193

A GENERALIZED BI-ORTHOGONAL HALFBAND FILTERBANK DESIGN FOR IMAGE ENCRYPTION

[1]Vivek P Khalane, [2]Shital Patil

[1,2]Department of Instrumentation Engineering – Ramrao Adik Institute of Technology, Navi Mumbai, Gmail : vivek.khalane@rait.ac.in

Abstract

Preventing the tampering of real-time signals via intrusion or unauthorized access is the necessity of the time. This paper presents a new technique of image encryption based on parameterized 9/7 wavelet filterbank. We have used 2-D Discrete wavelet transform (DWT) to decompose the input image. The new parameterization approach is proposed to design 9/7 length filterbank. The proposed 9/7 filters are used in wavelet decomposition. Then, filter design parameters, level of decomposition, sequence of code, approximation and detail subband coefficients are arranged uniquely in bookkeeping vector S. The above said factors arranged in stack format of S acts as a key feature of proposed image encryption and decryption process. Therefore, image decryption is possible only when the client knows S. The proposed algorithm is difficult to break and has low computational complexity. The proposed filters satisfy the perfect reconstruction property.

Keywords: fast neutron - free path - half layer thickness - polyethylene - concrete.

1- Introduction

With the advent of new cryptography techniques a secure multimedia transmission can be established that denies unauthorized access. Applications of images processing are spread across domains such as aerospace, military, and aviation. Thus, establishing a secure and safe gateway of such multimedia signals has become necessary. To this end, Wavelet-based image encryption is a widely accepted technique. The one-dimensional (1-D) and two-dimensional (2-D) FIR wavelet filler banks are the most promising methods in image processing. The phase characteristics of 1-D filterbanks are as promising as their low coefficient of sensitivity [1]–[4]. The Filterbank relies on segmentation and time-reversal techniques to split the input signal into multiple components [5]–[7]. Some secured have been proposed in [8]–[11]. In [12] Parameterized 9/7 wavelet filter bank designed on basis of lifting scheme. In [10], Wavelet filter bank 5/3 improved frequency response using higher order half band product polynomial.

The cryptography techniques for RGB images with the use of random matrix affine ciphers have been proposed in [13]. Fractional order Fourier transforms and Wavelet-based decomposition techniques with application to multiple image encryption have been proposed in [14]. The encryption of multiple images is done effectively with the help of fractional fourier transform and decomposition of wavelet transform. A chaotic map-based fractional wavelet

transform have been proposed in [15] that delivers higher performance. Spatial and transform domain based techniques with significant remedies to numerical as well as differential attacks. Integer wavelet transforms have been proposed in [16], [17]. Furthermore Chirkov standard maps, integer wavelet transforms have been proposed in [18]–[21] are the interesting developments in the domain of image encryption.

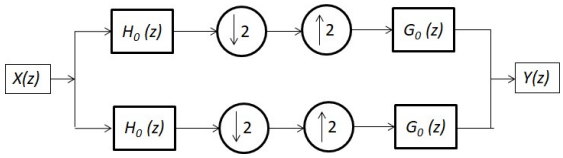

Figure 1. Structure of Two-channel bi-orthogonal filter bank.

This paper presents a new methodology that encrypts images based on parameterized 9/7 wavelet filter bank. The discrete wavelet transform is applied to perform cryptography related operations. The input signal, x passes through the low pass filters and then it is convolved with an impulse signal as shown below:

$$y[n] = (x * g)[n] = \sum_{k=-\infty}^{\infty} x[k]g[n-k]$$

x is decomposed via low pass H0 and high pass H1 filters with impulse responses. The output of these is rendered as the coefficients of approximation and detail, respectively. Discrete wavelet transform is harnessed to decompose the image and the compression is carried out by using thresholds on the decomposed images. A bookkeeping vector S is found, as discussed in next section.

The paper is organized as follows: Section II briefly introduces the two channel filter bank and proposes design of 9/7 filterbank. Section III presents the methodology for image encryption that uses the parameterized 9/7 wavelet filterbank. Section IV concludes the paper.

2 - Review of Filter Bank

Fig. 1 shows the structure of two-channel bi-orthogonal filter bank. The output of filter bank is given as:

$$\begin{aligned} Y(z) &= \frac{1}{2}\left[G_0(z)H_0(z) + G_1(z)H_1(z)\right]X(z) \\ &+ \frac{1}{2}\left[G_0(z)H_0(-z) + G_1(z)H_1(-z)\right]X(-z) \end{aligned} \quad (1)$$

Advances in Mechanics
Volume 11, Issue 2, 2023
Page 186-193

Equation (1) assures constraint for perfect signal reconstruction. The perfect reconstruction (PR) condition can be written as:

Where, Analysis filter is represented by $B_0(z)$, $B_1(z)$ and synthesis filter by $A_0(z)$, $A_1(z)$. Assume that equation (4.6) fulfills the necessary and sufficient requirements for perfect reconstruction.

$$B_0(z)A_0(z)+B_1(z)A_1(z)= C\,z^{-D} \quad (2)$$

By replacing z with –z in equations (1) and (2), the following equations as constraints required for perfect reconstruction.

3 - Design of 9/7 Filter Bank for Image Encryption

This section focuses on novel approach to design 9/7 wavelet filter bank for image encryption application. Initially, the designing of parameterized filterbank is explained in detail and designed filter bank applied to image encryption technique in subsequent section.

A. Design of parameterized 9/7 wavelet filter bank

The set of symmetric linear phase function enforced by group of perfect reconstruction parameters. The resulted parameters applied to different cases of 9/7. By replacing z by –z in equation (1) and (2), we find out below equations to fulfil required perfect reconstruction condition.

In the JPEG2000 standard, 9/7 filters have naturally infinite precision. However, the extended design may be converted into finite precision by relaxing the regularity criterion. (At z = -1, a certain number of zeros is required).

We can design the 9/7 filler from symmetry/linear phase.

$$H_0(z) = p_0 + p_1z^{-1} + p_2z^{-2} + p_3z^{-3} + p_4z^{-4} + p_3z^{-5} + p_2z^{-6} + p_1z^{-7} + p_0z^{-8} \quad (3)$$

$$H_1(z) = q_0 + q_1z^{-1} + q_2z^{-2} + q_3z^{-3} + q_2z^{-4} + q_1z^{-5} + q_0z^{-6} \quad (4)$$

$$G_0(z) = r_0 + r_1z^{-1} + r_2z^{-2} + r_3z^{-3} + r_2z^{-4} + r_1z^{-5} + r_0z^{-6} \quad (5)$$

$$G_1(z) = s_0 + s_1z^{-1} + s_2z^{-2} + s_3z^{-3} + s_4z^{-4} + s_3z^{-5} + s_2z^{-6} + s_1z^{-7} + s_0z^{-8} \quad (6)$$

Using the same procedures as the 5/3 filters and using Perfect reconstruction condition, by simplification of these simultaneous equations, we derived filter equation as below:

$$\frac{p_1}{p_0} = \frac{q_1}{q_0} = k \quad (7)$$

$$P_4 = \frac{2p_3q_2 - 2p_2q_1 + 2p_1q_0 - \frac{q_0}{r_0}}{r_3} \quad (8)$$

$$q_1 = kq_0 \quad (9)$$

$$q_3 = \frac{p_3 q_0 + k p_0 q_2 - k p_2 q_0}{p_0} \quad (10)$$

$$r_1 = -k r_0, r_2 = \frac{q_2 r_0}{q_0}, r_3 = \frac{-q_3 r_0}{q_0}, s_1 = \frac{r_1 s_0}{r_0} \quad (11)$$

$$s_2 = \frac{p_0 r_2 + p_1 r_1 + p_2 r_0 + q_1 s_1 + q_2 s_0}{-q_0} \quad (12)$$

$$s_3 = \frac{s_2 r_1 - s_1 r_2 + s_0 r_3}{r_0} \quad (13)$$

$$s_4 = \frac{2 s_1 r_0 - 2 s_2 r_1 + 2 s_3 r_2 - \frac{r_0}{q_0}}{r_3} \quad (14)$$

When the above-derived relationships are re-entered into perfect reconstruction conditions, it creates a new constraint for filter bank design.

$$s_0 = \frac{-p_0 q_0}{r_0} \quad (15)$$

$$p_3 = f(p_0, p_1, p_{2,} q_0, \mathrm{q}_2, \mathrm{r}_0) \quad (16)$$

These equation gives the generalized 9/7 filter bank as a function of the independent parameter $(p_0, p_1, p_{2,} q_0, \mathrm{q}_2, \mathrm{r}_0)$.

Design Example: We structured our own filter that relies upon six parameters in stack format which are specific parameter. For Illustration purpose, we have added frequency response of G0 and G1 shown in Fig. 3. The key formation of encryption technique shows in Fig. 2.

B. Image Encryption

The image information is decomposed in various frequency bands using wavelet filter bank. In the proposed method, 1-D wavelet transform decomposed image up to level 3. As a result the image is encrypted by approximation sub bands, detail subbands and derived filter coefficients from parameterized filter bank. After operating converse operation, the reconstructed image is just replica of original image.

The designed filter bank is applied upto 3 decomposition level as shown in Fig. 2. For 1st level decomposition, we assumed 3rd code parameterized low pass filter and high pass filter. Similarly, 2nd and 3rd level decomposition for 1st and 2nd code parameterized low and high pass filters are assumed. Proposed filter satisfy the perfect reconstruction property, hence during decryption process, we get perfectly reconstructed original image without any loss of information. In this approach, filter design parameters (p0, p1, p2, q0, q2, r0), approximation subband (CA3) and detail

subband (CD1,CD2,CD3) form the Bookkeeping vector S. Also, we have added level of decomposition and sequence of code as extra key parameter as shown in Fig. 2. This makes the Bookkeeping vector unique, which is a major and important characteristic for encryption process. The correlation between decomposed and input image should be less. The correlation coefficients for various filter parameters are calculated as shown in Table I.

Table 1: Key Generation for Encryption using 9/7 filter bank

Code	**Filter parameters**	**One sided Coefficients**	**Correlation Coefficient**
1	P_0 = - 0.5 P_1 = 0.5 q_0 = - 0.5 r_0 = 0.5	A_0 = [0.5 0.5 0.5] A_1 = [-0.5 -0.5 -0.5 -0.5 -0.5] B_0 = [-0.5 -0.5 -0.5 -0.5 -0.5] B_1 = [-0.5 0.5 -0.5]	0.8115
2	P_0 = 0.025 P_1 = −0.025 q_0 = 0.0125 r_0 = −0.1	A_0 = [0.5 1.0 0.5] A_1 = [-0.25 -0.5 -0.25 -0.5 -0.25] B_0 = [-0.25 0.5 -0.25 0.5 -0.25] B_1 = [-0.5 -1.0 -0.5]	0.8126
3	P_0 = 0.025 P_1 = −0.025 q_0 = 0.0125 r_0 = −0.0875	A_0 = [0.5 1.0 0.5] A_1 = [0.125 0.5 0.25 0.25 0.125] B_0 = [-0.125 0.25 0.25 -0.125] B_1 = [-0.5 -1.0 -0.5]	0.712

Note that, we have kept filter design parameter, level of decomposition, sequence of code, detail and approximation subband coefficient in one stack format which is unique and known to client only. It is ensured that, the original image can be decrypted only when key parameters are known to the client. To enhance the frequency resolution and approximation coefficient, the decomposition process is repeated up to level 5. The encryption time is determined for each decomposition level as tabulated in Table II. The relationship between encryption time at the particular decomposition level is shown in Fig. 4.

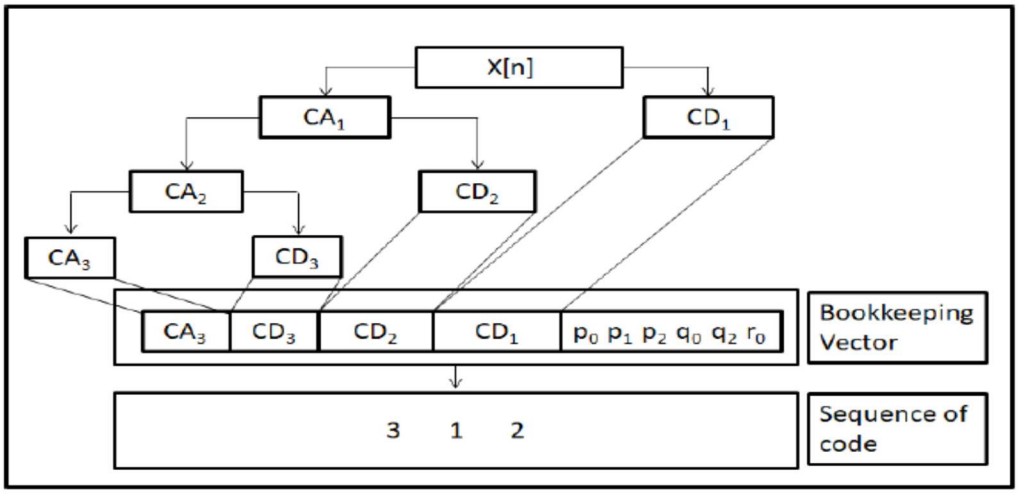

Figure 2. Key structure for image encryption.

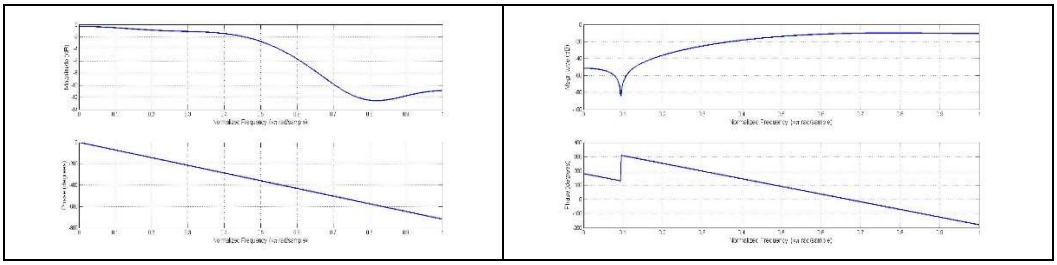

Figure 3. Frequency response of G_0 and G_1 filters

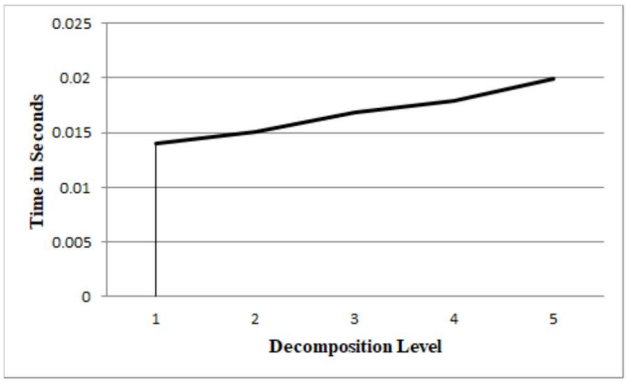

Figure. 4. Relationship between encryption time and decomposed level.

4 - CONCLUSION

This paper proposes a novel technique of image encryption based on parameterized 9/7 wavelet filter bank. The filter design parameters, level of decomposition, approximation and detail subband coefficient act as unique key parameters to enhance security of the system. It has been ensured that, the proposed encryption algorithm give less correlation coefficient value. Therefore,

proposed encryption algorithm is robust and powerful to prevent several cryptography interferences. It is difficult to break and the proposed algorithm has low computing complications.

References

[1] B. Patil, P. Patwardhan, and V. Gadre, "On the design of FIR wavelet filter banks using factorization of a halfband polynomial," IEEE Signal Processing Letters, vol. 15, pp. 485–488, 2008.
[2] M. B. Nagare, B. D. Patil, and R. S. Holambe, "Design of two-dimensional quincunx fir filter banks using eigen filter approach," in 2016 International Conference on Signal and Information Processing (IConSIP), pp. 1–5, Oct 2016.
[3] M. B. Nagare, B. D. Patil, and R. S. Holambe, "A multi directional perfect reconstruction filter bank designed with 2-d eigenfilter approach: Application to ultrasound speckle reduction," Journal of Medical Systems, vol. 41, no. 2, p. 31, 2016.
[4] V. P. Khalane and U. Bhadade, "Image encryption using wavelet transform over finite field," in Proceedings of the 10th International Conference on Security of Information and Networks, SIN '17, (New York, NY, USA), pp. 257–261, ACM, 2017.
[5] A. D. Rahulkar and R. S. Holambe, "Partial iris feature extraction and recognition based on a new combined directional and rotated directional wavelet filter banks," Neurocomputing, vol. 81, pp. 12 – 23, 2012.
[6] A. K. Naik and R. S. Holambe, "Design of low-complexity high performance wavelet filters for image analysis," IEEE Transactions on Image Processing, vol. 22, pp. 1848–1858, May 2013.
[7] B. Patil, P. Patwardhan, and V. Gadre, "Eigenfilter approach to the design of one-dimensional and multidimensional two-channel linear phase FIR perfect reconstruction filter banks," IEEE Transactions on Circuit and Systems Vol-I,, 2008.
[8] M. Sharma, A. P. V., R. B. Pachori, and V. M. Gadre, "A parametrization technique to design joint time frequency optimized discrete-time biorthogonal wavelet bases," Signal Processing, vol. 135, pp. 107 – 120, 2017.
9] A. D. Rahulkar, B. D. Patil, and R. S. Holambe, "A new approach to the design of biorthogonal triplet half-band filter banks using generalized half-band polynomials," Signal, Image and Video Processing, vol. 8, pp. 1451–1457, Nov 2014.
[10] B. Patil, P. Patwardhan, and V. Gadre, "A generalized approach for finite precision 5/3 filter designs," In the Proceedings of National conference on Communications NCC 2007,, pp. 112–115, 2007.
[11] A. D. Rahulkar and R. S. Holambe, Iris Image Recognition- Wavelet Filter-banks Based Iris Feature Extraction Schemes. Springer Briefs in Signal Processing.
[12] A. K. Naik and R. S. Holambe, "New approach to the design of low complexity 9/7 tap wavelet filters with maximum vanishing moments," IEEE Transactions on Image Processing, vol. 23, pp. 5722–5732, Dec 2014.

[13] M. Kumar, D. Mishra, and R. Sharma, “A first approach on an RGB image encryption,” Optics and Lasers in Engineering, vol. 52, pp. 27 –34, 2014.
[14] K. Dezhao and S. Xueju, “Multiple-image encryption based on optical wavelet transform and multichannel fractional Fourier transform,” vol. 57, pp. 343–349, 04 2014.
[15] G. Bhatnagar, Q. J. Wu, and B. Raman, “Discrete fractional wavelet transform and its application to multiple encryption,” Inf. Sci., vol. 223, pp. 297–316, Feb. 2013.
[16] Z. G. M. S. Zhang, X., “Remote-sensing image encryption in hybrid domains,” Optics Communications, vol. 285, p. 1736-1743, 2012.
[17] S. Tedmori and N. Al-Najdawi, “Image cryptographic algorithm based on the haar wavelet transform,” Inf. Sci., vol. 269, pp. 21–34, June 2014.
[18] S. Vijay and N. Sethi, “Comparative image encryption method analysis using new transformed - mapped technique,” in Conference on Advances in Communication and Control Systems CAC2S 2013, 2013.
[19] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, “A visually secure image encryption scheme based on compressive sensing,” Signal Process., vol. 134, pp. 35–51, May 2017.
[20] Y. Luo, M. Du, and J. Liu, “A symmetrical image encryption scheme in wavelet and time domain,” Communications in Nonlinear Science and Numerical Simulation, vol. 20, no. 2, pp. 447–460, 2015.
[21] B. D. Patil and V. M. Gadre, “Novel approaches to the design of one dimensional and multidimensional two channel filter banks,” PhD Thesis, Indian Institute of Technology, Bombay,2008.