Image Cryptography using Parameterized Multiband Eigen Wavelet Filterbank

Vivek P. Khalane[1], Umesh S. Bhadade[2]

[1]Depaertment of Instrumentation Engineering,
Ramrao Adik Institute of Engineering and Technology, Nerul, Navi Mumbai
vivekpkhalane@gmail.com

[2]Department of Information Technology
SSBTs College of Engineering and Technology, Bambhori, Jalgaon,
umeshbhadade@gmail.com

Abstract*: *This paper introduces an eigen filterbank based design for image cryptography. The proposed method consists of designing a wavelet filterbank using eigenfilter based approach and use the designed filterbank for image encryption with new methodology. Design of multilevel two-channel filter bank is extension of an eigenfilter based methodology. This technique is based on designing analysis filter and complementary multilevel synthesis filter. The designed filterbank has various user defined parameters (key) like, number of bands in the filter spectrum, cutoff frequency of individual frequency band and the level of decomposition. Based on the selection of these parameters, we can design a unique filterbank which can be used for the image encryption. At the decryption end, the original image can be reconstructed only if user selected parameters are known. We present few design examples for the illustration purpose. We also give detail of complexity analysis of the entire cryptography system and also present the time analysis. The proposed approach provides a greater number of user parameters as compared to modern methods, which can be used as more secure key. It is also noticed that the encryption time of the proposed methodology is comparable.

***Keywords*: Eigen Filterbanks, Cryptography, Wavelets.**

(Article history: Received: 7th Feb. 2020 and accepted 31st July 2020)

I. Introduction

In the growing technologies of multimedia and networks system, we need to transmit and store large number of images over the internet and wireless networks. In medical, military and legal field, the images are transferred in encrypted format for security purpose. It will be sent only to particular client, hence interpolar cannot see the images. It becomes more important to maintain privacy in data transmission. The image encryption differs from the data encryption techniques. To provide data security to the user, image encryption is very essential to protect from any unauthorized user access. The image encryption differs from the data encryption techniques. the secured encryption algorithm is used to secured the transmitted data [1].

Therefore, it is necessary to design cryptography algorithm or encryption process to ensure the security of given data over communication channel. The commonly used encryption methods fail to give better results in terms of compatibility and encryption quality of images. The text encryption methods frequently create issues in cryptographic systems in terms of incompetence of encryption and decryption, less feasibility and less security [2]–[5]. Therefore, it becomes necessary to investigate cryptography algorithm or encryption process to ensure the security of given data over a communication channel [6]-[9]. With the increasing demand for image encryption, many researchers have been proposed various encryption methods [10]. The commonly used algorithms and methods includes image encryption based on random sequence, image encryption using different image decomposition techniques pixel transformation, and based on key parameter [2], [3], [5]. Most of these techniques involves different mathematical transformation of image pixel. The quality of encryption is decided by the complexity of the mathematical transformation.

The chaos technology is difficult to decrypt. The randomness in the transformation makes the digital image encryption technology more secure. The chaos techniques have been introduced by many researchers to increase the accuracy in the security. In [10], new method has introduced logistic chaotic system for image encryption. In this method, the stream encryption technology has been used as an encryption technology, which specifically combines the chaotic power and cryptography. Although, the encryption techniques cannot meet the commercial requirements in terms of encryption precision, encryption security capability and actual encryption efficiency. It plays an important role in the design of chaotic encryption technology. The iterative encryption method of chaotic cipher is a major breakthrough for chaotic encryption technology [11]. In recent time, many authors have proposed transform domain image encryption. In these approaches image in transform into other domain such that the correlation between the input image and the transformed data is minimal, hence it cannot be decoded easily. The most classical transformation is finite field transforms [12]. This work exploits the modulo arithmetic to transform the data into the random format to achieve high complexity. Along with this, the research has been initiated in the filterbank based encryption [13].

This paper introduces new method of image encryption using eigen filterbank. We extend the wavelet filterbank design using eigenfilter approach to a multiband wavelet. In proposed design, the user facilitates to choose the shape of analysis filter. We design the analysis filter with multiband spectrum, which is defined by the number of bands and the start and stop cuttoff frequencies (user parameters) of each band. The user defined parameters are used as key in encryption & decryption process. The encryption process is performed by means of selecting the user parameters randomly in the order to increase complexity and the decryption process is based on the nature of scrambling and applying the synthesis filterbank (complimentary to analysis filterbank defined by user parameters).

This paper is structured as follows: The review of two channel wavelet filterbank is presented in section II. Section III explains the eigenfilter framework for the wavelet filterbank design and its extension to the multiband wavelet for cryptography application. In Section IV, we proposed method of image cryptography using designed multiband wavelet filterbank. Section V presents experimentation for the proposed method and results discussion and we conclude the paper in section VI.

II. Review of Wavelet Filter bank

In this section, The review of two channel wavelet filterbank is presented [14]–[19].

The intention of analysis filter is to split the input signal spectrum into multiple frequency bands. In contrast to analysis filter, synthesis filter recombines the spitted band into original signal as shown in Figure 1.

$$Y(z) = \frac{1}{2}[A_0(z)S_0(z) + A_1(z)S_1(z)]X(z) + \frac{1}{2}[A_0(z)S_0(-z) + A_1(z)S_1(-z)]X(-z) \quad (1)$$

Y(Z) is a linear combination of *X(Z)* and *X(−Z)* in *Z* domain ($Z=e^{j\omega}$). The $A_0(z)$, $S_0(z)$ are lowpass filters and $A_1(z)$, $S_1(z)$ are highpass filters of analysis & synthesis side. To meet perfect reconstruction (PR) condition, following conditions needs to be satisfied:

$$A_0(z)S_0(z) + A_1(z)S_1(z) = Cz^{-D} \quad (2)$$

$$A_0(-z)S_0(z) + A_1(-z)S_1(z) = 0 \quad (3)$$

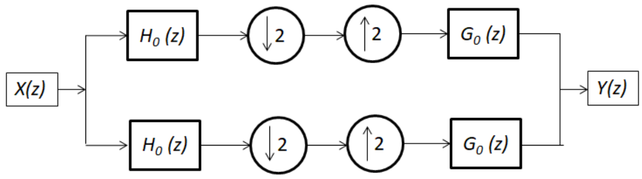

Fig. 1. Structure of Two channel filter bank.

The alias cancellation constraint is expressed in (3). We select C=2 for clarification in (2) where C is scalar constant and D is delay occurred in the filter bank system. The synthesis filter satisfied the requirements for (2) and (3).

$$A_0(z) = S_1(-z) \quad (4)$$

$$A_1(z) = -S_0(-z) \quad (5)$$

The product polynomial in Z-domain is given as,

$$p(z) = A_0(z)S_0(z) \quad (6)$$

It is seen that the perfect reconstruction condition is fulfilled by *P(z)* if the even power terms of z in *P(z)* except origin should be zero. Above relationship shows that, the design of two channel wavelet filterbank is nothing but to design a $A_0(z)$ filter alone. Once $A_0(z)$ filter is designed, (6) gives $S_0(z)$ analysis highpass and synthesis highpass filters are obtained by (4) and (5) to complete a wavelet filtebank. There are multiple approaches available in literature for the design of $H_o(z)$ filter. The most common used approaches are [20]-[23]. In most of the applications, it is desirable to have a filter with linear phase property. The analysis and design of linear-phase wavelet filterbank have received a lot of attention in the literature [24]-[25].

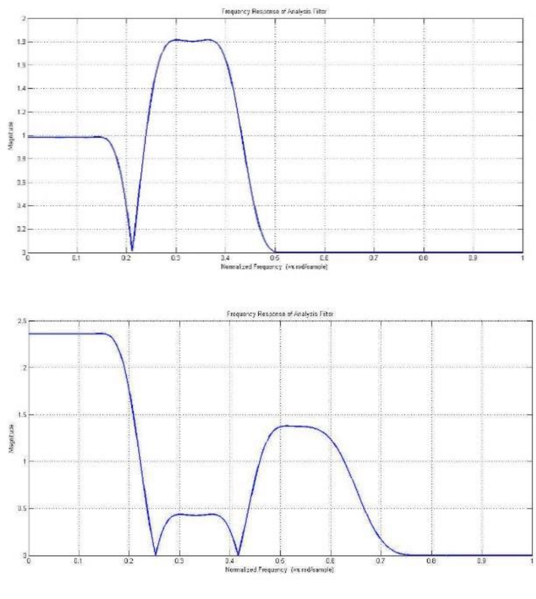

Fig. 2. Frequency spectrum of 2 band and 3 band analysis filter

Among these approaches we focus on the eigen filter based approach as, by vary design of the filter can have user defined parameters and which can be used as a cryptography key.

III. Design of Multiband Wavelet Filter bank using Eigen Filter Approach

A. Review of Eigenfilter approach for filterbank design

The least square error function E is defined as E= $\mathbf{a}^T\mathbf{P}$a where **a** is a real vector& **P** is positive definite matrix. The filter coefficients are related to the element of vector $\bar{\boldsymbol{a}}$ which minimizes **E**. According to Rayleigh principle, minimum eigen vector of P gives eigen vector as solution vector. The trivial solution is avoided by forcing the constraints $\mathbf{a}^T\mathbf{a}$=1. The frequency response of linear phase filter *h[n]* where $-N \le n \le N$ having length of $2N+1$ is given as:

$$H(\omega) = h[0] + \sum_{n=1}^{N} 2.h[n]\cos(n\omega) \qquad (7)$$

This can be written as $H(\omega) = a^T c(\omega)$, where,

$$a = [h[0]\ \ h[1]\ \ h[2]\ \cdots\ h[N-1]\ \ h[N]]^T \qquad (8)$$

$$c(\omega) = [1\ \ 2\cos(\omega)\ \cdots\ 2\cos(N\omega)]^T \qquad (9)$$

This can be written as $H(\omega) = a^T c(\omega)$.

The desired frequency response for 1-D low-pass filter can be given by,

$$D(\omega) = \begin{cases} 1 & 0 \le \omega \le \omega_p \\ 0 & \omega_s \le \omega \le \pi \\ Don't\ Care & \omega_p \le \omega \le \omega_s \end{cases} \qquad (10)$$

Where ω_p and ω_s passband and stopband cutoff frequencies. Therefore, by considering this *D*(*w*), the stopband error can be written as:

$$E_s = \int_{\omega_s}^{\pi} \left[D(\omega) - H(\omega)\right]^2 dw \qquad (11)$$

E_S can be written as:

$$E_S = a^T P_s a \qquad (12)$$

where,

$$P_s = \int_{\omega_s}^{\pi} c(\omega)c(\omega)^T d\omega \qquad (13)$$

P_S is real, symmetric and positive definite matrix.

The passband error given as:

$$E_p = \int_0^{\omega_p} \left[e_p(\omega)\right]^2 d\omega \qquad (14)$$

where, $e_p(\omega)$ is given as:

$$e_p(\omega) = a^T\left[c(0) - c(\omega)\right] \qquad (15)$$

and *Ep* can be written in the form

$$E_p = a^T P_p a \qquad (16)$$

Where,

$$P_P = \int_0^{\omega_p} [c(0) - c(\omega)][c(0) - c(\omega)]^T dw \qquad (17)$$

P_p is real symmetric, positive definite matrix. Total error to be minimized is:

$$F = \alpha E_p + \beta E_s = a^T P_a \qquad (18)$$

Where,

$$P = \alpha P_p + \beta P_s$$

Where, α and β are the weighing constants for passband error and stopband error respectively.

The vector $\bar{\boldsymbol{a}}$ can be used to obtain the optimum filter coefficient. The optimal filter coefficients for analysis low-pass filter are obtained from (8). These coefficients are used in product filter *P(z)* i.e. in (6) to obtain synthesis low pass filter and analysis highpass and synthesis highpass filters are obtained by (4) and (5).

B. Extension of Eigenfilter Method for design of Multiband Filterbank for Cryptography application

As discussed in the previous section, the frequency spectrum of the designed filters is governed by the loss function given in (18). The loss function is divided into the passband and stopband by selection of cuttoff frequency. In other word current design will have single cutoff frequency as a user defined parameter. To use designed filterbank for the

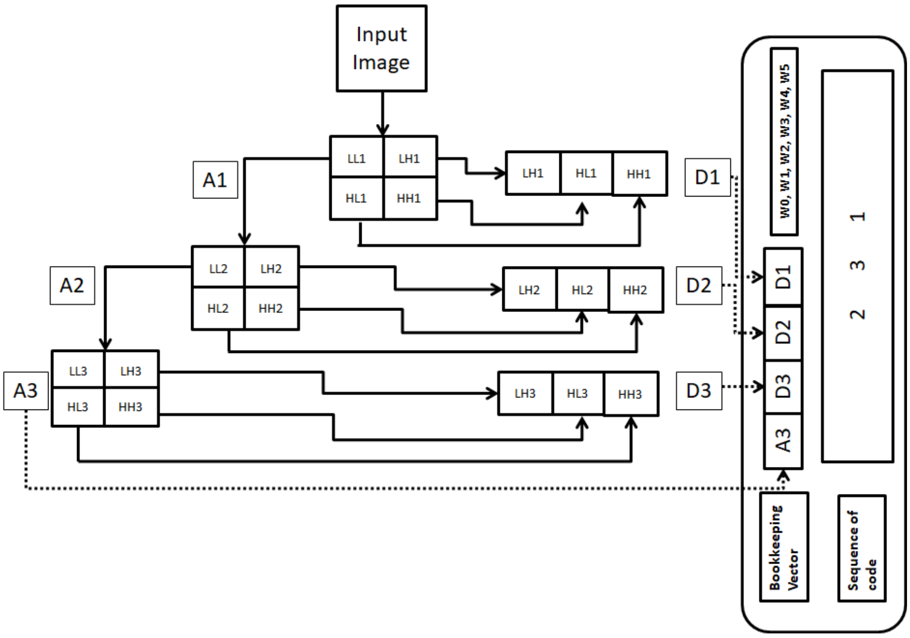

Fig. 3. Proposed image encryption and its key structure

cryptography application we need to have multiple user parameter which will govern the frequency spectrum of the filters. To achieve this, we split the passband and stopband of the filters hence to have a multiband spectrum, wherein each band will have start cutoff and stop cutoff frequency. For two band spectrums of given filter, we will have eight users defined frequency cuttoff and for three band twelve frequency cutoffs. By extending the current eigen filter approach to multiband, we can have a filterbank as a multi variable system and these variables can be used as the keys for cryptography. Passband error for new multiband filter can be defined as the summation of pass band error over different frequency cutoffs. For two band case, pass band error is given as,

$$E_p = \int_{\omega_1}^{\omega_2} [D(\omega) - H(\omega)]^2 d\omega + \int_{\omega_3}^{\omega_4} [D(\omega) - H(\omega)]^2 d\omega \quad (19)$$

Similarly, the stopband error is defined as

$$E_s = \int_{\omega_5}^{\omega_6} [H(\omega)]^2 d\omega + \int_{\omega_7}^{\omega_8} [D(\omega) - H(\omega)]^2 d\omega \quad (20)$$

Rest of the design steps for the filter design remain same as the previous section. For illustration purpose, we have designed the analysis filter with two band and three band spectrums as shown in Figure 2.

IV. Proposed Method for Image Encryption Using Multiband Wavelet Filter Bank

In this section, we present the proposed image encryption algorithm using the filterbank designed in the above section. We decomposed the input image (which is to be encrypted) using the filterbank deigned in previous section in various frequency bands. Wavelet transform can decompose the image up to *N* level for a image of size *2N* × *2N*. For illustration

purpose we decomposed image up to level 3. As a result, the image is encrypted in approximation and detail sub bands at three level and these subbands will be a dependent on the filter coefficients from parameterized filterbank, as mention in above section. At the reconstruction end by operating converse operation, the image is reconstructed which is just replica of original image.

As shown in Figure 3 For 1st level input image decomposition, we use the multiband wavelet filterbank designed in above section with user parameters (cutoff frequencies) e.g. w_0, w_1, w_2, w_3, w_4, w_5 Similarly, 2nd and 3rd level decomposition are performed. In this approach, filter design parameters, approximation subband *A3* and detail subband *D1, D2, D3* form the Bookkeeping vector S. Also, we have added level of decomposition and sequence of code as extra key parameter. This makes the Bookkeeping vector unique, which is a major and important characteristic for encryption process.

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 complexity of key, the decomposition process is repeated up to level 5. The encryption time is determined for each decomposition level.

Steps of the encryption algorithms are,

1. Select number of bands for the analysis filter.

2. Select cutoff frequencies for passband and stopbands.
3. Design a multiband wavelet filterbank.
4. Select level of decomposition.
5. Wavelet decomposition of input image
6. Scrambling of the wavelet band order.
7. Create a book keeping vector as per Figure 3

Steps at the decryption end would be,

1. Design the synthesis filterbank using the cutoff frequencies in bookkeeping vector.
2. Re-order the wavelet bands form bookkeeping vector.
3. Wavelet reconstruction (based on level of decomposition mention in bookkeeping vector).

V. Experimentation and Results

For experimentation purpose, we have applied the encryption algorithms given in the above section on standard Lena image. The size of image we have choose is 256 × 256. The resolution of the image is 8 (bits per pixel) bpp. We have done the experimentation on MATLAB and the system memory is 4GB with Intel core 3 processor. Figure 4 and 6 shows first level wavelet decomposition of the Lena and Cameraman image respectively using two band analysis filter. Similarly, Figure 5 and 7 shows first level wavelet decomposition of the Lena and Cameraman image respectively using three band analysis filter. To enhance the complexity of key (bookkeeping vector), the decomposition process is repeated up to level 5.

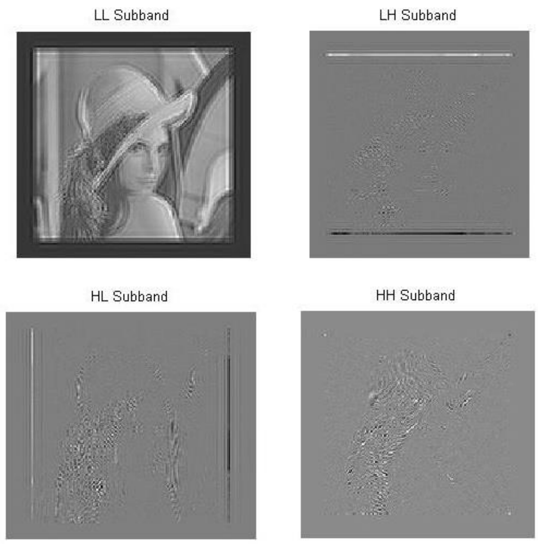

Fig. 4. Wavelet decomposition of Lena image at 1st decomposition level using 2 band analysis wavelet filter

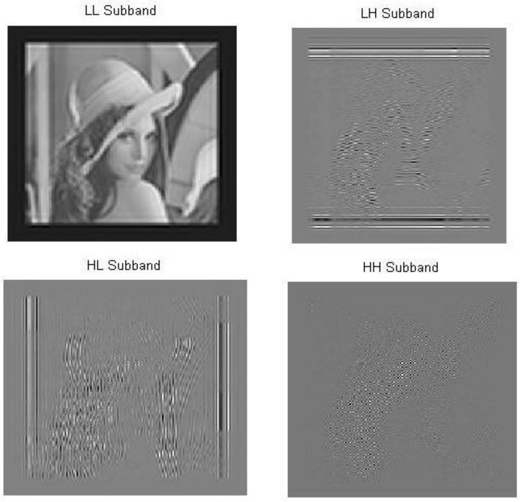

Fig. 5. Wavelet decomposition of Lena image at 1st decomposition level using 3 band analysis wavelet filter

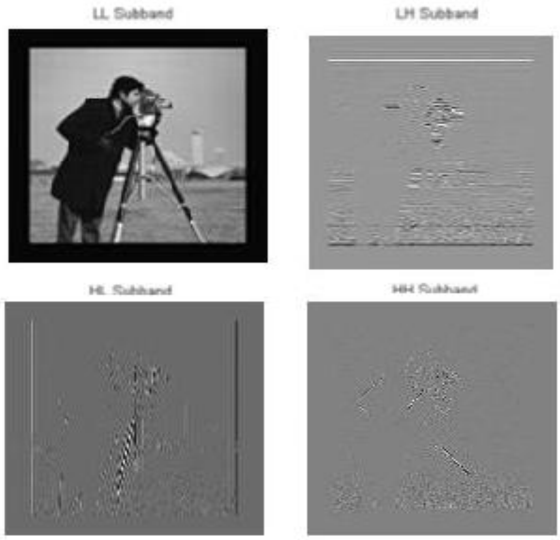

Fig. 6. Wavelet decomposition of Cameraman image at 1st decomposition level using 2 band analysis wavelet filter

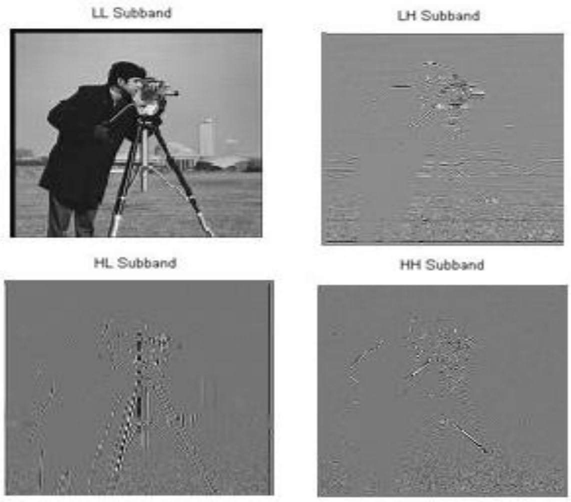

Fig. 7. Wavelet decomposition of Cameraman image at 1stdecomposition level using 3 band analysis wavelet filter

The correlation between decomposed and input image should be less [26]. The encryption time is determined for each decomposition level as tabulated in Table I.

TABLE I.

ENCRYPTION TIME FOR DECOMPOSITIONLEVEL

Level of decomposition	Encryption Time in second
I	0.01401
II	0.01512
III	0.016823
IV	0.0179478
V	0.019945

The correlation coefficients and Information entropy of Lena image and cameraman image for various level of decomposition is given in Table II.

TABLE II.
CORRELATION COEFFICIENT AND INFORMATION ENTROPY FOR A DECOMPOSITION LEVEL

Decomposition Level	Correlation Coefficient		Information Entropy	
	Lena Image	Cameraman Image	Lena Image	Cameraman Image
I	0.8115	0.7945	7.4451	7.0097
II	0.8078	0.7838	6.9832	6.4256
III	0.7165	0.6958	5.8821	5.2121
IV	0.6531	0.6285	3.6712	3.1156
V	0.5936	0.5678	2.5672	2.0526

The expectation is to have low correlation between the input image and the decomposed one at each level. Table II shows that, as we increase the level of decomposition the correlation values and Information entropy decreases which shows better encryption. Time and correlation analysis of proposed algorithm with respect to level of decomposition is displayed in Figure 8. The performance of the proposed algorithm is better than the state of art methods [26-29].

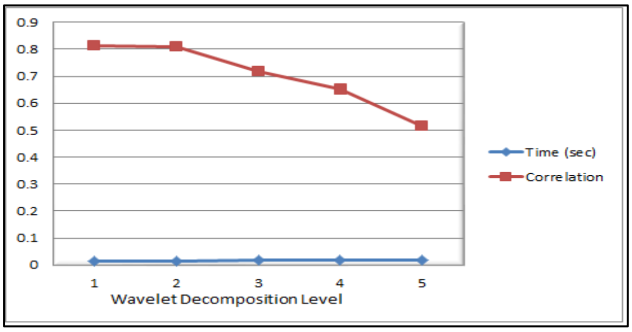

Fig. 8. Time and correlation analysis of proposed algorithm with respect to level of decomposition

TABLE III.
COMPARISON WITH DIFFERENT FILTERBANK ALGORITHMS

Method	Number of user parameters	Encryption time in second	Correlation Coefficient	Information Entropy
FFWT [13]	3	0.01381	0.0123	0.0231
PHFBs [10]	5	0.01265	0.9235	0.9366
DWT [26]	4	0.01545	0.9813	0.9688
Fractional Fourier [30]	2	0.05632	0.0468	0.0659
Fresnel Transform [31]	4	0.02369	0.9821	0.9703
Proposed Method	6	0.01401	0.7945	7.0097

To demonstrate the effectiveness of the proposed design, we have compared the designed filters with existing methods in terms of number of user parameters and encryption time measures. The strength of the encryption algorithm is based on the complexity of unique key, which is defined by the number of user parameters. We have compared proposed algorithm with the similar state of the art algorithms such as, finite field wavelet transform (FFWT) [13], parameterized halfband filterbank (PHFBs) approach [10], discrete wavelet transform (DWT) algorithm [26], Fractional Fourier Transform [30] and Fresnel Transform [31]. Table III shows the comparison of the different algorithms. It has been observed that the proposed algorithm has a greater number of user parameters, hence more complex key for a comparable encryption time.

V. CONCLUSION

This paper proposes a novel technique of image encryption based on eigen filterbank. 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 gives comparable correlation coefficient value while having more number of user selection parameters as a key. More the user selects parameters, the more complex is the cryptosystem to external attacks. 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] V. P. Khalane and U. S. Bhadade, “A review on encryption techniques in signal processing,”

[2] R. M. Redlich and M. A. Nemzow, “Digital information infrastructure and method for security designated data and with granular data stores,” June 18 2013. US Patent 8,468,244.

[3] Z. Han, S. Huang, H. Li, and N. Ren, “Risk assessment of digital library information security: a case study,” The Electronic Library, vol. 34, no. 3, pp. 471–487, 2016.

[4] C. Zhou, Y. Guo, W. Huang, H. Jiang, B. Li, and J. Chen, “Information security defense method of electric power control system based on digital watermark,” in 2016 3rd International Conference on Materials Engineering, Manufacturing Technology and Control, Atlantis Press, 2016.

[5] E. Chisanga and E. K. Ngassam, "Towards a conceptual framework for information security digital divide," in 2017 IST-Africa Week Conference (IST-Africa), pp. 1–8, IEEE, 2017.

[6] T. Caulfield, C. Ioannidis, and D. Pym, "Discrete choice, social interaction, and policy in encryption technology adoption (short paper)," in International Conference on Financial Cryptography and Data Security, pp. 271–279, Springer, 2016.

[7] A. E. A. Elnajjar and S. S. A. Naser, "Des-tutor: An intelligent tutoring system for teaching des information security algorithm," 2017.

[8] C.-H. Huang, S.-C. Chuang, Y.-L. Huang, and J.-L. Wu, "Unseen visible watermarking: a novel methodology for auxiliary information delivery via visual contents," IEEE Transactions on Information Forensics and Security, vol. 4, no. 2, pp. 193–206, 2009.

[9] S.-W. Lee, S.-M. Park, and K.-B. Sim, "Smart door lock systems using encryption technology," Journal of Korean Institute of Intelligent Systems, vol. 27, no. 1, pp. 65–71, 2017.

[10] V. P. Khalane and U. S. Bhadade, "A parameterized halfband filterbank design for image encryption," in 2018 IEEE 13th International Conference on Industrial and Information Systems (ICIIS), pp. 32–35, IEEE, 2018.

[11] J. Matthews and A. Moffat, "Wr 40: coherence or chaos?," Astronomy and Astrophysics, vol. 283, pp. 493–507, 1994.

[12] T. Habutsu, Y. Nishio, I. Sasase, and S. Mori, "A secret key cryptosystem by iterating a chaotic map," in Workshop on the Theory and Application of of Cryptographic Techniques, pp. 127–140, Springer, 1991.

[13] 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, pp. 257–261, ACM, 2017.

[14] M. B. Nagare, B. D. Patil, and R. S. Holambe, "On the design of biorthogonal halfband filterbanks with almost tight rational coefficients," IEEE Transactions on Circuits and Systems II: Express Briefs, pp. 1–1, 2019.

[15] B. D. Patil, P. G. Patwardhan, and V. M. 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.

[16] B. Patil, G. Sharma, P. Patwardhan, and V. Gadre, "A generalized approach for finite precision 5/3 filter design," in In the Proceedings of National conference on Communications NCC 2007, pp. 112–115, 2007.

[17] B. Patil, P. Patwardhan, and V. Gadre, "Filter bank design using a factorization of parameterized half band filters," NCC-08, pp. 404–408, 2008.

[18] 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, 2017.

[19] Nagare M. B., Patil, B.D. & Holambe R..S. Design of two-dimensional PR quincunx filter banks with Euler–Frobenius polynomial and lifting scheme. Sadhana vol. 44, P. 165 June, 2019.

[20] P. P. Vaidyanathan, Multirate Systems and Filter banks. NJ: Englewood Cliffs Prentice-Hall, 1993.

[21] P. P. Vaidyanathan and T. Nguyen, "Eigenfilters: A new approach to least squares FIR filter design and applications including Nyquist filters," IEEE Transaction on Circuits and Systems, vol. 34, no. 1, pp. 11–23, 1987.

[22] 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.

[23] G. Strang and T. Nguyen, Wavelets and Filter Banks. NY: Wellesley-Cambridge, 1996.

[24] A. Tkacenko, P. P. Vaidyanathan, and T. Nguyen, "On the eigenfilter design method and its applications: A tutorial," IEEE Transaction on Circuits and Systems, vol. 50, pp. 497–517, 2003.

[25] S. P. Madhe, B. D. Patil, and R. S. Holambe, "On the design of arbitrary shape two-channel filter bank using eigenfilter approach," Circuits, Systems, and Signal Processing, vol. 36, no. 11, pp. 4441–4452, 2017.

[26] D. Goswami, N. Rahman, J. Biswas, A. Koul, R. L. Tamang, and Bhattacharjee, "A discrete wavelet transform based cryptographic algorithm," IJCSNS, vol. 11, no. 4, p. 178, 2011. Stand. Abbrev., in press.

[27] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[28] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[29] Nagare, M.B., Patil, B.D. & Holambe, R.S. "Design of Two Channel Biorthogonal Filterbanks using Euler Frobenius Polynomial" J Sign Process Syst (2020). https://doi.org/10.1007/s11265-019-01515-z

[30] Hennelly, Bryan M., and John T. Sheridan. "Image encryption and the fractional Fourier transform." *Optik* 114.6 (2003): 251-265.

[31] Luan, Guangyu, et al. "Asymmetric image encryption and authentication based on equal modulus decomposition in the Fresnel transform domain." *IEEE Photonics Journal* 11.1 (2018): 1-7.

Vivek P. Khalane is assistant professor in Instrumentation Engineering department of Ramrao Adik Institute of Technology, Navi Mumbai. He received the B.E. degree in Instrumentation engineering from Kavayitri Bahinabai Chaudhri North Maharashtra University, Jalgaon, India in 2002 and M.E. degree in Instrumentation Engineering from Shri Guru Gobind Singhji Institute of Engineering and Technology, Nanded, India in 2006, His primary research interests are in the areas of signal processing, wavelets and filter banks.

Umesh Bhadade is Professor in the department of Information Technology at the SSBT's College of Engineering and Technology, Bambhori, Jalgaon. He is a fellow of IETE, and Life member of ISTE. His areas of expertise are information security and embedded system

He is Bachelor of Electronics Engineering from Pune University in 1993, Master of Electronics Engineering from Amravati University in 2002 and PhD in Electrical Engineering from M. S. University of Baroda Gujrat in 2012. He has a teaching experience of 25 years.

He is also on examination panel at Gujrat Technological University, Pune University, Mumbai University and Calcutta University. He has published 40+ papers in various National/International Conference/Journal.