International Conference on Recent Innovations in Science, Technology, Management and Environment
Indian Federation of United Nations Associations, New Delhi (India) (ICRISTME-16)
19th June 2016, www.conferenceworld.in ISBN: 978-81-931039-1-3

IMPLEMENTATION OF IMAGE FORGERY DETECTION USING LIFTING SCHEME BASED DYADIC FRAMELETS

Uma B S[1], Shashidhara H R[2], P M Shivakumara Swamy[3]

[1, 2&3] *Dept. of Electronics and Communication, JSSATE, Bengaluru, (India)*

ABSTRACT

Due to availability of low cost manipulation tools, image forgery detection has received enormous attention. There are various forgeries possible on digital images which are impossible to detect through naked eyes such as image splicing, image retouching, copy-move forgery etc,. The manipulations are typically based on resampling using some form of interpolation. This paper provides an overview of methods of image forgery detection followed by the proposed approach. The LDyWT is shown efficient in terms speed and accuracy.

Keywords: ***Digital forensics, resampling, LDyWT, Dyadic framelets, Riesz basis, flipping structure.***

I. INTRODUCTION

From many years, images had been generally accepted as an evidence proof of any depicted event. The rapid growth of image manipulation/processing software and advancement in digital cameras has given rise to wide amount of altered/manipulated images with no obvious traces. As a result, this affects the creditability of digital image presented in court since evidence or any newspaper no longer can be differentiated. Digital image forgery is growing problem in criminal case and public course. Large amount of forgeries could be seen in magazines, fashion industry, legal court, journals, media outlets, images in emails/Facebook timeline etc,. Over a recent past, forgery detection algorithms have emerged to help to restore some trust to digital images. Those algorithms detect such modification underdone. Digital watermarking is a means of checking authenticity in images. However, the major drawback in digital watermarking is the insertion of watermark at the time of recording which would limit this approach in many digital cameras. This paper presents the statistical method to detect forgeries in an image in the absence of digital watermark. These approaches may work on the assumption that digital forgeries may alter the underlying characteristics of an image. Consider an example, the creation of digital forgery that shows Bin Laden shot dead which became viral on internet. Such Photograph can be created by splicing individual images. Another example depicts where an image shows two tables, instead of a single table in original image. Such image is created by copying a block of image and pasting in another block in the same image. In order to obtaina convincingmatch, it is often necessary to resize or rotate portion of an image or an entire image, applying luminance to compensate the brightness in the portion, adding noise to conceal the tampering and resaving the final image with lossy compression. Although thesealterations are invisible to human eye, they may introduce specific correlations in the image. When detected, represents the evidence of forgery. These manipulations require resampling an image on to a new image lattice using some form of interpolation [1]. Resampling is the mathematical technique used to create a new version of an image with different widths/heights in pixels. Consider 1D discretely sampled signal x[n] with m samples. The number of samples can be increased or decreased by factor p/q to n samples in three steps [2]:

1. Up-sample: Create a new signal $x_u[n]$ with pm samples, where $x_u[pn]= x[n]$, n=1,2,…m.
2. Interpolate: Convolve x[n] with low pass filter: $x_f[n]= x_u[n] * h[n]$
3. Down-sample: Pick every q sample, where $x_d[n]=x_f[qn]$, n=1,2…..t. Denote the resampled signal as $y[n]= x_d[n]$.

II. RELATED WORK

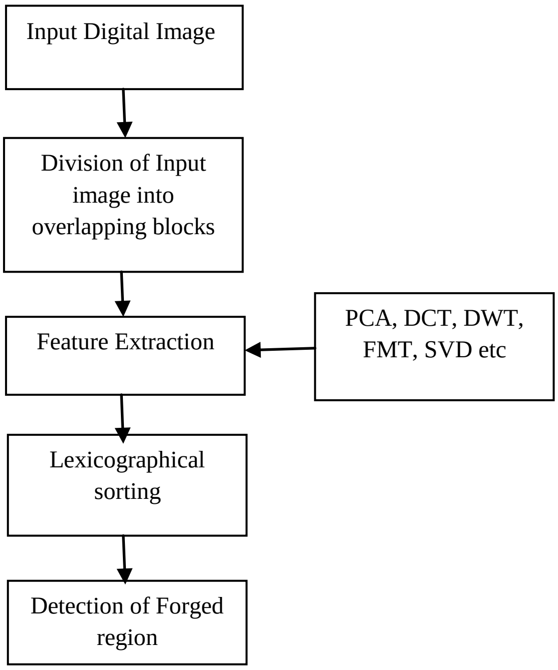

Fig.1. Block Diagram of Image Forgery Detection System

Fridrich et al [3], proposed a method for detecting copy-move forgery using DCT (Discrete Co-sine Transform). In this paper, the digital image is partitioned into 16x16 overlapping blocks. DCT is applied to each block and corresponding DCT filter coefficients are generated for extraction of feature. Then, all the DCT coefficients are sorted in lexical order to detect the forgery. The author proposed robust method for retouching operations on images. However, the authors did do any robustness tests. However, DCT requires additional effort as scaling adds on. DCT functions are fixed and cannot be extended to source anymore and also low performance in binary images. Popsecu et al [4], presented a technique for detecting forged regions by applying PCA (Principle Component Analysis) onsmall fixed size image blocks (16x16 or 32x32). Authors computed eigen distance or hamming distance for each block followed by lexicographical sorting to detect duplicated regions. This method is an efficient and robust technique to detect tampered regions even if the image is compressed or noisy.
X. kang et al [5] proposed the use of SVD to identify the tampered regions in digital image. Authors used SVD (Singular Value Decomposition) for feature extraction and dimension reduction. Then Gi Li et al [6] proposed DWT and SVD to detect the specific artifact. In this method, the authors applied DWT to an image followed by

SVD on fixed size blocks of low frequency components in wavelet subbands to yield a reduced dimension representation. Then the SV vectors are lexicographically sorted and forged image blocks will be close in the sorted list and therefore will be compared during the detection steps. This approach reduced the computation complexity and accurately detects the duplicated regions even though the image is highly compressed. J Huang et al [7] presented a method to detect forgeries based on local image statistical features known as Scale Invariant Features Transform (SIFT). SIFT technique is invariant to change in illumination, rotation and scaling proposed by Hwei-Jenet al [8] with limited rotation angles and Xunyu Pan et al [9] with continuous rotation angles. First, the SIFT discriptors of the image are extracted and matched between each other for any possible forgery. The major disadvantage is the only possible extraction of the key points from peculiar points of the image. Zhang et al [10] proposed a new approach for detecting forgeries using DWT and divided low frequency bands into 4 non overlapping blocks where phase correlation is adopted to compute the spatial offset between the copied regions. Ghorbani et al [11] proposed DWT-DCT (QCD) approach. Authors used DWT to decompose an image into subbands and applied DCT-QCD (Quantization Co-efficient Decomposition) in row vectors to reduce vector length. After lexicographically sorting the row vectors, the shift vector iscomputed. That shift vector is compared with threshold to detect the forgery. Lin et al [12] proposed integrated technique to detect splicing and copy move forgery. Authors converted image into YCbCr color space where DCT is applied for decomposition. SURF technique is used to detect copy move forgery. Cao et al [13] proposed a robust detection algorithm for detecting copy move forgery. Authors used DCT for finding DC co-efficient where each block is represented by circle block.

III. PROPOSED METHODOLOGY

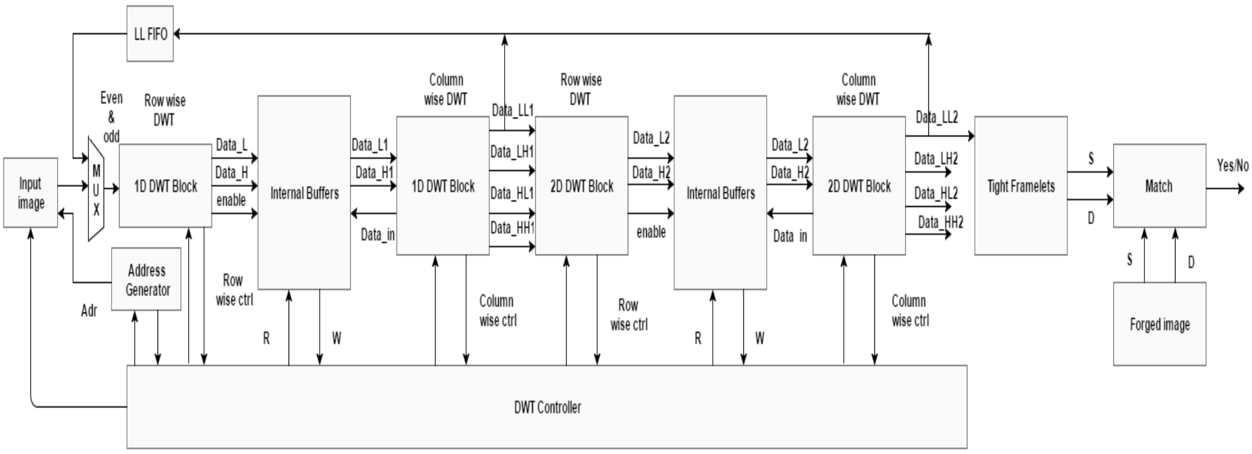

Fig.2. System design of Image Forgery Detection System

3.1 Dyadic Wavelet Transform (DyWT)

Discrete Wavelet Transform (DWT) is a highly flexible and highly efficient method for subband coding of a signal. It decomposes an image into LL LH, HL and HH subbands. The representation of signals in time domain is obtained by digital filtering techniques.

In order to satisfy additional scaling property, dyadic wavelets are used. The term Dyadic wavelet comes from definition of multiresolution analysis performed by DWT.

A large sequence Sj, j in Z, of subspaces of $L^2(R)$ is an approximation of multiresolution and can be expressed as

$$F(u,2^j) = \int_{-\infty}^{+\infty} f(t)\,\frac{1}{\sqrt{2^j}}\varphi\,\frac{(t-u)}{2^j}dt = f * \varphi 2^j(u) \qquad (1)$$

where the family of dyadic wavelets is called framelets in $L^2(R)$ expressed as

$$A \leq \sum_{-\infty}^{+\infty} |\varphi(2^j\, w)|^2 \leq B \qquad (2)$$

If A=B, then frame is called a tight frame. A frame is a family of vectors that represent finite energy signals by its inner products. A Riesz basis is a frame whose vectors are linearly independent. The frames are supposed to be in unit form. The frame is said to be orthonormal if A=B, otherwise it is said to be redundant frames.

3.2 Lifting scheme based Dyadic Wavelet Transform (LDyWT)

The Lifting scheme based DWT requires fewer computations compared to convolution based DWT and hence leads to faster, fully in-place implementation of the wavelet transform attractive to both high throughput and low power applications. The basic idea of lifting scheme is to first compute trivial wavelet by splitting original 1D signal into odd and even sub sequences and then modifying these values using alternate predict and update steps [14].

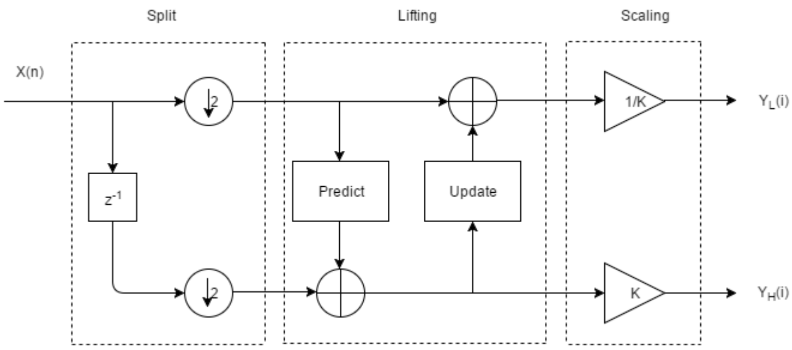

Fig.3. Lifting scheme of 1D DWT

The lifting scheme based wavelet transform basically consists of 3 major steps shown I figure 3:

Split: The original signal x[n] is split into odd x[2i] and even samples x[2i+1].

Predict: The even samples are multiplied by the predict factor and then the result is added to the odd samples to generate detailed coefficients (dj) using high pass filtering.

Update: The detailed coefficients computed by the predict step are multiplied by the update factors and then the results are added to the even samples to get the approximate coefficients using low pass filtering.

When using 9/7 wavelet, there are two predict and update stages.

$$Predict\ P1: d[i] = x_o[i] + a(x_e[i] + x_e[i+1]) \qquad (3)$$

$$Update\ U1: s[i] = x_e[i] + b(d[i-1] + d[i]) \qquad (4)$$

$$Predict\ P2: Y_H[i] = d[i] + c(s[i] + s[i+1]) \qquad (5)$$

$$Update\ U2: Y_L[i] = s[i] + d(Y_H[i-1] + Y_H[i]) \qquad (6)$$

The predict, update and scaling coefficients a, b, c, d and k are derived from 9/7 filter coefficients where,

$a = -1.586134342$

$b = -0.0529801185$

$c = 0.882911076$

$d = -0.443506852$

$k = -1.149604398$

$Y_H[i] = K\ Y_H[i](7)$

$Y_L[i] = \frac{1}{K} Y_L[i](8)$

The DWT is implemented using high and low passfilters and can be expressed as below [14]:

$$p(z) = \begin{pmatrix} 1 & \alpha(1+z-1) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \beta(1+z) & 1 \end{pmatrix} \begin{pmatrix} 1 & \gamma(1+z-1) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \delta(1+z) & 1 \end{pmatrix} \begin{pmatrix} \zeta & 0 \\ 0 & \frac{1}{\zeta} \end{pmatrix} \qquad (9)$$

3.3 Flipping Structure

The accumulation of time delay becomes more from input node to computation node in computation unit. This can be overcome by using flipping structure [15]. Basic idea of flipping structure is to eliminate the multipliers which liebetween input and computation node. Flipping is to multiply the inverse coefficient for an each edge on the feed-forward cutset, which is done through selected multiplier. Then, each computation node can be divided into two adders, one for parallel processing with computation units and another is on accumulative path. The multipliers can also be merged together to reduce the multiplier count.

The schemes employed for DWT depends on computation levels. The path delay for lifting coefficients is 5Tm+8Ta where Tm and Ta are multiplier and adder delays. The main reason for this major delay is because of large stack of multipliers used between inputs and outputs. To overcome this disadvantage, lifting scheme using flipping structure is used. As a result, the delay gets reduced to 3Tm+4Ta. The flipping structure of 2D DWT is shown in fig 4. The processing rate increases when flipping structure is used for mapping in hardware architecture. The delay gets greatly reduced by flipping and shifting the DWT coefficients. In order to optimize more delay and power, pipeline architecture style is proposed.

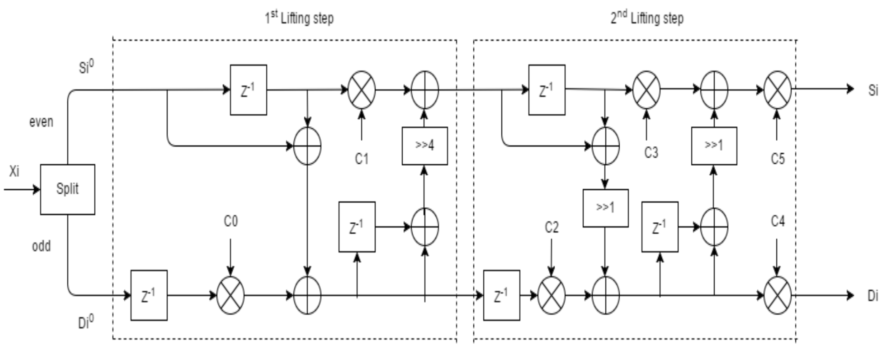

Fig.4. Flipping structure of 2D DWT

Here,

$C0 = {}^{1}/_{\alpha} = -0.6304366206$

$C1 = {}^{1}/_{(\alpha\beta)} = 0.74375024721$

$$C2 = {}^{1}/_{\gamma} = 1.13261689$$

$$C3 = {}^{1}/_{(\gamma\delta)} = 0.638443851$$

$$C4 = {}^{(\alpha\beta\delta)}/_{\zeta} = 2.065244244$$

$$C5 = \alpha\beta\gamma\delta\zeta = 2.42102115$$

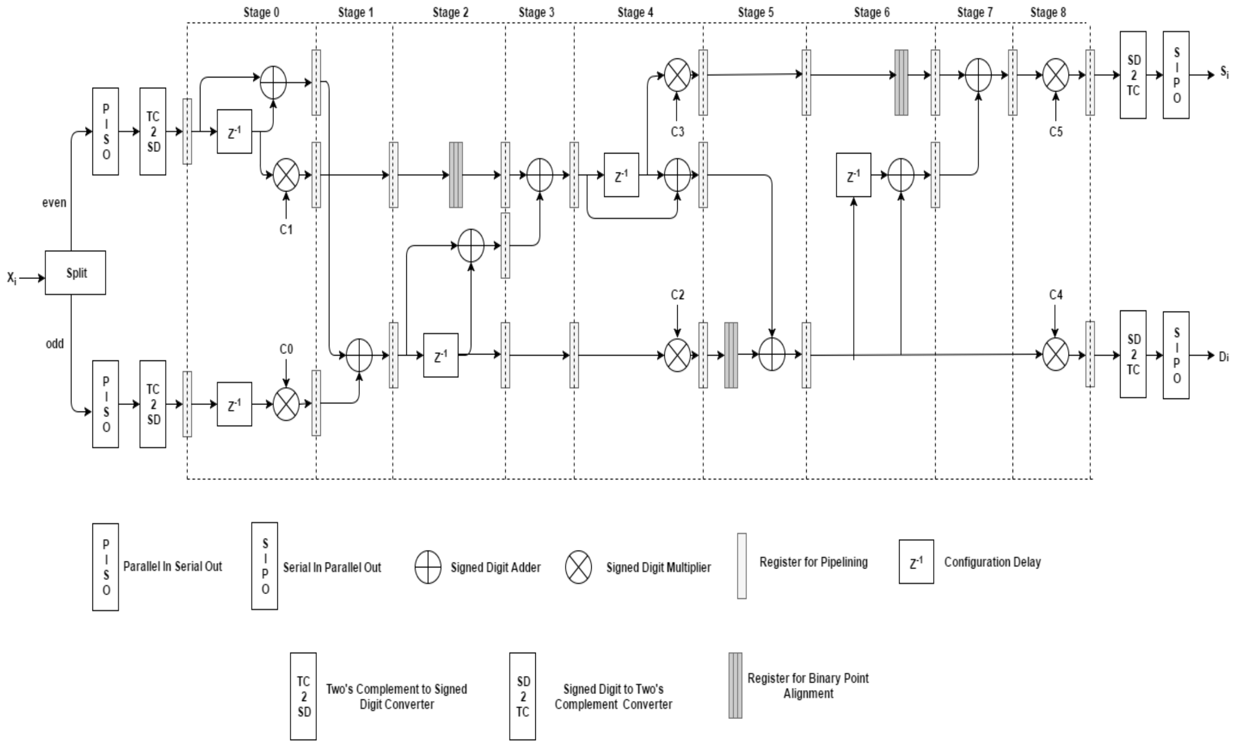

Fig.5. Architecture of 9/7 DWT dataflow

The above figure 5 shows the 9/7 lifting based DyWT using flipping structure. There are 9 low pass components and 7 high pass components. The DyWT architecture is developed based on above equations. During the even clock cycle, half of the registers operate and during odd clock cycle, the other half will operate. The input image converted to bit file arrive serially and passes through the splitter for odd and even values. The obtained odd and even values are predicted and updated by low and high pass filters. The final output is the segmented and de-segmented values of the input image.

Algorithm

$$\textbf{Step 1}: Start$$

$$\textbf{Step 2}: For\ input\ image\ x[n], Compute\ d = x_{odd} - P(x_{even})$$

$$and\ s = x_{even} + U(d)$$

$$representing\ P\ \&\ U\ in\ matrix,$$

$$\begin{bmatrix} x_{even(z)} \\ d(z) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ t(z) & 1 \end{bmatrix} \begin{bmatrix} x_{even(z)} \\ x_{odd(z)} \end{bmatrix}$$

$$\begin{bmatrix} s(z) \\ d(z) \end{bmatrix} = \begin{bmatrix} 1 & s(z) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x_{even(z)} \\ d(z) \end{bmatrix}$$

$$\textbf{Step 3}: For\ 2D\ lifting\ scheme, compute\ approximate\ s(z)$$

 ISBN: 978-81-931039-1-3

$$\text{and detail coefficients } d(z)$$

$$\begin{bmatrix} s(z) \\ d(z) \end{bmatrix} = \begin{bmatrix} k & 0 \\ 0 & 1/_k \end{bmatrix} \prod_{i=1}^{2} \begin{bmatrix} 1 & S_i(z) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ t_i(z) & 1 \end{bmatrix} \begin{bmatrix} x_{even(z)} \\ x_{odd(z)} \end{bmatrix}$$

$$\textbf{Step 4}: \text{Compute DWT filter coefficients},$$

$$E(z) = \begin{bmatrix} h_e(z) & h_o(z) \\ g_e(z) & g_0(z) \end{bmatrix} = \begin{bmatrix} k & 0 \\ 0 & 1/_k \end{bmatrix} \prod_{i=1}^{2} \begin{bmatrix} 1 & S_i(z) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ t_i(z) & 1 \end{bmatrix} \begin{bmatrix} x_{even(z)} \\ x_{odd(z)} \end{bmatrix}$$

$$h_e \text{ and } h_o \rightarrow \text{even and odd components of LPF},$$

$$g_e \text{ and } g_o \rightarrow \text{even and odd components of HPF},$$

$$s_i(z) \text{ and } d_i(Z) \rightarrow \text{filter coefficients}$$

$$\textbf{Step 5}: if\,(S(z)_{input\ image} == S(z)_{forged\ image})$$

$$m = 1;$$

$$else$$

$$m = 0;$$

$$\textbf{Step 6}: end$$

IV. RESULTS

The simulation results using Modelsim is shown below:

The fig.6 shows the segmented and de-segmented values of a decomposed image using lifting scheme based DWT. The split data is given in two's complement. The incoming data is first serialized and converted into signed digits. The serial signed digits are then passed into the DWT, which is partitioned into 9 pipeline stages. After the final stage, the DWT transformed data is converted back into two's complement giving segmented and de-segmented values.

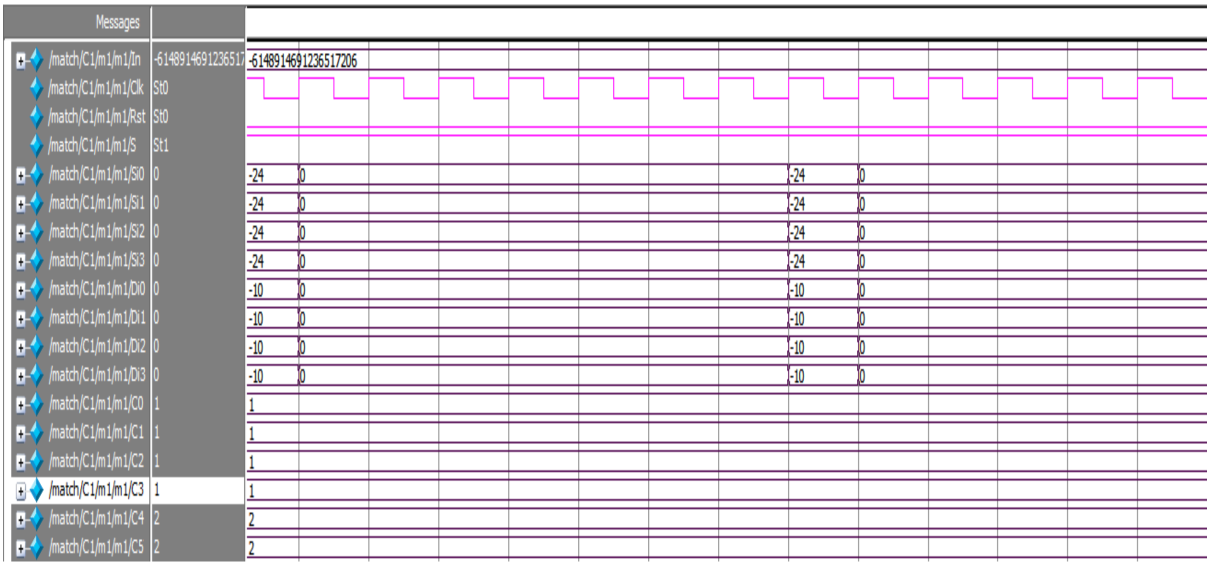

Fig.6. Simulation result of DWT module

The fig.7 shows the simulated output of symmetry checker. The de-segmented values are then passed to tight frame generator for feature extraction.

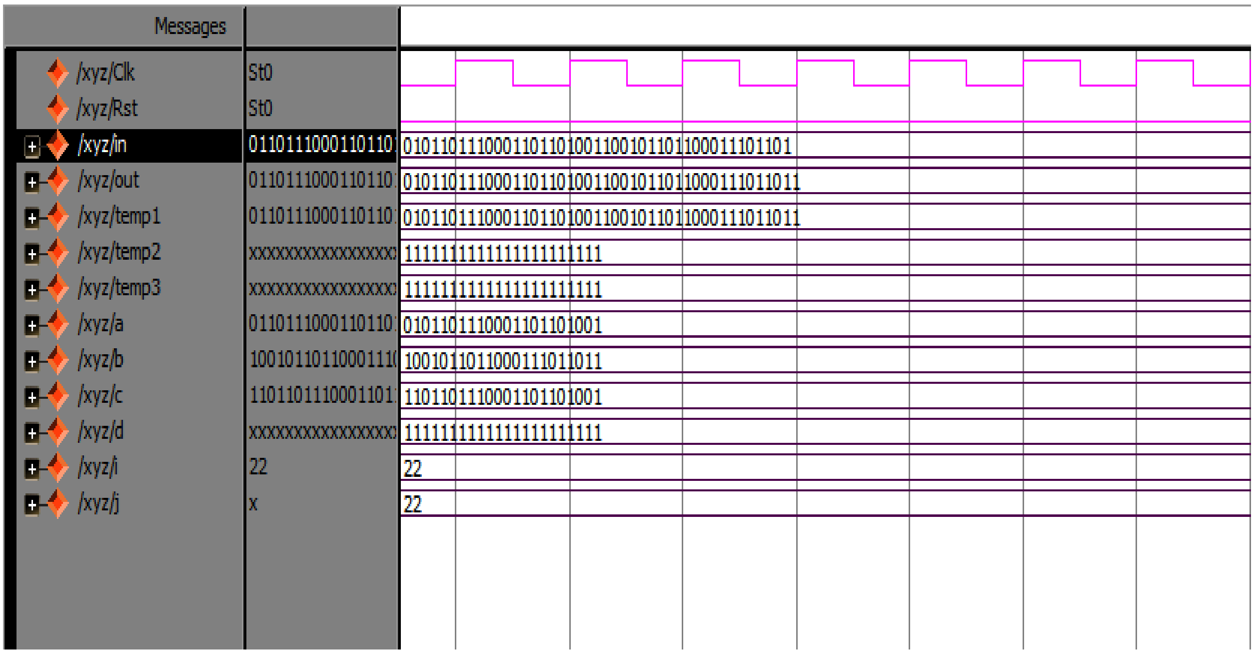

Fig.7 Simulation result of Tight Frame generator

The fig. 8 shows detection of forgery in an image. Here original and altered image is converted into bit map files followed by decomposition using DWT and extraction of feature using symmtery checker. The extracted fetures of both the images are then compared.

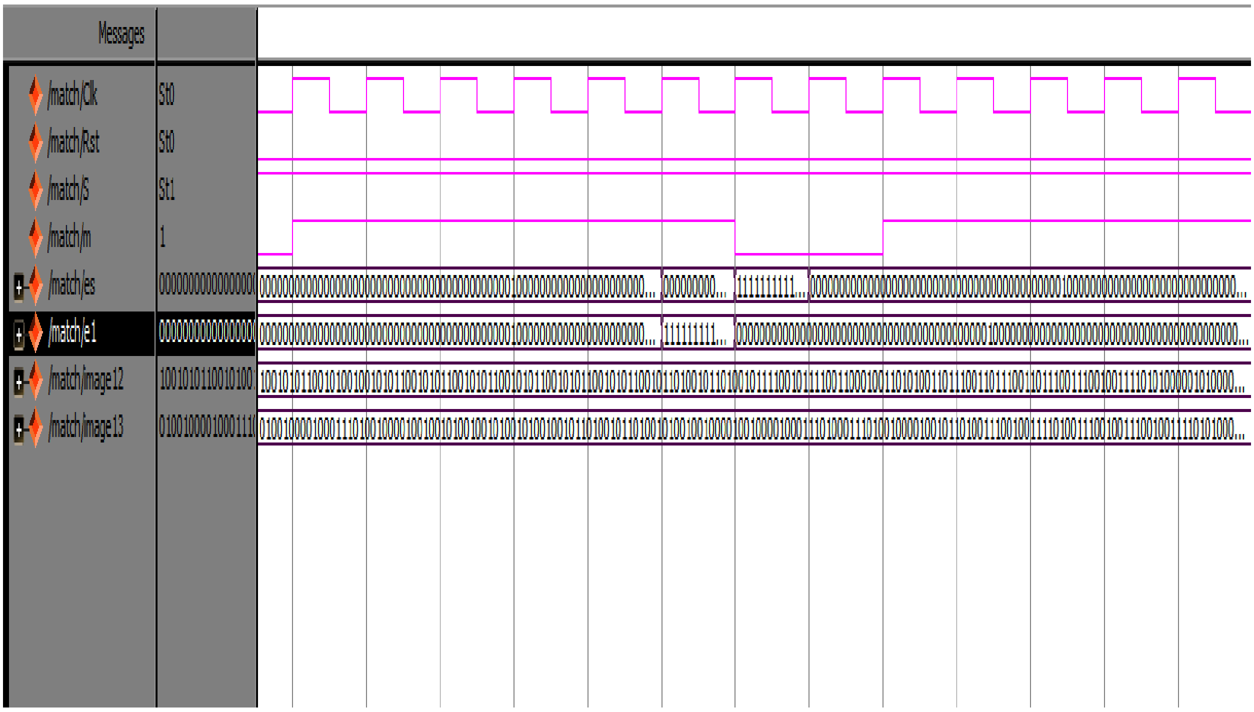

Fig.8. Simulation result showing forgery detection

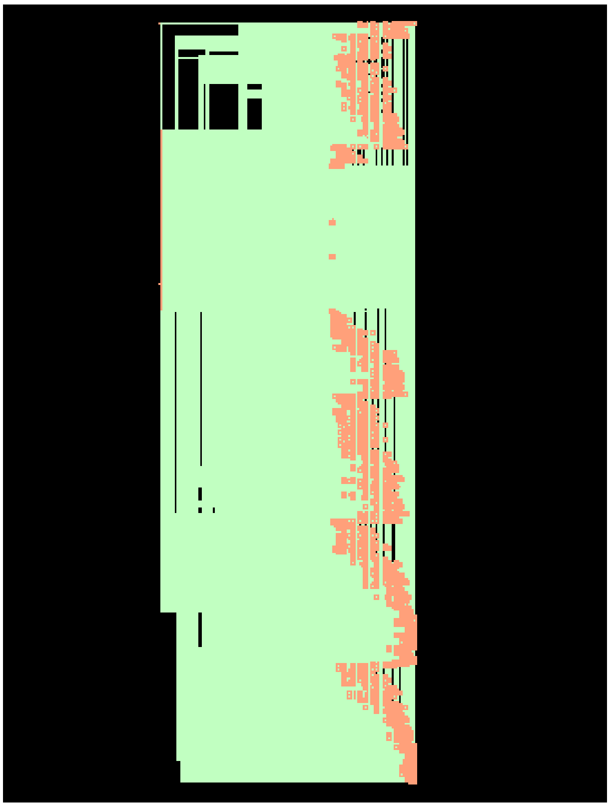

Fig.9. RTL schematic of top level module

The RTL schematic of top level module is shown in fig 9 and the generated synthesis report with associated gate count is shown in table I and II

Table I. Synthesis Report

Cell area	2112nm^2
Total cells	186477
Delay	0.210ns
Power	42.31mW

Table II. Gate Count

Type	Instances	Area
Sequential	114881	1.711mm^2
Inverter	7128	15.08um^2
Unresolved	20	0.00
Logic	64468	385.5um^2

V. CONCLUSION

This paper presents the problem of image forgery detection. To detect the forgeries under the modifications, we proposed to use lifting based DWT followed by tight frames generator for feature extraction. Our experimental results show that we can detect forgery accurately even if the image has undergone rotation, scaling or compression. The system functionality is successfully verified through hardware simulation achieving great optimization in power, area and delay constraints.

REFERENCES

[1] Saba Mushtaq and AjazHussain Mir, "Digital Image Forgeries and Passive Image Authentication Techniques: A survey". International Journal of Science and Technology, vol.73, 2014, pp.15-32

[2] Baba Mahdian and StanislavSaic, "Detection of Resampling Supplemented with Noise Inconsistencies Analysis for Image Forensics", IEEE explore, june 2008

[3] J.Fridrich, D.Soukal and J.Lukas, "Detection of Copy-move forgery in gigital images", in Proceedings of the Digital Forensics Research Laboratory, Aug 2003, pp.5-8

[4] A.C.Popsecu and H.Farid, "Exposing Digital Forgeries by detecting duplicated image regions", Dept. of Computer Science, Dartmouth College, Tech Rep TR2004-515, 2004

[5] X.kang and S.Wei, "Identifying tampered regions using Singular Value Decomposition on digital image forensics", in International Conference on Computer Science and Software Engineering, 2008, Vol.3, pp.926-30

[6] G. H. Li, Q. Wu, D. Tu, and S. J. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWTand SVD," in Proceedings of IEEE International Conference on Multimedia and Expo, Beijing, Jul. 2007, pp.1750_3.

[7] W. Q. Luo, J. W. Huang, and G. P. Qiu, "Robust detection of region-duplication forgery in digital image," in Proceedings of18th ICPR, Vol. 5, pp. 746_9, 2006

[8] Hwei Jen. Lin, C.W. Wang and Y.T. Kao, "Exposing Digital forgeries by detecting duplicated image regions", Dept. Computer Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004

[9] X. Pan, and S. Lyu, "Region duplication detection using image feature matching", IEEE Trans.Inf.Foren.Sec., Vol 5, no. 4, pp. 857_67, Dec. 2010

[10] J. Zhang, Z. Feng, and Y. Su, "A new approach for detecting copy-move forgery in digital images", in IEEE International Conference on Communication Systems, China, 2008, pp.362_6.

[11] M.Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy-move forgery detection", in 18th IEEE International Conference on Systems, Signals and Image Processing (IWSSIP), pp. 1-4, 2011

[12] Z. Lin et al., "Fast automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis", Pattern Recogn., Vol. 42, pp. 2492_250, 2009

[13] Yanjun Cao, T. Gao and Qunting Yang, "A robust detection algorithm for copy-move forgery in digital images", Forensic Int. Vol. 214, pp. 33_43, 2012

[14] M. Nagabushanam, S. Ramachandran, P. Kumar, "FPGA Implementation of 1D and 2D DWT Architecture using Modified Lifting Scheme", WSEAS Transactions on Signal processing, Issue 4, Volume 9, October 2013

[15] S. Senthilkumar, Dr. R. Radhakrishnan, M. Gokula Krishnan, "A Survey on VLSI Architectures of Lifting Based 2D Discrete Wavelet Transform", International Journal of Advanced Computer Technology (IJACT), VOL 3, no. 6, 2010