# Wavelet Based Compression and Key Hashing Encryption of Image on FPGA

[I]Rahul Unnikrishnan, [II]Umesh A C
[I]Dept. of Electronics, Rajiv Gandhi Institute of Technology (RIT), Kottayam, Kerala, India
[II]Dept. of Electronics, GEC Wayanad, Wayanad, Kerala, India

## Abstract

*Digital images are important sort of information source. In many applications like medical imaging, remote sensing encryption of the compressed image is vital in hiding the data. Wavelet based image compression technique can reduce the storage capacity and thereby communication cost. Secured Hash Algorithm (SHA-1) is used for key hashing encryption. Implementing this in FPGA can achieve a greater performance, reduced cost and reconfigurable architecture of FPGA adds up the advantage. SHA-1 is implemented in Verilog HDL and compression of image is done using Xilinx System generator.*

## Keywords

*Wavelet based compression, SHA-1, FPGA, Verilog HDL, and Xilinx System Generator*

## I. Introduction

A digital image is a 2-D matrix which is the combination of information and redundancy. Compression of the image is that keeping the information portion of data as it is and removing the redundant part of data as much as possible.

Compression is useful as it reduces the storage space that is the usage of expensive resources, such as memory (hard disks) and also it reduces the required bandwidth while transferring the image. On the other side compression of image will result in distortion and also it requires additional computational resources at both transmitting and receiving end.

The objective of image compression is to reduce redundancy of the image data in order to store or transmit data in an efficient form. Image compression can be categorized into lossy and lossless compression. The lossless compression are widely used in medical imaging, preserving an artistic image etc. The lossy compression technique is used where required a high compression ratio like remote sensing, satellite communication etc.

Removal or reduction in data is typically achieved by transforming the original data from one form or representation to another. The popular techniques used in the redundancy reduction step are prediction of the data samples using some model, transformation of the original data from spatial domain such as Discrete Cosine Transform (DCT)[1], [2] decomposition of the original data set into different sub-bands such as Discrete Wavelet Transform (DWT)[3]-[8].

Encrypted images are widely used in internet communication, multimedia systems, tele-medicine, medical imaging and military communication. Although there are many conventional encryption schemes like AES, RSA, DES can be used for the image encryption SHA [9], [10] is more suitable for the encryption. The secured Hash algorithm is introduced a keyed hash function to generate a 128-bit hash value so that the scheme could be used to encrypt and authenticate. The hashvalue of the key is one way irreversible hash function which is used to encrypt the image is very secure. Creating specialized hardware would greatly reduce the time consumed for these processes. Also, the use of predominant algorithms would greatly increase the speed and effectiveness of the overall process. For this reason, reconfigurable hardware implementation of the image compression-encryption is proposed. Field Programmable Gate Array (FPGA) technology which supports reconfigurable computing technology has become a viable target for the implementation of algorithms suited to image processing applications. The design has been developed using System Generator (XSG) of Xilinx ISE design tool configured with MATLAB that integrates Xilinx Block-set and Matlab Simulink environment.

This paper is organized as follows. A brief description of proposed system is given in Section I. Section II, provides a detailed portrayal of the DWT. Secured Hash Algorithm. (SHA-1) is presented in Section III. Simulation and results are addressed in Section IV. Finally, conclusions are drawn in Section V.

## II. Proposed image compression-encryption model

The proposed image compression is done by using Cohen-Daubechies-Feauveau Wavelet, which is a bi-orthogonal wavelet. Image is a 2-D arrangement of coefficients which represents the brightness of that particular point. The image characteristics are two types the smooth variation in color that is low frequency component and the sharp variations; high frequency component. The separation of these smooth and detail components is done using octave-band decomposition with CDF 9/7 for lossy compression. This separation is obtained by the filtering by low pass and high pass filters called analysis filter bank.

After the compression the image is encrypted using a 160 bit hashing function, the proposed system uses a SHA-1 algorithm to generate the hash function. The security nature of the SHA can utilize for the encryption of image. Fig.1 illustrates the proposed system.

## III. Discrete Wavelet Transform

The discrete wavelet transform is a promising approach for the image compression. By using octave-band decomposition the 2-D digital image can be decomposed into approximation and detail coefficients [11]-[15]. A 9/7 Cohen-Daubechies Feauveau Wavelet is used for the lossy compression of image.

© IJARET All Rights Reserved

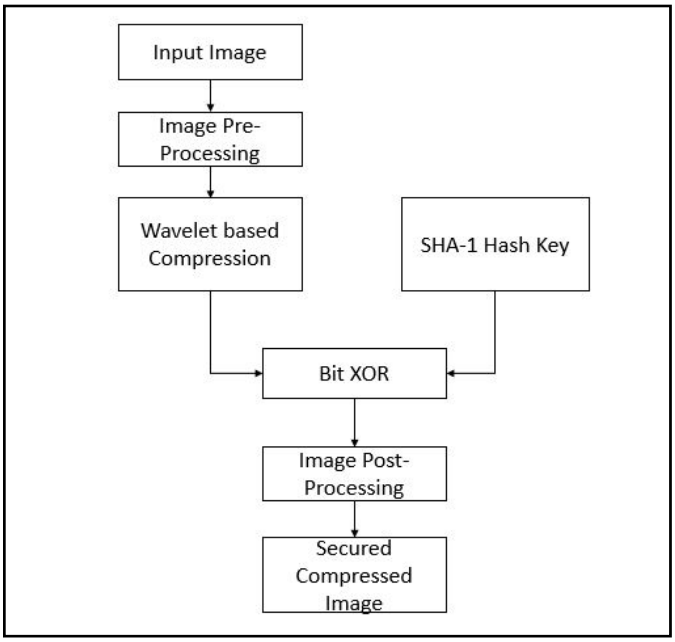

Fig.1: Proposed image compression-encryption model

The decomposition of the image is shown in the Fig. 2. A 9/7 CDF analysis filters are arranged and after the first decomposition four sub bands are obtained LL1,HL1, LH1, HH1. The LL1 sub band has the low frequency smooth coefficients and all other three sub bands will have the high frequency detail coefficients. LL1 is the coarser approximation which will be same as that of the input image.This can be further decomposed into sub bands.

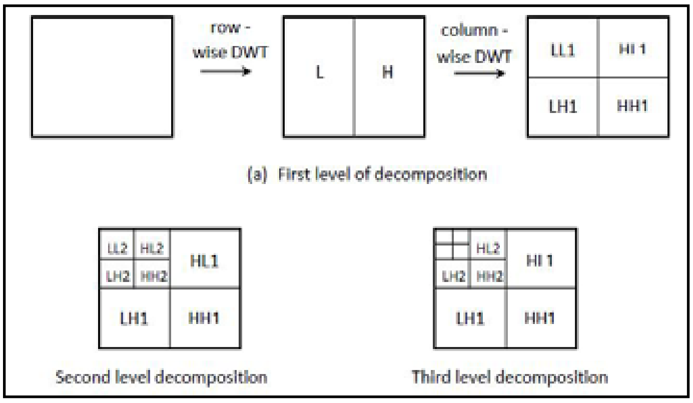

Fig.2: Row column computation of 2D-DWT

## IV. Design of Sub-band Filters

The filters are designed in Simulink using Xilinx block set and system generator.Filter coefficients entered using FDA tool box. The coefficients of the low pass and high pass filters are carefully chosen for the specified application.For CDF 9/7 wavelet, low pass filter coefficients are considered as shown in Table I and high pass filter coefficients are shown in Table II.

Table I : Low Pass Filter Coefficients

| Index No: | Coefficients |
|---|---|
| K=0 | 0.029 |
| K=±1 | 0.2666 |
| K=±2 | -0.0782 |
| K=±3 | -0.0168 |
| K=±4 | 0.0267 |

Table II : High Pass Filter Coefficients

| Index No: | Coefficients |
|---|---|
| K=0 | 1.1150 |
| K=±1 | -0.5912 |
| K=±2 | -0.0575 |
| K=±3 | 0.0912 |

## V. Secured Hash Algorithm (SHA-1)

The input of SHA is a message which is no longer than $2^{64}$ bit, and it can generate a 160 bit message abstract. If a message is no longer than bit, it needs to be added zeroes to make the message become a $2^{64}$bit one. And if a message longer than $2^{64}$ bit, it need to be separated into several groups. Every group contains $2^{64}$bit. Then the message groups will be converted into message abstract groups by SHA algorithm. When message abstract is generated, five 32 bit initial values A, B, C, D, E will be used.

$A = 0x67452301$

$B = 0xefcdab89$

$C = 0x98badcfe$

$D = 0x10325476$

$E = 0xc3d2e1f0$

Every time SHA-1 operate, non-linear function $F_t$, constant $W_t$and $K_t$are different if t is different value. According to parameter t, the non-linear function $F_t$is

$F_t(x, y, z) = (x.y) + (\overline{x}.\ z) \qquad t = 0\ to\ 19$

$F_t(x, y, z) = x \oplus y \oplus z \qquad t = 20\ to\ 39$

$F_t(x, y, z) = (x.y) + (x.z) + (y.z) \qquad t = 40\ to\ 59$

$F_t(x, y, z) = x \oplus y \oplus z \qquad t = 60\ to\ 79$

Constant $K_t$is different according to parameter t.

$Kt \ = 0x5a82799 \quad (t \ = 0\ to\ 19)$

$Kt \ = 0x6ed9eba1 \quad (t \ = 20\ to\ 39)$

$Kt \ = 0x8f1bbcdc \quad (t \ = 40\ to\ 59)$

$Kt \ = 0xca62c1d6 \quad (t \ = 60\ to\ 79)$

The message m should be separated into groups. Every group contains 512 bit. Then every group needs to be separated into 16 sub-groups $W_t$t which contains 32 bit in everyone. The basic diagram of the SHA is shown in the Fig. 3.

$Wt \ = \ Mt \qquad t = 0\ to\ 15$

$Wt = \ M_{t-3} \oplus M_{t-8} \oplus M_{t-14} \oplus M_{t-16} << 1\ t = 16\ t0\ 79$

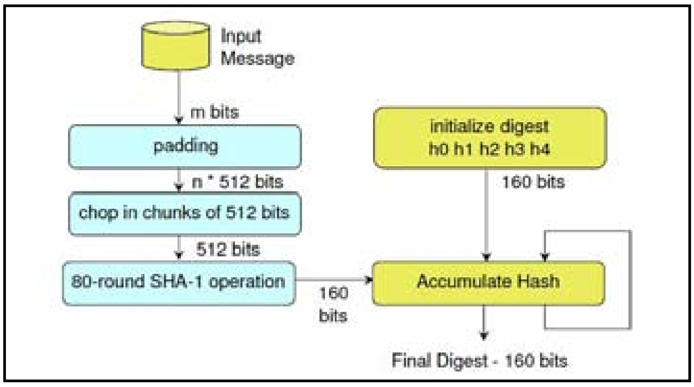

Fig.3: Basic block diagram of SHA-1

## VI. Simulation Studies

The design has been developed using System Generator (XSG) of Xilinx ISE design tool configured with MATLAB that integrates Xilinx Block set and Mat lab Simulink environment which supports Virtex 6 FPGA. Using MATLAB Simulink to assist the system generator verification relies on co-simulating the two environments. The co-simulation interface must provide sufficient capabilities and reasonable simulation speeds. System generator automatically specifies the details of FPGA with the help of Xilinx DSP block set for Simulink, then FPGA has been programmed.

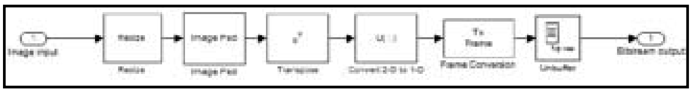

Fig.4: Image pre-processing block

The image compression is done in the MATLAB Simulink with Xilinx system generator. A 512×512 image is given as input. Image is pre-processed after DWT compression as shown in the Fig. 4. After preprocessing the image is converted to a serial bit stream and then, the image bit stream data have been applied as inputs to system generator DWT building blocks of analysis filters (low-pass and high-pass) through Gateway In. These filters separate each input bit stream into approximation and detail coefficients. These coefficients have been obtained by convolving the input values with the low pass filter for approximation and with the high-pass filter for detail and results into a collection of sub-bands with smaller bandwidths and slower sample rates. The design of the DWT filter banks are shown in the Fig. 5. After the compression using the filter banks the serial bit stream of image is bit XOR ed by using the key hash generated by SHA. This algorithm is implemented in Verilog HDL in Xilinx ISE. After the encryption the bit stream is converted back to 2D matrix and this is done by using the post-processing block as shown in Fig. 6.

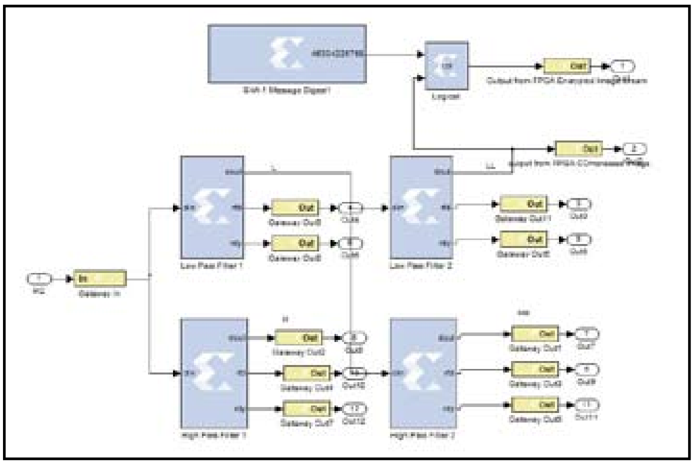

Fig.5: DWT Filter Design

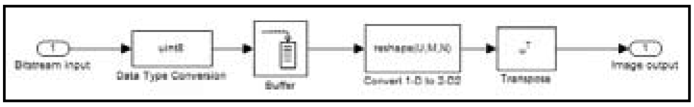

Fig.6: Image post-processing block

### A. Simulation Results

The simulation waveform of the SHA-1 algorithm is shown in the Fig. 7, the idata indicates the input message and hash indicates the generated message digest. The key generated by this is taken and used for encryption of the serial-stream. The input test image is a 512×512 which is converted to a 128×128 grayscale image as shown in Fig. 8.

Fig. 9 shows the image after encryption that is the bit XOR-ed result of image with the SHA message digest.

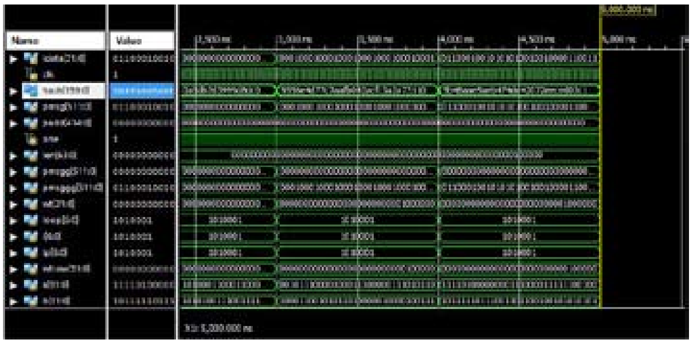

Fig.7: SHA-1 output waveform

### B. Histogram Analysis

The encrypted image should be entirely different from the input image to ensure the security. Histogram analysis is a statistical method to plot the characteristics of the image. This analysis clarifies how pixels in an image are distributed by plotting the number of pixels at each intensity level. Fig. 10 shows histogram analysis of the input test image. The histogram of the plain input test image contains large sharp rises followed by sharp declines. The encrypted image histogram shown in Fig. 11 is quite different from the input test image.

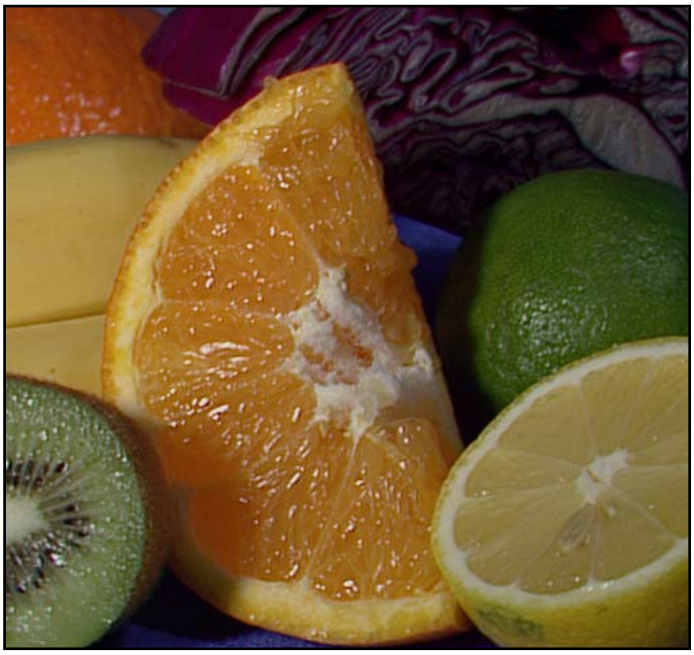

Fig. 8: Input test image fruits.jpg

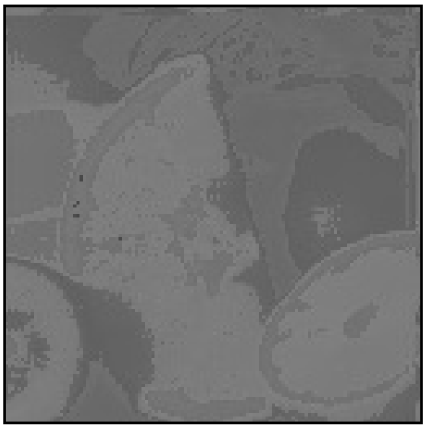

Fig. 9: Encrypted image

## VII. Conclusion

Image Compression is very important in reducing the storage capacity and also to reduce the bandwidth requirement while transfer of image. This work enables a DWT based image compression in FPGA, the image compression part is done in the Simulink using Xilinx System Generator and also to add up the security a key hashing encryption is added. This algorithm is implemented in Verilog HDL using Xilinx ISE and the message digest generated is used for encryption.Based on the histogram analysis it is clear that the encrypted image is entirely different from the test input image. This FPGA based image compression can be extend to compressing the video and this can be implemented in the area's where the software solution for compression-encryption are not effective.

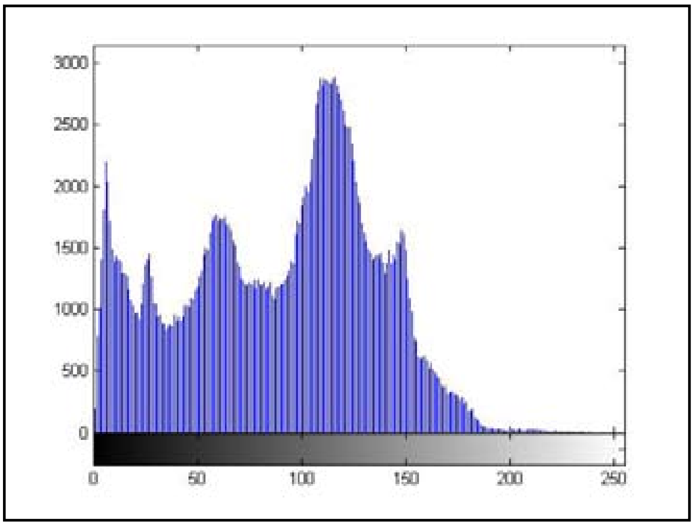

Fig.10: Histogram of input test image

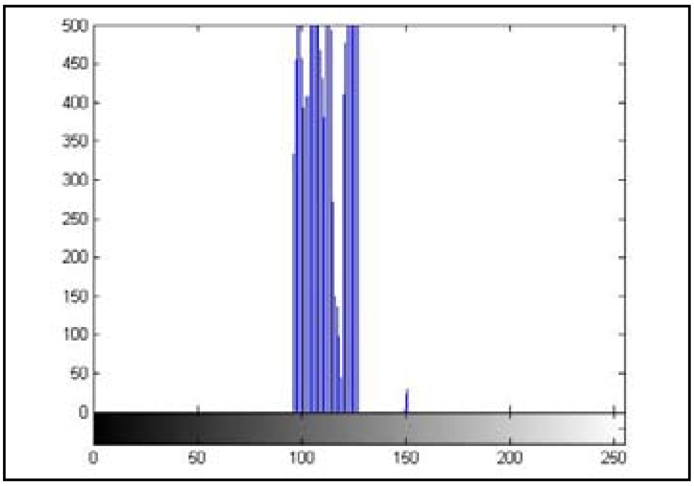

Fig.11: Histogram of encrypted image

## References

[1]. *Chang Sun & En-Hui Yang, "An Efficient DCT-Based Image Compression System Based on Laplacian Transparent Composite Model", IEEE Transaction on Image Processing, VOL 24, No: 3, March 2015*

[2]. *Nikolay N. Ponomarenko, Karen O. Egiazarian & Vladimir V. Lukin"High-Quality DCT-Based Image Compression Using Partition Schemes", IEEE SIGNAL PROCESSING LETTERS, VOL. 14, NO. 2,FEBRUARY 2007*

[3]. *Tapas Bandyopadhyay, B Bandyopadhyay & B N Chatterji, "Secure Image encryption through key hashing and wavelet transformtechniques", International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 2, Issue 2, February 2012*

[4]. *M. Nagabushanam, S. Ramachandran, & P. Kumar "FPGAImplementation of 1D and 2D DWT Architecture using Modified Lifting Scheme", WSEAS TRANSACTIONS on SIGNAL PROCESSING 2014*

[5]. *Bhonde Nilesh, Shinde Sachin, Nagmode Pradip, & D.B. Rane "ImageCompression Using Discrete Wavelet Transform",International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 3, Special Issue, March-April 2013*

[6]. *M. Mozammel Hoque Chowdhury & Amina Khatun "Image CompressionUsing Discrete Wavelet Transform", IJCSI International Journal ofComputer Science Issues, Vol. 9, Issue 4, No 1, July 2012*

[7]. *Tsung-Hsi Chiang & Lan-Rong Dung "A VLSI Progressive Coding forWavelet-based Image Compression ", IEEE conference paper 2007*

[8]. *Zhijun Fang, Naixue Xiong,Xingming Sun, & Yan Yang "Interpolation-Based Direction-Adaptive Lifting DWT and Modified SPIHT for Image Compression in Multimedia Communications", IEEE SYSTEMS JOURNAL, VOL. 5, NO. 4, DECEMBER 2011*

[9]. *Cheng Xiao-hui & Deng Jian-zhi "Design of SHA-1 Algorithm based on FPGA", 2010 Second International Conference on Networks Security,Wireless Communications and Trusted Computing*

[10]. *Jianhua He, Hu Chen & Huaqiang Huang "A Compatible SHA Series Design Based on FPGA", Electrical Engineering/Electronics Computer Telecommunications and Information Technology (ECTI-CON), 2010 International Conference on Year: 2010*

[11]. *Thomas W. Fry & Scott A. Hauck,"SPIHT Image Compressionon FPGAs", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 15, NO. 9, September 2005*

[12]. *J. Jyotheswar & Sudipta Mahapatra, "Efficient FPGA implementationof DWT and modified SPIHT for lossless image compression",Elsevier Journal of Systems Architecture 53 (2007) 369378*

[13]. *T. Vijayakumar & S. Ramachandran "Design and FPGA Implementationof High Speed DWT-IDWT Architecture with Pipelined SPIHTArchitecture for Image Compression System", Global Journal ofComputer Science and Technology, Volume 14 Issue 1 Version 1.0 Year 2014*

[14]. *R. Vanaja & N. Lakshmi Praba "FPGA Implementation of PipelinedArchitecture For SPIHT Algorithm",2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013)*

[15]. *T. Vijayakumar & S. Ramachandran "FPGA Implementation of 2DDWTand SPIHT Architecture for Lossless Medical Image Compression", International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August-2013 ISSN 2229-5518*