ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

Design and Implementation of Stegnosystem using VLSI

M. Karthik, T. Karthik, M. Darani Kumar

Assistant Professor, Department of ECE, Karpagam College of Engineering, Coimbatore, India

ABSTRACT: With rapid increases in communication and network applications, Steganography has become a crucial issue to ensure the security of transmitted information. An algorithmic optimization or refinement can thus be made at a higher level based on the Reconfigurable data path. Experimental results show that the developed processor has full cryptography algorithm flexibility, high hardware utilization, and high performance[1]. In this paper propose a scheme to meet this need by incorporating a watermarking solution into a traditional crypto signature scheme to make the digital signatures robust to image degradations. The proposed approach is compatible with traditional crypto signature schemes except that the original image needs to be watermarked in order to guarantee the robustness of its derived digital signature. The proposed approach demonstrates the effectiveness of this proposed scheme through practical experimental results as well as illustrative analysis. Steganography seems to be much better than traditional encryption methods used today. Steganography is the new direction of cryptography. It makes use of chaotic system properties such as sensitive to initial condition and loss of information. In order to reach higher performance, these methods take advantage of the more and more complex behavior of chaotic signals. This paper contributes by comparing and analyzing the performance of the past Steganography schemes.

KEYWORDS: 3D-DWT, Compression, Lifting Scheme Algorithm, SHA, Encryption and Decryption.

I.INTRODUCTION

Steganography is the practice of hiding information “in plain sight”. This technique relies on a message being encoded and hidden in a transport layer in such a way as to make the existence of the message unknown to an observer. Importantly, the transport layer - the carrier file - is not secret and can therefore be viewed by observers from whom the secret message itself should be concealed. The power of steganography is in hiding the secret message by obscurity, hiding its existence in a non-secret file[2]. In that sense, steganography is different from cryptography, which involves making the content of the secret message unreadable while not preventing non-intended observers from learning about its existence. observer would not suspect it is there at all, the greatest effort must go into ensuring that the message is invisible unless one knows what to look for. The way in which this is done will differ for the specific media that are used to hide the information. In each case, the value of a steganographic approach can be measured by how much information can be concealed in a carrier before it becomes detectable, each technique can thus be thought of in terms of its capacity for information hiding. Steganography has been used to hide secret messages in various types of files, including digital images, audio and video. This work focuses on encryption and decryption steganography.

DWT Algorithm

The discrete wavelet transform was computed by changing the scale of the analysis window, shifting the window in time, multiplying by the signal, and integrating over all times. In the discrete case, filters of different cutoff frequencies are used to analyze the signal at different scales. The signal is passed through a series of high pass filters to analyze the high frequencies, and it is passed through a series of low pass filters to analyze the low frequencies. The resolution of the signal, which is a measure of the amount of detail information in the signal, is changed by the filtering operations, and the scale is changed by upsampling and downsampling (subsampling) operations. Sub sampling a signal corresponds to reducing the sampling rate, or removing some of the samples of the signal. For example[3], subsampling by two refers to dropping every other sample of the signal. Subsampling by a factor *n* reduces the number of samples in the signal *n* times.

II.LIFTING SCHEME ALGORITHM

The wavelet Lifting Scheme is a method for decomposing wavelet transforms into a set of stages. Lifting scheme algorithms have the advantage that they do not require temporary arrays in the calculations steps and have lesscomputation. Using the lifting coefficients to represent the discrete wavelet transform kernel.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

***Need for lifting scheme algorithm*:**

Perfect Reconstruction in a Finite World

One of the features of wavelets that is critical in areas like signal processing and compression is what is referred to in the wavelet literature as **perfect reconstruction.** A wavelet algorithm has perfect reconstruction when the inverse wavelet transform of the result of the wavelet transform yields exactly the original data set:

IWT (WT (D)) = *D*

Many wavelet equations that have the property of perfect reconstruction for infinite data sequences do not have this property for finite data sequences. Since sound files, financial time series, images and other data sets to which wavelets are applied are finite this can be a problem[4]. There are several methods proposed in the wavelet literature for dealing with the edges of finite data sets.

STEPS INVOLVED:

PREDICT PHASE:

A good predictor has to generate a signal of coefficients with suitable properties for compression. According to the coding theory, a signal with minimum variance will be coded with the highest efficiency. Indeed, quantization error is a function of the signal energy. The optimal bit allocation defines quantization steps for a given bit-rate, called target bitrate. The model-based bit allocation characterizes the high frequency signal by a Gaussian or other model of probability density. They define the quantization steps, which minimize the distortion. The distortion is therefore dependent on the signal variance. Then, a reliable and adequate criterion for the application of a coder is to minimize the variance of the wavelet coefficients signal.

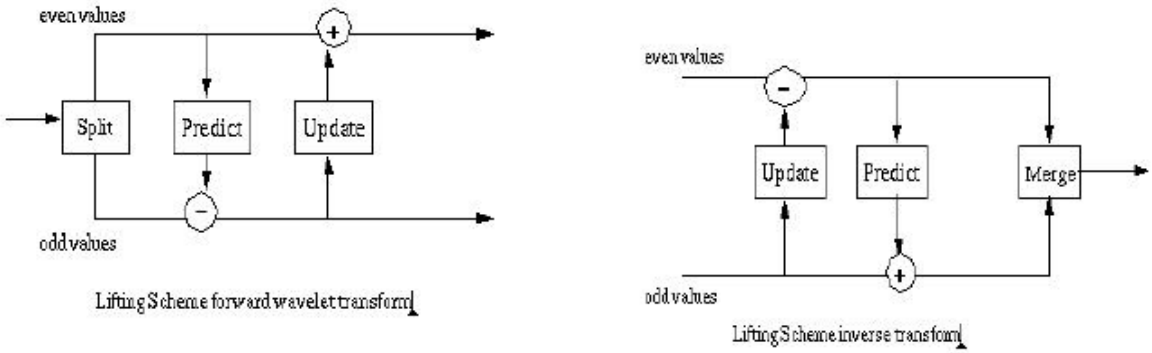


fig1 .a). FORWARD TRANSFORM b.) REVERSE TRANSFORM

UPDATE PHASE:

The update step replaces the even elements with an average. This result in a smoother input for the next step of the next step of the wavelet transforms. The odd elements also represent an approximation of the original data set, which allows filters to be constructed. The update phase follows the predict phase. The original value of the odd elements has been overwritten by the difference between the odd element and its even "predictor". So in calculating an average the update phase must operate on the differences that are stored in the odd elements.

even $j+1,i$ = even j,i + ***U***(odd $j+1,i$)

SPLIT PHASE:

The split phase that starts each forward transform step moves the odd elements to the second half of the array, leaving the even elements in the lower half. At the end of the transform step the odd elements are replaced by the differences

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

and the even elements are replaced by the averages. The even elements become the input for the next step, which again starts with the split phase. The first element in the array contains the data average. The differences (coefficients) are ordered by increasing frequency. One of the elegant features of the lifting scheme is that the inverse transform is a mirror of the forward transform. In the case of the Haar transform, additions are substituted for subtractions and subtractions for additions. The merge step replaces the split step.

III.IMPLEMENTATION OF DWT AND IDWT ALGORITHM

In this section we will discuss how to implement 3D FDWT and IDWT together with thresholding in MATLAB. In the FDWT part the input data will be transferred from time domain to scale domain. Then in thresholding part some of the coefficients will be set to zero and in the IDWT part the coefficients will be transferred back into time domain. While implementing the algorithm in MATLAB the matrix multiplication method has been used. We have tested the 'barbara.png'[8] as the image input file and also 8 randomly chosen image co-efficients for MATLAB simulation.

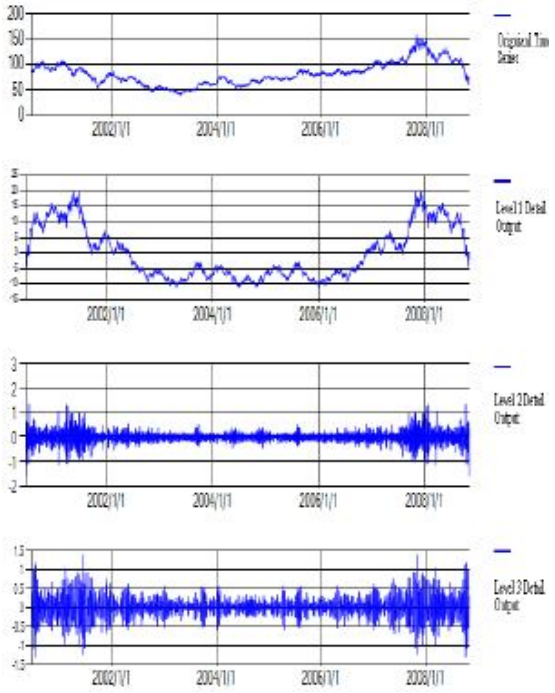


Fig.2. THREE LEVELS OF DECOMPOSITION

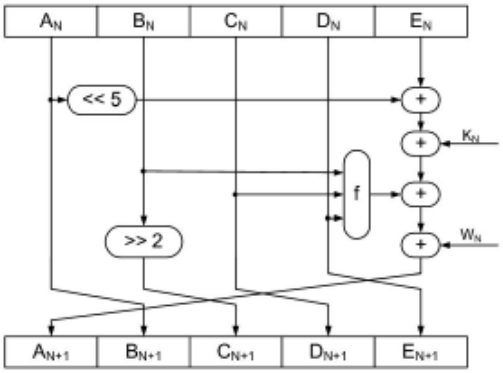
After we have achieved satisfactory result in MATLAB we proceed to the next stage where we translate the code into VHDL. The development of algorithm in VHDL is different in some aspects. The main difference is unlike MATLAB, VHDL does not support many built in functions such as convolution, max, mod, flip and many more. So while Implementing the algorithm in VHDL, linear equations of FDWT and IDWT is used. The floating point operations have been avoided here. The VHDL code is compiled and simulated using Aldec Active HDL 3.5 software. 8 image co- efficient that have been used in MATLAB were also used in VHDL simulation.

SHA-1HASH FUNCTION

SHA-1 is very similar to SHA-0, but corrects an error in the original SHA hash specification that led to significant weaknesses. The SHA-0 algorithm was not adopted by many applications. SHA-2 on the other hand significantly differs from the SHA-1 hash function.SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used security applications and protocols. Although no successful attacks have yet been reported on the SHA-2 variants, they are algorithmically similar to SHA-1 and so efforts are underway to develop improved alternatives.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013



One iteration within the SHA-1 compression function:
A, B, C, D and E are 32-bit words of the state;
F is a nonlinear function that varies;
n denotes a left bit rotation by *n* places;
n varies for each operation;
W t is the expanded message word of round t;
K t is the round constant of round t;

SHA-1 produces a 160-bit message digest based on principles similar to those used by Ronald L. [7]Rivest of MIT in the design of the MD4 and MD5 message digest algorithms, but has a more conservative design.SHA-1 differs from SHA-0 only by a single bitwise rotation in the message schedule of its compression function.

STEPS INVOLVED:

Appending Padding Bits
The b-bit M is padded in the following manner: a single 1-bit is added into the end of M, after which 0-bits are added until the length of the message is congruent to 448, modulo 512.

Appending Length
A 64-bit representation of b is appended to the result of the above step.Thus, the resulted message is a multiple of 512 bits.

Buffer Initialization
Let H0, H1, H2, H3and H be 32-bit hash value registers. These registers are used in the derivation of a 160-bit hash H.

At the beginning, they are initialized as follows

H0=X"67452301"

H1= X"EFCDAB89"

H2= X"98BADCFE" (1)

H3= X"10325476"

H4= X"C3D2E1F0"

IV.CONCLUSION

Thus the comparison of DWT and IDWT algorithms were implemented and the results were obtained as discussed in the paper. By using image processing tool box in MATLAB the image stengography has been successfully implemented.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

REFERENCES

[1] Rafael C. GONZALEZ Richard E. WOODS. Digital image processing: second ed [M]. Beijing Publishing House of Electronics Industry 2002。
[2] Marc ANTONINI Michel BARLAUD Pierre MATHIEU et al. Image coding using wavelet transform [J]. IEEE Trans. Image Processing 1992 **1**(2) 205-220
[3] Cheng Li-chi, Wang Hong-xia, Luo Yong. Wavelet theory and applications. Beijing: Science Press,2004(chinese)
[4] J. M. SHAPIRO. Embedded image coding using zero tree of wavelets coefficients [J]. IEEE Trans. Signal Processing 1993 41(12)3445-346 2
[5] Amir SAID William A.PEARLMAN . A new fast and efficient imagecodec based on set partitioning in hierarchical trees [J]. IEEE Transactions On Circuits and Systems for Video Technology 1996 6(3) 243-250
[6] FAN Qi-bin. Wavelet analysis. Wuhan: Wuhan University Press, 2008.