A Secure Scheme for Multiple Images Transmission and Its VLSI Realization

K.Deergha Rao
R&T Unit for NavigationalElectronics
Osmania University
Hyderabad, India.

Ch. Gangadhar
Dept. of ECE
Siddhartha Institute of Technology Vijayawada,India.

P.V.Murali Krishna
Dept. of ECE
Vasavi College of Engg.
Hyderabad, India

ABSTRACT
Wavelet packet-division multiplexing (WPDM) is a high-capacity, flexible, and robust multiple-signal transmission technique in which the properties of wavelet packet basis functions are used for orthogonal multiplexing. In this paper, a new algorithm based on finite field wavelet packet division multiplexing (FFWPDM) is proposed for secure orthogonal multiplexing of images. Further, VLSI architecture of the proposed algorithm is designed. The VLSI architecture is implemented on images using XILINX ISE and ModelSim to demonstrate the effectiveness of the proposed scheme.

General Terms
Security, Algorithms.

Keywords
cryptography, wavelet packet division multiplexing, VLSI

1. INTRODUCTION
The advances in communication technology have seen strong interest in digital signal transmission. However, illegal data access has become more easy and prevalent in wireless and general communication networks. It is generally difficult to handle image encryption by conventional encryption algorithms such as DES, AES, IDEA, and RSA due to inherent features of images, such as the huge data and the high correlation among pixels [1].

Wavelet packet-division multiplexing (WPDM) is a high-capacity, flexible, and robust multiple-signal transmission technique in which the properties of wavelet packet basis functions are used for orthogonal multiplexing [2]. Wavelet transform over Galois fields are developed in [3]. VLSI implementation of finite field arithmetic is discussed in [4]. Finite field wavelet packet-division multiplexing(FFWPDM) provides orthogonal multiplexing of the images and encrypt the images. Finite field Wavelet packet-division multiplexing convert the input images data to a sequence similar to white noise. Hence, in this paper a new algorithm is proposed for secure transmultiplexer for images based on finite field wavelet packet-division multiplexing(FFWPDM). In finite field wavelet packet-division multiplexing(FFWPDM), the synthesis and analysis filter coefficients work as keys for encryption. Further, for the hardware implementation of the developed algorithms for practical use, VLSI architectures of the proposed algorithms are developed and realized using Xilinx ISE VLSI software.

2. FINITE FIELD WAVELET PACKET-DIVISION MULTIPLEXING
The wavelet system can be implemented using a two-band analysis-synthesis filter bank. Fig. 1 shows the analysis and synthesis banks of a two-channel perfect reconstruction filter bank. More specifically, the analysis bank performs the wavelet transform and the synthesis bank performs the inverse wavelet transform. $x(n)$ is the input data and the sequences labeled $y_0(n)$, $y_1(n)$ are the wavelet coefficients.

Let $H_s(z)$, $G_s(z)$ where $s=0,1$, be the polynomial representation of the filters $h_s(n)$, $g_s(n)$ in Fig. 1. Suppose that these polynomials have order $2N+1$ with polyphase components $E_{s0}(z)$, $E_{s1}(z)$, $R_{0s}(z)$ and $R_{1s}(z)$ so that

$$H_s(z) = E_{s0}(z^2) + z^{-1}E_{s1}(z^2) \quad (1)$$

$$G_s(z) = z^{-1}R_{0s}(z^2) + R_{1s}(z^2) \quad (2)$$

Using the polyphase representation for the two-band orthogonal filter banks, the following can be deduced:

$$H_1(z) = -z^{-(2N+1)}H_0(-z^{-1}) \ ,$$

$$G_0(z) = H_1(-z) \ , \ G_1(z) = -H_0(-z) \quad (3)$$

Any two polynomials $A(Z)$ and $B(Z)$ over a Galois field $F(Z)$ that satisfy the polynomial equation[2]

$$A(z)A^c(z) + B(z)B^c(z) = Z^M \quad (4)$$

can be used to generate the coefficients of wavelet filter banks.

The polynomials $A(Z)$ and $B(Z)$ over a Galois field $F(Z)$ are defined as

$$A(z) = \sum_{i=0}^{M} a_i z^i, \ a_0 \neq 0, \ B(z) = \sum_{i=0}^{M} b_i z^i, \ b_k \neq 0, \quad (5)$$

$$a_i, b_i \in GF(p^r)$$

where M is a positive integer satisfying $M <= N$. In our notation, the superscript c means the reciprocal of the

polynomial which is defined as $q^c(z) = z^M q(z^{-1})$. The coefficients of the two polynomials $A(Z)$ and $B(z)$ are related to the poly phase components $E_{00}(z)$ and $E_{01}(z)$ by

$$E_{00}(z) = A(z^{-1}) \ , \ E_{01}(z) = z^{M-N} B(z^{-1}) \qquad (6)$$

The K channel transmultiplexer is shown fig. 2 . Finite field two-band orthogonal filter banks are used to construct a finite field wavelet packet-division multiplexing(FFWPDM) transmultiplexer for four-users which is shown fig. 4.

3. VLSI Architecture

The architecture of FFWPDM multiplexer for two users is shown in Fig. 3(a). The architecture of FFWPDM multiplexer for four users is shown in Fig. 4(a). The architecture of FFWPDM demultiplexer for two users is shown in Fig. 3(b). The architecture of FFWPDM demultiplexer for four users is shown in Fig. 4(b). The architecture for FFWPDM synthesis filters is shown in Fig. 5. The architecture for FFWPDM analysis filters is shown in Fig. 6.

4. Simulation Results

The secure transmultiplexer for four users is implemented using FFWPDM on the 8 bits per pixel 256X256 Tree,factory, goldenear and IC images in GF(2^{18}). The original Tree,factory, goldenear and IC images are shown in Fig. 6(a). In the implementation of secure transmultiplexer using FFWPDM , the filter banks are constructed over GF(2^{18}) with the primitive polynomial $q(x) = x^{18} + x^7 + 1$. The polynomials $A(z) = 131009 + 7z$ and $B(z) = 131014 + z$ are used. The corresponding polyphase components $E_{00}(z) = 131009 + 7z^{-1}$, $E_{01}(z) = 131014 + z^{-1}$. The multiplexed image obtained using secure transmultiplexer using FFWPDM is shown in Fig. 6(b). From Fig.6 (b), it can be observed that the secure transmultiplexer using FFWPDM has created highly disordered image of the original images. The demultiplexed images using secure transmultiplexer using FFWPDM are same as original images as FFWPDM is lossless transform.

Table.1 Hardware complexity of the proposed VLSI architecture for secure transmultiplexer for four images

Hardware component	Transmitter	Reciever
1-bit register	0	9
18-bit register	12	18
32-bit register	0	9
36-bit register	6	0
19-bit 2-to-1 multiplexer	1248	1248
18-bit xor2	18	0
18-bit xor4	0	6
19-bit xor2	1248	1248

We designed our secure transmultiplexer using FFWPDM using VHDL and executed logic simulation with the use of ModelSim. The result of simulation using (256×256) Tree and factory images shows that the number of cycles needed for FFWPDM for two images is 65536(256×256). The result of simulation using (256×256) Tree,factory, goldenear and IC images shows that the number of cycles needed for FFWPDM for four images is 196608(3×256×256).

The maximum delay is 4 ns for FFWPDM synthesis filters unit. The maximum delay is 4 ns for FFWPDM analysis filters unit, which is concluded by XILINX ISE. The hardware requirements for implementation of the VLSI architecture of the proposed method using XILINX software are shown in Table 1.

5. Conclusions

In this paper, a secure transmultiplexer for images using finite field wavelet packet-division multiplexing(FFWPDM) is proposed. The effectiveness of the VLSI architecture designed for the proposed algorithm is demonstrated through implementation on four images using XILINX ISE and ModelSim. The compression algorithms like compressed sensing can be added to proposed algorithm to achieve image compression in transmultiplexer.

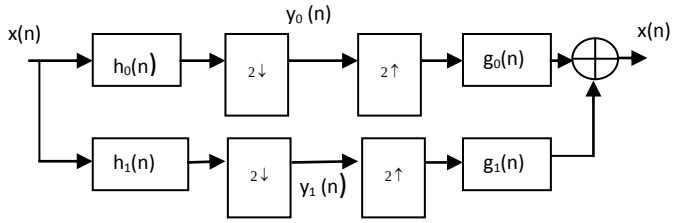

Fig 1: Two channel filter bank

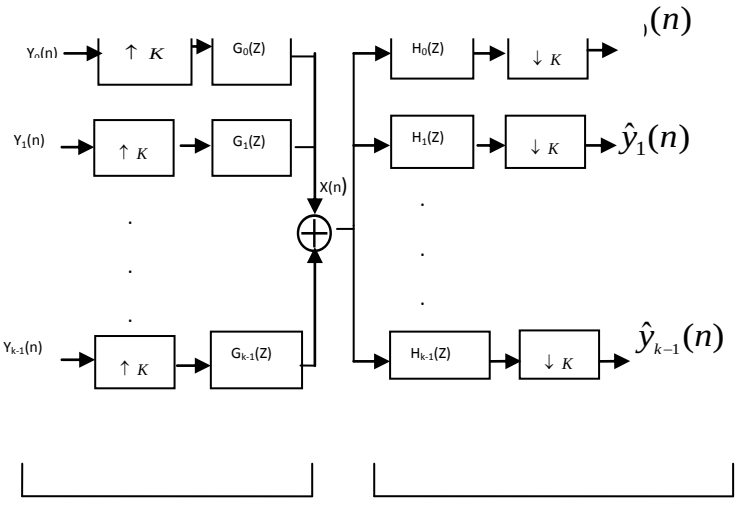

Fig 2 K channel transmultiplexer Synthesis(Transmitting) Bank

K channel transmultiplexer Analysis(Receiving) Bank

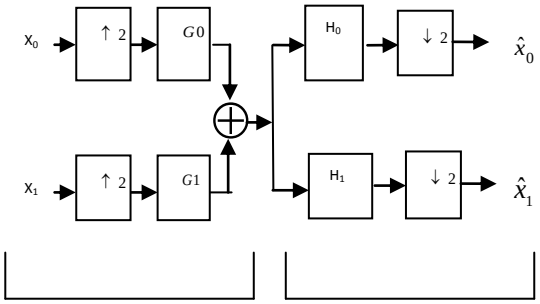

Fig 3(a): Two user FFWPDM synthesis bank (Multiplexer)

Fig 3(b): Two user FFWPDM analysis bank (Demultiplexer)

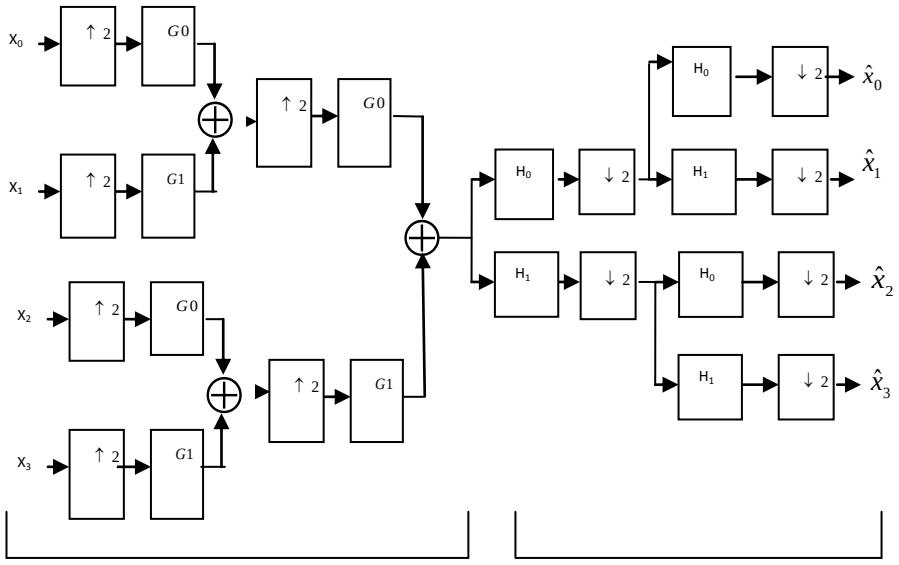

Fig 4(a): Four user FFWPDM synthesis bank (Multiplexer)

Fig 4(b): Four user FFWPDM analysis bank (Demultiplexer)

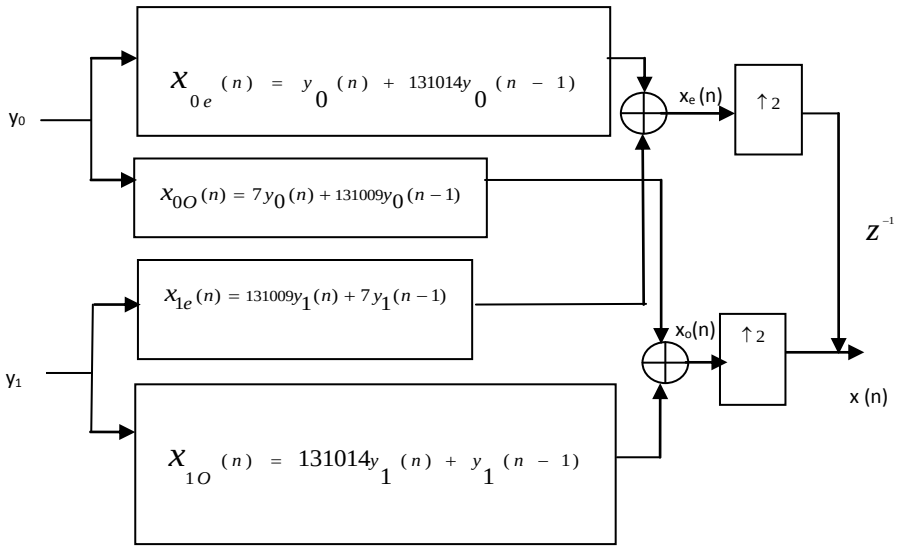

Fig 5: Architecture of FFWPDM synthesis lowpass filter and high pass filter

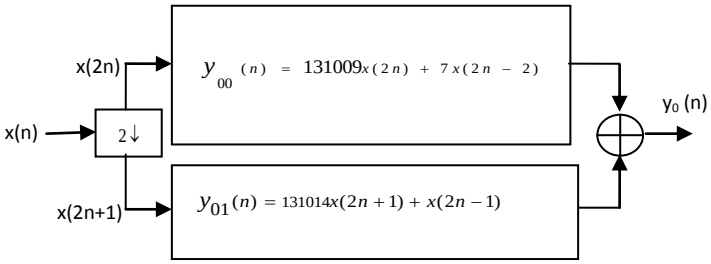

Fig 6(a): Architecture of FFWPDM analysis low pass filter

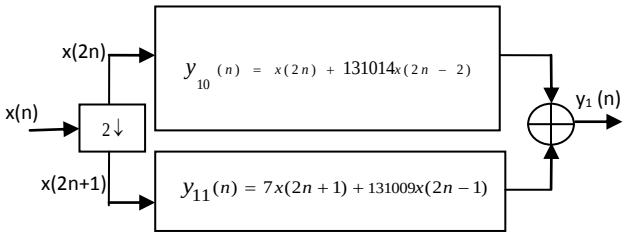

Fig 6(b): Architecture of FFWPDM analysis high pass filter

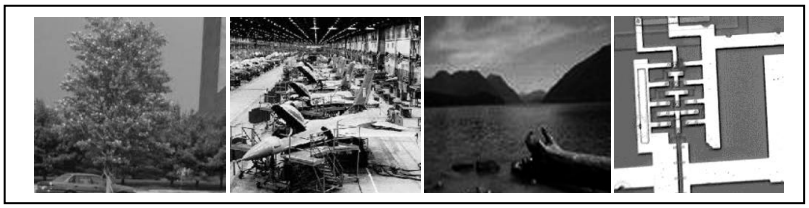

Fig 7(a): Original images tree, factory, goldenear and IC

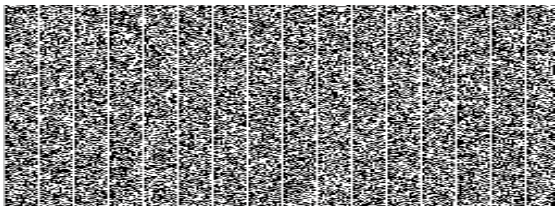

Fig 7(b): Multiplexed image using FFWPDM Multiplexer

6. REFERENCES

[1] B. Furht and D. Socek. Multimedia security: encryption techniques. In IEC Comprehensive Report on Information Security, International Engineering Consortium,Chicago, IL, pages 335.349, 2004.

[2] Kon Max Wong, Jiangfeng Wu and Tim N. Davidson "Wavelet Packet Division Multiplexing and Wavelet Packet Design Under Timing Error Effects," IEEE Transactions on Signal Processing, Vol. 45, No. 12, December 1997.

[3] Fekri, F. ; Mersereau, R.M. ; Schafer, R.W. "Theory on wavelet transform on finite fields". Proc. IEEE conference, ICASSP 1999, vol.3 Pp.1213 – 1216.

[4] Xilinx Coolrunner-II CPLD Galois Field GF(2^m) Multiplier, XAPP371 (v1.0) September 26, 2003.