DESAIN DAN SIMULASI
PERLINDUNGAN PROPERTI INTELEKTUAL
MENGGUNAKAN ALGORITME FILTER DIGITAL

PROPOSAL TUGAS AKHIR

Kelompok Kompetensi : Arsitektur Komputer

Oleh

Hanjara Cahya Adhyatma

1104131113

Program Studi Sarjana Sistem Komputer

Fakultas Teknik Elektro

Universitas Telkom

Bandung

2016

LEMBAR PERSETUJUAN

Desain dan Simulasi Perlindungan Properti Intelektual Menggunakan Algoritme Filter Digital

Design and Simulation of Intelectual Properties Protection using Digital Filter Algorithm

HANJARA CAHYA ADHYATMA
1104131113

Disusun dalam rangka memenuhi persyaratan dalam mengajukan Tugas Akhir
Pada
Program Studi Sarjana Sistem Komputer
Fakultas Teknik Elektro
Universitas Telkom

Proposal ini disetujui untuk menyelesaikan Tugas Akhir
Bandung, Oktober 2016

Calon Pembimbing I	Calon Pembimbing II
Surya Michrandi Nasution, ST., MT.	Fairuz Azmi, ST., MT.
NIK : 13860021	NIK : 15890008

ABSTRAK

System on a Chip (SoC) adalah sebuah modul *embedded system* yang memiliki fungsi tertentu dalam sebuah papan chip silicon yang juga bisa disebut dengan *Veri Large Scale Integration* (VLSI). Pemilik dari desain *SoC* memiliki hak cipta atas desain sistem yang telah dibuat. *Fabless manufacturing* merupakan cara pencetakan modul perangkat keras yang desainer *Integrated Circuit* (IC) adalah *Outsourching* dari luar pabrik percetakan.

Fabless manufacturing dari desain IC memiliki celah pencurian desain ketika desain akan dicetak atau ketika proyek membutuhkan *mutiple module* dengan berbagai fungsi dari berbagai desainer. Oleh karena itu setiap modul VLSI dari desainer *chip* ini membutuhkan bukti *ownership* dari perancang atau perusahaan produksi.

Dalam penelitian ini berencana membuat rancangan verifikasi *ownership* dengan 2 kunci khusus verifikasi yaitu *Polygate* sebagai kunci utama yang akan mengaktifkan kunci kedua, dan kunci kedua akan aktif yang prosesnya menggunakan algoritme filter digital.

Keyword: VLSI, *Intelectual Property Protection*, *Digital Signal Processing*, *Polygate* Watermark.

KATA PENGANTAR

Puji syukur terhadap Tuhan Yang Maha Esa yang telah memberikan rahmat dan hidayah Nya serta nikmat sehat dan nikmat waktu sehingga proposal ini diselesaikan. Ucapan terima kasih juga diperuntukkan untuk orang tua dan saudara – saudara saya yang telah memberikan semangat, serta teman-teman membantu dalam pengerjaan proposal ini. Ucapan terima kasih juga di-peruntukan kepada Dosen-dosen pembimbing proposal Tugas Akhir Telkom University yang memberikan masukan dan saran terhadap proposal ini.

Proposal penelitian ini bertujuan untuk mengembangkan ilmu teknologi serta keamanan dalam bidang *System on a Chip* (SoC) yang masih jarang dikembangkan di Indonesia.

Bandung, Oktober 2016

Penulis

DAFTAR ISI

LEMBAR PERSETUJUAN.....ii
ABSTRAK.....iii
KATA PENGANTAR.....iv
DAFTAR ISI.....v
DAFTAR GAMBAR.....vi
DAFTAR ISTILAH.....viii
BAB I PENDAHULUAN.....1
1.1 Latar Belakang.....1
1.2 Rumusan Masalah.....2
1.3 Tujuan.....2
1.4. Batasan.....3
1.5. Hipotesis.....3
BAB II KAJIAN PUSTAKA.....4
2.1 Pekerjaan Sebelumnya dan Keterkaitan.....4
2.2 Perancangan dan Implementasi Algoritme DSP untuk IPP.....5
BAB III METODOLOGI PENELITIAN.....6
3.1 Studi Literatur.....6
3.2 Analisis.....6
3.3 Perancangan.....6
3.4 Pengujian.....8
3.5 Keluaran yang diharapkan.....9
BAB IV JADWAL KEGIATAN.....10
4.1 Jadwal Kegiatan.....10
DAFTAR PUSTAKA.....11
LAMPIRAN.....13

DAFTAR GAMBAR

Gambar 2.1: Alur Desain Watermark.....5

Gambar 3.2: HDMI connector[11].....6

Gambar 3.3: FPGA sebagai HDMI controller [11].....7

Gambar 3.4: Contoh Polymorph Gate [12].....7

Gambar 3.5: Alur pemilihan filter dengan polygates.....8

DAFTAR TABEL

Tabel 4.1: Rencana Kegiatan.....10

DAFTAR ISTILAH

FPGA : *Field-programmable Gate Array* (Digunakan pertama pada hal. 6)

HDMI : *High-Definition Multimedia Interface* (Digunakan pertama pada hal. 6)

IC : *Integrated Circuit* (Digunakan pertama pada hal. 1)

DSP : *Digital Signal Processing* (Digunakan pertama pada hal. 4)

SOC : *System-on-Chip* (Digunakan pertama pada hal. 1)

VLSI : *Very-Large-Scale IC* (Digunakan pertama pada hal. 1)

BAB I PENDAHULUAN

1.1 Latar Belakang

Integrated Circuit (IC) merupakan modul teknologi dasar dari perangkat elektronika tertanam modern. Dengan berkembangnya teknologi IC yang mengutamakan ukuran kecil, dan performa yang tinggi serta dengan harga yang murah membuat teknologi IC semakin diminati [1].

Dengan ukuran modul yang sangat kecil dan banyaknya komponen pembangun, kerja sama antara desainer dilakukan untuk membangun sebuah modul VLSI sehingga setiap desainer dapat fokus mendesain salah satu fungsi yang terdapat dalam modul tersebut. Kerja sama dilakukan untuk mempermudah pembuatan desain VLSI yang memiliki tingkat kerumitan yang tinggi. Desainer juga dapat mempercepat waktu mendesain dengan menggunakan kode sumber yang sudah ada atau bekerja sama secara paralel membuat masing-masing modul yang nantinya akan digabung menjadi sebuah modul utama VLSI.

Setelah modul selesai dibuat maka modul siap untuk di-produksi. Dalam proses produksi modul perusahaan tempat desainer bekerja tidak perlu memiliki pabrik produksi modul sendiri, perusahaan dapat bekerja sama dengan mitra percetakan yang akan memproduksi modul buatan perusahaan modul tersebut. Cara kerja sama seperti ini disebut dengan *Fabless Manufacturing* [2]. Ketika akan memproduksi IC, perusahaan harus menyerahkan *blueprint* modul VLSI ke percetakan, namun *blueprint* tersebut tidak terjamin kerahasiaan nya serta memungkinkan plagiarisme desain oleh oknum perusahaan atau pihak ketiga yang tertarik menggunakan desain VLSI yang telah diserahkan untuk di-produksi.

Dengan memberikan rangkaian watermark sebagai pengamanan pada *blueprint* VLSI siap cetak yang menandakan kepemilikan dari desainer atau perusahaan produsen modul akan melindungi dari kecurangan pihak lain yang akan mencuri desain. Sehingga kemungkinan pencurian atau plagiarisme yang menyebabkan kerugian pada perusahaan atau desainer karena desain nya dicuri atau di-plagiat berkurang [3][4][5][6]

1.2 Rumusan Masalah

Berikut ini dijelaskan rumusan masalah yang dihadapi dalam proposal penelitian *Intelectual Property Protection* (IPP) menggunakan metode *Digital Filter Algorithm using Logical Polymorph Gate Key Verification* :

a) Dengan metode *Fabless Manufacturing*, desain modul yang siap diproduksi diserahkan kepada perusahaan percetakan mitra sehingga mitra dapat mengetahui desain modul dari desainer yang memungkinkan desain dapat dicuri oleh oknum percetakan atau pihak ketiga yang tertarik dengan desain tersebut.
b) Desain modul rawan terhadap plagiarisme karena desain elektronik sangat mudah ditiru, sehingga pengamanan desain harus dilakukan agar desain tidak mudah untuk dicuri atau di-plagiat.
c) Apabila pihak ketiga mencuri desain, desainer dapat mengklaim modul tersebut dengan bukti dari pengamanan watermark yang telah tertanam dalam IC menggunakan teknik pemanggilan watermark yang hanya diketahui oleh desainer yang mendesain IC tersebut.

1.3 Tujuan

Berikut merupakan tujuan pengamanan desain modul yang siap cetak sehingga aman terhadap pencurian hak cipta :

a) Merancang rangkaian pengamanan dalam sebuah *chip design* sebagai bukti kepemilikan desain (*ownership*) atau watermarking.
b) Desain *chip* yang telah diberi rangkaian watermark akan dianalisis perubahan performa dari desain sebelum dan sesudah watermarking serta kemungkinan watermark di-modifikasi oleh pihak lain atau *reverse engineering* untuk digunakan kembali oleh pengguna yang tidak sah.
c) Rangkaian ini akan ditanam di dalam *chip* yang pemanggilan informasi pemilik dari *chip* hanya diketahui oleh pemilik cipta.

1.4. Batasan

Dalam penelitian ini rancangan desain VLSI yang disisipkan *watermark* membatasi masalah serta pembahasan yang akan diteliti sebagai berikut :

a) Tidak membuat modul IC VLSI spesifik, namun menggunakan yang sudah ada dan menyisipkan dengan watermark.
b) Menyisipkan rangkaian dengan data watermark dan tidak membahas detail data dari pemilik cipta.
c) Watermarking yang dilakukan untuk satu *chip* IC dan tidak me-watermark masing-masing modul yang ter-integrasi dalam *chip* IC.

1.5. Hipotesis

Desain modul akan disisipkan watermark sehingga pihak lain yang mencuri desain dan ketika desain telah tercetak, desainer dapat mengklaim modul tersebut dengan memasukkan kombinasi kode khusus yang hanya diketahui oleh desainer. Apabila desain IC membutuhkan banyak modul di dalamnya hal ini akan memungkinkan pendesain IC tersebut akan mencuri modul dari desainer lain sehingga kepemilikan dari modul tersebut tertutupi oleh berbagai integrasi modul yang digabungkan dalam IC yang dibuat.

BAB II KAJIAN PUSTAKA

2.1 Pekerjaan Sebelumnya dan Keterkaitan

Secara garis besar teknik *Intelectual Property Protection* (IPP) watermarking dapat diklasifikasikan menjadi 2 kelas yaitu *Dynamic Watermarking* dan *Static Watermarking*. *Dynamic Watermarking* merupakan watermark yang tidak dapat terdeteksi kecuali dengan menjalankan IP yang telah di-watermark untuk mendeteksi sinyal yang dihasilkan, seperti *digital signal processing* (DSP), atau *finite state mechine* (FSM) watermarking. *Static Watermarking* merupakan watermark yang mengacu pada properti dari sebuah desain, dan hanya bisa terdeteksi dengan cara statis yang berbeda, seperti jalur dan penempatan watermarking [7].

Salah satu pengamanan lain adalah mengonversi fail simulasi dari fail. RTL *source code* yang memungkinkan tidak mudah untuk di-*reverse-engineering* oleh pihak ketiga, sehingga model tidak dapat dirubah dan digunakan kembali dengan keperluan lain oleh pihak ketiga dan pengguna yang tidak bertanggung jawab.[8][9]

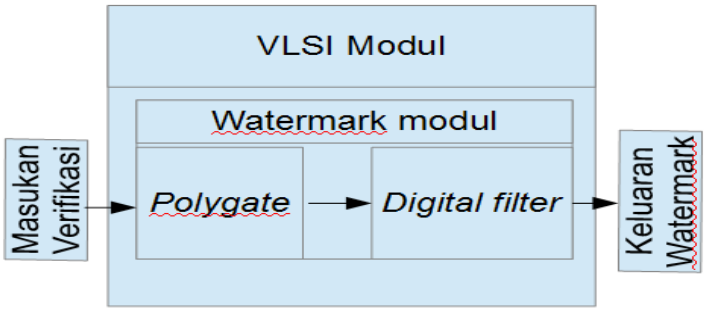
Namun cara tersebut hanya melindungi dari sisi *softwere* yang melindungi IP agar tidak di-salah-gunakan oleh pengguna pihak ketiga. Untuk pengamanan IP yang digunakan dalam *sharing project* dan reusable project dapat digunakan dengan pengamanan *Digital Signal Processing cell* yang memungkinkan integrasi dalam sistem.

Dalam penelitian kali ini akan melakukan kombinasi dari proteksi IP *polimorph gate* dengan algoritme filter digital. Menggunakan gabungan dari dua teknik ini akan memberikan tambahan keamanan pada proteksi IP yang kemungkinan tingkat *over write* watermark lebih kecil. Oleh karena itu dalam penelitian ini mengajukan sebuah gabungan metode yang sudah ada untuk meningkatkan kemampuan pengamanan dalam sebuah modul VLSI yang sudah ada. Dengan menggabungkan *polygate* sebagai kunci kombinasi untuk mengaktifkan modul filter digital yang akan digunakan sebagai watermark.

2.2 Perancangan dan Implementasi Algoritme DSP untuk IPP

Melakukan analisis terhadap masalah yang dikaji kemudian akan dilakukan rancangan *Intelectual Property Protection* (IPP) dengan algoritme Filter Digital yang dibangun meliputi rangkaian uji. Dari desain modul VLSI yang telah ada akan diuji coba kan performa sebelum diberi watermark.

Dengan memberikan rangkaian watermark sebagai pengamanan pada *blueprint* VLSI siap cetak yang menandakan kepemilikan dari desainer atau perusahaan produsen modul akan melindungi dari kecurangan pihak lain yang akan mencuri desain tersebut. Sehingga kemungkinan pencurian atau plagiarisme berkurang yang menyebabkan kerugian pada perusahaan atau desainer karena desain nya dicuri atau diplagiat.



Gambar 2.1: Alur Desain Watermark

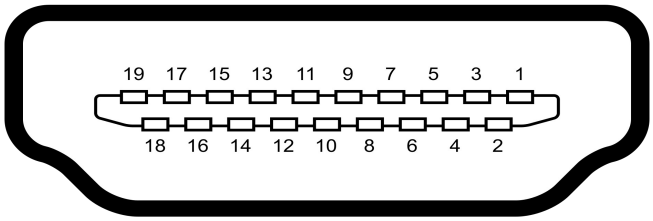
Desain akan dirancang dengan kombinasi *Low Pass Filter*, *High Pass Filter*, *Band Pass Filter*, dan *Band Reject Filter*. Kombinasi ini akan ditentukan dan diaktifkan oleh *polygate* sebagai kunci pengaktifan kombinasi Filter digital. Setelah Filter digital aktif maka kombinasi data akan melewati kombinasi filter yang diaktifkan dari kombinasi *polygate*. Kemudian data hasil kombinasi proses ini akan membentuk pola khusus yang menjadi data watermark dari desainer yang mencirikan identitas desainer. Setelah diberikan watermark maka modul akan diuji coba kan kembali performa nya. Bila terjadi penurunan performa maka akan dilakukan perbaikan algoritma kemudian dilakukan diuji kembali performa nya. Hingga didapat performa yang paling baik dari beberapa uji coba yang akan dilakukan.

BAB III METODOLOGI PENELITIAN

3.1 Studi Literatur

Melakukan studi literatur dengan mengumpulkan dan mempelajari teori-teori serta konsep dari *Digital Signal Algorithm*, implementasi *Digital Signal Algorithm* pada *Intelectual Properties Protection*, dan modifikasi *Digital Signal Algorithm* dari buku, artikel, jurnal dan referensi lainnya. Hasil studi literatur yang didapatkan akan dijadikan bahan untuk dasar teori dalam pembuatan tugas akhir ini. Dalam rencana penelitian kali ini akan menggunakan HDMI *controller* sebagai *chip* VLSI yang akan diberi watermark.

HDMI (*Hight-Definition Multimedia Interface*) merupakan antarmuka multimedia yang men–*tranfer* vidio atau audio tanpa kompresi maupun terkompresi dari sumber media *controller* ke perangkat keluaran yang *competible* seperti Monitor, Proyektor, Digital Televisi [10]**.**



Gambar 3.2: HDMI connector[11]

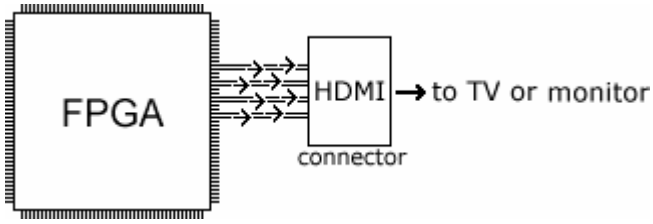
3.2 Analisis

Analisis dilakukan untuk mengkaji masalah yang ada, mendefinisikan batasan dalam masalah, lalu mencari solusi dari masalah tersebut. Analisis juga meliputi performa rancangan modul yang telah diberi watermark yang diuji coba dalam *board* FPGA.

3.3 Perancangan

Pada tahap ini dilakukan pengkajian masalah serta pendefinisian batasan masalah. Pencarian solusi atas masalah yang muncul juga dilakukan. Tahap ini juga meliputi analisis penempatan dan penentuan jalur dalam pemasangan

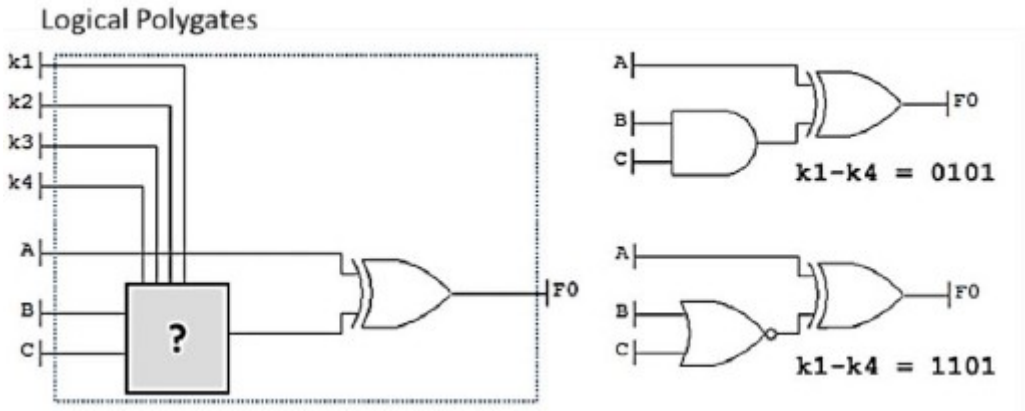
rangkaian uji IP *Protection* pada VLSI.



Gambar 3.3: FPGA sebagai HDMI controller [11]

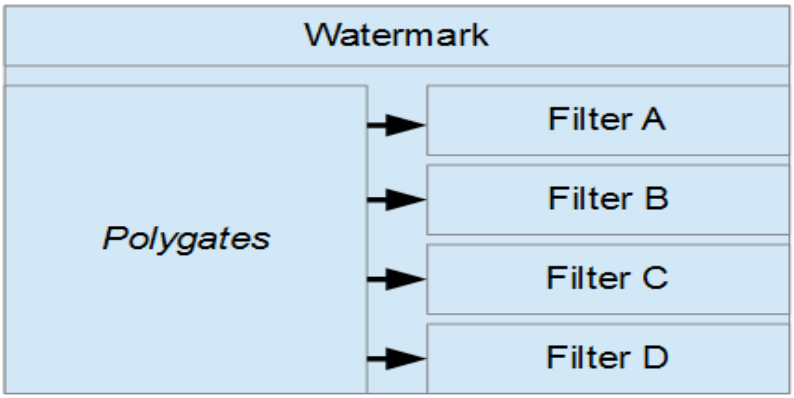
Penelitian kali ini akan melakukan simulasi desain *controller* HDMI menggunakan FPGA. Desain *controller* ini akan di-tes performa-nya dengan menjalankan fail multimedia. *Controller* akan disambung-kan ke *connector* HDMI lalu menampilkan hasil keluaran multimedia pada monitor atau TV. Kemudian di dalam *controller* HDMI ini akan disisipkan rangkaian watermark dan akan dilakukan pengecekan performa-nya lagi untuk mengetahui terjadinya penurunan performa karena watermark.

Dalam penelitian ini teknik watermark yang digunakan adalah menggabungkan rangkaian *logical polimorph gate* sebagai kunci utama untuk mengaktifkan rangkaian *Digital Signal Filter* yang akan diberi masukan kunci kedua untuk memanggil data watermark dalam *chip*.



Gambar 3.4: Contoh Polymorph Gate [12]

Setelah *unique key* dari *Polygates* di masukan (contoh: K1 - K4), maka pin *input* untuk algoritme DSP aktif (contoh: pin A – C) yang kemudian akan mengolah *key* untuk penampilan watermark dalam *chip*.



Gambar 3.5: Alur pemilihan filter dengan polygates

Setelah *polygate* mengaktifkan filter yang dipilih maka data dari pin input DSP (contoh: pin A – C) masuk ke dalam filter yang aktif dan akan diolah sebagai data input watermark.

3.4 Pengujian

Pada tahap ini dilakukan serangkaikan uji coba untuk mengukur parameter performa rangkaian VLSI yang telah disisipkan rangkaian uji IP *Protection. Petitcolas* [13] mengidentifikasi beberapa hal yang menjadi bahan evaluasi untuk IP *Protection* :

a) Kerahasiaan algoritme

Merujuk pada aturan keamanan yang dijelaskan oleh *Kerckhoffs* [14] pada tahun 1883, setiap enkripsi atau teknik keamanan tidak boleh mengandalkan kerahasiaan suatu algoritme, tetapi pada kompleksitas matematis algoritme tersebut.

b) Tingkat Ketahanan Uji

Ini adalah aspek yang sangat penting. Aspek ini berisi tentang ketahanan algoritme dari serangan dan persentase dari IP *Protection* tak terdeteksi.

Kemungkinan *detector* salah mendeteksi algoritme pada rangkaian tanpa algoritme juga diperhitungkan di aspek ini.

c) Tingkat Penurunan Performa

Penurunan performa saat menyisipkan suatu metode IP *Protection* adalah hal yang tak dapat dihindari. Tetapi penurunan performa yang terlalu besar akan menjadi masalah. Maka dari itu, perbandingan performa antara rangkaian yang telah disisipkan IP *Protection* dan rangkaian tanpa IP *Protection* harus dilakukan.

d) Tingkat Deteksi

Penyisipan watermark merupakan bagian dari proses, pelacak-kan dan deteksi dalam teknik watermark IC. Pelacak-kan dan deteksi watermark pada kemungkinan penyerangan merupakan aspek yang akan dijadikan pertimbangan pada teknik watermark.

3.5 Keluaran yang diharapkan

Metode yang akan digunakan merupakan simulasi pada *board* FPGA dengan desain modul yang sudah ada dan menyisipkan suatu rangkaian tambahan watermarking dan menguji perubahan performa modul yang telah di sisipkan watermark tersebut.

Dalam penelitian ini akan menggunakan teknik *Digital Signal Processing Watermarking* pada modul yang telah ada dengan kombinasi perhitungan *loop* biner dengan *output* yang akan membentuk nama dari produsen asli modul tersebut. Modul yang telah diberi watermark akan tetap dapat diuji keabsahan pemiliknya walaupun modul telah digabungkan dengan modul lain dalam sebuah proyek modul VLSI.

Kemudian setelah modul disisipkan watermark, kami akan menguji performa modul tersebut dengan mengharapkan tidak ada perubahan berarti terhadap modul yang telah diberi watermark tersebut.

BAB IV JADWAL KEGIATAN

4.1 Jadwal Kegiatan

Agar pembuatan tugas akhir ini berjalan dengan baik dan sesuai dengan yang diharapkan, maka diperlukan suatu jadwal kegiatan pembuatan tugas akhir. Adapun jadwal kegiatan yang direncanakan adalah sebagai berikut:

Tabel 4.1: Rencana Kegiatan

No.	Rencana	Januari				Februari				Maret				April			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Pengumpulan Data																
2	Perancangan Rangkaian																
3	Perhitungan Performa																
4	Optimasi Rangkaian																
5	Membandingkan performa																
6	Pembuatan Buku TA																

DAFTAR PUSTAKA

[1] Raj Kamal, 2011, *Embedded Systems Architecture, Programming and design second edition, Amerika Serikat*, The McGraw Hill Education.

[2] Chris A. Malachowsky, 2006, *Managing test, yield, quality, and cost in fabless manufacturing model,* International, IEE Test Confrence.

[3] Dai, Wei, H.K. Kwan, Huapeng Wu, 2005, *IP protection for FPGA implementation of DSP algorithms. 48th Midwest Symposium on Circuits and Systems*, Vol. 2, pp. 1418-1421.

[4] Lach, J., W.H.Mangione-Smith, M.Potkonjak, 2001, *Fingerprinting Techniques for Field-Programmable Gate Array Intellectual Property Protection*, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol 20, No.10, pp. 1253-1261.

[5] Petitcolas, F.A.P., 2000, *Watermarking Schemes Evaluation*, IEEE Magazine on Signal Processing, vol. 17, no. 5, pp. 58–64.

[6] Amr T Ah, S Tahar, El Mostapha, 2015, *A Survey on IP Watermarking Techniques*. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 23, No. 5

[7] AMR T. Abdel-Hamid., S. Tahar., EL Mostapha., 2004, *A Survey on IP Watermarking Techniques,* Netherland, Spring Science + Bussiness Media, Inc.

[8] R Chapman., Tariq SD., 2000, *IP Protection of DSP Algortihm for System on Chip Implementation*. IEEE Transactions on Signal Processing, Vol. 48, No. 3, pp. 854-861.

[9] Nie, Tingyuan, Yansheng Li, Xiaoke Xu, 2010, *Performance Evaluation for Watermarking Techniques*, Biomedical Engineering and Computer Science (ICBECS)

[10] http://www.hdmi.org/learningcenter/faq.aspx di-akses pada 18 Oktober 2016

[11] http://fpga4fun.com/HDMI.html di-akses pada 18 Oktober 2016

[12] Petitcolas, F.A.P. *Watermarking Schemes Evaluation*. *IEEE Magazine on Signal Processing*, vol. 17, no. 5, pp. 58–64, 2000.

[13] McDonald, Jeffrey T., et al, 2016, *Fuctional Polymorphism for Intellectual Property Protection*, IEEE International Symposium on Hardware Oriented Security and Trust (HOST).

[14] Kerckhoffs, A., 1883, *Journal des sciences militaires*, La Cryptographie Militaire vol. 9.

LAMPIRAN