SKRIPSI

ANALISIS IMPLEMENTASI ALGORITMA ENKRIPSI VIDEO RVEA(BHARGAVA) MENGGUNAKAN FPGA

Disusun dan diajukan oleh :

ELBERT TIMOTHY THOMAS

D42116015

DEPARTEMEN TEKNIK INFORMATIKA

FAKULTAS TEKNIK UNIVERSITAS HASANUDDIN

MAKASSAR

2023

LEMBAR PENGESAHAN SKRIPSI

ANALISIS IMPLEMENTASI ALGORITMA ENKRIPSI VIDEO RVEA(BHARGAVA) MENGGUNAKAN FPGA

Disusun dan diajukan oleh

ELBERT TIMOTHY THOMAS

D42116015

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Program Studi Teknik Informatika Fakultas Teknik Universitas Hasanuddin pada tanggal 22 Februari 2023 dan dinyatakan telah memenuhi syarat kelulusan.

Menyetujui,

Pembimbing Utama,	Pembimbing Pendamping,
Dr. Adnan, ST.,MT.	Dr.Eng. Ady Wahyudi Paundu, ST.,MT.
Nip. 197404262003121002	Nip. 197503132009121003

Ketua Program Studi,

Prof. Dr. Ir. Indrabayu, ST., MT., M.Bus.Sys., IPM, ASEAN. Eng.
Nip. 19750716 200212 1 004

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama : Elbert Timothy Thomas

NIM : D42116015

Departemen : Teknik Informatika

Jenjang : S1

Menyatakan dengan ini karya tulisan saya berjudul:

ANALISIS IMPLEMENTASI ALGORITMA ENKRIPSI VIDEO RVEA(BHARGAVA) MENGGUNAKAN FPGA

Adalah karya tulisan saya sendiri dan bukan merupakan pengambilalihan tulisan orang lain bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan skripsi ini hasil karya orang lain, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Makassar, 16 Maret 2023

Yang menyatakan,

Elbert Timothy Thomas

ABSTRAK

Dalam era globalisasi saat ini, perkembangan teknologi informasi dan komunikasi telah menjadikan media video sebagai salah satu sumber hiburan yang utama.Kemunculan serta popularitas pesat berbagai layanan streaming video menghadirkan kebutuhan akan sistem enkripsi yang aman dan efisien.

Dibandingkan dengan algoritma enkripsi lainnya yang melakukan enkripsi pada seluruh plaintext, algoritma Bhargava melakukan enkripsi selektif terhadap bit-sign yang terdapat pada video MPEG untuk mengurangi kebutuhan sumber daya komputasi. Penggunaan Field Programmable Gate Array (FPGA) sebagai media implementasi dapat mengurangi biaya operasi dengan menyediakan efisiensi energi tinggi dan Time to Market yang kompetitif. Penggunaan bersama antara algoritma Bhargava dan Field Programmable Gate Array dapat menjadi solusi optimal untuk menyediakan keamanan tinggi dengan penggunaan sumber daya yang ekonomis.

Dalam proses evaluasi, uji fungsionalitas telah berhasil dilakukan menggunakan perangkat FPGA dengan antarmuka UART(Universal Asynchronous Receiver Transmitter). Dari uji performa yang dilakukan dengan menggunakan fitur simulasi pada file sampel, diperoleh data bahwa implementasi enkripsi video menggunakan algoritma Bhargava pada FPGA dapat menghasilkan throughput sebesar 74,48 MiB per detik dengan kecepatan clock 200MHz, 4.9% dari *throughput* implementasi DES murni dengan *pipeline* penuh, investigasi selanjutnya menunjukkan bahwa titik *bottleneck* terdapat pada modul VLD.

Kata Kunci: Enkripsi Video, Bhargava, Field Programmable Gate Array, Enkripsi Selektif

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa, yang telah memberikan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan laporan tugas akhir dengan judul "Analisis Implementasi Algoritma Enkripsi Video RVEA(Bhargava) Menggunakan FPGA". Laporan tugas akhir ini merupakan salah satu syarat untuk memperoleh gelar Sarjana Strata Satu (S1) pada Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin.

Dalam proses pembuatan laporan tugas akhir ini, penulis banyak mendapat bimbingan, arahan, dan bantuan dari berbagai pihak sehingga penulis dapat menyelesaikan laporan ini tepat pada waktunya. Oleh karena itu dengan segala kerendahan hati, penulis mengucapkan terima kasih sebesar-besarnya kepada:

1. Kedua orang tua penulis, Bapak Erwin dan Ibu Meyly beserta keluarga atas segala doa, dukungan, semangat, pengorbanan, dan kasih sayang yang telah diberikan.
2. Bapak Dr. Adnan, ST., MT atas bimbingannya selama masa perkuliahan penulis dan sebagai Dosen Pembimbing I yang telah memberikan bimbingan dan masukan yang sangat bermanfaat dalam penyusunan laporan skripsi ini.
3. Bapak Dr-Eng. Ady Wahyudi Paundu, ST., M.T selaku Dosen Pembimbing II yang telah memberikan bimbingan dan masukan yang sangat bermanfaat dalam penyusunan laporan skripsi ini.
4. Seluruh Dosen dan Staf Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin.

5. Teman-teman angkatan Teknik Informatika 2016 selaku rekan belajar sejak dari awal hingga akhir masa perkuliahan.
6. Serta seluruh pihak yang tak sempat kami sebutkan satu persatu yang telah banyak meluangkan tenaga, waktu, dan pikiran selama penyusunan laporan skripsi ini.

Akhirnya dengan segala kerendahan hati, penulis menyadari masih banyak kesalahan dan kekurangan dalam penyusunan laporan skripsi ini baik dari isi maupun cara penyajiannya. Oleh karena itu penulis mengharapkan adanya saran dan kritik yang bersifat membangun demi kesempurnaan laporan ini. Penulis berharap semoga laporan skripsi ini dapat memberikan manfaat bagi pembaca pada umumnya dan penulis khususnya.

Makassar, Agustus 2022

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam era globalisasi ini, perkembangan teknologi informasi dan komunikasi meluncurkan media video menjadi sumber hiburan yang terutama. Sepuluh tahun terakhir ini melihat kemunculan berbagai layanan streaming video baru seperti TikTok, Disney+, Tencent Video, Hulu HBO Max, dan perkembangan pesat layanan- layanan yang telah ada. Menurut Statista, perusahaan multinasional dibidang data konsumen, Youtube mengalami perkembangan pesat dalam berbagai metrik, jumlah pengguna tahunan meningkat dari 0.8 milliar pengguna pada tahun 2012, menjadi 2.6 milliar pada tahun 2022, dengan pendapatan meningkat dari 0.8 milliar dollar amerika pada tahun 2010, menjadi 28.8 milliar dollar pada tahun 2022. peningkatan volume data video terutama konten yang memiliki hak cipta memunculkan permasalahan baru yaitu, meningkatnya kebutuhan akan solusi kriptografi yang aman, dan berefisiensi tinggi.

Algoritma Bhargava merupakan algoritma enkripsi video yang menggunakan sistem enkripsi selektif, dimana algoritma hanya mengenkripsi sebagian dari data sumber(plaintext). Algoritma Bhargava hanya melakukan enkripsi pada sign bit pada video MPEG, mengurangi kebutuhan sumber daya dalam pengamanan media video. Berkurangnya target enkripsi pada Algoritma Bhargava tidak mengurangi keamanan enkripsi, sebab perubahan

pada sign bit memiliki efek berantai yang mengacaukan seluruh video.

Field Programmable Gate Array atau FPGA merupakan sirkuit terintegrasi yang dapat dikonfigurasikan ulang setelah manufaktur. FPGA telah berkembang pesat, dari teknologi pendahulu seperti PLD dan CPLD, menjadi teknologi berdasar LUT dengan fitur tambahan seperti blok pengali dan memory menjadikan FPGA solusi komputasi dengan efisiensi energi dan potensi paralelisasi tinggi.

Digunakan bersama, implementasi algoritma Bhargava pada Field Programmable Gate Array diharapkan dapat menjadi solusi optimal yang menyedikan keamanan tinggi dengan penggunaan sumber daya rendah

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka penulis dapat merumuskan permasalahan-permasalahan yaitu :

1. Bagaimana cara mengimplementasikan algorima enkripsi video Bhargava dengan menggunakan *Field Programmable Gate Array*?
2. Bagaimanakah kinerja implementasi algortma enkripsi video Bhargava pada Field Programmable Gate Array berdasarkan parameter throughput data?

1.3 Tujuan Penelitian

Tujuan akhir dari penelitian ini yaitu :

1. Mengimplementasikan enkripsi video Bhargava pada Field Programmable Gate Array.
2. Menganalisa kinerja enkripsi video Bhargava pada Field

Programmable Gate Array dengan parameter throughput data.

1.4 Batasan Penelitian

Batasan masalah pada penelitian ini adalah :

1. Enkripsi dilakukan terhadap video dengan format MPEG-1
2. Implementasi hanya dilakukan terhadap algoritma Bhargava RVEA dengan menggunakan algoritma DES

1.5 Manfaat Penelitian

Dengan dilakukannya penelitian ini, diharapkan manfaat yang didapatkan antara lain:

1. Dengan mengimplementasikan algoritma enkripsi video Bhargava RVEA pada Field Programmable Gate Array, pengguna dapat memberikan perlindungan lebih maksimal terhadap keamanan data video dengan penggunaan sumber daya yang optimal.
2. Sebagai bahan referensi untuk penelitian-penelitian selanjutnya.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini akan dijelaskan teori-teori yang menunjang percobaan yang dilakukan.

BAB III METODOLOGI PENELITIAN

Bab ini berisi analisis kebutuhan sistem, perancangan sistem, dan skenario

pengujian.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini berisi hasil penelitian dan pembahasan.

BAB V PENUTUP

Bab ini berisi kesimpulan hasil penelitian dan saran.

BAB II

LANDASAN TEORI

2.1 Kriptografi

2.1.1 Definisi Kriptografi

Kriptografi berasal dari bahasa Yunani, menurut bahasa dibagi menjadi dua *kryptos* dan *graphein*, *kryptos* berarti *secret* (rahasia) dan *graphein* berarti *writing* (tulisan). Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan ketika dikirim dari sebuah sumber informasi ke suatu tujuan pengiriman informasi (Konheim, 2007). Sistem kriptografi terdiri dari dari 5 bagian yaitu:

1) *Plaintex*t: pesan asli berupa kumpulan karakter yang dapat berupa abjad, angka atau simbol tertentu yang dapat dibaca. *Plaintext* adalah masukan bagi algoritma enkripsi. Istilah teks asli akan digunakan sebagai padanan kata *plaintext* untuk selanjutnya.
2) Secret Key: suatu variabel terhadap teks asli yang menjadi penentu hasil dari algoritma enkripsi. Bersama dengan teks asli, secret key menjadi masukan bagi algoritma enkripsi. Istilah kunci rahasia akan digunakan sebagai padanan kata secret key untuk selanjutnya.
3) Ciphertext: hasil dari algoritma enkripsi yang tidak dapat secara langsung. Tingkat kualitas Ciphertext diukur dari tingkat kesulitan membacanya. Istilah teks sandi akan digunkan sebagai

padanan kata ciphertext untuk selanjutnya.

4) Algoritma Enkripsi: memiliki tugas utama melakukan perubahan terhadap teks asli menggunakan kunci rahasia sehingga menghasilkan teks sandi yang sulit dibaca.
5) Algoritma Dekripsi: bertugas memulihkan kembali teks sandi menjadi teks asli menggunaan kunci rahasia. Kunci rahasia yang digunakan untuk algoritma dekripsi dapat saja sama ataupun berbeda dengan kunci rahasia yang digunakan untuk algoritma enkripsi tergantung algoritma kriptografi yang digunakan (Sadikin, 2012).

2.1.2 Jenis-Jenis Algoritma Kriptografi

Berdasarkan dari kunci yang digunakannya, algoritma kriptografi di bagi menjadi dua bagian, yaitu algoritma simetris dan algoritma asimetris.

2.1.2.1 Algoritma Simetris

Algoritma Simetris adalah algoritma di mana kunci untuk proses enkripsi sama dengan dan proses dekripsi, misalnya permutasi, subtitusi, DES, AES (Konheim, 2007). Sehingga algoritma ini juga sering disebut algoritma klasik. Algoritma ini sudah ada lebih dari 4000 tahun yang lalu. Untuk menggunakan algoritma ini, penerima pesan harus tahu kunci yang digunakan pengirim untuk mengamankan pesan agar dapat melakukan dekripsi sehingga pesan dapat dibaca oleh penerima (Prayoga,

2018).

Jenis kriptografi ini menawarkan processing time yang baik, namun konsekuensi yang harus dibayar adalah kunci yang dipakai harus dijaga kerahasiaannya oleh pengirim dan penerima.

2.1.2.2 Algoritma Asimetris

Algoritma kriptografi asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Kelebihan algoritma ini adalah kunci untuk enkripsi dibuat umum (*public key*) atau dapat diketahui oleh setiap orang, tapi kunci untuk dekripsi hanya diketahui oleh orang yang berwenang mengetahui data yang disandikan atau sering disebut kunci pribadi (*private key*) (Nahwi, 2016).

Teknik enkripsi Asimetris ini jauh lebih lambat ketimbang enkripsi dengan kunci simetris. Oleh karena itu, biasanya bukanlah pesan itu sendiri yang disandikan dengan kunci asimetris, namun hanya kunci simetrislah yang disandikan dengan kunci asimetris. Sedangkan pesannya dikirim setelah disandikan dengan kunci simetris tadi. Contoh algoritma terkenal yang menggunakan kunci Asimetris adalah RSA (*Rivest Shamir Adleman*) (Alasi, 2007).

2.2 MPEG

MPEG-1(Moving Picture Experts Group Phase 1) merupakan standar kompresi *lossy* untuk video dan audio, MPEG didesain untuk menkompresi

video dan audio digital mentah dengan kualitas VHS menjadi alur data dengan laju 1.5 Mbit per detik(rasio kompresi 26:1 dan 6:1), tanpa pengurangan kualitas yang signifikan, memungkinkan terciptanya CD video, TV kabel/ satelit digital, dan penyiaran audio digital. (Le Gall, D, 1991).

Saat ini MPEG-1 merupakan format kompresi lossy video dan audio dengan kompatibilitas terluas didunia yang masih digunakan oleh sejumlah produk dan teknologi.

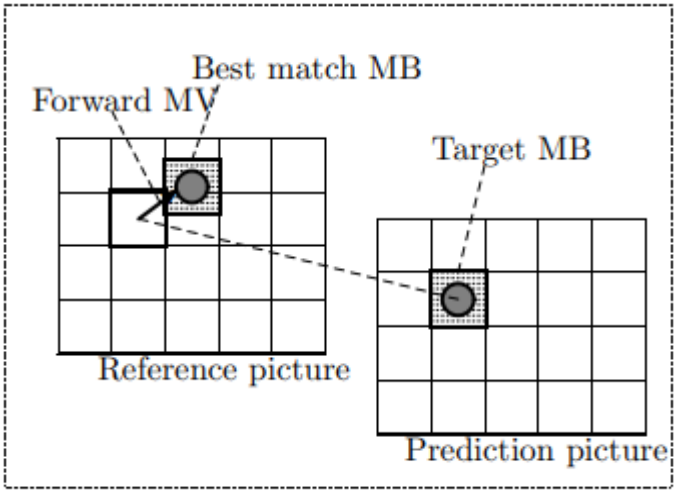
Standar MPEG-1 dipublikasikan sebagai ISO/IEC 11172 -*information technology- Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s*. Standar MPEG terdiri dari 5 bagian, yaitu sistem(penyimpanan dan sinkronisasi video, audio dan data lainnya), video(konten video terkompresi), audio(konten audio terkompresi), tes keabsahan(metode pengujian keabsahan implementasi standar), dan perangkat lunak referensi(contoh implementasi standar) (ISO/IEC, 1993a, 1993b, 1993c, 1995, 1998).

2.2.1 Struktur Video Stream MPEG

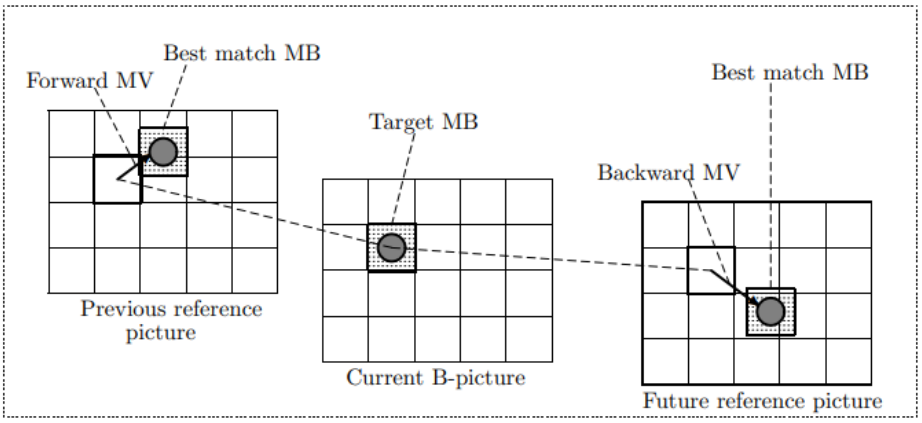
Stream video MPEG terdiri dari sejumlah grup gambar(*group of picture*), dan tiap grup gambar terdiri dari sejumlah gambar(*picture*)yang terdiri dari 3 jenis, gambar I, gambar P dan gambar B. Gambar I dikode secara intra, tanpa referensi dari picture(gambar) lainnya. Gambar P dikode secara prediktif menggunakan gambar I atau P sebelumnya. Gambar B dikode secara 2 arah (*Bidirectional*) diinterpolasi menggunakan gambar sebelum dan

sesudah gambar tersebut.

Tiap gambar terdiri dari kumpulan makroblok. Makroblok merupakan barisan sebesar 16 x 16 pixel. Makroblok yang terletak dalam gambar I dikode secara spasial. sedangkan makroblok yang terletak dalam gambar B atau P diinterpolasi secara temporal menggunakan gambar yang terkait dengan perbedaan nilai dihitung menggunakan selisih antara data referensi dan data sebenarnya. Proses interpolasi juga menghasilkan satu atau dua vektor gerak(vektor prediksi mundur dan vektor prediksi maju) untuk tiap makroblok dalam gambar referensi, seperti yang diilustrasikan pada gambar 2.1 dan gambar 2.2.

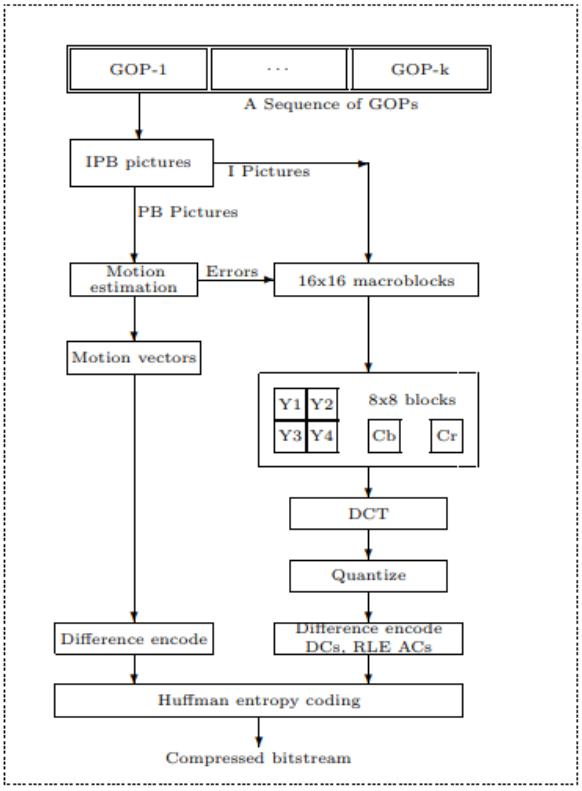


Gambar 2.1 Proses referensi gambar P



Gambar 2.2 Proses interpolasi gambar B

Setiap makroblok terdiri dari 4 blok 8x8 komponen Y (*luminance* atau pencahayaan), dan 2 blok 8x8 komponen warna, Cr(*chrominance* red) dan Cb(*chrominance blue*), seperti yang ditunjukkan pada gambar 2.3.



Gambar 2.3 Struktur video stream MPEG

Blok-blok tersebut selanjutnya melewati proses DCT(*Discrete Cosine Transform*), kuantisasi dan penkodean Huffman. Proses DCT memusatkan informasi pada frekuensi spasial rendah dan proses Kuantisasi membuat sebagian besar Koefisien DCT menjadi 0. Hasil kuantisasi lalu dilinearkan sesuai urutan zig-zag menjadi vektor <DC, AC_1, AC_2, ..., AC_{63}>. Koefisien DC menkodekan pencahayaan rata rata dalam blok, sedangkan koefisien AC memuat detil gambar.

RLE(*Run Length Encoding*) merubah vektor <AC_1, AC_2, ..., AC_{63}> menjadi pasangan lompatan dan nilai(*skip*, *value*) yang diubah menjadi stream video terkompresi menggunakan tabel kode Huffman. Tabel mengalokasikan nilai yang sering muncul dengan jumlah bit kecil untuk mencapai rasio kompresi tinggi. Setiap kode Huffman memiliki signbit(bit tanda) yang dikode terpisah, dimana 0 berarti positif dan 1 berarti negatif.(Bhargava, Shi, dan Wang, 2004)

2.3 Algoritma Bhargava

Bharat Bhargava, Changgui Shi, dan Sheng-Yih Wang mempublikasikan 4 algoritma enkripsi selektif untuk video MPEG, dimana setiap algoritma merupakan pengembangan dari algoritma sebelumnya, algoritma tersebut adalah Algoritma I, VEA, MVEA, dan RVEA.

2.3.1 Algoritma I

Algoritma I merupakan algoritma enkripsi video MPEG yang menyisipkan proses enkripsi/ dekripsi pada proses kompresi MPEG sehingga keduanya dilakukan dengan 1 tahap. Algoritma I melakukan

permutasi pada tabel kode Huffman, memanfaatkannya sebagai kode rahasia. Proses *encoding* dan *decoding* menggunakan tabel yang telah dipermutasi dan bukan tabel standar, sehingga pihak yang tak memiliki kunci rahasia akan menerima video yang berbeda.

Algoritma I memiliki kelemahan yaitu batasan *key space*. Rasio kompresi MPEG bergantung pada daftar kode Huffman, sehingga perubahan daftar ini dapat menurunkan rasio kompresi, selain itu, tak semua daftar kode Huffman dapat digunakan sebagai kunci enkripsi, hal ini menyulitkan generasi kunci sebab kunci yang dibuat perlu dites validitasnya sebelum digunakan. (Bhargava dan Shi, 1998a)

2.3.2 VEA

Algoritma VEA tak lagi memiliki kelemahan yang terdapat pada Algoritma I. Algoritma VEA merupakan algoritma enkripsi selektif yang hanya melakukan enkripsi terhadap signbit koefisien DCT pada video MPEG. Kunci rahasia VEA, k merupakan bitstream dengan panjang m yang dibangkitkan secara acak, dimana $k = b_1, b_2, \ldots, b_m$. Bila video MPEG S dilambangkan sebagai $S = \ldots s_1 \ldots s_2 \ldots s_m \ldots s_{m+1} \ldots s_{m+2} \ldots S_{2m}$ dimana s_i $(i = 1, 2, \ldots)$ merupakan sign bit koefisien DC dan AC, Algoritma enkripsi VEA Ek dapat dijabarkan sebagai berikut:

$$Ek(S) = \ldots(b_1 \oplus s_1)\ldots (b_m \oplus s_m)\ldots(b_1 \oplus s_{m+1})\ldots(b_m \oplus s_{2m}) \ldots$$

dimana $\oplus$ merupakan operasi XOR biner.

Algoritma VEA tak lagi memiliki batasan panjang kunci seperti Algoritma I namun algoritma VEA memiliki kelemahan lain, yaitu

lemah terhadap *Known Plaintext Attack*, jika pihak penyerang memiliki potongan video asli dan video terenkripsi, penyerang dapat dengan mudah mendapatkan kunci rahasia VEA. (Bhargava dan Shi 1998b)

2.3.3 MVEA

Algoritma MVEA merupakan modifikasi dari Algoritma VEA dimana selain mengubah koefisien DC dari gambar I, algoritma ini juga mengubah secara acak vektor gerak yang terdapat pada gambar B dan P.

Perubahan pada vektor gerak mengakibatkan decoder penyerang mereferensi makroblok yang salah, selain itu, karena vektor gerak dikode secara diferensial, perubahan signbit akan sekaligus mempengaruhi besar nilai vektor. (Bhargava dan Shi 1998c)

2.3.4 RVEA

Algoritma VEA dan MVEA menggunakan kode rahasia untuk mengubah secara acak sign bit koefisien DCT dan vektor gerak. Algoritma tersebut memberi hasil enkripsi yang cukup dengan biaya komputasi yang minim, namun algoritma yang telah dibahas sebelumnya sangat lemah terhadap serangan menggunakan plaintext. Bagian ini akan memaparkan algoritma RVEA yang resistan terhadap serangan plaintext maupun ciphertext.

RVEA merupakan algoritma enkripsi selektif yang hanya bekerja pada signbit dari koefisien DCT dan vektor gerak. RVEA dapat menggunakan algoritma apa saja(seperti DES atau IDEA) untuk mengenkripsi bit-bit tersebut. Untuk mengilustrasikan proses operasi

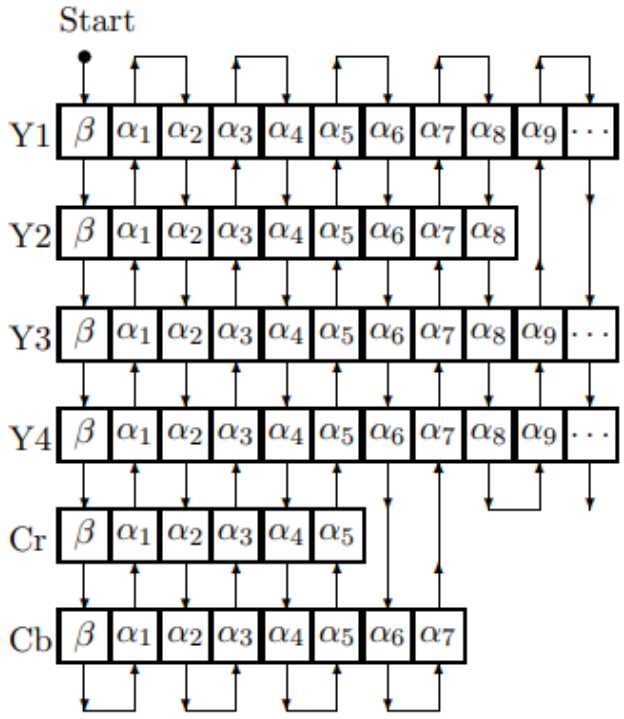
RVEA, bit lain dalam video MPEG selain signbit dapat diabaikan sehingga video MPEG S dapat dilambangkan sebagai:

$S = ...s_1...s_2...s_m...$

dimana s_i (i = 1, 2,...) merupakan signbit koefisien DCT atau vektor gerak.

Video dienkripsi slice per slice, RVEA memilih maksimum 64 sign bit(8 byte) dari setiap makroblok. blok 8 x 8 pada video MPEG dapat dilambangkan sebagai β, a_1, a_2, a_3 dimana β merupakan signbit koefisien DC, dan a_i merupakan kode koefisien AC bukan-nol ke-i.

Tiap makroblok terdiri dari enam blok 8x8, Y1, Y2, Y3, Y4, Cr dan Cb. Gambar 2.4 menunjukkan cara algoritma RVEA memilih β dan a_i dari tiap makroblok.

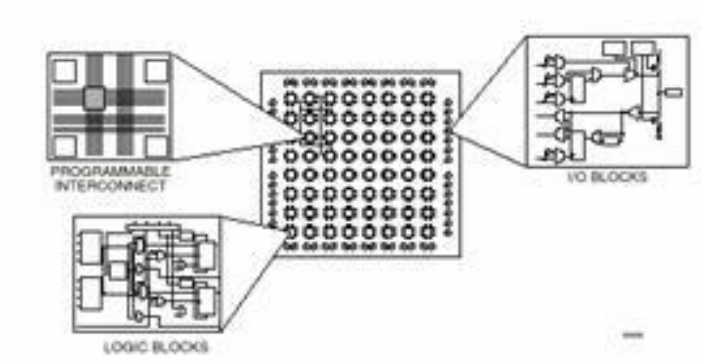


Gambar 2.4 Urutan pemilihan *signbit* algoritma RVEA

Signbit dipilih dengan cara ini sebab koefisien DC mengandung informasi yang lebih signifikan dari pada koefisien AC dan koefisien AC berfrekuensi rendah lebih signifikan dari pada koefisien AC berfrekuensi tinggi. RVEA mengurangi dan membatasi waktu komputasi dengan membatasi jumlah maksimum bit yang dipilih. *Signbit* yang dipilih selanjutnya dienkripsi/ dekripsi menggunakan algoritma enkripsi yang dipilih dan dikembalikan ke lokasi semula. operasi dekripsi RVEA sama dengan proses ekripsinya. (Bhargava dan Shi 1999)

2.4 FPGA

FPGA(*Field Programmable Gate Array*) merupakan sirkuit terintergrasi yang dapat dikonfigurasikan ulang oleh pengguna setelah proses manufaktur. FPGA terdiri dari blok blok logika yang dapat diprogram ulang, jalur interkoneksi yang menghubungkan blok blok tersebut, Blok I/O yang menghubungkan FPGA dan sirkuit eksternal, dan blok blok tambahan lainnya. Blok logika dapat dikonfigurasi untuk melakukan fungsi kombinatorial kompleks ataupun operasi sederhana seperti AND atau XOR. Blok logika juga memiliki elemen *memory* seperti flip-flop memungkinkan implementasi logika sekuensial dan *pipelining*. Jalur interkoneksi terdiri dari lajur penghubung dan *switch* yang dapat diprogram. FPGA juga dapat memiliki blok tambahan lainnya seperti blok DSP atau blok *memory* yang dapat digunakan untuk mengimplementasi modul penyimpanan seperti FIFO dan RAM.(Simpson, 2015)



Gambar 2.5 Arsitektur FPGA

2.4.1 Xilinx 7 Series

Xilinx 7 Series merupakan seri FPGA yang dirilis oleh Xilinx pada tahun 2010. Xilinx 7 Series menggunakan teknologi proses 28nm menghadirkan peningkatan performa yang signifikan dengan kapasitas hingga 2 juta sel logika dan penggunaan energy 50% lebih rendah dari generasi sebelumnya menjadikan Xilinx 7 Series alternatif ASSP dan ASIC yang dapat diprogram ulang.(Xilinx, 2020)

2.4.2 Configurable Logic Block

Configurable Logic Block(CLB) merupakan satuan blok logika yang digunakan pada Xilinx 7 series. 1 CLB terdiri dari 2 Slice, dan tiap slice memiliki 4 LUT 6-input yang dapat digunakan untuk mengimplementasikan logika kombinatorial 6 input apa saja, 8 Flip-Flop, 1 full adder, 2 Multiplexer 2-input, dan input khusus carry chain.

25% hingga 50% slice pada FPGA 7 Series(SLICE-M) dapat digunakan sebagai unit memory, memungkinkan LUT pada slice tersebut digunakan sebagai blok RAM sebesar 64x1, yang dapat dirantai bersama untuk mengimplementasikan RAM, FIFO atau *shift*

register.(Xilinx, 2016)

2.4.3 Block RAM

Blok memori pada Xilinx 7 Series memiliki ukuran 36 Kb, dengan lebar port maksimum 72 bit. Blok memori dapat dipecah menjadi 2 blok memori independen dengan ukuran 18 Kb ataupun dirangkai bersama untuk membentuk modul memori dengan ukuran atau lebar port yang lebih besar. Blok memory Xilinx 7 Series mendukung implementasi modul memori dengan clock dan lebar port input dan output yang berbeda(hingga 1:8 atau 8:1). Implementasi RAM dengan lebar 64-bit dapat menggunakan 8 bit tambahan kode Hamming yang dapat memperbaiki 1 bit error dan mendeteksi 2 bit error. (Xilinx, 2019)

2.4.4 Clock Management Tile

Clock Management Tile(Blok Managemen Clock) merupakan Blok manipulasi clock yang terdapat pada Xilinx 7 Series. Satu CMT terdiri dari 1 MMCM(*Mixed Mode Clock Manager*) dan 1 PLL(*Phase Locked Loop*). MMCM memiliki fitur tambahan dibanding PLL standar seperti inversi clock output, pengali dan pembagi fraksional, dan perubahan fase clock yang dapat diubah sesuai input.(Xilinx, 2018)