Implementasi Algoritma AES Rijndael pada Proses Enkripsi Hemat Energi Untuk Video Streaming dalam Jaringan Sensor Nirkabel

Syarifuddin
Jurusan Teknik Elektro
Fakultas Teknologi Industri
Institut Teknologi Sepuluh Nopember
Surabaya, Indonesia
gzsadp_04@yahoo.co.id

Oxy Riza Primasetiya
Jurusan Teknik Elektro
Fakultas Teknologi Industri
Institut Teknologi Sepuluh Nopember
Surabaya, Indonesia
rizaoxy@gmail.com

Wirawan
Jurusan Teknik Elektro
Fakultas Teknologi Industri
Institut Teknologi Sepuluh Nopember
Surabaya, Indonesia
wirawan@ee.its.ac.id

***Abstrak*—Enkripsi selektif untuk video streaming ditujukan dalam hal efisiensi perlindungan konten multimedia. Namun, isu gabungan optimalisasi kualitas video, perlindungan konten, dan efisiensi energi komunikasi pada Jaringan Sensor Nirkabel (JSN) belum sepenuhnya dibahas dalam literatur. Di sini diusulkan skema untuk mengoptimalkan energi dan performansi enkripsi video streaming di JSN.**

Skema ini tujukan untuk meningkatkan pemahaman tentang keamanan data pada teknologi multimedia, bagaimana enkripsi dan dekripsi bisa diimplementasikan untuk aplikasi video dalam Jaringan Sensor Nirkabel dan meningkatkan enkripsi selektif untuk H.264/AVC. Ada dua fungsi utamanya; pertama proses encoding/enkripsi stream video melalui dua proses (sekuens input video akan dikompresi terlebih dahulu dengan encoder H.264/AVC kemudian bit stream frame I dienkripsi dengan cipher blok AES. Fungsi kedua adalah mendekripsi/decoding video terenkripsi dengan mendekripsi frame I dan didekodekan dengan decoder H.264/AVC.

Simulasi percobaan menunjukkan bahwa skema enkripsi selektif ini dapat meningkatkan kualitas transmisi video secara signifikan dengan perlindungan konten dan efisiensi energi yang terjamin.

Kata kunci—AES; Enskripsi Selektif; H.264/AVC; JSN; Video Streaming

I. PENDAHULUAN

Jaringan Sensor Nirkabel (JSN) adalah sebuah kelas jaringan yang memungkinkan penggunaannya pada berbagai aplikasi potensial dalam bidang kesehatan, militer dan pemantauan lingkungan. Secara umum, jaringan ini sering digunakan untuk melakukan pengamatan dalam kondisi daerah pengamatan dan tempat pengamat berada pada posisi yang saling berjauhan, sehingga dibutuhkan media yang memadai untuk dapat mengirimkan data-data hasil suatu pengamatan. Secara umum pula, data-data hasil pengamatan tersebut ada yang berupa gambar dua dimensi maupun gambar video [1]. Khususnya Protokol Video streaming seperti MPEG-4 H.264/AVC yang sudah cukup dikenal karena aplikasinya yang luas dalam Jaringan Sensor Nirkabel.

Dalam aplikasinya, informasi inti multimedia dan konten video sangatlah sensitif pada berbagai tindak kejahatan seperti penyadapan karena gangguan trafik dan manipulasi arus media. Oleh karena itu dibutuhkan skema enkripsi yang bisa menjamin keamanannya.

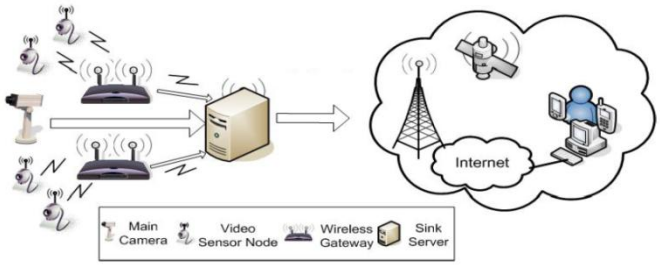
Pada penelitian ini diusulkan skema komunikasi multimedia yang aman dengan meningkatkan kualitas transmisi video, mengurangi konsumsi energi, dan menjamin keamanan. Dikarenakan terbatasnya komputasi dan sumber energi, enkripsi selektif sangat cocok untuk JSN. Alasannya pertama, enkripsi elektif bisa mengurangi beban komputasi dengan mengatur sedikit bagian dari informasi posisi dalam struktur stream multimedia. Informasi magnitude akan sia-sia dalam dekripsi tanpa informasi posisi yang benar dalam stream bit. Kedua, JSN memiliki sumber energi yang terbatas sehingga membutuhkan efisiensi energi yang tinggi dalam berkomunikasi dengan menggunakan pengalokasian sumber JSN.

II. TEORI PENUNJANG

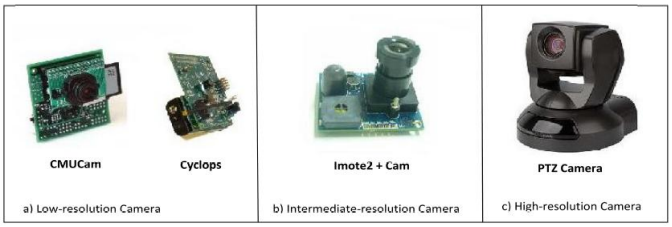
A. Video Streaming dalam JSN

Di sini akan dijelaskan tentang perangkat multimedia yang biasa digunakan dalam Jaringan Sensor Nirkabel khususnya untuk video. Dari gambar 1 terlihat bahwa konten video yang dikumpulkan oleh node sensor dikirim ke gateway wireless dan diteruskan ke sink server. Sink server bisa menyusun informasi video berdasarkan korelasi informasi dari karma utama maupun node sensor. Kemudian video akan distreamingkan hingga diterima oleh end user.

Agar bisa mengurangi sejumlah energi yang dibutuhkan dalam transmisi multimedia (gambar atau video) pada Jaringan Sensor Nirkabel, konten multimedia harus bisa diproses menggunakan kompresi yang sesuai dan algoritma-algoritma yang lain dengan baik. Oleh karena itu, sensor kamera bisa saja berpasangan dengan processor tambahan (microcontroller, DSP, FPGA, dll) dan sumber memori sebelum meneruskan data ke mote wireless untuk komunikasi nirkabel.



Gambar 1. Ilustrasi jaringan sensor multimedia nirkabel[2]



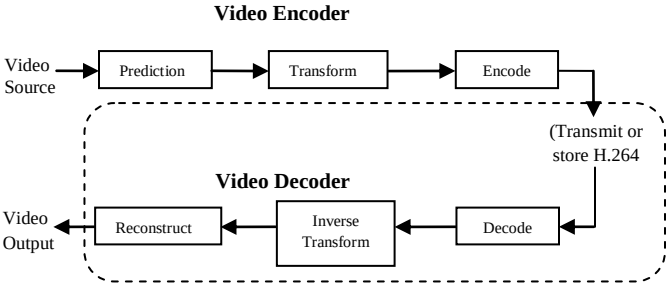
Gambar 2. Contoh node kamera sensor[3]

B. Standar Video H.264/AVC

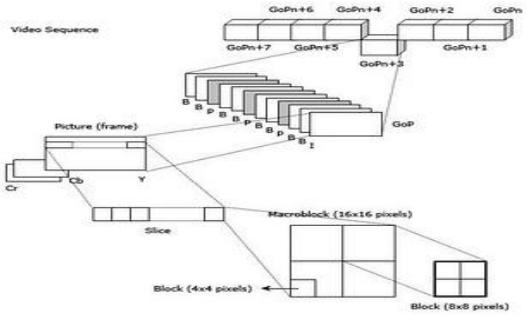
H.264 adalah suatu standar industri untuk kompresi video dimana terjadi proses konversi suatu video digital kedalam format yang berkapasitas lebih kecil ketika disimpan atau ditransmisikan. Rekomendasi H.264. *Advanced Video Coding* (AVC) adalah sebuah dokumen yang diterbitkan oleh lembaga standar internasional ITU-T (Internasional Telecommunication Union) dan ISO/IEC (International Organization for Standardization / International Electrotechnical Commission). Di dalamnya ditentukan sebuah format (*syntax*) untuk video terkompresi dan sebuah metode untuk mendekodekan *syntax* tersebut sehingga dihasilkan sekuen video. Gambar 3 dan 4 menunujukkan dan proses *encode* serta *decode* yang termasuk dalam standar H.264

Struktur tersebut adalah:

1. *Video sequence*, diawali dengan *sequence header* berisi satu group gambar atau lebih, diakhiri dengan *code end-of-sequence*
2. GoP (*Group Of Pictures*), sebuah header dan rangkaian dari satu atau beberapa gambar.
3. *Picture/Frame*, *primary coding uni*t dari *video sequence*, merepresentasikan nilai *luminance* (Y) dan *chrominance* (U dan V). Terdapat tiga tipe frame:
   - Frame I (*Intra Coded*)
   - Frame P (*Predictive Coded*)
   - Frame B (*Bi-directional Coded*)
4. *Block*, *coding unit* terkecil dapat berupa salah satu dari *luminance*, *red chrominance*, atau *blue chrominance*. Pada H.264 ukuran blok terkecil adalah 4x4 pixel.



Gambar 3. Proses Encoding dan Decoding Video



Gambar 4. Struktur Video H.264[4]

5. *Slice*, kumpulan *macroblock* dalam satu *picture*.
6. *Macroblock*, berisi MB tunggal yang terdiri dari sejumlah *block* tergantung pada struktur piksel kroma. MB merupakan *basic coding unit* dalam sebuah frame yang terdiri dari 4 *luminance*, 1 Cr dan 1 Cb.

C. Enkripsi Selektif

Dalam transmisi video digital, dibutuhkan metodologi enkripsi yang bisa melindungi video digital dari berbagai serangan selama transmisi. Dikarenakan ukuran video digital yang besar, biasanya video digital akan ditransmisi dalam format terkompresi seperti MPEG 10 atau H.264/AVC. Dengan demikian algoritma enkripsi untuk video digital selalu bekerja dalam domain kompresi. Beberapa algoritma untuk mengamankan video streaming sudah diusulkan. Kebanyakan dari algoritma-algoritma tersebut mencoba untuk mengoptimalkan proses dalam hal kecepatan enkripsi dan proses penampilan video.

Metode lain dalam enkripsi video adalah mengenkripsi byte-byte data video dengan menggunakan enkripsi simetri berbasis blok kuat seperti AES. Walaupun memiliki komputasi yang agak berat, tetapi bisa diatasi dengan metode enkripsi selektif atau mengenkripsis hanya sebagian data yang dianggap paling sensitif[5].

D. *Algoritma Enkripsi AES Rijndael*[6]

Rijndael termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan *cipher block*. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu. *Rijndael* mendukung berbagai variasi ukuran blok dan kunci yang akan digunakan. Namun *Rijndael* mempunyai ukuran blok dan kunci yang tetap sebesar 128, 192, 256 bit. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi.

Algoritma AES Rijndael mempunyai tiga parameter:

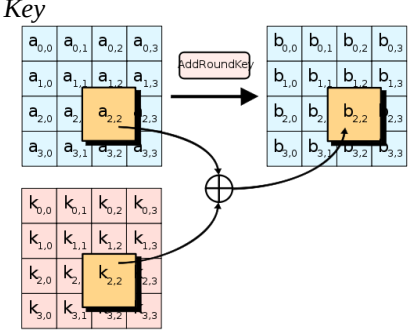
1. Plaintext: array berukuran 16 byte yang berisi data masukan
2. Chipertext: array berukuran 16 byte yang merupakan hasil enkripsi
3. Key: array 16 byte yang berisi kunci chipering (chiper key)

Key Schedule

Proses *key schedule* diperlukan untuk mendapatkan *subkey-subkey* dari kunci utama agar cukup untuk melakukan enkripsi dan dekripsi. Proses ini terdiri dari beberapa operasi, yaitu:

- Operasi *Rotate*, yaitu operasi perputaran 8 bit pada 32 bit dari kunci.
- Operasi *SubBytes*
- Operasi *Rcon*. Nilai-nilai dari *Rcon* kemudian akan di-XOR dengan hasil operasi *SubBytes*.
- Operasi XOR dengan w[i-Nk] yaitu word yang berada pada Nk sebelumnya.

Add Round Key



Gambar 5. Proses Add Round Key

Pada proses ini *subkey* digabungkan dengan *state*. Proses penggabungan ini menggunakan operasi XOR untuk setiap byte dari *subkey* dengan byte yang bersangkutan dari *state*. Untuk setiap tahap, *subkey* dibangkitkan dari kunci utama dengan menggunakan proses *key schedule*. Setiap *subkey* berukuran sama dengan *state* yang bersangkutan.

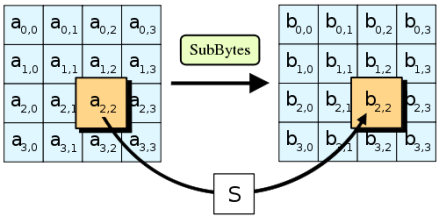
SubBytes

Proses *SubBytes* adalah operasi yang akan melakukan substitusi tidak linear dengan cara mengganti setiap *byte state* dengan *byte* pada sebuah tabel yang dinamakan tabel SBox.

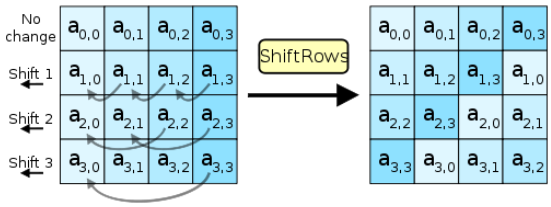
Sebuah tabel S-Box terdiri dari 16x16 baris dan kolom dengan masing-masing berukuran 1 *byte*.

Shift Rows

Proses *Shift Rows* akan beroperasi pada tiap baris dari tabel *state*. Proses iniakan bekerja dengan cara memutar *byte-byte* pada 3 baris terakhir (baris 1, 2, dan 3) dengan jumlah perputaran yang berbeda-beda. Baris 1 akan diputar sebanyak 1 kali, baris 2 akan diputar sebanyak 2 kali, dan baris 3 akan diputar sebanyak 3 kali. Sedangkan baris 0 tidak akan diputar. Proses *ShiftRows* diperlihatkan pada Gambar 7.

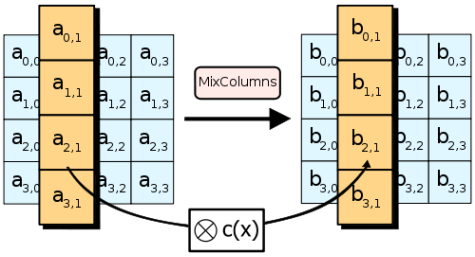


Gambar 6. Proses *sub bytes*



Gambar 7. Proses *shift rows*.

MixColumns



Gambar 8. Proses *mix columns*

Operasi ini menggabungkan 4 *bytes* dari setiap kolom tabel *state* dan menggunakan transformasi linier. Operasi *Mix Columns* memperlakukan setiap kolom sebagai polinomial 4 suku dalam *Galois field*. Operasi *MixColumns* juga dapat dipandang sebagai perkalian matrix.

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Operasi penjumlahan di atas dilakukan dengan operasi XOR, sedangkan operasi perkalian dilakukan dalam *Galois field*.

D. PSNR (Peak Signal To Noise Ratio)

PSNR adalah metrik yang umum digunakan untuk mengukur kualitas citra atau video secara objektif.

$$PSNR = 10\log_{10}\left[\frac{255^2}{[MSE(Y)+MSE(U)+MSE(V)]}\right] \quad (1)$$

$$MSE = \frac{1}{N}\sum_i \sum_j \left(Y_{ref}(i,j) - Y_{prc}(i,j)\right)^2 \quad (2)$$

Dimana:

$Y_{ref}(i,j)$ = nilai-nilai pixel dari frame referensi
$Y_{prc}(i,j)$ = nilai-nilai pixel dari frame yang diproses
N = jumlah total pixel dalam frame

III. PERENCANAAN DAN SIMULASI SISTEM

Dalam penelitian ini perancangan sistem secara umum seperti blok diagram pada Gambar 9

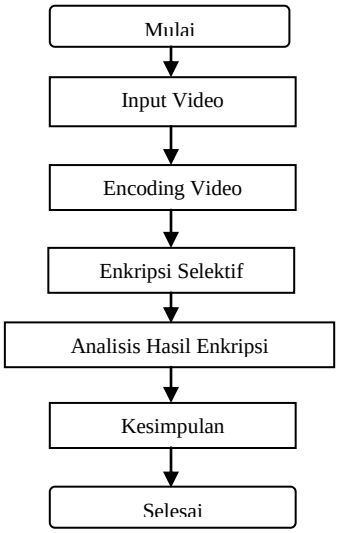
A. Perangkat Penelitian

a. *Hardware*

CPU Test Platform: Intel® Core™2 CPU T5200 @1.6 GHz, 3 GB of RAM.

b. *Software*

- Matlab R2008a
- JM-14.2
- Microsoft Visual Studio 2005
- Elecard software: Elecard Stream Eye dan Elecard Stream Analyzer
- YUV-player



Gambar 9. Diagram Blok Perancangan Sistem

TABLE I. PARAMETER INPUT

Input source video	Foreman
Width	176
Height	144
Total frame	19
Frame rate	30 fps
Quantization Parameter	24, 28, 32
Format chroma video	4:2:0

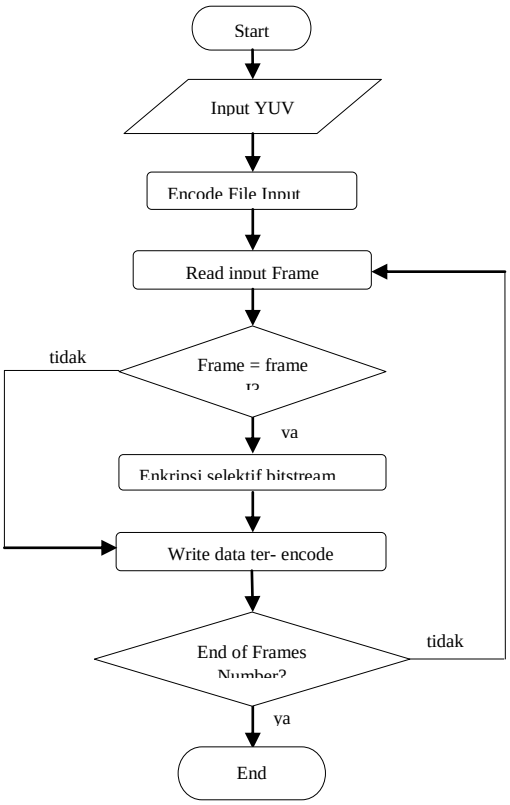
B. Pengkodean Video

Proses pengkodean/kompresi video menggunakan *Joint Model* (JM) versi 14.2 manual *software* referensi dari H.264/AVC, berupa source code C++ yang dikompilasi dengan Microsoft Visual Studio 2005. Software JM ini terdiri dari encoder dan *decoder* yang dikenal dengan Codec.

C. Penerapan Enkripsi Selektif

Pada tahap enkripsi ini dilakukan beberapa operasi sesuai algoritma Rijndael. Initiate State yang telah ditentukan akan dijadikan sebagai input atau plaintext. Setelah dijalankan dengan program Matlab akan dihasilkan state akhir dengan ukuran yang sama dengan initate state yaitu 16 byte. State akhir ini yang disebut ciphertext yang akan dimasukkan kembali dalam bitsream frame I dengan mengganti 16 byte plaintext sebelumnya.

Gambar 10 adalah diagram alir penerapan enkripsi selektif pada Penelitian ini.



Gambar 10. Diagram Alir Enkripsi Selektif

D. Kebutuhan Energi

Encryption budget akan dihitung berdasarkan kebutuhan bit pada setiap plaintext yang decipher. Setiap perubahan dari byte Hex akan dikonversi kedalam biner. Sedangkan Perhitungan besar operasi algoritma AES ini diperlihatkan oleh *Round Transformation* sesuai gambar 11

```
Round (State, RoundKey) {
SubBytes (State);
ShiftRows (State);
MixColoumns (State);
AddRoundKey (State, RoundKey);
}
```

(a)

```
FinalRound (State, RoundKey) {
SubBytes (State);
ShiftRows (State);
AddRoundKey (State, RoundKey);
}
```

(b)

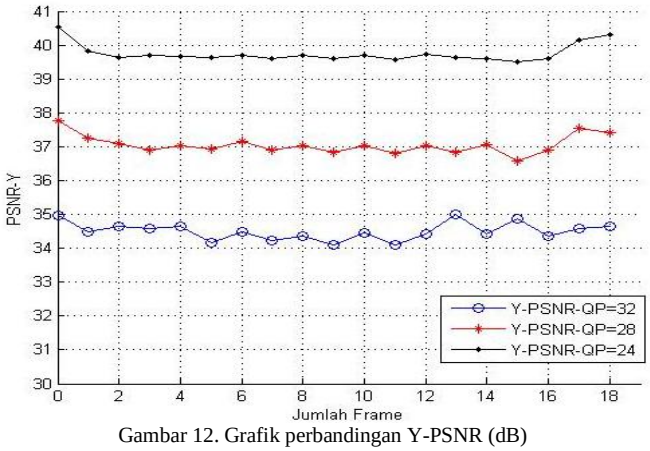
Gambar 11. (a) Empat *Round Transformations*
(b) *Final Round*

IV. ANALISA DATA DAN PEMBAHASAN

A. Hasil Pengkodean H.264/AVC

TABLE II. PERBANDINGAN HASIL KOMPRESI

Parameter	Foreman		
	QP		
	24	28	32
Encoding time (sec)	202.811	211.645	197.467
Total bit	178696	110912	69320
Bit rate (kbps)	141.08	87.56	54.73
Average Y-PSNR (dB)	39.75	37.06	34.40
Size (kb)	22	14	9



Gambar 12. Grafik perbandingan Y-PSNR (dB)
Foreman antara QP=24, 28 dan 32

Sebuah teknik kompresi memiliki kinerja yang baik ketika menghasilkan nilai rasio kompresi yang besar. Hasil kompresi dengan kualitas terbaik pada QP = 32. Jadi, semakin besar nilai parameter quantisasi maka semakin besar nilai rasio kompresi yang diperoleh.

Dari grafik pada Gambar 12 dapat dilihat bahwa semakin besar nilai QP maka nilai PSNR semakin kecil. Pengkodean dikatakan semakin bagus terbukti dengan semakin kecilnya ukuran file output yang dihasilkan. Namun, dengan semakin bagusnya pengkodean menyebabkan nilai PSNR semakin kecil dan kondisi ini akan semakin rentan terhadap pengaruh error.

B. Analisis Enkripsi Selektif

Sebelum dienkrisi, posisi frame I akan ditentukan terlebih dahulu. Objek video pada pengujian ini menggunakan dua frame I (satu GoP) untuk mempermudah pengalokasian frame I nya. Pada tahap enkripsi selektif ini dari 19 frame video terkompresi yang ada hanya dua frame yang di-*cipher* yakni frame I sedangkan frame selain I tidak di-*cipher*.

Dari gambar 14 bisa dilihat bahwa dengan mencipher sebagian dari bitstream frame I bisa mengakibatkan rusaknya video tersebut karena error nya bit informasi dalam frame I. Error ini ditandai dengan sulitnya frame tersebut dikenali. Efek ini semakin terlihat dimana frame P maupun frame B ikut rusak karena kedua frame ini mereferensi frame I. Dengan kata lain, dengan rusaknya frame I maka keseluruhan video akan rusak dan dampaknya tidak akan bisa didekodekan. Dari sini bisa diambil sebuah kesimpulan bahwa dengan mengubah sejumlah bit bisa mengakibatkan desinkronisasi bitstream dan lebih jauh lagi bisa mengakibatkan cacat visual pada video bila dilakukan pada frame I.

Plaintext

4C	0A	DC	28
5A	06	11	58
DF	27	FD	41
A0	3E	CA	FD

(a)

Ciphertext

D4	5A	2C	54
D4	9A	9F	93
81	E5	B9	06
C6	E8	2B	36

(b)

Gambar 13. Hasil Ciphering (a) plaintext 1,
(b) Ciphertext 1

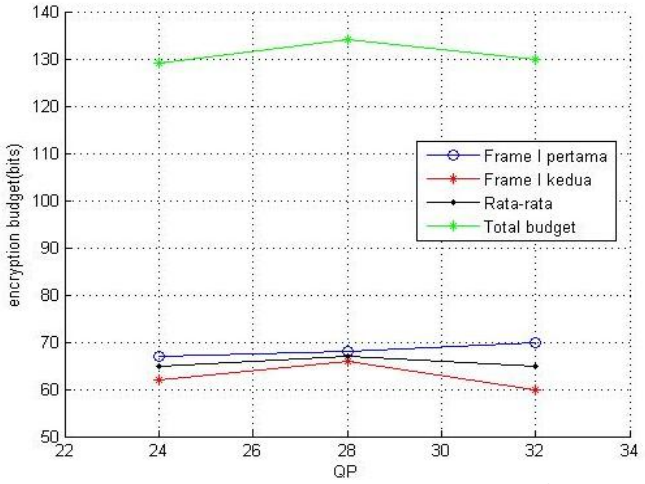
(a)

(b)

(c)

Gambar 14. Perbandingan (a) frame I, (b) frame P, dan (c) frame B sebelum dan setelah frame I dienkripsi selektif

Gambar 15 Video foreman setelah di-*decode*



Gambar 16. *Encryption Bugdet* (Bits) metode selektif

TABLE III. PERBANDINGAN HASIL *DECODE*

Objek YUV	SNR-Y (dB)	Total Decoding Time
Sebelum Transmisi	35,25	2,128
Setelah Transmisi	26,87	2,483

Dari gambar 15 terlihat bahwa ketika telah sampai di penerima yang sah –yang memiliki kunci simeteris-, video yang dikirim ini mengalami beberapa *error* pixel di beberapa bagian. Hal ini menandakan bahwa dalam transmisinya, video terkompresi tersebut mengalami desinkronisasi di udara. Dari tabel tersebut bisa dijelaskan bahwa terjadi penurunan kualitas video ter-decode setelah ditransmisikan.

C. Analisis Kebutuhan Energi

Pada metode selektif dalam penelitian ini membutuhkan rata-rata *Encryption Bugdet* sebesar 66 bit untuk setiap plaintext yang dicipher. Sesuai informasi pada tabel 5 setidaknya terdapat plaintext sejumlah 1396 dan 866 untuk metode konvensional pada kompresi QP 24 dan QP 32. Juga plaintext sejumlah 541 pada kompresi QP 32. Sesuai budget untuk setiap plaintext dari gambar 16, maka untuk metode konvensional, *total encryption budget*-nya:

QP 24= 1396 x 66 bits = 92136 bits
QP 28= 866 x 66 bits = 57156 bits
QP 32= 541 x 66 bits = 35706 bits

TABLE IV. OPERASI ALGORITMA AES

No	Round	Transformasi State	Perulangan	Total Transformasi
1	Initial Round	1	1	1
2	9 Rounds	4	9	36
3	Final Round	3	1	3
Jumlah Operasi				40

TABLE V. PERBANDINGAN JUMLAH OPERASI ENKRIPSI SELEKTIF DENGAN ENKRIPSI KONVENSIONAL

Enkripsi	Selektif			Konvensional		
	24	28	32	24	28	32
Frame Terenkripsi	2	2	2	19	19	19
Jumlah Plaintext	2	2	2	1396	866	541
Total Byte Terenkripsi	32	32	32	22336	13856	8656
Jumlah Operasi	80	80	80	55840	34640	21640

Selanjutnya jika efisiensi metode selektif ini dilihat dari jumlah operasinya, maka untuk setiap 16 byte, jumlah operasi algoritma ini ditunjukkan oleh tabel 5

Dengan jumlah frame yang sama metode selektif hanya membutuhkan 80 operasi untuk setiap QP. Sedangkan metode konvensional membutuhkan jumlah operasi yang kauh lebih besar. Nilai perbandingan antara operasi Enkripsi Selektif dibandingkan dengan Enkripsi Konvensional sebagai berikut

QP 24 = 80 : 55840 = 0.0014 atau 1 : 698
QP 28 = 80 : 34640 = 0.0023 atau 1 : 433
QP 32 = 80 : 21640 = 0.0036 atau 1 : 270

Dengan demikian terlihat jelas bahwa dengan metode enkripsi selektif yang digunakan pada penelitian ini bisa memberikan penghematan yang besar dalam streaming suatu video

V. KESIMPULAN

Berdasarkan analisis simulasi dan pengujian pada penelitian ini, bisa diambil beberapa kesimpulan:

1. Semakin besar nilai Quantization Parameter, maka semakin tinggi pula hasil kompresi yang dihasilkan. Namun nilai PSNR nya semakin menurun yang bisa mengakibatkan rendahnya kualitas video dengan bitrate yang kecil.
2. Penggunaan AlgoritmaEnkripsi AES pada video streaming ini bisa memberikan keamanan video terkompresi dengan baik. Hal ini terlihat dari perubahan struktur video H.264/AVC dengan kunci 128 bit yang video sulit untuk dikenali (unreadable), namun tidak menurunkan kualitas video dimana menghasilkan Y-SNR video sebesar 26,87 dB setelah transmisi
3. Metode enkripsi selektif pada frame I dimana menjadi dasar referensi dari frame P dan frame B, bisa mengurangi beban komputasi dengan penurunan yang cukup signifikan. Hal ini juga menandakan besarnya penghematan energi yang bisa diberikan oleh skema enkripsi selektif ini.
4. Dengan adanya jaminan keamanan dan penghematan energi yang tinggi dalam transmisi yang dapat diberikan, metode Enkripsi Selektif ini bisa diterapkan di Jaringan sensor Nirkabel

DAFTAR PUSTAKA

[1] I. Politis, M. Tsagkaropoulos, S. Kotsopoulos, "*Optimizing Video Transmission over Wireless Multimedia Sensor Networks*", GLOBECOM 117-122, 2008

[2] Zhuo Xue, K.K. Loo, J. Cosmas, P.Y. Yip, "*Distributed Video Coding in Wireless Multimedia Sensor Network for Multimedia Broadcasting*", WSEAS Transactions On Communications, 2008

[3] I. T. Almalkawi, M. G. Zapata, J. N. Al-Karaki, and J. Morillo-Pozo 1, "*Wireless Multimedia Sensor Networks: Current Trends and Future Directions*", Sensors, 2010

[4] J.C Ikuno, M. Rupp, "*Performance of an Error Detection Mechanism for Damaged H. 264/AVC Sequences*", Master Thesis, Vienna University of Technology, 2007.

[5] M. Abomhara, Omar Zakaria, Othman O. Khalifa, A.A Zaidan, B.B Zaidan., "*Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard*", International Journal of Computer Theory and Engineering, Vol. 2, No. 2 April, 2010

[6] FIPS PUB 197, "*Advanced Encryption Standard (AES)*", National Institute of Standards and Technology, U.S. Department of Commerce, November 2001.