IMPLEMENTASI ALGORITMA CHAOTIC DISKRET 128 BIT UNTUK KRIPTOGRAFI SINYAL SUARA BERBASIS FPGA SPARTAN-3 DAN BAHASA PEMROGRAMAN VHDL

Natanael Pandapotan[*)], Munawar Agus Riyadi, and Teguh Prakoso

Jurusan Teknik Elektro, Universitas Diponegoro Semarang
Jl. Prof. Sudharto, SH, Kampus UNDIP Tembalang, Semarang 50275, Indonesia

[*)] *Email :natanaelpandapotan@gmail.com*

Abstrak

Penggunaan layanan komunikasi suara terus berkembang baik pada saluran analog (telepon) maupun saluran digital (Selular dan VoIP). Saluran tersebut digunakan untuk pertukaran informasi yang bersifat sensitif dan rahasia seperti pada bidang militer, pemerintahan, bahkan transaksi keuangan. Kriptografi dibutuhkan sebagai sistem pengaman informasi untuk mengacak pesan suara yang dikirimkan. Pada penelitian membahas algoritma kriptografi Chaotic 128 bit dengan mode *Cipher Feedback*. Algoritma kriptografi ini diimplementasikan pada FPGA karena dinilai memiliki kecepatan proses tinggi dan waktu tunda rendah yang dibutuhkan untuk komunikasi suara. Perancangan sistem kriptografi ini ditanamkan pada dua buah FPGA yang masing-masing berfungsi sebagai pengirim sekaligus proses enkripsi dan yang lain sebagai penerima sekaligus proses dekripsi. Pengujian dan analisa dilakukan pada empat kondisi yaitu: enkripsi *off* - dekripsi *off*, enkripsi *on* - dekripsi *on*, enkripsi *on* - dekripsi *off*, enkripsi *off* - dekripsi *on*. Hasil pengujian menunjukkan sistem bekerja dengan baik dan berhasil melakukan proses enkripsi. Sistem juga dapat mengembalikan informasi asli dengan proses dekripsi. Didapat nilai rata-rata parameter MSE, waktu tunda, dan THD-N untuk kondisi *off-off* masing-masing adalah 0,3513 V^2, 202 μs, dan 17,52 %. Sedangkan untuk kondisi *on-on* didapatkan nilai rata-rata MSE 0,3794 V^2, waktu tunda 202 μs, dan THD-N 20,45%.
Kata kunci : Komunikasi Suara, Kriptografi, Chaotic, FPGA

Abstract

The use of voice communications services continues to grow both in analogue channels (telephone) also digital channels (Mobile and VoIP). The channel is used to exchange sensitive and confidential information such as in the military, government, even financial transactions. Cryptography is needed as a information safety system to scramble sent voice messages. This study discusses 128 bit Chaotic cryptographic algorithm with Cipher Feedback mode. The Cryptographic algorithm was implemented on FPGA because it is considered to have a high processing speed and low delay required for voice communication. The design of the cryptographic system was implanted on two FPGA, each of which serves as transmitter once encryption process and the other as receiver once decryption process. Testing and analysis were performed on four conditions, namely: the encryption off - decryption off, the encryption on - decryption on, the encryption on - decryption off, encryption off - decryption on. The test results show system work well and successfully perform the encryption process. It could restore the original information with the decryption process. Average values of MSE, delay, and THD-N parameters to the condition off-off obtained are 0.3513 V^2, 202 μs, and 17.52% respectively. As for the conditions of on-on the average values obtained are MSE 0.3794 V^2, delay 202 μs, and THD-N 20.45%.

Keyword: Voice communications, Cryptography, Chaotic, FPGA

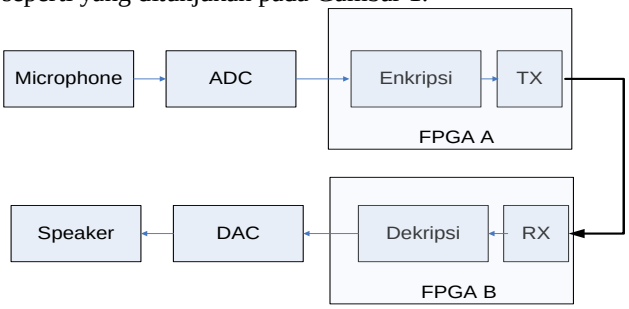
1. Pendahuluan

Komunikasi aman untuk informasi yang bersifat sensitif menjadi hal yang sangat diperlukan pada bidang militer, institusi pemerintahan, sektor bisnis, bahkan urusan pribadi. Panggilan suara adalah contoh komunikasi yang terus berkembang baik itu berupa saluran analog (telepon) ataupun digital (seluler dan VoIP). Kecepatan dan kapasitas saluran terus ditingkatkan seiring dengan penggunaannya yang semakin luas. Bukan hanya untuk percakapan semata namun berbagai informasi penting seperti transaksi bisnis, panggilan darurat dan lainnya dilewatkan pada saluran ini[1].Kriptorafi dibutuhkan sebagai sistem pengaman informasi untuk mengacak

pesan yang dikirimkan melewati saluran komunikasi tersebut. Chaotic adalah algoritma yang dibangkitkan dari persamaan acak dan memiliki sifat peka terhadap kondisi awal, sedikit saja nilai awal berubah maka ciphertext yang dihasilkan akan berbeda signifikan[4]. Chaotic merupakan jenis algoritma enkripsi stream cipher dan mulai menjadi perhatian karena dianggap sesuai untuk data-data yang bersifat real time. Algoritma lain seperti AES, DES, dan RSA tidak cocok untuk enkripsi data real time karena cipher ini memerlukan waktu komputasi yang besar dan daya komputasi tinggi[5].Penelitian kirptografi dengan algoritma chaotic pernah dilakukan oleh N.K. Pareek, Vinod Patidar, dan K.K. Sud dengan judul "Discrete chaotic cryptography using external key"[6]. Selain itu penelitian lain oleh Emad Mosa, Nagy W. Messiha, dan Osama Zahran menjelaskan mengenai enkripsi sinyal suara dengan algoritma chaotic dan kelebihannya[7].

2. Metode

Sistem kriptografi pada penelitian ini akan dirancang pada dua buah FPGA yang masing-masing berfungsi sebagai pengirim sekaligus melakukan proses enkripsi dan sisi yang lain sebagai penerima dan sekaligus proses dekripsi seperti yang ditunjukan pada Gambar 1.



Gambar 1 Blok Perancangan Sistem

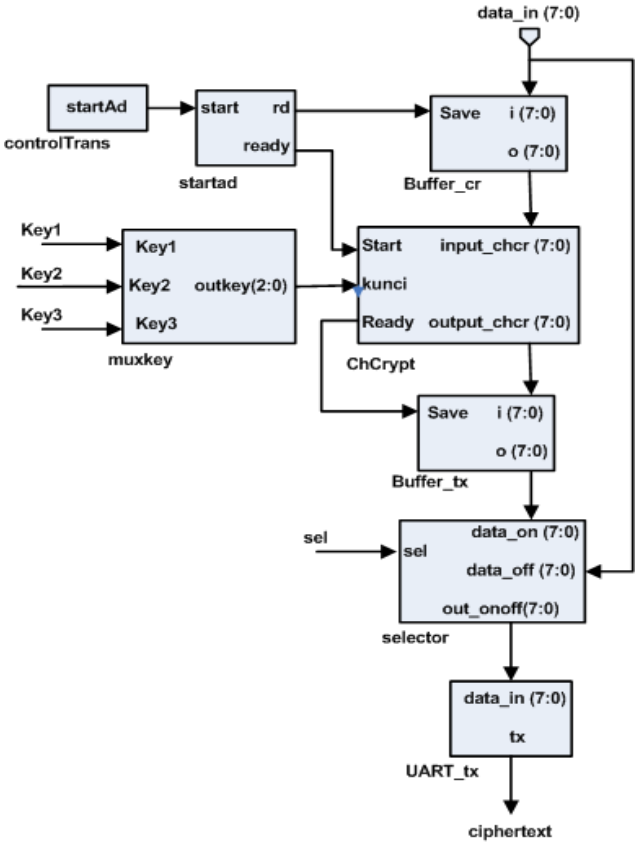
Data hasil enkripsi akan diubah menjadi data serial untuk dikirimkan melalui pin Tx pada FPGA A menuju pin Rx pada FPGA B melalui sebuah kabel. Antarmuka pada sisi pengirim berupa mikrofon dan ADC yang berfungsi untuk menangkap sinyal suara dan mengkonversinya menjadi data digital. Sedangkan pada bagian penerima DAC dan pengeras suara digunakan untuk mengubah data digital keluaran FPGA menjadi sinyal analog dan diteruskan ke pengeras suara.

2.1 Perancangan Sistem Digital FPGA

Sistem digital adalah program yang akan ditanamkan ke dalam FPGA Spartan-3 sebagai papan eksekusi dari proses enkripsi dan dekripsi. Perancangan sistem digital ini dilakukan pada perangkat lunak Xilinx ISE Design Suite 14.6. Selain mengerjaskan proses enkripsi-dekripsi, sistem digital juga berfungsi mengatur komunikasi serial antara FPGA A dan FPGA B.

2.1.1 Blok Pengirim

Blok pengirim adalah sistem digital yang ditanamkan pada FPGA A yang berfungsi sebagai antarmuka dengan ADC. Masukan dari FPGA A adalah data paralel 8 bit yang diterima dari ADC. Data masukan ini akan disampling oleh *clock* sebesar 25KHz yang bersumber dari FPGA.Masukan pin `key1`, `key2`, dan `key3` digunakan untuk memilih kunci yang akan digunakan untuk proses enkripsi pada blok `ChCrypt` seperti yang ditunjukkan pada Gambar 2. Masing-masing kunci ini dihubungkan dengan *switch selector* pada FPGA yang dapat memberikan masukan nilai '1' atau '0'. Nilai ini akan diolah dalam blok multiplexer untuk menghasilkan sebuah inisial data dengan panjang 3 bit.



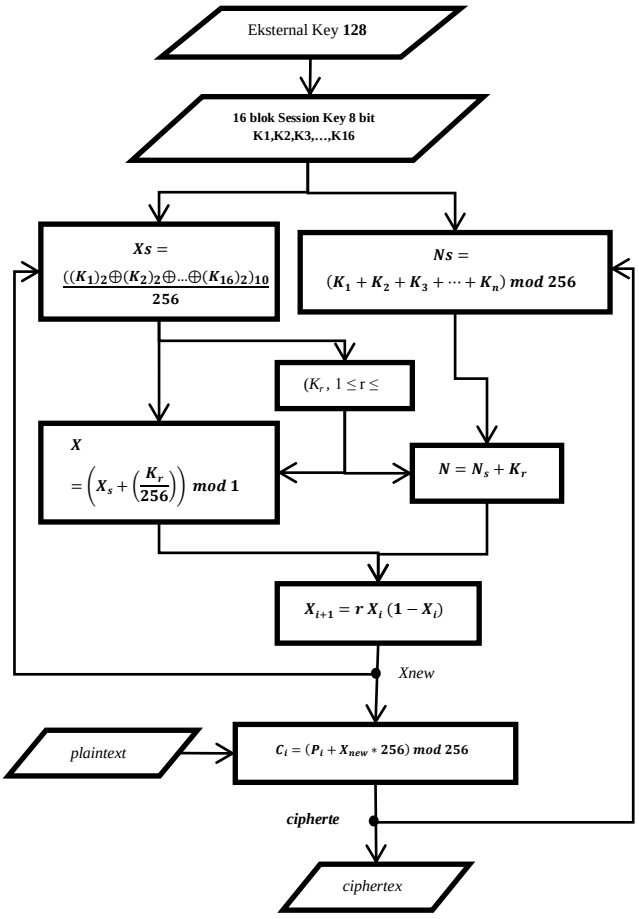
Gambar 2 Penyederhanaan RTL Blok Pengirim

Perancangan sistem pengirim dibuat ke dalam dua kondisi yang bergantung pada masukan pin `sel`. Jika *selector* `sel` bernilai '1' maka kondisi sistem dalam keadaan *on*, artinya data masukan akan diproses dalam blok `ChCrypt`. Jika pin `sel` '0' yang berarti kondisi *off*, maka data masukan akan langsung diubah menjadi data serial dan dikirimkan oleh blok `UART`. `Buffer_cr` dan `buffer_tx` adalah blok yang akan menyimpan sementara data hasil proses enkripsi dan data masukan hingga blok tersebut mendapatkan sinyal `ready` dari blok `ChCrypt` dan blok `startad`.Komponen

controlTrans dan startad. Blok tersebut berfungsi sebagai penghubung antara masukan dari ADC dan blok enkripsi. Komponen controlTrans berfungsi sebagai pewaktu, komponen ini menghitung dari 0 sampai 1000 kemudian mengirimkan sinyal start_AD ke komponen startad. Komponen startad berfungsi memberikan tundaan setelah mendapat sinyal start_AD. Setelah waktu tunda selesai komponen startad mengirim sinyal rd ke buffer_cr.

2.1.2 Blok Enkripsi

Blok enkripsi menggunakan algoritma chaotic dengan panjang kunci rahasia 128 bit yang dibagi menjadi blok berukuran 8 bit yang disebut dengan *session key*. Masukan *plaintext* akan ditambahkan langsung dengan *pad* (urutan kunci rahasia yang dibangkitkan dengan *session key*) untuk menghasilkan *ciphertext*. Algoritma pada Gambar 3 disebut *The Advanced Cipher* karena menggunakan mekanisme *feedback* dalam sistem. Pada proses kriptografi selanjutnya nilai dari *Xnew* akan diumpanbalikkan menjadi Xs sedangkan *ciphertext* diumpanbalikkan menjadi Ns dimana keduanya merupakan *initial parameter*.

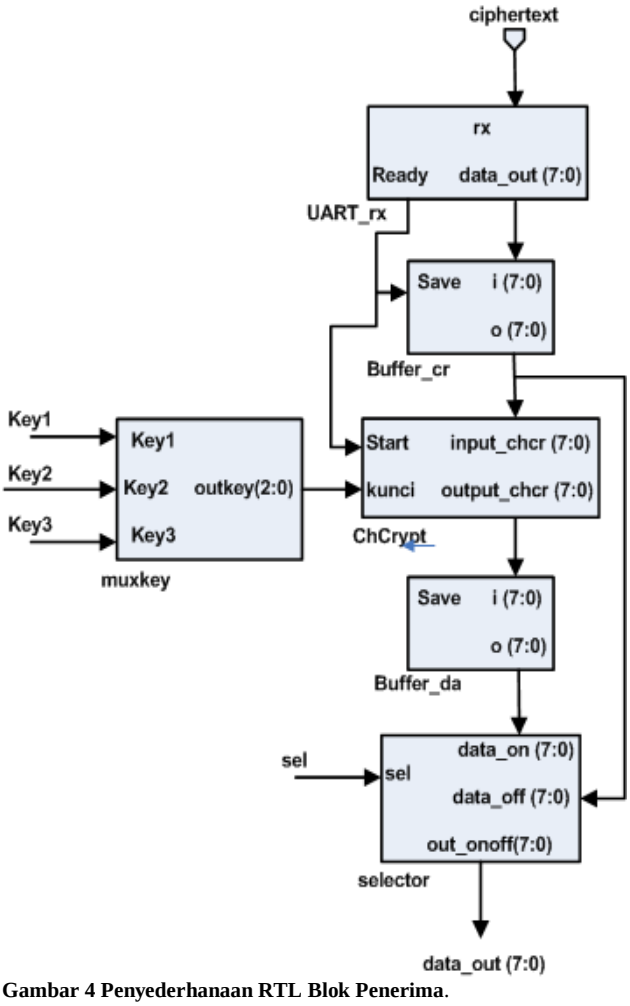


Gambar 3 Algortima Enkripsi Chaotic

2.1.3 Blok Penerima

Blok penerima ditanamkan pada FPGA B yang berfungsi untuk menerima dan mengubah data serial dari FPGA A menjadi data paralel untuk selanjutnya dilakukan proses dekripsi. Gambar 4 menunjukkan komponen penyusun dari blok penerima. Komponen hampir sama dengan blok pengirim hanya saja alur prosesnya mengalami pembalikan. Masukan *ciphertext* yang diterima oleh pin rx merupakan data serial yang dikirimkan oleh blok pengirim melalui sebuah kabel. Pada blok UART terjadi pengubahan data serial menjadi data paralel 8 bit yang akan menjadi data masukan pada proses dekripsi. Namun sebelumnya data ini akan disimpan sementara pada blok buffer_cr hingga blok tersebut menerima sinyal ready dari blok UART.

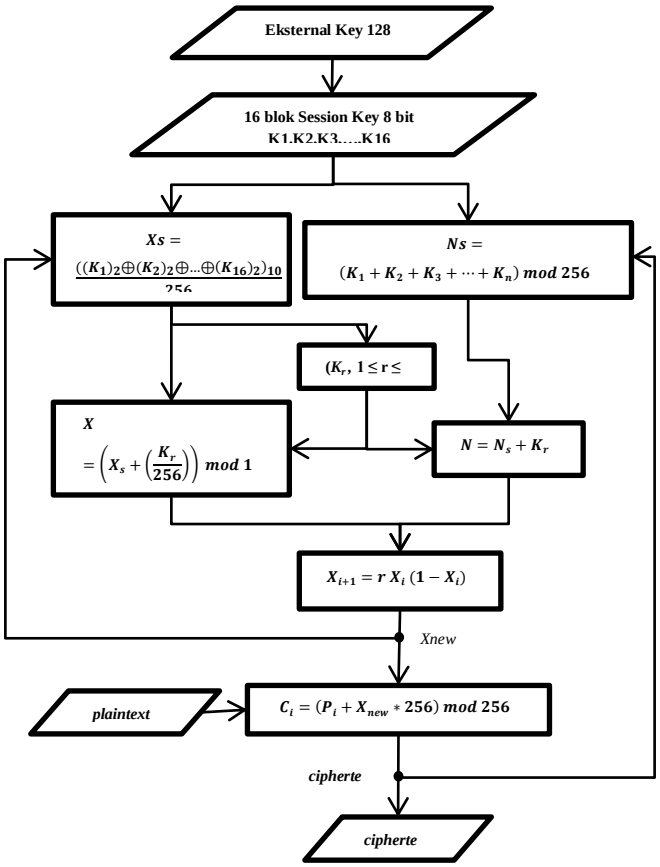
Pada blok ini juga dirancang dua kondisi yaitu dekripsi *on* dan dekripsi *off*. Kondisi tersebut ditentukan pada blok selector dan bergantung pada masukan pin sel. Kondisi pertama adalah dekripsi *on*, kodisi ini terjadi bila pin sel bernilai '1'. Tapi jika sel bernilai '0' maka proses dekripsi akan dalam kondisi *off*.



Gambar 4 Penyederhanaan RTL Blok Penerima.

2.1.4 Blok Dekripsi

Blok dekripsi dengan menggunakan algoritma chaotic memiliki alur yang hampir sama dengan proses enkripsinya yang membedakan hanya pada perhitungan calc_cipi. Dekripsi dengan panjang kunci rahasia 128 bit yang dibagi menjadi blok berukuran 8 bit yang disebut dengan *session key*. Masukan data *ciphertext* paralel akan dikurangkan langsung dengan *pad* (urutan kunci rahasia yang dibangkitkan dengan *session key*) untuk menghasilkan kembali pesan asal atau *plaintext*. Gambar 5 adalah algoritma dekripsi chaotic yang terdapat dalam blok ChCrypt dekripsi yang ditanamkan pada FPGA B. Jika dibandingkan dengan algoritma enkripsinya, maka dapat dilihat bahwa proses dekripsi memiliki langkah dan perhitungan yang hampir sama. Perbedaan hanya pada perhitungan *ciphertext/plaintext.*



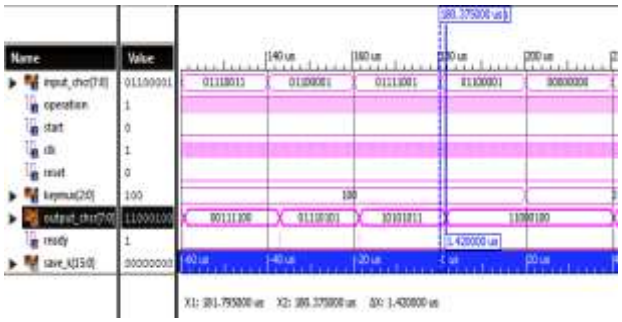
Gambar 5 Algortima Dekripsi Chaotic

3. Hasil dan Analisa

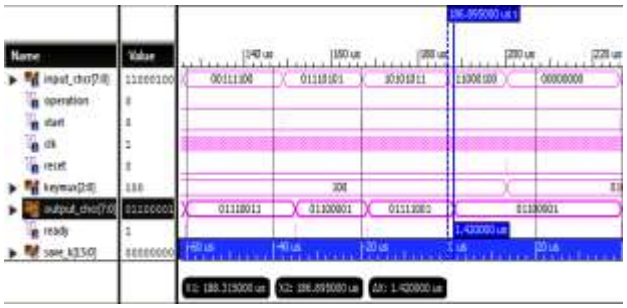
Pengujian simulasi dengan *testbench* pada perangkat lunak Xilinx ISE 14.6 untuk melihat keluaran dari sistem atas masukan tertentu. Pengujian secara langsung menggunakan sinyal sinus dengan variasi frekuensi 500, 1000, 2000, dan 34000 Hz oleh bantuan perangkat lunak *Frequency Generator* dan rekaman pidato. Keempat frekuensi dipilih berdasarkan pada rentang frekuensi yang digunakan untuk percakapan pada saluran telepon.

3.1 Pengujian Blok Enkripsi dan Dekripsi

Gambar 6 memperlihatkan masukan "01100001" dienkripsi menjadi *ciphertext* "11101000" dengan kunci `muxkey` "100". Dapat dilihat juga untuk data dan kunci yang sama dapat menghasilkan *ciphertext* yang berbeda seperti pada tabel 1. Gambar 7 menunjukkan hasil dekripsi dengan masukan berupa *ciphertext* dan menghasilkan *plaintext* seperti pada tabel 2.



Gambar 6 *Testbench* blok Encryption



Gambar 7 *Testbench* blok Decryption

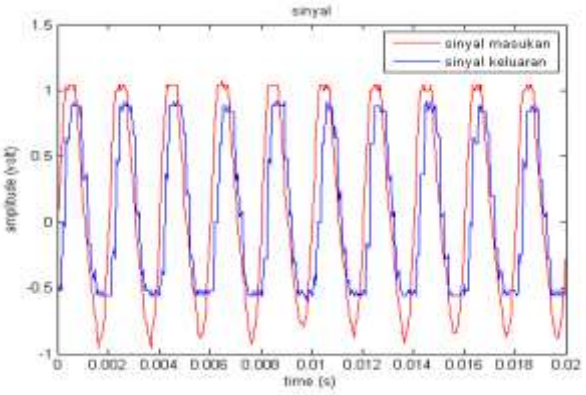
Tabel 1 Masukan input_chcr dan Keluaran output_chcr Blok Encryption

Input_chcr		Output_chcr		muxkey
Biner	*Hex*	Biner	*Hex*	
01110011	73	00111100	3c	100
01100001	61	01110101	75	100
01111001	79	10101011	ab	100
01100001	61	11000100	4c	100

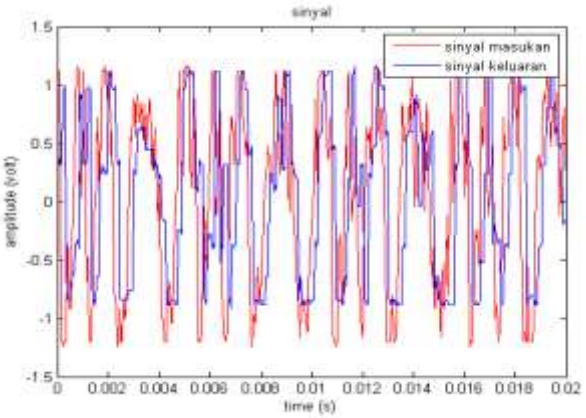
Tabel 2 Masukan input_chcr dan Keluaran output_chcr Blok Decryption

Input_chcr		Output_chcr		muxkey
Biner	*Hex*	Biner	*Hex*	
00111100	3c	01110011	73	100
01110101	75	01100001	61	100
10101011	Ab	01111001	79	100
11000100	4c	01100001	61	100

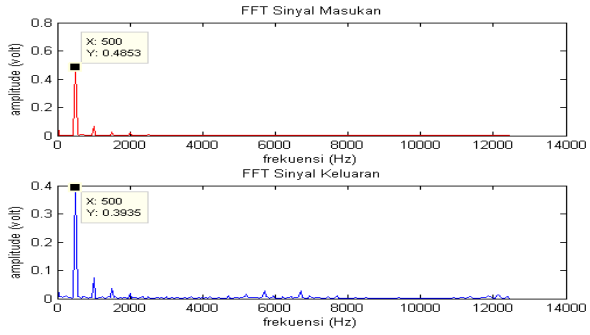
3.2 Pengujian Sistem dengan Suara



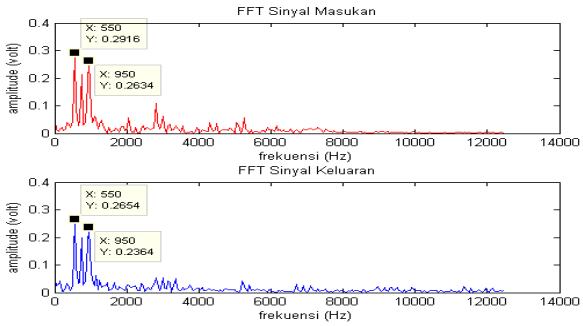
Gambar 8 Sinyal Masukan dan Keluaran Frekuensi 500 Hz Kondisi *Off-off*



Gambar 9 Sinyal *Specch* Kondisi *Off-off*



Gambar 10 FFT Sinyal Frekuensi 500 Hz Kondisi *Off-off*



Gambar 11 FFT Sinyal *Speech* Kondisi *Off-off*

Pada pengujian ini, sistem diberi masukan suara melalui mikropon. Hasil keluaran sistem diambil pada port keluaran DAC. Frekuensi telepon berkisar antara 300Hz-3400Hz, oleh karena itu pada pengujian diberi sinyal masukan dengan variasi frekuensi 500Hz, 1KHz, 2KHz, 3.4KHz dan rekaman orang berpidato. Pembangkitan suara menggunakan aplikasi *frequency generato*r pada smartphone android. Sehingga dapat diatur frekuensi yang diinginkan.

Gambar 8 dan 9 menunjukkan sinyal masukan dan keluaran untuk sinyal 500 Hz dan rekaman pidato. Dapat dilihat bahwa sinyal keluaran berwarna biru tertinggal dari sinyal masukan berwarna merah. Selisih waktu tunda tersebut menunjukkan waktu proses yang dibutuhkan pada FPGA A dan FPGA B. Dengan menggeser sinyal dapat dihitung waktu tunda yang terjadi dengan matlab dan diperoleh nilai 200 us untuk frekuensi 500 Hz dan rekaman pidato pada kondisi *off-off*. Semakin kecil waktu tunda maka sekamin baik sistem untuk komunikasi *real time* yang memiliki toleransi maksimum untuk waktu tunda sebesar 150 ms.

Parameter lainnya yang dapat dihitung dari data diatas ialah MSE (*Mean Square Error*). MSE merupakan satuan yang digunakan untuk melihat perbedaan kedua grafik. Sehingga dapat dilihat penurunan kualitas data sebelum dan sesudah melewati sistem. Didapat dari hasil perhitungan setelah menggeser sinyal keluaran atas keterlambatannya MSE untuk sinyal 500Hz adalah sebesar 0,0493 V. Semakin rendah MSE yang dihasilkan menandakan sistem semakin baik karena tidak banyak perubahan yang terjadi terhadap sinyal keluaran.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(xi - yi)^2 \qquad (1)$$

Parameter lainnya untuk mengukur kinerja suatu kinerja sistem audio ialah THD-N yaitu Total Harmonic Distortion with Noise. Parameter tersebut digunakan untuk mengukur power harmonisa yang timbul akibat proses perubahan sinyal analog ke digital dan perubahan digital ke analog.
Pada gambar 10 dan 11 terlihat FFT sinyal keluaran, terdapat harmonisa pada frekuensi kelipatan dari frekuensi fundamental.

$$THD = \sqrt{\frac{\sum_{k=2}^{\infty} x_k^{\,2}}{x_1^{\,2}}} x100\% \qquad (2)$$

Dimana $\boldsymbol{X_1}$merupakan frekuensi fundamental sedangkan $\boldsymbol{X_k}$merupakan frekuensi harmonisa. Selain harmonisa pada perhitungan THD-N mempertimbangkan nilai noise atau sinyal yang tidak diinginkan, maka nilai $\boldsymbol{X_k}$ sama dengan selisih FFT antara sinyal masukan dan keluaran. Nilai $\boldsymbol{X_k}$ sama dengan nilai sinyal masukan, karena pengertian frekuensi fundamental ialah sinyal yang diinginkan. Melalui perhitungan pada MATLAB diperoleh THD untuk frekuensi 500 Hz sebesar 8,88%. Nilai THD yang semakin kecil menunjukkan performa yang lebih baik karena distorsi yang diakibatkan oleh noise semakin kecil.

Tabel 3 menunjukan bahwa terjadi penurunan kualitas suara setelah melewati sistem walaupun tanpa proses enkripsi dan dekripsi. Nilai MSE tersebut diakibatkan karena error sampling. Sedangkan nilai THD-N dikarenakan perubahan pada ranah waktu mengakibatkan terjadi perubahan pada ranah frekuensi sehingga muncul harmonisa dan noise. Semakin kecil nilai MSE dan THD-N menandakan sistem yang lebih baik karena tidak banyak mengubah sinyal keluaran.

Melalui cara perhitungan yang sama pada kondisi enkripsi *off* dan dekripsi *off* dilakukan pengujian pada kondisi enkripsi *on* dan dekripsi *on*. Diperoleh Tabel 4.Tabel 4 menunjukan bahwa terjadi penurunan kualitas suara setelah melewati sistem dengan proses enkripsi dan dekripsi. Bila dibandingkan dengan tabel 3 (tanpa proses enkripsi dan dekripsi) keduanya menunjukan terjadi penurunan kualitas suara.

Pada parameter *delay* didapatkan nilai yang sma antara kondisi *off-off* dan *on-on*, hal ini membuktikan bahwa algoritma kriptografi *stream cipher* cocok digunakan untuk komunikasi *real time* karena *delay* yang dihasilkan untuk proses enkripsi-dekripsinya kecil. Melalui pengujian dengan masukan rekaman suara dapat diketahui bahwa sistem bekerja dengan benar karena keluaran suara dapat dimengerti oleh pendengar.

Gambar 12 menunjukkan grafik perbandingan nilai MSE pada kondisi *on-on* dan *off-off*. Terlihat grafik merah dan biru tidak dalam renggan yang jauh, hal ini menunkukkan bahwa MSE rata-rata dari sinyal yang mengalami enkripsi-dekripsi tidak berbeda jauh dengan MSE rata-rata dari sinyal yang tidak mengalami proses enkripsi-dekripsi. Nampak pada rntang frekuensi 500 – 1000 Hz kenaikan MSE tidak begitu signifikan. Tapi jika dilihat pada frekuensi 1000 – 2000 Hz dan 2000 – 3400 Hz terjadi kenaikan MSE yang cukup signifikan. Hal ini menunjukkan bahwa performa dari sistem akan menurun apabila frekuensi sinyal yang diproses semakin tinggi.

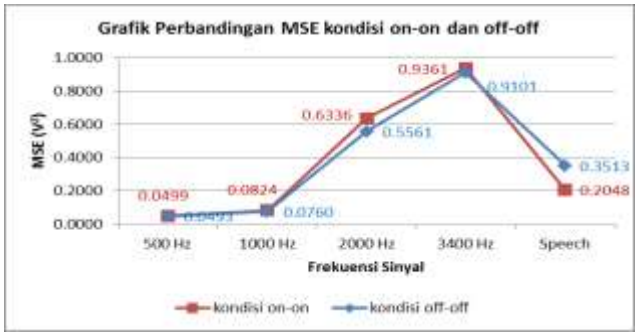
Gambar 13 adalah grafik perbandingsn nilai THD-N antara kondisi on-on dengan kondisi off-off. Terlihat bahwa kedua kurva memiliki *trend* yang sama dan tidak memiliki kerenggangan yang cukup besar. Hal ini menunjukkan bahwa proses enkripsi-dekripsi tidak memberi pengaruh yang besar terhadap nilai dari THD-N. Jika diamati nilai THD-N meningkat seiring dengan kenaikan frekuensi. Hal ini menandakan bahwa sistem yang dirancang akan menghasilkan distorsi harmonik yang besar untuk frekuensi tinggi. Pada *speech*, nilai THD-N tampak menurun. Hal ini disebabkan karena rekaman pidato yang digunakan memiliki rentang frekuensi antara 600 – 1200 Hz.

Tabel 3 Parameter kondisi enkripsi *off* dekripsi *off*

No.	Frekuensi	MSE	Delay	THD-N
1	500 Hz	0,0493 V^2	0,2ms	8,88 %
2	1000 Hz	0,0760 V^2	0,18ms	15,6 %
3	2000 Hz	0,5561 V^2	0,2ms	25,28 %
4	3500 Hz	0,9101 V^2	0,23ms	34,7 %
5	Rekaman	0,1648 V^2	0,2ms	3,15 %
Rata Rata		0,35126 V^2	0,202ms	17,52 %

Tabel 4 Parameter kondisi enkripsi *on* dekripsi *on*

No.	Frekuensi	MSE	Delay	THD-N
1	500 Hz	0,0499 V^2	0,2ms	7,66%
2	1000 Hz	0,0824 V^2	0,18ms	15,70%
3	2000 Hz	0,0636 V^2	0,22ms	23,90%
4	3400 Hz	0,9261 V^2	0.21ms	33,06%
5	Rekaman	0,2048 V^2	0,2ms	4,41%
Rata Rata		0,26536 V^2	0,202ms	20,45%



Gambar 12 Grafik Perbandingan MSE Kondisi *on-on* dan *off-off*

Gambar 13 Grafik Perbandingan MSE Kondisi *on-on* dan *off-off*

Dengan perhitungan seperti kondisi *off-off* dan *on-on* didapat nilai dari parameter pengukuran kondisi *on-off* dan *off-on.* Tabel 5 adalah nilai parameter MSE danTHD-N untuk kondisi *on-off*. Nilai MSE yang dihasilkan rata-rata 2,2425 V^2. Nilai rata-rata THD-N adalah 52,356 %.

Nilai parameter untuk kondisi *off-on* ditunjukkan oleh tabel 6. Rata-rata untuk parameter MSE adalah 2,3004 V^2 dan rata-rata THD-N adalah 57,438 %.

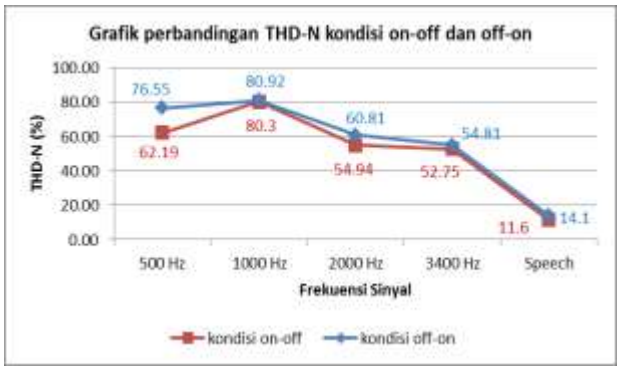
Tabel 5 Parameter kondisi enkripsi *on* dekripsi *off*

No.	Frekuensi	MSE	THD-N
1	500 Hz	2,0609 V²	62,19 %
2	1000 Hz	2,0585 V²	80,30 %
3	2000 Hz	2,8323 V²	54,94 %
4	3400 Hz	2,7087 V²	52,75 %
5	*Speech*	1,5470 V²	11,60 %
	Rata-rata	2,2415 V²	52,356 %

Tabel 6 Parameter kondisi enkripsi *off* dekripsi *on*

No.	Frekuensi	MSE	THD-N
1	500 Hz	2,2142 V²	76,55 %
2	1000 Hz	2,0678 V²	80,92 %
3	2000 Hz	3,0471 V²	60,81 %
4	3400 Hz	3,0886 V²	54,81 %
5	*Speech*	1,0843 V²	14,10 %
	Rata-rata	2,3004 V²	57,438 %

Gambar 14 Grafik Perbandingan MSE Kondisi *on-off* dan *off-on*



Gambar 15 Grafik Perbandingan THD-N Kondisi *on-off* dan *off-on*

Gambar 14 adalah grafik perbandingan parameter MSE untuk kondisi on-off dan off-on. Sedangkan perbandingan parameter THD-N ditunjukkan oleh Gambar 15. Kondisi on-off digunakan untuk mengetahui bentuk sinyal ciphertext pada keluaran dari blok dekripsi. Kondisi off-on adalah kondisi salah yang harus dihindari karena kondisi ini menghasilkan keluaran berupa sinyal acak pada sisi penerima.

3.3 Hasil Perancangan Core pada FPGA

Tabel 7 *Design Summary* Perancangan FPGA A / Blok Enkripsi

No	*Logic*	Digunakan	Tersedia	Penggunaan
1	Slice	1345	3584	37 %
2	Slice Flip-Flop	275	7168	3 %
3	4 Input LUT	2462	7168	34 %
4	I/O Block	25	173	14 %
5	Gate Clock	1	8	12 %

Tabel 8 *Design Summary* Perancangan FPGA B / Blok Dekripsi

No	*Logic*	Digunakan	Tersedia	Penggunaan
1	Slice	1384	3584	38 %
2	Slice Flip-Flop	345	7168	4 %
3	4 Input LUT	2495	7168	34 %
4	I/O Block	23	173	13 %
5	Gate Clock	1	8	12 %

Pada *design summary* Xilinx 14.6 dapat dilihat parameter penggunaan FPGA atas sistem yang dirancang dan ditanamkan pada FPGA seperti Tabel 7. Dari Tabel 7 terlihat penggunaan FPGA dari sistem enkripsi sekitar sepertiga dari kapasistas total yang dimiliki oleh FPGA Spartan-3. Dari hasil tersebut dapat diketahui bahwa FPGA Spartan-3 mampu untuk memproses algoritma kriptografi chaotic dengan kunci 128 bit.
Dari Tabel 8 terlihat sistem yang dirancang memiliki penggunaan yang hampir sama dengan blok enkripsi / FPGA B. Hal ini dikarenakan proses yang dilakukan pada blok dekripsi hampir serupa dengan blok enkripsi. Komponen-komponen penyusun blok dekripsi juga hampir sama dengan blok enkripsi.

4. Kesimpulan

Berdasarkan hasil dan analisis yang sudah dilakukan maka dapat disimpulkan beberapa hal sebagai berikut:

Telah berhasil diimplementasikan algoritma kriptografi Chaotic untuk enkripsi-dekripsi sinyal suara dengan kunci 128 bit pada FPGA Spartan-3 dengan penggunaan resource 37% untuk blok enkripsi dan 38% untuk blok dekripsi.

Pada kondisi off-off dan on-on sinyal keluaran sudah dapat dimengerti dengan parameter galat rata-rata untuk kondisi off-off sebesar 0,35196 V^2 dan 0,26536 V^2 untuk kondisi on-on. Hal ini menunjukkan bahwa proses enkripsi dan dekripsi bekerja dengan baik dan tidak memberikan perubahan yang besar terhadap dinyal yang diproses.

Pada kondisi off-off dan on-on didapatkan nilai waktu tunda rata-rata sebesar 202 dan 202 µs. Nilai ini jauh lebih kecil dari batas waktu tunda maksimum yang dapat ditoleransi untuk komunikasi suara secara real time. Ada pun waktu tunda antara kondisi *off-off* dan *on-on* tidak berbeda menunjukkan bahwa mode kriptografi *stream cipher* cocok digunakan untuk kriptografi komunikasi *real time.*

Pada parameter THD-N bernilai rata-rata 17,52% dan 20,45% untuk kondisi *off-off* dan *on-on*. Nilai ini menunjukkan besarnya distorsi yang terjadi terhadap sinyal keluaran akibat perubahan sinyal analog – digital – analog. Distorsi ini akan mengabikatkan terjadinya harmonisa pada frekuensi kelipatan sinyal masukan. Semakin kecil nilai THD-N menyatakan sistem yang lebih baik dan tidak terjadi banyak perubahan akibat harmonisa yang terjadi.

Pada parameter *on-off* dan *off-on* menghasilkan MSE yang sangat besar disbanding dengan kondisi *on-on* dan *off-off*. Hal ini menyatakan bahwa sinyal keluaran kondisi *on-off* dan *off-on* tidak lagi sama dan mengandung informasi asli dimana *ciphertext* yang dihasilkan tidak dapat dimengerti.

Referensi

[1] J. R. Vacca, P. Liu, T. F. LaPorta, and K. Kotapati, *Network and System Security*. 2013.

[2] D. R. Stinson, "Cryptography: Theory and Practice." 2005.

[3] W. Stallings, *Cryptography and Network Security Principles and Practice 5th*, vol. 139, no. 3. 2011.

[4] K. Roskin and J. Casper, "From chaos to cryptography," *Univ. California, St. Cruz*, 1999.

[5] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, 2006.

[6] N. K. Pareek, V. Patidar, and K. K. Sud, "Discrete chaotic cryptography using external key," *Phys. Lett. Sect. A Gen. At. Solid State Phys.*, vol. 309, no. 1–2, pp. 75–82, 2003.

[7] E. Mosa, N. W. Messiha, O. Zahran, and F. E. Abd El-Samie, "Chaotic encryption of speech signals," *Int. J. Speech Technol.*, vol. 14, no. 4, pp. 285–296, 2011.

[8] B. Schneier, *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth)*. John Wiley & Sons, Inc., 1996.

[9] [10] L. Kocarev and S. Lian, *Chaos-Based Cryptography*. warsaw: springer, 2011.

[11] O. A. Susanto, "Penerapan Teori Chaos di Dalam Kriptografi," no. 13506087.

[12] R. Munir, B. Riyanto, and S. Sutikno, "Perancangan Algoritma Kriptografi Stream Cipher dengan Chaos," no. August, 2015.

[13] A. N. Pisarchik and M. Zanin, "Chaotic map cryptography and security," *Encryption Methods, Softw. Secur.*, pp. 1–28, 2010.

[14] Ferry Wahyu Wibowo, "*FPGA & VHDL Teori, Antarmuka dan Aplikasi*." deepublish, sleman, 2014.

[15] V. a Pedroni, *circuit design with VHDL*. london: MIT Press, 2004.

[16] Ms. Dipl.Ing Asril Jarin, "Komunikasi Serial," UMB, 2008.

[17] Pong P. Chu, *FPGA Prototyping by VHDL Examples*. New Jersey: A JOHN WILEY & SONS, INC., PUBLICATION, 2008.

[18] K. Architecture, "KeyStone Architecture Universal Asynchronous Receiver / Transmitter (UART) User Guide," no. November, 2010.

[19] Albert Malvino, "*Electronic Principles 7th edition*." McGraw-Hill Education, 2006.

[20] Didik Hariyanto, "Analog to Digital Converter," vol. 153, pp. 3–10, 2015.

[21] ITU-T Study Group 12, "ITU-T P.861 - Objective quality measurement of telephone- band (300-3400 Hz) speech codecs," vol. 861, 1998.

[22] T. Installations and L. Line, "P.931 (12/98)," vol. 931.

[23] International Telecommunication Union, "ITU-T Recommendation G. 1010: End-user multimedia QoS categories (Quality of service and performance)," *Int. Telecommun. Union*, vol. 1010, 2001.