PERANCANGAN DAN IMPLEMENTASI SISTEM KOMUNIKASI DIGITAL YANG AMAN BERBASIS CHAOS DENGAN MENGGUNAKAN FPGA

Heru Supriyono
Jurusan Teknik Elektro, Universitas Muhammadiyah Surakarta
Jl. A. Yani Tromol Pos I Pabelan Kartasura, Surakarta 57102.
Email: herusupriyono@yahoo.com

ABSTRAKSI

Aplikasi sistem chaos dalam bidang komunikasi sudah mendapat perhatian yang besar dari para peneliti dewasa ini terutama dalam bidang komunikasi yang aman karena sifat system chaos yang non-periodik. Dalam sistem komunikasi berbasis chaos baik pengirim (transmitter) maupun penerima (receiver) harus mempunyai sistem chaos yang benar-benar identik polanya dan sama nilai awalnya.Dalam makalah ini, akan dibahas perancangan dan implementasinya sistem komunikasi yang aman berbasis chaos. Model sistem komunikasi yang akan digunakan adalah Chaotic Pulse Posistion Modulation (CPPM). Dalam CPPM sinyalatau informasi yang akan dikirimkan dimodulasikan dalam sinyal chaos yang akan menghasilkan sinyal yang termodulasi. Sinyal yang termodulasi inilah yang akan dikirimkan ke penerima. Penerima akan menerjemahkan sinyal yang termodulasi ini dan merekonstruksi sinyal asli. Dalam makalah ini CPPM didesain dan diimplementasikan pada sebuah Field Programmable Logic Array (FPGA). Hasil pengujian menunjukkan bahwa penerima dapat merekonstuksi informasi yang dikirimkan dengan sedikit tunda (delay)

Kata kunci: *sistem chaos, kondidi awal, CPPM, FPGA.*

PENDAHULUAN

Beberapa penelitian yang memanfaatkan potensi chaos dalam bidang komunikasi, terutama komunikasi yang aman, dapat dilihat pada daftar pustaka. Salah satunya adalah skema komunikasi yang diajukan oleh (Suschick et al, 2000) yaitu *ChaoticPulse Position Modulation* (CPPM). Baik pengirim maupun penerima dalam model CPPM akan berisi sebuah *Chaotic Signal Generator* (CSG) yang benar-benar sama baik strukturnya maupun nilai awalnya karena sebuah sistem chaos sangat dipengaruhi oleh nilai awalnya. Pada skema komunikasi ini informasi yang akan dikirimkan, dengan alasan kemudahan dan kesederhanannya digunakan sebuah informasi biner yang bernilai ‘1” atau ‘0” saja, dimodulasikan pada sinyal chaos yang dibangkitkan oleh CSG. Sinyal yang sudah dimodulasi ini kemudian dikirimkan ke penerima. Penerima akan merekonstruksi sinyal termodulasi ini untuk menghasilakn informasi yang dikirimkan.

Selain diimplementasikan dalam sistem komunikasi dengan kabel, CPPM juga sudah berhasil diimplementasikan dalam sistem komunikasi nir-kabel (*wireless communication*). Hasilnya menunjukkan bahwa CPPM mampu meningkatkan keamanan dan privasi dalam berkomunikasi karena skema ini mempunyai probabilitas intercept yang lebih rendah dibandingkan dengan sistem komunikasi berbasis chaos yang lain. Selain itu dengan menggunakan skema CPPM hanya akan menambah sedikit tambahan rangkaian elektronik sehingga tidak akan menambah rumit rangkaian (Suschick et al, 2000).

Piranti digital dewasa ini mengalami perkembangan yang sangat pesat. Dalam sistem komunikasi khususnya, hampir semua piranti mengalami apa yang disebut digitalisasi karena keunggulan system digital diantaranya yaitu lebih cepat, dimensinya lebih kecil, membutuhkan daya yang lebih kecil, dan lebih tahan terhadap derau. Dalam penelitian ini, skema komunikasi CPPM akan diimplementasikan dengan piranti digital yaitu *Field Programmable Logic Array* (FPGA). Kelebihan FPGA dibandingkan dengan *chips* prosesor yang lain adalah “logika” atau isi gerbang-gerbang logika chips ini dapat di-download dan dihapus dengan mudah tidak seperti *dedicated chips* seperti mikrokontroller dll.

LANDASAN TEORI

Sinyal yang termodulasi dalam skema komunikasi *Chaotic Pulse Position Modulation* (CPPM) adalah berupa deretan pulsa (*pulses train*) yang mempunyai amplitude dan lebar pulsa yang sama tetapi jarak waktu antar pulsanya berbeda. Jarak waktu ini dibangkitakan oleh sinyal chaos yang dipakai dalam system komunikasi. Secara matematis, deretan pulsa (pulses train dapat dirumuskan sebagai berikut:

$$U(t) = \sum_{j=0}^{\infty} \omega(t - t_j) \qquad (1)$$

dengan $\omega(t - t_j)$ adalah bentuik gelombang pulsa yang dibangkitkan pada waktu $t_j = t_0 + \sum_{n=0}^{j} T_n$, T_n adalah interval waktu antara pulsa ke-*n* dank e-(*n* – 1).

Sehingga, persamaan (1) diatas dapat dinyatakan sebagai berikut:

$$U(t) = \sum_{j=0}^{\infty} \omega(t - t_0 - \sum_{n=0}^{j} T_n) \quad (2)$$

U(t) adalah deretan pulsa yang mempunyai amplitude dan lebar pulsa yang sama tetapi mempunyai waktu antar pulsa atau interval waktu yang berbeda. T_n dihasilkan oleh iterasi proses chaos. Untuk pola satu dimensi, interval waktu dapat dinyatakan sebagai $T_n = F(T_n - 1)$ dengan *F(·)* adalah fungsi non linear.

Informasi yang akan dikirimkan di-decode-kan kedalam sinyal pulsa chaos. Secara matematis dapat dinyatakan sebagai:

$$T_n = F(T_{n-1}) + d + mS_n \quad (3)$$

dengan S_n adalah informasi yang akan dikirimkan, *d* adalah delay yang ditambahakan sesuai dengan sinyal informasi, *m* adalah amplitudo modulasi. Untuk masukan digital, informasi yang dikirimkan hanya terdiri dari sinyal biner i.e. "1" and "0". Oleh karena itu, S_n sama dengan "1" atau "0". Waktu interval, T_n, akan ditambah dengan delay sebesar *d* jika informasi S_n adalh "1" selain itu tidak berubah.

Agar dapat mendeteksi sinyal yang dikirimkan, *U(t)*, penerima harus di-trigger oleh sinyal ini. Kemudian penerima mampu mengukur interval waktu diantara dua buah pulsa yang beruruatan diatara T_n dan T_{n-1}. Berdasarkan pengukuran ini, penerima mampu mengekstrak informasi yang dikirimkan dengan menggunakan rumus berikut:

$$S_n = (T_n - F(T_{n-1}) - d)/m \quad (4)$$

dengan S_n, *F(·), d,* dan *m* adalah parameter yang sama dengan persamaan (3).

Jika penerima mengetahui fungsi non-linera *F(·),* parameter tunda *d,* dan amplitude modulasi *m* maka penerima akan dapat meng-ekstrak sinyal informasi S_n dengan mudah. Jika penerima tidak mempunyai fungsi non linear yang sama dengan *F(·),* ia akan gagal mendapatkan sinyal informasi S_n yang benar. Oleh karena itu, kedua fungsi non-linear harus benar-benar sama. Dengan car ini, orang yang tidak mempunyai informasi mengenai fungsi pembangkit pulsa *U(t)* tidak akan dapat mendeteksi apakah pulsa tertunda atau tidak sehingga tidak dapat mengenali apakah informasi yang dikirimkan "1" atau "0".

Dalam penelitian ini, sinyal chaos yang akan digunakan mempunyai bentuk atau pola tenda (tent-map) yang dapat dinyatakan sebagai berikut:

F(·): $$x_{n+1} = \alpha\left|0.5 - \left|0.5 - x_n\right|\right| \quad (5)$$

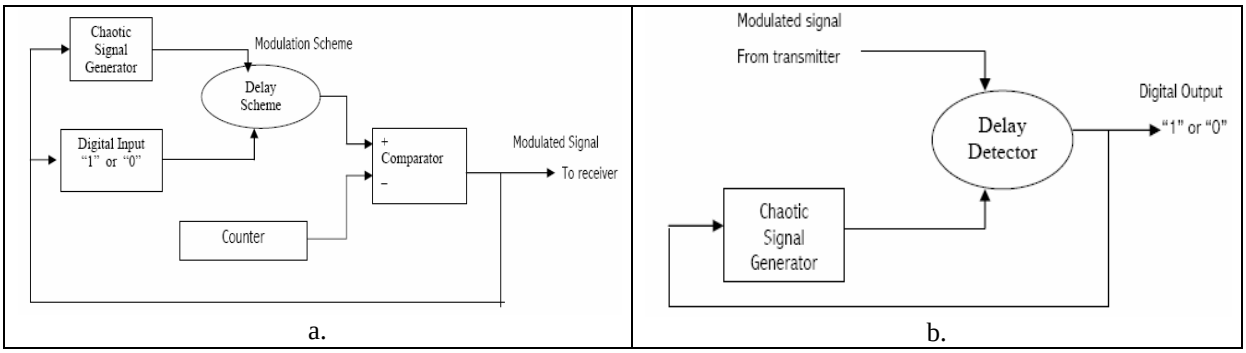
dengan, α = 1.3 dan x_n = nilai sebelumnya. Jadi sinyal chaos tent-mapmenggunakan keluaran sebelumnya sebagai masukan sekarang.

METODE PENELITIAN

Tahapan-tahapan yang akan dilakukan dalam penelitian ini adalah pertama-tama pengirim dan penerima pada skema komunikasi CPPM akan dirancang dan diimplementasikan dalam system FPGA dengan menggunakan perangkat lunak (*software*) Xilinx System Generator sebagai piranti perancangannya (*design tool*). Kemudian unjuk kerja (*performance*) penerima akan diamati dengan cara mengubah-ubah nilai awal sinyal chaos yang berpola tent-map pada pengirim sedangkan pada penerima dibuat tetap. Akan dilihat apakah penerima mampu mendapatkan sinyal informasi dengan benar atau tidak.

SIMULASI DAN ANALISIS

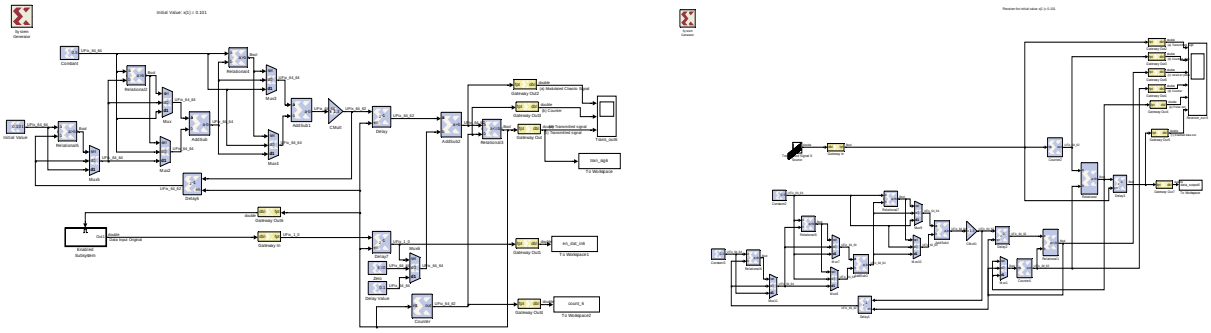
Secara grafis blok diagram pengirim dan penerima dapat dilihat dalam gambar di bawah ini:



Gambar 1. Diagram blok: a. pengirim, b. penerima

Dalam gambar diagram blok diatas *Chaotic Signal Generator* yang digunakan dalam bagian penerima dan pengirim benar-benar sama baik strukturnya maupun nilai awalnya. Implementasi pengirim dan penerima diatas dengan

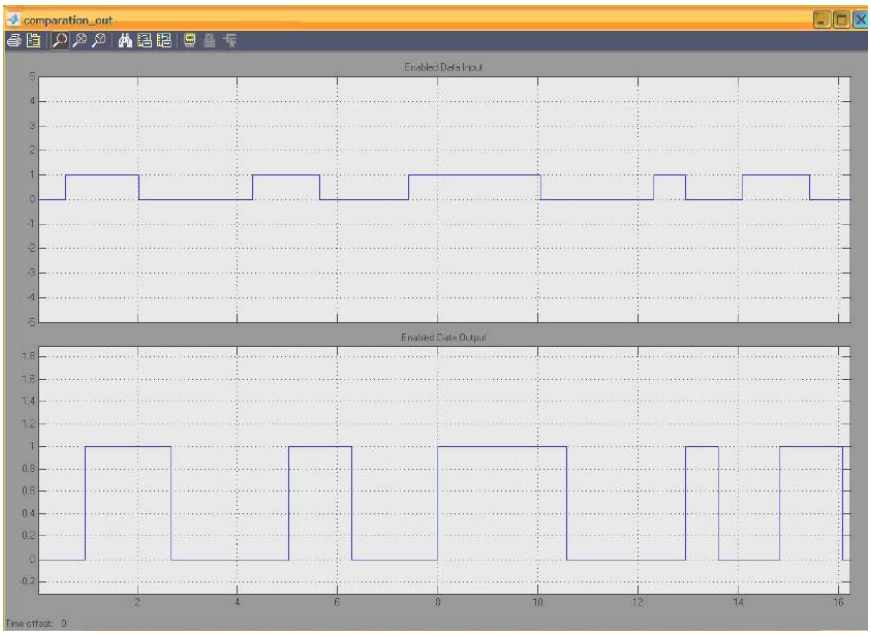
menggunakan FPGA dapat dilihat dalam Gambar 2 berikut.



(a) (b)

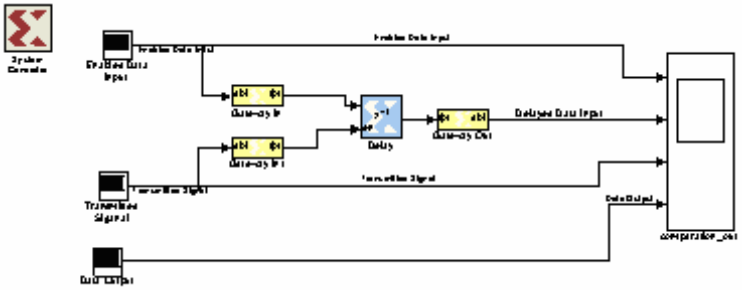
Gambar 2. Implementasi CPPM dengan FPGA: (a) pengirim, (b) penerima

Hasil simulasi dapat dilihat dalam gambar berikut ini:



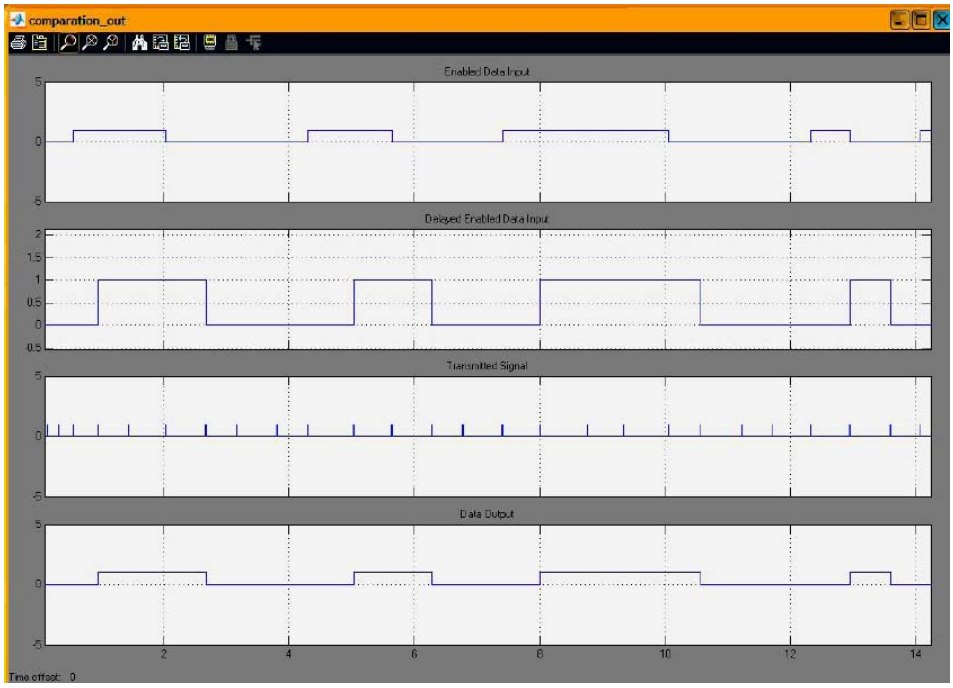
Gambar 3. Perbandingan antara informasi yang dikirim (atas) dengan informasi hasil rekonstruksi (bawah).

Dari gambar diatas dapat dilihat bahwa secara umum, dilihat dari pola sinyalnya, informasi hasil rekonstruksi adalah persis sama dengan informasi yang dikirimkan. Hanya saja ada *delay* (tunda waktu). Untuk mendapatkan pengetahuan yang eksak nilai delaynya, sebuah komponen tunda ditambahkan pada keluaran rangkaian pengirim seperti yang dapat dilihat dalam rangkaian di bawah ini:



Gambar 4. Sebuah komponen penunda ditambahkan pada keluaran rangkaian penerima

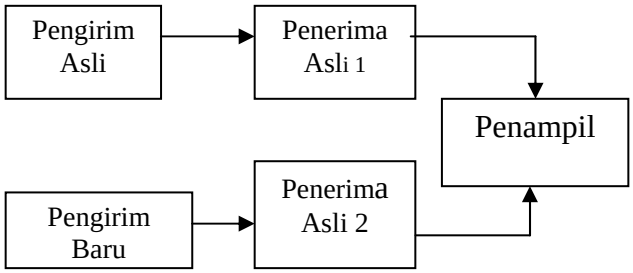
Setelah diberi rangkaian penunda, perbandingan antara informasi asli yang dikirim dengan informasi hasil rekonstruksi dapat dilihat dalam gambar di bawah ini:



Gambar 5. Perbandingan sinyal setelah ditambahkan unit penunda pada keluaran pengirim: sinyal informasi asli yang dikirimkan (paling atas), sinyal informasi asli setelah diberi unit penunda (kedua dari atas), sinyal informasi hasil rekonstruksi (paling bawah).

Dari gambar diatas dapat dilihat bahwa antara sinyal informasi yang tertunda satu periode sinyal sama persis dengan hasil rekonstruksi.

Selanjutnya, unjuk kerja rangkaian penerima yang sudah dirancang diatas akan diuji dengan cara mengubah-ubah nilai awal sinyal chaos pengirim. Secara grafis mekanisme pengujian dapat digambarkan sebagai berikut:

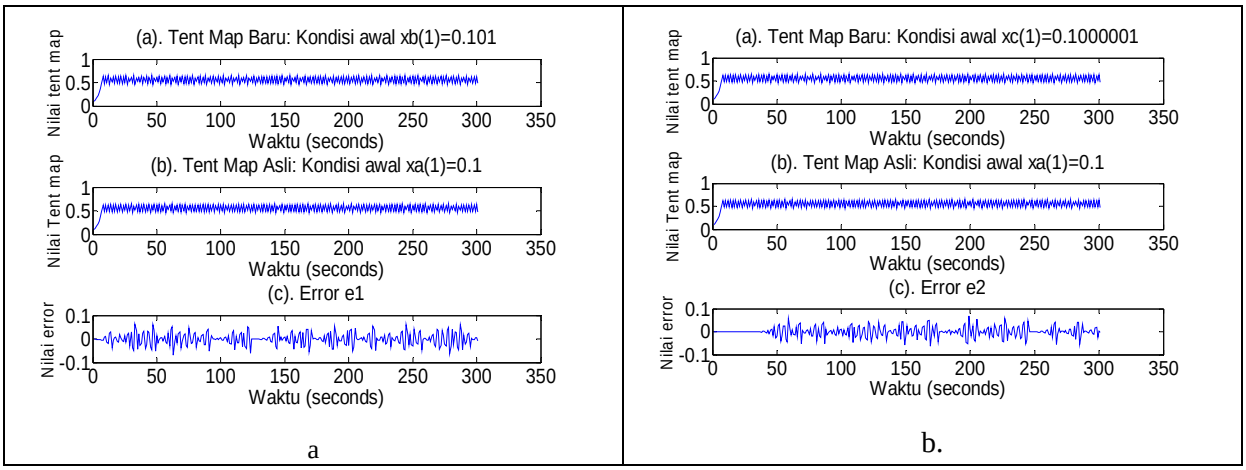


Gambar 6. Diagram blok mekanisme pengujian.

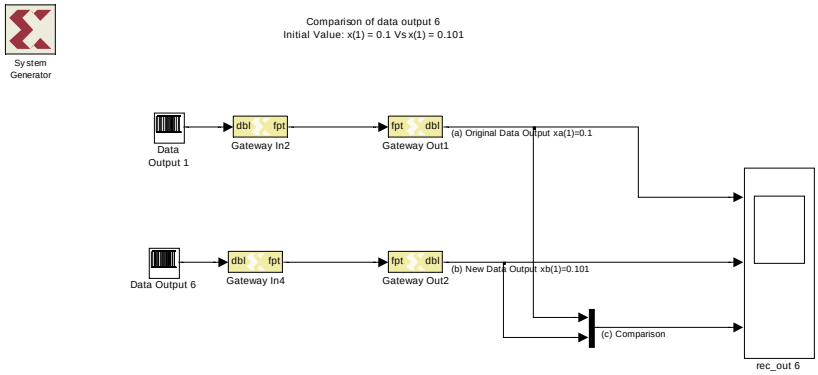
Pada gambar diatas, Pengirim Asli, Penerima Asli 1, dan Penerima Asli 2 menggunakan sinyal chaos dengan kondisi awal asli. Sedangkan Pengirim Baru menggunakan sinyal chaos dengan kondisi awal yang sudah diubah-ubah. Dalam penelitian ini kondisi awal fungsi tent-map asli adalah *xa(1)* = 0.1. Kemudian kondisi awal akan diubah menjadi *xb(1)* = 0.101 dan *xc(1)* = 0.1000001. Sinyal keluaran yang dihasilkan oleh sebuah sistem chaos sangat dipengaruhi oleh kondisi awalnya. Perbandingan antara sinyal chaos dengan ketiga buah kondisi awal diatas dapat dilihat dalam Gambar 7. di bawah.

Seperti yang digambarkan dalam gambar diatas, dalam untuk keperluan pengujian unjuk kerja skema ini dibutuhkan 2 buah pengirim dan dua buah penerima. Keluaran Penerima Asli 1 dan Penerima Asli 2 kemudian dikirimkan ke Matlab *workspace*. Kedua sinyal ini kemudian dibandingkan dengan menggunakan blok Simulink dan ditampilkan dengan menggunakan blok *Scope*. Implementasinya dapat dilihat dalam Gambar 8 dibawah.

 ISSN: 1907-5022

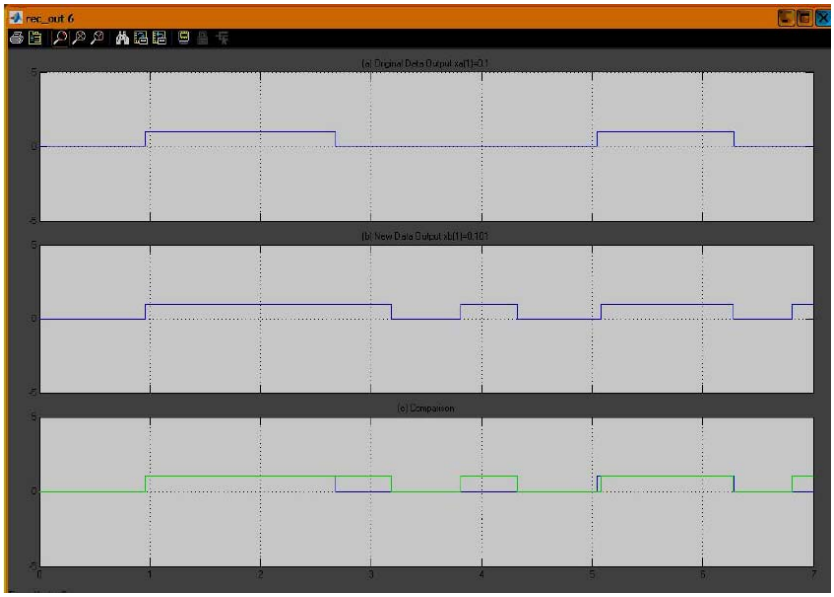


Gambar 7. Perbandingan sinyal chaos tent-map dengan tiga buah kondisi awal: a. Kondisi awal xa(1)=0.1 Vs xb(1) 0.101, b. Kondisi awal xa(1)=0.1 Vs xc(1)=0.1000001



Gambar 8. Membandingkan keluaran Penerima Asli 1 dan Penerima Asli 2 dengan menggunakan *System Generator* dan Simulink

Kondisi awal : *xa(1)*=0.1 Vs *xb(1)*=0.101

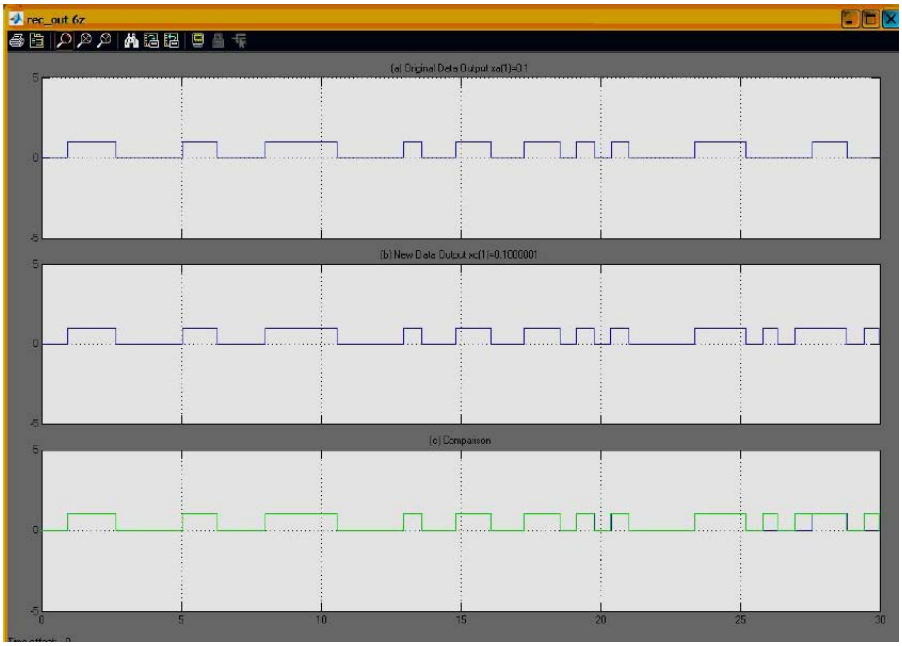


Gambar 9. Perbandingan keluaran Penerima Asli 1 (paling atas), Penerima Asli 2 (no.2 atas), dua buah sinyal dalam satu window: Penerima Asli 1 (Biru) dan Penerima Asli 2 (Hijau)

Percobaan pertama yang dilakukan : kondisi awal Pengirim Asli, Penerima Asli 1, Penerima Asli 2 adalah xa(1)=0.1 sedangkan kondisi awal Pengirim Baru adalah xb(1)=0.101. Dari Gambar 9 diatas dapat dilihat bahwa Penerima Asli 2 gagal merekonstruksi sinyal informasi dengan benar. Hal ini dilihat bahwa keluaran Penerima Asli 2 (grafik warna biru) tidal *match* dengan keluaran Penerima 1 (grafik warna hijau).

Kondisi awal xa(1)=0.1 vs xc(1)=0.1000001

Percobaan kedua yang dilakukan adalah kondisi awal Pengirim Asli, Penerima Asli 1. Penerima Asli 2 adalah *xa(1)*=0.1 sedangkan kondisi awal Pengirim Baru adalah *xc(1)*=0.1000001. Gambar 10 di bawah menunjukkan Penerima 2 hanya dapat merekonstruksi informasi dengan benar disaat-saat awal dimana galat (*error*) diantara sinyal chaos, setelah itu akan gagal seiring dengan adanya *galat*. Ini menunjukkan bahwa perubahan kondisi awal walaupun sekecil apapun akan menyebabkan perubahan yang besar dalam jangka panjang pada sistem chaos



Gambar 10. Perbandingan keluaran Penerima Asli 1 (paling atas), Penerima Asli 2 (tengah), dan kedua buah keluaran penerima dalam satu window (paling bawah : Penerima Asli 1 (biru) dengan Penerima Asli 2 (hijau)

KESIMPULAN

Dari hasil percobaan dapat dilihat bahwa apabila seseorang yang tidak mempunyai informasi mengenai sinyal chaos yang digunakan untuk memodulasi informasi yang dikirim, maka dia tidak akan dapat merekonstruksi informasi yang dikirimkan dengan tepat. Juga dapat disimpulkan bahwa kondisi awal pada sistem chaos merupakan kunci rahasis bagi komunikasi yang berbasis sinyal chaos. Untuk dapat merekonstruksi informasi dengan benar, penerima harus mempunyai pembangkit sinyal chaos dan kondisi awal yang benar-benar sama dengan pengirim.

DAFTAR PUSTAKA

Rulkov,N., Suschik, M., Tsimring, L., and Volkovskii, A., 2001, "*Digital Communication Using Chaotic-Pulse-Position Modulation",* IEEE Transaction on Circuits and Systems-I. Fundamental Theory and Application, Vo. 48, no. 12, December 2001.

Suschik Jr, M., Rulkov, N., Larson, L., Tsimring, L., Abardanel, H., Yao, K., Volkovskii, A., 2000, "*Chaotic Pulse Position Modulation: A Robust Method of Communicating with Chaos",* IEEE Communication Letters, Vol. 4, no. 4, April 2000.

Supriyono, H., 2005, "*Chaos-based Digital Communication Systems*", Jurnal Teknik Gelagar English Edition, October 2005.

----------, 2005, "*Xilinx system Generator v2.1 for Simulink"*, Internet Web page: http://brwc.eecs.berkeley.edu/classes/cs152/handouts/Tutorial_book.pdf (Accessed 10 June 2005).