

Prenos podataka pomoću sinhronizovanih haotičnih kola

U radu je ispitana mogućnost prenosa podataka pomoću sinhronizovanih haotičnih kola. Kao izvor haotičnih oscilacija korišćeno je kolo Leona Čue. Sinhronizacija je uspešno uspostavljena, a prenos podataka je omogućen u opsegu od 15 Hz do 2.5 kHz. Digitalni signal je frekventno modulisan i uspešno prenesen kroz sistem, a kôd demodulatora je u fazi razvoja. Emitovan signal je haotično modulisan i pokazuje sve osobine haosa, što je značajno za bezbednost podataka.

Uvod

Pod pojmom haos podrazumeva se neuređena promena stanja nekog sistema. Deterministički haos označava neregularno, nepredvidivo ponašanje nekog sistema izazvano tačno definisanim procedurama, odnosno jednačinama (Belić 1990). Da bi se u nekom sistemu pojavili pokazatelji haosa, neophodno je da je taj sistem opisan diferencijalnim jednačinama, najmanje drugog stepena, koje moraju biti nelinearne. Linearni sistemi nikada ne ispoljavaju haotična svojstva.

Ove jednačine nemaju rešenje u analitičkom obliku, već se rešavaju numeričkim metodama. To predstavlja jedan od razloga zašto je razvoj ove teorije povezan sa pojavom prvih računara, koji su korišćeni za rešavanje ovakvih jednačina (Gleick 2001). Grafički prikaz oscilovanja stanja haotičnih sistema predstavlja čudni atraktor. To je skup putanja koje su međusobno različite ali se grupišu, konvergiraju ka određenom obliku (orbita) i nikada se ne seku. Karakteristična osobina haotičnih sistema je velika osetljivost na početne uslove. Ukoliko se u evoluciji ovakvih sistema pođe od dve bliske tačke, odnosno trajektorije, u faznom prostoru, onda će se one posle

dovoljno dugo vremena naći proizvoljno daleko jedna od druge. Ta karakteristika se često naziva „efekat leptira“ (Belić 1990). Stepenn udaljavanja dve početno bliske trajektorije kvantitativno je izraženo Ljapunovim eksponentom, datim formulom:

$$\lambda = \lim_{\substack{t \rightarrow \infty \\ \Delta x_0 \rightarrow 0}} \frac{1}{t} \ln \frac{\Delta x(x_0, t)}{\Delta x_0}$$

gde je Δx_0 vrlo mala promena početne vrednosti stanja x , dok $\Delta x(x_0, t)$ predstavlja priraštaj stanja x u vremenu t . Kada je vrednost λ pozitivna, orbite atraktora su nestabilne i haotične. Negativna vrednost eksponenta ukazuje na stabilnost sistema.

Haotična kola osciluju na širokom opsegu frekvencija, pa su haotični signali širokopojasni. Istraživanja mogućnosti sinhronizacije haotičnih kola koja su sproveli Pecora i Carroll dovela su do velikog interesovanja za prenos informacija pomoću širokopojasnog haotičnog signala. Emitovan signal, koji sadrži poruku i haotičnu komponentu, zbog širokog opsega postojećih frekvencija, podseća na šum. Prijemnik sadrži haotično kolo koje proizvodi haotičnu komponentu identičnu onoj u izlaznom signalu predajnika, što omogućava ekstrakovanje emitovane poruke iz primljenog signala. Ovaj vid komunikacije oslanja se na dve karakteristike haotičnih sistema – mogućnost sinhronizacije i nepredvidivost stanja haotičnog kola. Izdvajanje poruke je moguće zahvaljujući mogućnosti sinhronizacije dva haotična kola. Kada je sinhronizacija postignuta, dva sistema osciluju identično. Bezbednost podataka omogućena je nepredvidivošću

Miodrag Basić (1990), Beograd, Bulevar Zorana Đinđića 47, učenik 4. razreda X gimnazije „Mihajlo Pupin“ u Beogradu

Smiljana Todorović (1993), Velika Plana, Stoje Novakovića 2, učenica 1. Razreda Gimnazije u Velikoj Plani

MENTOR: Teo Šarkić, Bitgear Wireless, Beograd

emitovanog signala, koji podseća na šum (Perruquetti i Barbot 2006).

U radu je razmotrena mogućnost kriptovanog prenosa analognih i digitalnih signala pomoću sinhronizovanih haotičnih kola.

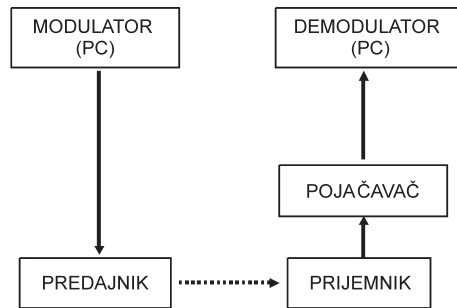
Cilj rada je utvrđivanje karakteristika opisanog sistema za prenos podataka, pre svega propusnog opsega i BER-a (Bit Error Rate).

Opis uređaja

Realizovan uređaj, kao sistem za prenos podataka podrazumeva sledeće celine (slika 1):

- predajnik sa modulatorom
- prijemnik sa demodulatorom
- pojačavači signala

Ukoliko se prenosi digitalni signal (digitalna fotografija, tekstualni fajl ili bilo koji digitalni dokument), potrebno je modulisati taj signal pre slanja na predajnik. Izabrana je frekventna modulacija, jer je manje osetljiva na šum u odnosu na amplitudnu ili faznu modulaciju, a i zbog jednostavnosti primene. Modulacija je vršena u Matlabu. Logička nula je predstavljena sinusoidom frekvencije 400 Hz, dok je logičkoj jedinici ekvivalentna učestanost od 700 Hz. Frekvencija odabiranja podešena je na 44 kHz. Svaki bit je predstavljen sa 5 ms (220 odbiraka) sinusnog signala odgovarajuće frekvencije. Prilikom modulacije podataka, korišćeni su bitovi parnosti, čija je funkcija da ukažu na eventualnu grešku prilikom pre-



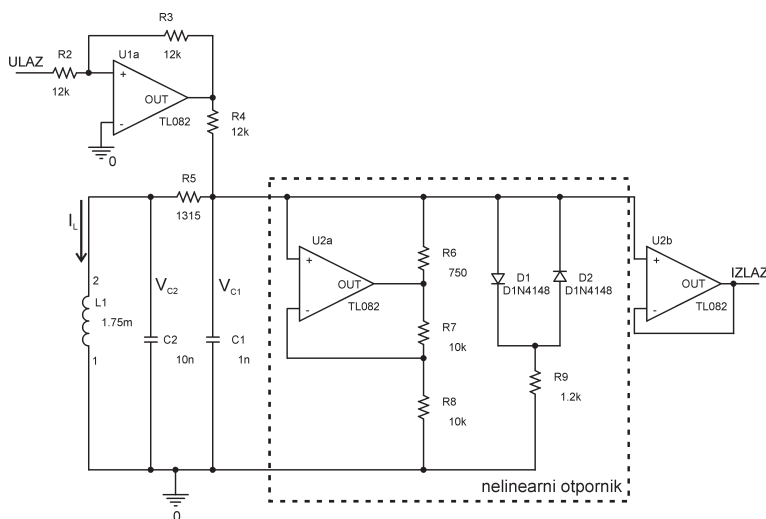
Slika 1. Blok šema sistema za prenos podataka

Figure 1. Simplified schematic of data transmission system (modulator, transmitter, receiver, amplifier, demodulator)

nosa. Na 7 bitova podataka korišćen je 1 bit parnosti, pa demodulator obrađuje primljeni signal u paketima od 8 bita. Ovako generisan signal pogodan je za prenos kroz analogni predajnik i prijemnik. U slučaju prenosa analognih podataka, kao što je zvuk, modulacija na računaru nije potrebna.

Predajnik se sastoji od haotičnog oscilatora i komponenta koje omogućavaju utiskivanje signala sa modulatora u haotični signal. Šema predajnika data je na slici 2.

Predajnik utiskuje modulisan signal u haotični signal. Kao izvor haotičnog signala u predajniku korišćeno je kolo Leona Čue. Čuino kolo predstavlja deo predajnika bez operacionih pojačavača U1a i



Slika 2. Predajnik

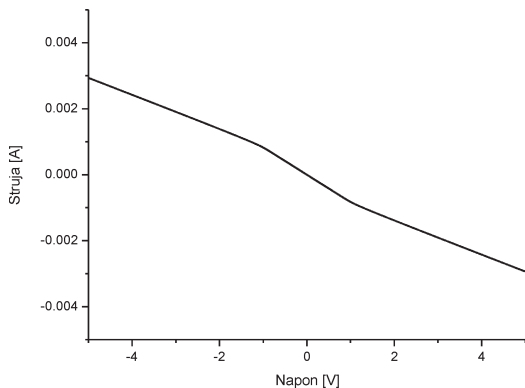
Figure 2. Transmitter

U2b. Ovo kolo opisuju sledeće naponsko-strujne jednačine:

$$\frac{dV_{C1}}{dt} = \frac{1}{RC_1}(V_{C2} - V_{C1}) - \frac{1}{C_1}i(V_{C1}) \quad (1a)$$

$$\frac{dV_{C2}}{dt} = \frac{1}{RC_2}(V_{C1} - V_{C2}) - \frac{1}{C_2}I_L \quad (1b)$$

$$\frac{dI_L}{dt} = -\frac{1}{L}V_{C2} \quad (1c)$$



Slika 3. Naponsko-strujna karakteristika nelinearnog otpornika

Figure 3. Voltage-current characteristic of a non-linear resistor

Gde je $i(V)$ naponsko-strujna karakteristika nelinearnog otpornika sa slike 2. Grafički prikaz $i(V)$ karakteristike dat je na slici 3.

Nelinearni otpornik svojom $i(V)$ karakteristikom unosi nelinearnost potrebnu za nastanak haosa. Fazni prostor je trodimenzionalan (V_{C1} , V_{C2} , I_L).

V - I karakteristika nelinearnog elementa u kolu može se opisati sa

$$i(V) = aV + \frac{b-a}{2}(|V+1| - |V-1|)$$

gde su a i b negativne konstante.

Kolo predajnika opisano je skupom nelinearnih diferencijalnih jednačina (2a, 2b, 2c):

$$\frac{dx}{dt} = f(x, y, z, \lambda) \quad (2a)$$

$$\frac{dy}{dt} = g(x, y, z) \quad (2b)$$

$$\frac{dz}{dt} = h(x, y, z) \quad (2c)$$

gde x , y i z definišu stanja sistema, λ predstavlja informacioni signal, dok je nezavisna promenljiva t . Da bi sistem bio haotičan, vrednost parametra λ mora biti u odgovarajućem opsegu.

Sinhroni podsistem (prijemnik) određen je sistemom jednačina:

$$\frac{dy_r}{dt} = g(x, y_r, z_r) \quad (3a)$$

$$\frac{dz_r}{dt} = h(x, y_r, z_r) \quad (3b)$$

Stanje sistema x se prenosi do prijemnika. Kada se stanja prijemnika y_r i z_r izjednače sa stanjima y i z u predajniku, kola su sinhronizovana. Parametrom λ se prenose informacije i on predstavlja modulacioni parametar u prijemniku. Radi demodulacije u prijemniku, uveden je nelinearni filter, čiji opis sledi. Ukoliko je u sistemu (2) f linearno po λ , važi:

$$f(x, y, z, \lambda) = f_0(x, y, z) + \lambda f_1(x, y, z) \quad (4)$$

Imajući ovo u vidu, jednačina (2a) može se zapisati kao:

$$\frac{dx}{dt} = f_0(x, y, z) + \lambda f_1(x, y, z) \quad (5)$$

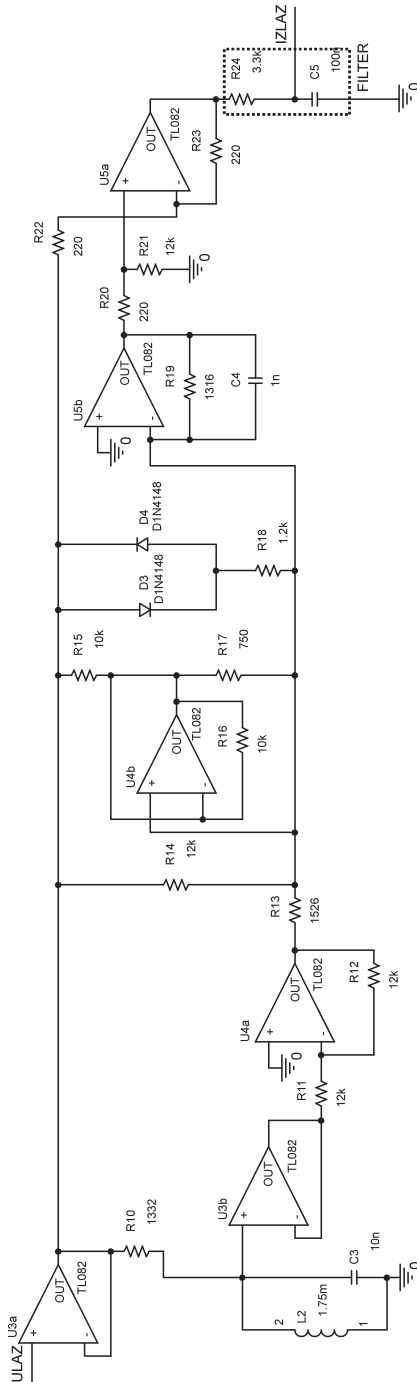
Integracijom se, pored oslobađanja od prvog izvoda uz x , uvodi i promenljiva koja ukazuje na početno stanje sistema, što nije poželjno. Zbog toga je obema stranama dodat član kx , uz množenje jednačine faktorom e^{kt} :

$$\frac{d}{dt}(xe^{kt}) = e^{kt}[f_0(x, y, z) + \lambda f_1(x, y, z) + kx] \quad (6)$$

gde je k proizvoljna pozitivna konstanta, čijom se modifikacijom vrši prilagođavanje filtera. Integracijom po vremenu i deljenjem sa eksponencijalnom funkcijom dobija se:

$$x - x_0 e^{k(t_0-t)} = \int_{t_0}^t [f_0(x, y_r, z_r) + kx] e^{k(t-\tau)} d\tau + \int_{t_0}^t \lambda f_1(x, y_r, z_r) e^{k(t-\tau)} d\tau \quad (7)$$

gde je x_0 početno stanje sistema, dok je λ funkcija vremena. S obzirom da λ sporo menja vrednost u odnosu na podintegralnu eksponencijalnu funkciju, može se smatrati konstantom i izvući ispred inte-



Slika 4. Prijemnik

Figure 4. Receiver

grala. Član sa leve strane jednakosti koji sadrži x_0 nestaje kako vreme raste, pa se može zanemariti. Uzimajući u obzir ove pretpostavke jednačina (7) se može napisati u obliku:

$$\lambda = \frac{x - \omega_1}{\omega_0} \quad (8)$$

$$\omega_1 \int_{t_0}^t f_1(x, y_r, z_r) e^{k(\tau-t)} d\tau \quad (9)$$

$$\omega_1 = \int_{t_0}^t [f_0(x, y_r, z_r) + kx] e^{k(\tau-t)} d\tau \quad (10)$$

Diferenciranjem izraza za ω_0 i ω_1 dobijene su jednačine koje opisuju prijemnik:

$$\omega_0 = f_0(x, y_r, z_r) + kx - k\omega_0 \quad (11)$$

$$\omega_1 = f_1(x, y_r, z_r) - k\omega_1$$

Procena signala data sa (8) sadrži singularitete za $\omega_0 \rightarrow 0$, pa je uveden nisko-propusni filter.

Kolo prijemnika je dato na slici 4. Modifikacijom vrednosti otpornika R19 omogućeno je fino podešavanje prijemnika, čime je omogućen kvalitetniji prijem.

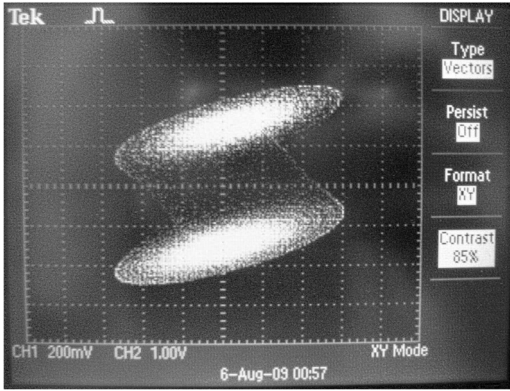
Kako je amplituda izlaznog signala relativno mala (videti rezultate) za obradu, operacioni pojačavač između prijemnika i demodulatora povećava amplitudu primljenog signala.

Demodulacija je vršena na PC računaru, u Matlab okruženju. Signal sa prijemnika je sniman pomoću linijskog ulaza, a zatim demodulisan.

Program najpre određuje početak i kraj korisnog signala i izdvaja ga iz primljenog niza. Zatim se obrađuju nizovi od po 220 odbiraka (1 bit) i određuje emitovan bit. Nakon demodulacije, vrši se poređenje poslanog i primljenog niza bitova i utvrđuje BER, kao odnos broja pogrešno prenetih i ukupno prenetih bitova.

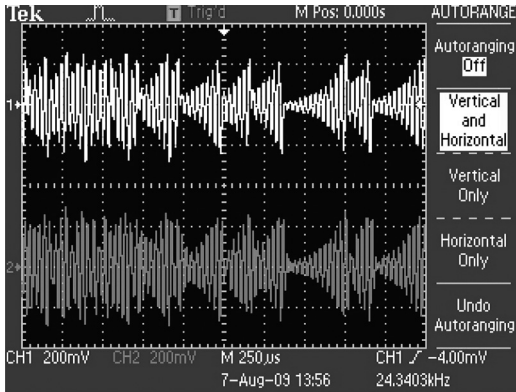
Rezultati i diskusija

Postignuto je haotično oscilovanje predajnika i prijemnika, kao i njihova sinhronizacija. Podešavanjem parametara kola sa slike 2, predajnik je doveden u haotično stanje, što se manifestuje na slici 5. Na x-osi osciloskopa je napon meren na kondenzatoru C2, a na y-osi napon na kondenzatoru C1. Čudni atraktor, prikazan na slici 5, karakterističan je za



Slika 5. Čudni atraktor dobijen podešavanjem kola predajnika

Figure 5. Strange attractor caused by adjusting parameters of transmitter circuit



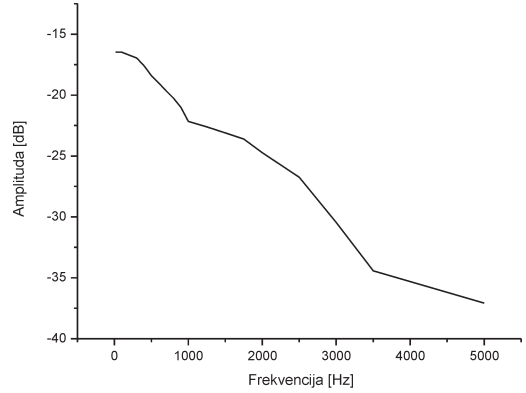
Slika 6. Pokazatelj sinhronizacije dva kola: CH1-napon na C2, CH2-napon na C3

Figure 6. Proof of synchronization: CH1-voltage over C2, CH2-voltage over C3

haotično kolo. Ova figura predstavlja napon na kondenzatoru C_1 u funkciji napona na kondenzatoru C_2 predajnika.

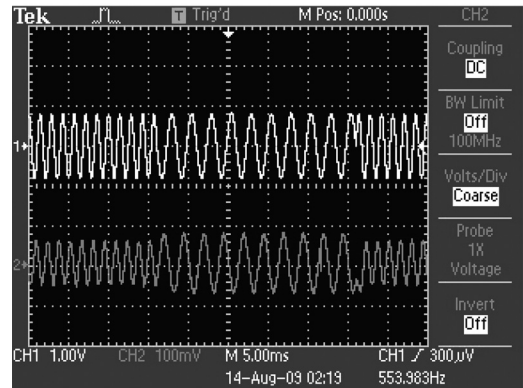
Sinhronizacija predajnika i prijemnika dokazana je poređenjem napona na kondenzatoru C_3 prijemnika i kondenzatoru C_2 predajnika. Ova dva napona pokazuju minimalne međusobne razlike (slika 6).

S obzirom da amplituda i frekvencija ulaznog (modulisanog) signala utiču na oblik atraktora i



Slika 7. Izlazna amplituda u zavisnosti od frekvencije

Figure 7. Output amplitude as a function of frequency



Slika 8. Frekventno modulisan signal

Figure 8. Frequency-modulated signal

stanje predajnika i prijemnika, ispitan je njihov uticaj na promenu atraktora. Ustanovljeno je da amplituda ulaznog signala ne utiče na atraktor identično na svim frekvencijama. Pri frekvenciji od 500 Hz, amplituda od 700 mV do 3V ne menja bitno oblik atraktora i ne ugrožava prenos podataka. S druge strane, pri frekvenciji od 2 kHz, amplitude manje od 700 mV su poželjne, dok više vrednosti znatno utiču na haotično kolo.

U cilju određivanja propusnog opsega, vršeno je merenje amplitude na izlazu prijemnika u zavisnosti

od frekvencije emitovanog signala na opsegu od 15 Hz do 5 kHz. Rezultati su prikazani na slici 7. Pri frekvenciji od 3 kHz, nivo šuma na izlazu značajno se uvećava, što čini signal neupotrebljivim, jer sinusoidea gubi oblik. Pri ovoj frekvenciji, nivo šuma dostiže polovinu amplitude sinusoide.

Planirano je i određivanje BER-a pri prenosu podataka između dva računara, koje će biti izvršeno u narednom periodu, s obzirom da se trenutno doraduje kôd demodulatora.

Slika 8 prikazuje izgled frekventno modulisanog signala. Gornja kriva predstavlja signal emitovan sa računara, dok je u donjem delu grafika prikazan primljen signal. Jasno su vidljivi prelazi između 400 i 700 Hz.

Zaključak

Pokazana je mogućnost prenosa podataka pomoću sinhronizovanih haotičnih kola, na opsegu od 15 Hz do 2.5 kHz. Frekventna modulacija zadovoljava uslove potrebne za primenu u ovom sistemu prenosa. Tokom daljih istraživanja, biće određen BER, kao pokazatelj mogućnosti primene opisanog komunikacionog sistema za digitalnu komunikaciju. Emitovan signal se raspoređuje po spektru haotičnog oscilatora, što povećava bezbednost informacija prilikom prenosa.

Zahvalnost. Autori se zahvaljuju mentoru Teu Šarkiću, kao i ostalim saradnicima seminara elektronike na pruženoj pomoći.

Literatura

- Belić M. 1990. *Deterministički haos*. Beograd: Institut za fiziku, Sveske fizičkih nauka
- Gleick J. 2001. *Haos*. Beograd: Narodna knjiga
- Perruquetti W., Barbot J. 2006. *Chaos in Automatic Control*. London: Taylor & Francis

Miodrag Basić and Smiljana Todorović

Data Transmission Using Synchronized Chaotic Circuits

In this work, possibility of data transfer through synchronized chaotic circuits has been examined. Chua's circuit has been used as a source of chaotic oscillations. Synchronization has been successfully implemented, while transfer is possible in a 15 Hz to 2.5 kHz range. A frequency modulated digital signal has been successfully transferred through the system, while a demodulator code is in the phase of development. The emitted signal is chaotically modulated and shows all properties of chaos, which is significant for data security. 