DOI: 10.19279/TVZ.PD.2017-5-1-04

POVRATNI INŽENJERING NA PRIMJERU INFRACRVENOG DALJINSKOG UPRAVLJAČA

REVERSE ENGINEERING THROUGH THE EXAMPLE OF AN INFRARED REMOTE CONTROLLER

Josip Kordek, Ivan Lujo

Tehničko veleučilište u Zagrebu, Zagreb, Hrvatska

Sažetak

U članku je objašnjen postupak povratnog inženjeringa na primjeru infracrvenog daljinskog upravljača i pripadajućeg detektora. U potpunom nedostatku dokumentacije za raspoloživi infracrveni upravljač/detektor sustav ostvarena je potpuna funkcionalnost. U postupku se koristi fleksibilna programska okolina za akviziciju podataka i upravljanje. Analizom infracrvenog signala daljinskog upravljača utvrđeni su binarni kodovi vezani uz pojedine tipke, te su naknadno ti kodovi upotrijebljeni za kontrolu drugih uređaja. Korišteni algoritam je dovoljno općenit da se može primijeniti na bilo koji infracrveni daljinski upravljač.

Ključne riječi: *Infracrveni daljinski upravljač, binarni kodovi, povratni inženjering*

Abstract

In this paper the process of reverse engineering through the case of an infrared remote control set (IR remote control with a complement sensor) is described. In spite of total absence of corresponding documentation for the available IR set, complete functionality is achieved. The process is based on a flexible programing control. Through the analysis of the remote control infrared signal the specific button binary codes are established, and are subsequently used to control other devices. The described process is general enough that it can be used with any IR remote control device. The modularity of the code enables easy integration and control within other parts of the code.

Keywords: *Infrared remote control, binary codes, reverse engineering*

1. Uvod

1. *Intoroduction*

Postupak povratnog inženjeringa predstavlja proučavanje svojstava gotovih tehničkih rješenja. Primjenom tako stečenih saznanja potom se ostvaruje poboljšana funkcionalnost postojećeg ili razvoj novih rješenja. Pri tome novo rješenje posjeduje određenu razinu sličnosti s proučavanim sustavom. Postupak se često svodi na analizu načina rada uređaja ili sustava za koje dokumentacija iz različitih razloga ne postoji ili nije dostupna.

Potreba za povratnim inženjeringom javila se kroz ideju za poboljšanje upravljanja maketom dizalice, koja je nastala kao studentski projekt u sklopu kolegija LabVIEW grafičko programiranje (LabVIEW - Laboratory Virtual Engineering Workbench). U prvotnoj varijanti maketom se upravljalo preko korisničkog sučelja na ekranu računala. Mogućnost daljinskog upravljanja se ponudila kao zanimljiva alternativa jer smo na raspolaganju imali infracrveni (IC) sustav upravljač/detektor. Kako je komplet izvorno pripadao TV kartici za računalo, za sam daljinski upravljač (i detektor) nije bila dostupna nikakva dokumentacija. Također na samom daljinskom taknuta nikakva oznaka proizvođača ili modela po kojoj bi se moglo pristupiti traženju pripadne dokumentacije. Način rada ovakvog sustava je načelno opće poznat, što je omogućilo da se uz fleksibilnost LabVIEW programskog paketa i MyDAQ kartice istraži način na koji su kodirane komande u IC signalu. Pri analizi signala korišteni su softverski digitalni filtri za smanjenje razine šuma, odnosno pročišćenje korisnog dijela prikupljenog signala [2].

Postupkom povratnog inženjeringa signala odaslanog prilikom pritiska tipki upravljača komande su uspješno dekodirane i povezane uz točno određene tipke [3]. Dohvat IC signala je obavljen pomoću pripadajućeg infracrvenog senzora koji je na računalo spojen posredstvom MyDAQ akvizicijske kartice, odnosno njenog analognog ulaza. Za pokretanje makete koriste se tri motora pri čemu dva koračna motora služe za rotacijsko pomicanje krana i podizanje odnosno spuštanje hvataljke. Treći, istosmjerni motor bez četkica, služi za otvaranje odnosno zatvaranje hvataljke. Navedeni projekt rezultirao je upravljanjem makete pomoću grafičkog sučelja unutar LabVIEW okoline, pri čemu se podizanje, spuštanje, otvaranje i zatvaranje hvataljke izvodilo tempiranjem pogona istosmjernog motora (kratkim pritiskom na tipkalo). Rotacijsko pomicanje krana izvodilo se kontinuiranim pritiskom tipkala na grafičkom sučelju programa. Primjenom IC daljinskog upravljača eliminirana je nužnost blizine kontrolama računala za upravljanje maketom dizalice. Slični projekti su realizirani u druge svrhe [1].

2. Analiza dohvaćenog signala

2. *Analysis of the captured signal*

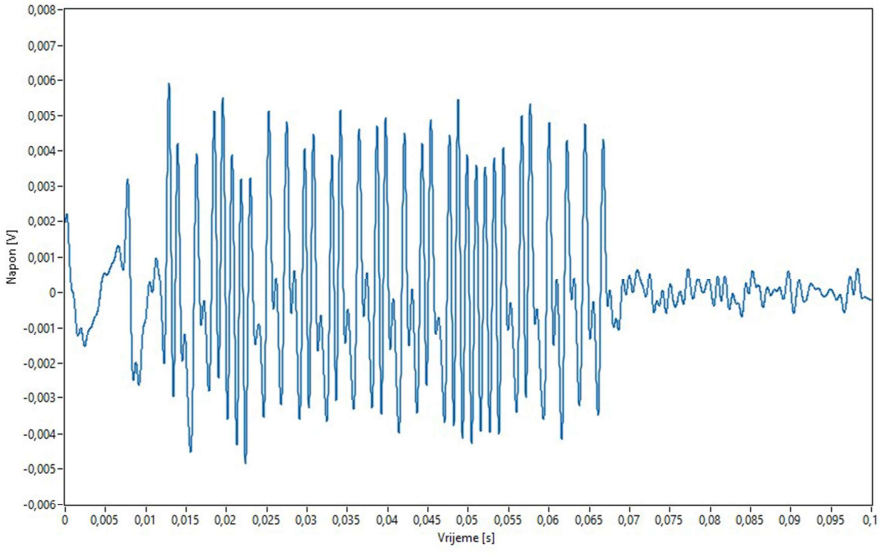
Snimanje analognog signala vršeno je frekvencijom uzorkovanja od 90 kHz. Usporedbom filtriranog analognog signala za pritisnute različite tipke daljinskog upravljača uočena je sličnost između pripadajućih oblika signala.

Na Sl.1 vidljive su kraće i dulje udaljenosti (vremenski razmaci) između susjednih vrhova signala. Broj uzoraka signala između udaljenijih vrhova (impulsa) signala dvostruko je veći od broja uzoraka između manje udaljenih vrhova (impulsa).
To zapažanje dalo je naslutiti da se na taj način prenosi informacija o tome koja je tipka pritisnuta. Konkretno, radi se o FSK (Frequency Shift Keying) modulaciji. Sljedeći problem bio je kako tu informaciju izvući iz detektiranog signala u nekom korisnom obliku, odnosno tako da se može dekodirati.

3. Detektiranje impulsa i broja uzoraka između istih

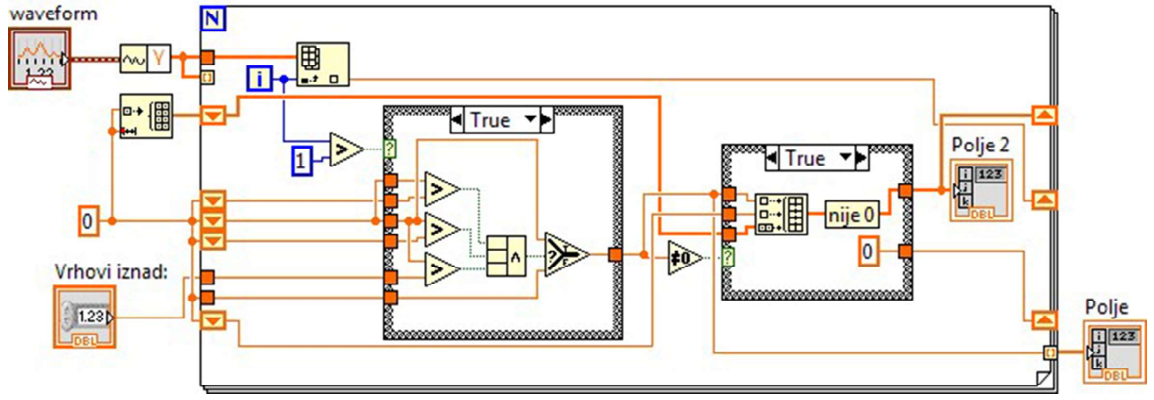
3. *Detecting the pulses and the number of samples between two samples*

Dio koda za spremanje vrijednosti vrhova (napona) signala u polje (Sl.2) također ima i funkciju spremanja broja uzoraka signala između dva susjedna vrha.
Pomoću Get Waveform Components funkcije uzimaju se Y vrijednosti valnog oblika u obliku jednodimenzionalnog polja numeričkih vrijednosti. FOR petlja izvodi se upravo onoliko puta koliko polje ima elemenata zbog funkcije indeksirajućeg ulaznog sučelja petlje za podatke (indeksirajući tunel).
U petlji se nalazi pet posmačnih (Shift) registara od kojih je prvi inicijaliziran kao polje numeričkih vrijednosti bez elemenata dok su ostala četiri inicijalizirana na numeričku vrijednost 0.



Slika 1 *Parametarsko crtanje u AutoCAD-u*

Figure 1 *Parametric Drawing in AutoCAD*



Slika 2 *Dio programa korišten za spremanje vrijednosti vrhova (napona) signala u polje*

Figure 2 *Part of the code used for storing maxima into array*

U posmačne registre se šalju po tri vrijednosti uzastopnih iteracija petlje. Zatim se provjerava je li vrijednost srednjeg posmačnog registra istovremeno veća od dvije susjedne (ranije i kasnije) što bi značilo da se radi o lokalnom maksimumu. Ako je ispitana vrijednost lokalni maksimum (jedan od vrhova valnog oblika) prosljeđuje se na daljnju obradu. Ako vrijednost nije vrh, prosljeđuje se vrijednost 0.

U drugoj izbornoj strukturi stvara se jednodimenzionalno polje numeričkih vrijednosti (slika 2). Ako je vrijednost dovedena iz prve izborne strukture različita od nule dodaje se u polje (Build Arrary) s time da se u polje naizmjence upisuju vrijednosti Y (napon odnosno vrijednost vrha) i broj uzoraka do susjednog vrha.

4. Utvrđivanje binarnih kodova

4. *Determining binary codes*

Iz ranije dobivenog polja prema kodu sa Sl.2 zaključeno je da se između detektiranih impulsa, uz stalnu frekvenciju uzorkovanja, ponavljaju dva različita broja uzoraka signala, oko 100, odnosno oko 200 uzoraka.

Radi bolje točnosti prepoznavanja raspon od 80 do 120 uzoraka smatra se logičkom nulom, dok se raspon od 180 do 220 uzoraka smatra logičkom jedinicom. Na taj način se smanjuju netočnosti uzrokovane slučajnim greškama, kratkim prekidima signala i sl.Kao rezultat navedenog dijela programa na Sl.3 popuni se jednodimenzionalno polje numeričkih vrijednosti (Polje 4) koje sadrži binarnu kombinaciju odnosno dekodiranje dijela signala koji se u tom trenutku analizira.

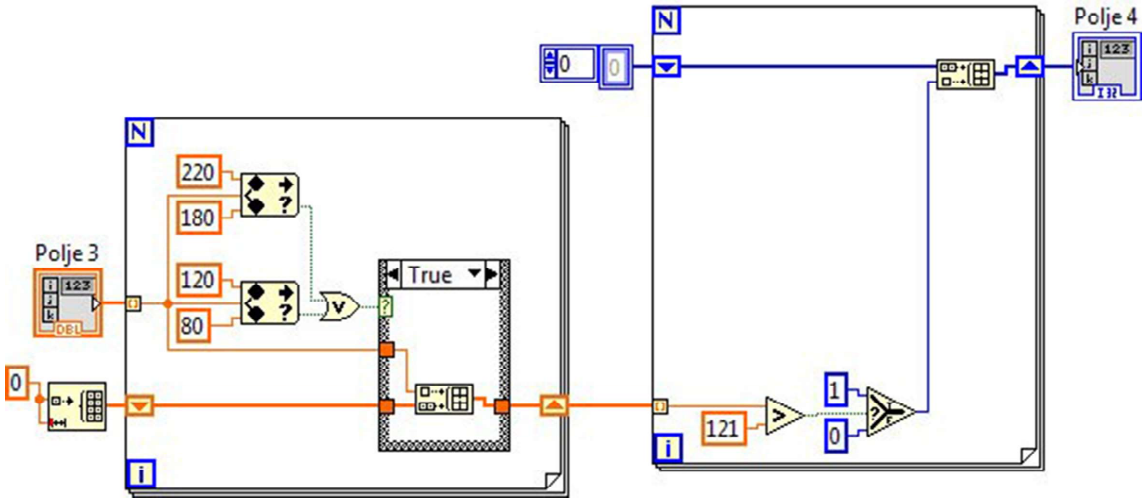
Time je, uporabom povratnog inženjeringa, bez popratne dokumentacije proizvođača daljinskog upravljača ustanovljena tablica binarnih kodova za svaku pojedinu tipku potrebnu za upravljanje maketom dizalice (tablica 1). Za prepoznavanje pritiska pojedine tipke nisu iskorišteni svi bitovi binarnog koda jer oni služe za razlikovanje daljinskih upravljača različitih proizvođača te u ovom slučaju nisu potrebni.

Dio koda (specifičan za proizvođača daljinskog upravljača) se ponavlja te se stoga uzima samo dio koji je različit za pojedine tipke, što olakšava postupak i brzinu rada. Taj je dio binarnog koda istaknut (tablica 1).

Tipka	Binarni kod
2	0110 0001 1101 0110 1101 0000 **0010 1111**
4	0110 0001 1101 0110 1010 0000 **0101 1111**
5	0110 0001 1101 0110 1001 0000 **0110 1111**
6	0110 0001 1101 0110 0101 0000 **0101 0111**
8	0110 0001 1101 0110 0101 0000 **1010 1111**

Tablica 1 *Popis binarnih kombinacija tipki koje se koriste za upravljanje maketom*

Table 1 *List of binary combinations for each of the buttons used in model crane control*



Slika 3 *Dio programa namijenjen za određivanje logičkih vrijednosti*

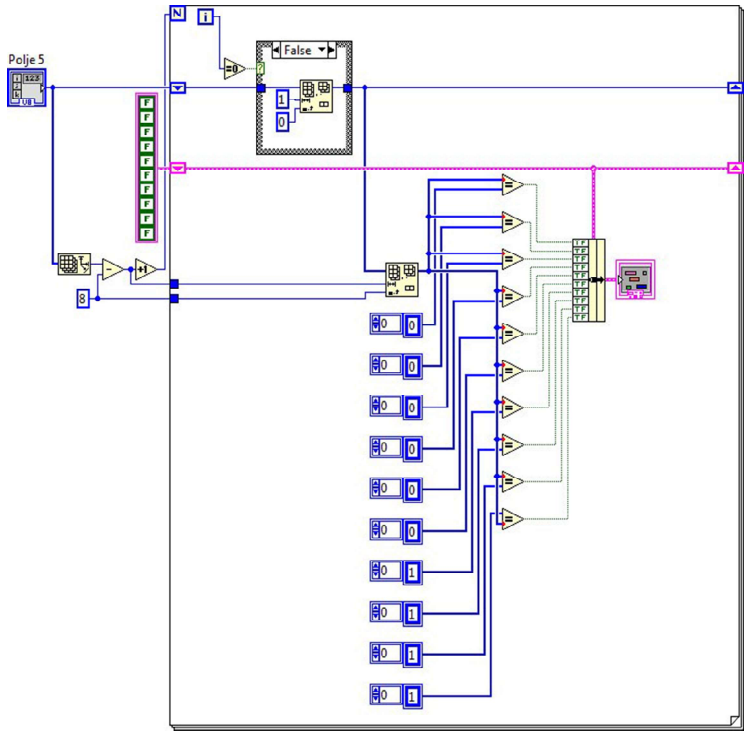
Figure 3 *Code used for determining logical values*

5. Raspoznavanje pritisnutih tipki
5. *Pressed button recognition*

Istaknuti dijelovi binarnih kodova (tablica 1) u programu se koriste kao konstante za usporedbu s kodovima detektiranim u infracrvenom signalu (slika 4). Za provjeru da li dio polja detektiranih vrijednosti (Polje 4) odgovara nekom od polja konstanti iskorišten je dio programa prikazan na Sl.4.
Rezultat prethodno navedenog dijela programa je klaster koji sadrži logičke (Boolean) vrijednosti.

Svaka logička vrijednost se odnosi na drugu tipku daljinskog upravljača čime je omogućeno njihovo prepoznavanje, odnosno prosljeđivanje u svrhu upravljanja drugim dijelova programa odnosno u ovom slučaju, elektromotorima koji pokreću maketu dizalice.

Zadržani su načini upravljanja maketom odnosno rotacija, podizanje i spuštanje, te otvaranje i zatvaranje hvataljke uz jednake interpretacije kao i za tipkala na grafičkom sučelju prvotnog upravljačkog programa.



Slika 4 *Dio programa korišten za prepoznavanje pritiska tipki dalj. upr.*

Figure 4 *Code used for button press recognition*

6. Zaključak
6. *Conclusion*

Zahvaljujući velikoj fleksibilnosti LabVIEW okoline jednostavno je istraženo na koji način infracrveni daljinski upravljač prenosi odnosno kodira informacije (binarne kombinacije za svaku pojedinu tipku) te kako ta saznanja primijeniti unutar drugih programa. Za cijeli postupak potrebna je bila samo MyDAQ akvizicijska kartica kao sučelje za dohvat signala iz infracrvenog senzora. Sva analiza i obrada signala je obavljena u LabVIEW programskoj okolini. Uz određene preinake i dodatke programu za prepoznavanje pritiska tipki moguće je bez dekodiranja binarnog signala iskoristiti daljinski upravljač bilo kojeg proizvođača, te jednostavno „snimiti“ valne oblike kodove za različite tipke i potom ih koristiti kao bazu za usporedbu i interpretaciju detektiranog signala. Postupak se može i automatizirati po potrebi.

Prvotni zadatak ovog projekta je u potpunosti ostvaren i omogućeno je korištenje nepoznatog daljinskog upravljača, usprkos potpunoj nedostupnosti popratne dokumentacije, za upravljanje drugim procesom – u ovom slučaju maketom građevinske dizalice.

7. Reference
7. *References*

[1] Chaodon W.; Yujun W.; The Multimedia Teaching System Based on Infrared Remote-Control Signal Decoder; 2008 International Conference on Computer Science and Software Engineering, DOI: 10.1109/CSSE.2008.112; Hubei, China, 2008.

[2] W. Zheng, L.L. Xie, and Z. Zhang, "Design of self-study infrared remote-controller based on microchip", Computer Measurement & Control, Vol. 15, No. 12, Dec. 2007, pp. 1758-1759.

[3] Sun I.W.F.; Zheng X.E.; A tidy design of decoding to infrared remote control code, Journal of Shandong University of Technology (Sci & Tech), Vol. 20, No. 6, Nov. 2005, ISSN: 1672-6197; pp. 26-29

AUTORI · *AUTHORS*

Josip Kordek
Josip Kordek rođen je 20.02.1993. u Zagrebu. Zbog zanimanja za tehnologiju upisuje Srednju školu Sesvete gdje završava smjer Tehničar za računalstvo. Daljnje školovanje nastavlja na Tehničkom veleučilištu u Zagrebu gdje razvija zanimanje za LabVIEW okolinu. 2016. godine stječe titulu inženjera elektrotehnike obranom završnog rada pod mentorstvom predavača Ivana Luja upravo na opisanu temu.

Korespodencija
josip.kordek@tvz.hr

Ivan Lujo
Ivan Lujo diplomirao je na Fakultetu elektrotehnike i računarstva u Zagrebu. Na Tehničkom veleučilištu Zagreb zaposlen je od 2007. godine. Između ostalih tema bavi se i podučavanjem LabVIEW programiranja koje koristi kao podlogu za brojne studentske projekte i radove.

Korespodencija
ivan.lujo@tvz.hr