Opis pronalaska:

POSTUPAK ZA SMANJENJE VEROVATNOĆE GREŠKE KOD PRODUŽENOG TELEFONSKOG BIRANJA NIZA CIFARA

Oblast tehnike na koju se pronalazak odnosi

Pronalazak pripada oblasti telekomunikacija, uklapa se u trend integracije telefona i računara, a odnosi se na postupak za povećanje pouzdanosti produženog telefonskog biranja niza cifara.

Ovaj pronalazak može biti efikasno primenjen u interaktivnim telefonskim informacionim automatima, posebno u primenama gde se bira niz cifara. Njegove osnovne karakteristike su:

- pouzdanija upotreba tonfrekvencijskog i impulsnog produženog telefonskog biranja,
- mogućnost daleko pouzdanije upotrebe automatskog prepoznavanja govora.

Prema Međunarodnoj klasifikaciji patenata (MKP) oznaka je: H03M 13/00 i H04M 11/00.

Tehnički problem

Produženo telefonsko biranje sve više se koristi u praksi. Ono omogućava automatsko (bez manuelnog posredovanja) biranje lokala, biranje opcija u interaktivnom telefonskom informacionom sistemu, biranje cifara za pristup računu u banci, itd.

Produženo telefonsko biranje omogućava interakciju čoveka i mašine kroz telefonski kanal. Tu komuniciraju čovek s telefonskim aparatom s jedne strane veze i mašina (npr. PC računar) s druge strane veze. U takvom sistemu čovek može direktno da prima samo govorne informacije, a računar može, uz odgovarajuću hardversku i softversku podršku, da prima instrukcije u vidu kodovanih tonfrekvencijskih, impulsnih, ili govornih komandi. U zavisnosti od

načina prenosa instrukcija, kvaliteta veze i korišćenog hardvera i softvera, dolazi do grešaka u prenosu instrukcija. Na slici 1 uticaj svih tih komponenti modelovan je impulsnim šumom.

Dakle, verovatnoća uspešnog opsluživanja klijenta zavisi kako od kvaliteta telefonske veze, tako i od načina prenošenja instrukcija: tonfrekvencijsko biranje, impulsno biranje ili govor. Tonfrekvencijsko biranje otporno je na šum i smetnje karakteristične za telefonske linije i signal tonfrekvencijskog biranja lako prolazi kroz audio interfejs govornih automata. Međutim, sa produženim impulsnim biranjem i prepoznavanjem izolovano izgovorenih cifara ne postiže se zadovoljavajuća tačnost, naročito kada je potrebno birati čitav niz cifara (npr. pristupni broj računa u banci).

Ovaj pronalazak povećava pouzdanost produženog telefonskog biranja niza cifara, tako što ispravlja željeni broj proizvoljnih grešaka, bez obzira da li se radi o impulsnom ili tonfrekvencijskom biranju, ili se produženo biranje vrši izolovanim izgovaranjem niza cifara. Naime, vrši se zaštitno kodovanje niza cifara, tj. koriste se samo oni nizovi cifara koji predstavljaju kodne reči; time se otvara mogućnost zaštitnog dekodovanja niza cifara, tj. detekcije i korekcije pogrešno prenetih cifara. Ovo se postiže i pored toga što je ukupna prenošena poruka kratka za standardne postupke zaštitnog kodovanja.

Stanje tehnike

Produženo telefonsko biranje služi za interakciju čoveka i mašine. Mašina treba da prihvati komande kodovane i prenete produženim biranjem i da ih izvrši, što obično obuhvata saopštavanje govornih informacija, slanje telefaksa i slično.

Produženo telefonsko biranje vrši se nakon uspostavljanja telefonske veze pomoću tonfrekvencijskog ili impulsnog biranja, ili izolovanim izgovaranjem cifara.

Signali tonfrekvencijskog biranja su birački signali koje telefonski aparat šalje svojoj centrali u toku uspostavljanja veze. U procesu produženog telefonskog biranja ovakvi signali se šalju kroz uspostavljenu vezu do odgovarajućeg prijemnika. Oni su kombinacija tonskih signala dve učestanosti iz opsega telefonskog kanala (engl. *dual tone multifrequency, DTMF*). Za razliku od dekadnog (impulsnog) biranja, gde jedan signal predstavlja jedan birački impuls, kod DTMF biranja jedan signal predstavlja jednu celu cifru. Jedan DTMF signal, odnosno biranje jedne cifre

traje oko 100ms (minimalno 40ms), pauza između dva DTMF signala je oko 100ms (minimalno 40ms). Najveći dozvoljeni protok kod DTMF biranja je 10 cifara u sekundi.

Tonfrekvencijsko biranje je za red veličine brže od impulsnog. Pored dekadnih cifara može da se bira još 6 različitih signala što se koristi za posebne usluge, a u procesu produženog biranja koji će biti opisan u ovoj patentnoj prijavi biće iskorišćeni za efikasno zaštitno kodovanje.

Tonfrekvencijsko biranje veoma se uspešno koristi u procesu produženog telefonskog biranja jer se tonfrekvencijski signali pouzdano prenose kroz telefonski kanal i kroz audio interfejs govornog automata.

Signali biranja sa brojčanika telefonskog aparata (engl. *rotary dial pulses*) su niz prekida DC linijske struje sa pauzama između prekida. Protok parova impuls-pauza može biti od 8 do 12 u sekundi. Birački impuls čini od 50% do 67% perioda impuls-pauza. Vremenski interval između dve birane cifre (serije biračkih impulsa) ne sme biti kraći od 320ms. Jedan impuls, tj. jedan signal označava jedan birački impuls (impulsno birana cifra “0” sastoji se od 10 impulsa tj. signala).

Problem primene impulsnog biranja u procesu produženog telefonskog biranja je što oblici električnih signala nastalih produženim impulsnim biranjem mogu biti veoma različiti. Takođe, analogni audio interfejs na prijemnoj strani ne propušta DC signale. Zato signal impulsnog biranja (prekidi jednosmerne struje) stiže u *prijemnik produženog biranja* kao niz klikova koje je mnogo teže detektovati nego tonske signale.

Da bi se omogućila pouzdanija primena impulsnog biranja u procesu produženog telefonskog biranja vrše se dva postupka. U prvom, signal impulsnog biranja se konvertuje u odgovarajući DTMF signal na prijemnom kraju veze; ovo je hardversko rešenje koje značajno poskupljuje sistem, a pouzdanost je manja od DTMF (npr. *Dialogic*, *PIKA*, ili Izraelski *Aerotel*). U drugom postupku, detektovani signal impulsnog biranja dovodi se direktno (a ne kroz audio interfejs) na prijemnu platformu kroz RS232 interfejs, gde se potom softverski dekoduje. Problem ovog pristupa je što oblici električnih signala nastalih produženim impulsnim biranjem mogu biti veoma različiti. Softverska rešenja se oslanjaju na tzv. *treniranje nule*, ali ostaju problemi kao što su: nizak nivo signala, lažni impulsi pre i posle serije biračkih impulsa (preklik i postklik), lažan dvostruki impuls pre niza cifara (niza serija biračkih impulsa), telefonski aparati sa 20 impulsa u sekundi, promena fizičkih karakteristika signala u vremenu, itd. Zato se softverska rešenja baziraju na DSP (*Digital Signal Processing*) procesorima koji svoju snagu koriste za analizu signala nastalih impulsnim biranjem. Tačnost koja se postiže bez treniranja nule kreće se oko 65-70%, a uz treniranje nule oko 90-95%, što je i više od nekih hardverskih rešenja, a još

nedovoljno za pouzdano korišćenje u mnogim primenama sistema s produženim telefonskim biranjem, naročito kada je potrebno birati čitav niz cifara.

Bolja i atraktivnija alternativa produženom tonfrekvencijskom biranju jeste produženo biranje pomoću izolovano izgovorenih cifara. Obimna istraživanja vrše se u svetu i razvijeni su različiti sistemi za prepoznavanje izolovano izgovorenih reči. Međutim, i verovatnoća tačnog automatskog prepoznavanja izolovano izgovorenih reči varira u zavisnosti od korišćenih reči, govornika, jezika, dijalekta i, naravno, kvaliteta veze. U laboratorijskim uslovima, u prepoznavanju izolovano izgovorenih cifara postižu se rezultati od 95% do 98%, dok je taj postotak dosta manji u frekvencijski ograničenim i šumom zagađenim telefonskim primenama.

Dakle, u sredinama sa kvalitetnom telefonskom infrastrukturom i velikim brojem telefona sa mogućnošću tonfrekvencijskog biranja, sistemi koji koriste produženo telefonsko biranje oslanjaju se na pouzdanost produženog tonfrekvencijskog biranja; tamo je impulsno biranje od sve manjeg interesa, a prepoznavanje izolovano izgovorenih cifara je složen problem i još uvek ne postiže zadovoljavajuću tačnost.

Sada će biti analiziran poznati primer primene produženog telefonskog biranja niza cifara - pristup računu u banci. Verovatnoća ispravnog prenosa niza cifara P zavisi od tačnosti prenosa pojedinačnih cifara p. Ako se radi o nizu od, na primer, N cifara, verovatnoća tačnog prenosa celog niza je

$$P_0 = p^N .$$

Na slici 2 dat je primer P_0 za $N = 15$ (kriva označena sa (0/15)); vidi se da sistem zahteva izuzetno veliku verovatnoću tačnog prenosa pojedinačnih cifara, tj. p od blizu 100%, da bi se postigla prihvatljiva verovatnoća ispravnog prenosa niza cifara od npr. $P_0 > 90\%$.

Obično se tih N cifara sastoje od broja računa (R cifara) i pristupne lozinke (L cifara). Takođe, uobičajeno je da poslednja cifra broja računa u banci bude kontrolna i ako se ona iskoristi kao indikacija greške, može se tražiti ponavljanje biranja broja računa. Slično, ako pristupna lozinka ne odgovara primljenom broju računa može se i tu iskoristiti mogućnost ponovljenog biranja lozinke. Na taj način povećava se verovatnoća uspešnog ostvarivanja veze na

$$P_0^A = \left(p^R + (1 - p^R) p^R \right) \cdot \left(p^L + (1 - p^L) p^L \right),$$

ali to ide na račun produženog zauzimanja sistema, zamaranja klijenta ponovnim unosom brojeva, pa i malim usložnjavanjem sistema koji sad vrši i proveru poslednje cifre računa i proveru slaganja broja računa i lozinke. Za primer $R = 9$ i $L = 6$ ($R + L = N$), kriva označena sa (0/15)A na slici

2 vidi se da sistem još uvek zahteva kvalitetnu liniju veze, tj. *p* od 97% ili bar 95% pa da ceo sistem funkcioniše relativno dobro ($P_0^A > 90\%$, odnosno $P_0^A > 80\%$).

Verovatnoća uspešnog ostvarivanja veze mogla bi se dalje povećavati omogućavanjem novih ponavljanja biranja, ali to nema smisla jer je naporno za klijenta, a zadržava sistem.

Na slici 2 (kriva (0/15)A) može se uočiti da je kod ovakvih sistema verovatnoća ispravnog prenosa niza cifara *P* manja od verovatnoće tačnog prenosa pojedinačne cifre *p*. Takođe, očigledan je veliki pad verovatnoće ispravnog prenosa niza cifara *P*, zbog relativno malog pada verovatnoće tačnog prenosa pojedinačnih cifara *p*, tako da ovi sistemi (postojeća rešenja) praktično ne funkcionišu čim je kvalitet telefonske veze takav da se pojedine cifre prenose tačno sa verovatnoćom *p* ispod 90%, jer je tada $P_0^A < 50\%$. Takav slučaj upravo imamo kada se za produženo telefonsko biranje koristi automatsko prepoznavanje govora, ili ako se koriste telefonski aparati s impulsnim biranjem. Zato je produženo telefonsko biranje niza cifara praktično ograničeno samo na primenu tonfrekvencijskog biranja.

Međutim, ako se (kako je predloženo u ovom pronalasku) konstruiše zaštitni kod koji bi omogućio da se npr. u nizu od sedam cifara jedna može popraviti, uz uobičajenu mogućnost jednog ponavljanja biranja, dobila bi se kriva (1/7)A na slici 2. Slično, zaštitno kodovanje para nizova od po sedam cifara, koje omogućuje ispravljanje do po dve greške u oba niza, daje verovatnoću tačnog prenosa čitavog niza od četrnaest cifara u funkciji verovatnoće tačnog prenosa pojedinačne cifre kao na krivoj (2/7)(2/7)A na slici 2. Konačno, zaštitno kodovanje para nizova od po pet cifara, koje omogućuje ispravljanje do po jedne greške u oba niza, daje verovatnoću tačnog prenosa čitavog niza od deset cifara u funkciji verovatnoće tačnog prenosa pojedinačne cifre kao na krivoj (1/5)(1/5)A na slici 2.

Sve ove krive u opsegu od interesa daju veću verovatnoću ispravnog prenosa niza cifara *P* od verovatnoće tačnog prenosa pojedinačnih cifara *p*, što se bez detekcije i korekcije grešaka ne može postići. Mada do sada niko nije ovako popravljao greške u primljenom signalu produženog biranja, slika 2 pokazuje da se postižu značajni rezultati.

Izlaganje suštine pronalaska

Kada se za produženo biranje niza cifara koristi impulsno biranje, ili u slučaju potrebe ili želje da se produženo biranje vrši izolovanim izgovaranjem cifara, kao i u slučaju lošeg kvaliteta telefonskih linija, potrebno je u ovakve sisteme ugraditi mogućnost zaštitnog kodovanja, tj. detektovanja i po mogućnosti ispravljanja pogrešno primljene poruke.

Postupak definisan u ovom pronalasku koristi se za automatsko detektovanje i ispravljanje proizvoljnih grešaka u toku produženog telefonskog biranja niza cifara. Dakle, ovaj postupak oslanja se na tehnike zaštitnog kodovanja. Međutim, većina dobrih zaštitnih kodova su binarni i to predstavlja ograničenje za njihovu primenu u ovakvim sistemima jer je telefonski brojčanik (tastatura) dekadni.

Međutim, ako se od deset cifara dekadnog birača koristi njih osam, može se, uz određene modifikacije, primeniti Reed-Solomon-ov zaštitni koder definisan nad konačnim poljem od 8 elemenata.

Reed-Solomon-ov zaštitni koder u polju sa 16 elemenata može se veoma efikasno koristiti, ali samo sa aparatima za tonfrekvencijsko biranje ili izgovaranjem reči.

Ovi zaštitni kodovi zahtevaju po dve redundantne cifre za ispravljanje po jedne proizvoljne greške u nizu cifara. To je ujedno i najbolje što se zaštitnim kodovanjem može postići. Primena ovog postupka obezbeđuje pouzdanu primenu (govornih, fax, …) informacionih sistema zasnovanih na interakciji telefona i PC računara (produženo biranje), jer u velikom opsegu verovatnoća ispravnog prenosa pojedinačnih cifara p (iznad 80%), obezbeđuje još veću verovatnoću ispravnog prenosa niza cifara P (vidi sliku 2). Time je, pored tonfrekvencijskog biranja, omogućena pouzdanija upotreba i impulsnog biranja, a produženo telefonsko biranje niza cifara pomoću automatskog prepoznavanja izolovano izgovorenih reči postaje značajno pouzdanije i efikasnije.

Kratak opis slika nacrta

Slika 1. - ***Ilustruje model produženog telefonskog biranja.***

Slika 2. - ***Prikazuje rezultat postojećih rešenja i poboljšanje koje pronalazak donosi****:* pokazuje verovatnoće *P* uspešnog prijema produženog biranja niza cifara u funkciji verovatnoće tačnog prenosa pojedinačnih cifara *p.*

Slika 3. - ***Blok dijagram osnovnog rešenja:*** definiše postupak šifrovanja i zaštitnog kodovanja koji se vrši samo jednom i definiše niz cifara koji će se birati

Slika 4. - ***Blok dijagram osnovnog rešenja:*** definiše postupak zaštitnog dekodovanja i dešifrovanja koji se vrši svaki put kada se vrši produženo biranje niza cifara

Slika 5. - ***Blok dijagram rešenja prema varijanti I:*** definiše postupak šifrovanja i zaštitnog kodovanja koji se vrši samo jednom i definiše niz cifara koji će se birati

Slika 6. - ***Blok dijagram rešenja prema varijanti I:*** definiše postupak zaštitnog dekodovanja i dešifrovanja koji se vrši svaki put kada se vrši produženo biranje niza cifara

Detaljan opis pronalaska

Na slici 1 ilustrovan je model sistema u kojem se vrši interakcija čovek-računar kroz telefonsku liniju. Nakon uspostavljanja telefonske veze komuniciraju čovek s telefonskim aparatom s jedne strane veze i mašina (npr. PC računar) s druge strane veze. U takvom sistemu, čovek može direktno da prima samo govorne informacije, a računar može, uz odgovarajuću hardversku i softversku podršku, da prima instrukcije u vidu kodovanih tonfrekvencijskih, impulsnih ili govornih komandi. U zavisnosti od načina prenosa instrukcija, kvaliteta veze i korišćenog hardvera i softvera, dolazi do grešaka u prenosu instrukcija koje na slici 1 simbolizuje *impulsni šum*.

Pronalazak se odnosi na postupke za smanjenje verovatnoće pogrešnog prijema instrukcija (niza cifara) koji se postiže dodatnom obradom signala na prijemu - zaštitno dekodovanje, uz prethodno definisanje mogućih nizova cifara (kodnih reči) - zaštitno kodovanje.

Kako je sada na prijemu potrebno razlikovati nizove cifara, za ispravljanje jedne pogrešno prepoznate cifre u nizu potrebno je produžiti niz cifara sa dve dodatne. Dva niza cifara već su se razlikovala bar na jednoj cifri. Dodavanje dve cifre vrši se tako da se sad dva niza razlikuju bar na tri cifre tako da greškom u prepoznavanju jedne cifre još uvek možemo tačno da prepoznamo pravi niz cifara.

Samo najefikasniji zaštitni koderi dostižu ovakve performanse. Takav je Reed-Solomon-ov (RS) koder i dekoder. Problem njegove primene u kompjuterskoj telefoniji ogleda se u tome što je telefonski birač dekadni a ovaj kod radi sa ciframa iz brojnih sistema sa osnovom brojanja 2^k. Korišćenje alfabeta sa 16 cifara (koje obuhvataju i 10 dekadnih cifara) zgodno je jer su u takvom RS kodu kodne reči od po 15 cifara što je dovoljno za mnoge aplikacije (npr. broj računa u banci i pristupna lozinka), međutim, problem je što nakon kodovanja dodatne cifre ne moraju biti dekadne. Za prenos ovih cifara dekadnim biračem potrebno je biranje dve dekadne cifre, što je nepraktično; alternativa - težinsko prevođenje heksadecimalnog niza cifara u dekadni nije primenjivo, jer greška u prenosu jedne takve dekadne cifre može prouzrokovati niz pogrešno prenetih heksadecimalnih cifara. Dakle, primena Reed-Solomon-ovog kodera u polju sa 16 elemenata neefikasna je sa impulsnim biranjem, ali može da bude veoma praktična sa telefonskim aparatima sa tonfrekvencijskim biranjem, jer oni mogu da biraju 16 različitih signala.

Rešenje koje omogućava nesmetanu upotrebu i telefona sa dekadnim biračem, jeste da se koristi samo osam od deset dekadnih cifara. Drugim rečima, u nizu cifara koje klijent bira ne pojavljuje se svih deset dekadnih cifara, što za njega uopšte i nije bitno. Upotrebom osam od deset dekadnih cifara, ne samo da je povećana pouzdanost prenosa pojedinačnih cifara (ne koriste se recimo dve cifre na kojima sistem za automatsko prepoznavanje govora najčešće greši) već je omogućena i direktna primena Reed-Solomon-ovog kodera na polju sa 8 elemenata $\mathrm{GF}(8) = \left(+, \cdot, \{0,1,2,3,4,5,6,7\}\right)$. U takvom RS kodu kodne reči sastoje se od po 7 oktalnih cifara, od kojih su npr. 5 niz koji se želi preneti i 2 redundantne koje omogućavaju ispravljanje jedne pogrešno prenete cifre u nizu od tih 7 cifara, ili, kodne reči od 7 oktalnih cifara od kojih su 3 informacione i 4 redundantne koje omogućavaju ispravljane do dve greške u nizu od 7 cifara.

Na primer, za jednoznačan pristup računu u banci, obično je dovoljno razlikovati do nekoliko desetaka hiljada računa. Za to je dovoljno 5 do 6 oktalnih cifara ($8^5 = 32768$, $8^6 = 262144$). Zato predlažemo da se ne prenosi 9 do 12 dekadnih cifara koje su stvarni broj računa u banci i pristupna lozinka od dodatnih 5-6 cifara, već da se klijentu dodeli šifrovani broj sa 5 ili 6 oktalnih cifara. Lozinka je sastavljena od onoliko cifara koliko je dugačak šifrovani (tajni) broj računa. Međutim kako je taj tajni broj zaštitno kodovan, nepoznanica su i dodatne (redundantne) cifre. Tako je lozinka ugrađena u ceo broj, tj. u N cifara, što je bolja kriptozaštita nego sa lozinkom od $L = 5$ ili 6 cifara koliko su imali prethodni sistemi. Kako su u RS koderu nad GF(8) kodne reči dužine 7, od kojih svake dve redundantne obezbeđuju ispravljanje po jedne proizvoljne greške, može se koristiti nekoliko sistema. Sledi **opis osnovnog rešenja**, koje je ilustrovano na slikama 3 i 4.

Neka je višecifreni broj koji treba da se prenese u procesu produženog telefonskog biranja jedan niz dekadnih cifara, smešten u blok 1 na slici 3. To je originalni niz cifara koji predstavlja npr. cifre iz broja računa u banci koje su karakteristične za samo jednog klijenta, npr. njegov redni broj. Šifrovanje 2 je proizvoljni postupak koji jednoznačno pridružuje niz od pet oktalnih cifara bilo kom od 32768 originalnih nizova cifara (npr. dekadnom broju 32768 dodeli se oktalni broj 12345). Šifrovani petocifreni oktalni broj računa memorisan je u bloku 3 na slici 3.

Zaštitno kodovanje 4 vrši se RS koderom definisanim nad poljem od 8 elemenata (cifre oktalnog alfabeta). U procesu zaštitnog kodovanja 4 izračunavaju se dve redundantne cifre (npr. 02) za dati niz od pet oktalnih cifara (npr. 12345) i njihovim dodavanjem na taj niz dobija se niz od sedam oktalnih cifara (npr. 1234502). To je broj koji se bira u procesu produženog telefonskog biranja i on je smešten u bloku 5 na slici 1. Taj sedmocifreni broj je broj koji se samo jednom određuje i sa kojim se uvek ubuduće pristupa željenom broju (npr. račun u banci). Pri tome je zaštitnim kodovanjem omogućeno ispravljanje jedne ili detektovanje dve pogrešno prenete oktalne cifre.

Ako se u toku produženog biranja sedam cifara jedna pogrešno primi (primljeni niz od sedam cifara je smešten u bloku 11 na slici 4) zaštitni dekoder 12 će detektovati i ispraviti tu grešku. Npr. ako se bira niz cifara 1237502 (sadržaj bloka 11), RS dekoder 12 će pomoću Berlkemp-Mesi-jevog i Forni-jevog algoritma analizirati primljenu sekvencu i odrediće lokaciju i vrednost pogrešno prenete cifre i ispraviće je. Rezultat dekodovanja je u bloku 13 na slici 4. Ako se desi više od jedne pogrešno prenete cifre u nizu od sedam cifara, dekoder će detektovati neispravljiv uzorak greške i daće jedan zahtev za ponovno biranje.

Dakle, šifrovani broj računa od pet oktalnih cifara $\underline{x} = (x_1, x_2, x_3, x_4, x_5)$ koduje se RS koderom $\underline{c} = RS(\underline{x})$ koji dodaje dve oktalne cifre $\underline{c} = (x_1, x_2, x_3, x_4, x_5, d_1, d_2)$ tako da dekoder može da popravi jednu ili da detektuje poziciju dve greške na prijemu. Klijent unosi samo sedam cifara ($\underline{c}$) koje samo on zna i koje samo računar u banci može da dekoduje (blok 12) i potom dešifruje (blok 14), tj. odredi odgovarajući stvarni broj računa (sadržaj bloka 15) i pristupi mu. Pored smanjenog opterećivanja klijenta (bira 7 umesto 15-tak cifara) verovatnoća uspešnog opsluživanja klijenta (tačnog dekodovanja) toliko je povećana da se mnogo pouzdanije mogu koristiti i sistemi sa prepoznavanjem izolovano izgovorenih cifara i sistemi sa impulsnim biranjem. Odgovarajuća kriva na slici 2 označena je sa (1/7)A i poboljšanje u odnosu na postojeća rešenja kao što je (0/15)A, veoma je značajno. Primer, ukratko

- klijentu se interno dodeli tajna šifra $\underline{x} = 12345$
- ona se koduje sa (taj broj klijent bira) $\underline{c} = 12345\ 02$
- neka se primi $\underline{c} + \underline{e} = 123\underline{7}5\ 02$

- dekoder će ispraviti grešku $(\vec{c} + \vec{e}) - \vec{e} = 12345\ 02$

$\vec{e}$ je greška koja se desila na liniji, a $\vec{e}$ je procena te greške do koje dolazi RS dekoder (blok 12) na osnovu primljene sekvence brojeva (sadržane u bloku 11). Može se uočiti sistematska struktura RS koda, tj. da su prve cifre kodne reči $\vec{c}$ iste kao šifrovani broj računa $\vec{x}$, a da se redundantne cifre dodaju na kraju kodne reči.

Osnovno rešenje koristi se kada je dovoljno razlikovati do 8^5= 32768 različitih brojeva računa, tj. nizova cifara. Ono obezbeđuje veću verovatnoću ispravnog prenosa celog niza cifara *P*, od verovatnoće tačnog prenosa pojedinačnih cifara *p*, za sve vrednosti $p > 78\%$ (videti krivu (1/7)A na slici 2.

Međutim, kada je potrebno razlikovati više od 8^5= 32768 a manje od 8^6= 262144 brojeva računa, potrebno je preneti niz od šest oktalnih cifara. Kako tada u kodnim rečima od sedam oktalnih cifara (RS kod u GF(8)) nema prostora ni za dve redundantne cifre koje bi obezbedile ispravljanje jedne greške, u ovoj varijanti rešenja vrši se podela 6-cifrenog šifrovanog broja računa na dva dela koji se nezavisno prenose u dve uzastopne kodne reči. U daljem tekstu dato je **rešenje prema varijanti I**. Ovaj algoritam ilustrovan je dijagramom toka na slikama 5 i 6.

Algoritam je sličan kao kod osnovnog rešenja, samo što se nakon šifrovanja 22 originalnog niza brojeva 21, šifrovani broj računa 23 sada sastoji od šest oktalnih cifara; on se u sledećem koraku 24 podeli na dva dela od po tri cifre (blokvi 25 i 26) koje se posebno koduju 27 dodavanjem po četiri redundantne cifre i omogućava se ispravljanje po do dve greške u obe kodne reči. Kodne reči - oktalni sedmocifreni brojevi iz 28 i 29 se nastavljaju 30 jedan iza drugog u niz od četrnaest cifara (sadržaj bloka 31). Ovaj postupak se uradi samo jedanput i on definiše pristupni broj od četrnaest cifara koje će klijent birati u procesu produženog telefonskog biranja za pristup informacijama o svome računu. Klijent unosi četrnaest cifara a dekoder ispravlja do četiri greške što daje veoma veliku verovatnoću ispravnog prenosa niza cifara. Odgovarajuća kriva na slici 2 označena je sa (2/7)(2/7)A. Blok dijagram postupka na prijemu prikazan je na slici 6. Primljeni niz od četrnaest cifara 41 podeli se 42 na dva niza: prvih (blok 43) i drugih (blok 44) sedam cifara. RS dekoder 45 dekoduje ta dva niza i kao rezultat daje dva niza od po tri oktalne cifre, 46 i 47, koji se nastavljaju 48 jedan na drugog i formiraju dekodovani šestocifreni oktalni broj sadržan u bloku 49. Taj broj se na kraju dešifruje 50 u originalni broj (npr. broj računa u banci) čiji je sadržaj dat u bloku 51 na slici 6.

Primer, ukratko:

- klijentu se interno dodeli tajna šifra $\vec{x} = 123456$
- ona se koduje sa (taj broj klijent bira) $\vec{c} = 123\ 2631\ \ 456\ 5264$

- neka se primi $\vec{c} + \vec{e} = 113\ 2637\ \ 706\ 5264$
- dekoder će ispraviti greške $(\vec{c} + \vec{e}) - \vec{e} = 123\ 2631\ \ 456\ 5264$

Rešenje prema varijanti I obezbeđuje veću verovatnoću ispravnog prenosa celog niza cifara *P*, od verovatnoće tačnog prenosa pojedinačnih cifara *p*, za sve vrednosti $p > 72\%$ (videti krivu (2/7)(2/7)A na slici 2.

Ako se želi smanjiti broj cifara koje klijent treba da bira može se koristiti **podvarijanta varijante I** osnovnog rešenja, sa skraćenim RS kodom. Sledi opis ove podvarijante.

Sistem je sličan prethodnom samo što se koristi skraćeni RS kod, gde se ne dodaje maksimalan broj redundantnih cifara. Na oba trocifrena oktalna broja dodaje se po dve redundantne cifre. Klijent bira 10 cifara, a popravljaju se do 2 greške. Odgovarajuća kriva na slici 2 označena je sa (1/5)(1/5). Na primer:

- klijentu se interno dodeli tajna šifra $\vec{x} = 123456$
- ona se koduje sa (taj broj klijent bira) $\vec{c} = 123\ 70\ \ 456\ 64$
- neka se primi $\vec{c} + \vec{e} = 123\ 60\ \ 406\ 64$
- dekoder će ispraviti greške $(\vec{c} + \vec{e}) - \vec{e} = 123\ 70\ \ 456\ 64$

Rešenje prema ovoj varijanti obezbeđuje veću verovatnoću ispravnog prenosa celog niza cifara *P*, od verovatnoće tačnog prenosa pojedinačnih cifara *p*, za sve vrednosti $p > 80\%$ (videti krivu (1/5)(1/5)A na slici 2.

Svi navedeni primeri rade tako da se kodovanje vrši Reed-Solomon-ovim zaštitnim koderom definisanim nad poljem od 8 elemenata, $\mathrm{GF}(8) = \left(+, \cdot, \{0,1,2,3,4,5,6,7\}\right)$. Dekodovanje primljenog niza brojeva vrši se na pojedinim kodnim rečima koje se sastoje od 7 uzastopnih cifara, ili od npr. 5 uzastopnih cifara u skraćenom kodu. Koristi se koder u sistematskom obliku. Za dekodovanje, tj. za procenu uzorka greške $\vec{e}$ koriste se Berlkemp-Mesi i Forni algoritmi za određivanje lokacija i intenziteta grešaka, respektivno.

^injenica je da su ovakvi zaštitni kodovi projektovani za kodovanje dugačkih binarnih sekvenci na kojima ispravljaju određen broj grešaka, npr. M. Verovatnoća da šum prevede jednu kodnu reč u oblast odlučivanja druge kodne reči srazmerna je sa $\left(1/M!\right)$ i predstavlja neželjen, ali za veliko M veoma malo verovatan događaj - neispravljiv uzorak greške. U sistemu koji je ovde opisan koristi se Reed-Solomon-ov zaštitni koder sa neuobičajeno kratkim kodnim rečima, koji nije u stanju da ispravi veliki broj grešaka M, pa je verovatnoća da se bira jedan niz brojeva (kodna reč) i da se dekoduje drugi niz brojeva relativno velika i iznosi

$$\frac{1}{M!} \cdot P(m > M),$$

gde je $P(m > M)$ verovatnoća da se dogodio veći broj grešaka (m) od onog koji sistem može da ispravi (M).

Srećom, u predloženoj primeni to nije ozbiljan problem jer cilj je bio da se isprave uzorci sa najviše M slučajnih grešaka (i to radi), a uzorci sa više od M pogrešno primljenih cifara svakako su izgubljen pokušaj za autorizovanog pozivaoca. Za neautorizovanog pozivaoca koji bez znanja lozinke pokuša da pristupi nekom konkretnom broju računa koji ga interesuje, jedini povoljan ishod bio bi da dobije baš taj račun.

Ovde je važno naglasiti da se zahtev za ponovno biranje broja dešava daleko ređe u sistemima koji imaju mogućnost automatskog ispravljanja grešaka. Ta verovatnoća jednaka je verovatnoći da se desi više grešaka od broja grešaka koje sistem može da ispravi. Značajnim smanjivanjem broja zahteva za ponavljanjem smanjuje se prosečno trajanje opsluživanja jednog klijenta. Drugim rečima, uz drastično povećanje tačnosti (slika 2), povećava se i efikasnost sistema, a klijenti se retko zamaraju ponavljanjem biranja broja. Sledi detaljan opis slike 2.

Slika 2. Verovatnoća *P* uspešnog prijema produženog biranja niza cifara u funkciji verovatnoće tačnog prenosa pojedinačnih cifara *p*. '(K/N)': bira se N cifara, a sistem ispravlja do K grešaka; 'A': označava jedno ponavljanje biranja

a) (0/15): Bira se 15 cifara. Sistem je bez mogućnosti za ispravljanje grešaka i bez automatskog zahteva za ponovnim biranjem;
b) (0/15)A: Bira se 15 cifara. Sistem je bez mogućnosti za ispravljanje grešaka ali sa mogućnošću jednog automatskog zahteva za ponovnim biranjem (tako radi većina postojećih sistema);
c) (1/7)A: Bira se samo 7 cifara. Sistem ispravlja 1 grešku i ima mogućnost jednog automatskog zahteva za ponovnim biranjem;
d) (1/5)(1/5)A: Bira se 10 cifara. Sistem ispravlja po 1 grešku u obe kodne reči od po 5 cifara i ima mogućnost jednog zahteva za ponovnim biranjem;
e) (2/7)(2/7)A: Bira se 14 cifara. Sistem ispravlja po najviše 2 greške u obe kodne reči od po 7 cifara i ima mogućnost jednog zahteva za ponovnim biranjem;

Način industrijske ili druge primene pronalaska

Primena u produženom biranju pristupnog niza cifara za npr. račun u banci: klijentima u banci jednoznačno se dodeli šifrovani broj računa - npr. niz od 6 oktalnih cifara, koji se podeli na dva niza po 3 cifre, a potom se za svake 3 cifre odrede 4 redundantne Reed-Solomon-ovim kodovanjem. Prenosi se 14 cifara, dekoduju se dve primljene kodne reči od po 7 cifara sa mogućnošću ispravljanja po 2 greške u obe kodne reči.

Ovaj pronalazak omogućuje veoma pouzdan rad (verovatnoću tačnog prenosa niza cifara P preko 97%) čak i za vrednosti p (verovatnoće tačnog prenosa pojedinih cifara) koje su u domenu praktično ostvarivih verovatnoća u sistemima za automatsko prepoznavanje izolovano izgovorenih cifara od npr. $p = 80\%$.

Dakle, primenom postupka iz ovog pronalaska omogućuje se uspešan rad sistema u kojima se vrši produženo biranje niza cifara čak i sa sistemima s impulsnim biranjem, a po prvi put postaje pouzdana upotreba atraktivnih sistema sa prepoznavanjem govora, kod kojih postoji mogućnost dodatne provere prava pristpa pomoću sistema za automatsku verifikaciju govornika analizom karakteristika njegovog glasa.

Potpis podnosioca prijave

_____

_____

Patentni zahtev

1. **Postupak za smanjenje verovatnoće greške kod produženog telefonskog biranja niza cifara** koji se koristi u sistemima sa manje od 8^5= 32768 nizova cifara, **naznačen time**, što se svakom nizu cifara pridružuje (po nekoj šifri) jedinstven petocifreni oktalni broj, koji se potom zaštitno koduje u Reed-Solomon-ovom koderu definisanom nad poljem od 8 elemenata, tako da mu se dodaju dve redundantne cifre i tako se formira sedmocifreni oktalni broj koji reprezentuje jedan od 32768 nizova cifara.
2. **Postupak prema patentnom zahtevu 1, naznačen time**, što se na prijemu sedmocifreni oktalni broj dekoduje u Reed-Solomon-ovom dekoderu, tako da se, ako postoji jedna pogrešno preneta cifra u nizu od sedam oktalnih cifara, ta greška detektuje i ispravi i tako dekoduje petocifreni oktalni broj i dešifruje njemu odgovarajući niz cifara, a ako se detektuje više od jedne greške u primljenom nizu od sedam oktalnih cifara, da se generiše zahtev za jednim ponavljanjem biranja niza cifara.
3. **Postupak prema patentnom zahtevu 1 i varijanti I,** koji se koristi u sistemima sa manje od 8^6= 262144 nizova cifara, **naznačen time**, što se svakom nizu cifara pridružuje (po nekoj šifri) jedinstven šestocifreni oktalni broj, koji se konvertuje u dva trocifrena broja od kojih se svaki zaštitno koduje u Reed-Solomon-ovom koderu definisanom nad poljem od 8 elemenata, tako da se svakom trocifrenom oktalnom broju dodaju po četiri redundantne oktalne cifre, a zatim se formira četrnaestocifreni oktalni broj tako što se iza prvog trocifrenog broja dodaju njegove četiri redundantne cifre, a zatim se nastavlja drugi trocifreni broj i njegove četiri redundantne cifre i tako se formira četrnaestocifreni oktalni broj koji reprezentuje jedan od 262144 nizova cifara.
4. **Postupak prema patentnom zahtevu 3, naznačen time**, što se na prijemu četrnaestocifreni oktalni broj deli na prvih i drugih sedam cifara, sedmocifreni oktalni brojevi se jedan po jedan dekoduju u Reed-Solomon-ovom dekoderu, tako da se, ako postoji do dve pogrešno prenete cifre u nizovima od po sedam oktalnih cifara, te greške detektuju i isprave i tako se dekoduju dva trocifrena oktalna broja, koja se nastave jedan na drugog i formira se šestocifreni oktalni broj koji se konačno dešifruje u njemu odgovarajući niz cifara, a ako se detektuje više od dve greške u nekom od primljenih nizova od po sedam oktalnih cifara, da se generiše zahtev za jednim ponavljanjem biranja niza cifara.
5. **Postupak prema patentnom zahtevu 1 i varijanti II,** koji se koristi u sistemima sa manje od 8^6= 262144 nizova cifara, **naznačen time**, što se svakom nizu cifara pridružuje (po nekoj šifri) jedinstven šestocifreni oktalni broj, koji se konvertuje u dva trocifrena broja od kojih se

svaki zaštitno koduje u skraćenom Reed-Solomon-ovom koderu definisanom nad poljem od 8 elemenata, tako da se svakom trocifrenom oktalnom broju dodaju po dve redundantne oktalne cifre, a zatim se formira desetocifreni oktalni broj tako što se iza prvog trocifrenog broja dodaju njegove dve redundantne cifre, a zatim se nastavlja drugi trocifreni broj i njegove dve redundantne cifre i tako se formira desetocifreni oktalni broj koji reprezentuje jedan od 262144 nizova cifara.

6. **Postupak prema patentnom zahtevu 5, naznačen time**, što se na prijemu desetocifreni oktalni broj deli na prvih i drugih pet cifara, petocifreni oktalni brojevi se jedan po jedan dekoduju u skraćenom Reed-Solomon-ovom dekoderu, tako da se, ako postoji najviše po jedna pogrešno preneta cifra u nizovima od po pet oktalnih cifara, te greške detektuju i isprave i tako se dekoduju dva trocifrena oktalna broja, koja se nastave jedan na drugog i formira se šestocifreni oktalni broj koji se konačno dešifruje u njemu odgovarajući niz cifara, a ako se detektuje više od jedne greške u nekom od primljenih nizova od po pet oktalnih cifara, da se generiše zahtev za jednim ponavljanjem biranja niza cifara.
7. **Postupak prema patentnom zahtevu 1 i varijanti III, naznačen time**, što se cifre u nizu od najviše 13 dekadnih cifara posmatraju kao heksadecimalni brojevi, pa se taj niz cifara zaštitno koduje u Reed-Solomon-ovom koderu definisanom nad poljem od 16 elemenata, tako da mu se dodaju redundantne heksadecimalne cifre i to tako da se formira niz od najviše 15 heksadecimalnih cifara koji reprezentuje polazni niz od najviše 13 cifara koje se biraju izolovanim izgovaranjem do 15 elemenata heksadecimalnog alfabeta ili tonfrekvencijskim biranjem.
8. **Postupak prema patentnom zahtevu 7, naznačen time**, što se na prijemu vrši dekodovanje u Reed-Solomon-ovom dekoderu koje kao rezultat daje dekodovani niz od najviše 13 cifara, a u slučaju ako se produženo biranje vrši izolovanim izgovaranjem reči, onda se vrši i dodatna automatska verifikacija govornika.

Potpis podnosioca prijave

_____

_____

Apstrakt

POSTUPAK ZA SMANJENJE VEROVATNOĆE GREŠKE KOD PRODUŽENOG TELEFONSKOG BIRANJA NIZA CIFARA

Verovatnoća tačnog prenosa niza cifara P u procesu produženog telefonskog biranja zavisi od verovatnoće tačnog prenosa pojedinačnih cifara p i od dužine niza N: $P = p^N$. Kako je p manje od 1, to je P manje ili daleko manje od p. Zato se pouzdano produženo biranje niza cifara moglo vršiti samo tonfrekvencijskim biranjem $(p \cong 100\%)$, a impulsno biranje i automatsko prepoznavanje izolovano izgovorenih cifara ne postižu zadovoljavajuću tačnost. Na primer, sa $p = 85 \div 95\%$ za $N = 15$ (npr. pristupni broj računu u banci) postiže se svega $P = 10 \div 50\%$ odnosno $30 \div 80\%$ ako je omogućeno jedno ponavljanje biranja.

Ovaj pronalazak definiše postupak zaštitnog kodovanja (detekcije i korekcije grešaka) produženog telefonskog biranja koji obezbeđuje da P bude veće od p u opsegu vrednosti p koje se mogu ostvariti i automatskim prepoznavanjem izolovano izgovorenih cifara ili impulsnim biranjem. Na primer, sa $p = 85 \div 95\%$ postiže se P veće od p, a uz jedno ponavljanje biranja postiže se P blizu 100%. Uz to, omogućavanjem ispravljanja grešaka smanjena je učestanost zahteva za ponovnim biranjem, čime je smanjeno prosečno trajanje opsluživanja jednog poziva i povećana efikasnost sistema. Ako se produženo biranje vrši govorom, postoji dodatna mogućnost provere prava pristupa pomoću sistema za automatsku verifikaciju govornika analizom karakteristika njegovog glasa.

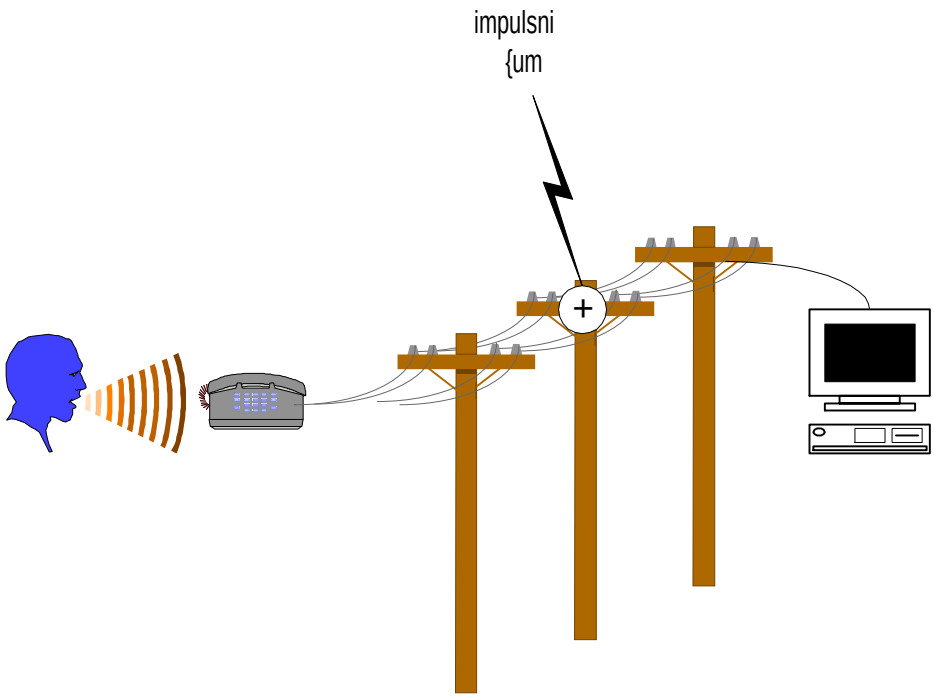
Potpis podnosioca prijave

_____

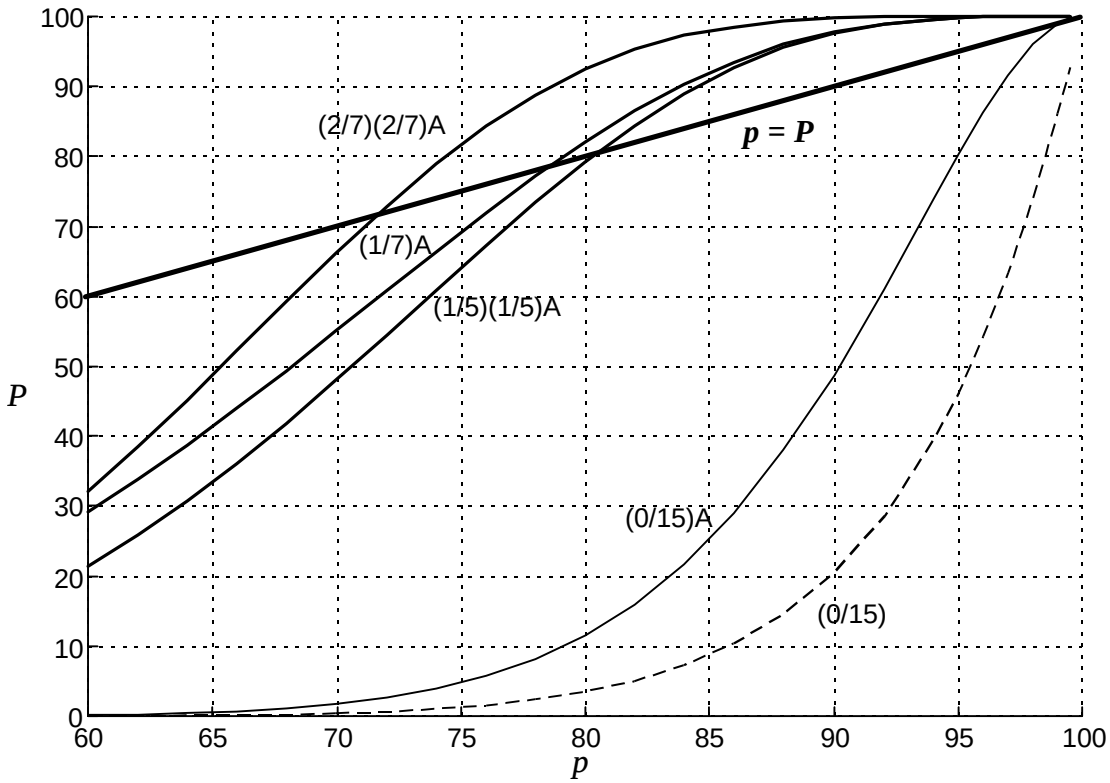
_____

Nacrt pronalaska

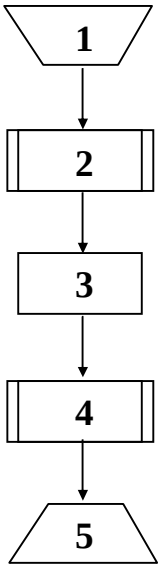
POSTUPAK ZA SMANJENJE VEROVATNOĆE GREŠKE KOD PRODUŽENOG TELEFONSKOG BIRANJA NIZA CIFARA



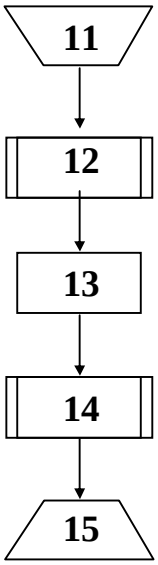
Slika 1.


100
90
80
70
60
50
40
30
20
10
0
P
60
65
70
75
80
85
90
95
100
p
(2/7)(2/7)A
p = P
(1/7)A
(1/5)(1/5)A
(0/15)A
(0/15)

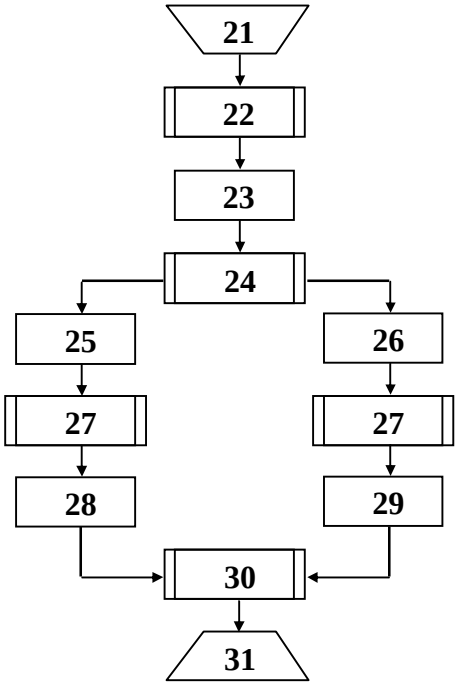
Slika 2.



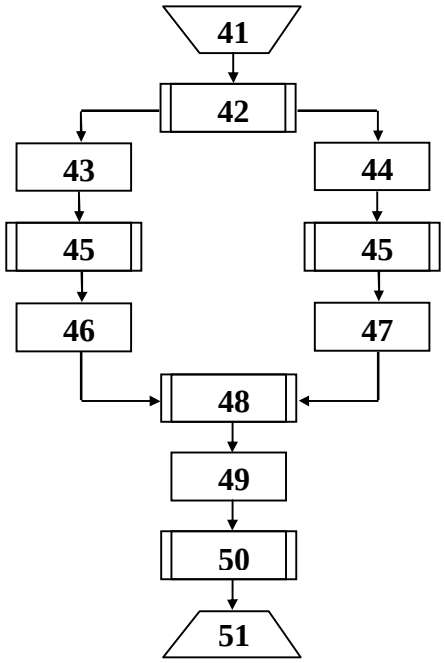
Slika 3.



Slika 4.



Slika 5.

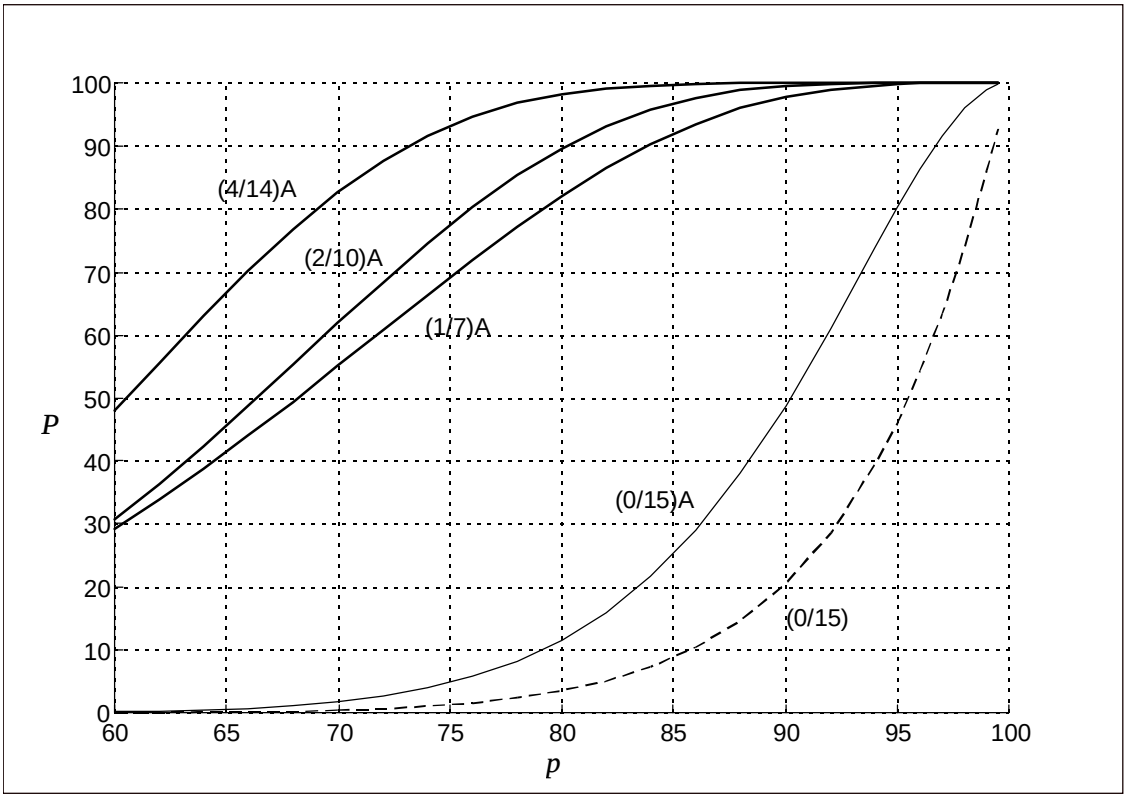


Slika 6.

Potpis podnosioca prijave

_____

_____



Patentni zahtev broj: P-434/97

Datum podnošenja: 4.XI’97.