



(19) REPUBLIKA HRVATSKA
DRŽAVNI ZAVOD ZA
INTELEKTUALNO VLASNIŠTVO

(21) Broj prijave:



HR P20000146A A2

HR P20000146A A2

(12) PRIJAVA PATENTA

(51) Int. Cl. 7: H 04 N 5/913

(22) Datum podnošenja prijave patenta u HR: 13.03.2000.

(41)(43) Datum objave prijave patenta u HR: 31.08.2000.

(86) Broj međunarodne prijave: PCT/IB98/01511

Datum podnošenja međunarodne prijave: 22.09.1998.

(87) Broj međunarodne objave: WO 99/16244

Datum međunarodne objave: 01.04.1999.

(31) Broj prve prijave: 97402238.6; (32) Datum podnošenja prve prijave: 25.09.1997.; (33) Država ili organizacija podnošenja prve prijave: EP

(71) Podnositelj prijave:

Canal + Societe Anonyme, 85/89, quai Andre Citroeen, 75711 Paris Cedex
15, FR

(72) Izumitelj:

Michel Maillard, 13, avenue du Parc, 78120 Rambouillet, FR

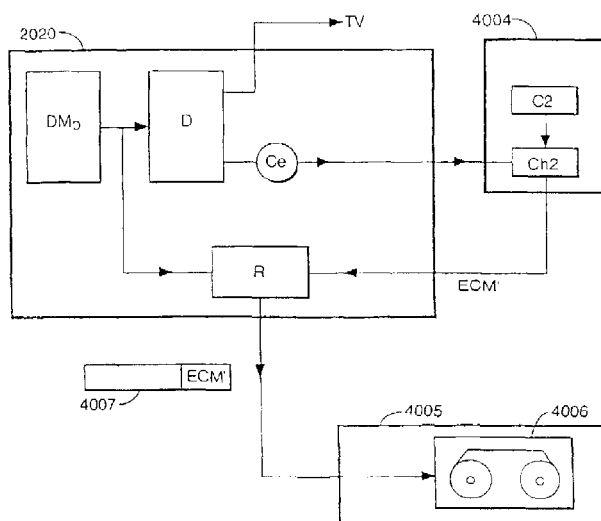
(74) Punomoćnik:

PRODUCTA d.o.o., ZAGREB, HR

(54) Naziv izuma:

METODE I UREĐAJI ZA SNIMANJE KODIRANIH DIGITALNIH PODATAKA

(57) Sažetak: Opisana je metoda za prijenos i zapisivanje enkriptirane informacije (Ce), u kojoj se informacija (Ce) enkriptira pomoću prvog ključa i prenosi u enkriptiranom obliku, te enkriptiranu informaciju prima dekodir (2020) koji posjeduje ekvivalent prvog ključa koji je neophodan da se dekriptira informacija i za kojega je karakteristično da se dekriptirana informacija (Ce) re-enkriptira pomoću drugog ključa (C2) koji je spremljen na prijenosnom uređaju nosiocu (4004) koji je prilagođen da ga prima dekodir (2020) i/ili digitalni uređaj za snimanje (4005), te se re-enkriptirana informacija nakon toga snima na digitalni medij za snimanje (4006). Kada se reproducira snimka, informacija se dekriptira pomoću drugog ključa (C2) koji je spremljen na sklopu nosiocu (4004). U osobito poželjnoj realizaciji, informacija (Ce) koja odgovara kontrolnoj riječi koja se rabi za kodiranje i dekodiranje transmitiranih podataka, re-enkriptirana kontrolna riječ (Ce) spremljena je na mediju za snimanje (4006) zajedno s još uvijek kodiranim transmitiranim podacima.



HR P20000146A A2

Područje izuma

Izum je iz područja telekomunikacije i računalne tehnike.

- 5 Ovaj izum odnosi se na metodu i uređaj za snimanje kodiranih digitalnih podataka, primjerice televizijskih prijenosa.

Stanje tehnike

- 10 Prijenos enkriptiranih podataka dobro je poznato na polju plaćenih TV sustava, gdje se kodirana audiovizualna informacija prenosi satelitski do određenog broja pretplatnika, te svaki pretplatnik ima dekodier ili prijemnik/dekodier koji može dekodirati emitirani program za naknadno gledanje.

- 15 U tipičnom sustavu, kodirani digitalni podaci prenose se zajedno s kontrolnom riječi za dekodiranje digitalnih podataka, pri čemu je sama kontrolna riječ enkriptirana pomoću prvog ključa i prenesena u enkriptiranom obliku, kodirani digitalni podaci i enkriptirana kodna riječ stižu u dekodier koji ima ekvivalent prvog ključa koji je neophodan za dekriptiranje enkriptirane kodne riječi i nakon toga dekodira prenesene podatke, dekodier je dodatno prilagođen za prolaz digitalnih podataka u još uvijek kodiranom obliku do digitalnog uređaja za snimanje. Pretplaćeni pretplatnik dobiva na mjesečnoj osnovi ključ koji je neophodan za dekriptiranje enkriptirane kontrolne riječi da se omogući gledanje određenog programa.

- 20 S dolazećom digitalnom tehnologijom, kakvoća prenesenih podataka se mnogostruko poboljšala. Konkretni problem koji je povezan s kakvoćom digitalnih podataka leži u jednostavnosti reprodukcije. kada dekodirani program prolazi analognom vezom (npr. "Peritel" veza) za gledanje i snimanje pomoću standardnog VCR kakvoća ostaje takvom kakva je za standardne analogne kazetne snimke. Rizik da se takva snimka koristi kao master traka za izradu piratskih kopija dakle nije veća nego za standardnu prodavaonicu i kupljenu analognu kazetu.

- 25 Nasuprot tome, bilo kakvi dekodirani digitalni podaci koji su stigli izravnom digitalnom vezom do jednog digitalnog uređaja za snimanje novije generacije (naprimjer DVHS rekorder) bit će jednake kvalitete kao i originalno emitirani program te se prema tome može reproducirati bilo koji broj puta bez ikakve degradacije obzirom na kvalitetu slike ili zvuka. Prema tome, postoji značajan rizik da će dekodirani podaci biti korišteni kao master snimka da se načine piratske kopije, bilo za daljnje digitalne kopije ili čak za jednostavne analogne VHS kopije.

- 30 Francuska patentna prijava 95 03859 pokazuje kako prevladati taj problem, pomoću sustava u kojem se dekodirani digitalni podaci nikad ne snimaju na medij za digitalno snimanje. Umjesto toga, dekodier koji je opisan u ovoj prijavi snima podatke u njihovom kodiranom obliku na medij za snimanje, zajedno s kontrolnom riječi koja je neophodna za dekodiranje podataka koji su ponovo enkriptirani pomoću drugog ključa. Ovaj novi ključ je poznat samo prijemniku/dekoderu i zamjenjuje prvi ključ koji je neophodan da se dobije kodna riječ za gledanje programa.

- 40 Prednost takvog sustava jest u tome da se podaci nikad ne spremaju u "čistom" obliku i ne mogu se gledati bez posjedovanja novog ključa, koji je spremljen u prijemnik/dekodier. Sustav također ima tu prednost da, budući da se ključ mijenja na mjesečnoj osnovi uporaba konstantnog ključa za ponovo enkriptiranje kontrolne riječi koja je registrirana na digitalnu traku znači da prijemnik/dekodier još uvijek može dekriptirati kontrolnu riječ koja je snimljena na traku čak i nakon kraja pretplatničkog mjeseca.

- 45 Nedostatak sustava koji je predložen u ovoj patentnoj prijavi je u tome što se snimka može gledati samo u sprezi s određenim prijemnikom/dekoderom. Ako se taj dekodier pokvari ili zamijeni, snimka se više ne može gledati. Isto tako, nije moguće reproducirati snimku izravno u digitalnom rekorderu bez povezivanja prijemnika/dekodera u sustav te gledalac prema tome mora održavati svoju pretplatu s dotičnom televizijskom tvrtkom da bi se zadržao dekodier kao i da bi se mogli gledati filmovi koji su već emitirani.

- 50 Cilj ovog izuma je da se prevladaju problemi povezani s ovim rješenjem pri čemu se zadržava sigurno snimanje digitalnih podataka koji se ne mogu jednostavno koristiti za izradu piratskih kopija emitiranih podataka.

- 55 Ovaj izum uključuje metodu za emitiranje i snimanje enkriptirane digitalne informacije pri čemu je digitalna informacija enkriptirana pomoću prvog ključa i prenesena u enkriptiranom obliku, a enkriptirana informacija je primljena u dekodier koji ima pristup do ekvivalenta prvog ključa koji je neophodan za dekriptiranje informacije i karakteriziran je time što je dekriptirana informacija nakon toga ponovo enkriptirana pomoću drugog ključa koji je spremljen u prijenosni uređaj-nosilac koji je prilagođen za prijem dekodierom ili pripadnim digitalnim rekorderom, ponovo enkriptirana informacija se nakon toga snima na medij za digitalno snimanje pomoću digitalnog rekordera.

- 60 Na taj način, ovaj izum prevladava probleme prethodne tehnike jer je naknadna reprodukcija snimljenih podataka neovisna o identitetu dekodera. kada se reproducira snimljeno, informacija se dekriptira pomoću drugog ključa koji je spremljen na noseći sklop.

Zamjena dekodera neće obezvrjediti snimku sve dok novi dekodera ima ležište za prijem uređaja-nosioca koji sadrži drugi ključ. Ako je opremljen odgovarajućim čitačem, digitalni rekorder može sam čitati drugi ključ i dozvoliti reproduciranje informacije bez potrebe za dekodera. Za razliku od dekodera, koji je razmjerno složeni komad opreme koji se može lako slomiti, prijenosni uređaj-nosilac može se ugraditi u jednostavnom otpornom obliku.

Informacija koja je ponovo enkriptirana pomoću drugog ključa i spremljena na digitalni medij za snimanje može odgovarati jednostavno audiovizualnoj informaciji. Međutim, u poželjnoj realizaciji, digitalna informacija odgovara kontrolnoj riječi kako je enkriptirana pomoću prvog ključa, kontrolna riječ je nakon toga dekriptirana pomoću ekvivalenta prvog ključa i ponovo enkriptirana pomoću drugog ključa, te su ponovo enkriptirana kontrolna riječ i kodirani podaci zatim snimljeni na medij za digitalno snimanje.

U posebno poželjnoj realizaciji prijenosni uređaj-nosilac je inteligentna kartica koja je prilagođena za prijem u čitaču inteligentnih kartica u dekoderu i/ili digitalnom dekoderu. U ovoj prijavi pojam "inteligentna kartica" koristi se za označavanje bilo kakve standardne čip-kartice koja ima, primjerice, mikroprocesor ili EEPROM memoriju za spremanje algoritma drugog ključa. Ovim pojmom su također obuhvaćeni uređaji koji imaju alternativni fizički oblik, primjerice uređaji koji su u obliku ključa koji se često rabe u televizijskim dekoderskim sustavima.

U jednoj realizaciji, inteligentna kartica također sadrži ekvivalent prvog ključa koji se rabi za dekriptiranje kontrolne riječi za početno dekodiranje podataka, npr. za gledanje u slučaju sustava televizijskog emitiranja. U takvom slučaju, inteligentna kartica čini dio sustava plaćene televizije i može također sadržavati osobni ključ koji je poznat transponderu da se selektivno identificira koji pretplatnik će primiti obnovljeni prvi ključ na kraju mjeseca.

U alternativnoj realizaciji, drugi ključ se sprema na inteligentnu karticu koja se razlikuje od one koja je upotrebljena za spremanje prvog ključa. U takvoj realizaciji, čitanje informacije koja je spremljena na digitalni medij postaje posve odvojena od sustava pretplatnika i, čak i kada je pretplatnik izašao iz sustava u njegova pretplatnička kartica je povučena, on može nastaviti gledanjem prethodno snimljenih filmova pod uvjetom da digitalni rekorder/player kojega ima bude prilagođen za čitanje popratne inteligentne kartice.

U takvom sustavu, jedna inteligentna kartica i drugi ključ mogu se koristiti za generiranje ponovno enkriptirane kodne riječi za množinu snimki. Na taj način, može se koristiti jedna "bibliotečna kartica" da se dekriptira bilo koji broj snimaka.

U jednoj realizaciji, inteligentna kartica može također sadržavati određeni broj kreditnih jedinica da se odredi koliko puta se može reproducirati snimka, pri čemu se taj broj jedinica smanjuje pri svakoj djelomično ili potpuno ponovljenoj reprodukciji snimke. Ove kreditne jedinice mogu se primjerice učitati u poruku zajedno s prenesenim prvim ključem.

U jednoj realizaciji kreditne jedinice su povezane s određenim segmentom snimanja tako da dio za reprodukciju snimke, primjerice prva četvrtina ili posljednja četvrtina sata snimke smanjuje određene kreditne jedinice koje su povezane s ovim dijelovima. Alternativno, kreditne jedinice su jednog tipa i smanjuju se reprodukcijom bilo kojeg dijela snimke.

Kao što je gore razmotreno, ovaj izum je posebice primjenljiv u slučaju kada je algoritam drugog ključa spremljen na inteligentnu karticu koja je povezana s medijem za snimanje. Međutim, u alternativnoj realizaciji, prijenosni nosilac je definiran samim snimanjem, drugi ključ je spremljen u integrirani krug ugrađen u kućište medija za digitalno snimanje.

Takva tehnika je već bila predložena, primjerice, u slučaju DVHS kazeta gdje se može načiniti skup metalnih kontakata na vanjskoj površini kućišta kazete, te kontakti vode do elektroničkog kruga, kao što je integrirani krug ili čip u unutrašnjosti kućišta. Ovi kontakti mogu se povezati s odgovarajućim skupom kontakata u ležištu rekordera da se omogući komunikacija između integriranog kruga i video rekordera.

U takvim sustavima sigurnost je još uvijek zadržana bez obzira na činjenicu što se ključ nosi uz snimku, jer se ključ ne može jednostavno kopirati s ugrađenog čipa. Varijacije koje su gore opisane glede realizacija inteligentne kartice su jednako primjenljive na sustave u kojima je nosilac definiran kućištem snimke.

Ovaj izum je osobito primjenljiv u metodi kojom se kodirani podaci koji odgovaraju audiovizualnim podacima koji su emitirani kodiranim televizijskim prijenosom.

Ovaj izum opisan je prije u odnosu na metodu ali se jednako odnosi i na uređaj. Pojam "kodiran" i "enkriptiran" te "kontrolna riječ" i "ključ" ovdje su korišteni samo zbog jasnoće jezika. Međutim, podrazumijeva se da nema temeljne razlike između "kodiranih podataka" i "enkriptiranih podataka" ili između "kontrolne riječi" i "ključa".

Na sličan način, premda se opis poziva na “prijemnik/dekoder” i “dekoder” – podrazumijeva se da se ovaj izum jednako odnosi na realizacije koje imaju prijemnik integriran s dekoderom ili dekodersku jedinicu koja funkcionira u kombinaciji s fizički odvojenim prijemnikom. Izum se jednako proširuje na realizacije u kojima je dekoder integriran s ostalim uređajima, kao što je televizor ili čak digitalni video rekorder.

Sada će biti opisana poželjna realizacija, samo kao primjer, prema priloženim slikama koje prikazuju sljedeće:

- Slika 1 prikazuje cjelokupnu arhitekturu digitalnog televizijskog sustava, koji se može prilagoditi ovim izumom da bude u interakciji s uređajem za digitalno snimanje;
- Slika 2 prikazuje sustav uvjetnog pristupa na televizijski sustav na slici 1;
- 10 Slika 3 prikazuje različite razine enkriptiranja u televizijskom sustavu;
- Slika 4 prikazuje strukturu poslanog digitalnog paketa u televizijskom sustavu, uključujući vizualne, audio i teletekst podatke i ECM dio poruke;
- Slika 5 prikazuje prvu realizaciju ovog izuma uključujući uređaj za digitalno snimanje i inteligentnu karticu koja sadrži drugi algoritam koji se koristi za enkriptiranje kodne riječi koja se registrirana na digitalnoj video kazeti;
- 15 Slika 6 prikazuje drugu realizaciju izuma u kojoj inteligentna kartica sadrži prvi i drugi ključ koji su neophodni za gledanje poslanog i emitiranog programa, zajedno s kreditnim jedinicama za određivanje koliko puta se može gledati program; i
- 20 Slika 7 prikazuje treću realizaciju izuma u kojoj je drugi ključ spremljen na integrirani krug koji je postavljen u kućište digitalne video kazete.

Digitalni televizijski sustav

Na slici 1 prikazan je pregled digitalnog televizijskog sustava 1. Digitalni televizijski sustav 1000 obuhvaća većinu uobičajenih digitalnih televizijskih sustava 2000 koji rabe poznati MPEG-2 sustav kompresije za prijenos komprimiranih televizijskih signala. MPEG-2 sustav kompresije 2002 u centru za emitiranje prima digitalni tok signala (tipično tok video signala). Kompresor 2002 povezan je s multiplekserom i koderom 2004 pomoću veze 2006. Multiplekser 2004 prima određeni broj ulaznih signala, stvara jedan ili nekoliko prijenosnih tokova i prenosi komprimirane digitalne signale do odašiljača 2008 centra za emitiranje putem veze 2010, koja naravno može poprimiti cijeli niz oblika uključujući telekomunikacijske veze. Odašiljač 2008 šalje elektromagnetske signale putem veze 2012 prema satelitskom prijenosniku 2014, gdje se elektronički obrađuju i difuzijski šalju vezom 2016 prema zemaljskom prijemniku 2018, koji je u obliku tanjura kojega kupuje ili iznajmljuje krajnji korisnik. Signali koje prima prijemnik 2018 prenose se u integrirani prijemnik/dekoder 2020 kojega kupuje ili iznajmljuje krajnji korisnik i koji je spojen s televizorom krajnjeg korisnika 2022. Prijemnik/dekoder 2020 dekodira komprimirani MPEG-2 signal u televizijski signal za televizor 2022.

Sustav uvjetnog pristupa 3000 povezan je s multiplekserom 2004 i prijemnikom/dekoderom 2020, te je djelomično smješten u centru za emitiranje, a djelomično u dekoderu. To omogućuje krajnjem korisniku pristup do digitalnih televizijskih stanica preko jednog ili više televizijskih proizvođača. Inteligentna kartica, koja može dekodirati poruke koje se odnose na komercijalnu ponudu (dakle jedan ili nekoliko televizijskih programa koje prodaje televizijski proizvođač), stavlja se u prijemnik/dekoder 2020. Koristeći dekoder 2020 i inteligentnu karticu, krajnji korisnik može kupiti komercijalnu ponudu bilo u obliku pretplate ili u “pay-per-view” načinu.

Interaktivni sustav 4000, koji je također povezan s multiplekserom 2004 i prijemnikom/dekoderom 2020 i koji je opet djelomično smješten u centru za emitiranje, a djelomično u dekoderu, omogućuje krajnjem korisniku interakciju s različitim aplikacijama putem modemiziranog povratnog kanala 4002.

Sustav uvjetnog pristupa

Prema slici 2, sustav uvjetnog pristupa 3000 sadrži sustav autorizacije pretplatnika (SAS) 3002. SAS 3002 je povezan s jednim ili više sustava za upravljanje pretplatnicima (SMS) 3004, jedan SMS za svakog televizijskog proizvođača, pomoću odgovarajuće TCP-IP veze 3006 (premda se ostali tipovi veza mogu alternativno koristiti). Alternativno, jedna SMS može se dijeliti između dviju televizijskih proizvođača ili jedan proizvođač može koristiti dva SMS-a itd.

Prva jedinica za enkriptiranje u obliku jedinice za kodiranje 3008 koristeći “matičnu” inteligentnu karticu 3010 vezana je za SAS vezom 3012. Druga jedinica za enkriptiranje opet u obliku jedinice za kodiranje 3014 koristeći matičnu karticu 3016 povezana je s multiplekserom 2004 pomoću veze 3018. Prijemnik/dekoder 2020 prima “nasljedničku” inteligentnu karticu 3020. Ona je povezana izravno sa SAS 3002 pomoću komunikacijskog servera 3022 s modemiziranim povratnim kanalom 4002. SAS šalje, između ostalog, pretplatnička prava nasljedničkoj kartici na zahtjev.

Inteligentne kartice sadrže tajne jednog ili više komercijalnih operatora. "Matična" inteligentna kartica enkriptira različite vrste poruka dok "nasljednička" inteligentna kartica dekriptira poruke, imaju li ovlasti za to.

5 Prva i druga jedinica za kodiranje 3008 i 3014 sadrže "rack", elektroničku VME karticu sa spremljenim softverom na EEPROM-u, do 20 elektroničkih kartica i jedna inteligentna kartica 3010 i 3016 za svaku elektroničku karticu, jedna (kartica 3016) za enkriptiranje ECM-ova i jedna (kartica 3010) za enkriptiranje EMM-ova.

10 Kao što će biti opisano, ECM-ovi ili naslovne kontrolne poruke su enkriptirane poruke ugrađene u tok podataka emitiranog programa koji sadrži kontrolnu riječ koja je neophodna za dekodiranje programa. Autorizacija danog prijemnika/dekoderu kontrolirana je pomoću EMM-ova ili naslovnih upravljačkih poruka, koje se prenose rjeđe, primjerice jednom mjesečno, kojima se dostavlja ovlaštenom prijemniku/dekoderu ključ koji je neophodan za dekodiranje ECM-a.

15 Rad sustava za uvjetni pristup 3000 digitalnog televizijskog sustava sada će biti detaljnije objašnjen obzirom na različite komponente televizijskog sustava 2000 i sustav uvjetnog pristupa 3000.

Multiplekser i koder

20 Prema slikama 1 i 2, u televizijskom centru za emitiranje, digitalni video signal se prvo komprimira (smanjuje mu se bitovna brzina), koristeći MPEG-2 kompresor 2002. Komprimirani signal se zatim prenosi do multipleksera i koderu 2004 putem veze 2006 da bi se multipleksirao s ostalim podacima, kao što su ostali komprimirani podaci.

25 Koder generira kontrolnu riječ Ce koja se koristi u procesu kodiranja i uključena je u MPEG-2 tok u multiplekseru 2004. Kontrolna riječ Ce je generirana interno i omogućuje da integrirani prijemnik/dekoder krajnjeg korisnika 2020 dekodira program. Pristupni kriteriji, koji pokazuju kako je program komercijaliziran, također se dodaju MPEG-2 toku. Program se može komercijalizirati u bilo kojem od "pretplatničkih" načina i/ili jednom od "pay-per-view" načina (PPV) ili događaja. U pretplatničkom načinu, krajnji korisnik pretplaćuje se na jednu ili više komercijalnih ponuda ili "buketa", tako da dobiva prava gledanja bilo kojeg kanala unutar ovog buketa. U poželjnoj realizaciji, do 960 komercijalnih ponuda može se odabrati iz buketa kanala. U "pay-per-view" načinu, krajnji korisnik ima mogućnost kupiti događaje koje želi. To se postiže bilo prethodnom rezervacijom događaja unaprijed ("pre-book" način) ili kupovinom događaja upravo kada se emitira (impulsni način).

35 I kontrolna riječ Ce i pristupni kriterij koriste se za izgrađivanje naslovne kontrolne poruke (ECM). To je poruka koja se šalje u odnosu na jedan kodirani program; poruka sadrži kontrolnu riječ (koja omogućuje dekodiranje programa) i pristupne kriterije emitiranog programa. Pristupni kriteriji i kontrolna riječ su preneseni do druge jedinice za enkriptiranje 3014 putem veze 3018. U ovoj jedinici generiran je ECM, enkriptiran pomoću prvog ključa Cex i prenesen do multipleksera i koderu 2004.

40 Svaka usluga televizijskim emitiranjem koju nudi davalac televizijskog programa u podacima sadrži određen broj odvojenih dijelova. primjerice, televizijski program sadrži video komponentu V, audio komponentu S, podnaslov ili teletext komponentu T itd. (vidi sliku 4). Svaka od ovih komponenti usluge je pojedinačno kodirana i enkriptirana za naknadno emitiranje do transpondera 2014. U odnosu na svaku kodiranu komponentu usluge, potreban je odvojeni ECM.

Prijenos programa

45 Multiplekser 2004 prima električne signale koji sadrže enkriptirane EMM-ove iz SAS 3002, enkriptirane ECM-ove iz druge jedinice za enkriptiranje 3014 i komprimirane programe iz kompresora 2002. Multiplekser 2004 kodira programe i prenosi kodirane programe, enkriptirani EMM (ako ga ima) i enkriptirane ECM-ove kao električne signale do odašiljača 2008 televizijskog centra putem veze 2010. Odašiljač 2008 prenosi elektromagnetske signale prema satelitskom transponderu 2014 putem satelitske veze 2012.

Prijem programa

55 Satelitski transponder 2014 prima i obrađuje elektromagnetske signale koje šalje odašiljač 2008 i prenosi signale do zemaljskog prijemnika 2018, koji je standardno u obliku tanjura kojega posjeduje ili je iznajmio krajnji korisnik, putem zemaljske veze 2016. Signali koje prima prijemnik 2018 se prenose do integriranog prijemnika/dekoderu 2020 kojega posjeduje ili je iznajmio krajnji korisnik koji je povezan s televizorom krajnjeg korisnika 2022. Prijemnik/dekoder 2020 demultipleksira signale da dobije kodirane programe s enkriptiranim EMM-ovima i enkriptiranim ECM-ovima.

60 Ako program nije kodiran, prijemnik/dekoder 2020 dekomprimira podatke i transformira signal u video signal za prijenos do televizora 2022.

Ako je program kodiran, prijemnik/dekoder 2020 ekstrahira odgovarajući ECM iz MPEG-2 toka i propušta ECM prema nasljedničkoj inteligentnoj kartici 3020 krajnjeg korisnika. Ona se stavlja u utore u kućištu prijemnika/dekodera 2020. Nasljednička inteligentna kartica 3020 kontrolira ima li krajnji korisnik pravo dekriptirati ECM da bi pristupio programu.

Ako krajnji korisnik nema neophodna prava, na prijemnik/dekoder šalje se negativna status 2020 da označi da se program ne može dekodirati. Ako krajnji korisnik nema prava, ECM se dekriptira i ekstrahira se kontrolna riječ. Dekoder 2020 može zatim dekodirati program koristeći kontrolnu riječ. MPEG-2 tok je dekompresiran i preveden u video signal te se prenosi televizoru 2022.

Korištene razine enkriptiranja sada će biti detaljnije objašnjene prema slici 3.

Sustav upravljanja pretplatnikom (SMS)

Sustav upravljanja pretplatnikom (SMS) 3004 uključuje bazu podataka 3024 koja upravlja, između ostalog, datotekama krajnjeg korisnika, komercijalnom ponudom (kao što su tarife i promocije), pretplate, pojedini PPV te podaci koji se odnose na potrošnju krajnjeg korisnika i ovlasti. SMS se može fizički odvojiti od SAS.

Svaki SMS 3004 prenosi poruke do SAS 3002 putem odgovarajuće linije 3006 da se omoguće promjene ili kreiranje naslovnih poruka za upravljanje (EMM) koje se šalju krajnjem korisniku.

SMS 3004 također prenosi poruke prema SAS 3002 koje ne uključuju modificiranje ili kreiranje EMM već uključuju samo promjenu stanja krajnjeg korisnika (odnosi se na ovlasti koje je dobio krajnji korisnik kada naručuje proizvode ili na iznos kojim će se teretiti krajnji korisnik).

Naslovne poruke za upravljanje (EMM)

EMM je poruka koja je namijenjena jednom krajnjem korisniku (pretplatniku) ili skupini krajnjih korisnika (za razliku od ECM, koji je namijenjen samo jednom kodiranom programu ili skupu kodiranih programa ako su dio iste komercijalne ponude). Skupina može sadržavati dani broj krajnjih korisnika. Ova organizacija skupine pomaže optimiziranju frekvencijskog raspona. Dakle, pristup jednoj skupini omogućuje stizanje do velikog broja krajnjih korisnika.

Različiti specifični tipovi EMM koriste se kada se ovaj izum koristi u praksi. Pojedinačni EMM namijenjeni su pojedinačnim pretplatnicima, te se tipično koriste za "pay-per-view" usluge – oni koriste identifikator skupine i položaj pretplatnika u skupini. Takozvana "skupna" pretplatnička EMM namijenjena je skupini od, recimo, 256 pojedinačnih korisnika, te se tipično koristi u administraciji nekih pretplatničkih usluga. Ova EMM ima identifikator skupine i bitnapu pretplatničke skupine. EM auditorija namijenjen je cijelom auditoriju, te se može primjerice koristiti ako određeni operator daje neke besplatne usluge. "Auditorij" je cjelokupnost pretplatnika koji imaju inteligentnu karticu s istim identifikatorom operatora (OPI). Najzad, "jedinstveni" EMM adresiran je jedinstvenom identifikatoru inteligentne kartice.

Razine enkriptiranja sustava

Sada će prema slici 3 biti opisane razine enkriptiranja u sustavu televizijskog emitiranja. Stupnjevi enkriptiranja koji su povezani sa televizijskim emitiranjem digitalnih podataka prikazani su na 4001, prijenosni kanal (npr. satelitska veza kao što je gore objašnjeno) na 4002 i stupnjevi enkriptiranja na prijemniku 4003.

Digitalni podaci N kodirani su pomoću kontrolne riječi Ce prije slanja na multiplekser Mp za naknadni prijenos. Kao što je prikazano na slici 4, poslani podaci uključuju ECM koji sadrži, između ostalog, kontrolnu riječ Ce kako je enkriptirana pomoću enkriptora Ch1 koji je kontroliran pomoću prvog ključa za enkriptiranje Cex. Na prijemniku/dekoderu, signal prolazi demultiplekserom DMp i dekoderom D prije nego se propusti do televizora 2022 za gledanje. Jedinica za dekriptiranje DCh1 također ima ključ Cex koji dekriptira ECM u demultipleksiranom signalu da se dobije kontrolna riječ Ce koja se jasnije koristi za dekodiranje signala.

Iz sigurnosnih razloga, kontrolna riječ Ce ugrađena je u enkriptirane promjene ECM prosječno svakih 10 sekundi. Naprotiv, prvi ključ za enkriptiranje Cex kojeg koristi prijemnik za dekodiranje ECM mijenja se svaki mjesec ili više pomoću EMM. Ključ za enkriptiranje Cex enkriptira se drugom jedinicom ChP koja koristi osobni ključ Cg koji odgovara identitetu dekodera. Ako je dekoder jedan od onih koji su izabrani da primi obnovljeni ključ Cex, jedinica za dekriptiranje DChP u dekoderu će dekriptirati poruku koristeći njen ključ Cg da se dobije onaj mjesečni ključ Cex.

Jedinice za dekriptiranje DChp i DCh1 i pridruženi ključevi drže se u inteligentnoj kartici dobiva pretplatnik i koja se stavlja u čitač inteligentne kartice u dekoderu. Ključevi se mogu generirati sukladno bilo kojem poznatom simetričnom algoritmu ključeva, kao što je DES. Alternativne realizacije koristeći algoritam javnog/osobnog ključa također su moguće.

Snimanje digitalnih podataka

Kao što je navedeno u uvodu, nije preporučljivo dozvoliti da se snime dekodirani digitalni podaci obzirom na rizik glede neovlaštenog kopiranja i piratstva. Kao što je prikazano na slici 5, ovaj izum definira sklop koji se prevladava ovaj problem.

Sustav sadrži inteligentnu karticu 4004, koja se stavlja u utor inteligentne kartice u prijemnik/dekoder zajedno s digitalnim rekorderom 4005, npr. DVHS rekorder, uključujući digitalni medij za snimanje 4006, kao što je DVHS kazeta.

U ovoj realizaciji, primljena kontrolna riječ dekriptirana je pomoću pripadne inteligentne kartice 3020 koja je stavljena u dekoder (vidi sliku 2). Dekodirana kontrolna riječ Ce (zajedno s bilo kakvim drugim podacima koji čine ECM, kao što je informacija koja kontrolira pristup itd) se zatim šalje mikroprocesoru koji je ugrađen u inteligentnu karticu 4004. Koristeći drugi ključ za enkriptiranje C2 i drugi algoritam enkriptiranja Ch2, inteligentna kartica 4004 generira novi ECM, koji je označen na slici sa ECM'. Ova naslovna poruka ECM' se zatim koristi da zamijeni ECM u toku kodiranih podataka iz demultipleksera DMp kao što je prikazano na slici 4007 te se kombinacija kodiranih podataka i nove naslovne poruke ECM' snima na DVHS kazetu 4006. Naslovna poruka ECM' može se ubaciti u tok podataka koji pomiče kontrolni registar pomaka R.

Na taj način, izumom se izbjegava snimanje dekodiran audiovizualne informacije na kazetu. Da bi se reproducirala kazeta, kartica se ponovo stavlja u dekoder, ključ C2 se koristi za dekodiranje naslovne poruke ECM', te se naknadno ekstrahirana kontrolna riječ Ce koristi za kontrolu dekodera da se dekodira program za gledanje.

U sustavu koji je prikazan na slici 5, inteligentna kartica 4004 razlikuje se od inteligentne kartice 3020 koja je prikazana na slici 2 televizijskog sustava koji sadrži ključ za enkriptiranje koji je neophodan za gledanje programa. Međutim, u alternativnoj realizaciji koja je prikazana na slici 6, inteligentna kartica 3020 sadrži prvi i drugi ključ za enkriptiranje Cex i C2 koji su potrebni za gledanje i snimanje programa. Kao što je prikazano, ključ Cex kontrolira dekriptiranje ECM da se generira kontrolna riječ koju koristi dekoder D za gledanje programa i nakon toga enkriptiranje pomoću ključa C2 da se dobije nova naslovna poruka ECM'.

Algoritmi DCh1 i DCh2 nisu ovdje zbog prostora prikazani. Kartica 3030 ustvari se obično inicijalizira pomoću osobnog ključa Cg (nije prikazan) koji omogućuje dekriptiranje EMM-ova tako da se dobije mjesečni ključ Cex koji se sprema u memoriju kartice. Mada je inteligentna kartica prikazana u obliku pravokutne kartice, mogući su i ostali fizički oblici, npr. oblik ključa.

ECM koji je prencsen s programom i dekriptiran pomoću kartice može također sadržavati kreditne jedinice U koje se naknadno spremaju u karticu i koje kontroliraju broj reprodukcija snimljenog film. U najjednostavnijoj realizaciji, kreditne jedinice mogu se smanjiti tijekom reprodukcije snimljenog filma svaki puta kada ECM prođe dekoder. Kada se jednom broj kredita smanji do nule, što znači da je snimka pregledana unaprijed određeni broj puta, dekoderu se šalje poruka da se spriječi daljnje gledanje filma, sve dok se kreditne jedinice ne obnove (naprimjer, izmjenom naredbe koja se šalje u EMM).

U alternativnoj realizaciji, kreditne jedinice mogu se smanjiti svakih deset ili sto ECM poruka. U daljnjim realizacijama, kreditne jedinice mogu odgovarati određenim dijelovima filma (primjerice prvih ili posljednjih 10 minuta filma), tako da reprodukcija ovih dijelova smanjuje kreditne jedinice koje su povezane s njima. Dijelovi se mogu identificirati označavanjem ECM poruka u tim odjeljcima.

Daljnja realizacija ovog izuma prikazana je na slici 7. U ovoj realizaciji, generiranje nove naslovne poruke EMM' kontrolirano je integriranim krugom ili čipom 4008 koji ima drugi ključ za enkriptiranje C2 i ugrađen je u kućište snimljene kazete 4006. Ugrađivanje mikroprocesora u kućište snimljenog medija je poznata tehnika i predloženo je u slučaju DVHS kazeta. U ovom primjeru, skup metalnih kontakata može se načiniti na vanjskoj površini kućišta kazete, te kontakti vode do elektroničkog kruga, kao što je integrirani krug ili čip u unutrašnjosti kućišta. Ovi kontakti mogu se spojiti s odgovarajućim skupom kontakata u ležištu rekordera da se omogući komuniciranje između integriranog kruga i video rekordera.

Premda se može izvršiti izravno kopiranje snimljenih (i kodiranih) digitalnih podataka, podaci koji su spremeni na čip bit će otporni na kopiranje i, kao s prethodnim realizacijama, kodirani podaci bit će neupotrebljivi bez ključa C2 koji je neophodan za otključavanje ECM' da se dobije kontrolna riječ koju koristi dekoder.

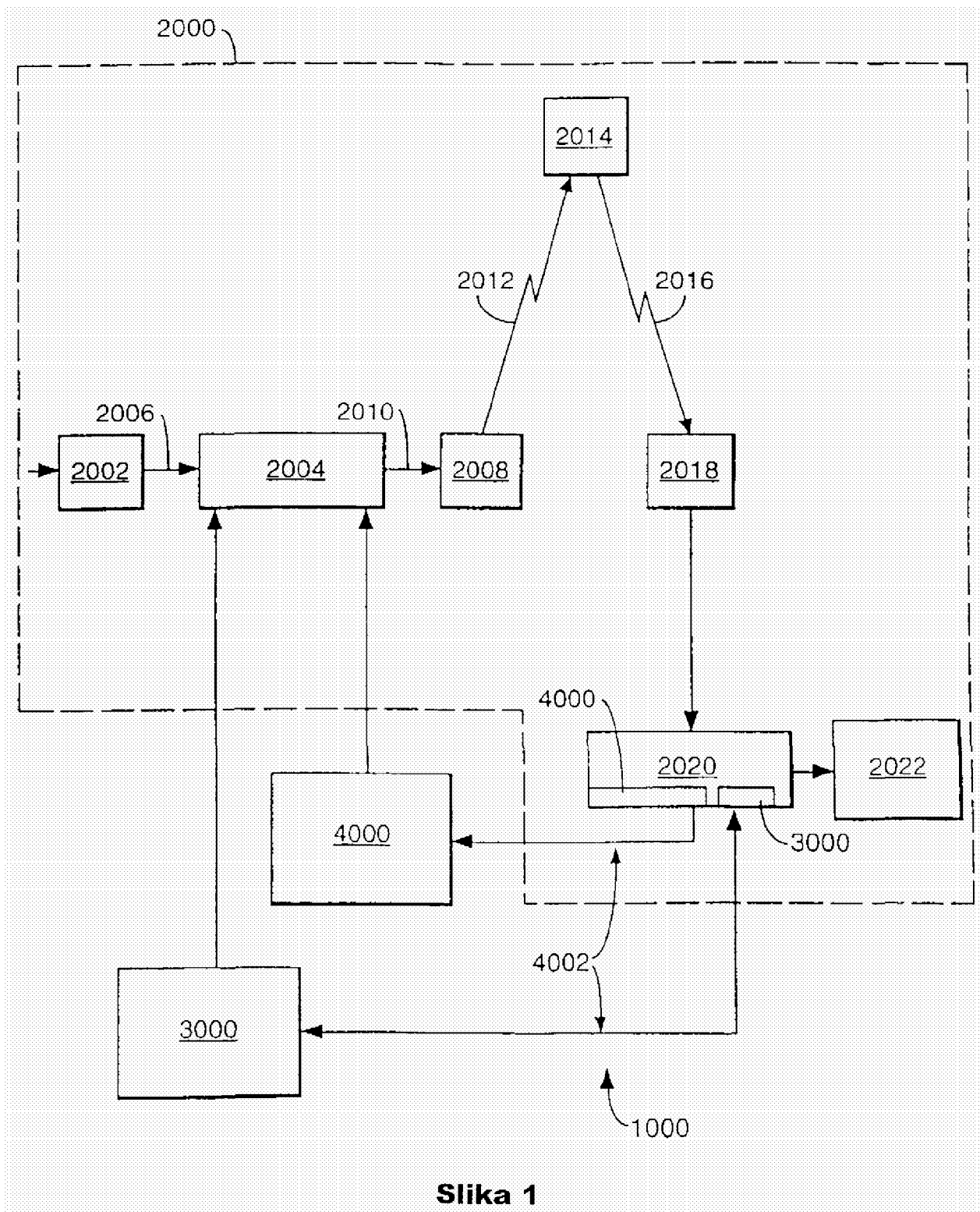
Podrazumijeva se, u svim opisanim realizacijama, elementi prijemnika/dekoder i uređaj za digitalno snimanje mogu se kombinirati ili međusobno zamijeniti, tako da digitalni rekorder ima utor inteligentne kartice za stavljanje inteligentne kartice, na primjer, i/ili neophodne elemente da dekodira program kada je jednom kontrolna riječ Ce ekstrahirana iz ECM poruke. Dekoder i/ili digitalni rekorder mogu isto tako biti integrirani zajedno s ostalim uređajima, kao što je primjerice televizija.

PATENTNI ZAHTEJEVI

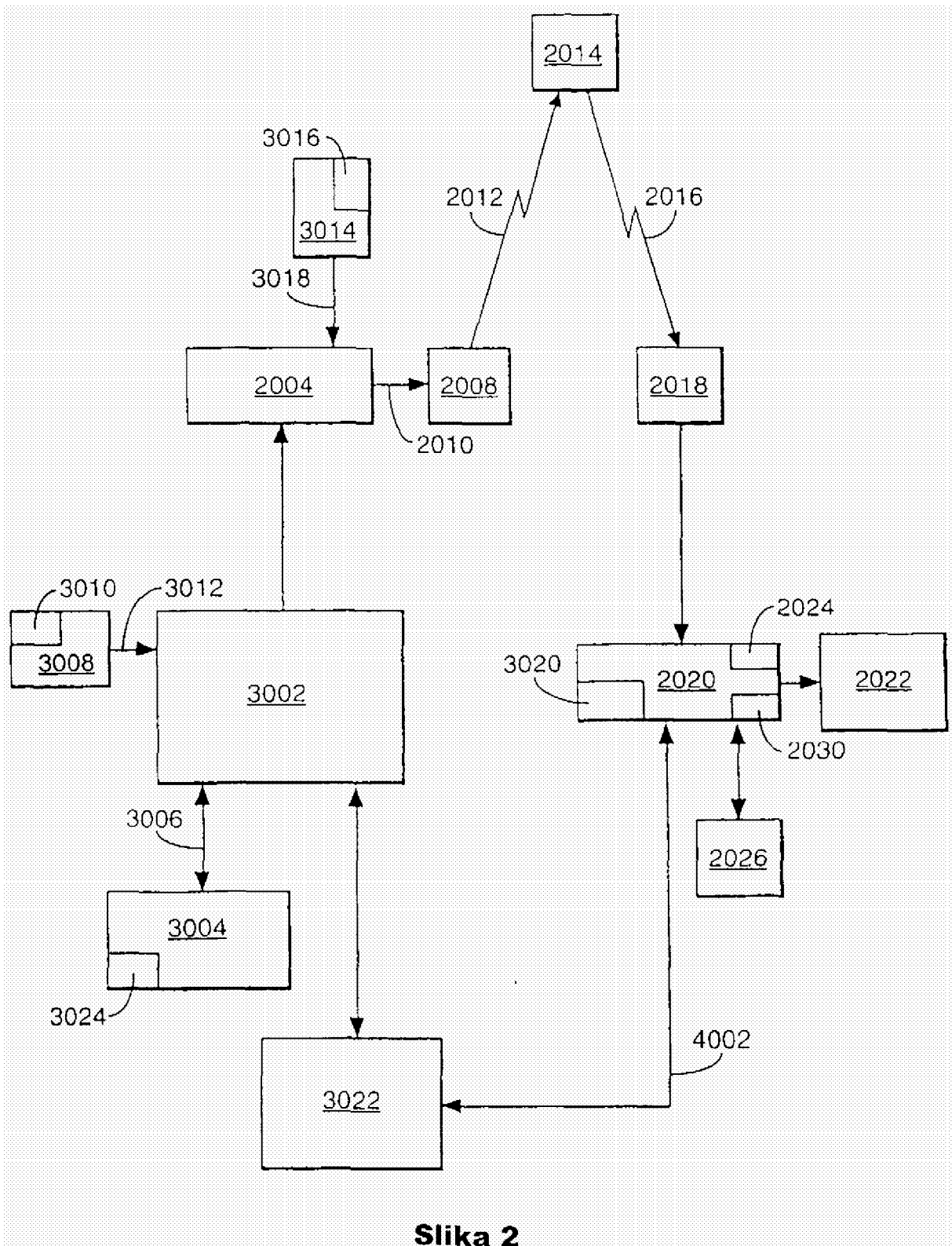
1. Metoda za prijenos i snimanje enkriptirane digitalne informacije, **naznačena time** što je digitalna informacija enkriptirana pomoću prvog ključa i prenesena u enkriptiranom obliku, enkriptiranu informaciju prima dekode koji ima pristup do ekvivalenta prvog ključa koji je neophodan za dekriptiranje informacije i karakteriziran je time što se dekriptirana informacija nakon toga ponovo enkriptira pomoću drugog ključa koji je spremljen u prijenosnom uređaju-nosiocu koji je prilagođen da ga primi dekode ili pridruženi digitalni dekode, ponovo enkriptirana informacija je nakon toga snimljena na digitalni medij za snimanje pomoću digitalnog rekordera.
2. Metoda prema zahtjevu 1, **naznačena time** što digitalna informacija odgovara kontrolnoj riječi za dekodiranje kodiranih digitalnih podataka, kodirani digitalni podaci prenose se zajedno s kontrolnom riječi kako je enkriptirana pomoću prvog ključa, kontrolna riječ je nakon toga dekriptirana pomoću ekvivalentnog prvog ključa i ponovo enkriptirana pomoću drugog ključa, te su ponovo enkriptirana kontrolna riječ i kodirani podaci snimljeni na digitalni medij za snimanje.
3. Metoda prema zahtjevu 1 ili 2, **naznačena time** što je prijenosni uređaj-nosilac inteligentna kartica koja je prilagođena da se stavi u čitač inteligentne kartice u dekode i/ili digitalni dekode.
4. Metoda prema zahtjevu 3, **naznačena time** što inteligentna kartica također sadrži ekvivalent prvog ključa koji se koristi za dekriptiranje kontrolne riječi za početno dekodiranje podataka.
5. Metoda prema zahtjevu 3, **naznačena time** što je drugi ključ spremljen na inteligentnu karticu koja je drukčija od sklopa kojega je koristio dekode za spremanje prvog ključa.
6. Metoda prema bilo kojem zahtjevu 3 do 5, **naznačena time** što se jedna inteligentna kartica i drugi ključ koriste za generiranje ponovo enkriptirane kodne riječi za množinu snimanja.
7. Metoda prema bilo kojem zahtjevu 3 do 6, **naznačena time** što inteligentna kartica također sadrži određen broj kreditnih jedinica da se odredi koliko puta se može reproducirati snimka, pri čemu se broj jedinica smanjuje za svakom djelomičnom ili potpunom reprodukcijom snimke.
8. Metoda prema zahtjevu 7, **naznačena time** što su kreditne jedinice povezane s određenim segmentom snimke tako da reprodukcija tog dijela snimke smanjuje određene kredite koji su povezani s tim dijelom.
9. Metoda prema zahtjevu 8, **naznačena time** što su kreditne jedinice jednog tipa i one se smanjuju s reprodukcijom bilo kojeg dijela snimke.
10. Metoda prema zahtjevu 1, **naznačena time** što je prijenosni nosilac definiran samim medijem za snimanje, pri čemu je drugi ključ spremljen u integrirani krug koji je ugrađen u kućište digitalnog medija za snimanje.
11. Uređaj prilagođen za prijenos i snimanje kodiranih digitalnih podataka prema bilo kojem zahtjevu 1 do 10, **naznačen time** što sadrži transmitter za enkriptiranje s prvim ključem digitalne informacije i prijenos navedene informacije u enkriptiranom obliku, dekode za prijem enkriptirane informacije koji ima pristup do ekvivalenta prvog ključa koji je neophodan za dekriptiranje informacije, te prijenosni uređaj-nosilac koji je prilagođen da ga primi dekode ili pridruženi digitalni rekorder i koji ima drugi ključ za ponovo enkriptiranje dekriptirane informacije za naknadni prijenos do digitalnog uređaja za snimanje za snimanje na digitalni medij za snimanje.
12. Dekode za uređaj prema zahtjevu 11 i prilagođen za uporabu u metodi prema bilo kojem zahtjevu 1 do 10, **naznačen time** što ima ležište za prihvata prijenosnog uređaja-nosioca koji sadrži drugi ključ za ponovo enkriptiranje dekriptirane informacije.
13. Dekode prema zahtjevu 12, **naznačen time** što je integriran s digitalnim uređajem za snimanje za snimanje ponovo enkriptirane informacije na digitalni medij za snimanje.

SAŽETAK

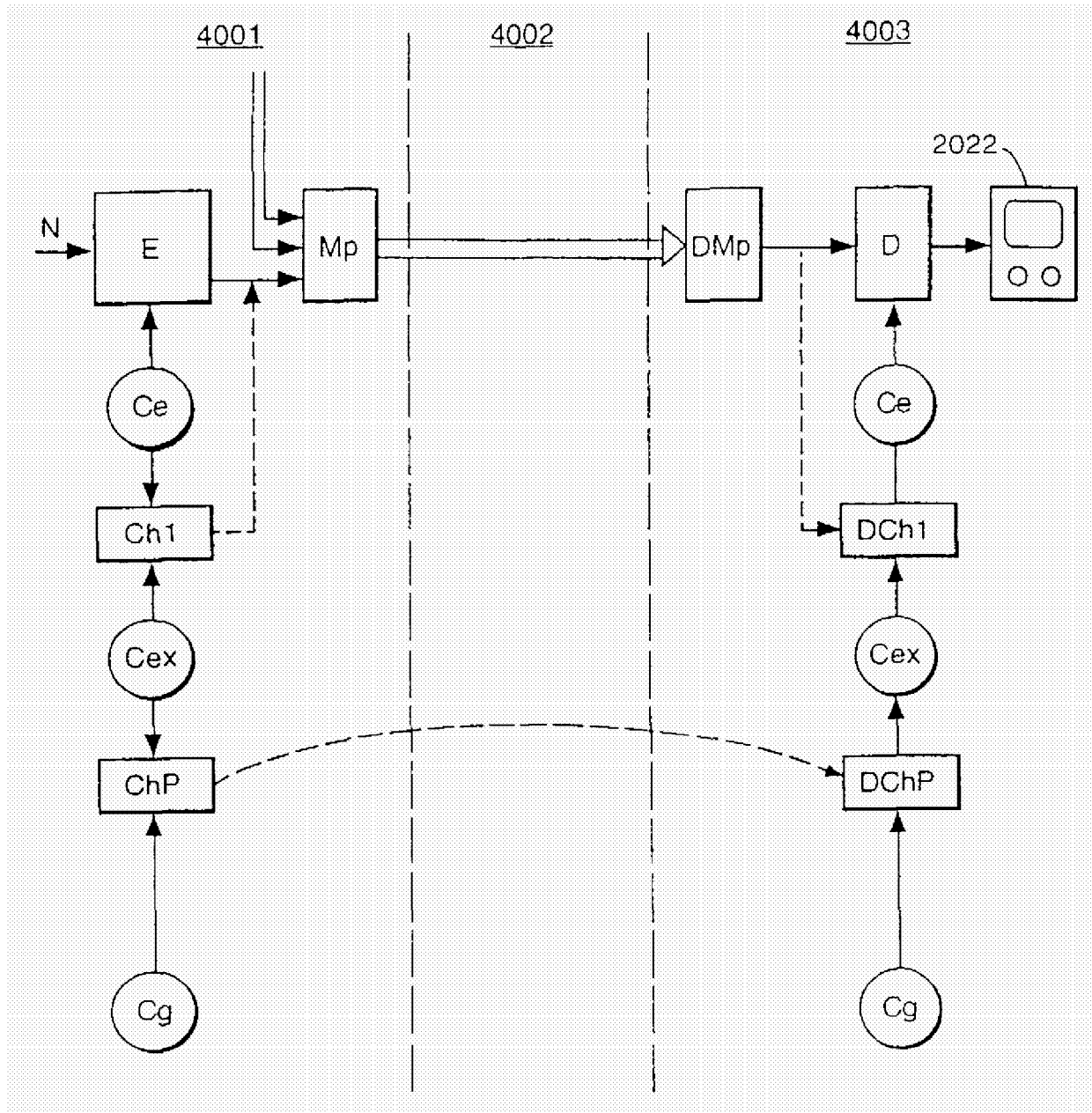
Opisana je metoda za prijenos i zapisivanje enkriptirane informacije (Ce), u kojoj se informacija (Ce) enkriptira pomoću prvog ključa i prenosi u enkriptiranom obliku, te enkriptiranu informaciju prima dekode (2020) koji posjeduje ekvivalent prvog ključa koji je neophodan da se dekriptira informacija i za kojega je karakteristično da se dekriptirana informacija (Ce) re-enkriptira pomoću drugog ključa (C2) koji je spremljen na prijenosnom uređaju nosiocu (4004) koji je prilagođen da ga prima dekode (2020) i/ili digitalni uređaj za snimanje (4005), te se re-enkriptirana informacija nakon toga snima na digitalni medij za snimanje (4006). Kada se reproducira snimka, informacija se dekriptira pomoću drugog ključa (C2) koji je spremljen na sklopu nosiocu (4004). U osobito poželjnoj realizaciji, informacija (Ce) koja odgovara kontrolnoj riječi koja se rabi za kodiranje i dekodiranje transmitiranih podataka, re-enkriptirana kontrolna riječ (Ce) spremljena je na mediju za snimanje (4006) zajedno s još uvijek kodiranim transmitiranim podacima.



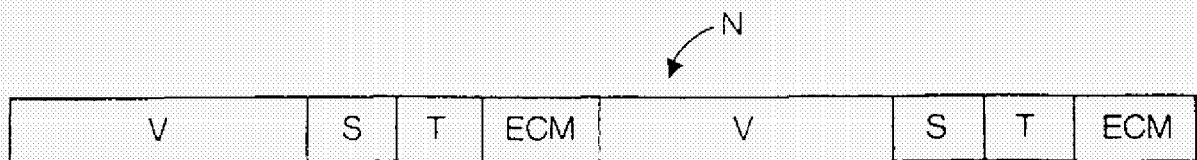
Slika 1



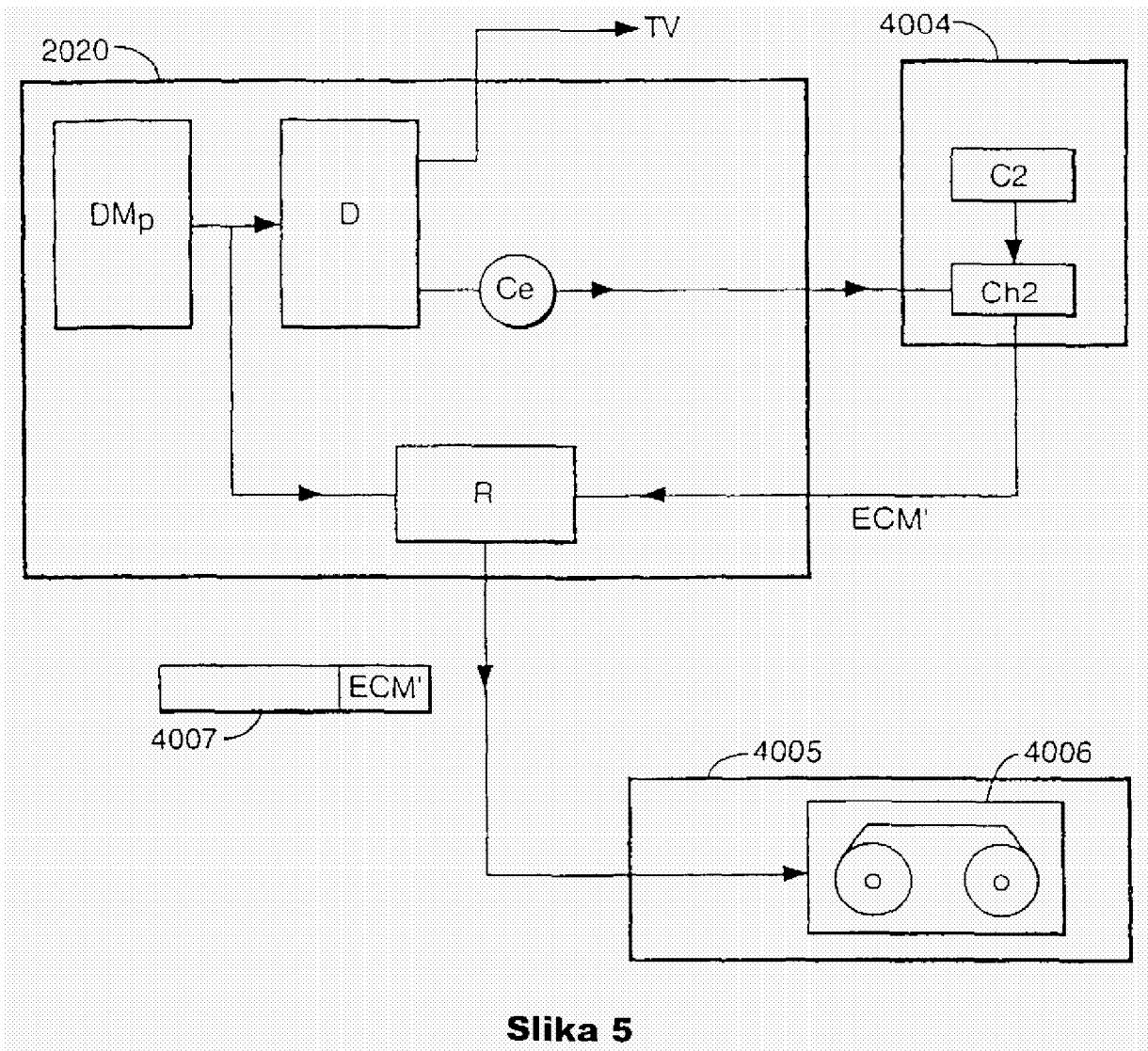
Slika 2



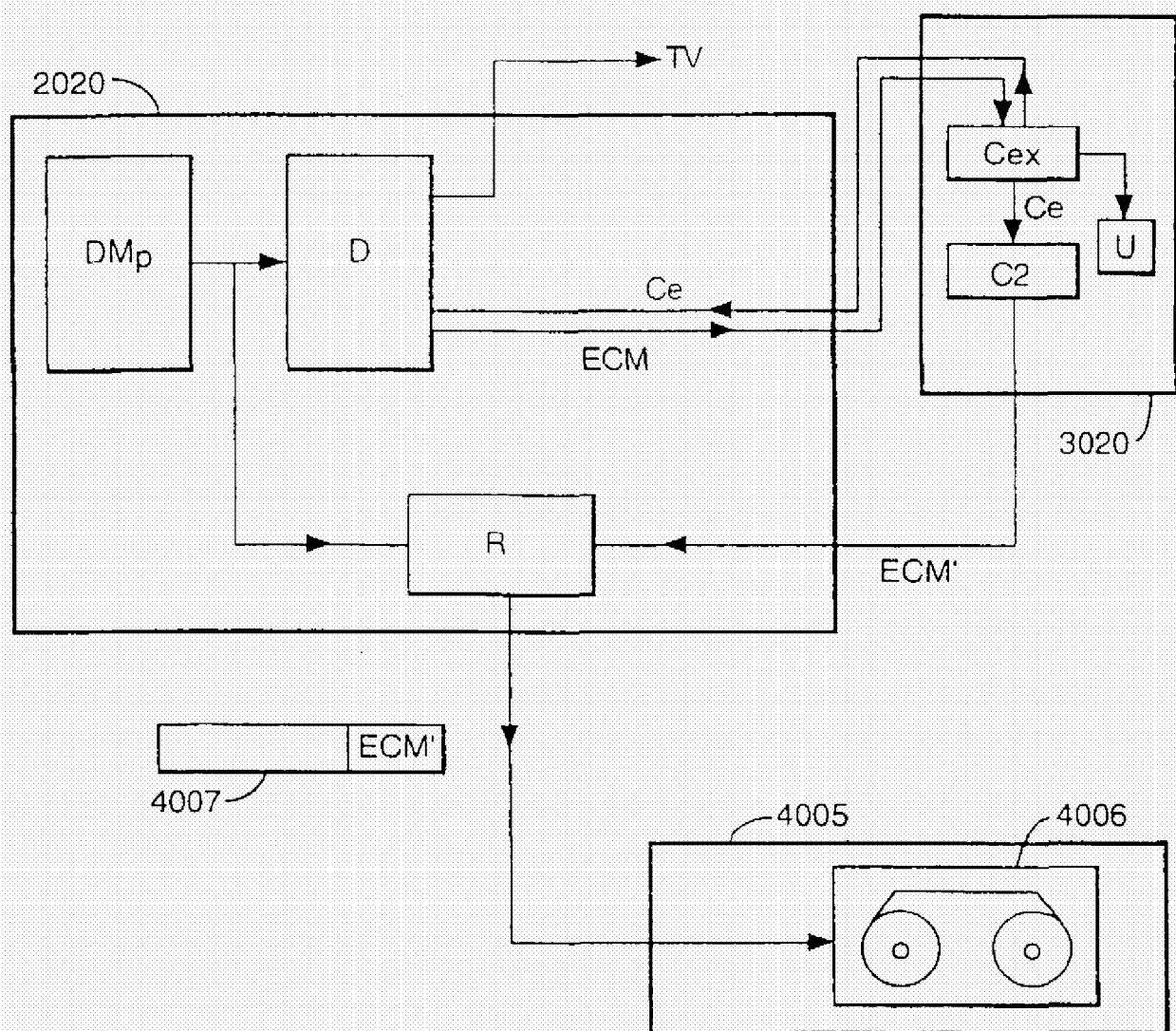
Slika 3



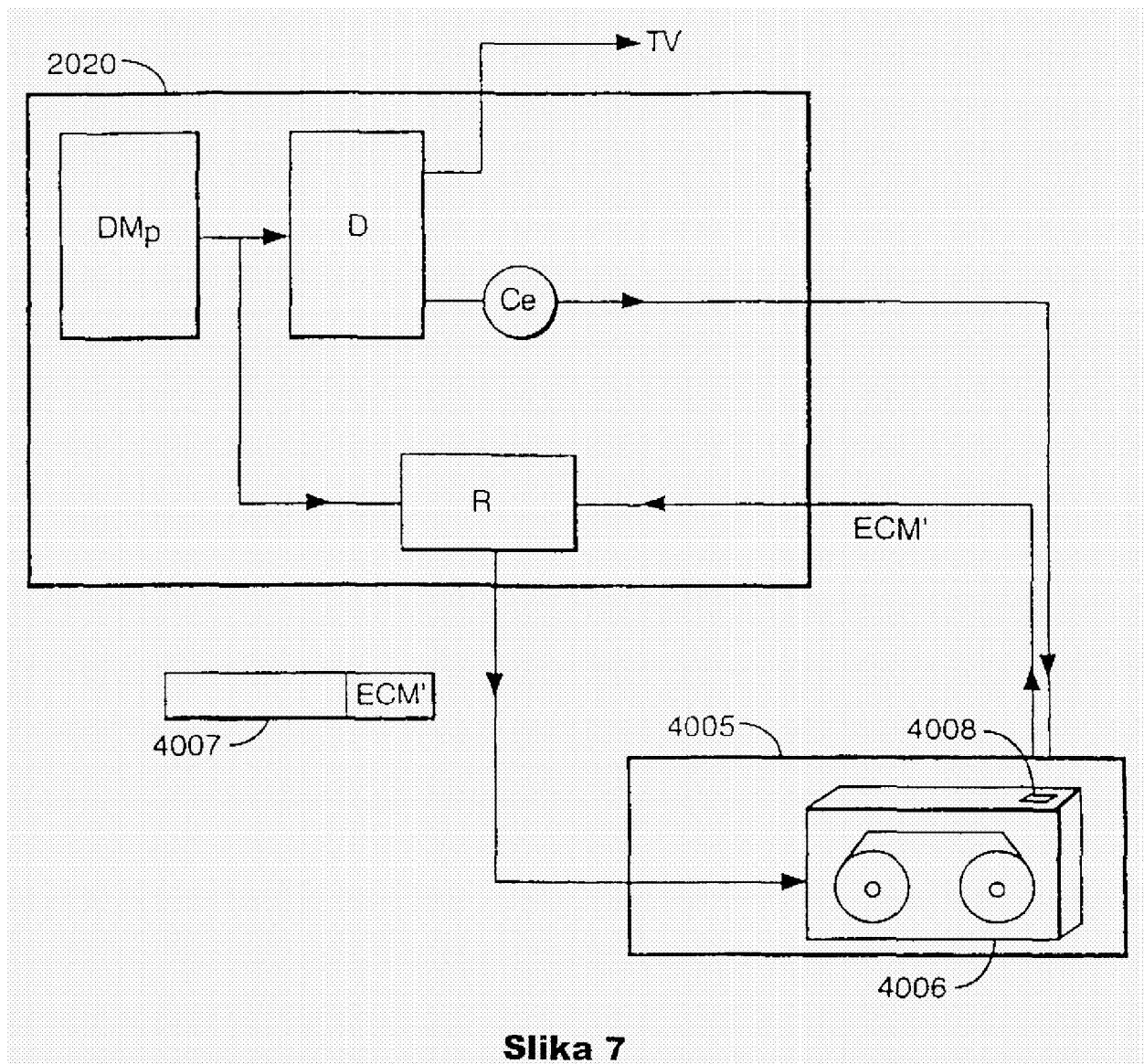
Slika 4



Slika 5



Slika 6



Slika 7