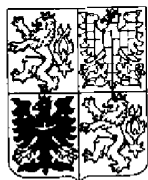


PŘIHLÁŠKA VYNÁLEZU

zveřejněná podle § 31 zákona č. 527/1990 Sb.

(19)
ČESKÁ
REPUBLIKA



ÚŘAD
PRŮMYSLOVÉHO
VLASTNICTVÍ

(22) Přihlášeno: **22.09.1998**

(32) Datum podání prioritní přihlášky: **25.09.1997**

(31) Číslo prioritní přihlášky: **1997/97402238**

(33) Země priority: **EP**

(40) Datum zveřejnění přihlášky vynálezu: **17.01.2001**
(Věstník č. 1/2001)

(86) PCT číslo: **PCT/IB98/01511**

(87) PCT číslo zveřejnění: **WO99/16244**

(21) Číslo dokumentu:

2000 - 1090

(13) Druh dokumentu: **A3**

(51) Int. Cl. ⁷:

H 04 N 5/913

(71) Přihlašovatel:

CANAL+SOCIETE ANONYME, Paris Cedex, FR;

(72) Původce:

Maillard Michel, Rambouillet, FR;

(74) Zástupce:

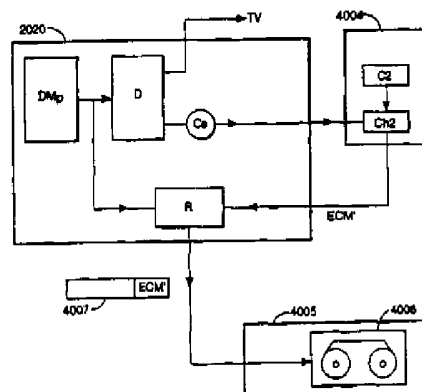
Korejzová Zdeňka JUDr., Spálená 29, Praha 1, 11000;

(54) Název přihlášky vynálezu:

**Způsob a zařízení pro vysílání a záznam
kódovaných digitálních dat**

(57) Anotace:

Způsob vysílání a záznamu kódovaných digitálních informací (Ce), ve kterém se digitální informace (Ce) kódují prostřednictvím prvního klíče a vysílají se v kódované formě, kódované informace (Ce) se přijímají dekodérem (2020), majícím přístup k ekvivalentu prvního klíče, který je potřebný pro dekódování informací. Dekódované informace (Ce) se potom opětovně kódují prostřednictvím druhého klíče (C2), uloženého v přenosném přídavném zařízení (4004), které je upraveno pro přijímání dekodérem (2020) nebo digitálním záznamovým zařízením (4005), přičemž opětovně kódované informace se potom zaznamenávají na digitálním záznamovém médiu (4006). Při přehrávání záznamu jsou informace dekódovány prostřednictvím druhého klíče (C2) uloženého na přídavném zařízení (4004). V obzvláště výhodném provedení informace (Ce) odpovídají fidicímú slovu, použitému pro kódování a dekódování vysílaných dat, přičemž opětovně kódované fidicí slovo (Ce) je uloženo na záznamovém médiu (4006) společně s ještě kódovanými vysílanými daty.



Způsob a zařízení pro vysílání a záznam kódovaných digitálních dat

Oblast techniky

5 Předkládaný vynález se týká způsobu a zařízení pro záznam kódovaných digitálních dat, například pro televizní přenosy.

Dosavadní stav techniky

10 Vysílání kódovaných dat je velmi dobře známé v oblasti systémů placené televize, kde kódované audiovizuální informace jsou přenášeny obvykle satelitem k množství účastníků, přičemž každý účastník má v držení dekodér nebo přijímač/dekodér schopný dekódování vysílaného programu pro následné sledování.

15 V typickém systému jsou kódovaná (šifrovaná) digitální data vysílána společně s řídicím slovem pro dekódování těchto digitálních dat, přičemž řídicí slovo samo je kódováno (šifrováno) prostřednictvím prvního klíče a vysíláno v kódované formě, a kódovaná digitální data a
20 kódované řídicí slovo jsou přijímány dekodérem obsahujícím ekvivalent prvního klíče, který je potřebný pro dekódování řídicího slova a potom pro dekódování vysílaných dat, přičemž dekodér je dále upraven pro předávání digitálních dat ještě v jejich kódované formě do digitálního záznamového zařízení.
25 Předplacený účastník bude přijímat měsíčně klíč potřebný pro dekódování kódovaného řídicího slova tak, aby mohl sledovat určitý program.

30 S nástupem digitálních technologií se kvalita vysílaných dat zvýšila mnohokrát. Určitý problém, spojený s

daty v digitální kvalitě, spočívá v jejich snadné reprodukci. Kde je dekodovaný program přenášena přes analogovou linku (například linku "Peritel") pro sledování a záznam prostřednictvím standardního VCR (videorekordéru) zůstává
5 kvalita ne větší, než bylo spojeno se standardním analogovým kazetovým záznamem. Riziko, že takový záznam může být použit jako matriční páska pro výrobu pirátských kopií tudíž není větší než u standardní v obchodě koupené analogové kazety.

Naproti tomu jakákoliv dekodovaná data přenášena pře
10 přímou digitální linku do jednoho z digitálních záznamových zařízení nové generace (například DVHS rekordér) budou na stejné kvalitě jako původně vysílaný program a mohou být tudíž reprodukovány v jakýchkoliv násobcích bez jakékoliv degradace v kvalitě obrazu nebo zvuku. Existuje tudíž poměrně
15 značné riziko, že dekodovaná data budou využívána jako matriční záznam pro výrobu pirátských kopií, a to buď dalších digitálních kopií nebo dokonce jednoduchých analogových VHS kopií.

Francouzská patentová přihláška 95 03859 popisuje
20 jednu z možností překonání tohoto problému prostřednictvím systému, ve kterém dekodovaným digitálním datům není nikdy umožněno, aby byla zaznamenána na digitální záznamové médium. Namísto toho dekodér, popisovaný v této přihlášce,
25 zaznamenává data v jejich kódované formě na záznamové médium společně s řídicím slovem potřebným pro dekodování dat opětovně kódovaných prostřednictvím dalšího klíče. Tento nový klíč je známý pouze přijímači/dekodéru a nahrazuje první klíč potřebný pro získání řídicího slova pro sledování programu.

Výhodou takového systému je to, že data nikdy nejsou
30 uložena v "čisté" formě a nemohou být sledována bez nového

klíče, který je uložen v přijímači/dekodéru. Tento systém rovněž má tu výhodu, že, protože první klíč se mění měsíčně, použití stálého klíče pro opětovné kódování řídicího slova zaznamenaného na digitální pásce znamená, že přijímač/dekodér bude stále schopen dekódovat řídicí slovo zaznamenané na pásce dokonce i po skončení předplaceného měsíce.

Nevýhodou systému navrženého v uvedené patentové přihlášce je to, že záznam může být sledován pouze ve spojení s určitým přijímačem/dekodérem. Pokud se tento dekodér porouchá, nebo je vyměněn, záznam již více nemůže být přehráván. Stejně tak není možné přehrávat záznam přímo v digitálním rekordéru bez spojení připojení přijímače/dekodéru do systému a divák tudíž musí udržovat svoji předplacenou službu u společnosti placené televize, aby udržel dekodér ve stavu umožňujícím sledovat filmy již vysílané.

Cílem předkládaného vynálezu je překonat výše uvedené problémy spojené s tímto řešením při současném podržení možnosti bezpečného záznamu digitálních dat, který nemůže být snadno použit pro vytváření pirátských kopií vysílaných dat.

Podstata vynálezu

Předkládaný vynález zahrnuje způsob vysílání a záznamu kódovaných digitálních informací, ve kterém se digitální informace kódují prostřednictvím prvního klíče a vysílají se v kódované formě, kódované informace se přijímají dekodérem majícím přístup k ekvivalentu prvního klíče, který je potřebný pro dekódování informací, přičemž podstata tohoto způsobu spočívá v tom, že dekódované informace se potom opětovně kódují prostřednictvím druhého klíče, uloženého v

5

10

15

20

25

30

Ve zvláště výhodném provedení je přenosným přídavným
zařízení inteligentní karta upravená pro přijetí ve čtecím
zařízení inteligentních karet v dekodéru a/nebo digitálním
rekordéru. V této přihlášce je termín "inteligentní karta"
5 použit pro označení jakéhokoliv běžného kartového zařízení na
bázi čipu, které obsahuje, například, mikroprocesor nebo
paměť EEPROM pro uložení algoritmu druhého klíče. V tomto
termínu jsou rovněž zahrnuta čipová zařízení mající
alternativní fyzické formy, například zařízení ve tvaru
10 klíčů, jak je často používáno v systémech televizních
dekodérů.

V jednom provedení vynálezu inteligentní karta rovněž
obsahuje ekvivalent prvního klíče, použitý pro dekodování
řídícího slova pro počáteční dekodování dat, například pro
15 sledování v případě televizního přenosového systému. V
takovém případě inteligentní karta tvoří součást systému
placené televize a může rovněž obsahovat osobní klíč známá
vysílači pro umožnění vysílači selektivně identifikovat,
kteří účastníci budou přijímat aktualizovaný první klíč na
20 konci měsíce.

V alternativním provedení vynálezu je druhý klíč
uložen na inteligentní kartě odlišné od té, která je použita
pro uložení prvního klíče. V takovém provedení se čtení
informací, uložených na digitálním záznamovém médiu, tudíž
25 stává zcela odděleným od účastnického systému a dokonce i
poté, co účastník odstoupil od systému a jeho účastnická
karta byla zrušena, může pokračovat ve sledování předtím
zaznamenaných filmů při zajištění, že digitální
rekordér/přehrávač, která má, je upraven pro čtení přidružené
30 inteligentní karty.

5

10

15

20

25

30

5

10

15

20

2.

3

5

10

15

20

25

30

Obr.6 znázorňuje druhé provedení vynálezu, ve kterém inteligentní karta obsahuje jak první tak i druhý klíč, potřebné pro sledování vysílaného respektive zaznamenaného programu,

společně s kreditními jednotkami pro určení počtu opakování, po který program může být sledován; a

Obr.7 znázorňuje třetí provedení vynálezu, ve které je druhý klíč uložen na integrovaném obvodu namontovaném v pouzdru digitální videokazety.

Příklady provedení vynálezu

Digitální televizní systém

Obr. 1 znázorňuje celkový přehled digitálního televizního vysílacího a přijímacího systému 1000, upravitelného pro předkládaný vynález. Tento systém zahrnuje většinou běžný digitální televizní systém 2000, který využívá známý MPEG-2 kompresní systém pro vysílání komprimovaných digitálních signálů. Přesněji MPEG-2 komprimátor 2002 ve vysílacím centru přijímá tok digitálního signálu (obvykle tok video signálů). Komprimátor 2002 je spojen s multiplexorem a kodérem 2004 prostřednictvím spojení 2006. Multiplexor 2004 přijímá množství dalších vstupních signálů, sestavuje jeden nebo více vysílacích toků a vysílá komprimované digitální signály do vysílače 2008 vysílacího centra přes spojení 2010, které samozřejmě může být představováno velkým množstvím různých forem včetně telekomunikačních linek. Vysílač 2008 vysílá elektromagnetické signály přes vzestupné spojení 2012 směrem k satelitnímu odpovídači 2014, kde jsou tyto signály elektronicky zpracovány a vysílány přes teoretické sestupné spojení 2016 do pozemního přijímače 2018, běžně ve formě parabolické antény vlastněné nebo pronajímané koncovým uživatelem. Signály přijímané přijímačem 2018 jsou vysílány do integrovaného přijímače/dekodéru 2020 vlastněného nebo

5

10

20

25

30

5

10

20

25

30

dekódování programu. Autorizace daného přijímače/dekodéru je řízena prostřednictvím zpráv EMM nebo opravňovacích správcovských (řídících) zpráv, vysílaných na méně častém základě, například každý měsíc, které dodávají do
5 autorizovaného přijímače/dekodéru klíč potřebný pro dekódování zpráv ECM.

Činnost systému 3000 podmíněného přístupu v digitálním televizním systému bude nyní popsána podrobněji ve spojení s odkazy na různé komponenty televizního systému 200
10 a systému 3000 podmíněného přístupu.

Multiplexor a kodér

Jak je patrné ze znázornění na obr. 1 a obr. 2, je ve vysílacím centru digitální video signál nejprve komprimován
15 (nebo je mu snížena bitová rychlost) s použitím MPEG-2 komprimátoru 2002. Tento komprimovaný signál je potom vysílán do multiplexoru a kodéru 2004 přes spojení 2006, aby byl multiplexován s dalšími daty, jako jsou další komprimovaná
20 data.

Kodér vytváří řídicí slovo Ce použité v kódovacím procesu a obsažené v toku MPEG-2 v multiplexoru 2004. Řídicí slovo Ce je vytvářeno vnitřně a umožňuje integrovanému přijímači/dekodéru 2020 koncového uživatele dekódovat
25 program. Přístupová kritéria, která indikují způsob komercializace programu, jsou rovněž přidávána do toku MPEG-2. Program může být komercializován kterýmkoliv jedním z množství "předplatitelských" módů a/nebo jedním z množství módů nebo událostí "placených za shlédnutí" (PPV). V
30 předplaceném módu koncový uživatel předplácí (účastní se)

jednu nebo více komerčních nabídek, nebo "soubory", což mu poskytuje práva sledovat každý kanál uvnitř těchto souborů. Ve výhodném provedení může být ze souboru kanálů zvoleno až 960 komerčních nabídek. V módu platby za shlédnutí je koncový uživatel vybaven možností kupovat události podle přání. To může být dosaženo buď předobjednáním události předem ("objednávkový mód"), nebo nákupem události, jakmile je vysílána ("impulzní mód").

Jak řídicí slovo Ce tak i přístupová kritéria jsou použita pro sestavení opravňovací řídicí zprávy (ECM); což je zpráva vysílaná ve spojení s jedním kódovaným programem; přičemž tato zpráva obsahuje řídicí slovo (které umožňuje dekódování programu) a přístupová kritéria vysílaného programu. Přístupová kritéria a řídicí slovo jsou vysílány do druhé šifrovací jednotky 3014 přes spojení 3018. V této jednotce je zpráva ECM vytvářena, kódována prostřednictvím exploatačního klíče Cex a vysílána na multiplexor a kodér 2004.

Každá služba vysílaná poskytovatelem vysílání v datech zahrnuje množství oddělených komponentů; například televizní program obsahuje video komponent V, audio komponent S, titulkovací nebo teletextový komponent T a podobně (viz obr. 4). Každý z těchto komponentů služby je individuálně šifrován a kódován pro následné vysílání do odpovídače 2014. Vzhledem ke každému kódovanému komponentu služby je vyžadována samostatná zpráva ECM.

Vysílání programů

Multiplexor 2004 přijímá elektrické signály zahrnující kódované zprávy EMM ze SAS 3002, kódované zprávy ECM z druhé šifrovací jednotky 3014 a komprimované programy z komprimátoru 2002. Multiplexor 2004 kóduje programy a vysílá kódované programy, kódované zprávy EMM (pokud jsou přítomné) a kódované zprávy ECM jako elektrické signály do vysílače 2008 vysílacího centra přes spojení 2010. Vysílač 2008 vysílá elektromagnetické signály směrem k satelitnímu odpovídáči 2014 přes vzestupné spojení 2012.

Přijímání programů

Satelitní odpovídáč 2014 přijímá a zpracovává elektromagnetické signály vysílané vysílačem 2008 a vysílá tyto signály k pozemnímu přijímači 2018, obvykle ve formě parabolické antény vlastněné nebo pronajaté koncovým uživatelem, přes sestupné spojení 2016. Signály přijímané pozemním přijímačem 2018 jsou vysílány do integrovaného přijímače/dekodéru 2020 vlastněného nebo pronajatého koncovým uživatelem a spojeného s televizním zařízením 2022 koncového uživatele. Přijímač/dekodér 2020 demultiplexuje signály, aby získal kódované programy s šifrovanými zprávami EMM a s šifrovanými zprávami ECM.

Pokud program není kódován, přijímač/dekodér 2020 dekomprimuje data a mění signál na video signál pro vysílání do televizního zařízení 2022.

Pokud program je kódován, přijímač/dekodér 2020 vybírá odpovídající zprávu ECM z toku MPEG-2 a předává tuto zprávu ECM "dceřiné" inteligentní kartě 3020 koncového uživatele. Ta je zasunuta do štěrby v pouzdru

přijímače/dekodéru 2020. Dceřiná inteligentní karta 3020 řídí, zda koncový uživatel má právo dekódovat zprávu ECM a právo přístupu k programu.

5 Pokud uživatel nemá potřebná práva, je do
přijímače/dekodéru 2020 předán negativní stav pro indikaci
toho, že program nemůže být dekódován. Pokud koncový uživatel
má příslušná práva, je zpráva ECM dekódována a je vyjmuto
řídící slovo. Dekodér 2020 potom může dekódovat program s
10 použitím tohoto řídícího slova. Tok MPEG-2 je dekomprimován a
převeden na video signál pro následné vysílání do televizního
zařízení 2022.

Použité úrovně kódování budou podrobněji popsány níže
ve spojení s odkazy na obr. 3.

15 Účastnický řídící systém (SMS)

Účastnický řídící systém (SMS) 3004 zahrnuje databázi
3024, která spravuje, kromě jiného, všechny soubory koncových
uživatelů, komerční nabídky (jako jsou tarify a reklamy),
20 předplacení, detaily PPV, a data týkající se spotřeby
koncových uživatelů a autorizace. SMS 3004 může být fyzicky
vzdálený od SAS 3002.

Každý SMS 3004 vysílá zprávy do SAS 3002 přes
odpovídající spojení 3006 pro umožnění modifikací nebo
25 vytváření opravňovacích řídících zpráv (EMM), určených k
vysílání ke koncovým uživatelům.

SMS 3004 rovněž vysílá zprávy do SAS 3002, které
nezahrnují jakékoliv modifikace nebo vytváření zpráv EMM, ale
30 zahrnují pouze změnu stavu koncového uživatele (týkající se
autorizace přidělené koncovému uživateli při objednávání

produktů nebo hodnoty, jaká bude koncovému uživateli účtována).

Opravnovací řídicí zpráv EMM nebo ECM

5

EMM je zpráva přidělená pouze jednotlivému koncovému uživateli (účastníkovi), nebo skupině koncových účastníků, (na rozdíl od zprávy ECM, která je přidělena pouze jednomu kódovanému programu nebo sadě kódovaných programů, pokud jsou součástí stejné komerční nabídky). Každá skupina může obsahovat daný počet koncových uživatelů. Tato organizace do skupin má za cíl optimalizovat využití šířky pásma; to znamená, že přístup k jedné skupině může umožnit dosažení většího počtu koncových uživatelů.

10

15

Různé specifické typy zprávy EMM jsou používány při uvádění předkládaného vynálezu do praxe. Jednotlivé zprávy EMM jsou přiděleny jednotlivým účastníkům a jsou obvykle používány při zajišťování služeb placených za shlednutí, přičemž tyto zprávy obsahují identifikátor skupiny a pozici účastníka v této skupině. Tak zvané "skupinové" účastnické zprávy EMM jsou přiděleny skupinám, řekněme o 256 jednotlivých účastnících, a jsou obvykle použity při spravování určitých účastnických služeb. Tato zpráva EMM má identifikátor skupiny a bitovou mapu skupiny účastníků.

20

25

Zveřejněné (volné) EMM jsou přiděleny celým publikům a mohly by být například použity určitým operátorem pro poskytování určitých volných služeb. "Publikum" je souhrn účastníků majících inteligentní karty, které nesou stejný identifikátor operátora (OPI). Nakonec "unikátní" zpráva EMM je adresována unikátnímu identifikátoru inteligentní karty.

30

Úrovně kódování v systému

Nyní budou ve spojení s odkazy na obr. 3 popsány úrovně kódování ve vysílacím systému. Na tomto obrázku jsou znázorněny fáze kódování 4001, spojené s vysíláním
5 digitálních dat, vysílací kanál 4002 (například satelitní spoj nebo modemový zpětný kanál jak bylo popisováno výše), a fáze 4003 dekódování v přijímači.

Digitální data N jsou kódována prostřednictvím
10 řídicího slova Ce předtím, než jsou vysílána do multiplexoru Mp pro následné vysílání. Jak bude patrné z obr. 4, obsahují vysílaná data zprávu ECM zahrnující, kromě jiného, řídicí slovo Ce, jak je kódováno prostřednictvím kódovacího prostředku Ch1 řízeného prvním kódovacím klíčem Cex. V
15 přijímači/dekodéru signál prochází skrz demultiplexor DMp a dekodér D předtím, než projde do televizního zařízení 2022 pro sledování. Dekódovací jednotka DCh1, která má rovněž klíč Cex, dekóduje zprávu ECM v demultiplexovaném signálu pro získání řídicího slova Ce následně použitého pro dekódování
20 signálu.

Z bezpečnostních důvodů se řídicí slovo Ce obsažené v kódované ECM mění průměrně každých 10 sekund nebo podobně. Naproti tomu první kódovací klíč Cex, použitý přijímačem pro dekódování ECM, je měněn každý měsíc, nebo podobně,
25 prostřednictvím zprávy EMM. Kódovací klíč Cex je kódován prostřednictvím druhé kódovací jednotky ChP s použitím individualizovaného klíče Cg odpovídajícího identitě dekodéru. Pokud dekodér je jedním z těch, které byly zvoleny pro přijetí aktualizovaného kódovacího klíče Cex, pak
30 dekodovací jednotka DChP v dekodéru bude dekódovat zprávu s

použitím jeho individualizovaného klíče Cg pro získání tohoto měsíčního kódovacího klíče Cex.

5 Dekódovací jednotky DChP a DCh1 a přidružené klíče jsou uchovány na inteligentní kartě poskytnuté účastníkovi a vložené do čtecího zařízení inteligentních karet v dekodéru. Klíče mohou být vytvářeny podle jakéhokoliv známého symetrického algoritmu pro vytváření klíčů, jako je DES. Alternativní provedení využívající algoritmy veřejných/privátních klíčů jsou rovněž možná.

Záznam digitálních dat

15 Jak bylo uvedeno v úvodu, není doporučeníhodné, aby dekódovaným digitálním datům bylo umožněno zaznamenání vzhledem k rizikům, která vznikají ve spojení s neautorizovaným kopírováním a s pirátstvím. Jak je znázorněno na obr. 5, předkládaný vynález zajišťuje prostředek pro překonání tohoto problému.

20 Systém zahrnuje inteligentní kartu 4004, vložitelnou do zdířky pro inteligentní kartu v přijímači/dekodéru, společně s digitálním rekordérem 4005, jako je například DVHS rekordér, obsahujícím digitální záznamové médium 4006, jako je DVHS kazeta.

25 V tomto provedení je přijaté řídicí slovo dekódováno prostřednictvím přidružené inteligentní karty 3020 vložené do dekodéru (viz obr. 2). Dekódované řídicí slovo Ce (společně s jakýmkoliv dalšími daty, která tvoří zprávu ECM, jako jsou přístupové řídicí informace a podobně), je potom předáno do mikroprocesoru zapuštěného v inteligentní kartě 4004. S
30 použitím druhého kódovacího klíče C2 a druhého kódovacího

algoritmu Ch2 inteligentní karta 4004 vytváří novou zprávu ECM, která je na obrázku označena jako zpráva ECM'. Tato opravňovací zpráva ECM' je potom použita pro nahrazení zprávy ECM v toku kódovaných dat z demultiplexoru Dmp, jak je
5 označen vztahovou značkou jako tok 4007 kódovaných dat, a kombinace těchto kódovaných dat a nové opravňovací zprávy ECM' je zaznamenána na DVHS kazetě 4006. Opravňovací zpráva ECM' může být vložena do datového toku procházejícího skrz posouvací řídicí registr R.

10 Tímto způsobem předkládaný vynález zamezuje záznamu dekódovaných audiovizuálních informací na kazetu. Aby bylo možné přehrávat kazetu, je do dekodéru vložena karta, klíč C2 je použit pro dekódování opravňovací zprávy ECM', a následně je vyjmuté řídicí slovo Ce použito pro řízení dekodéru pro
15 dekódování programu pro sledování.

V systému znázorněném na obr. 5 je inteligentní karta 4004 odlišná od inteligentní karty 3020, znázorněné na obr. 2 pro televizní systém, která obsahuje kódovací klíče potřebné pro sledování programu. V alternativním provedení znázorněném
20 na obr. 6 ale inteligentní karta 3020 obsahuje jak první tak i druhý kódovací klíč Cex a C2, které jsou potřebné pro sledování respektive pro záznam programu. Jak je reprezentováno, klíč Cex řídí dekódování zprávy ECM pro vytvoření řídicího slova Ce, použitého dekodérem D pro
25 sledování programu a následně kódovaného klíčem C2 pro vytvoření nové opravňovací zprávy ECM'.

Algoritmy DCh1 a DCh2 nebyly z prostorových důvodů znázorněny. Inteligentní karta 3020 je ve skutečnosti obvykle
30 rovněž inicializována individualizovaným klíčem Cg (není znázorněn) umožňujícím dekódování zpráv EMM tak, aby byl

získán měsíční klíč Cex uložený v paměti karty. Ačkoliv inteligentní karta byla znázorněna ve formě v podstatě obdélníkové karty, jiné fyzické formy, jako jsou tvary klíčů a podobně, jsou samozřejmě možné.

5 Zpráva ECM vysílaná s programem a dekodovaná prostřednictvím inteligentní karty může rovněž obsahovat kreditní jednotky U následně uložení v kartě, které řídí počet opakování, po který zaznamenaný film může být sledován. V nejjednodušším provedení mohou být kreditní jednotky
10 odečítány během přehrávání zaznamenaného filmu pokaždé, když dekodérem projde zpráva ECM'. Jakmile počet kreditů již byl snížen na nulu, což indikuje, že záznam již byl sledován po předem stanovený počet opakování, je do dekodéru vyslána zpráva pro zabránění dalších sledování filmu, pokud kreditní
15 karty nejsou opětovně doplněny (prostřednictvím, například, dobíjecí instrukce vyslané ve zprávě EMM).

V alternativních provedeních mohou být kreditní jednotky odečítány po každých deseti nebo sto zprávách ECM'. V ještě dalších provedeních kreditní jednotky mohou odpovídat
20 určitým úsekům filmu (například prvním nebo posledním 10 minutám filmu) tak, že přehrávání těchto úseků odečte kreditní jednotky sdružené s těmito úseky. Úseky mohou být identifikovány prostřednictvím příslušného označení příznaky
25 zpráv ECM' v těchto úsecích.

Další provedení předkládaného vynálezu je znázorněno na obr. 7. V tomto provedení je vytváření nové opravňovací zprávy EMM' řízeno prostřednictvím integrovaného obvodu nebo
30 čipu 4008, který obsahuje druhý kódovací klíč C2 a je zapuštěn v pouzdru záznamové kazety 4006. Začlenění mikroprocesoru do pouzdra záznamového média je známá technika

a byla navržena, například, pro pouzdra DVHS kazet. V tomto příkladu může být na vnějším povrchu pouzdra kazety vytvořena sada kontaktů, přičemž tyto kontakty vedou k elektronickému obvodu, jako je integrovaný obvod nebo čip, ve vnitřku pouzdra. Tyto kontakty mohou být uvedeny do záběru s odpovídající sadou kontaktů v zásuvce (nebo zdířce rekordéru pro umožnění spojení mezi integrovaným obvodem a videorekordérem.

Jak bude zcela zřejmé, ačkoliv je jednoduché kopírovat zaznamenaná (a kódovaná) digitální data, data uložená na čipu budou odolná proti kopírování a, jako u předcházejících provedení, kódovaná data budou nepotřebná bez klíče C2 potřebného pro dekódování zprávy ECM' pro získání řídicího slova použitého dekodérem.

Jak by mělo být zcela zřejmé, ve všech popsanych provedeních mohou být prvky přijímače/dekodéru a digitálního záznamového zařízení kombinovány nebo vzájemně zaměňovány, takže digitální rekordér má například štěrbinu (zdířku) pro inteligentní kartu pro příjem této inteligentní karty a/nebo potřebné prvky pro dekódování programu, jakmile již bylo řídicí slovo Ce vyjmuta ze zprávy ECM'. Dekodér a/nebo digitální dekodér může být stejně tak integrován společně s dalšími zařízeními, jako je například televize.

Zastupuje :

P A T E N T O V É N Á R O K Y

1. Způsob vysílání a záznamu kódovaných digitálních informací, ve kterém se digitální informace kódují prostřednictvím prvního klíče a vysílají se v kódované formě, kódované informace se přijímají dekodérem majícím přístup k ekvivalentu prvního klíče, který je potřebný pro dekódování informací, **vyznačující se tím, že** dekódované informace se potom opětovně kódují prostřednictvím druhého klíče, uloženého v přenosném přídavném zařízení, které je upraveno pro přijímání dekodérem nebo přidruženým digitálním rekordérem, přičemž opětovně kódované informace se potom zaznamenávají na digitálním záznamovém médiu prostřednictvím digitálního rekordéru.

2. Způsob podle nároku 1, **vyznačující se tím, že** digitální informace odpovídají řídicímu slovu pro dekódování kódovaných digitálních dat, přičemž kódovaná digitální data se vysílají společně s řídicím slovem tak, jak byly kódovány prostřednictvím prvního klíče, řídicí slovo se potom dekóduje prostřednictvím ekvivalentu prvního klíče a opětovně se kóduje druhým klíčem a toto opětovně kódované řídicí slovo a kódovaná data se potom zaznamenávají na digitálním záznamovém médiu.

3. Způsob podle nároku 1 nebo 2, **vyznačující se tím, že** přenosným přídavným zařízením je inteligentní karta upravená pro přijetí ve čtecím zařízení inteligentních karet v dekodéru a/nebo digitálním dekodéru.

4. Způsob podle nároku 3, **vyznačující se tím, že** inteligentní karta rovněž obsahuje ekvivalent prvního klíče,

použitý pro dekódování řídicího slova pro počáteční dekódování dat.

5 5. Způsob podle nároku 3, **vyznačující se tím, že** druhý klíč se uloží na inteligentní kartě odlišné od prostředku použitého dekodérem pro uložení prvního klíče.

10 6. Způsob podle kteréhokoliv z nároků 3 až 5, **vyznačující se tím, že** jedna inteligentní karta a druhý klíč se použijí pro vytvoření opětovně kódovaného řídicího slova pro množství záznamů.

15 7. Způsob podle kteréhokoliv z nároků 3 až 6, **vyznačující se tím, že** inteligentní karta rovněž obsahuje počet kreditních jednotek pro určení, kolikrát záznam může být přehrán, přičemž počet jednotek se snižuje s každým následným částečným nebo úplným přehráním záznamu.

20 8. Způsob podle nároku 7, **vyznačující se tím, že** kreditní jednotky jsou sdruženy s určitým segmentem záznamu tak, že přehránění úseku záznamu snižuje určité kredity sdružené s tímto úsekem.

25 9. Způsob podle nároku 8, **vyznačující se tím, že** kreditní jednotky jsou jednoho typu a jejich počet se snižuje s přehráním jakéhokoliv úseku záznamu.

30 10. Způsob podle nároku 1, **vyznačující se tím, že** přenosné přídatné zařízení je definováno samotným záznamovým médiem, přičemž druhý klíč se uloží v integrovaném obvodu zapuštěném v pouzdru digitálního záznamového média.

35 11. Zařízení k provádění způsobu vysílání a záznamu kódovaných digitálních dat podle kteréhokoliv z nároků 1 až

10, **vyznačující se tím, že** zahrnuje vysílač pro kódování digitálních informací s prvním klíčem a pro vysílání těchto informací v kódované formě, dekodér pro příjem kódovaných informací, který má přístup k ekvivalentu prvního klíče, 5 potřebného pro dekódování informací, a přenosné přídavné zařízení upravené pro přijetí dekodérem nebo přidruženým digitálním rekordérem, které má druhý klíč pro opětovné kódování dekódovaných informací pro následné vysílání do digitálního záznamového zařízení pro zaznamenání na 10 digitálním záznamovém médiu.

12. Dekodér pro zařízení podle nároku 11 a adaptér pro použití ve způsobu podle kteréhokoliv z nároků 1 až 10, **vyznačující se tím, že** obsahuje zásuvku pro přijetí 15 přenosného přídavného zařízení majícího druhý klíč pro opětovné kódování dekódovaných informací.

13. dekodér podle nároku 12, **vyznačující se tím, že** je integrován s digitálním záznamovým zařízením pro zaznamenání opětovně kódované informace na digitálním záznamovém médiu.

20 **Zastupuje :**

25

30

Fig.1.

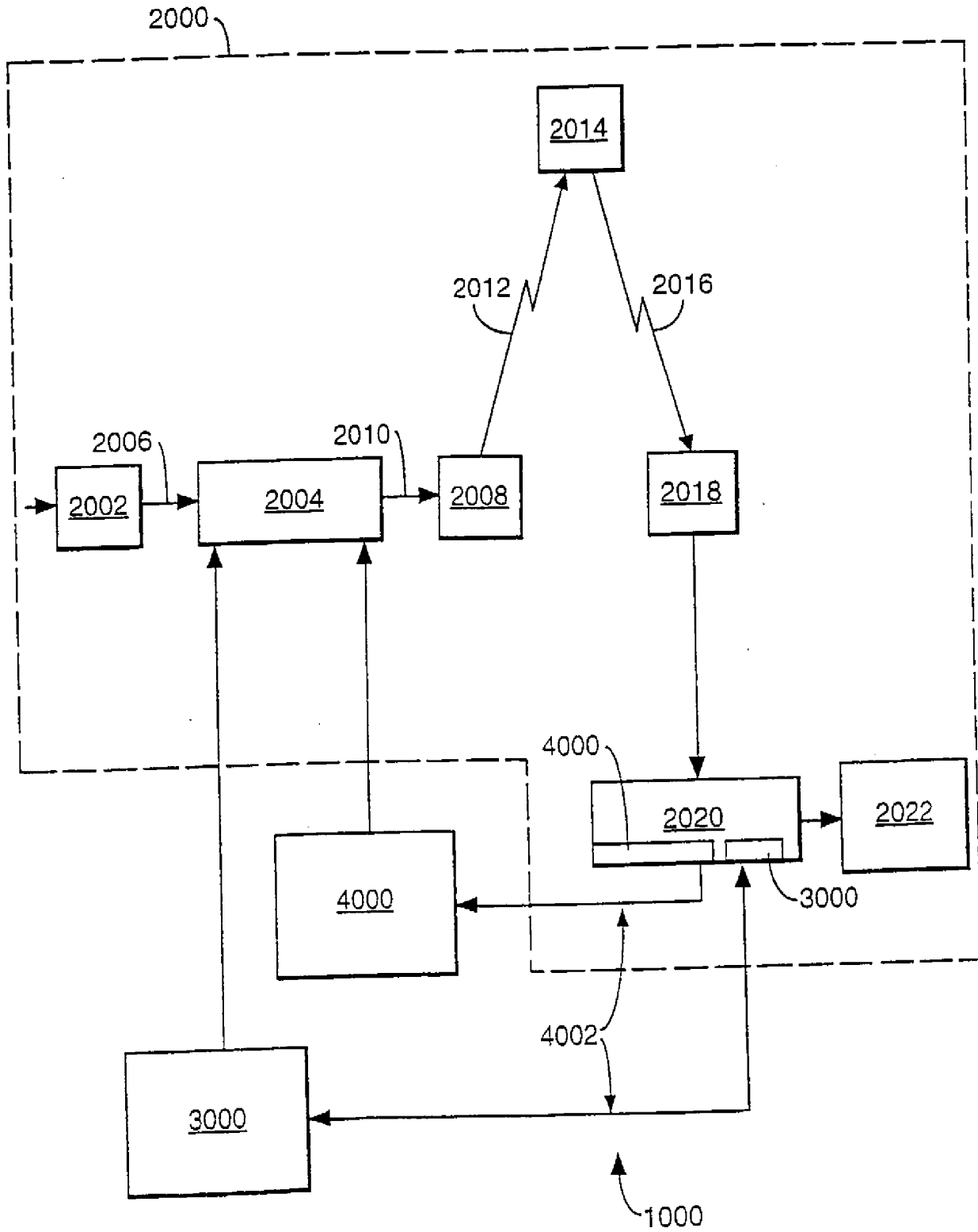


Fig.2.

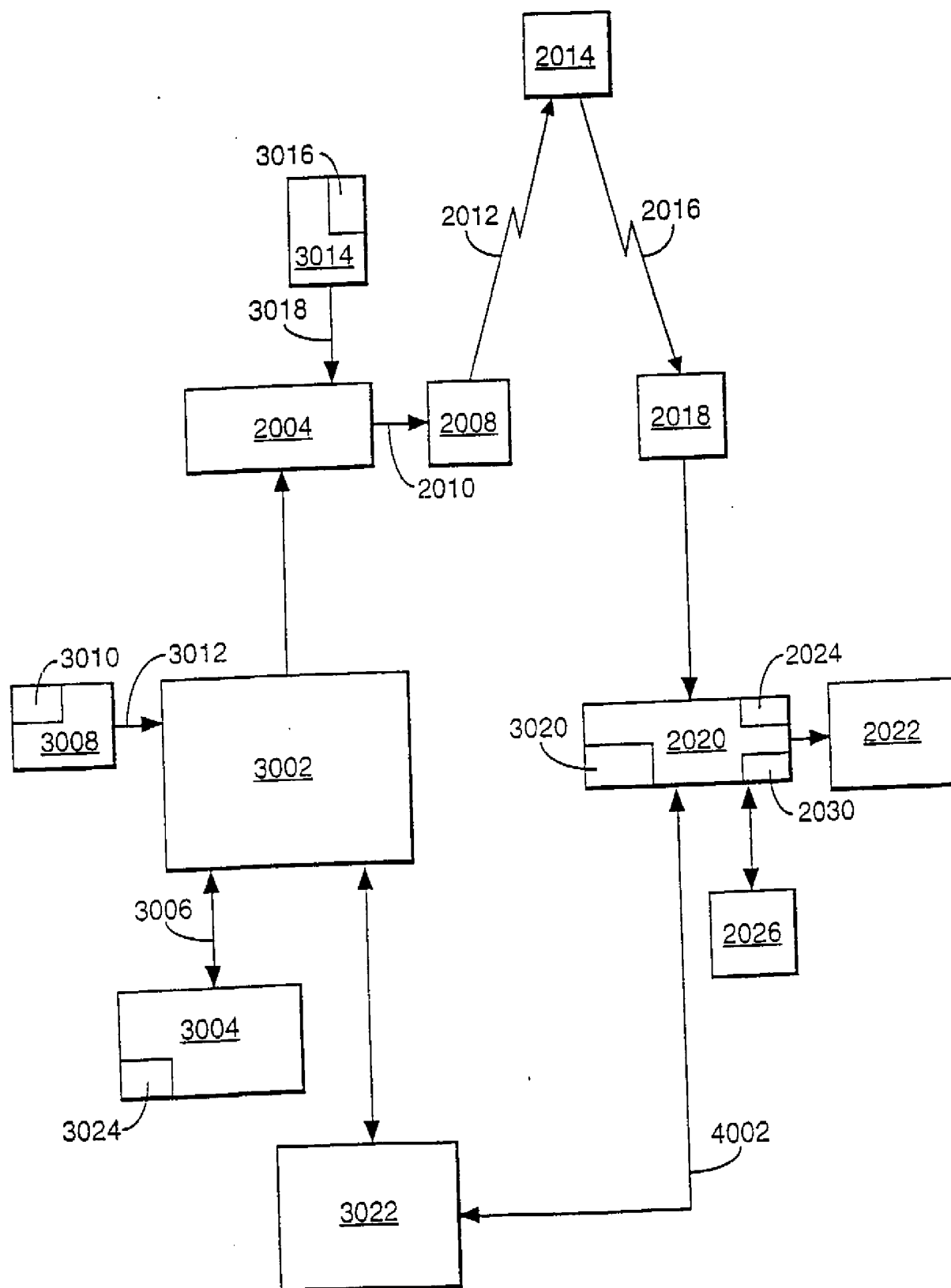


Fig.3.

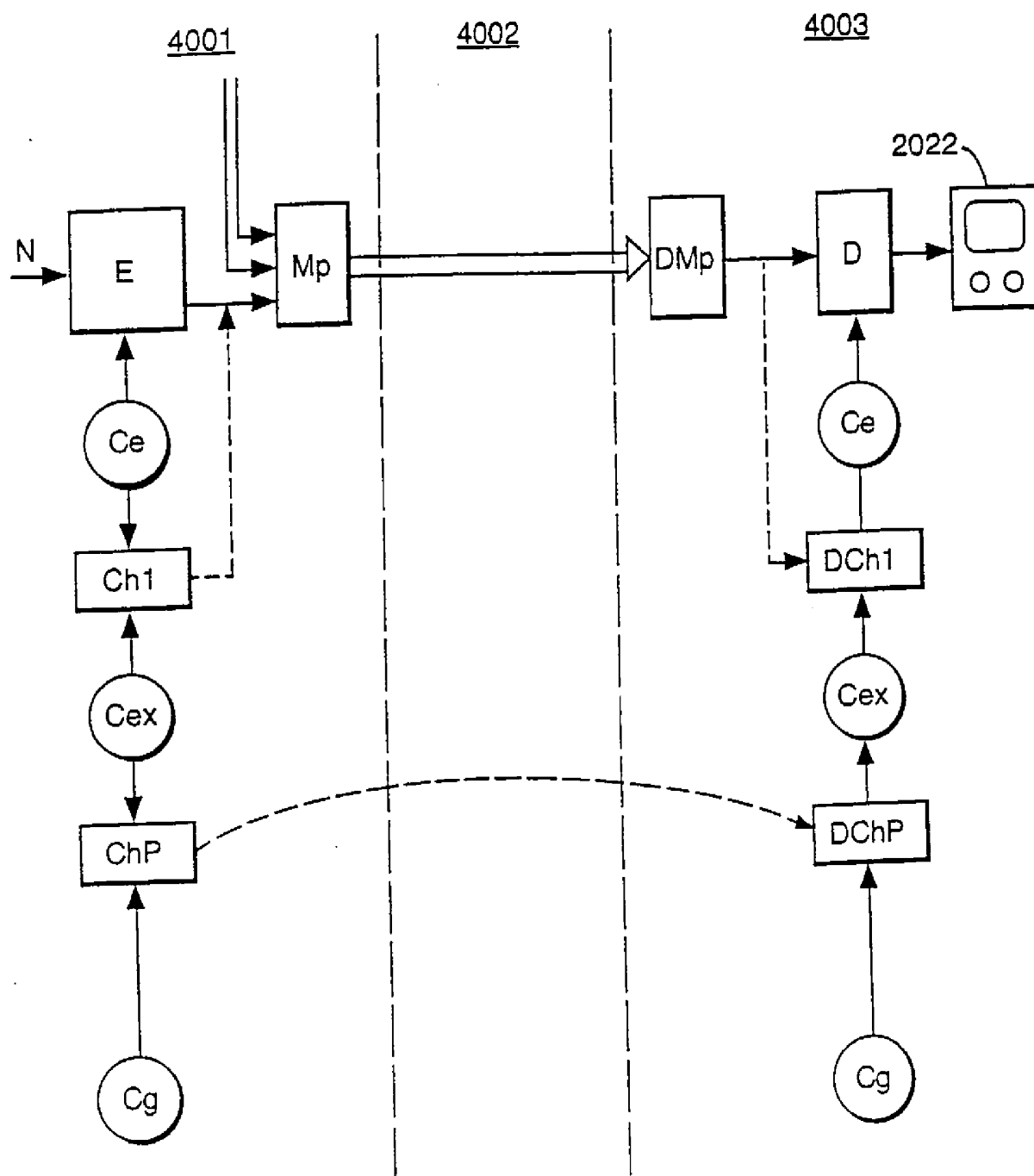


Fig.4.

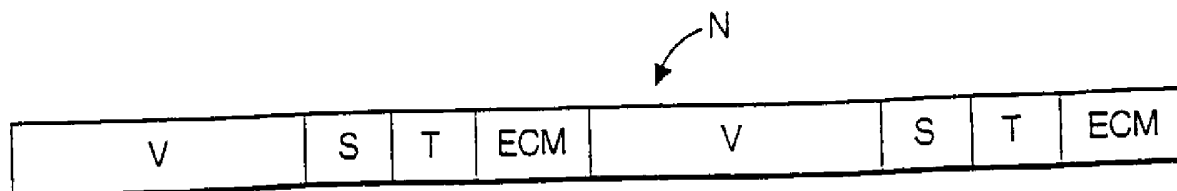


Fig.5.

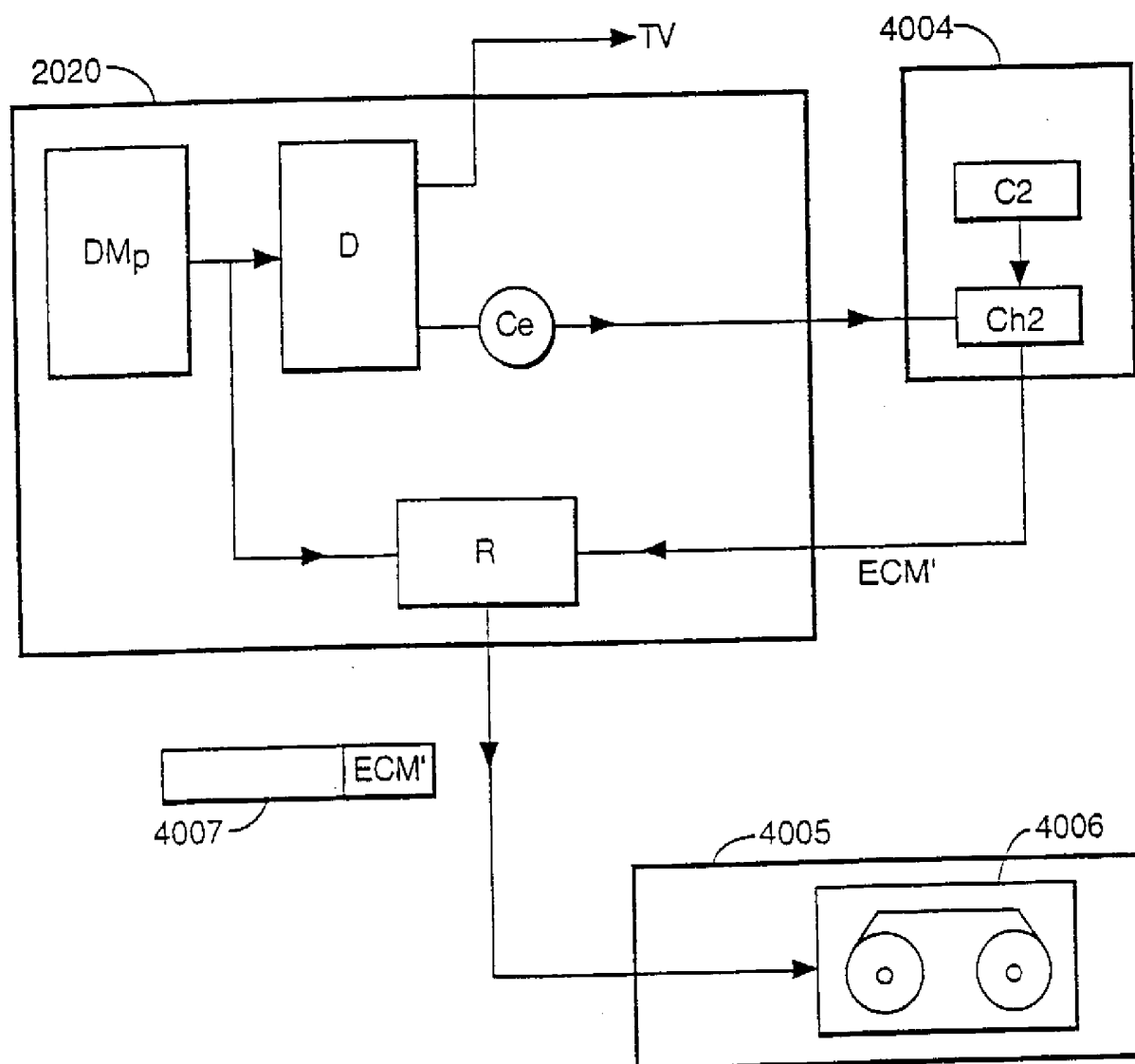


Fig.6.

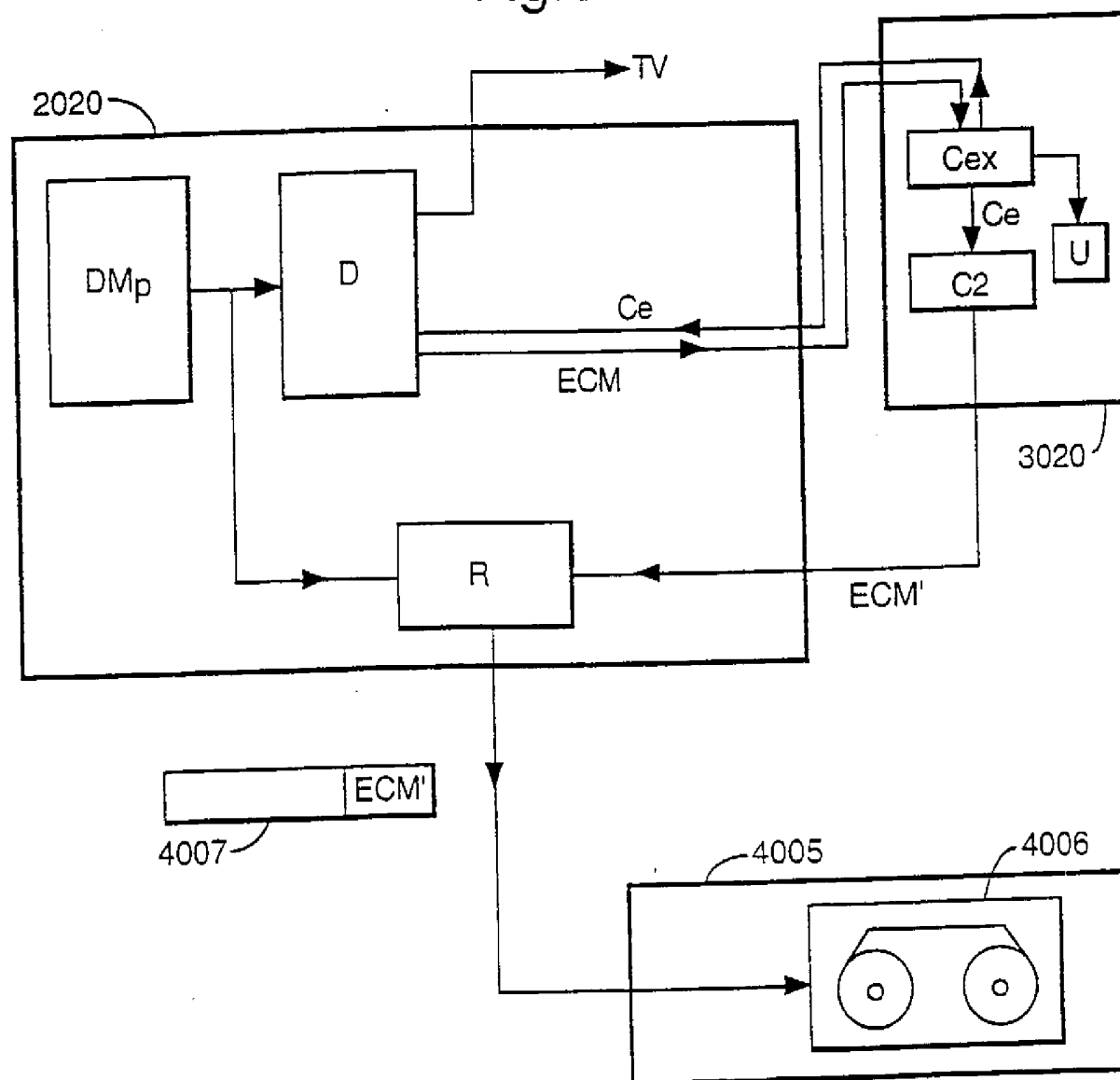


Fig.7.

