

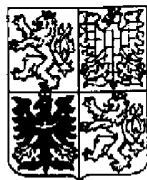
PŘIHLÁŠKA VYNÁLEZU

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

(21) Číslo dokumentu:

1999 - 3313

(19)
ČESKÁ
REPUBLIKA



ÚŘAD
PRŮMYSLOVÉHO
VLASTNICTVÍ

(22) Přihlášeno: **25.04.1997**

(32) Datum podání prioritní přihlášky: **21.03.1997**

(31) Číslo prioritní přihlášky: **1997/97400650**

(33) Země priority: **EP**

(40) Datum zveřejnění přihlášky vynálezu: **12.07.2000**
(Věstník č. 7/2000)

(86) PCT číslo: **PCT/EP97/02111**

(87) PCT číslo zveřejnění: **WO98/43431**

(13) Druh dokumentu: **A3**

(51) Int. Cl. ⁷:

H 04 N 7/167

(71) Přihlašovatel:
CANAL+ SOCIÉTÉ ANONYME, Paris, FR;

(72) Původce:
Sarfati Jean-Claude, Epinay sur Seine, FR;
Meric Jérôme, Saint Lis, FR;

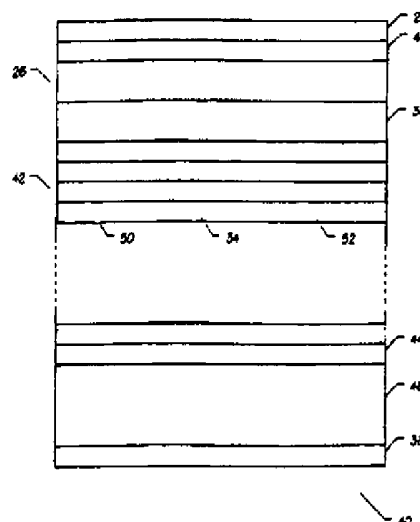
(74) Zástupce:
Korejzová Zdeňka JUDr., Spálená 29, Praha 1, 11000;

(54) Název přihlášky vynálezu:
**Způsob zavádění dat do MPEG
přijímače/dekodéru a MPEG vysílací systém pro
jeho realizaci**

(57) Anotace:

V digitálním satelitním televizním systému, ve kterém televize přijímá svůj signál přes přijímač/dekodér (2020), jako je nastavovací řídící skříň, mohou být interaktivní aplikace stahovány a spouštěny na přijímači/dekodéru (2020). Aplikační kód je uspořádán ve formě modulů a stahování modulů předchází vyhledání adresářového modulu uvnitř specifikovaných místních adres. Moduly jsou označeny (podepsány) a adresářový modul je podepsán a kódován tak, že jedno kódování platí pro všechny moduly tvořící aplikaci. Vícenásobné veřejné kódovací klíče jsou uloženy v ROM přijímače/dekodéru (2020), takže aplikace mohou být vytvářeny různými zdroji, aniž by tyto zdroje musely vzájemně znát ostatní privátní kódovací klíče. Je zajištěno opatření pro umožnění dočasného uložení kódovacího klíče v RAM přijímače/dekodéru (2020), takže výrobce přijímače/dekodéru (2020) může ověřit jeho funkčnost. Podpis adresáře může být skrytý na různých polohách v bloku fiktivních dat v adresářovém modulu. Aplikace určené ke stažení mohou být kontrolovány vzhledem k bitové mapě pro ověření platnosti aplikace, uložené v přijímači/dekodéru (2020). Dále je předmětem vynálezu přijímač/dekodér (2020) pro použití při realizaci tohoto způsobu, který zahrnuje prostředek pro přijímání MPEG tabulek, prostředek pro ukládání množství veřejných klíčů a zpracovatelský prostředek

naprogramovaný pro zvolení jednoho z uložených veřejných klíčů.



Způsob zavádění dat do MPEG přijímače/dekodéru a MPEG vysílací systém pro jeho realizaci

Oblast techniky

Předkládaný vynález se týká:-

• způsobu zavádění (stahování) dat do MPEG
přijímače/dekodéru;

- MPEG přijímače/dekodéru; a
- MPEG vysílacího systému.

Dosavadní stav techniky

Nástup digitálních vysílacích systémů určených
primárně pro vysílání televizních signálů, zejména, ale ne
výhradně, satelitních televizních systémů, otevřel možnost
využití těchto systémů pro další účely. Jedním z těchto účelů
je zajištění interaktivity s koncovým uživatelem.

Jedním způsobem pro realizaci tohoto záměru je
spustit aplikaci na přijímači/dekodéru, kterým je přijímán
televizní signál. Kód pro aplikaci by mohl být trvale uložen
v přijímači/dekodéru. Ovšem toto uspořádání by bylo spíše
omezující. Výhodně by měl být přijímač/dekodér schopen
stahovat kód pro požadovanou aplikaci. Tímto způsobem může
být dosaženo větší pružnosti a aplikace mohou být
aktualizovány podle požadavků bez jakýchkoliv zásahů na
straně uživatele.

V MPEG systému může být aplikační kód stahován v MPEG
tabulkách. Je zde ale omezení ve velikosti jednoho kódu,
který může být stažen prostřednictvím jedné MPEG tabulky.
Navíc, pokud je požadováno, aby byla stažena celá aplikace
předtím, než může být spuštěna, může tímto způsobem vzniknout

zpoždění, které je pro uživatele zcela nepřijatelné. Existuje tudíž potřeba možnosti stahovat aplikace ve formě množství modulů. To ale potom vytváří problém s možností identifikace a vyjímání z MPEG bitového toku modulů požadovaných pro určitou aplikaci. První aspekt předkládaného vynálezu se zabývá tímto problémem.

Podstata vynálezu

Podle prvního aspektu předkládaného vynálezu je tedy navržen způsob zavádění alespoň části aplikace do MPEG přijímače/dekodéru, který zahrnuje kroky: rozdělení aplikace do množství modulů; formátování každého z modulů jako odpovídající MPEG tabulku, přičemž tyto tabulky mají stejnou tabulkovou identifikaci ("TID") a odpovídající odlišná tabulková identifikační rozšíření ("TID-rozšíření") jiná, než je předem stanovené TID-rozšíření; vytvoření adresářové MPEG tabulky pro moduly, která má stejnou uvedenou TID a uvedené předem stanovené TID-rozšíření, přičemž adresář obsahuje pro každý modul jméno tohoto modulu a odpovídající TID-rozšíření; cyklického vysílání adresářové MPEG tabulky a modulových MPEG tabulek v MPEG bitovém toku; a v MPEG přijímači/dekodéru: - přijímání MPEG bitového toku; stahování té jedné z MPEG tabulek, která má předem stanovené TID-rozšíření tak, aby byla stažena adresářová MPEG tabulka; určování z obsahu adresářové MPEG tabulky TID-rozšíření modulových MPEG tabulek; a stahování alespoň jedné z modulových MPEG tabulek majících stejnou TID, jako je TID stažené adresářové MPEG tabulky, a TID-rozšíření určené ze stažené adresářové MPEG tabulky.

Podle toho tedy může být aplikace sestavena z určitého počtu modulů, které mohou být staženy, a pokud je to vhodné spuštěny, podle požadavku. Adresářová tabulka může být snadno identifikována, protože má určité TID-rozšíření, a jakmile již byla stažena, umožňuje tato tabulka přijímači/dekodéru identifikovat modulové tabulky z jejich příslušných TID-rozšíření.

Způsob výhodně dále zahrnuje kroky: začlenění do vysílané adresářové MPEG tabulky identifikaci verze pro tuto tabulku; a v přijímači/dekodéru:- určování zda identifikace verze právě vysílané adresářové PMT MPEG tabulky je aktuálnější než identifikace verze právě stažené adresářové MPEG tabulky, a pokud ano, opakování kroků stahování adresářové MPEG tabulky, určování TID-rozšíření, a stahování alespoň jedné z modulových MPEG tabulek.

Podle toho tedy, pokud by aplikace byla měněna, může to být automaticky zjištěno a mohou být staženy aktualizovaný adresář a jakékoliv aktualizované moduly.

Alespoň jedna z modulových MPEG tabulek může být formátována jako množství MPEG úseků, které jsou vysílány samostatně v MPEG bitovém toku, přičemž každý tento MPEG úsek obsahuje v jeho předem stanovené části identifikaci tohoto MPEG úseku v MPEG tabulce a indikaci počtu úseků v MPEG tabulce.

Podle druhého aspektu předkládaného vynálezu je vytvořen MPEG přijímač/dekodér pro použití při realizaci části způsobu podle prvního aspektu předkládaného vynálezu, který zahrnuje: přijímač pro přijímání MPEG bitového toku; paměťový prostředek; a zpracovatelský prostředek, který je

naprogramován pro řízení stahování té jedné z přijímaných MPEG tabulek, která má předem stanovené MPEG-rozšíření, do paměťového prostředku, určování z obsahu adresářové MPEG tabulky TID-rozšíření modulových MPEG tabulek, a pro řízení stahování do paměťového prostředku alespoň jedné z modulových MPEG tabulek, která má stejnou TID, jako je TID stažené adresářové MPEG tabulky, a TID-rozšíření určené ze stažené adresářové MPEG tabulky.

Výhodně je zpracovatelský prostředek naprogramován pro určování, zda identifikace verze právě přijímané adresářové MPEG tabulky je aktuálnější, než je identifikace verze stažené adresářové MPEG tabulky, a pokud ano, pro opakování stahování adresářové MPEG tabulky, určování TID-rozšíření a stahování alespoň jedné z modulových MPEG tabulek.

V případě, ve kterém je přijímač/dekodér uspořádán pro přijímání alespoň jedné z modulových tabulek formátovaných jako množství samostatně vysílaných úseků, je zpracovatelský prostředek výhodně naprogramován pro řízení opakovaného stahování MPEG úseků do paměťového prostředku, dokud zpracovatelský prostředek neurčí z identifikací úseků a indikace počtu úseků stahovaných úseků, že již byly staženy všechny z úseků.

Výhodně přijímač/dekodér dále zahrnuje paralelní port a/nebo sériový port uspořádaný pro přijetí aplikace formátované jako alespoň jedna MPEG tabulka, přičemž v tomto případě je výhodně použito krátkého formátu MPEG-2, zatímco dlouhý MPEG-2 formát je výhodně použit pro dálkový příjem, například prostřednictvím satelitu nebo kabelu.

To je obzvláště užitečné v případě, ve kterém si výrobce přeje testovat určité znaky přijímače/dekodéru, protože aplikace může být stažena, aniž by musela být vysílána přes satelitní televizní systém.

5 Podle třetího aspektu předkládaného vynálezu je vytvořen MPEG vysílací systém, který zahrnuje: prostředek pro rozdělení aplikace určené ke stažení do MPEG přijímače/dekodéru na množství modulů; prostředek pro formátování každého z modulů jako odpovídající MPEG tabulky, 10 přičemž tyto tabulky mají stejnou TID a příslušná odlišná TID-rozšíření, jiná než je předem stanovené TID-rozšíření; prostředek pro vytváření adresářové MPEG tabulky pro moduly, která má stejnou uvedenou TID a uvedené předem stanovené TID-rozšíření, přičemž adresář obsahuje pro každý z modulů 15 jméno tohoto modulu a příslušné TID-rozšíření; a prostředek pro cyklické vysílání adresářové MPEG tabulky a modulových MPEG tabulek v MPEG bitovém toku.

Výhodně systém dále zahrnuje prostředek pro vytváření identifikace verze pro adresářovou MPEG tabulku; přičemž 20 prostředek pro vytváření adresářové MPEG tabulky je uspořádán pro začlenění do adresářové MPEG tabulky vytvořené identifikace verze pro tuto tabulku.

Prostředek pro formátování modulů může být uspořádán 25 pro formátování alespoň jedné z modulových MPEG tabulek jako množství MPEG úseků, z nichž každý v jeho předem stanovené části obsahuje identifikaci tohoto MPEG úseku v této MPEG tabulce a indikaci počtu MPEG úseků v této MPEG tabulce.

Výhodně by přijímač/dekodér měl být chráněn proti 30 stahování neautorizovaných aplikací, které by mohly

obsahovat, například, viry. Podle toho lze tedy předpokládat určité koncepty kódování a označování (podepisování) alespoň části aplikačního kódu.

Podle čtvrtého aspektu předkládaného vynálezu je
5 navržen způsob zavádění dat do MPEG přijímače/dekodéru, který zahrnuje kroky: vytváření podpisu pro data určená ke stažení; kódování podpisu s použitím privátního klíče; formátování dat určených ke stažení, kódovaného podpisu a identifikace pro
10 privátní klíč jako MPEG tabulky; vysílání MPEG tabulky; a v přijímači/dekodéru:- přijímání MPEG tabulky; zvolení jednoho z množství veřejných klíčů podle identifikace klíče v přijaté MPEG tabulce; dekódování kódovaného podpisu v přijaté MPEG tabulce s použitím zvoleného veřejného klíče pro vytvoření dekódovaného podpisu; vytváření podpisu pro data v přijaté
15 MPEG tabulce; a porovnání dekódovaného podpisu a podpisu vytvořeného v přijímači/dekodéru pro přijatá data.

Podle toho tedy může být přijímač/dekodér použit pro
20 stahování aplikací majících kódované podpisy z více než jednoho zdroje, aniž by tyto zdroje musely znát všechny ostatní privátní klíče.

Tento způsob podle vynálezu může dále zahrnovat
25 kroky: stahování do přijímače/dekodéru aplikace mající podpis kódovaný s použitím privátního klíče majícího předem stanovenou identifikaci klíče; spuštění aplikace v přijímači/dekodéru pro řízení přijímače/dekodéru pro přijetí dalšího klíče; uložení tohoto dalšího klíče v oblasti energeticky závislé paměti přijímače/dekodéru. V tomto případě může být v průběhu kroku spuštění aplikace další klíč
30 předáván lokálně do přijímače/dekodéru, například přes paralelní port, sériový port nebo čtecí zařízení

inteligentních karet přijímače/dekodéru. Pokud přijímač/dekodér má modemové připojení, je tento přijímač/dekodér výhodně uspořádán pro zabránění tomu, aby nějaký takový další klíč byl předáván přes modem.

5 Tyto znaky umožňují výrobci, který může potřebovat otestovat přijímač/dekodér, stahovat klíč do přijímače/dekodéru.

10 Způsob podle vynálezu může dále zahrnovat kroky: v přijímači/dekodéru: vyhledávání v chráněné oblasti paměti přijímače/dekodéru příznaku platnosti pro zvolený veřejný klíč; a zamezení nebo přerušení stahování dat, pokud vyhledaný příznak platnosti není nastaven.

15 Podle toho tedy, přestože v paměti přijímače/dekodéru může být permanentně zajištěno množství veřejných klíčů, může být kterýkoliv z nich selektivně zablokován, což může být potřebné v tom případě, například, kdy bylo narušeno soukromí privátního klíče sdruženého s nějakým určitým veřejným klíčem, nebo kdy se dva operátoři, kteří používali stejné
20 klíče, rozhodnou, že si přejí používat samostatné klíče.

V případě, ve kterém je přijímač/dekodér uspořádán pro stahování aplikace mající podpis kódovaný s použitím privátního klíče majícího předem stanovenou identifikaci klíče, jak bylo uvedeno výše, může mít v chráněné oblasti
25 paměti přijímače/dekodéru privátní klíč mající předem stanovenou identifikaci klíče příznak platnosti, který může být měněn prostřednictvím uvedené aplikace, přičemž schopnost přijímat další klíč je určena v závislosti na stavu tohoto příznaku platnosti.

Tyto posledně uvedené znaky příznaků platnosti pro veřejné klíče mohou být zajištěny nezávisle na čtvrtém aspektu předkládaného vynálezu. Podle toho tedy je podle pátého aspektu předkládaného vynálezu navržen způsob zavádění dat do MPEG přijímače/dekodéru, který zahrnuje kroky:

5 vytváření podpisu pro data určená ke stažení; kódování podpisu s použitím privátního klíče; formátování dat určených ke stažení, kódovaného podpisu a identifikace pro privátní klíč jako MPEG tabulky; vysílání MPEG tabulky; a v

10 přijímači/dekodéru:- přijímání MPEG tabulky; vyhledávání v chráněné oblasti paměti přijímače/dekodéru příznaku platnosti pro veřejný klíč odpovídající privátnímu klíči identifikovanému v přijaté MPEG tabulce; a pokud je vyhledaný příznak platnosti nastaven:- dekódování kódovaného podpisu v

15 přijaté MPEG tabulce s použitím veřejného klíče odpovídajícího privátnímu klíči identifikovanému v přijaté MPEG tabulce pro vytvoření dekódovaného podpisu; vytváření podpisu pro data v přijaté MPEG tabulce; a porovnání dekódovaného podpisu a podpisu vytvořeného v

20 přijímači/dekodéru pro přijatá data.

Způsoby podle čtvrtého a pátého aspektu předkládaného vynálezu výhodně dále zahrnují kroky:- vytvoření ověřovacího kódu pro data určená ke stažení, přičemž tento ověřovací kód je kódován s podpisem v kódovacím kroku a je dekódován s

25 podpisem v dekódovacím kroku; vyhledání uloženého ověřovacího kódu v chráněné oblasti paměti přijímače/dekodéru; a porovnání vyhledaného ověřovacího kódu a dekódovaného ověřovacího kódu.

Podle tohoto přijímač/dekodér může být nastaven pro

30 přijímání pouze určitých aplikací nebo typů aplikací.

Tyto znaky mohou být zajištěny nezávisle na čtvrtém a pátém aspektu předkládaného vynálezu. Podle toho tedy je podle šestého aspektu předkládaného vynálezu navržen způsob zavádění dat do MPEG přijímače/dekodéru, který zahrnuje

5 kroky:- vytváření ověřovacího kódu pro data určená ke stažení; vytváření podpisu pro data určená ke stažení, nebo jejich části; kódování ověřovacího kódu a podpisu s použitím privátního klíče; formátování dat určených ke stažení a kódovaného ověřovací kódu a podpisu jako alespoň jedné MPEG

10 tabulky; vysílání uvedené jedné nebo každé MPEG tabulky; a v přijímači/dekodéru:- přijímání uvedené jedné nebo každé MPEG tabulky; dekódování kódovaného ověřovacího kódu a podpisu v přijatých MPEG tabulkách s použitím veřejného klíče odpovídajícího privátnímu klíči; vyhledání uloženého

15 ověřovacího kódu v chráněné oblasti paměti přijímače/dekodéru; porovnání vyhledaného ověřovacího kódu a dekódovaného ověřovacího kódu; vytváření podpisu pro data v přijatých MPEG tabulkách, nebo jejich část; a porovnání dekódovaného podpisu s podpisem vytvořeným v

20 přijímači/dekodéru pro přijatá data.

Výhodně způsob podle vynálezu dále zahrnuje krok zamezení nebo přerušení stahování dat, pokud si v kroku porovnávání ověřovacích kódů vyhledaný ověřovací kód a dekódovaný ověřovací kód vzájemně neodpovídají.

25 Ve čtvrtém až šestém aspektu předkládaného vynálezu může být zajištěno, že podpis dat určených ke stažení je kódován v bloku dat, včetně dalších dat, se zvoleným posunutím mezi začátkem datového bloku a začátkem podpisu, a kódovaný datový blok je dekódován v kroku dekódování v

30 přijímači/dekodéru, přičemž způsob podle vynálezu dále

zahrnuje kroky v přijímači/dekodéru:- vyhledávání alespoň jednoho uloženého posunutí v chráněné oblasti paměti přijímače/dekodéru; a vyjmutí podpisu z dekódovaného datového bloku s použitím uvedeného jednoho vyhledaného posunutí od začátku dekódovaného datového bloku.

Podle toho tedy podpis může být skrytý mezi dalšími fiktivními daty, čímž je dosaženo toho, že je mnohem obtížnější nalézt umístění podpisu. Alternativně, nebo přídavně, tento znak umožňuje, aby data byla vytvořena jako přístupná pouze pro jednu nebo více určitých skupin přijímačů/dekodérů.

Tyto znaky mohou být zajištěny nezávisle na čtvrtém až šestém aspektu předkládaného vynálezu. Podle toho je tedy podle sedmého aspektu předkládaného vynálezu navržen způsob zavádění dat do MPEG přijímače/dekodéru, který zahrnuje kroky:- vytváření podpisu pro data určená ke stažení; začlenění podpisu a dalších dat do bloku dat se zvoleným posunutím mezi začátkem datového bloku a začátkem podpisu; kódování datového bloku s použitím privátního klíče; formátování dat určených ke stažení a kódovaného datového bloku jako MPEG tabulky; vysílání této MPEG tabulky; a v přijímači/dekodéru:- přijímání MPEG tabulky; dekódování kódovaného datového bloku v přijaté MPEG tabulce s použitím veřejného klíče odpovídajícího privátnímu klíči; vyhledání alespoň jednoho uloženého posunutí v chráněné oblasti paměti přijímače/dekodéru; vyjmutí podpisu z dekódovaného datového bloku s použitím uvedeného jednoho vyhledaného posunutí od začátku dekódovaného datového bloku; vytváření podpisu pro data v přijaté MPEG tabulce; a porovnání podpisu vyjmutého z

dekódovaného datového bloku s podpisem vytvořeným v přijímači/dekodéru pro přijatá data.

5 V případě, ve kterém uvedená chráněná oblast paměti má alespoň dvě takováto uložená posunutí, pak, pokud v kroku porovnání si vyjmutý podpis a vytvořený podpis vzájemně neodpovídají, zahrnuje způsob výhodně kroky opakování kroků vyhledání, vyjmutí a porovnání s použitím dalšího z uložených posunutí.

10 Alespoň nějaká z uvedených dalších dat v bloku dat mohou být fiktivní nebo libovolná data, ale pokud je tomu tak, pak výhodně žádný úsek těchto fiktivních dat neopakuje podpis.

15 Ve čtvrtém až sedmém aspektu předkládaného vynálezu mohou být data stahována jako množství modulů dat, přičemž způsob podle předkládaného vynálezu může zahrnovat kroky:- vytváření modulového podpisu pro každý modul dat, určený ke stažení; formátování modulů dat jako příslušných modulových MPEG tabulek; vytváření adresáře včetně identifikace každé
20 modulové MPEG tabulky a příslušného podpisu, přičemž tento adresář je subjektem kroku vytváření podpisu; a v přijímači/dekodéru:- vytváření příslušného modulového podpisu pro každý z modulů v přijatých modulových MPEG tabulkách; a porovnání každého modulového podpisu v přijaté adresářové
25 MPEG tabulce s příslušným modulovým podpisem vytvořeným v přijímači/dekodéru.

Podle toho tedy, přestože data určená ke stažení jsou sestavena z množství modulů, je vyžadován pouze jeden kódovací proces za účelem kódování modulů, a je požadován

pouze jeden dekódovací proces za účelem umožnění ověření podpisů.

Tyto znaky mohou být zajištěny nezávisle na čtvrtém až sedmém aspektu předkládaného vynálezu. Podle toho tedy
5 podle osmého aspektu předkládaného vynálezu je navržen způsob zavádění množství modulů dat do MPEG přijímače/dekodéru, který zahrnuje kroky:- vytváření modulového podpisu pro každý modul dat určených ke stažení; formátování modulů dat jako
10 příslušných modulových MPEG tabulek; vytváření adresáře včetně identifikace každé modulové MPEG tabulky a příslušného podpisu; vytváření adresářového podpisu pro adresář; kódování adresářového podpisu s použitím privátního klíče; formátování adresáře a kódovaného adresářového podpisu jako adresářové
15 MPEG tabulky; vysílání adresářové a modulových MPEG tabulek; a v přijímači/dekodéru:- přijímání adresářové a modulových MPEG tabulek; dekódování kódovaného adresářového podpisu v přijaté adresářové MPEG tabulce s použitím veřejného klíče odpovídajícího privátnímu klíči; vytvoření adresářového podpisu pro adresář v přijaté adresářové MPEG tabulce;
20 porovnání dekódovaného adresářového podpisu a adresářového podpisu vytvořeného v přijímači/dekodéru; vytvoření příslušného modulového podpisu pro každý z modulů v přijatých modulových MPEG tabulkách; a porovnání každého modulového podpisu v přijaté adresářové MPEG tabulce s příslušným
25 modulovým podpisem vytvořeným v přijímači/dekodéru.

Způsob podle vynálezu výhodně dále zahrnuje krok zabránění nebo přerušení stahování takového modulu dat, pokud
30 v kroku porovnání modulových podpisů si modulový podpis v přijaté adresářové MPEG tabulce a příslušný modulový podpis

vytvořený v přijímači dekodéru pro tento modul vzájemně neodpovídají.

5 Způsoby popisované výše výhodně rovněž zahrnují krok zabránění nebo přerušení stahování dat, pokud si v kroku (krocích) porovnání jeden nebo každý dekódovaný podpis a vytvořený podpis vzájemně neodpovídají.

10 Podle devátého aspektu předkládaného vynálezu je vytvořen MPEG přijímač/dekodér pro použití při realizaci způsobu podle čtvrtého aspektu předkládaného vynálezu, který zahrnuje: prostředek pro přijímání MPEG tabulek; prostředek pro ukládání množství veřejných klíčů a identifikace pro každý z veřejných klíčů; a zpracovatelský prostředek, který je naprogramován pro zvolení jednoho z uložených veřejných klíčů podle identifikace klíče v přijaté MPEG tabulce; pro 15 dekódování kódovaného podpisu v přijaté MPEG tabulce s použitím zvoleného veřejného klíče pro vytvoření dekódovaného podpisu; pro vytvoření podpisu pro data v přijaté MPEG tabulce; a pro porovnání dekódovaného podpisu a podpisu vytvořeného v přijímači/dekodéru pro přijatá data.

20 Paměťový prostředek pro uložení klíčů je výhodně zajištěn prostřednictvím ROM, a identifikace pro každý z veřejných klíčů může být zajištěna prostřednictvím paměťového místa tohoto veřejného klíče v paměťovém prostředku pro uložení klíčů.

25 Přijímač/dekodér může dále zahrnovat oblast energeticky závislé paměti, přičemž zpracovatelský prostředek může být uspořádán pro stahování aplikace mající podpis kódovaný s použitím privátního klíče majícího předem stanovenou identifikaci klíče, pro spuštění této aplikace pro 30

řízení přijímače/dekodéru pro přijetí dalšího klíče, a pro řízení uložení tohoto dalšího klíče do oblasti energeticky závislé paměti.

5 Přijímač/dekodér může dále zahrnovat prostředek pro přijetí takového dalšího klíče, který je předáván lokálně do přijímače/dekodéru, jako je paralelní port, sériový port a/nebo čtecí zařízení pro čtení inteligentních karet v přijímači/dekodéru. Energeticky závislá paměť je výhodně
10 zajištěna prostřednictvím RAM. Opět, pokud přijímač/dekodér má modemové spojení, je tento přijímač/dekodér výhodně uspořádán pro zabránění předání takového dalšího klíče přes modem.

15 Přijímač/dekodér může dále zahrnovat chráněnou oblast paměti pro uložení příznaku platnosti pro každý z alespoň nějakých veřejných klíčů, přičemž zpracovatelský prostředek může být naprogramován pro vyhledání v této chráněné oblasti paměti příznaku platnosti pro zvolený veřejný klíč, a pro zabránění nebo přerušení stahování dat, pokud tento vyhledaný
20 příznak platnosti není nastaven.

25 Přijímač/dekodér může rovněž dále zahrnovat chráněnou oblast paměti pro uložení příznaku platnosti pro privátní klíč mající předem stanovenou identifikaci klíče, přičemž zpracovatelský prostředek může být uspořádán při spuštění uvedené aplikace pro změnu tohoto příznaku platnosti a je uspořádán pro umožnění takového uložení dalšího klíče v závislosti na stavu tohoto příznaku platnosti.

30 Tento posledně uvedený znak může být zajištěn nezávisle na devátém aspektu předkládaného vynálezu. Podle toho tedy je podle desátého aspektu předkládaného vynálezu

vytvořen MPEG přijímač/dekodér, který zahrnuje: prostředek
pro přijímání MPEG tabulek; prostředek pro ukládání veřejného
klíče a identifikace pro tento veřejný klíč; a chráněnou
oblast paměti pro uložení příznaku platnosti pro veřejný
5 klíč; a zpracovatelský prostředek, který je naprogramován pro
vyhledání v této chráněné oblasti paměti přijímače/dekodéru
příznaku platnosti pro veřejný klíč odpovídající privátnímu
klíči identifikovanému v přijaté MPEG tabulce; a, pokud je
vyhledaný příznak platnosti nastaven, pro dekódování
10 kódovaného podpisu v přijaté MPEG tabulce s použitím
veřejného klíče odpovídajícího privátnímu klíči
identifikovanému v přijaté MPEG tabulce pro vytvoření
dekódovaného podpisu; pro vytvoření podpisu pro data v
přijaté MPEG tabulce; a pro porovnání dekódovaného podpisu a
15 podpisu vytvořeného v přijímači/dekodéru pro přijatá data.

Paměť pro uložení příznaku (příznaků) platnosti pro
klíče je výhodně zajištěna prostřednictvím přepisovatelné
paměti nezávislé na zdroji energie.

20 V případě, ve kterém je uloženo množství takových
veřejných klíčů, je paměť pro uložení příznaku (příznaků)
platnosti výhodně uspořádána jako bitová mapa.

Přijímač/dekodér podle devátého nebo desátého aspektu
předkládaného vynálezu může dále zahrnovat chráněnou oblast
25 paměti pro uložení ověřovacího kódu, přičemž zpracovatelský
prostředek může být naprogramován pro dekódování ověřovacího
kódu v přijaté MPEG tabulce, pro vyhledání uloženého
ověřovacího kódu, a pro porovnání vyhledaného ověřovacího
kódu a dekódovaného ověřovacího kódu.

Tento posledně uvedený znak může být zajištěn nezávisle na devátém nebo desátém aspektu předkládaného vynálezu. Podle toho tedy je podle jedenáctého aspektu předkládaného vynálezu vytvořen MPEG přijímač/dekodér, který zahrnuje: prostředek pro přijímání MPEG tabulek; prostředek pro ukládání veřejného klíče a identifikace pro tento veřejný klíč; chráněnou oblast paměti pro uložení ověřovacího kódu; a zpracovatelský prostředek, který je naprogramován pro dekódování kódovaného ověřovacího kódu a podpisu v přijatých MPEG tabulkách s použitím uloženého veřejného klíče odpovídajícího privátnímu klíči; pro vyhledání uloženého ověřovacího kódu v chráněné oblasti paměti; pro porovnání vyhledaného ověřovacího kódu a dekódovaného ověřovacího kódu; pro vytvoření podpisu pro data v přijaté MPEG tabulce nebo jejich část; a pro porovnání dekódovaného podpisu a podpisem vytvořeným v přijímači/dekodéru pro přijatá data.

Zpracovatelský prostředek je výhodně naprogramován pro zabránění nebo přerušení stahování dat, pokud si vyhledaný ověřovací kód a dekódovaný ověřovací kód vzájemně neodpovídají.

Paměť pro uložení ověřovacích kódů je výhodně zajištěna prostřednictvím prepisovatelné paměti nezávislé na zdroji energie, přičemž tato paměť a může být uspořádána jako bitová mapa.

Přijímač/dekodér podle devátého až jedenáctého aspektu předkládaného vynálezu může dále zahrnovat chráněnou oblast paměti pro uložení alespoň jednoho posunutí, přičemž zpracovatelský prostředek může být naprogramován pro dekódování kódovaného datového bloku v přijaté MPEG tabulce, pro vyhledání uvedeného jednoho uloženého posunutí v chráněné

oblasti paměti, a pro vyjmutí podpisu z dekódovaného datového bloku s použitím vyhledaného posunutí od začátku dekódovaného datového bloku.

5 Tento posledně uvedený znak může být zajištěn
nezávisle na devátém až jedenáctém aspektu předkládaného
vynálezu. Podle toho tedy je podle dvanáctého aspektu
předkládaného vynálezu vytvořen MPEG přijímač/dekodér, který
zahrnuje: prostředek pro přijímání MPEG tabulek; prostředek
10 pro uložení veřejného klíče a identifikace pro tento veřejný
klíč; chráněnou oblast paměti pro uložení alespoň jednoho
posunutí; a zpracovatelský prostředek, který je naprogramován
pro dekódování kódovaného datového bloku v přijaté MPEG
tabulce s použitím uloženého veřejného klíče odpovídajícího
privátnímu klíči; pro vyhledání uvedeného jednoho uloženého
15 posunutí v chráněné oblasti paměti; pro vyjmutí podpisu z
dekódovaného datového bloku s použitím vyhledaného posunutí
od začátku dekódovaného datového bloku; pro vytvoření podpisu
pro data v přijaté MPEG tabulce; a pro porovnání podpisu
vyjmutého z dekódovaného datového bloku s podpisem vytvořeným
20 v přijímači/dekodéru pro přijatá data.

Paměť pro uložení posunutí je výhodně zajištěna
prostřednictvím přepisovatelné paměti nezávislé na zdroji
energie.

25 V přijímači/dekodéru podle devátého až dvanáctého
aspektu předkládaného vynálezu může být zpracovatelský
prostředek naprogramován pro vytvoření příslušného modulového
podpisu pro každý z modulů v přijatých MPEG tabulkách, a pro
porovnání každého modulového podpisu v přijaté adresářové
30 MPEG tabulce s příslušným modulovým podpisem vytvořeným v
přijímači/dekodéru.

Tento posledně uvedený znak vynálezu může být zajištěn nezávisle na devátém až dvanáctém aspektu předkládaného vynálezu. Podle toho tedy je podle třináctého aspektu předkládaného vynálezu vytvořen MPEG

5 přijímač/dekodér, který zahrnuje: prostředek pro přijímání adresářové a modulových MPEG tabulek; prostředek pro uložení veřejného klíče a identifikace pro tento veřejný klíč; a zpracovatelský prostředek, který je naprogramován pro dekódování kódovaného adresářového podpisu v přijaté
10 adresářové MPEG tabulce s použitím uloženého veřejného klíče odpovídajícího privátnímu klíči; pro vytvoření adresářového podpisu pro adresář v přijaté adresářové MPEG tabulce; pro porovnání dekódovaného adresářového podpisu a adresářového podpisu vytvořeného v přijímači/dekodéru; pro vytvoření
15 příslušného modulového podpisu pro každý z modulů v přijatých modulových MPEG tabulkách; a pro porovnání každého modulového podpisu v přijaté adresářové tabulce s příslušným modulovým podpisem vytvořeným v přijímači/dekodéru.

20 Zpracovatelský prostředek je výhodně naprogramován pro zabránění nebo přerušení stahování modulu dat, pokud si modulový podpis v přijaté adresářové MPEG tabulce a příslušný modulový podpis vytvořený v přijímači/dekodéru pro tento modul vzájemně neodpovídají.

25 V přijímači/dekodéru podle kteréhokoliv z devátého až třináctého aspektu podle vynálezu je zpracovatelský prostředek výhodně naprogramován pro zabránění nebo přerušení stahování dat, pokud si jeden nebo každý dekódovaný podpis a vytvořený podpis vzájemně neodpovídají.

V následujícím popisu budou popsány výhodné znaky předkládaného vynálezu čistě prostřednictvím příkladů ve spojení s odkazy na připojené výkresy.

Přehled obrázků na výkresech

- 5
- Obr.1 znázorňuje celkovou architekturu digitálního televizního systému;
- 10
- Obr.2 znázorňuje architekturu interaktivního systému digitálního televizního systému podle obr. 1;
- Obr.3 je schematické znázornění rozhraní přijímače/dekodéru, který tvoří část systému podle obr. 1 a obr. 2;
- 15
- Obr.4 je schematické znázornění dálkového ovladače použitého v digitálním televizním systému;
- Obr.5 znázorňuje uspořádání souborů uvnitř modulu staženého do paměti interaktivního přijímače/dekodéru;
- 20
- Obr.6 ilustruje vzájemný vztah mezi množstvím komponentů MPEG datového toku;
- Obr.7 ilustruje, jak může být aplikace sestavena z modulů/tabulek, které dále mohou být sestaveny z úseků;
- 25
- Obr.8 ilustruje obsah adresářového modulu;
- Obr.9 ilustruje ve větším detailu část obsahu adresářového modulu; a
- 30
- Obr.10 ilustruje různé oblasti paměti v přijímači/dekodéru televizního systému.



Příklady provedení vynálezu

Celkový přehled digitálního televizního systému 1000 podle předkládaného vynálezu je znázorněn na obr. 1. Vynález 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 pronajímaného koncovým uživatelem a spojeného s televizním zařízením 2022 koncového uživatele. Přijímač/dekodér 2020 dekóduje komprimovaný MPEG-2 signál na televizní signál pro televizní zařízení 2022.

Systém 3000 podmíněného přístupu je spojen s multiplexorem 2004 a přijímačem/dekodérem 2020 a je umístěn částečně ve vysílacím centru a částečně v dekodéru. Tento systém umožňuje koncovému uživateli přístup k digitálním

televizním vysíláním (přenosům) od jednoho nebo více
dodavatelů (poskytovatelů) vysílání. Inteligentní karta,
schopná dekódování zpráv týkajících se komerčních nabídek (to
jest jeden nebo několik televizních programů, které jsou
5 prodávány dodavatelem vysílání), může být vložena do
přijímače/dekodéru 2020. S použitím dekodéru 2020 a
inteligentní karty může koncový uživatel nakupovat komerční
nabídky buď v módu předplacení nebo v módu platby za
shlédnutí.

10 S multiplexorem 2004 a přijímačem/dekodérem 2020 je
rovněž spojen interaktivní systém 4000, který je opět umístěn
částečně ve vysílacím centru a částečně v dekodéru a který
umožňuje koncovému uživateli interagovat s různými aplikacemi
přes modemový zpětný kanál 4002.

15 Obr. 2 znázorňuje obecnou architekturu interaktivního
televizního systému 4000 digitálního televizního systému 1000
podle předkládaného vynálezu.

20 Například tento interaktivní systém 4000 umožňuje
koncovým uživatelům nakupovat položky z katalogů zobrazených
na obrazovce (on-screen), konzultovat místní zprávy a
meteorologické mapy na požádání a hrát hry prostřednictvím
jejich televizních zařízení.

25 V přehledu zahrnuje interaktivní systém 4000 čtyři
hlavní prvky:-

- tvůrčí nástroj 4004 ve vysílacím centru nebo kdekoli
jinde pro umožnění poskytovateli vysílání vytvářet,
vyvíjet, ladit a testovat aplikace;
- aplikační a datový obslužný kanál 4006 ve vysílacím
30 centru, spojený s tvůrčím nástrojem 4004 pro umožnění

poskytovateli vysílání připravovat, ověřovat a
formátovat aplikace a data pro dodání do multiplexoru a
kodéru 2004 pro začlenění do MPEG-2 transportního
datového toku (obvykle jeho privátní části), aby byla
vysílána ke koncovému uživateli;

- virtuální počítač včetně prováděcího prostředku (RTE)
4008, který je v proveditelném kódu nainstalován v
přijímači/dekodéru 2020 vlastněném nebo pronajatém
koncovým uživatelem pro umožnění koncovému uživateli
přijímat, ověřovat, dekomprimovat a stahovat (zavádět)
aplikace do pracovní paměti dekodéru 2020 pro vykonání.
Tento prováděcí prostředek 4008 rovněž realizuje
rezidentní aplikace obecného účelu. Prováděcí
prostředek 4008 je nezávislý na hardwaru a operačním
systému;
- modemový zpětný kanál 4002 mezi přijímačem/dekodérem
2020 a aplikačním a datovým obslužným kanálem 4006 pro
umožnění signálům instruujícím tento aplikační a datový
obslužný kanál 4006 zavádět data a aplikace do MPEG-2
transportního datového toku na žádost koncového
uživatele.

Interaktivní televizní systém pracuje s použitím
"aplikací", které řídí funkce přijímače/dekodéru a různých
zařízení v něm obsažených. Aplikace jsou reprezentovány v
prováděcím prostředku 4008 jako "zdrojové soubory". "Modul"
je sestava zdrojových souborů a dat. "Objem paměti"
přijímač/dekodéru je paměťový prostor pro moduly. Moduly
mohou být stahovány do přijímače/dekodéru 2020 z MPEG-2
transportního datového toku.



Fyzická rozhraní (propojení) přijímače/dekodéru 2020 jsou použita pro stahování dat. Ve spojení s odkazy na obr. 3 je patrné, že dekodér 2020 obsahuje, například, šest zaváděcích (stahovacích) zařízení; ladič 4028 MPEG toku, sériové rozhraní 4030, paralelní rozhraní 4032, modem 4034 a dvě zařízení 4036 pro čtení inteligentních karet.

Pro účely tohoto popisu je aplikace úsek strojového kódu pro řízení vysokoúrovňových funkcí výhodně přijímače/dekodéru 2020. Například, když koncový uživatel namíří ohnisko dálkového ovladače 2026 (jak je detailněji znázorněno na obr. 4) na tlačítkový objekt viděný na obrazovce televizního zařízení 2022 a stlačí potvrzovací klávesu, spustí se sekvence instrukcí, sdružená s tímto tlačítkem.

Interaktivní aplikace nabízí menu a vykonává příkazy na žádost koncového uživatele a poskytuje data týkající se účelu této aplikace. Aplikace mohou být buď rezidentními aplikacemi, to znamená, že jsou uloženy v ROM (nebo FLASH nebo jiné energeticky nezávislé paměti) přijímače/dekodéru 2020, nebo mohou být vysílány a stahovány do RAM (nebo FLASH) tohoto dekodéru 2020.

Příklady aplikací jsou:-

- Inicializační aplikace. Přijímač/dekodér 2020 je vybaven rezidentní inicializační aplikací, která je adaptabilním souhrnem modulů (tento termín je podrobněji definován níže), umožňujícím přijímači/dekodéru 2020 okamžitě pracovat v prostředí MPEG-2. Tato aplikace zajišťuje základní znaky, které mohou být modifikovány poskytovatelem vysílání, pokud je to



žádoucí. Tato aplikace rovněž zajišťuje rozhraní mezi rezidentními aplikacemi a stahovanými aplikacemi.

- Spouštěcí aplikace. Spouštěcí aplikace umožňuje jakékoliv aplikaci, ať již stahované nebo rezidentní, pracovat v přijímači/dekodéru 2020. Tato aplikace působí jako samozaváděcí program vykonaný při vstupu do služby za účelem spuštění aplikace. Spouštěcí aplikace je stažena do RAM a tudíž může být snadno aktualizována. Může být uspořádána tak, že interaktivní aplikace dostupné na každém kanálu mohou být zvoleny a spuštěny buď bezprostředně po stažení nebo po stažení předem. V případě stažení předem je aplikace stažena do paměti 2024 a je aktivována spouštěcí aplikací na požádání.
- Programový průvodce. Programový průvodce je interaktivní aplikace, která poskytuje ucelenou informaci o programech. Například může poskytovat informaci, řekněme, o televizních programech na jeden týden, které budou uváděny na každém kanálu souboru digitální televize. Stlačením klávesy na dálkovém ovladači 2026, koncový uživatel vstoupí do přídatné obrazovky, překrývající událost (relaci) znázorněnou na obrazovce televizního zařízení 2022. Tato přidaná obrazovka je vyhledávač (browser) poskytující informaci o současných a následujících událostech (relacích) na každém kanálu souboru digitální televize. Stlačením další klávesy na dálkovém ovladači 2026 koncový uživatel vstoupí do další aplikace, která zobrazí seznam informací o událostech během jednoho týdne. Koncový uživatel může rovněž vyhledávat a třídit

události podle jednoduchých a přizpůsobených kritérií. Koncový uživatel může rovněž vstoupit přímo do zvoleného kanálu.

- 5 • Aplikace plateb za zhlédnutí. Aplikace plateb za shlédnutí je interaktivní služba dostupná na každém PPV kanálu souboru digitální televize ve spojení se systémem 3000 podmíněného přístupu. Koncový uživatel může vstoupit do této aplikace s použitím programového průvodce nebo vyhledávače kanálů. Navíc se aplikace 10 spustí automaticky, jakmile je PPV událost zjištěna na PPV kanálu. Koncový uživatel potom může koupit probíhající událost buď prostřednictvím své dceřinné inteligentní karty 3020 nebo přes komunikační obslužný kanál 3022 (s použitím modemu, telefonu a DTMF kódů, 15 systému MINITEL nebo podobně). Tato aplikace může být buď rezidentní v ROM přijímače/dekodéru 2020 nebo stažitelná do RAM přijímače/dekodéru 2020.
- 20 • Aplikace PC stahování. Na žádost může koncový uživatel stahovat počítačový software s použitím této aplikace PC stahování.
- 25 • Aplikace časopisový vyhledávač. Tato aplikace časopisového vyhledávače zahrnuje cyklické video vysílání obrazů s navigací koncového uživatele prostřednictvím tlačítek znázorněných na obrazovce.
- Aplikace kviz. Kviz aplikace je výhodně synchronizována s vysíláním kviz programu. Například jsou na obrazovce televizního zařízení 2022 zobrazeny otázky s několika 30 odpověďmi a koncový uživatel může zvolit odpověď s použitím dálkového ovladače 2026. Aplikace kviz může

informovat uživatele, zda odpověď je správná nebo ne, a může počítat skóre uživatele.

- Aplikace teleshopping. V jednom příkladu tato aplikace teleshopping jsou nabídky zboží na prodej vysílány do přijímače/dekodéru 2020 a zobrazovány na televizním zařízení 2022. S použitím dálkového ovladače 2026 může uživatel zvolit určitou položku, kterou chce koupit. Objednávka této položky je vyslána přes modemový zpětný kanál 4002 do aplikačního a datového obslužného kanálu 4006 nebo do samostatného prodejního systému, jehož telefonní číslo bylo staženo do přijímače/dekodéru 2020, případně s příkazem pro zatížení účtu kreditní karty, která byla vložena do jednoho zařízení 4036 pro čtení inteligentních karet v přijímači/dekodéru 2020.
- Aplikace telebanking. V jednom příkladu této aplikace telebanking uživatel vloží bankovní kartu do jednoho ze zařízení 4036 pro čtení inteligentních karet v přijímači/dekodéru 2020. Přijímač/dekodér 2020 zavolá banku uživatele s použitím telefonního čísla uloženého v bankovní kartě nebo uloženého v přijímači/dekodéru 2020, a potom tato aplikace poskytuje množství možností, které mohou být zvoleny s použitím dálkového ovladače 2026, například stažení přes telefonní linku stavu účtu, převod položek mezi účty, žádost o šekovou knížku a podobně.
- Aplikace internetovský vyhledávač. V jednom příkladu této aplikace internetovského vyhledávače jsou instrukce od uživatele, jako je žádost o sledování webové stránky mající určité URL, zadávány s použitím dálkového ovladače 2026 a tyto instrukce jsou vysílány



prostřednictvím modemového zpětného kanálu 4002 do
aplikačního a datového obslužného kanálu 4006.

Příslušná webová stránka je potom začleněna do vysílání
z vysílacího centra, přijata přijímačem/dekodérem 2020
přes vzestupné spojení 2012, odpovídač 2014 a sestupné
spojení 2016, a je zobrazena na televizním zařízení
2022.

Aplikace jsou uloženy v paměťových místech
přijímači/dekodéru 2020 a jsou reprezentovány jako zdrojové
soubory. Zdrojové soubory zahrnují soubory jednotky popisu
grafických objektů, soubory jednotky proměnných bloků,
soubory instrukčních sekvencí, aplikační soubory a datové
soubory.

Soubory jednotek popisu grafických objektů popisují
obrazovky, rozhraní mezi člověkem a počítačem aplikace.
Soubory jednotek proměnných bloků popisují datové struktury
zpracovávané aplikací. Soubory instrukčních sekvencí popisují
zpracovatelské operace aplikace. Aplikační soubory zajišťují
vstupní body pro aplikace.

Aplikace tvořené tímto způsobem mohou využít datové
soubory, jako jsou knihovní soubory ikon, obrazové soubory,
soubory znakových fontů, soubory tabulek barev a ASCII
textové soubory. Interaktivní aplikace mohou rovněž získat
přímá (on-line) data provedením vstupů a/nebo výstupů.

Prováděcí prostředek 4008 zavádí do své paměti pouze
ty zdrojové soubory, které potřebuje v daném okamžiku. Tyto
zdrojové soubory jsou čteny ze souborů jednotek popisu
grafických objektů, souborů instrukčních sekvencí a

aplikačních souborů; soubory jednotek proměnných bloků jsou uloženy v paměti následně po vyvolání procedury pro stažení modulů a zde zůstávají zajištěny, dokud není provedeno specifické volání procedury pro vyjmutí modulů.

5 Ve spojení s odkazy na obr. 3 je modul 4010, jako je nákupní modul popisovaný podrobněji níže, sestava zdrojových souborů a dat, která zahrnuje následující:

jeden aplikační soubor 4012;

10 neurčený počet souborů 4014 jednotky popisu grafických objektů;

neurčený počet souborů 4016 jednotky proměnných bloků;

15 neurčený počet souborů 4018 instrukčních sekvencí; a

kde je to vhodné, datové soubory 4020, jako jsou knihovní soubory ikon, obrazové soubory, soubory znakových fontů, soubory tabulek barev a ASCII textové soubory.

20 Ve spojení s odkazy na obr. 5 je modul 4010, jako je nákupní modul popisovaný podrobněji níže, sestava zdrojových souborů a dat, která zahrnuje následující:

jeden aplikační soubor 4012;

25 neurčený počet souborů 4014 jednotky popisu grafických objektů;

neurčený počet souborů 4016 jednotky proměnných bloků;

neurčený počet souborů 4018 instrukčních sekvencí; a

kde je to vhodné, datové soubory 4020, jako jsou knihovní soubory ikon, obrazové soubory, soubory znakových fontů, soubory tabulek barev a ASCII textové soubory.

Koncept modulů společně s konceptem stahování malých částí kódu umožňuje snadný vývoj aplikací. Aplikace mohou být staženy do permanentní FLASH paměti dekodéru 2020 jako rezidentní software, nebo mohou být vysílány, aby byly staženy do RAM dekodéru 2020, pouze když je koncový uživatel potřebuje.

Pro stažení modulu 4010 z nosného signálu je nejprve stažen adresář dostupný na nosném signálu. Tento adresář jednoduše obsahuje seznam jmen modulů 4010, které mohou být staženy z nosného signálu. Jakmile již byl tento adresář stažen, je možné stahovat pro aplikaci jeden nebo více modulů 4010. V případě MPEG toku je adresář transportován v jedné samostatné MPEG tabulce. Navíc je v jedné samostatné tabulce transportován jeden modul 4010. V případě modulů vysílaných do ladiče 4028 MPEG toku je použito dlouhého formátu MPEG-2 s delším záhlavím a CRC kódem. To je rovněž případ pěti dalších rozhraní (sériové rozhraní 4030, paralelní rozhraní 4032, modem 4034 a dvě zařízení 4036 pro čtení inteligentních karet) až na to, že je použito "krátkého" MPEG-2 formátu s kratším záhlavím a bez CRC kódu.

jak je patrné zejména z obr. 6 a jak je známo, zahrnuje MPEG-2 bitový tok tabulku 10 přístupu do programů ("PAT"), která má identifikaci paketu ("PID") na hodnotě 0. PAT 10 obsahuje odkazy na PID tabulek 12 mapování programů ("PMT") množství programů. Každá PMT 12 obsahuje odkazy na PID toků audio MPEG tabulek 14 a video MPEG tabulek 16 pro tento program. Paket mající PID nula, to jest tabulka 10

5

10

15

25

30

ostatních modulů/tabulek 24 mají nenulová TID-rozšíření 34.
Záhlaví 26 rovněž zahrnuje číslo 48 verze pro adresářovou
tabulku 40. Adresářová část 42 zahrnuje pro každý z dalších
modulů/tabulek 24 tvořících aplikaci 22 jméno 50 tohoto
5 modulu 24, TID-rozšíření 34 pro tento modul 24 a podpis 52
tohoto modulu 24. Adresářová část může rovněž zahrnovat pro
každý z dalších modulů/tabulek 24 délku tohoto modulu 24 a
číslo verze tohoto modulu 24.

Jak je opět patrné z obr. 6, jsou při činnosti
10 systému PAT 10, PMT 12 a aplikační a datové tabulky 18, 20
cyklicky vysílány, přičemž jsou aktualizovány podle potřeby.
Každá aplikace, která je vysílána má příslušnou předem
stanovenou TID 28. Pro stažení aplikace je do
přijímače/dekodéru 2020 stažena MPEG tabulka mající
15 odpovídající TID a TID-rozšíření s hodnotou nula. To je tedy
adresářová tabulka 40 pro požadovanou aplikaci. Data v
adresáři jsou potom zpracována přijímačem/dekodérem 2020 pro
určení TID-rozšíření 34 modulových tabulek tvořících tuto
požadovanou aplikaci, a potom může být stažena jakákoliv
20 požadovaná modulová tabulka mající stejnou TID jako
adresářová tabulka a TID-rozšíření určené z adresáře.

Přijímač/dekodér 2020 je uspořádán pro ověření
adresářové tabulky pro její jakoukoliv aktualizaci. To může
být provedeno prostřednictvím stahování adresářové tabulky
25 periodicky vždy znovu, například každých 30 sekund, nebo
jednu či pět minut, a porovnáváním čísla verze čerstvě
stažené adresářové tabulky s číslem verze předtím stažené
adresářové tabulky. Pokud čerstvě stažené číslo verze je
pozdější, pak jsou moduly sdružené s předcházející
30 adresářovou tabulkou, nebo jakékoliv takové moduly, pro které

jsou zde starší čísla verzí, demontovány a pozdější moduly jsou staženy a namontovány. V alternativním uspořádání je přicházející bitový tok filtrován s použitím masky odpovídající TID, TID-rozšíření a číslu verze, s hodnotami nastavenými na TID aplikace, TID-rozšíření nula a číslo verze o jednu větší, než je číslo verze právě staženého adresáře. Podle toho tedy může být detekován přírůstek v číslu verze, a jakmile je detekován, je adresář stažen a aplikace je aktualizována, jak je popisováno výše. Další popis takového filtrování je popsán v souběžné patentové přihlášce (číslo zástupce: 73151/PT). Pokud aplikace má být ukončena, je vysílán prázdný adresář s příštím číslem verze, ale bez jakýchkoliv modulů uvedených v tomto adresáři. V odezvě na přijetí takového prázdného adresáře je přijímač/dekodér 2020 naprogramován pro demontáž aplikace.

Použití podpisů a kódování pro aplikační tabulky bude nyní popsáno poněkud podrobněji.

Jak je popisováno výše, zahrnuje vstup pro každý modul v adresářové tabulce 40 modulový podpis. Modulový podpis je vytvořen s použitím známého procesu vytvářejícího MD5 podpis na datech v odpovídající modulové tabulce.

Navíc adresářová tabulka 40 zahrnuje kódovaný podpis 46, který je vytvářen způsobem, který bude nyní popsán ve spojení s odkazy na obr. 9. Je vytvořen blok 54 o 64 bytech dat. První byte 56 je nula. Následující tři byty 58 mohou zahrnovat fiktivní nebo libovolná data. Následujících osm bytů 60 vytvářejí bitovou mapu pro ověření platnosti aplikace, která bude dále popsána. Poslední čtyři byty 62 jsou rezervovány. Zbývajících 32 bytů obsahuje 16-bytový podpis 64, který začíná v posunutí mezi 0 a 31 bytem po

prvním bytu následujícím po bytech bitové mapy 60 pro ověření platnosti aplikace. Fiktivní data 66 jsou vložena mezi bitovou mapu 60 pro ověření platnosti aplikace a podpis 64 a/nebo mezi podpis 64 a rezervované byty 62. Podpis 64 je
 5 vytvářen s použitím známého procesu pro vytváření MD5 podpisu na adresářové části 42 v adresářové tabulce 40. Blok 54 je potom kódován s použitím známého kódovacího procesu a určitého privátního klíče pro vytvoření bloku 46 kódovaného podpisu a kódované bitové mapy pro věření platnosti aplikace.
 10 Tento datový blok 46 je začleněn do adresářové tabulky 40, a jedno-bytová identifikace privátního klíče, který byl použit pro kódování tohoto bloku, je začleněna do adresářové tabulky jako identifikace 44 klíče.

Pro shrnutí vytváření aplikace a její vysílání
 15 zahrnuje následující kroky:-

- vytvoření aplikace jako množství modulů;
- zaznamenání předem stanovené TID 28 pro aplikaci;
- přidělení jmen a nenulových TID-rozšíření 34 pro moduly;
- 20 • formátování každého modulu jako MPEG tabulky 24 nebo úseků 18 MPEG tabulky;
- vytvoření MD5 podpisu 52 každého modulu;
- vytvoření adresáře 42;
- vytvoření MD5 podpisu 64 pro adresář;
- 25 • zvolení bitu platnosti v bitové mapě 60 pro ověření platnosti aplikace;
- zvolení posunutí;
- vytvoření bloku 54;
- kódování bloku 54 s použitím kódování se zvoleným
 30 privátním klíčem;

- vytvoření adresářové MPEG tabulky 40 s přidělenou PID 28, TID-rozšířením nula, adresářem 42, identifikací 44 privátního klíče a kódovaným podpisem 46;
- vysílání adresářové tabulky 40 a modulových tabulek 24 nebo úseků 18.

V následujícím popisu bude popsána činnost přijímače/dekodéru 2020 při zpracovávání podpisů a při dekódování v průběhu stahování aplikace. Jak je patrné z obr. 10, zahrnuje přijímač/dekodér 2020 paměti EEPROM 68, ROM 70 a RAM 72. EEPROM 68 zahrnuje chráněnou oblast 74, která je používána virtuálním počítačem a kam může zapisovat pouze virtuální počítač (a ne běžná aplikace). Tato chráněná oblast 74 zahrnuje bitovou mapu 76 pro ověření klíče o velikosti 16 nebo 256 bitů, bitovou mapu 78 pro ověření aplikace o velikosti 64 bitů, a bitovou mapu 80 posunutí o velikosti 32 bitů. ROM 70 zahrnuje v jednom provedení šestnáct veřejných klíčů 82, přičemž v tomto případě je použito 16-bitové bitové mapy 76 pro ověření klíče, a v dalším provedení 256 veřejných klíčů 82, přičemž v tomto případě je použité 256-bitové bitové mapy 76 pro ověření klíče. Veřejné klíče 76 jsou identifikovány prostřednictvím jejich fyzických poloh v ROM 70, nebo alternativně mohou být začleněny ve vyhledávací tabulce, přičemž identifikace určitého klíče bude ukazovat na odpovídající veřejný klíč 76. RAM 72 může být použita pro uložení dočasného klíče 84.

Jak bylo zmiňováno výše, když má být stažena aplikace, je nejprve stažena adresářová tabulka mající předem stanovenou TID pro tuto aplikaci a TID-rozšíření nula. Identifikace 44 klíče je potom vyjmuta z adresářové tabulky a je provedeno ověření bitové mapy 76 pro ověření klíče v

chráněné oblasti 74, že bit odpovídající vyjmuté identifikaci 44 klíče je nastaven. Pokud není, pak další stahování aplikace je přerušeno. Pokud je ale příslušný klíč nastaven, pak je z ROM 70 zvolen veřejný klíč 82 odpovídající vyjmuté identifikaci 44 klíče. Zvolený veřejný klíč 82 a známý dekódovací proces jsou potom použity pro dekódování kódovaného bloku 46 v adresářové tabulce 40 pro vytvoření bloku 54. Potom je z dekódovaného bloku 54 vyjmuta bitová mapa 60 pro ověření platnosti aplikace a je s ní proveden logický součin (funkce AND) s bitovou mapou 78 pro ověření platnosti aplikace, která je uložena v chráněné oblasti 74 paměti. Pokud výsledek funkce AND je nula, pak další stahování aplikace je přerušeno. Pokud je ale výsledek funkce AND nenulový, pak je vyhledáno posunutí v bitové mapě 80 posunutí v chráněné oblasti 74 paměti, nebo, pokud je nastaven více než jeden bit posunutí, je vyhledán každý bit posunutí, a z dekódovaného bloku 54 je vyjmuta šestnáct bytů dat začínajíc s vyhledaným posunutím od prvního bytu za bitovou mapou 60 pro ověření platnosti aplikace. Pro uvedené jedno nebo každé vyhledané posunutí, je těchto 16 bytů považováno za podpis vysílaný s adresářovou tabulkou 40. Podpis vstupů v adresářové části 42 adresářové tabulky 40 je vypočítán s použitím známého MD5 procesu a tento vypočítaný podpis je porovnán s podpisem vyjmutým z bloku 54. Pokud si tyto dva podpisy pro uvedené jedno nebo každé vyhledané posunutí nedopovídají, pak je další stahování aplikace přerušeno. Pokud ale jeden z podpisů odpovídá, pak může pokračovat stahování modulů specifikovaných v adresářové části 42. Jak bylo zmiňováno výše, pro stažení určitého modulu je z adresářové části 42 získáno TID-rozšíření pro

5

10

15

20

30

tomto případě tento klíč nevyžaduje bit v bitové mapě 76 pro ověření klíče. Podle toho tedy může být tento bit použit pro jiný účel. Přesněji tedy aplikace, která již byla ověřena s použitím klíče 15, může být uspořádána pro nastavení tohoto určitého bitu na 1, přičemž v tomto případě je přijímač/dekodér 2020 naprogramován pro umožnění stažení dočasného klíče 84 do RAM 72, ale pouze tehdy, když je to prostřednictvím sériového rozhraní 4030, paralelního rozhraní 4032 nebo jednoho ze dvou zařízení 4036 pro čtení inteligentních karet. Toto opatření může být využito, například, výrobcem přijímače/dekodéru 2020, kterým může být zadána aplikace pro použití aktivace stahování dočasného klíče do přijímače/dekodéru 2020, takže tento přijímač/dekodér 2020 může být testován.

Kódovací a podpisové uspořádání popisované výše zajišťuje množství důležitých znaků. Zejména:-

- aplikace může být stažena pouze tehdy, když přijímač/dekodér 2020 má ve své paměti uložen příslušný veřejný klíč odpovídající identifikaci 44 klíče ve stažené adresářové tabulce;
- pro všechny až na jeden z klíčů může být aplikace stažena pouze s použitím určitého klíče, pokud je v paměti přijímače/dekodéru 2020 nastavena bitová mapa 76 pro ověření klíče tak, že umožňuje použití tohoto klíče;
- aplikace může být stažena pouze, když nastavený bit v bitové mapě 80 posunutí, uložené v paměti přijímače/dekodéru 2020, odpovídá posunutí použitému při vytváření adresářové tabulky;

- aplikace může být stažena pouze tehdy, když je bitová mapa 78 pro ověření platnosti aplikace, uložená v paměti přijímače/dekodéru 2020, vhodně nastavena pro umožnění stažení aplikace;
- 5 • aplikace může být stažena pouze tehdy, když adresářová tabulka nebyla poškozena poté, co byl původně vytvořen její podpis;
- • každý modul aplikace může být stažen pouze tehdy, když odpovídající modulová tabulka nebyla poškozena poté, co
- 10 • byl původně vytvořen její podpis;
- • při přípravě aplikace pro stažení je vyžadován pouze jeden kódovací proces bez ohledu na to, že aplikace je sestavena z několika MPEG tabulek, a pro stažení celé aplikace je v přijímači/dekodéru 2020 vyžadován pouze
- 15 • jeden dekódovací proces;
- • může být použito vícenásobných klíčů, takže různí poskytovatelé služeb mohou mít různé privátní klíče;
- • může být použit dočasný klíč, například výrobcem, pro testovací účely.

20 Mělo by být zcela zřejmé, že předkládaný vynález byl popsán výše čistě prostřednictvím příkladu, a že v rozsahu tohoto vynálezu mohou být provedeny modifikace jednotlivých detailů.

• 25 Každý znak popisovaný v popisu a (kde je to vhodné) v nárocích a na výkresech může být vytvořen nezávisle nebo v jakékoli vhodné kombinaci.

30 Ve shora zmiňovaných výhodných provedeních byly určité znaky předkládaného vynálezu realizovány s použitím počítačového softwaru. Ovšem osobám v oboru znalým je přirozeně zcela zřejmé, že jakýkoliv z těchto znaků může být

realizován s použitím hardwaru. Navíc by mělo být zcela zřejmé, že funkce prováděné hardwarem, počítačovým softwarem a podobně jsou prováděny na nebo s použitím elektrických a podobných signálů.

5 Na tomto místě je učiněn odkaz na souběžné patentové přihlášky stejného přihlašovatele, které mají stejné datum podání a následující názvy: vytváření a vysílání signálů (značka zástupce: 73142/PT), Inteligentní karta pro použití s přijímačem kódovaných vysílaných signálů a přijímač (značka
10 zástupce: 73143/PT), Vysílací a přijímací systém a systém s podmíněným přístupem (značka zástupce: 73145/PT), Stahování počítačového souboru z vysílače přes přijímač/dekodér do počítače (značka zástupce: 73146/PT), Vysílání a příjem televizních programů a jiných dat (značka zástupce:
15 73147/PT), Způsob zavádění dat do MPEG přijímače/dekodéru a MPEG vysílací systém pro jeho realizaci (značka zástupce: 73148/PT), Organizace počítačové paměti (značka zástupce: 73149/PT), Způsob vývoje a testování řídicího programu (značka zástupce: 73150/PT), Vybírání datových úseků z
20 vysílaného datového toku (značka zástupce: 73151/PT), Systém řízení přístupu (značka zástupce: 73152/PT), Systém pro zpracování dat (značka zástupce: 73153/PT), Vysílací a přijímací systém, přijímač/dekodér a vzdálená řídicí jednotka (značka zástupce: 73154/PT). Popisy těchto dokumentů jsou
25 začleněny do tohoto popisu prostřednictvím odkazu. Seznam přihlášek obsahuje předkládanou přihlášku.

Zastupuje :

P A T E N T O V É N Á R O K Y

1. Způsob zavádění alespoň části aplikace do MPEG
přijímače/dekodéru, v y z n a č u j í c í s e t í m , že
zahrnuje kroky:

5 rozdělení aplikace do množství modulů;

• formátování každého z modulů jako odpovídající MPEG tabulku,
příčemž tyto tabulky mají stejnou tabulkovou identifikaci

• ("TID") a odpovídající odlišná tabulková identifikační
rozšíření ("TID-rozšíření") jiná, než je předem stanovené
10 TID-rozšíření;

vytvoření adresářové MPEG tabulky pro moduly, která má
stejnou uvedenou TID a uvedené předem stanovené
TID-rozšíření, přičemž adresář obsahuje pro každý modul jméno
tohoto modulu a odpovídající TID-rozšíření;

15 cyklického vysílání adresářové MPEG tabulky a modulových MPEG
tabulek v MPEG bitovém toku; a

v MPEG přijímači/dekodéru:-

 přijímání MPEG bitového toku;

20 stahování té jedné z MPEG tabulek, která má předem
stanovené TID-rozšíření tak, aby byla stažena
adresářová MPEG tabulka;

 určování z obsahu adresářové MPEG tabulky TID-rozšíření
modulových MPEG tabulek; a

25 stahování alespoň jedné z modulových MPEG tabulek
majících stejnou TID, jako je TID stažené adresářové
MPEG tabulky, a TID-rozšíření určené ze stažené
adresářové MPEG tabulky.

30 2. Způsob podle nároku 1, v y z n a č u j í c í s e
t í m , že dále zahrnuje kroky:

 začlenění do vysílané adresářové MPEG tabulky identifikaci

verze pro tuto tabulku; a

v přijímači/dekodéru:-

určování zda identifikace verze právě vysílané
adresářové PMT MPEG tabulky je aktuálnější než
5 identifikace verze právě stažené adresářové MPEG
tabulky, a pokud ano, opakování kroků stahování
adresářové MPEG tabulky, určování TID-rozšíření, a
stahování alespoň jedné z modulových MPEG tabulek.

3. Způsob podle nároku 1 nebo 2, v y z n a č u j í c í
10 s e t í m , že alespoň jedna z modulových MPEG tabulek je
formátována jako množství MPEG úseků, které jsou vysílány
samostatně v MPEG bitovém toku, přičemž každý tento MPEG úsek
obsahuje v jeho předem stanovené části identifikaci tohoto
15 MPEG úseku v MPEG tabulce a indikaci počtu úseků v MPEG
tabulce.

4. MPEG přijímač/dekodér pro použití při realizaci části
způsobu podle kteréhokoliv z předcházejících
nároků, v y z n a č u j í c í s e t í m , že zahrnuje:

20 přijímač pro přijímání MPEG bitového toku;

paměťový prostředek; a

zpracovatelský prostředek, který je naprogramován pro řízení
stahování té jedné z přijímaných MPEG tabulek, která má
předem stanovené MPEG-rozšíření, do paměťového prostředku,
25 pro určování z obsahu adresářové MPEG tabulky TID-rozšíření
modulových MPEG tabulek, a pro řízení stahování do paměťového
prostředku alespoň jedné z modulových MPEG tabulek, která má
stejnou TID, jako je TID stažené adresářové MPEG tabulky, a
TID-rozšíření určené ze stažené adresářové MPEG tabulky.

5. Přijímač/dekodér podle nároku 4 pro použití se způsobem podle nároku 2, v y z n a č u j í c í s e t í m , že zpracovatelský prostředek je naprogramován pro určování, zda identifikace verze právě přijímané adresářové MPEG tabulky je
5 aktuálnější, než je identifikace verze stažené adresářové MPEG tabulky, a pokud ano, pro opakování stahování adresářové MPEG tabulky, určování TID-rozšíření a stahování alespoň jedné z modulových MPEG tabulek.

10 6. Přijímač/dekodér podle nároku 4 nebo 5 pro použití se způsobem podle nároku 3, v y z n a č u j í c í s e t í m , že zpracovatelský prostředek je naprogramován pro řízení opakovaného stahování MPEG úseků do paměťového prostředku, dokud zpracovatelský prostředek neurčí z
15 identifikací úseků a indikace počtu úseků stahovaných úseků, že již byly staženy všechny z úseků.

7. Přijímač/dekodér podle kteréhokoliv z nároků 4 až 6, v y z n a č u j í c í s e t í m , že dále zahrnuje paralelní port a/nebo sériový port uspořádaný pro přijetí
20 aplikace formátované jako alespoň jedna MPEG tabulka.

8. MPEG vysílací systém, v y z n a č u j í c í s e t í m , že zahrnuje:

prostředek pro rozdělení aplikace určené ke stažení do MPEG přijímače/dekodéru na množství modulů;

25 prostředek pro formátování každého z modulů jako odpovídající MPEG tabulky, přičemž tyto tabulky mají stejnou TID a příslušná odlišná TID-rozšíření, jiná než je předem stanovené TID-rozšíření;

30 prostředek pro vytváření adresářové MPEG tabulky pro moduly, která má stejnou uvedenou TID a uvedené předem stanovené

TID-rozšíření, přičemž adresář obsahuje pro každý z modulů jméno tohoto modulu a příslušné TID-rozšíření; a prostředek pro cyklické vysílání adresářové MPEG tabulky a modulových MPEG tabulek v MPEG bitovém toku.

5 9. Systém podle nároku 8, v y z n a č u j í c í s e t í m , že dále zahrnuje prostředek pro vytváření identifikace verze pro adresářovou MPEG tabulku; přičemž prostředek pro vytváření adresářové MPEG tabulky je uspořádán pro začlenění do adresářové MPEG tabulky vytvořené
10 identifikace verze pro tuto tabulku.

10. systém podle nároku 8 nebo 9, v y z n a č u j í c í s e t í m , že prostředek pro formátování modulů je uspořádán pro formátování alespoň jedné z modulových MPEG
15 tabulek jako množství MPEG úseků, z nichž každý v jeho předem stanovené části obsahuje identifikaci tohoto MPEG úseku v této MPEG tabulce a indikaci počtu MPEG úseků v této MPEG tabulce.

20 11. Způsob zavádění dat do MPEG přijímače/dekodéru, v y z n a č u j í c í s e t í m , že zahrnuje kroky: vytváření podpisu pro data určená ke stažení; kódování podpisu s použitím privátního klíče; formátování dat určených ke stažení, kódovaného podpisu a identifikace pro privátní klíč jako MPEG tabulky;
25 vysílání MPEG tabulky; a v přijímači/dekodéru:-

přijímání MPEG tabulky;

zvolení jednoho z množství veřejných klíčů podle identifikace klíče v přijaté MPEG tabulce;

30 dekódování kódovaného podpisu v přijaté MPEG tabulce s

použitím zvoleného veřejného klíče pro vytvoření
dekódovaného podpisu;
vytváření podpisu pro data v přijaté MPEG tabulce; a
porovnání dekodovaného podpisu a podpisu vytvořeného v
5 přijímači/dekodéru pro přijatá data.

12. Způsob podle nároku 11, v y z n a č u j í c í s e
t í m , že dále zahrnuje kroky: stahování do
přijímače/dekodéru aplikace mající podpis kódovaný s použitím
privátního klíče majícího předem stanovenou identifikaci
10 klíče; spuštění aplikace v přijímači/dekodéru pro řízení
přijímače/dekodéru pro přijetí dalšího klíče; uložení tohoto
dalšího klíče v oblasti energeticky závislé paměti
přijímače/dekodéru.

13. Způsob podle nároku 12, v y z n a č u j í c í s e
t í m , že v průběhu kroku spuštění aplikace je další klíč
předáván lokálně do přijímače/dekodéru.

14. Způsob podle nároku 13, v y z n a č u j í c í s e
t í m , že další klíč je předáván do přijímače/dekodéru přes
20 paralelní port, sériový port nebo čtecí zařízení
inteligentních karet přijímače/dekodéru.

15. Způsob podle kteréhokoliv z nároků 11 až
14, v y z n a č u j í c í s e t í m , že dále zahrnuje
kroky: v přijímači/dekodéru: vyhledávání v chráněné oblasti
25 paměti přijímače/dekodéru příznaku platnosti pro zvolený
veřejný klíč; a zamezení nebo přerušení stahování dat, pokud
vyhledaný příznak platnosti není nastaven.

16. Způsob podle nároku 15 závislého na kterémkoliv z
nároků 12 až 14, v y z n a č u j í c í s e t í m , že v
chráněné oblasti paměti přijímače/dekodéru privátní klíč
mající předem stanovenou identifikaci klíče má příznak
5 platnosti, který může být měněn prostřednictvím uvedené
aplikace, přičemž schopnost přijímat další klíč je určena v
závislosti na stavu tohoto příznaku platnosti.

17. Způsob zavádění dat do MPEG přijímače/dekodéru,
v y z n a č u j í c í s e t í m , že zahrnuje kroky:-
10 vytváření podpisu pro data určená ke stažení;
kódování podpisu s použitím privátního klíče;
formátování dat určených ke stažení, kódovaného podpisu a
identifikace pro privátní klíč jako MPEG tabulky;
vysílání MPEG tabulky; a
15 v přijímači/dekodéru:-

přijímání MPEG tabulky;
vyhledávání v chráněné oblasti paměti
přijímače/dekodéru příznaku platnosti pro veřejný klíč
odpovídající privátnímu klíči identifikovanému v
20 přijaté MPEG tabulce; a
pokud je vyhledaný příznak platnosti nastaven:-

dekódování kódovaného podpisu v přijaté MPEG
tabulce s použitím veřejného klíče odpovídajícího
privátnímu klíči identifikovanému v přijaté MPEG
25 tabulce pro vytvoření dekódovaného podpisu;
vytváření podpisu pro data v přijaté MPEG tabulce;
a porovnání dekódovaného podpisu a podpisu
vytvořeného v přijímači/dekodéru pro přijatá data.

18. Způsob podle kteréhokoliv z nároků 11 až 17, v y z n a č u j í c í s e t í m , že dále zahrnuje kroky:-

vytvoření ověřovacího kódu pro data určená ke stažení,
5 přičemž tento ověřovací kód je kódován s podpisem v kódovacím kroku a je dekódován s podpisem v dekódovacím kroku;
vyhledání uloženého ověřovacího kódu v chráněné oblasti paměti přijímače/dekodéru; a
porovnání vyhledaného ověřovacího kódu a dekódovaného
10 ověřovacího kódu.

19. Způsob zavádění dat do MPEG přijímače/dekodéru, v y z n a č u j í c í s e t í m , že zahrnuje kroky:-

vytváření ověřovacího kódu pro data určená ke stažení;
15 vytváření podpisu pro data určená ke stažení, nebo jejich části;

kódování ověřovacího kódu a podpisu s použitím privátního klíče;

formátování dat určených ke stažení a kódovaného ověřovací kódu a podpisu jako alespoň jedné MPEG tabulky;

20 vysílání uvedené jedné nebo každé MPEG tabulky; a v přijímači/dekodéru:-

přijímání uvedené jedné nebo každé MPEG tabulky;

dekódování kódovaného ověřovacího kódu a podpisu v
přijatých MPEG tabulkách s použitím veřejného klíče
25 odpovídajícího privátnímu klíči;

vyhledání uloženého ověřovacího kódu v chráněné oblasti paměti přijímače/dekodéru;

porovnání vyhledaného ověřovacího kódu a dekódovaného
30 ověřovacího kódu;

vytváření podpisu pro data v přijatých MPEG tabulkách,

nebo jejich část; a
porovnání dekodovaného podpisu s podpisem vytvořeným v
přijímači/dekodéru pro přijatá data.

5 20. Způsob podle nároku 18 nebo 19, v y z n a č u j í c í
s e t í m , že dále zahrnuje krok zamezení nebo přerušení
stahování dat, pokud si v kroku porovnávání ověřovacích kódů
vyhledaný ověřovací kód a dekodovaný ověřovací kód vzájemně
neodpovídají.

10 21. Způsob podle kteréhokoliv z nároků 11 až
20, v y z n a č u j í c í s e t í m , že podpis dat
určených ke stažení je kódován v bloku dat, včetně dalších
dat, se zvoleným posunutím mezi začátkem datového bloku a
začátkem podpisu, a kódovaný datový blok je dekodován v kroku
15 dekodování v přijímači/dekodéru, přičemž způsob podle
vynálezu dále zahrnuje kroky v přijímači/dekodéru:-
vyhledávání alespoň jednoho uloženého posunutí v chráněné
oblasti paměti přijímače/dekodéru; a vyjmutí podpisu z
dekodovaného datového bloku s použitím uvedeného jednoho
20 vyhledaného posunutí od začátku dekodovaného datového bloku.

22. Způsob zavádění dat do MPEG přijímače/dekodéru,
v y z n a č u j í c í s e t í m , že zahrnuje kroky:-
vytváření podpisu pro data určená ke stažení;
začlenění podpisu a dalších dat do bloku dat se zvoleným
25 posunutím mezi začátkem datového bloku a začátkem podpisu;
kódování datového bloku s použitím privátního klíče;
formátování dat určených ke stažení a kódovaného datového
bloku jako MPEG tabulky;
vysílání této MPEG tabulky; a
30 v přijímači/dekodéru:-

přijímání MPEG tabulky;

dekódování kódovaného datového bloku v přijaté MPEG
tabulce s použitím veřejného klíče odpovídajícího
privátnímu klíči;

5 vyhledání alespoň jednoho uloženého posunutí v chráněné
oblasti paměti přijímače/dekodéru;

vyjmutí podpisu z dekódovaného datového bloku s
použitím uvedeného jednoho vyhledaného posunutí od
začátku dekódovaného datového bloku;

10 vytváření podpisu pro data v přijaté MPEG tabulce; a
porovnání podpisu vyjmutého z dekódovaného datového
bloku s podpisem vytvořeným v přijímači/dekodéru pro
přijatá data.

15 23. Způsob podle nároku 21 nebo 22, v y z n a č u j í c í
s e t í m , že uvedená chráněná oblast paměti má alespoň
dvě takováto uložená posunutí, přičemž, pokud v kroku
porovnání si vyjmutý podpis a vytvořený podpis vzájemně
neodpovídají, zahrnuje způsob dále kroky opakování kroků
20 vyhledání, vyjmutí a porovnání s použitím dalšího z uložených
posunutí.

24. Způsob podle kteréhokoliv z nároků 21 až
23, v y z n a č u j í c í s e t í m , že alespoň nějaká z
uvedených dalších dat v bloku dat jsou fiktivní nebo
25 libovolná data.

25. Způsob podle kteréhokoliv z nároků 11 až
24, v y z n a č u j í c í s e t í m , že data jsou
stahována jako množství modulů dat, přičemž způsob dále
zahrnuje kroky:-
30 vytváření modulového podpisu pro každý modul dat, určený ke

stažení;

formátování modulů dat jako příslušných modulových MPEG
tabulek;

vytváření adresáře včetně identifikace každé modulové MPEG

5 tabulky a příslušného podpisu, přičemž tento adresář je
subjektem kroku vytváření podpisu podle kteréhokoliv z nároků
11 až 24; a

v přijímači/dekodéru:-

10 vytváření příslušného modulového podpisu pro každý z
modulů v přijatých modulových MPEG tabulkách; a
porovnání každého modulového podpisu v přijaté
adresářové MPEG tabulce s příslušným modulovým podpisem
vytvořeným v přijímači/dekodéru.

15 26. Způsob zavádění množství modulů dat do MPEG
přijímače/dekodéru, v y z n a č u j í c í s e t í m , že
zahrnuje kroky:-

vytváření modulového podpisu pro každý modul dat určených ke
stažení;

20 formátování modulů dat jako příslušných modulových MPEG
tabulek;

vytváření adresáře včetně identifikace každé modulové MPEG
tabulky a příslušného podpisu;

vytváření adresářového podpisu pro adresář;

25 kódování adresářového podpisu s použitím privátního klíče;

formátování adresáře a kódovaného adresářového podpisu jako
adresářové MPEG tabulky;

vysílání adresářové a modulových MPEG tabulek; a

v přijímači/dekodéru:-

30 přijímání adresářové a modulových MPEG tabulek;

dekódování kódovaného adresářového podpisu v přijaté

adresářové MPEG tabulce s použitím veřejného klíče
odpovídajícího privátnímu klíči;
vytvoření adresářového podpisu pro adresář v přijaté
adresářové MPEG tabulce;

5 porovnání dekódovaného adresářového podpisu a
adresářového podpisu vytvořeného v přijímači/dekodéru;
vytvoření příslušného modulového podpisu pro každý z
modulů v přijatých modulových MPEG tabulkách; a
porovnání každého modulového podpisu v přijaté
10 adresářové MPEG tabulce s příslušným modulovým podpisem
vytvořeným v přijímači/dekodéru.

27. Způsob podle nároku 25 nebo 26, v y z n a č u j í c í
s e t í m , že dále zahrnuje krok zabránění nebo přerušení
15 stahování takového modulu dat, pokud v kroku porovnání
modulových podpisů si modulový podpis v přijaté adresářové
MPEG tabulce a příslušný modulový podpis vytvořený v
přijímači dekodéru pro tento modul vzájemně neodpovídají.

28. Způsob podle kteréhokoliv z nároků 11 až
20 27, v y z n a č u j í c í s e t í m , že zahrnuje krok
zabránění nebo přerušení stahování dat, pokud si v kroku
(krocích) porovnání jeden nebo každý dekódovaný podpis a
vytvořený podpis vzájemně neodpovídají.

29. MPEG přijímač/dekodér pro použití při realizaci způsobu
25 podle nároku 11, v y z n a č u j í c í s e t í m , že
zahrnuje:

prostředek pro přijímání MPEG tabulek;
prostředek pro ukládání množství veřejných klíčů a
identifikace pro každý z veřejných klíčů; a
30 zpracovatelský prostředek, který je naprogramován pro zvolení

jednoho z uložených veřejných klíčů podle identifikace klíče v přijaté MPEG tabulce; pro dekódování kódovaného podpisu v přijaté MPEG tabulce s použitím zvoleného veřejného klíče pro vytvoření dekódovaného podpisu; pro vytvoření podpisu pro data v přijaté MPEG tabulce; a pro porovnání dekódovaného podpisu a podpisu vytvořeného v přijímači/dekodéru pro přijatá data.

30. Přijímač/dekodér podle nároku 29, v y z n a č u j í c í s e t í m , že paměťový prostředek pro uložení klíčů je zajištěn prostřednictvím ROM.

31. Přijímač/dekodér podle nároku 29 nebo 30, v y z n a č u j í c í s e t í m , že identifikace pro každý z veřejných klíčů je zajištěna prostřednictvím paměťového místa tohoto veřejného klíče v paměťovém prostředku pro uložení klíčů.

32. Přijímač/dekodér podle kteréhokoliv z nároků 29 až 31 pro použití ve způsobu podle nároku 14, v y z n a č u j í c í s e t í m , že dále zahrnuje oblast energeticky závislé paměti, přičemž zpracovatelský prostředek je uspořádán pro stahování aplikace mající podpis kódovaný s použitím privátního klíče majícího předem stanovenou identifikaci klíče, pro spuštění této aplikace pro řízení přijímače/dekodéru pro přijetí dalšího klíče, a pro řízení uložení tohoto dalšího klíče do oblasti energeticky závislé paměti.

33. Přijímač/dekodér podle nároku 32, v y z n a č u j í c í s e t í m , že dále zahrnuje prostředek pro přijetí takového dalšího klíče, který je předáván lokálně do přijímače/dekodéru.

34. Přijímač/dekodér podle nároku 33, v y z n a č u j í c í s e t í m , že prostředkem pro přijetí dalšího klíče je paralelní port, sériový port a/nebo čtecí zařízení pro čtení inteligentních karet v přijímači/dekodéru.

5 35. Přijímač/dekodér podle kteréhokoliv z nároků 32 až 34, v y z n a č u j í c í s e t í m , že energeticky závislá paměť je zajištěna prostřednictvím RAM.

10 36. Přijímač/dekodér podle kteréhokoliv z nároků 29 až 35 pro použití ve způsobu podle nároku 15, v y z n a č u j í c í s e t í m , že dále zahrnuje chráněnou oblast paměti pro uložení příznaku platnosti pro každý z alespoň nějakých veřejných klíčů, přičemž zpracovatelský prostředek je naprogramován pro vyhledání v této chráněné oblasti paměti
15 příznaku platnosti pro zvolený veřejný klíč, a pro zabránění nebo přerušení stahování dat, pokud tento vyhledaný příznak platnosti není nastaven.

20 37. Přijímač/dekodér podle nároku 36 závislého na kterémkoliv z nároků 32 až 35, v y z n a č u j í c í s e t í m , že dále zahrnuje chráněnou oblast paměti pro uložení příznaku platnosti pro privátní klíč mající předem stanovenou identifikaci klíče, přičemž zpracovatelský prostředek je uspořádán při spuštění uvedené aplikace pro změnu tohoto
25 příznaku platnosti a je uspořádán pro umožnění takového uložení dalšího klíče v závislosti na stavu tohoto příznaku platnosti.

30 38. MPEG přijímač/dekodér pro použití při realizaci části způsobu podle nároku 17, v y z n a č u j í c í s e t í m , že zahrnuje:
prostředek pro přijímání MPEG tabulek;

prostředek pro ukládání veřejného klíče a identifikace pro tento veřejný klíč; a

chráněnou oblast paměti pro uložení příznaku platnosti pro veřejný klíč; a

5 zpracovatelský prostředek, který je naprogramován pro vyhledání v této chráněné oblasti paměti přijímače/dekodéru příznaku platnosti pro veřejný klíč odpovídající privátnímu klíči identifikovanému v přijaté MPEG tabulce; a, pokud je vyhledaný příznak platnosti nastaven, pro dekódování
10 kódovaného podpisu v přijaté MPEG tabulce s použitím veřejného klíče odpovídajícího privátnímu klíči identifikovanému v přijaté MPEG tabulce pro vytvoření dekódovaného podpisu; pro vytvoření podpisu pro data v přijaté MPEG tabulce; a pro porovnání dekódovaného podpisu a
15 podpisu vytvořeného v přijímači/dekodéru pro přijatá data.

39. Přijímač/dekodér podle kteréhokoliv z nároků 36 až 38, v y z n a č u j í c í s e t í m , že paměť pro uložení příznaku (příznaků) platnosti pro klíče je zajištěna prostřednictvím přepisovatelné paměti nezávislé na zdroji
20 energie.

40. Přijímač/dekodér podle kteréhokoliv z nároků 36 až 39, v y z n a č u j í c í s e t í m , že v případě, ve kterém je uloženo množství takových veřejných klíčů, je paměť
25 pro uložení příznaku (příznaků) platnosti uspořádána jako bitová mapa.

41. Přijímač/dekodér kteréhokoliv z nároků 29 až 40 pro použití ve způsobu podle nároku 17, v y z n a č u j í c í s e t í m , že dále zahrnuje chráněnou oblast paměti pro
30 uložení ověřovacího kódu, přičemž zpracovatelský prostředek

je naprogramován pro dekodování ověřovacího kódu v přijaté MPEG tabulce, pro vyhledání uloženého ověřovacího kódu, a pro porovnání vyhledaného ověřovacího kódu a dekodovaného ověřovacího kódu.

5 42. MPEG přijímač/dekodér pro použití při realizaci části způsobu podle nároku 17, v y z n a č u j í c í s e
• t í m , že zahrnuje:
• prostředek pro přijímání MPEG tabulek;
10 prostředek pro ukládání veřejného klíče a identifikace pro tento veřejný klíč;
chráněnou oblast paměti pro uložení ověřovacího kódu; a
zpracovatelský prostředek, který je naprogramován pro dekodování kódovaného ověřovacího kódu a podpisu v přijatých MPEG tabulkách s použitím uloženého veřejného klíče
15 odpovídajícího privátnímu klíči; pro vyhledání uloženého ověřovacího kódu v chráněné oblasti paměti; pro porovnání vyhledaného ověřovacího kódu a dekodovaného ověřovacího kódu;
pro vytvoření podpisu pro data v přijaté MPEG tabulce nebo jejich část; a pro porovnání dekodovaného podpisu s podpisem
20 vytvořeným v přijímači/dekodéru pro přijatá data.

43. Přijímač/dekodér podle nároku 41 nebo
• 42, v y z n a č u j í c í s e t í m , že zpracovatelský prostředek je naprogramován pro zabránění nebo přerušení
• 25 stahování dat, pokud si vyhledaný ověřovací kód a dekodovaný ověřovací kód vzájemně neodpovídají.

44. Přijímač/dekodér podle kteréhokoliv z nároků 41 až 43, v y z n a č u j í c í s e t í m , že paměť pro uložení ověřovacích kódů je zajištěna prostřednictvím
30 přepisovatelné paměti nezávislé na zdroji energie.

45. Přijímač/dekodér podle kteréhokoliv z nároků 41 až 43, v y z n a č u j í c í s e t í m , že paměť pro uložení ověřovacích kódů je uspořádána jako bitová mapa.

46. Přijímač/dekodér podle kteréhokoliv z nároků 29 až 45 pro použití ve způsobu podle nároku 21, v y z n a č u j í c í s e t í m , že dále zahrnuje chráněnou oblast paměti pro uložení alespoň jednoho posunutí, přičemž zpracovatelský prostředek je naprogramován pro dekódování kódovaného datového bloku v přijaté MPEG tabulce, pro vyhledání uvedeného jednoho uloženého posunutí v chráněné oblasti paměti, a pro vyjmutí podpisu z dekódovaného datového bloku s použitím vyhledaného posunutí od začátku dekódovaného datového bloku.

47. MPEG přijímač/dekodér pro použití při realizaci způsobu podle nároku 22, v y z n a č u j í c í s e t í m , že zahrnuje:

prostředek pro přijímání MPEG tabulek;

prostředek pro uložení veřejného klíče a identifikace pro

tento veřejný klíč;

chráněnou oblast paměti pro uložení alespoň jednoho posunutí;

zpracovatelský prostředek, který je naprogramován pro

dekódování kódovaného datového bloku v přijaté MPEG tabulce s

použitím uloženého veřejného klíče odpovídajícího privátnímu

klíči; pro vyhledání uvedeného jednoho uloženého posunutí v

chráněné oblasti paměti; pro vyjmutí podpisu z dekodovaného

datového bloku s použitím vyhledaného posunutí od začátku

dekódovaného datového bloku; pro vytvoření podpisu pro data v

přijaté MPEG tabulce; a pro porovnání podpisu vyjmutého z

dekódovaného datového bloku s podpisem vytvořeným v přijímači/dekodéru pro přijatá data.

48. Přijímač/dekodér podle nároku 46 nebo

47, v y z n a č u j í c í s e t í m , že alespoň dvě takováto posunutí jsou uložena v chráněné oblasti paměti, přičemž zpracovatelský prostředek je uspořádán, pokud si vyjmutý podpis a vytvořený podpis vzájemně neodpovídají, pro opakování vyhledání, vyjmutí a porovnání s použitím dalšího z uložených posunutí.

49. Přijímač/dekodér podle kteréhokoliv z nároků 46 až 48, v y z n a č u j í c í s e t í m , že paměť pro uložení posunutí je zajištěna prostřednictvím přepisovatelné paměti nezávislé na zdroji energie.

50. Přijímači/dekodér podle kteréhokoli z nároků 29 až 49 pro použití ve způsobu podle nároku 25, v y z n a č u j í c í s e t í m , že zpracovatelský prostředek je naprogramován pro vytvoření příslušného modulového podpisu pro každý z modulů v přijatých MPEG tabulkách, a pro porovnání každého modulového podpisu v přijaté adresářové MPEG tabulce s příslušným modulovým podpisem vytvořeným v přijímači/dekodéru.

51. MPEG přijímač/dekodér pro použití při realizaci způsobu podle nároku 26, v y z n a č u j í c í s e t í m , že zahrnuje:

prostředek pro přijímání adresářové a modulových MPEG
tabulek;

prostředek pro uložení veřejného klíče a identifikace pro tento veřejný klíč; a

zpracovatelský prostředek, který je naprogramován pro

Fig. 1.

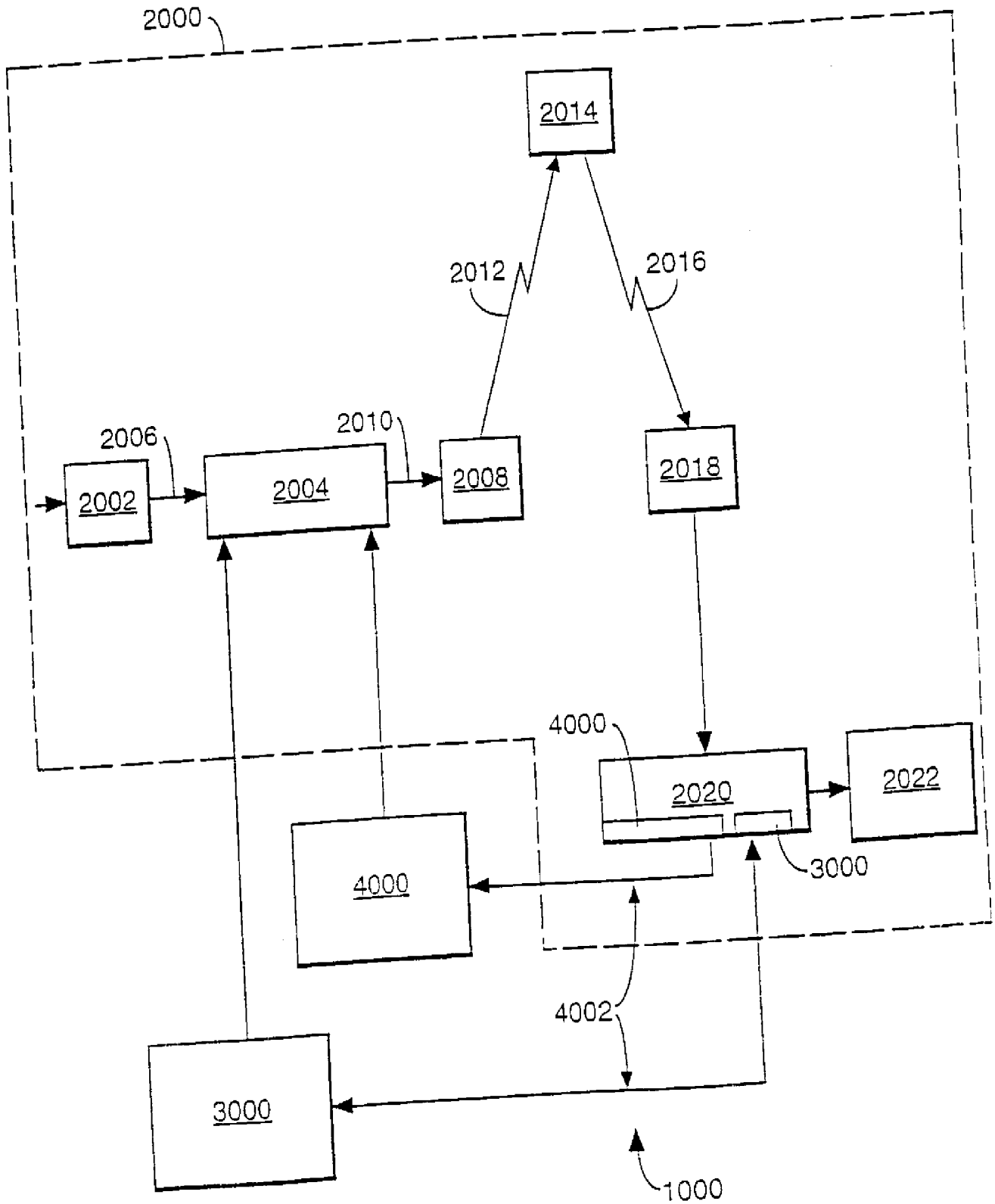


Fig.2.

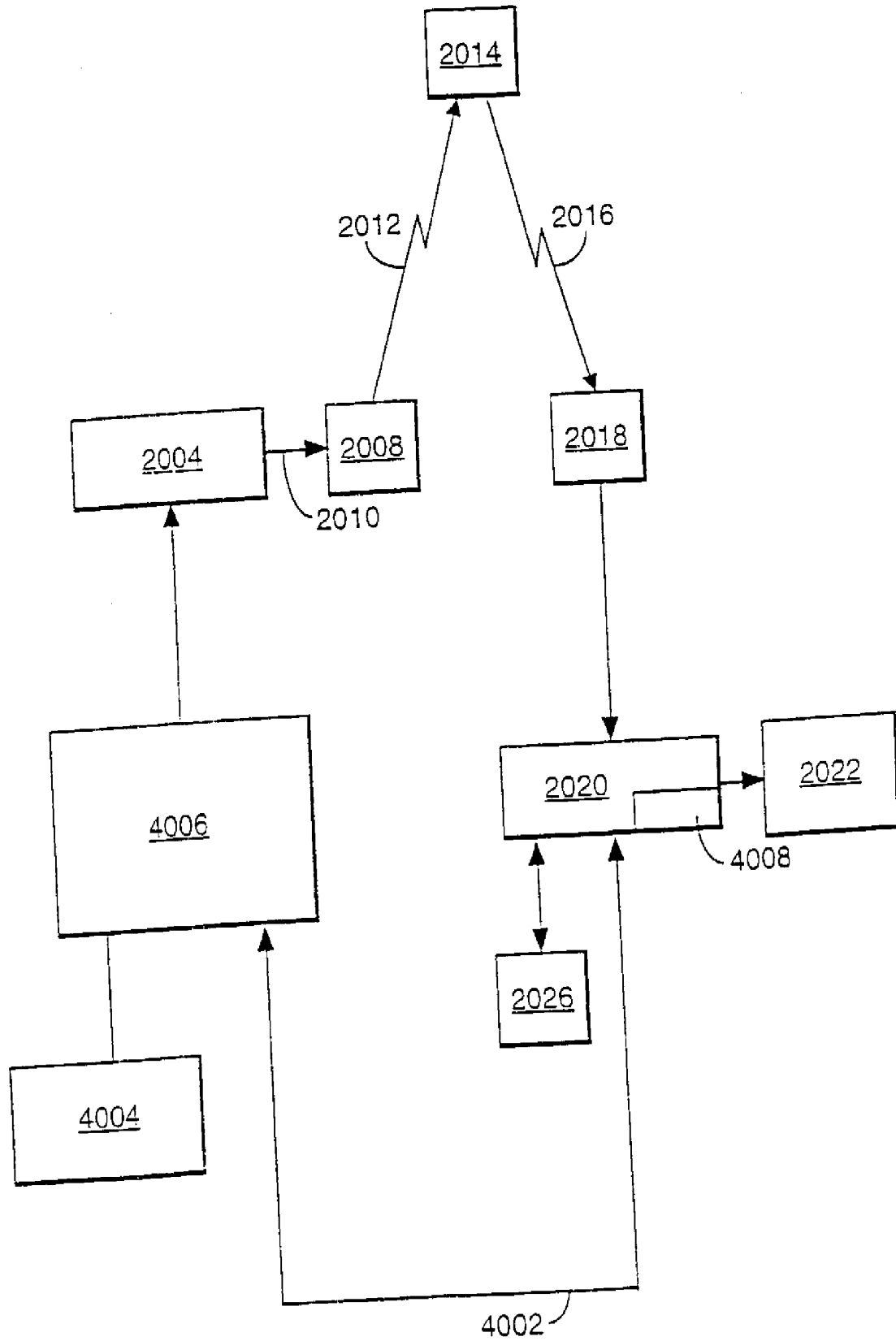


Fig.3.

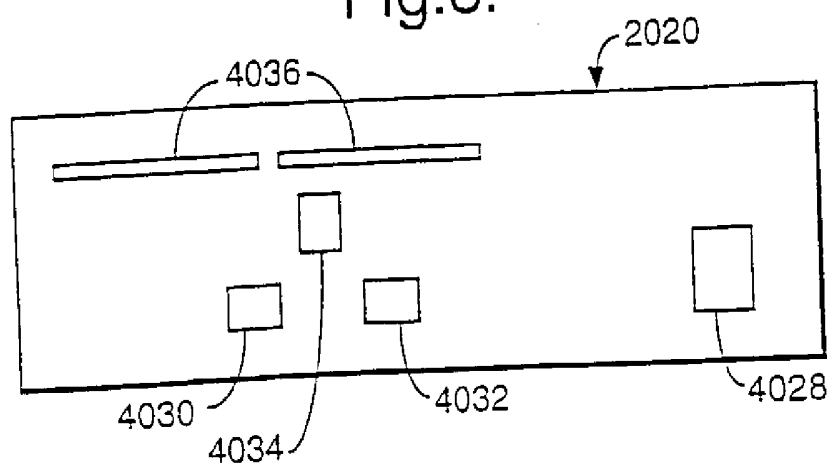


Fig.4.

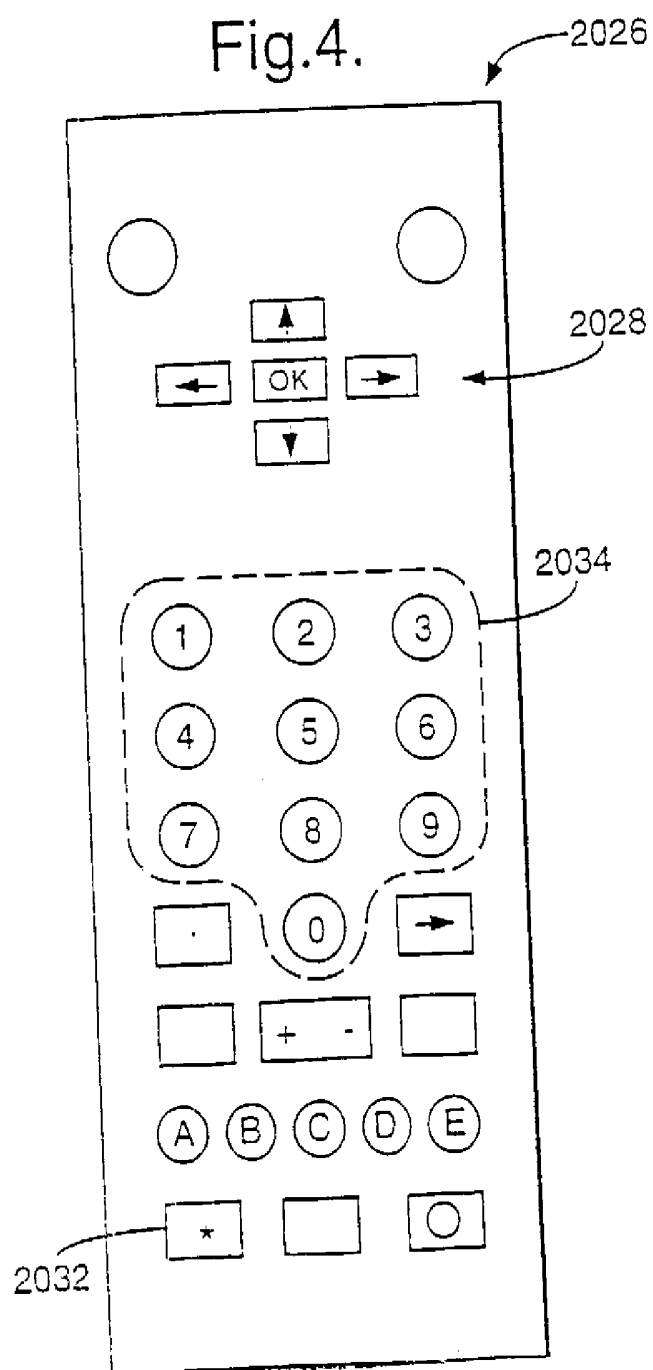
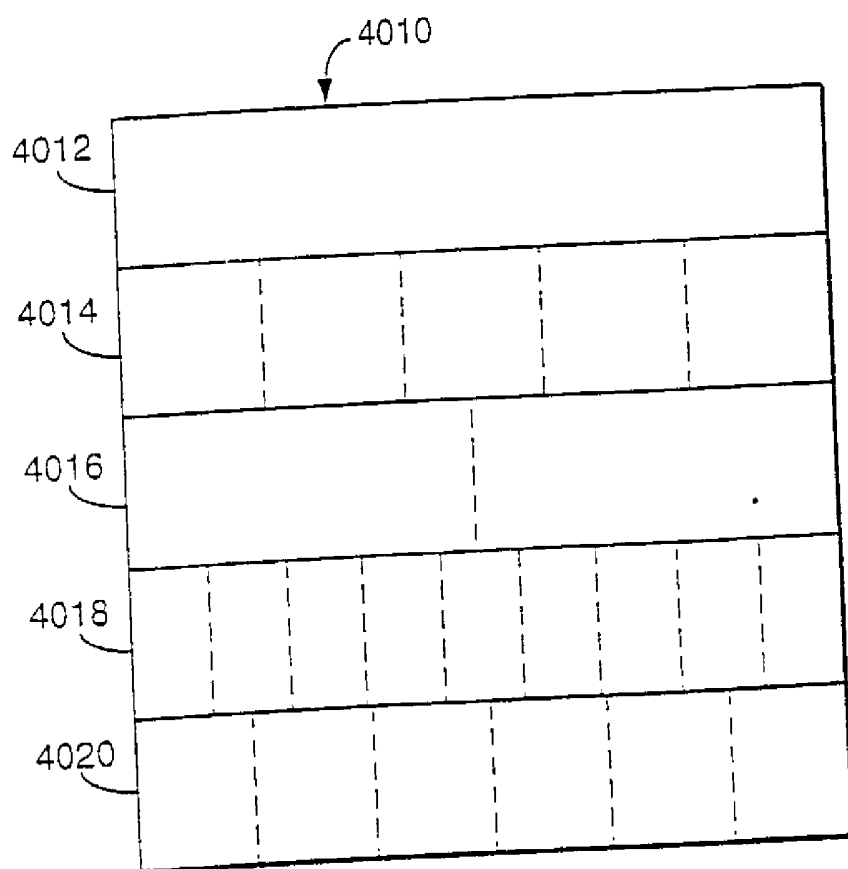


Fig.5.



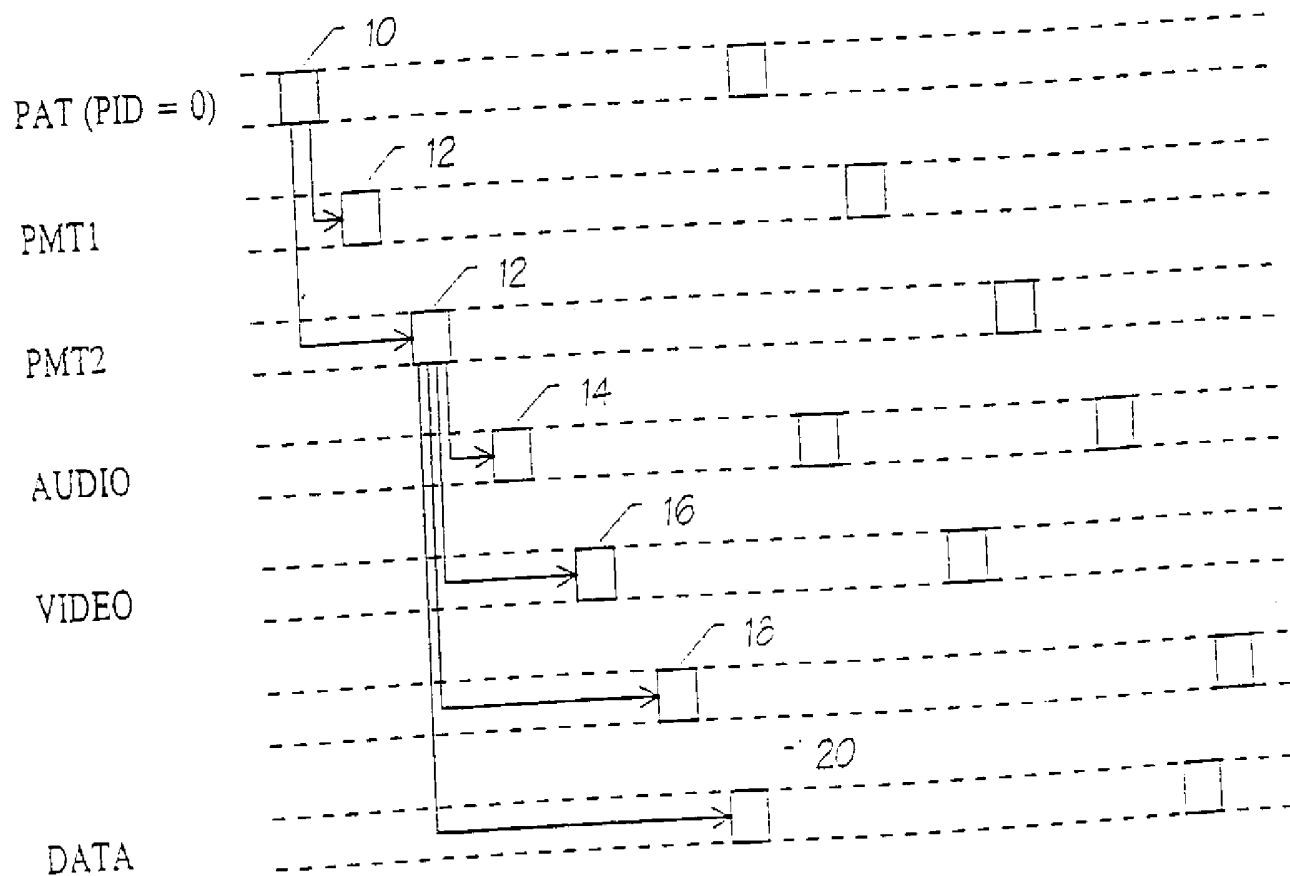


FIG. 6

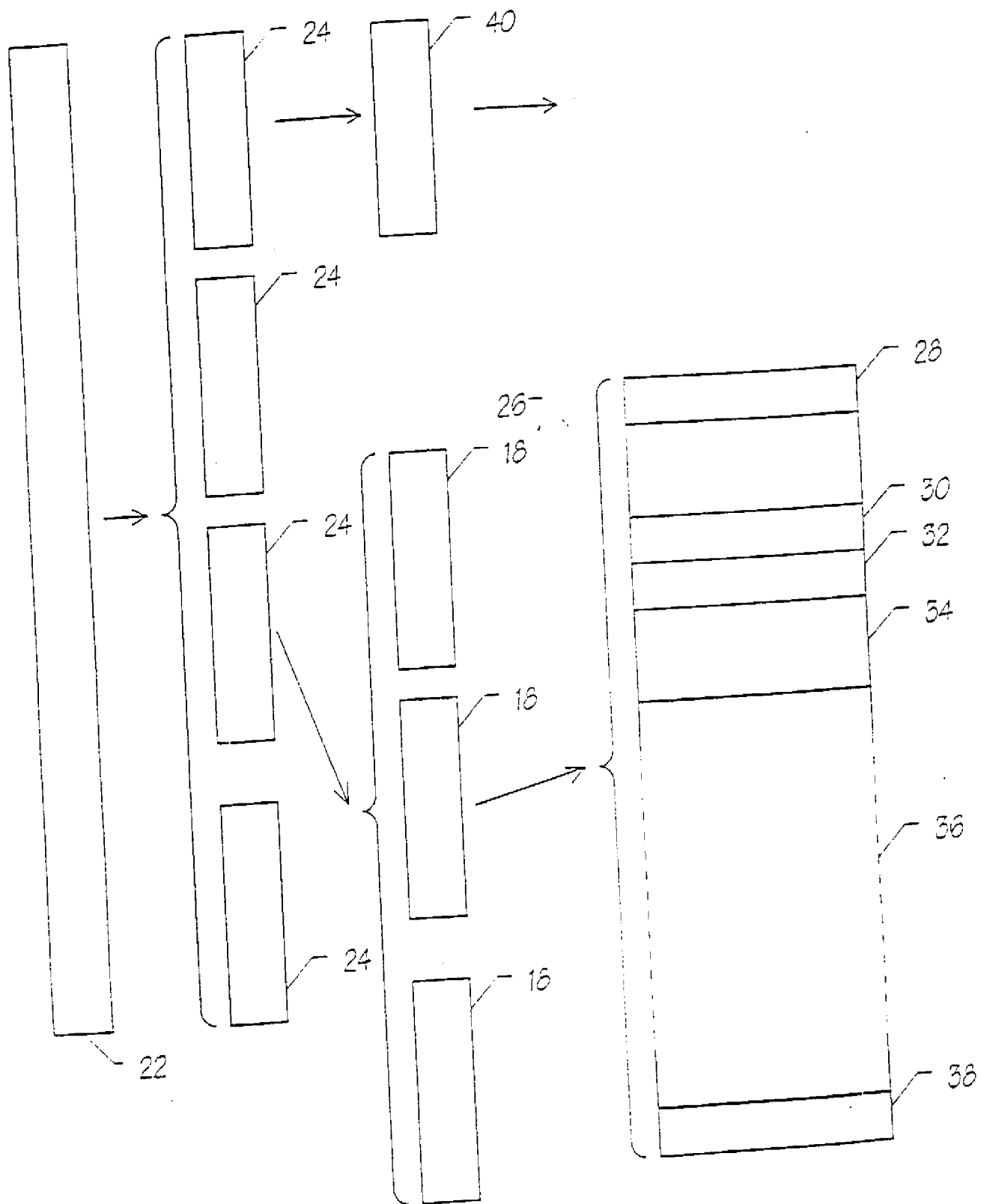


FIG. 7

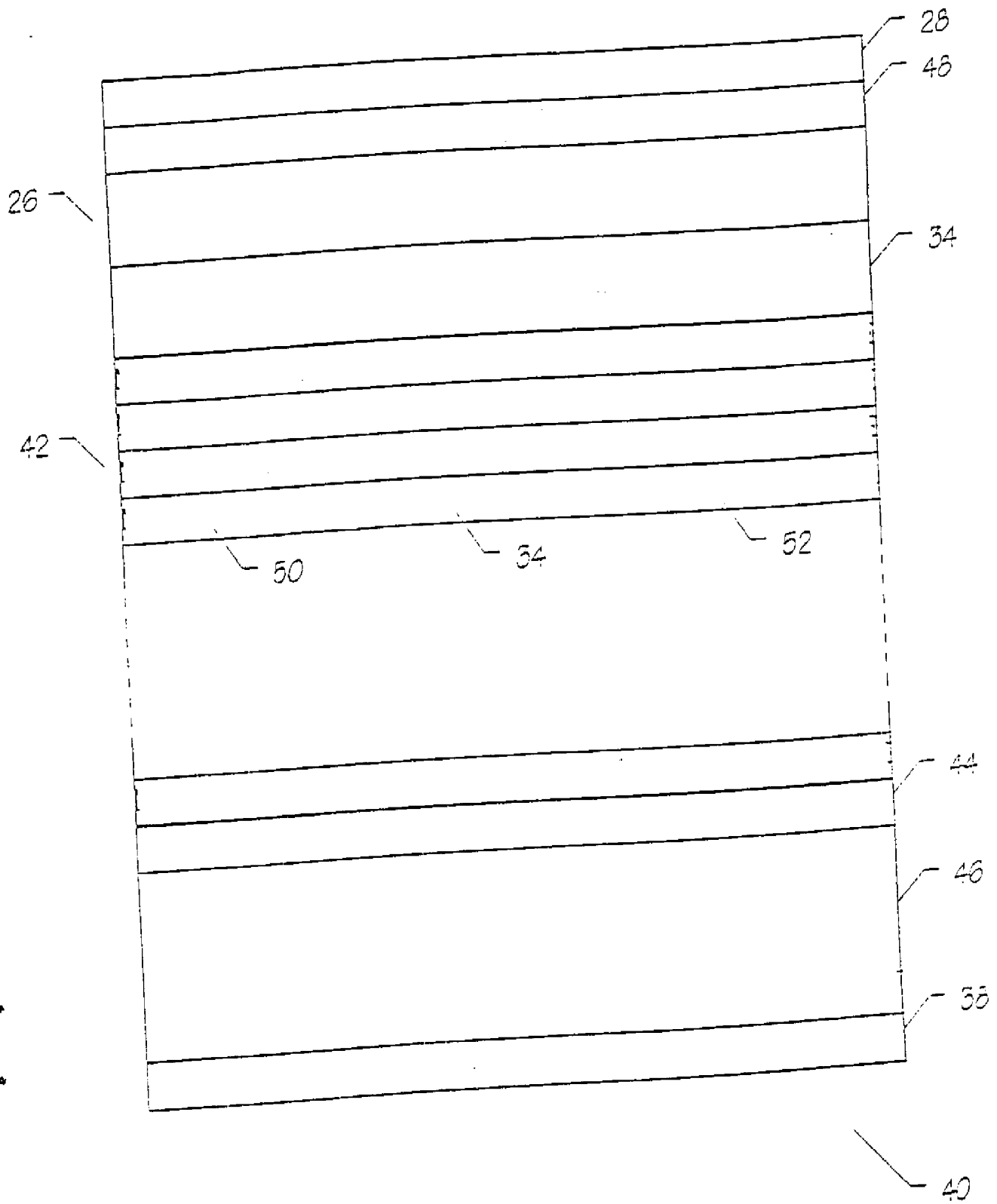


FIG. 8

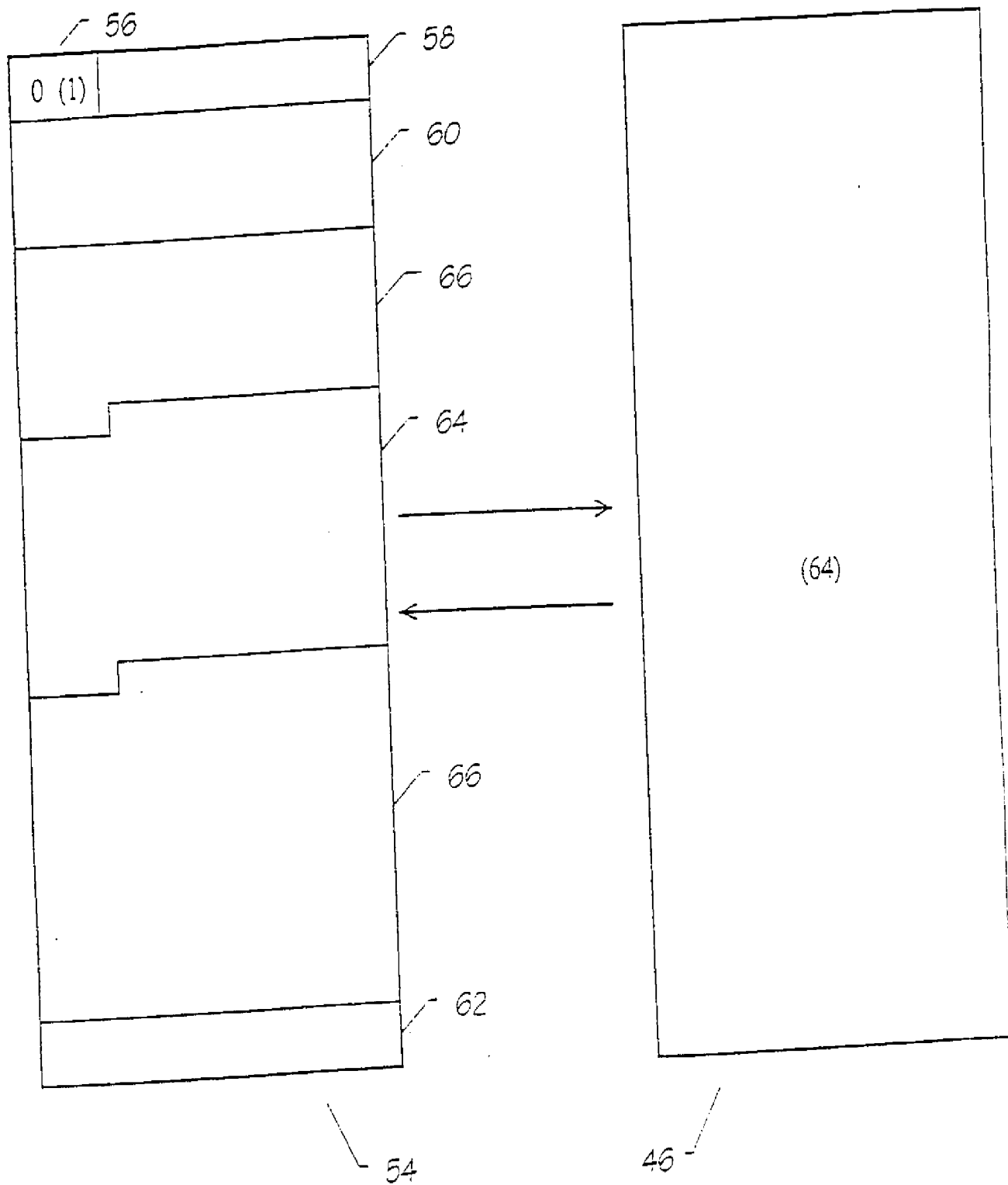


FIG. 9

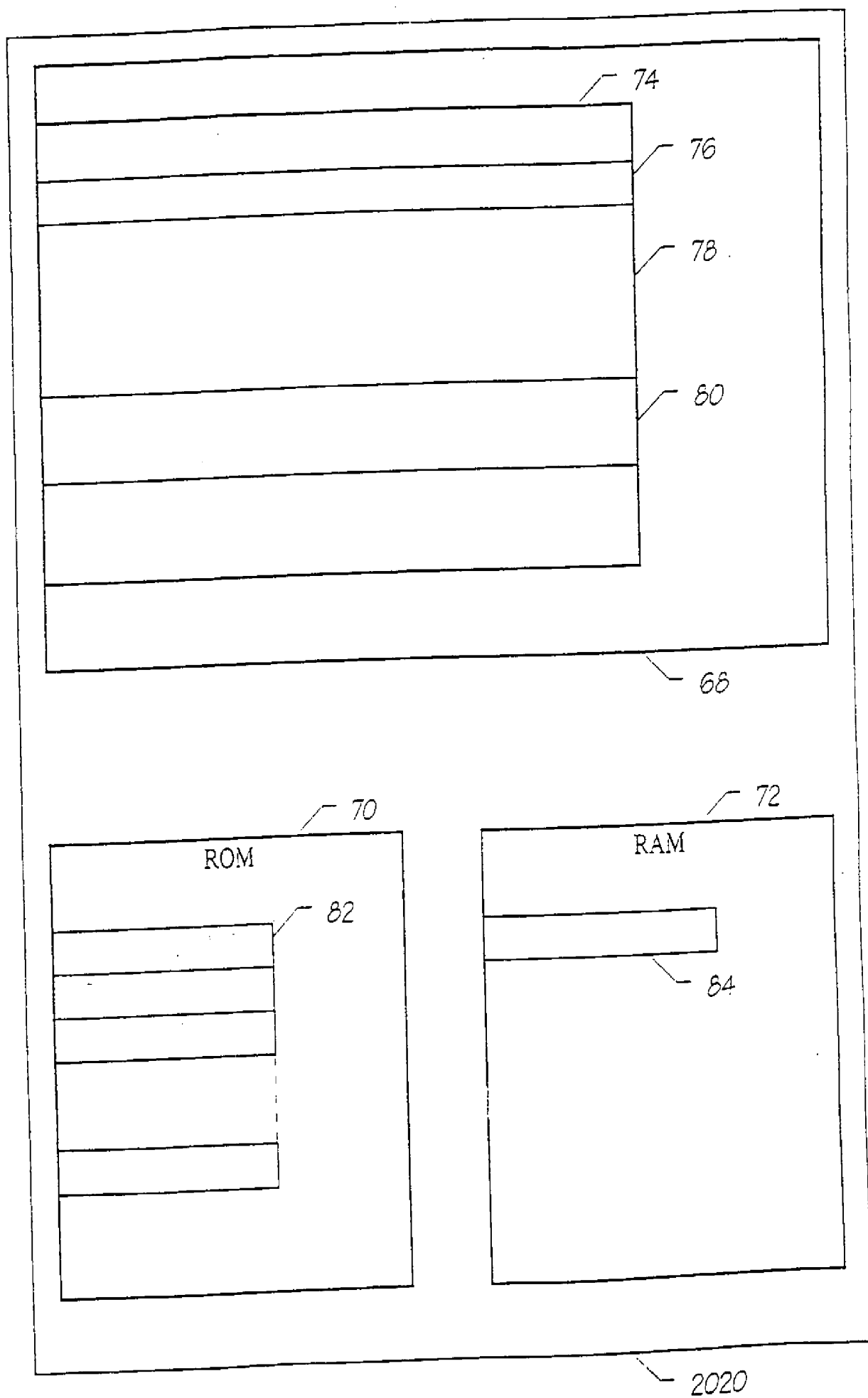


FIG. 10