SLOVENSKÁ REPUBLIKA

(19) **SK**

ÚRAD
PRIEMYSELNÉHO
VLASTNÍCTVA
SLOVENSKEJ REPUBLIKY

ZVEREJNENÁ PRIHLÁŠKA VYNÁLEZU

(22) Dátum podania: 29.09.94

(31) Číslo prioritnej prihlášky: 9407038.0

(32) Dátum priority: 08.04.94

(33) Krajina priority: GB

(40) Dátum zverejnenia: 04.02.98

(86) Číslo PCT: PCT/GB94/02116, 29.09.94

(21) Číslo dokumentu:

1285-96

(13) Druh dokumentu: **A3**

(51) Int. Cl.[6] :

H 04N 7/16,
H 04N 7/169

(71) Prihlasovateľ: AMSTRAD PUBLIC LIMITED COMPANY, Brentwood, Essex, GB;

(72) Pôvodca vynálezu: Davies Donald Watts, Sunbury on Thames, Middlesex, GB;

(54) Názov prihlášky vynálezu: **Spôsob vysielania a prijímania šifrovaných signálov a zariadenie na vykonávanie tohto spôsobu**

(57) Anotácia:
Šifrovaný signál kompatibilný s prvým a druhým šifrovacím systémom je získaný tak, že sú vygenerované šifrovacie dátové signály týkajúce sa jednotlivých šifrovacích systémov. Z dvoch šifrovacích dátových signálov je odvodený rozdielový signál a signál, ktorý má byť šifrovaný, je zašifrovaný podľa jedného zo šifrovacích systémov. Na výstupe je k dispozícii šifrovaný signál, dva šifrovacie signály a rozdielový signál. V dekodéri, kompatibilnom napr. s prvým šifrovacím systémom, sú prijaté šifrované dáta, druhý šifrovací dátový signál a rozdielový signál. Dekodér potom môže odvodiť prvý šifrovací dátový signál z druhého dátového šifrovacieho signálu a z rozdielového signálu a potom môže dekódovať šifrovaný signál.

Spôsob a zariadenie na vysielanie a prijímanie šifrovaných signálov

Oblasť techniky

Vynález sa týka spôsobu a zariadenia pre vysielanie a prijímanie šifrovaných signálov, zvlášť potom televíznych signálov, ku ktorým je riadený prístup pomocou rôznych spôsobov utajenia.

Doterajší stav techniky

Systémy s riadeným prístupom sa stali dôležitými napr. pre prevádzateľa satelitných televízií, pretože im umožňujú obmedziť geograficky oblasti, v ktorých môže byť program sledovaný: to môže byť dôležité pre vyhovenie programovému rozvrhu alebo povinnostiam vyplývajúcich z autorských práv. Riadený prístup tiež umožňuje prevádzateľom zaistiť, aby televízne signály s riadeným prístupom mohli sledovať len diváci so zaplateným predplatným. Ďalej umožňuje zavedenie rôznych pravidiel platenia za jednotlivé vstupy.

Utajovanie (šifrovanie) televíznych signálov predstavuje dobre zavedenú techniku, ktorá môže byť použitá kedykoľvek tam, kde príslušné signály sú určené len pre obmedzenú podmnožinu potenciálnych príjemcov. Pre utajovanie existuje množstvo rôznych spôsobov. Jedným z najlepšie zavedených je spôsob "prerušenia & prehodenia" (cut & rotate"), ktorý bol pôvodne vyvinutý firmou Westinghouse. Pri spôsobe "prerušenia & prehodenia", tak ako bol aplikovaný na PAL Európsky štandardný televízny obrazový signál, je každý z aktívnych obrazových riadkov z celkového počtu 625 obrazových riadkov jednej obrazovej snímky prerušený v rozdielnom bode; takto vzniknuté dve časti obrazového riadku sú potom vzájomne prehodené a spojenie

medzi týmito preusporiadanými časťami je vyhladené. Taký riadok potom nazývame "utajený"; televízny prevádzateľ, ktorý si praje vysielať takéto utajené obrázky môže zabudovať do vysielacej stanice určitý druh prostriedku alebo zariadenia pre "prerušenie & prehodenie" (jednotku pre aktívnu rotáciu riadku) tak, aby vysielané obrazové signály boli utajené. Snímka takto utajených riadkov môže byť prijímaná diváckym prijímačom, ale ak tento prijímač nevie vykonávať proces presne inverzný k utajovaciemu procesu, potom snímka vypadá celkom nezrozumiteľne. Tento proces zahrňuje prerušenie každého aktívneho obrazového riadku v správnom "prerušovacom bode" (cut-point) a rotáciu časti každého riadku tak, aby bola preusporiadaná do svojej pôvodnej neutajenej podoby. Prijímač musí vedieť, kde sa nachádzajú všetky "prerušovacie body".

Keby dáta o "prerušovacích bodoch" boli zahrnuté v obrazovom signále, potom by (a) zaberali podstatnú časť prenosového pásma a (b) umožňovala pirátske vytvorenie prijímača, ktorý môže nájsť miesta prerušovacích bodov a tým zmariť celý účel systému s obmedzeným prístupom. Z týchto dôvodov boli vytvorené šifrovacie techniky, ktoré umožňujú vygenerovanie dát o prerušovacích bodoch interne z dát, ktoré sú vysielané spoločne s obrazovým signálom. Samé vysielané dáta neudávajú žiadnu informáciu o dátach určujúcich prerušovaný bod.

Existuje množstvo rôznych šifrovacích techník, ktoré boli zavedené pre tento účel. Jedna z týchto techník je popísaná v Európskej patentovej prihláške č.9030131.9 pod menom News Data Security Product Limited, ktorá popisuje bezkľúčový šifrovací proces, ktorý sa stal široko používaným vo Veľkej Británii ako súčasť systému VideoCrypt. Tento systém bude detailnejšie popísaný v nasledujúcej časti tohto popisu.

Tento vynález nie je obmedzený žiadnym utajovacím

spôsobom. V digitálnej televízii môžu byť v tomto utajení zahrnuté i audio a dátové signály. Pre ilustratívne účely bude v nasledujúcich príkladoch použitý spôsob "prerušenia & prehodenia". Obdobne, vynález nie je obmedzený žiadnym šifrovacím procesom pre vygenerovanie prerušovacích bodov. Pre ilustratívne účely bude v nasledujúcich príkladoch použitý proces VideoCrypt. Skúsení odborníci si ľahko predstavia aplikáciu patentových techník popísaných v tejto špecifikácii na iné spôsoby utajovania, ako je priame šifrovanie kódovaného signálu, rovnako ako na iné spôsoby šifrovacích procesov.

Ak sa prevádzateľ vysielača raz rozhodne používať zvláštny šifrovací proces, obecne tiež zmieňovaný ako "šifrovací systém", pre jednotlivý kanál, potom sa zaväzuje, že bude používať pre tento kanál len zmienený šifrovací systém. To je z toho dôvodu, aby sa tí, ktorí sa chcú dívať na tento kanál, mohli kúpiť "dekódovaciu" jednotku, ktorá vie dekódovať signály špecifické pre zmienený šifrovací systém. Bolo by nepraktické zavádzať nový šifrovací systém pre tento kanál, pretože to by vyžadovalo, aby si zavedení diváci nakúpili nové "dekódovacie" jednotky. Ak sa rozhodne prevádzateľ vysielača pre jediný šifrovací systém, môže to pre neho znamenať niektoré komerčné výhody, napr. ak má výhradné práva na šifrovací systém, potom ich iný prevádzatelia nemôžu využívať. Následne, ak sa diváci rozhodnú investovať do dekódovacej jednotky pre tento šifrovací systém, potom je nepravdepodobné, že si zakúpia druhú jednotku pre príjem kanálov iných prevádzateľov.

Ak by však jednotlivé utajené kanále boli kompatibilné s niekoľkými systémami, potom môže prevádzateľ vysielača dosiahnuť väčšiu pružnosť. Napr. rozsah jedného kanálu môže dobre pokrývať mnoho zemí; môže byť užitočné umožniť rozdelenie rozsahu podľa národných hraníc tak, že v rozdielnych zemiach budú zavedené rozdielne šifrovacie

systémy. Tiež paralelne so s prvšími verziami môžu byť použité dokonalejšie verzie šifrovacieho systému; toto umožní zavedenie nového systému bez toho aby sa starší dekódovací systém stal nepoužiteľný. Ďalej, počet potencionálnych divákov by narástol tak, aby zahrňoval všetkých divákov s dekodérmi kompatibilným so všetkými rôznymi šifrovacími systémami podporovanými jednotlivým šifrovaným kanálom.

Doteraz bolo považované za nemožné vytvorenie bezpečného spôsobu alebo prístroja pre vysielanie a prijímanie signálu, ktorý je kompatibilný s viac ako jedným šifrovacím systémom.

Podstata vynálezu

V súlade s prvým uskutočnením prvého hľadiska predstavovaného vynálezu predkladáme spôsob vysielania signálu kompatibilného s prvým, a druhým šifrovacím systémom, ktorý obsahuje nasledujúce kroky:

- prijatie obrazového signálu, ktorý má byť vysielaný;
- vygenerovanie druhej signálovej sady v prvom signálovom generátore v závislosti na prvom balíka dát;
- vygenerovanie druhej signálovej sady v druhom signálovom generátore v závislosti na druhom balíka dát;
- získanie rozdielového signálu vzájomným porovnaním prvej a druhej signálovej sady;
- utajenie obrazového signálu v závislosti na prvej signálovej sade a tým vygenerovanie utajeného obrazového signálu;
- dodanie nasledujúcich signálov kompatibilných s prvým šifrovacím systémom k vysielaniu: [1] utajeného obrazového signálu, [2] prvého balíka dát; a

- dodanie nasledujúcich signálov kompatibilných s druhým šifrovacím systémom k vysielaniu: [1] druhého balíka dát a [2] rozdielového signálu.

Pre vysielania, ktoré sú kompatibilné len s prvým šifrovacím systémom, t.j. konvenčný prístup, stačí vysielať len utajený obrazový signál spoločne s prvým balíkom dát. Často je prvý balík dát vysielaný v jednej sade riadkov intervalu snímkového zatemnenia alebo "VBI" (vertical blanking intervals). Často tieto dáta tvoria časť tzv. šifrovacích dát. Typicky bude takéto šifrovacie dáta prenášať len malý počet týchto riadkov, napr. osem alebo menej.

Pre vysielania, ktoré sú kompatibilné s druhým šifrovacím systémom, je vysielaný druhý balík dát spoločne s rozdielovým signálom. Zavedením rozdielového signálu je umožnené diváckemu dekodéru, kompatibilnému len s druhým šifrovacím systémom, spracovanie prvej signálovej sady; je to práve tento signál, ktorý je potrebný pre divácky dekodér; bol použitý pre utajovanie obrazového signálu a musí byť teda použitý v dekodéri, aby mohla byť uskutočnená operácia inverzná k utajovacej operácii.

Rozdielový signál môže byť odôvodnený z prvej a druhej signálovej sady mnohými rôznymi spôsobmi. Napr., ak označíme prvú signálovú sadu číslom A a druhú signálovú sadu číslom B, potom rozdielový signál je daný číslom [A-B]. To môžeme označiť ako číslo D. Druhá signálová sada môže byť pripočítaná k tomuto rozdielovému signálu D a tým vytvorí [A-B+B], ktoré je rovno A, t.j. prvej signálovej sade.

Skúsený odborník si predstaví mnoho rôznych prístupov pre získavanie rozdielového signálu, v ktorom nie všetky vyžadujú, aby rozdielový signál bol daný rozdielom dvoch čísiel, t.j. na výstupe odčítacieho procesu. Napr. rozdielový signál môže byť získaný aplikáciou operácie exkluzívnej OR [t.j.XOR] na prvú a druhú signálovú sadu.

Potom D = A XOR B. Druhá signálová sada potom môže byť kombinovaná s rozdielovým signálom D pomocou operácie D XOR B, ktorá vytvorí A XOR B XOR B, čo je rovno A, prvej signálovej sade. Pojem "rozdielový signál" sa vzťahuje na všetky signály, ktoré môžu byť použité v spojení s druhou signálovou sadou tak, aby reprodukovali prvú signálovú sadu, bez ohľadu na matematickú operáciu použitú pre ich odvodenie.

Konvenčne môžu byť pre prenos šifrovacích dát kompatibilných s druhým šifrovacím systémom a rozdielového signálu použité rôzne sady VBI riadkov. Preto je možné, aby jednotlivý kanál bol utajený podľa prvého šifrovacieho systému, potom vysielaný v jednej sade VBI riadkov so šifrovacími dátami kompatibilnými s prvým šifrovacím systémom a v ďalšej sade VBI riadkov so šifrovacími dátami kompatibilnými s druhým šifrovacím systémom. Diváci s dekodérom kompatibilným s prvým šifrovacím systémom môžu získať dáta z prvej sady VBI riadkov, zatiaľ čo diváci s dekodérom kompatibilným s druhým šifrovacím systémom môžu získať dáta z druhej sady VBI riadkov.

V uskutočnení druhého hľadiska predstavovaného vynálezu obsahuje spôsob prijímania vysielania z vysielača, utajeného podľa prvého šifrovacieho systému, nasledujúce kroky:

- prijatie [1] utajeného obrazového signálu, [2] druhého balíka dát a [3] rozdielového signálu;
- vygenerovanie signálovej sady z [1] druhého balíka dát a [2] z rozdielového signálu, kde táto signálová sada je zhodná s prvou signálovou sadou, odvodenou v súlade s prvým šifrovacím systémom a použitou pre utajenie obrazového signálu ešte pred vysielaním z vysielača;
- odtajenie utajeného obrazového signálu v závislosti na signálovej sade.

V jednom uskutočnení tohto hľadiska, ako je doložené na

príklade systému VideoCrypt, obsahuje prvá signálová sada primárne hodnoty vygenerované podľa prvého strihacieho algoritmu a dáta o prerušovaných bodoch vygenerované použitím týchto primárnych hodnôt ako počiatočných hodnôt pre generátor pseudo-náhodných binárnych sekvencií [PRBS] (pseudo-randon binary seguence). Táto prvá signálová sada je používaná v šifrovacom systéme VideoCrypt I. Druhá signálová sada obsahuje rozdielne primárne hodnoty vygenerované podľa druhého strihacieho algoritmu. Táto druhá signálová sada je použitá v ďalšom šifrovacom systéme, v systéme System X. Obidva systémy používajú zhodné PRBS. Podľa prvého hľadiska potom generátory signálov obsahujú strihacie algoritmy, ktoré generujú primárne hodnoty, a prvý signálový generátor tiež obsahuje generátor PRBS, ktorý generuje dáta o prerušovacích bodoch na základe vstupných primárnych hodnôt. Obecne, pre každý šifrovací systém sú použité rôzne strihacie algoritmy.

V tomto uskutočnení nie sú samotné primárne hodnoty vysielané. Miesto toho sú vysielané kontrolne signály, ktoré sú privádzané do strihacích algoritmov a z ktorých sú generované primárne hodnoty. Tie sa potom vo vysielaní objavujú aké sekvencie náhodných čísiel. Tieto kontrolne signály sa šifrovane vzťahujú k prvej a druhej signálovej sade, pretože prvá a druhá signálová sada sú tvorené, prinajmenšom čiastočne, z týchto kontrolných signálov pomocou činnosti strihacieho algoritmu. Obecne budú použité pre každý šifrovací systém rôzne kontrolne signály, aj keď to nie je nutné.

Podľa uskutočnenia ďalšieho hľadiska predstavovaného vynálezu je predložený prístroj pre vysielanie signálu kompatibilného s prvým a druhým šifrovacím systémom obsahujúci:

- vstup pre prijímanie obrazového signálu, ktorý môže byť vysielaný;

- prvý signálový generátor pre vygenerovanie prvej signálovej sady v závislosti na prvom balíka dát;
- druhý signálový generátor pre vygenerovanie druhej signálovej sady v závislosti na druhom balíka dát;
- porovnávacie zariadenie pre získavanie rozdielového signálu vzájomným porovnaním prvej a druhej signálovej sady;
- utajovač pre utajenie obrazového signálu v závislosti na prvej signálovej sade a tým pre vygenerovanie utajeného obrazového signálu;
- výstup dodávajúci k vysielaniu nasledujúce signály kompatibilné s prvým šifrovacím systémom: [1] utajený obrazový signál, [2] prvý balík dát; a
- výstup dodávajúci k vysielaniu nasledujúce signály kompatibilné s druhým šifrovacím systémom: [1] druhý balík dát a [2] rozdielový signál.

Vo zvláštnom uskutočnení tohto kódovacieho zariadenia môžu byť začlenené generátory prvého a druhého signálu, celé alebo čiastočne umiestnené na zvláštnych moduloch, ktoré sú vybrateľné zo zariadenia. Typicky môžu byť tieto moduly tvorené prenosnými elektronickými zariadeniami vo forme malých kariet. Podľa uskutočnenia ďalšieho hľadiska predstavovaného vynálezu je zavedená malá karta obsahujúca signálový generátor tohto zariadenia.

Prehľad obrázkov na výkresoch

Vynález bude teraz detailnejšie popísaný pomocou príkladu s odkazom na pripojené výkresy na ktorých predstavuje obr.1 schematické zobrazenie prístroja pre vysielanie signálu zahrňujúce predstavovaný vynález, a obr.2 schematické zobrazenie prístroja pre prijímanie signálov zahrňujúce predstavovaný vynález.

Príklady uskutočnenia vynálezu

Teraz sa budeme zaoberať obr.1, ktorý predstavuje schematické zobrazenie prístroja pre vysielanie signálov. Takže, obr.1 ukazuje v zjednodušenej schematickej forme kódovacie zariadenie pre dva šifrovacie systémy VideoCrypt I a System X. V popise je obecne zamýšľané, že utajovanie pokrýva spracovanie analógových a digitálnych televíznych signálov. Novšie je tento termín obecne nazývaný šifrovanie (encryption).

Systém VideoCrypt I je obecnejšie popísaný V európskej patentovej prihláške č.9030131.9 pod menom News Data Security Products Limited, na ktorý sa tiež odkazujeme. Hlavnými rozdielmi medzi systémom popísaným v tejto prvšej prihláške a v predstavovanej špecifikácii je to, že predstavovaná prihláška umožňuje odtajenie jedného utajovaného signálu dvoma šifrovacími systémami.

Ak sa vrátime k obr.1, je tu zobrazený generátor balíka dát 10. Tento balík dát obsahuje malý balík, balík primárnych hodnôt a náhodné čísla. Podrobný popis funkcie týchto balíkov je mimo rámec tejto špecifikácie. Balík dát systému VideoCrypt I, je vyslaný do strihacieho algoritmu 11 systému VideoCrypt I, ktorý vygeneruje výstup nazývaný primárna hodnota 12. Táto primárna hodnota je potom použitá ako začiatočná hodnota pre generátor PRBS 13, ktorý generuje prerušovacie body. Strihací algoritmus predstavuje najtajnejšiu časť systému; vytvára daný výstup pre daný vstup, avšak bez vzájomného vzťahu medzi týmito dvoma. Obvykle je obsiahnutý na malej karte dodanej užívateľovi, skôr ako by bol súčasťou samotného kódovacieho zariadenia. Také usporiadanie, spoločne s komunikačnými spojmi medzi malou kartou a ďalšími prvkami prístroja, sú kompletnejšie popísané v Európskej patentovej prihláške č.9030131.9.

Balík dát 10 je pravidelne znovu posielaní do

strihacieho algoritmu 11 systému VideoCript I, čím je zaistené, že sú stále generované nové primárne hodnoty. Pretože každý balík dát obsahuje náhodné sekvencie čísiel, každý balík dát bude rozdielny od predchádzajúceho balíka dát, a nasledovne každá primárna hodnota 12 bude rôzna. Typicky bude nová primárna hodnota vygenerovaná každých niekoľko sekúnd alebo častejšie. Takže zo strihacieho algoritmu 11 systému VideoCrypt I je získavaný často sa meniaci výstup primárnych hodnôt 12.

Primárne hodnoty sú privádzané do generátora pseudo-náhodných binárnych sekvencií 13. Generátor PRBS 13 používa každú vstupnú primárnu hodnotu ako počiatočnú hodnotu pre náhodnú sekvenciu čísiel; nasledovne jednotlivá vstupná počiatočná hodnota vedie k rýchle a náhodne sa meniacu sekvenciu výstupných čísiel. Tieto výstupné čísla sú použité pre definovanie polôh prerušovacích bodov pre každý nasledujúci obrazový riadok neutajeného televízneho signálu riadením jednotky pre aktívnu rotáciu riadkov 14, ktorá vykonáva skutočné utajenie typu "prerušenie & prehodenie" každého takého nasledujúceho obrazového riadku video signálu 15. Výstupom jednotky pre aktívnu rotáciu riadkov 14 je utajený obrazový signál 16. Tento signál je vedený z kódovacieho zariadenia k vonkajšiemu vysielaniu cez zlučovač 17.

Pretože nové primárne hodnoty sú vybavované každých niekoľko sekúnd alebo častejšie, generátor PRBS je v reakcii reštartovaný každých niekoľko sekúnd alebo častejšie; toto má určité výhody, ako zaistenie synchronizácie a to, že po vyladení utajeného kanálu sú rýchle získané informácie potrebné pre odtajenie.

Ďalej je zobrazený generátor balíka dát 20 pre System X. Tento balík dát zase obsahuje malý balík, balík primárnych hodnôt a náhodné čísla. Dátový balík System X je poslaný do strihacieho algoritmu 21 systému System X, ktorý

vygeneruje druhý výstup primárnych hodnôt 22. Rovnako ako u balíka dát systému VideoCrypt I, druhý balík dát je pravidelne znovu-posielaný do strihacieho algoritmu 21 systému System X, čím je zaistené stále generovanie nových primárnych hodnôt. Zase, pretože každý balík dát bude rozdielny od predchádzajúceho balíka dát, a nasledovne každá primárna hodnota bude rozdielna. Typicky bude nová primárna hodnota 22 vygenerovaná každých niekoľko sekúnd alebo častejšie. Takže zo strihacieho algoritmu 21 systému System X je zase získavaný často sa meniaci výstup primárnych hodnôt 22.

Primárne hodnoty 12, 22 sú privádzané do porovnávacieho zariadenia 24, ktoré určuje rozdiel primárnych hodnôt 12, 22. Výstupom porovnávacieho zariadenia 24 je rozdielový signál 25. Rozdielový signál môže byť odôvodnený z prvej a druhej signálovej sady mnoho rôznymi spôsobmi. Napr., ak je primárna hodnota 12 daná číslom A a primárna hodnota 22 číslom B, potom rozdielovým signálom 25 je číslo [A-B]. To môžeme označiť ako číslo D. Primárna hodnota 38 B môže byť pripočítaná k rozdielovému signálu D a tým získame [A-B+B], čo je rovno A, primárnej hodnote 12.

Skúsený odborník si predstaví mnoho rôznych prístupov ako získať rozdielový signál, z ktorých nie všetky vyžadujú, aby rozdielový signál 25 bol rozdielom dvoch čísiel, t.j. na výstupe odčítacieho procesu. Rozdielový signál môže byť získaný napr. pomocou operácie exkluzívnej OR [XOR] aplikovanej na dve primárne hodnoty 22 a 12. Potom D = A XOR B. Primárna hodnota 22 potom môže byť kombinovaná s rozdielovým signálom 25 D pomocou operácie D XOR B, čo vytvorí A XOR B XOR B, a to je rovno A, t.j. primárnej hodnote 12. Existujú iste ďalšie možnosti, ktoré budú jasné odborníkom v tomto odbore.

Posledným krokom pre kódovacie zariadenie je dodanie nasledujúcich signálov na výstup k vysielaniu: [1] utajeného

obrazového signálu 16 a [2] balíka dát 10 systému VideoCrypt I neseného sadou riadkov VBI (intervalov snímkového zatemnenia) pridelených systému VideoCrypt I. Paralelne s tým produkuje kódovacie zariadenie na výstupu tiež nasledujúce signály nesené rôznymi sadami VBI riadkov pridelených systému System X: [1] balík dát 20 systému System X a [2] rozdielový signál 25. Toto je uskutočnené v zmešovači 17 predtým, ako sú signály vyslané.

Obr.2 obsahuje schematické zobrazenie prístroja pre prijímanie signálov systému System X podľa predstavovaného vynálezu. Tento prístroj je obecne dodávaný ako jedna jednotka a často je zmieňovaný ako "integrovaný prijímač/dekodér" alebo "IRD" (Integrated Receiver/Decoder). Je možné mať oddelený prijímač a dekodér, ale toto uskutočnenie tu nebolo popísané. IRD 30 systému System X je napojený nasledujúcimi RF signálmi z parabolickej antény pomocou vedenia 32:

[1] utajeným obrazovým signálom, ktorý je utajený podľa systému VideoCrypt I;

[2] balíkom dát systému System X; a

[3] rozdielovým signálom 25.

Prijímač 32 v IRD 30 zaisťuje, aby tieto RF signály boli riadne vyladené, a potom vyšle balík dát 20 systému System X a rozdielový signál 25 do jednotky pre odvodenie dát 34. Jednotka pre odvodenie dát odvodí a oddelí balík dát 20 systému System X a rozdielový signál 25 od utajeného video signálu, a potom ho pošle do overovacej jednotky 35. Overovacia jednotka 35 vykoná výpočty kontrolných súčtov, aby zistila prípadné prenosové chyby, a potom pošle balík dát 20 systému System X a rozdielový signál 25 do malej karty 36. Malá karta 36 obsahuje strihací algoritmus systému System X 37, ktorý je zhodný so strihacím algoritmom systému System X 21 na malej karte nachádzajúci sa v kódovacom zariadení. Strihací algoritmus systému System X produkuje na

výstupe primárne hodnoty 38.

Malá karta tiež obsahuje zlučovací obvod 39, ktorý vykonáva inverznú operáciu k tej, ktorá vykonáva porovnávacie zariadenie 24 v kódovacom zariadení; konkrétne na vstupu spracováva primárne hodnoty z vstupu 38 strihacieho algoritmu systému System X 37 a rozdielový signál 25 a z nich generuje výstupné primárne hodnoty 40. Výstupná primárna hodnota je zhodná s primárnou hodnotou 12 systému VideoCrypt I. Potom je vedená do generátora pseudo-náhodných binárnych sekvencií 41, ktorý je zhodný s generátorom PRBS 13 v kódovacom zariadení. Nasledovne generátor PRBS 41 vygeneruje ako výstupné čísla prerušovacie body 42, ktoré sú presne rovnaké ako prerušovacie body vygenerované v kódovacom zariadení: tieto sú vedené do jednotky pre aktívnu rotáciu riadkov 43 [ALR], ktorá je zhodná s ALR v kódovacom zariadení. Jednotka ALR je preto schopná prerušiť každý utajený riadok, prijatý ako video vstup 44, v presne zhodnom bode, v ktorom bol pôvodne prerušený neutajený riadok, a potom preusporiadať riadok do jeho pôvodného neutajeného stavu. Na výstupu 45 je potom produkovaný neutajený obrazový signál.

Je jasné, že vyššie popísaný systém môže byť použitý i opačne. To uvádzame preto, aby bolo jasné, že môže byť použitý pre dekódovanie signálu šifrovaného v systéme System X z prvého balíka dát a z rozdielového signálu.

Vynález môže byť použitý tiež tam, kde sú vysielania k lokálnym vysielačom uskutočnené v prvom šifrovacom systéme a ďalšie vysielania, t.j. napr. po kábelovom vedení, sú uskutočnené v druhom šifrovacom systéme. V lokálnych vysielačoch potom druhé balíky dát a rozdielový signál musí byť len vyslaný s utajeným obrazovým signálom. Prijímače sú potom schopné získať prerušované body z prvého šifrovacieho systému a tým dekódovať obraz.

Vynález nie je obmedzený len na šifrovanie televíznych

signálov a môže byť použití v akomkoľvek šifrovacom systéme, kde je vyžadovaná bezpečnosť a kompatibilita.

UPRAVENÉ PATENTOVÉ NÁROKY

1. Spôsob vysielania signálu kompatibilného s prvým a druhým šifrovacím systémom, vyznačujúci sa tým, že obsahuje nasledujúce kroky:
   - prijatie obrazového signálu, ktorý má byť vysielaný;
   - vygenerovanie prvej signálovej sady v prvom signálovom generátore v závislosti na prvom balíku dát;
   - vygenerovanie druhej signálovej sady v druhom signálovom generátore v závislosti na druhom balíku dát;
   - získanie rozdielového signálu vzájomným porovnaním prvej a druhej signálovej sady;
   - zašifrovanie obrazového signálu v závislosti na prvej signálovej sade a tým vygenerovanie šifrovaného obrazového signálu;
   - dodanie nasledujúcich signálov kompatibilných s prvým šifrovacím systémom k vysielaniu: [1] utajeného obrazového signálu, [2] prvého balíka dát; a
   - dodanie nasledujúcich signálov kompatibilných s druhým šifrovacím systémom k vysielaniu: [1] druhého balíka dát a [2] rozdielového signálu.

2. Prístroj pre vysielanie signálu kompatibilného s prvým a druhým šifrovacím systémom, vyznačujúci sa tým, že obsahuje:
   - vstup pre prijímanie obrazového signálu, ktorý má byť vysielaný;
   - prvý signálový generátor pre vygenerovanie prvej signálovej sady v závislosti na prvom balíku dát;
   - druhý signálový generátor pre vygenerovanie druhej signálnej sady v závislosti na druhom balíku dát;
   - porovnávacie zariadenie pre získavanie rozdielového

signálu vzájomným porovnávaným prvej a druhej signálovej sady;
- šifrovacie zariadenie pre zašifrovanie obrazového signálu v závislosti na prvej signálovej sade a tým pre vygenerovanie šifrovaného obrazového signálu;
- výstup dodávajúci k vysielaniu nasledujúce signály kompatibilné s prvým šifrovaným systémom: [1] šifrovaný neusporiadaný obrazový signál, [2] prvý balík dát; a
- výstup dodávajúci k vysielaniu nasledujúce signály kompatibilné s druhým šifrovaným systémom: [1] druhý balík dát a [2] rozdielový signál.

3. Spôsob podľa nároku 1, vyznačujúci sa tým, že prvý balík dát je vysielaný v jednej sade riadkov intervalov snímkového zatemnenia a druhý balík dát je vysielaný v inej sade riadkov intervalov snímkového zatemnenia.

4. Spôsob podľa nároku 1 alebo 3, vyznačujúci sa tým, že prvá signálová sada obsahuje primárne hodnoty vygenerované prvým strihacím algoritmom spracovávajúcim prvý balík dát a prvý signálový generátor obsahuje program so strihacím algoritmom, ktorý generuje primárne hodnoty.

5. Spôsob podľa nároku 4, vyznačujúci sa tým, že druhá signálová sada obsahuje rozdielne primárne hodnoty vygenerované druhým strihacím algoritmom spracovávajúcim druhý balík dát a druhý signálový generátor obsahuje program so strihacím algoritmom, ktorý generuje tieto primárne hodnoty.

6. Spôsob podľa nároku 4, vyznačujúci sa tým, že rozdielový signál je získaný porovnaním primárnych

hodnôt prvej a druhej riadiacej signálovej sady.

7. Prístroj podľa nároku 2, vyznačujúci sa tým, že prvý balík dát je vysielaný v jednej sade riadkov intervalov snímkového zatemnenia a druhý balík dát je vysielaný v inej sade riadkov intervalov snímkového zatemnenia.

8. Prístroj podľa nároku 2 alebo 6, vyznačujúci sa tým, že prvá signálová sada obsahuje primárne hodnoty vygenerované prvým strihacím algoritmom spracovávajúcim prvý balík dát a prvý signálový generátor obsahuje program so strihacím algoritmom, ktorý generuje primárne hodnoty.

9. Prístroj podľa nároku 8, vyznačujúci sa tým, že druhá signálová sada obsahuje rozdielne primárne hodnoty vygenerované druhým strihacím algoritmom spracovávajúcim druhý balík dát a druhý signálový generátor obsahuje program so strihacím algoritmom, ktorý generuje tieto primárne hodnoty.

10. Prístroj podľa nároku 9, vyznačujúci sa tým, že rozdielový signál je získaný porovnaním primárnych hodnôt prvej a druhej riadiacej signálovej sady.

11. Malá karta, vyznačujúca sa tým, že obsahuje prvý a/alebo druhý signálový generátor podľa ľubovoľného z nárokov 2 a 7-10.

12. Spôsob prijímania signálu, ktorý je šifrovaný podľa prvého šifrovacieho systému s prvou signálovou sadou odvodenou z prvého balíka dát, vyznačujúci sa tým, že obsahuje nasledujúce kroky:
- prijatie [1] šifrovaného obrazového signálu, [2]

druhého balíka dát a [3] rozdielového signálu týkajúceho sa rozdielu medzi prvými a druhými balíkmi dát;

- vygenerovanie signálovej sady z [1] druhého balíka dát a [2] z rozdielového signálu, pričom táto signálová sada je zhodná s prvou signálovou sadou, odvodenou podľa prvého šifrovacieho systému a použitou pre šifrovanie obrazového signálu ešte pred vysielaním z vysielača;
- dekódovanie šifrovaného signálu v závislosti na zmienenej signálovej sade.

13. Prístroj pre prijímanie signálu, ktorý je šifrovaný podľa prvého šifrovacieho systému s prvou signálovou sadou odvodenou z prvého balíka dát, vyznačujúci sa tým, že obsahuje:

- vstup pre prijímanie [1] šifrovaného obrazového signálu, [2] druhého balíka dát a [3] rozdielového signálu týkajúceho sa rozdielu medzi prvými a druhými balíkmi dát;
- signálový generátor prispôsobený pre vygenerovanie signálovej sady z [1] druhého balíka dát a [2] z rozdielového signálu, pričom táto signálová sada je zhodná s prvou signálovou sadou, odvodenou podľa prvého šifrovacieho systému a použitou pre šifrovanie obrazového signálu ešte pred vysielaním z vysielača;
- dekódovacie zariadenie prispôsobené pre dekódovanie šifrovaného signálu v závislosti na zmienenej signálovej sade, ktorá je zhodná s prvou signálovou sadou.

14. Prístroj podľa nároku 9, vyznačujúci sa tým, že signálový generátor obsahuje strihací algoritmus špecifický pre druhý šifrovací systém v tom, že keď sú

na vstup takého šifrovacieho algoritmu privedené druhé riadiace signály, vygeneruje sekvencie primárnych hodnôt.

15. Prístroj podľa nároku 12, vyznačujúci sa tým, že signálový generátor vykonáva kombinovanie sekvencií primárnych hodnôt vygenerovaných strihacím algoritmom špecifickým pre druhý šifrovací systém s rozdielovým signálom, čo vedie k získaniu ďalších primárnych hodnôt, ktoré sú zhodné so sekvenciou primárnych hodnôt prvej signálovej sady, a ďalej vedie tieto ďalšie primárne hodnoty do generátora pseudo-binárnych sekvencií, kde sú vygenerované sekvencie prerušovacích bodov zhodné so sekvenciami prerušovacích bodov prvej signálovej sady.

16. Malá karta obsahujúca signálový generátor prístroja podľa nároku 15, vyznačujúca sa tým, že signálový generátor je upravený tak, aby generoval primárne hodnoty s použitím programu so strihacím algoritmom a kombinoval tieto primárne hodnoty s rozdielovým signálom, čo vedie k získaniu ďalších primárnych hodnôt, ktoré sú zhodné so sekvenciou primárnych hodnôt prvej signálovej sady.

17. Spôsob šifrovania signálu tak, aby bol kompatibilný s prvým a druhým šifrovacím/dekódovacím systémom, vyznačujúci sa tým, že obsahuje nasledujúce kroky:
- prijatie signálu, ktorý má byť vysielaný;
- vygenerovanie prvého a druhého šifrovacieho dátového signálu, vzťahujúceho sa k prvému a druhému šifrovaciemu/dekódovaciemu systému;
- zašifrovanie signálu v závislosti na prvých šifrovacích dátach;

- získanie rozdielového signálu z prvého a druhého šifrovacieho dátového signálu; a
- dodanie šifrovaného signálu, prvého a druhého šifrovacieho dátového signálu a rozdielového signálu na výstup.

18. Spôsob prijímania a dekódovania signálu šifrovaného podľa prvého šifrovacieho/dekódovacieho systému, vyznačujúci sa tým, že obsahuje nasledujúce kroky:
- prijatie šifrovaného signálu;
- prijatie šifrovacích dát vzťahujúcich sa na druhý šifrovací/dekódovací systém;
- prijatie rozdielového signálu;
- odvodenie šifrovacích dát vzťahujúcich sa na prvý šifrovací/dekódovací systém z prijatých šifrovacích dát a z rozdielového signálu; a
- dekódovanie šifrovaného signálu v závislosti na takto odvodených šifrovacích dátach.

19. Prístroj pre prijímanie a dekódovanie signálu šifrovaného podľa prvého šifrovacieho/dekódovacieho systému, vyznačujúci sa tým, že obsahuje:
- prostriedky pre prijímanie šifrovaného signálu;
- prostriedky pre prijímanie šifrovacích dát vzťahujúcich sa na druhý šifrovací/dekódovací systém a pre prijímanie rozdielového signálu;
- prostriedky pre odvodzovanie šifrovacích dát vzťahujúcich sa na prvý šifrovací systém z prijatých šifrovacích dát a z rozdielového signálu; a
- prostriedky pre dekódovanie šifrovaného signálu v závislosti na takto odôvodnených šifrovacích dátach.

20. Prístroj pre šifrovanie signálu tak, aby bol

kompatibilným s prvým a druhým šifrovacím/dekódovacím systémom, vyznačujúci sa tým, že obsahuje:

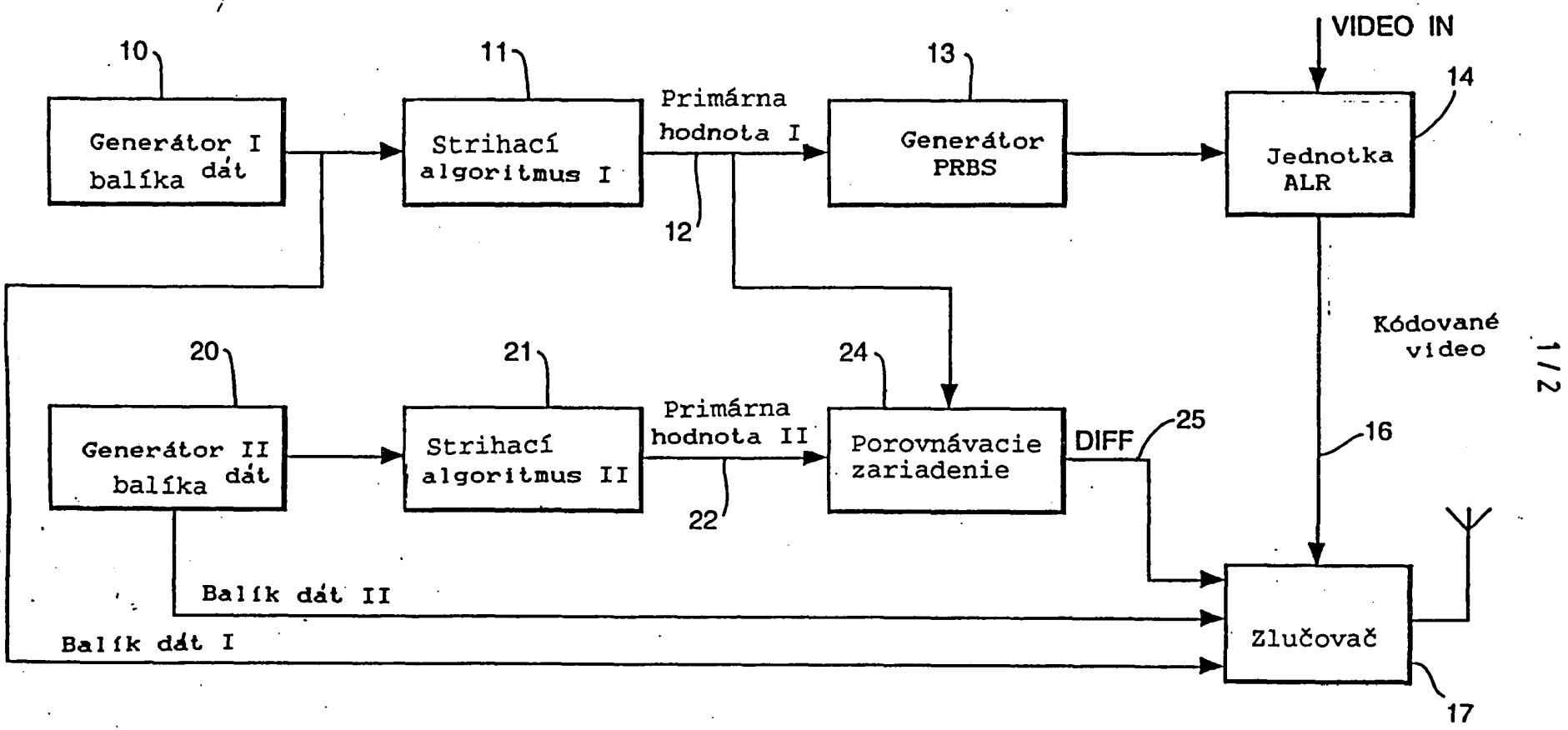
- prostriedky pre vygenerovanie prvého a druhého šifrovacieho dátového signálu vzťahujúceho sa na prvý a druhý šifrovací/dekódovací systém;
- prostriedky pre šifrovanie signálu v závislosti na prvom šifrovacom dátovom signáli;
- prostriedky pre odvodzovanie rozdielového signálu z prvého a druhého dátového signálu; a
- výstupné prostriedky pre šifrovaný signál, prvý a druhý šifrovací dátový signál a pre rozdielový signál.

21. Prenosné elektronické zariadenie pre použitie v prístroji pre prijímanie a dekódovanie signálov šifrovaných podľa prvého šifrovacieho/dekódovacieho systému, vyznačujúce sa tým, že obsahuje:

- prostriedky pre prijímanie šifrovacích dát vzťahujúcich sa na druhý šifrovací/dekódovací systém a pre prijímanie rozdielového signálu; a
- prostriedky pre odvodzovanie šifrovacích dát, vzťahujúcich sa na prvý šifrovací/dekódovací systém, z prijatých šifrovacích dát a z rozdielového signálu.

22. Malá karta vyznačujúca sa tým, že obsahuje zariadenie podľa nároku 21.

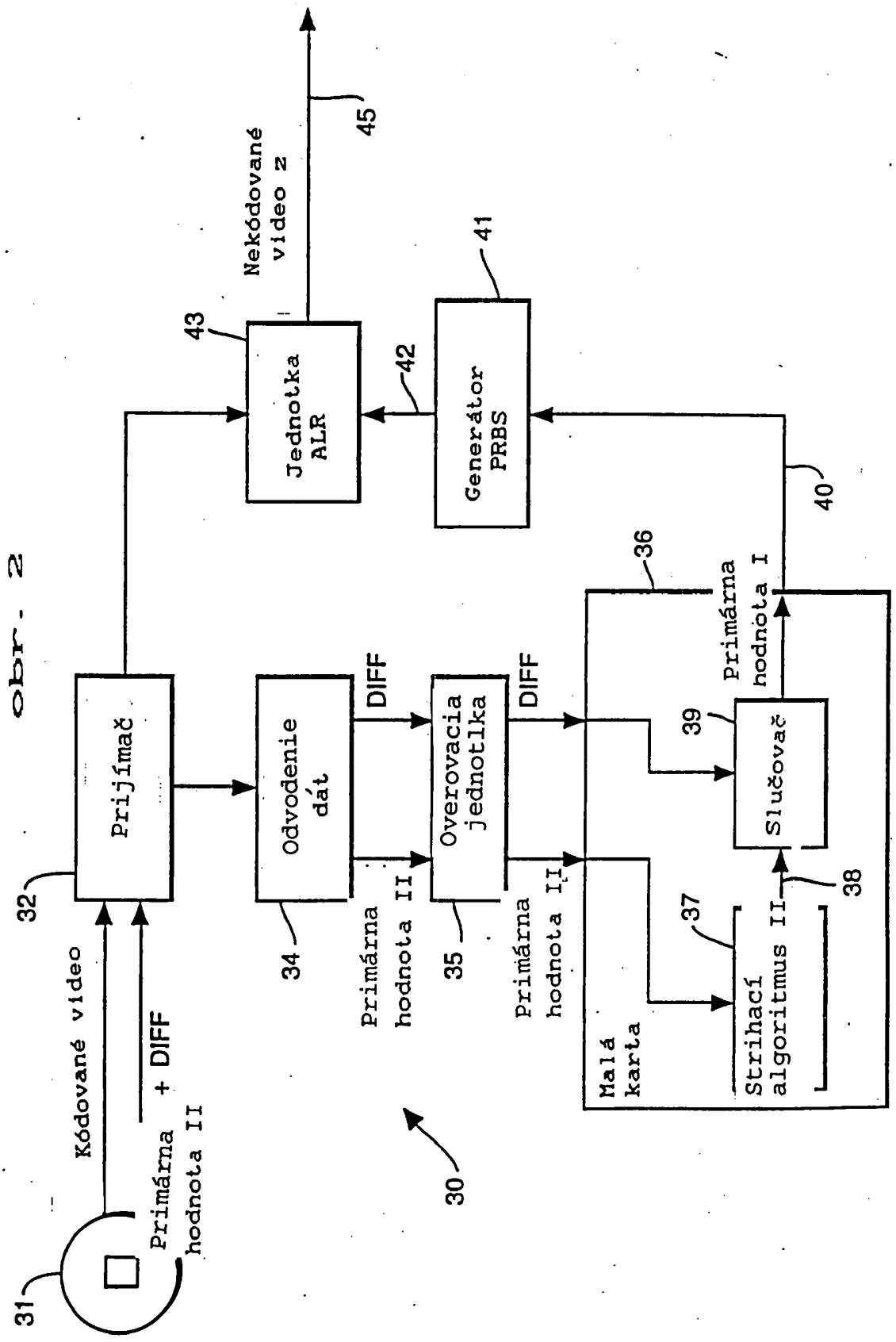
obr. 1



1/2

PV 1285-96

PV 1285-96



obr. 2