(12) Patentskrift (10) SE 534 208 C2

Sverige

(21) Patentansökningsnummer: 0700601-8
(45) Patent meddelat: 2011-05-31
(41) Ansökan allmänt tillgänglig: 2007-09-16
(22) Patentansökan inkom: 2007-03-13
(24) Löpdag: 2007-03-13
(83) Deposition av mikroorganism: ---
(30) Prioritetsuppgifter: 2006-03-15 US 11/377082

(51) Internationell klass:
H04L 9/32 (2006.01)
G06F 21/24 (2006.01)

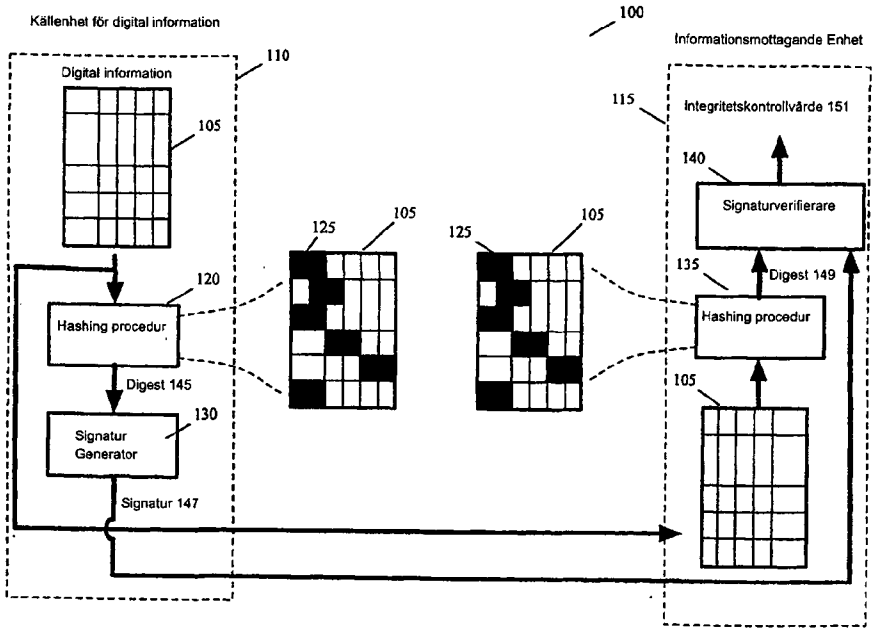
(73) Patenthavare: Apple Inc, M/S 38-PAT 1 Infinite Loop, Cupertino CA 95014 US
(72) Uppfinnare: Augustin J Farrugia, Cupertino CA 95014 US
Jean-Francois Riendeau, Cupertino CA 95014 US
(74) Ombud: Hynell Patenttjänst AB, Box 138, 683 23 Hagfors SE

(54) Benämning: Optimerade förfaranden för integritetsverifiering

(56) Anförda publikationer: EP 1496419 A1 • EP 0328232 B1 • US 20030131239 A1

(47) Sammandrag:

En del utföringsformer av uppfinningen tillhandahåller en metod för verifiering av integriteten för digital information. Vid en källa till den digitala informationen genererar metoden en signatur för den digitala informationen genom att applicera en hashing-funktion till en speciell del av den digitala informationen, varvid den speciella delen är mindre än den totala digitala informationen. Metoden förser en enhet med signaturen och den digitala informationen. I enheten applicerar metoden hashing-funktionen på den speciella delen av den digitala informationen för att verifiera den överförda signaturen och därmed verifiera integriteten för den överförda digitala informationen.



SAMMANDRAG AV UPPFINNINGEN

En del utföringsformer av uppfinningen tillhandahåller en metod för verifiering av integriteten för digital information. Vid en källa till den digitala informationen genererar metoden en signatur för den digitala informationen genom att applicera en hashing-funktion till en speciell del av den digitala informationen, varvid den speciella delen är mindre än den totala digitala informationen. Metoden förser en enhet med signaturen och den digitala informationen. I enheten applicerar metoden hashing-funktionen på den speciella delen av den digitala informationen för att verifiera den överförda signaturen och därmed verifiera integriteten för den överförda digitala informationen.

OPTIMERADE FÖRFARANDEN FÖR INTEGRITETSVERIFIERING

TEKNISKT OMRÅDE

Den föreliggande uppfinningen avser optimerade förfaranden för integritetsverifiering.

TEKNIKENS STÅNDPUNKT

Skyddet av digitala data överförda mellan datorer över ett nätverk är fundamentalt viktigt för många företag idag. Företag försöker åstadkomma detta skydd genom implementering av någon form av Digital Rights Management (DRM) förfarande. DRM förfarandet innefattar ofta kryptering av informationen (t.ex. kryptering av den binära formen av informationen) för att begränsa användningen till de personer som har fått tillstånd att utnyttja densamma.

Kryptering är den traditionella metoden för att skydda digital information, som t.ex. data, under överföring i ett nätverk. I sin typiska applikation skyddar kryptering digital information från stöld genom attack mot data under överföring mellan två parter med ömsesidigt förtroende. För många applikationer av digital filöverföring idag (t.ex. för överföring av audio eller video information) har emellertid paradigmet förskjutits, eftersom en part som mottager informationen (det vill säga "den mottagande parten") kanske försöker att knäcka DRM krypteringen som parten som tillhandahöll informationen (det vill säga den "sändande parten") har applicerat på informationen. Med spridningen av nätverksattacker kan dessutom en tredje part få tillgång till den mottagande partens dator och således till den skyddade informationen.

Utöver kryptering och dekryptering kan digital information behöva andra skyddsskikt. Äkthetsbevisning är ett annat viktigt skyddsskikt. Vid mottagandet av digital information behöver ofta mottagaren "verifiera" källan till den digitala informationen. Med andra ord, behöver mottagaren verifiera integriteten för den digitala informationen genom att försäkra sig om att informationen kom från en äkthetsbevisad källa och inte manipulerats på sin väg till mottagaren.

Till idag har ett antal förfaranden för verifiering av integriteten för digital information föreslagits. Dessa förfaranden applicerar typiskt en hashing-funktion till textversionen av informationen för att åstadkomma en hash-digest (också kallad en hash eller en digest), vilken sedan utnyttjas för att generera en signatur för informationen. En fundamental egenskap för alla "hash-funktioner" är att om två "hasher" är olika så var

de två ingångsdata olika i något avseende. När två "hasher" är identiska för två olika ingångsdata, föreligger en hash-kollision. Det är viktigt i ett krypteringssystem att hash-funktionen har mycket låg kollisionssannolikhet.

Traditionella förfaranden för integritetsverifiering är beräkningsintensiva, speciellt för portabla enheter med begränsade beräkningsresurser. Det finns av den anledningen ett behov inom denna teknik av ett förfarande för integritetsverifiering, som är mindre beräkningsintensivt. Det vore idealiskt om en sådan process tillät en portabel enhet att snabbt verifiera integriteten av en digital information som den mottager.

SAMMANFATTNING AV UPPFINNINGEN

Några utföringsformer av uppfinningen tillhandahåller en metod för verifiering av integriteten hos en digital information. Vid en källa till den digitala informationen genererar metoden en signatur för den digitala informationen genom att applicera en hashing-funktion till en speciell del av den digitala informationen, varvid den speciella delen är mindre än den totala digitala informationen. Metoden förser en enhet med signaturen och den digitala informationen. I enheten applicerar metoden hashing-funktionen på den speciella delen av den digitala informationen för att verifiera integriteten för den överförda signaturen och därmed verifiera integriteten för den överförda digitala informationen.

Den speciella delen av den digitala informationen inkluderar flera olika sektioner av den digitala informationen. I några utföringsformer konfigurerar metoden källan och enheten för att utvälja en förutbestämd uppsättning av sektioner av den digitala informationen som den speciella delen av den digitala informationen. Enheten inkluderar i några utföringsformer ett read-only minne som (1) lagrar kod för identifiering av den speciella delen, och (2) lagrar hashing-funktionen.

I några utföringsformer genererar metoden en signatur för den digitala informationen vid källan genom att (1) applicera hashing-funktionen på den speciella delen för att generera en hash digest, och sedan (2) generera signaturen från hash digesten. Metoden kan implementeras i antingen ett asymmetriskt eller symmetriskt förfarande för integritetsverifiering. I några utföringsexempel applicerar metoden till exempel hashing funktionen vid enheten genom att (1) applicera hashing funktionen på den speciella delen för att generera en hash digest, och (2) överföra digesten och den mottagna signaturen till en signaturverifierande process som bestämmer autenticiteten för signaturen baserat på den tillhandahållna digesten. I några utföringsexempel applicerar

metoden alternativt hashing funktionen vid enheten genom att (1) generera en andra signatur baserad på hash digesten, och (2) jämföra de första och andra signaturerna för att bestämma integriteten för den överförda digitala informationen.

Källan till den digitala informationen kan vara olika i olika utföringsexempel. Till exempel kan källan vara informationens upphovsman, distributör, etc. Enheten som mottager den digitala informationen kan också vara olika i olika utföringsformer. Exempel på en sådan enhet inkluderar en portabel audio/video spelare (t.ex. iPod), en laptop, en mobiltelefon, etc. Den digitala informationen kan också vara olika i olika utföringsformer. Den digitala informationen kan t.ex. vara firmware-updateringar till operativsystemet för enheten, tredje-part applicationer för att köras på enheten, audio/video filer för att spelas på enheten etc.

FIGURBESKRIVNING

Uppfinningens nya egenskaper framgår av de bifogade kraven. För en närmare förklaring beskrives emellertid ett flertal utföringsformer i de följande figurerna.

Figur 1 visar ett system för integritetsverifiering enligt några utföringsformer av uppfinningen.

Figur 2 visar ett annat system för integritetsverifiering enligt några utföringsformer av uppfinningen.

Figur 3 visar ett DRM system som implementerar systemet för integritetsverifiering enligt några utföringsformer av uppfinningen.

Figur 4 visar ett förfarande för integritetsverifiering som utföres med hjälp av en eller flera DRM servrar i några utföringsformer av uppfinningen.

Figur 5 visar ett förfarande för integritetsverifiering som utföres med hjälp av en portabel multimediaenhet i några utföringsformer av uppfinningen.

Figur 6 visar ett diagram för ett datorsystem som konceptuellt illustrerar komponenterna i en typisk DRM server, användardator eller portabel enhet implementerande några utföringsformer av uppfinningen.

DETALJERAD BESKRIVNING AV UPPFINNINGEN

I den följande beskrivningen kommer ett antal detaljer att tas med för att underlätta förklaringen. Fackmannen inser emellertid att uppfinningen kan utföras utan användning av dessa speciella detaljer. I andra fall visas välkända strukturer och enheter i form av blockdiagram för att inte belasta beskrivningen av uppfinningen med onödiga detaljer.

I. ÖVERSIKT

Några utföringsformer av uppfinningen tillhandahåller en metod för verifiering av integriteten hos en digital information. Vid en källa till den digitala informationen genererar metoden en signatur för den digitala informationen genom att applicera en hashing-funktion till en speciell del av den digitala informationen, varvid den speciella delen är mindre än den totala digitala informationen. Metoden förser en enhet med signaturen och den digitala informationen. I enheten applicerar metoden hashing-funktionen på den speciella delen av den digitala informationen för att verifiera integriteten för den överförda signaturen och därmed verifiera integriteten för den överförda digitala informationen.

Den speciella delen av den digitala informationen inkluderar flera olika sektioner av den digitala informationen. I några utföringsformer konfigurerar metoden källan och enheten för att utvälja en förutbestämd uppsättning av sektioner av den digitala informationen som den speciella delen av den digitala informationen. Enheten inkluderar i några utföringsformer ett read-only minne som (1) lagrar kod för identifiering av den speciella delen, och (2) lagrar hashing-funktionen.

I några utföringsformer genererar metoden en signatur för den digitala informationen vid källan genom att (1) applicera hashing-funktionen på den speciella delen för att generera en hash digest, och sedan (2) generera signaturen från hash digesten. Metoden kan implementeras i antingen ett asymmetriskt eller symmetriskt förfarande för integritetsverifiering. I några utföringsexempel applicerar metoden till exempel hashing funktionen vid enheten genom att (1) applicera hashing funktionen på den speciella delen för att generera en hash digest, och (2) överföra digesten och den mottagna signaturen till en signaturverifierande process som bestämmer autenticiteten för signaturen baserat på den tillhandahållna digesten. I några utföringsexempel applicerar metoden alternativt hashing funktionen vid enheten genom att (1) generera en andra signatur baserad på hash digesten, och (2) jämföra de första och andra signaturerna för att bestämma integriteten för den överförda digitala informationen.

Källan till den digitala informationen kan vara olika i olika utföringsexempel. Till exempel kan källan vara informationens upphovsman, distributör, etc. Enheten som mottager den digitala informationen kan också vara olika i olika utföringsformer. Exempel på en sådan enhet inkluderar en portabel audio/video spelare (t.ex. iPod), en laptop, en mobiltelefon, etc. Den digitala informationen kan också vara olika i olika utföringsformer. Den digitala informationen kan t.ex. vara firmware-updateringar till operativsystemet för enheten, tredje-part applikationer för att köras på enheten, audio/video filer för att spelas på enheten etc.

II. SYSTEM FÖR INTEGRITETSVERIFIERING ENLIGT NÅGRA UTFÖRINGSFORMER

Figur 1 visar konceptuellt en mer detaljerad version av ett system för integritets-verifiering 100 för någon utföringsform av uppfinningen. Som visas i denna figur innehåller detta system en källenhet för digital information 110 och en informations-mottagande enhet 115. Som visas i figur 1 överför källenheten för digital information 110 åtminstone ett block av digital information 105 till den informationsmottagande enheten 115. En informationskälla är varje part inblandad i skapandet av informationen, dess försäljning eller distribution. Exempel på en sådan part inkluderar informationens upphovsman, försäljare, distributör etc. Källenheten för digital information 110 kan bestå av en eller flera stationära eller portabla enheter, datorer, servrar, etc. Som visas i figur 1 utför källenheten för digital information 110 en hashing-procedur 120 och en signaturgenereringsprocedur 130. Hashing-proceduren 120 applicerar en hash-funktion på en del av den digitala informationen 105. Denna del är ett speciellt mönster av bitar 125 vilket visas konceptuellt som svärtade sektioner av den digitala informationen 105 i figur 1.

I några utföringsformer är detta bitmönster specificerat på ett sätt som (till exempel av källenheten för digital information 110, av en DRM-server som styr enheten 110, etc.) säkerställer att tillräcklig digital information hashas för att uppnå tre mål. För det första måste bitmönstret specificeras så att manipulering med den digitala informationen kräver manipulering med en av sektionerna som hashas, vilket skulle avslöja manipuleringen eftersom manipuleringen skulle ändra den följande signaturen. För det andra måste bitmönstret specificeras så att två olika delar av digital information som hashas av proceduren 120 inte kolliderar (det vill säga, inte producerar samma hash). För det tredje, eftersom den informationsmottagande enheten 115 kommer att utnyttja samma bitmönster för sin hashing-procedur, så bör bitmönstret utnyttja minsta antalet

bitar som behövs för att uppfylla de två första målen, så att hashing-proceduren kommer att minimalt utnyttja beräkningsresurserna för den informationsmottagande enheten 115.

Hashing-proceduren 120 är i några utföringsformer konfigurerad att välja bitmönstret 125 kvasi-slumpartat, eller systematiskt (t.ex. baserat på ett ordnat mönster av bitar) i andra utföringsformer. I några utföringsformer kan t.ex. den digitala informationen bestå av objektkod till ett program (som t.ex. operativsystemet för den informationsmottagande enheten 115, en tredjeparts-applikation som körs på den informationsmottagande enheten 115, etc.)

I en del av dessa utföringsformer inkluderar koden en uppsättning op-koder (det vill säga instruktionskoder) och ingen eller flera operander (det vill säga ingen eller flera databitar) för varje op-kod. En del av dessa utföringsformer applicerar således hash-funktionen på så stor del av op-koderna och operanderna som behövs för att maximera detekteringen av manipulering, minimera hash-kollisioner och minimera användningen av beräkningsresurser.

I en del utföringsformer utnyttjar t.ex. den informationsmottagande enheten en ARM mikroprocessor. I en sådan mikroprocessor kallas varje rad av objektkod (som inkluderar en op-kod och dess tillhörande operand) en mikroprocessor-operationsenhet (MOU), vilken har en statistisk längd av fyra bytes. En del utföringsformer använder därför fyra-bytes avståndet för att identifiera gränsen mellan varje kodrad, och använder sedan denna information för att utvälja en eller flera bytes från varje MOU. Valet av byte från varje MOU kan utföras på olika sätt i olika utföringsformer. En del utföringsformer inkluderar en kvasi-slumpartad blandning av op-koder och operander i bitmönstret, som skall hashas. Andra utföringsformer kanske endast inkluderar op-koder (till exempel de flesta eller alla op-koder) i en koddel, som hashas och signeras. Ytterligare andra utföringsformer kan utvälja en bestämd byte (till exempel alltid den första) i varje instruktionsrad. En del utföringsformer utnyttjar en hemlig funktion, vilken för varje MOU producerar en heltalsmodul för MOU-längden och sedan utväljer sektionen eller sektionerna i MOUn som svarar mot denna modul. Andra utföringsformer kan utnyttja andra mikroprocessorer som till exempel mikroprocessorer tillhandahållna av Motorola Corporation, Intel Corporation, AMD Corporation, IBM Corporation, etc.

I olika utföringsformer applicerar hashing-proceduren 120 olika hashing-funktioner på den speciella delen av den digitala informationen. Exempel på hashing-funktioner som

utnyttjas i olika utföringsformer inkluderar MD5, SHA-1, etc. Hashing-funktioner kan utnyttjas med eller utan en nyckel (det vill säga hashing-funktioner kan vara nycklade hashing-funktioner).

Som ovan nämnts är en hashing-funktion en transformation som typiskt tar en form av data (t.ex. en textform) och överför den till en förvrängd output som kallas digest eller hash. Digesten har typiskt ett bestämt antal bits, som tjänar som ett unikt "fingeravtryck" för den ursprungliga informationen. Om det ursprungliga meddelandet ändras och hashas igen produceras med mycket hög sannolikhet en annan digest. Hash-funktioner kan således användas för att detektera ändrade och förfalskade dokument. De tillhandahåller meddelande-integritet, vilken försäkrar informationsmottagaren att informationen inte har ändrats eller förvanskats.

Som visas i figur 1 mottager signaturgeneratorn 130 digesten, som hashing-funktionen i hashing-proceduren 120 producerar. Signaturgeneratorn 130 producerar en signatur 147 för informationen 105 utifrån den mottagna digesten 145. För att producera en sådan signatur kan generatorn 130 använda vilken som helst av ett antal kända tekniker som till exempel: SHA-1, MD5 MAC.

I systemet 100 överföres den digitala informationen 105 och den genererade signaturen 147 till den informationsmottagande enheten 115, såsom visas i figur 1. Olika utföringsformer överför dessa data till den mottagande enheten 115 på olika sätt. En del utföringsformer distribuerar till exempel dessa data via ett kommunikationsnätverk som till exempel ett LAN, WAN eller ett nätverk av nätverk (till exempel Internet). Den informationsmottagande enheten 115 kan dessutom via ett nätverk mottaga dessa data direkt från upphovsmannen, försäljaren eller distributören av informationen eller indirekt via en eller flera mellankopplade servers, som en eller flera DRM servers, informations-caching servers, etc.

En informationsmottagare är varje part inblandad i användandet eller distributionen av informationen. Exempel på en sådan part inkluderar informationens användare, distributör, etc. Den informationsmottagande enheten 115 kan vara en stationär eller portabel enhet, dator, server, audio/video spelare, en kommunikationsenhet (till exempel telefon, pager, textmeddelare, etc.), fickdator, etc.

I systemet 100 utnyttjar källenheten för digital information 110 och den informationsmottagande enheten 115 ett asymmetriskt förfarande för

integritetsverifiering. Den informationsmottagande enheten 115 utför således två förfaranden, en hashing-procedur 135 och en signatur-verifierande procedur 140. Hashing-proceduren 135 applicerar samma hash-funktion på samma sektioner av den digitala informationen 105 som hashing-proceduren 120 i källenheten för digital information 110. Speciellt i en del utföringsformer är hashing-proceduren 135 i den mottagande enheten 115 konfigurerad att utvälja samma bitmönster i den digitala informationen 105 som hashing-proceduren 120 i källenheten för digital information 110. Figur 1 illustrerar detta konceptuellt genom att visa att hashing-procedurerna 120 och 135 utnyttjar identiska svärtade bitmönster 125 i den digitala informationen 105. Valet i hashing-proceduren 135 av samma bitmönster 125 kan göras på ett kvasi-slumpartat eller systematiskt sätt vilket leder till valet av samma bitmönster som i hashing-proceduren 120.

Appliceringen av hashing-funktionen i hashing-proceduren 135 på informationen 105 åstadkommer en digest 149. Denna digest bör vara identisk med digesten 145 genererad av hashing-funktionen i hashing-proceduren 120 då den digitala informationen som mottages av procedurerna 120 och 135 är densamma, eftersom båda procedurerna utväljer samma uppsättning av sektioner i den digitala informationen.

Som visas i figur 1 mottager signaturgeneratorn 140 digesten 149, som hashing-funktionen i hashing-proceduren 135 producerar. Signaturverifieraren 140 mottager också signaturen 147 genererad av signaturgeneratorn 130 i källenheten för digital information 110. Verifieraren 140 bestämmer sedan om den mottagna signaturen 147 är den korrekta signaturen för den mottagna digitala informationen 105 genom att bestämma om signaturen 147 är korrekt för digesten 149. För att bestämma om signaturen 147 är korrekt för digesten 149 kan verifieraren 140 använda sig av vilken som helst av ett antal kända tekniker som till exempel SHA-1 or MD5.

Baserat på jämförelsen mellan digesten 149 och signaturen 147 levererar sedan verifieraren 140 ett integritetskontrollvärde 151. Detta värde specificerar huruvida den mottagna signaturen 147 är den korrekta signaturen för den mottagna digitala informationen 105. I en del utföringsformer är t.ex. integritetskontrollvärdet ett Boolskt värde, som är sant då den digitala informationens integritet has verifierats (det vill säga den mottagna signaturen motsvarar den mottagna digitala informationen), och är falskt då den digitala informationens integritet inte har verifierats. I andra utföringsformer är integritetskontrollvärdet vilken som helst annan typ av binärt värde, med ett värde indikerande att den digitala informationens integritet har verifierats och det andra värdet

indikerande att den digitala informationens integritet inte har verifierats. Integritetskontrollen kommer att specificera att integriteten för informationen inte är verifierad då en eller flera delar av den digitala informationen manipulerats efter det att signaturen 147 har genererats och dessa delar inkluderar en eller flera informationssektioner som användes för att generera hash-digesten 145 och 149.

Andra utföringsformer kan implementeras i andra system för integritetsverifiering. Figur 2 visar till exempel en utföringsform av uppfinningen i ett symmetriskt system för integritetsverifiering 200. Systemet 200 liknar systemet 100 så när som på att dess informationsmottagande enhet 115 inte inkluderar den asymmetriska signaturverifieraren 140 utan inkluderar en signaturgenerator 240 och en symmetrisk signaturverifierare 250.

Liksom signaturgeneratorn 130 i källenheten för digital information 110 genererar signaturgeneratorn 240 en signatur 253 ur hash-digesten 149, som den mottager. Den genererade signaturen 253 överföres sedan till signaturverifieraren 250 tillsammans med den mottagna signaturen 147. Verifieraren 250 jämför sedan de två signaturerna för att specificera integritetskontrollvärdet 151. Integritetskontrollvärdet 151 indikerar att den mottagna digitala informationen inte har manipulerats då de två signaturerna 147 och 253 motsvarar varandra. Då dessa två signaturer inte motsvarar varandra indikerar integritetskontrollvärdet att informationen har manipulerats (det vill säga den mottagna signaturen 147 motsvarar inte den mottagna digitala informationen).

För att konceptuellt illustrera att olika delar av den digitala informationen kan hashas i olika utföringsformer eller för olika delar av informationen, visar figur 2 ett annat svärtat bitmönster 225 i informationen 105 än mönstret visat i figur 1. De svärtade sektionerna i figur 2 har olika längder för att konceptuellt illustrera att sektioner av olika storlek kan hashas i en del utföringsformer av uppfinningen.

III. DRM SYSTEM IMPLEMENTERANDE SYSTEMET FÖR INTEGRITETSVERIFIERING ENLIKT NÅGRA UTFÖRINGSFORMER

Systemet för integritetsverifiering enligt några utföringsformer är implementerat i ett DRM system, som distribuerar information på ett sätt som säkerställer den legala användningen av informationen. Såsom visas i figur 3 inkluderar DRM systemet 300 en uppsättning DRM servers 310 som distribuerar information till en uppsättning av N användardatorer 315. Uppsättningen av servrar 310 är ansluten till användardatorerna 315 via ett datornätverk 320, som till exempel ett LAN, WAN, ett nätverk av nätverk

(till exempel Internet), etc. Varje användardator 315 är ansluten till en uppsättning av en eller flera portabla multimedia enheter 330.

Genom nätverksanslutningen kommunicerar användardatorerna 315 med uppsättningen DRM servrar 310 för att köpa, erhålla en licens för, uppdatera eller på annat sätt mottaga information i vissa utföringsformer. Under det att i en del utföringsformer uppsättningen av DRM servrar 310 således säljer eller licensierar information till användardatorerna så säljer eller licensierar denna uppsättning inte informationen i andra utföringsformer. I en del utföringsformer verkställer uppsättningen av DRM servrar 310 bara distributionen av information till auktoriserade datorer utan något finansiellt intresse.

I en del utföringsformer inkluderar uppsättningen av DRM servrar 310 en informations-caching server som levererar krypterad information till en användardator 310 via nätverket 320 efter det att en annan DRM server 310 bestämt att datorn 310 har rätt till informationen. I en del utföringsformer utnyttjar systemet 300 ett antal caching-servrar för att lagra information på olika ställen i nätverket för att öka hastigheten och effektiviteten vid nedladdning av information över nätverket.

Som ovan nämnts kommunicerar en användardator 315 med uppsättningen av DRM servrar 310 för att köpa, erhålla en licens för, uppdatera eller på annat sätt mottaga information via nätverket 320. I en del utföringsformer överför uppsättningen av DRM servrar 310 en signatur för en informationsmängd som distribueras till en användardator 315, varvid signaturen genereras genom hashning av endast en del av informationen, enligt en del utföringsformer av uppfinningen.

Figur 3 visar speciellt en användardator 315a som sänder en begäran om en informationsmängd "A" till uppsättningen av DRM servrar 310. Denna begäran kan vara en begäran om köp, om att erhålla en licens för, eller på annat sätt få tillgång till informationen. Alternativt, då informationen är en applikation eller ett operativsystem, som körs på användardatorn eller en av dess associerade multimedia enheter 330, kan begäran vara en begäran om en uppdatering till applikationen eller operativsystemet. Denna begäran kan vara en explicit begäran eller en implicit begäran i en procedur för uppdateringskontroll utförd på användardatorn 315, vilken med eller utan ingripande från användaren letar efter uppdateringar till applikationen eller operativsystemet.

Såsom visas i figur 3 mottager uppsättningen av DRM servrar 310 begäran om informationen A från användardatorn 315a. En eller flera av DRM datorerna utför sedan proceduren 400 illustrerad i figur 4 för att generera en signatur för den begärda informationen A. Såsom visas i figur 4 genererar proceduren 400 till att börja med (vid 405) en digest genom att applicera en hash-funktion på endast en del av den begärda informationen A. Applicering av en hash-funktion på endast en del av en informationsmängd har beskrivits i sektionerna I och II ovan. Såsom ovan nämnts och ytterligare beskrivet nedan applicerar proceduren 400 hash-funktionen på samma del av informationen A som hashing-funktionerna i användardatorn 315a och dess associerade multimedia enhet 330a.

Efter applicering av hashing-funktionen vid 405 genererar proceduren 410 (vid 410) en signatur baserad på hash-digesten genererad vid 405. Generering av en signatur baserat på hash-digesten har beskrivits ovan i sektionerna I och II. Efter generering av signaturen vid 410, överför proceduren den begärda informationen A och dess associerade signatur till användardatorn 315a, och avslutas därefter.

I en del utföringsformer utnyttjar användardatorn 315a den överförda signaturen för att verifiera integriteten för den mottagna informationen A. För att göra detta genererar användardatorn 315a en hash-digest för informationen A genom att applicera hashing-funktionen på samma del av informationen A som hashing-funktionen i uppsättningen av DRM servrar 310. Den utnyttjar sedan denna digest för att verifiera integriteten för signaturen genom att utnyttja en asymmetrisk signaturverifierande metod (såsom den visad i figur 1) eller en symmetrisk signaturverifierande metod (såsom den visad i figur 2).

I en del utföringsformer mottager en multimedia enhet 330a ansluten till användardatorn 315a också informationen A och signaturen A för denna information då den synkroniseras med datorn 315a. När således informationen A är information avsedd för multimedia enheten 330a registrerar i en del utföringsformer användardatorn 315a (till exempel i ett dataminne) behovet att ladda ned informationen A och dess signatur till enheten 330a då enheten 330a synkroniserar nästa gång med datorn 315a.

På samma sätt som användardatorn 315a genererar multimedia enheten 330a en hash-digest för informationen A genom att applicera hashing-funktionen på samma del av informationen A som hashing-funktionen i uppsättningen av DRM servrar 310. Den utnyttjar sedan denna hash-digest för att verifiera integriteten för informationen genom

att utnyttja en asymmetrisk signaturverifierande metod (såsom den visad i figur 1) eller en symmetrisk signaturverifierande metod (såsom den visad i figur 2). Figur 5 illustrerar ett mera detaljerat exempel på förfarandet för integritetsverifiering 500, som multimedia enheten 330a utför i en del utföringsexempel. Denna procedur utföres under en synkroniseringsoperation som laddar exekverbar information (det vill säga kod för uppdatering av operativsystemet, för uppdatering av existerande applikationer, för nya applikationer, etc.) på multimedia enheten 330a. Såsom visas i denna figur mottager till att börja med proceduren 500 (vid 505) exekverbar information och signatur för denna information under en synkroniseringsoperation som säkerställer att enheten har all information, som användardatorn indikerar att den skall ha.

Efter synkroniseringen återstartar proceduren (vid 510), eftersom i en del utförings-exempel den integritetsverifierande proceduren utgör en del av boot-sekvensen vid start. Speciellt utför i en del utföringsformer boot-sekvensen vid start en procedur för integritetsverifikation för varje del av nyss mottagen kod även om i exemplet visat i figur 5 det antages att endast en informationsmängd laddas ner i enheten vid 505. I en del utföringsformer är boot-sekvensen (inkluderande förfarandet för integritets-verifiering) lagrad i ett permanent read-only minne i enheten 315a. Detta säkerställer att förfarandet för integritetsverifiering inte kan manipuleras efter försäljning av enheten.

Således genererar proceduren 500 (vid 515) under boot-sekvensen vid start en hash-digest för den mottagna informationen genom att applicera hashing-funktionen på samma del av informationen som hashing-funktionen i uppsättningen av DRM servrar 310. Den utnyttjar sedan (vid 520) denna hash-digest för att verifiera integriteten för signaturen. Proceduren 500 kan till exempel utnyttja en asymmetrisk signatur-verifierande metod (såsom den visad i figur 1) eller en symmetrisk signaturverifierande metod (såsom den visad i figur 2).

Då proceduren inte kan verifiera (vid 520) integriteten av den nyss mottagna koden (det vill säga då den nyss mottagna signaturen inte motsvarar digesten genererad av enheten för den nyss mottagna informationen) stoppar proceduren utan att specificera att informationen kan laddas i det exekverbara minnet. Alternativt, då proceduren verifierar (vid 520) integriteten för den nyss mottagna koden, så specificerar proceduren (vid 525) att koden är exekverbar. I en del utföringsformer laddar proceduren (vid 525) koden i ett exekverbart minne och exekverar koden. DRM systemet 300 i figur 3 har mer än en användardator som mottager digital information och signaturer för sådan information enligt förfarandena för integritetsverifiering i en del utföringsformer av uppfinningen.

Figur 3 visar speciellt en användardator 315n, som begär om en informationsmängd (det vill säga mängden B) från uppsättningen av DRM servrar 310. Såsom visas i denna figur mottager användardatorn 315n den begärda informationen B och en signatur för denna information från uppsättningen av DRM servrar 310. Enligt uppfinningen genereras signaturen för informationen B genom hashning av endast en del av informationen B. Användardatorn 315n och dess associerade uppsättning av portabla enheter 330 verifierar sedan integriteten för informationen B genom hashning av samma del av informationen B som uppsättningen av DRM servrar ungefär på samma sätt som beskrivits ovan för användardatorn 315a och dess associerade enheter 330a.

IV. SYSTEMDIAGRAM

Figur 6 visar ett diagram för ett datorsystem som konceptuellt illustrerar komponenterna i en typisk DRM server, användardator eller portabel enhet implementerande några utföringsformer av uppfinningen. Datorsystemet 600 inkluderar en buss 605, en processor 610, ett systemminne 615, ett read-only minne 620, ett permanent minne 625, input enheter 630 och output enheter 3035.

Bussen 605 representerar kollektivt alla system-, perifera- och chipsetbussar som sköter kommunikationen mellan interna enheter i datorsystemet 600. Bussen 605 sammanbinder till exempel kommunikativt processorn 610 med read-only minnet 620, systemminnet 615 och den permanenta lagringsenheten 625. Från dessa olika minnesenheter hämtar processorn 610 instruktioner att exekvera och data att behandla för att exekvera proceduren enligt uppfinningen. Read-only minnet (ROM) 620 lagrar statiska data och instruktioner som behövs för processorn 610 och andra moduler i datorsystemet. I fallet med en portabel enhet som implementerar uppfinningen lagrar read-only minnet boot-sekvensen och hashing-proceduren i en del utföringsformer, såsom nämnts ovan.

Den permanenta lagringsenheten 625 å andra sidan är en read-and-write minnesenhet. Denna enhet är en permanentminnesenhet, som lagrar instruktioner och data även då datorsystemet inte är i drift. En del utföringsformer av uppfinningen utnyttjar en massminnesenhet (som en magnetisk eller optisk skiva med tillhörande diskdrive) som den permanenta minnesenheten 625. Andra utföringsformer utnyttjar en extern minnesenhet (som ett minneskort eller minnessticka) som permanent minnesenhet.

Liksom den permanenta lagringsenheten 625 är systemminnet 615 en read-and-write minnesenhet. Till skillnad från lagringsenheten 625 är emellertid systemminnet ett

flyktigt read-and-write minne, som ett random access minne. Systemminnet lagrar en del av de instruktioner och data som processorn behöver då den arbetar. I en del utföringsformer är uppfinningens procedurer lagrade i systemminnet 615, den permanenta lagringsenheten 625 och/eller read-only minnet 620.

Bussen 605 är också förbunden med input och output enheterna 630 och 635. Inputenheterna gör det möjligt för användaren att överföra information och välja kommandon för datorsystemet. Inputenheterna 630 inkluderar alfanumeriska tangentbord och styrenheter för pekare. Outputenheterna 635 visar bilder genererade av datorsystemet. Outputenheterna inkluderar printrar och displayenheter såsom displayenheter med katodstrålerör (CRT) eller flytande kristaller (LCD). Slutligen, som visas i figur 6, inkluderar också vissa konfigurationer av datorn 600 en nätverksadapter 640 ansluten till bussen 605. Via nätverksadaptern 640 kan datorn vara en del av ett nätverk av datorer (som ett lokalt nätverk ("LAN"), ett vidsträckt nätverk ("WAN") eller ett Intranet) eller ett nätverk av nätverk (som Internet). Vilken som helst eller alla komponenterna i datorsystemet 600 kan användas tillsammans med uppfinningen. Fackmannen inser emellertid att vilken som helst annan systemkonfiguration också kan användas tillsammans med uppfinningen.

V. FÖRDELAR

Fackmannen förstår att de ovan beskrivna förfarandena för integritetsverifiering har flera fördelar. Då man laddar ned ny exekverbar kod till en enhet, till exempel, är det viktigt att verifiera integriteten för koden eftersom sådan kod ger ett lämpligt tillfälle att utsätta enheten för en attack. Integritetsprocedurerna, som ovan beskrivits, anvisar ett enkelt sätt att kontrollera integriteten för koden även på portabla enheter med begränsade beräkningsresurser.

En del utföringsformer inkorporerar också procedurerna för integritetsverifiering under boot-sekvensen vid start av enheten för att minimera möjligheten till manipulering av integritetsproceduren. För att ytterligare minimera denna möjlighet har en del utföringsformer integritetsprocedurerna lagrade i ett read-only minne i enheten.

Även om uppfinningen har beskrivits med referens till ett stort antal specifika detaljer så inser fackmannen att uppfinningen kan realiseras i andra specifika former utan att man därvid lämnar uppfinningens ide. Som nämnts ovan, till exempel, kan en del utförings-former utnyttja en nycklad hashing-funktion. Om en nyckel användes kan både symmetriska (en enda hemlig nyckel) och asymmetriska nycklar (publika/privata

nyckelpar) användas. Ett exempel på en nycklad hash-funktion är en nycklad MD5 teknik. En sändare lägger till en slumpartat genererad nyckel vid slutet på ett meddelande och hashar sedan meddelande-nyckel kombinationen under användande av en MD5 hash för att åstadkomma en digest. Därefter tages nyckeln bort från meddelandet och krypteras med sändarens privata nyckel. Meddelandet, meddelande-digesten och den krypterade nyckeln skickas till mottagaren som öppnar nyckeln med sändarens publika nyckel (validerande på så sätt att meddelandet verkligen är från sändaren). Mottagaren lägger sedan till nyckeln till meddelandet och applicerar samma hash som sändaren. Meddelande-digesten bör motsvara meddelande-digesten som sänts med meddelandet.

Flera av de ovan beskrivna utföringsformerna utväljer också bitmönster i objektkod-formatet för en information. Andra utföringsformer kan utvälja andra mönster av sektioner då informationen har ett annat format (till exempel är i källkod eller XML-format). Fackmannen inser således att uppfinningen inte är begränsad av de beskrivna illustrativa detaljerna utan istället skall definieras av de bifogade patentkraven.

NYA PATENTKRAV

1. En metod innefattande:
för en speciell information, vilken innefattar en uppsättning sektioner, val av en del-sektion från var och en av ett flertal sektioner i nämnda uppsättning sektioner, varvid del-sektionen av varje sektion väljes med användning av en kvasi-slumpartad operation;
generering för den speciella informationen av en digital signatur utifrån endast de valda del-sektionerna av den speciella informationen; och
tillhandahållande av den digitala signaturen.

2. Metoden enligt patentkrav 1, i vilken genereringen av den digitala signaturen innefattar:
användning av en hashfunktion på endast delen av den speciella informationen för att generera en hash;
generering av den digitala signaturen från hashen.

3. Metoden enligt patentkrav 1, i vilken del-sektionerna är valda för att maximera detekteringen av manipulering av den speciella informationen.

4. Metoden enligt patentkrav 1, i vilken del-sektionerna är valda för att minimera hash-kollisioner.

5. Metoden enligt patentkrav 1, i vilken del-sektionerna är valda för att minimera beräkningsresurser.

6. Metoden enligt patentkrav 1, i vilken den speciella informationen innefattar videoinformation.

7. Metoden enligt patentkrav 1, i vilken den speciella informationen innefattar audioinformation.

8. Metoden enligt patentkrav 1, i vilken den speciella informationen innefattar en uppdatering av firmware för en speciell enhet.

9. Metoden enligt patentkrav 1, i vilken den speciella informationen är en applikation avsedd att köras på en speciell enhet.

10. Metoden enligt patentkrav 9, i vilken enheten är en portabel spelare.

11. Metoden enligt patentkrav 1, i vilken den speciella informationen innefattar objektkod.

12. Metoden enligt patentkrav 11, i vilken objektkoden innefattar en uppsättning op-koder och en associerad uppsättning operander varvid de valda del-sektionerna innefattar op-koder och operander.

13. Metoden enligt patentkrav 1 ytterligare innefattande tillhandahållande av den speciella informationen.

14. Ett datorläsbart medium lagrande ett datorprogram som är exekverbart med åtminstone en processor varvid datorprogrammet innefattar uppsättningar av instruktioner för:
för en speciell information, vilken innefattar en uppsättning sektioner, val av en del-sektion från var och en av ett flertal sektioner i nämnda uppsättning sektioner, varvid de valda del-sektionerna tillsammans innefattar ett ordnat mönster av bits;
generering för den speciella informationen av en digital signatur utifrån endast de valda del-sektionerna av den speciella informationen; och
tillhandahållande av den digitala signaturen.

15. Det datorläsbara mediet enligt patentkrav 14, i vilket uppsättningen av instruktioner för generering av den digitala signaturen innefattar uppsättningar av instruktioner för:
användning av en hash-funktion på endast de valda del-sektionerna av den speciella informationen för att generera en hash; och
generering av den digitala signaturen från hashen.

16. Det datorläsbara mediet enligt patentkrav 14, i vilket den speciella informationen innefattar objektkod.

17. Det datorläsbara mediet enligt patentkrav 16, i vilket objektkoden innefattar en uppsättning op-koder och en associerad uppsättning operander varvid de valda del-sektionerna endast innefattar op-koder.

18. Det datorläsbara mediet enligt patentkrav 16, i vilket objektkoden innefattar en uppsättning op-koder och en associerad uppsättning operander varvid de valda del-sektionerna innefattar op-koder och operander.

19. Det datorläsbara mediet enligt patentkrav 14, i vilket datorprogrammet ytterligare innefattar en uppsättning av instruktioner för tillhandahållande av den speciella informationen.

20. En metod innefattande:
a) mottagande av en speciell information innehållande ett flertal uppsättningar op-koder och operander; och
b) verifiering av autenticiteten för den speciella informationen genom användning av en digital signatur som utvinnes från endast en del av den speciella informationen, varvid delen innefattar en del från varje uppsättning op-koder och operander.

21. Metoden enligt patentkrav 20, i vilken den digitala signaturen utvinnes ur en hash som genereras genom applicering av en hash-funktion endast på delen av den speciella informationen.

22. Metoden enligt patentkrav 20, i vilken verifiering av autenticiteten för den speciella informationen innefattar användningen av en asymmetrisk integritetsprocedur.

23. Metoden enligt patentkrav 22, i vilken användningen av den asymmetriska integritetsproceduren innefattar:
a) beräkning av en speciell hash för endast delen av den mottagna informationen; och
b) bestämning huruvida den speciella hashen är korrekt för den mottagna digitala signaturen.

24. Metoden enligt patentkrav 23, ytterligare innefattande generering av ett integritetskontrollvärde för att indikera huruvida den speciella hashen är korrekt för den mottagna digitala signaturen.

25. Metoden enligt patentkrav 23, i vilken den speciella informationen verifieras som autentisk då det bestämts att den speciella hashen är korrekt för den mottagna digitala signaturen.

26. Metoden enligt patentkrav 20, i vilken verifiering av autenticiteten för den speciella informationen innefattar användningen av en symmetrisk integritetsprocedur.

27. Metoden enligt patentkrav 26, i vilken användningen av den symmetriska integritetsproceduren innefattar:
a) generering av en speciell hash för endast delen av den mottagna informationen;
b) generering av en andra digital signatur baserad på den speciella hashen; och
c) bestämning huruvida den mottagna digitala signaturen överensstämmer med den andra digitala signaturen.

28. Metoden enligt patentkrav 27, i vilken den speciella informationen verifieras som autentisk då det bestämts att de två digitala signaturerna överensstämmer.

29. Metoden enligt patentkrav 20, ytterligare innefattande val av den speciella delen av den speciella informationen baserat på ett regelbundet mönster av bitar i den speciella informationen.

30. Metoden enligt patentkrav 20, ytterligare innefattande val av den speciella delen av den speciella informationen baserat på en kvasi-slumpartad operation.

31. Metoden enligt patentkrav 20, i vilken den speciella informationen innefattar videoinformation.

32. Metoden enligt patentkrav 20, i vilken den speciella informationen innefattar audioinformation.

33. Metoden enligt patentkrav 20, i vilken den speciella informationen innefattar en uppdatering av firmware för en speciell enhet.

34. Metoden enligt patentkrav 20, i vilken den speciella informationen är en applikation avsedd att köras på en speciell enhet.

35. Metoden enligt patentkrav 34, i vilken enheten är en portabel spelare.

36. Metoden enligt patentkraven 20 och 89, varvid den speciella delen endast innefattar op-koder.

37. Metoden enligt patentkraven 20 och 89, varvid den speciella delen innefattar en kvasi-slumpartad mix av op-koder och operander.

38. Metoden enligt patentkrav 20, ytterligare innefattande utförandet av en synkroniseringsoperation med en enhet som skall mottaga den speciella informationen och digitala signaturen.

39. Metoden enligt patentkrav 38, i vilken enheten är en första enhet varvid mottagandet, verifieringen och utförandet handhas av en andra enhet.

40. Metoden enligt patentkrav 39, i vilken verifieringen utföres under en boot-sekvens för den andra enheten.

41. Metoden enligt patentkrav 20, i vilken verifieringen utföres åtminstone delvis med hjälp av en uppsättning instruktioner som är lagrad i ett read-only minne i en enhet.

42. Ett datorläsbart medium innefattande ett datorprogram som är exekverbart med åtminstone en processor varvid datorprogrammet innefattar uppsättningar av instruktioner för:
mottagande av en speciell information innehållande ett flertal uppsättningar op-koder och operander; och
verifiering av autenticiteten för den speciella informationen genom användning av en digital signatur som utvinnes från endast en del av den speciella informationen, varvid delen innefattar en kvasi-slumpartat vald del från varje uppsättning op-koder och operander.

43. Det datorläsbara mediet enligt patentkrav 42, i vilket den digitala signaturen utvinnes ur en hash som genereras genom applicering av en hash-funktion endast på delen av den speciella informationen.

44. Det datorläsbara mediet enligt patentkrav 42, i vilket uppsättningen av instruktioner för verifiering av autenticiteten för den speciella informationen innefattar en uppsättning av instruktioner för utnyttjande av en asymmetrisk integritetsprocedur.

45. Det datorläsbara mediet enligt patentkrav 44, i vilket uppsättningen av instruktioner för utnyttjande av den asymmetriska integritetsproceduren innefattar uppsättningar av instruktioner för:

a) beräkning av en speciell hash för endast delen av den mottagna informationen; och
b) bestämning huruvida den speciella hashen är korrekt för den mottagna digitala signaturen.

46. Det datorläsbara mediet enligt patentkrav 45, i vilket den speciella informationen verifieras som autentisk då det bestämts att den speciella hashen är korrekt för den mottagna digitala signaturen.

47. Det datorläsbara mediet enligt patentkrav 42, i vilket uppsättningen av instruktioner för verifiering av autenticiteten för den speciella informationen innefattar en uppsättning av instruktioner för utnyttjande av en symmetrisk integritetsprocedur.

48. Det datorläsbara mediet enligt patentkrav 47, i vilket en uppsättning av instruktioner för utnyttjande av den symmetriska integritetsproceduren innefattar uppsättningar av instruktioner för:
a) generering av en speciell hash för endast delen av den mottagna informationen;
b) generering av en andra digital signatur baserad på den speciella hashen; och
c) bestämning huruvida den mottagna digitala signaturen överensstämmer med den andra digitala signaturen.

49. Det datorläsbara mediet enligt patentkrav 48, i vilket den speciella informationen verifieras som autentisk då det bestämts att de två digitala signaturerna överensstämmer.

50. Det datorläsbara mediet enligt patentkrav 42, varvid den speciella delen innefattar op-koder och operander.

51. Det datorläsbara mediet enligt patentkrav 42, ytterligare innefattande en uppsättning av instruktioner för utförande av en synkroniseringsoperation med en enhet som skall mottaga den speciella informationen och digitala signaturen, varvid enheten är en första enhet och varvid uppsättningen av instruktioner för mottagandet, verifieringen och utförandet handhas av en andra enhet.

52. Det datorläsbara mediet enligt patentkrav 51, i vilket uppsättningen av instruktioner för verifieringen utföres under en boot-sekvens för den andra enheten.

53. Det datorläsbara mediet enligt patentkrav 42, i vilket uppsättningen av instruktioner för verifiering utföres åtminstone delvis med hjälp av en uppsättning instruktioner som är lagrad i ett read-only minne i en enhet.

54. En enhet för åtkomst av information, innefattande:
en lagringsenhet för lagring av en speciell information innehållande ett flertal uppsättningar op-koder och operander; och
en elektronisk enhet för utnyttjande av en digital signatur för verifiering av den speciella informationen, varvid den digitala signaturen utvunnits från endast en del av den speciella informationen varvid delen innefattar endast en op-kod från vardera av flertalet av uppsättningar.

55. Enheten enligt patentkrav 54, i vilken den elektroniska enheten dessutom är avsedd att generera den digitala signaturen från endast delen av den speciella informationen.

56. Enheten enligt patentkrav 55, i vilken den elektroniska enheten genererar den digitala signaturen genom att först generera en hash från endast delen av den speciella informationen och sedan generera signaturen från den genererade hashen.

57. Enheten enligt patentkrav 55, i vilken den elektroniska enheten utnyttjar den digitala signaturen genom att jämföra den genererade digitala signaturen med en digital signatur som enheten mottager.

58. Enheten enligt patentkrav 54, i vilken den digitala signaturen är en signatur som enheten mottager.

59. Enheten enligt patentkrav 54, i vilken enheten är en dator.

60. Enheten enligt patentkrav 54, i vilken enheten är en portabel spelare.

61. Enheten enligt patentkrav 54, ytterligare innefattande ett ROM för lagring av en uppsättning instruktioner för utnyttjande av den digitala signaturen för verifiering av informationen.

62. Enheten enligt patentkrav 54, i vilken uppsättningen av instruktioner innefattar instruktioner för att generera den digitala signaturen från endast delen av den speciella informationen.

63. Ett system för distribution av information innefattande:
a) en uppsättning datorer för tillhandahållande av en speciell information; som innefattar en uppsättning av sektioner och
b) en enhet för utnyttjande av en digital signatur för verifiering av den speciella informationen, i vilken den digitala signaturen utvinnes från endast en del av den speciella informationen, vilken del innefattar en delsektion av ett flertal av sektioner i nämnda uppsättning sektioner, varvid delsektionerna tillsammans omfattar ett ordnat mönster av bitar.

64. Systemet enligt patentkrav 63, i vilket uppsättningen datorer dessutom utnyttjas för:
a) användning av en hash-funktion på endast delen av den speciella informationen för att generera en hash; och
b) generering av den digitala signaturen från hashen.

65. Systemet enligt patentkrav 64, i vilket uppsättningen av datorer genererar hashen genom att utvälja den speciella delen av den speciella informationen anordnad att maximera detekteringen av manipulering av den speciella informationen.

66. Systemet enligt patentkrav 64, i vilket uppsättningen av datorer genererar hashen genom att utvälja den speciella delen av den speciella informationen anordnad att minimera hash-kollisioner.

67. Systemet enligt patentkrav 64, i vilket uppsättningen av datorer genererar hashen genom att utvälja den speciella delen av den speciella informationen anordnad att minimera behovet av beräkningsresurser.

68. Systemet enligt patentkrav 63, i vilket enheten innefattar ett read-only minne för lagring av en uppsättning av instruktioner för verifiering av den speciella informationen.

69. Systemet enligt patentkrav 63, i vilket uppsättningen datorer innefattar en dator.

70. Systemet enligt patentkrav 63, i vilket uppsättningen datorer innefattar fler än en dator.

71. Systemet enligt patentkrav 63, i vilket enheten utnyttjar den digitala signaturen för verifiering av den speciella informationen genom användning av en asymmetrisk integritetsprocedur.

72. Systemet enligt patentkrav 63, i vilket enheten utnyttjar den digitala signaturen för verifiering av den speciella informationen genom användning av en symmetrisk integritetsprocedur.

73. Systemet enligt patentkrav 63, i vilket den digitala signaturen är en signatur tillhandahållen av uppsättningen av datorer.

74. Systemet enligt patentkrav 73, i vilket enheten utnyttjar den digitala signaturen genom att bestämma huruvida en hash beräknad av enheten är korrekt för den mottagna digitala signaturen.

75. Systemet enligt patentkrav 63, i vilket den digitala signaturen genereras av enheten.

76. Systemet enligt patentkrav 75, i vilket enheten utnyttjar den digitala signaturen genom att jämföra den digitala signaturen genererad av enheten med en annan digital signatur tillhandahållen av uppsättningen av datorer.

77. En metod innefattande:
a) generering av en signatur för en digital information som innefattar ett flertal uppsättningar av op-koder och operander genom applicering av en hashing-funktion på en speciell del av den digitala informationen, varvid nämnda speciella del inte innefattar hela den digitala informationen, men en del av varje uppsättning av op-koder och operander,
b) överföring av signaturen och den digitala informationen till en enhet; och
c) i enheten applicering av hashing-funktionen på den speciella delen av den digitala informationen för att verifiera signaturen överförd med den digitala informationen och därmed verifiera integriteten för den överförda digitala informationen.

78. Metoden enligt patentkrav 77, ytterligare innefattande:
a) vid källan för den digitala informationen utvälja den speciella delen av digital information; och
b) vid enheten utvälja samma speciella del av digital information.

79. Metoden enligt patentkrav 78, i vilken källan är en upphovsman till den digitala informationen.

80. Metoden enligt patentkrav 78, i vilken källan är en distributör av den digitala informationen i ett digitalt rättsförvaltande system.

81. Metoden enligt patentkrav 77, ytterligare innefattande lagringskod som identifierar den speciella delen i ett read-only minne i enheten.

82. Metoden enligt patentkrav 77, ytterligare innefattande lagring av hashing-funktionen i ett read-only minne i enheten.

83. Metoden enligt patentkrav 77, i vilken generering av en signatur för den digitala informationen innefattar:
a) applicering av hashing-funktionen på den speciella delen för att generera en hash; och
b) generering av signaturen från hashen.

84. Metoden enligt patentkrav 77, i vilken appliceringen av hashing-funktionen i enheten på den speciella delen innefattar:
a) applicering av hashing-funktionen på den speciella delen för att generera en hash; och
b) utnyttja den genererade hashen för att verifiera integriteten för den överförda signaturen.

85. Metoden enligt patentkrav 84, ytterligare innefattande, i enheten, tillhandahållande av den genererade hashen och signaturen till en signaturverifierande process som bestämmer autenticiteten för signaturen baserat på den tillhandahållna hashen.

86. Metoden enligt patentkrav 84, i vilken signaturen överförd till enheten är en första signatur varvid utnyttjandet av den genererade hashen innefattar:
a) i enheten, generering av en andra signatur baserad på den genererade hashen; och
b) i enheten, jämförelse mellan de första och andra signaturerna för att bestämma integriteten för den mottagna digitala informationen.

87. Metoden enligt patentkrav 77, i vilken den digitala informationen innefattar kod för exekvering på enheten varvid appliceringen av hashing-funktionen i enheten innefattar att applicera hashing-funktionen innan koden laddas i det exekverbara minnet.

88. Metoden enligt patentkrav 77, i vilken den digitala informationen innefattar kod för modifiering av ett operativsystem för enheten.

89. En metod innefattande:
för en speciell information, vilken innefattar ett flertal uppsättningar av op-koder och operander, val av en del av den speciella informationen så att en del av varje uppsättning utgör en del av den valda delen; generering av en digital signatur för den speciella informationen utifrån endast delen av den speciella informationen; och tillhandahållande av den digitala signaturen för användning vid en senare verifiering av hela den speciella informationen.

90. En metod innefattande:
a) mottagning av en speciell information i en portabel mediaspelare, vilken information innefattar objektkod, varvid objektkoden innefattar en uppsättning av op-koder samt associerad uppsättning av operander
b) mottagning i nämnda spelare av en digital signatur genererad utifrån endast en del av den speciella informationen, varvid den speciella informationen bara innefattar op-koder; och
c) verifiering i nämnda spelare av hela den speciella informationen med hjälp av den digitala signaturen.

91. En metod innefattande:
för en speciell information, vilken innefattar ett flertal uppsättningar av exekverbar objektkod, varvid varje uppsättning innefattar ett flertal bytes, val av en del av den speciella informationen, varvid delen av den speciella informationen innefattar en del-uppsättning av var och en av uppsättningarna av exekverbar objektkod, varvid varje del-uppsättning innefattar samma bestämda byte;generering av en digital signatur utifrån endast den valda delen av den speciella informationen för verifiering av hela den speciella informationen; och tillhandahållande av den speciella informationen och den digitala signaturen.

92. En portabel mediaspelare vilken mottager en speciell information och en signatur för verifiering av hela den speciella informationen, varvid den speciella informationen innefattar objektkod, vilken innefattar en uppsättning op-koder samt associerad uppsättning operander, varvid signaturen tidigare genererats utifrån endast en del av den speciella informationen som innefattar op-koder samt operander, varvid den portabla mediaspelaren innefattar:

a) en digest generator för generering av en digest utifrån endast samma del av den speciella informationen som innefattar op-koder och operander; och
b) en signaturverifierare för verifiering av hela den speciella informationen.

93. Den portabla mediaspelaren enligt patentkrav 92, i vilken signaturverifieraren verifierar den speciella informationen genom att säkerställa att den mottagna signaturen passar den genererade digesten.

94. Den portabla mediaspelaren enligt patentkrav 93dessutom innefattande en signaturgenerator för generering av en signatur utifrån den genererade digesten, varvid verifieraren jämför signaturen genererad av signaturgeneratorn med den mottagna signaturen.

95. Den portabla mediaspelaren enligt patentkrav 92, i vilken den speciella informationen är en uppdatering av applikation som körs på den portabla mediaspelaren.

96. Den portabla mediaspelaren enligt patentkrav 92, i vilken digestgeneratorn genererar digesten genom applicering av en hashfunktion på endast nämnda del av den speciella informationen.

97. En metod innefattande:
sändning, vid en portabel mediaspelare, av en begäran till en digital rättsförvaltande (DRM) server om en applikation innefattande exekverbar kod för mediaspelaren;mottagning i den portablamediaspelaren av den begärda applikationen innefattande exekverbar kod för spelaren; mottagning i spelaren av en digital signatur för applikationen, varvid den digitala signaturen genererats utifrån endast en del av applikationen; och verifiering av hela applikationen genom användning av signaturen.

98. Metoden enligt patentkrav 97, varvid den mottagna applikationen är en uppdatering av en existerande applikation.

99. Metoden enligt patentkrav 98, varvid den existerande applikationen utgör firmware för spelaren.

100. Metoden enligt patentkrav 97, varvid verifieringen innefattar:
a) generering av en digital signatur i den portabla mediaspelaren utifrån endast samma del av den mottagna applikationen som användes för att generera den mottagna digitala

signaturen; och
b) jämförelse av den genererade digitala signaturen med den mottagna digitala signaturen.

101. Metoden enligt patentkrav 100, varvid generering av den digitala signaturen innefattar applicering av en hashfunktion på endast nämnda del av den mottagna applikationen som användes för att generera den mottagna digitala signaturen.

102. Metoden enligt patentkrav 20, i vilken den speciella delen innefattar en op-kod och åtminstone en operand från varje sektion.

103. Metoden enligt patentkrav 89, i vilken genereringen av den digitala signaturen innefattar:
användning av en hash-funktion på endast delen av den speciella informationen för att generera en hash; och
generering av den digitala signaturen från hashen.

104. Metoden enligt patentkrav 91, i vilken genereringen av den digitala signaturen innefattar:
användning av en hash-funktion på endast delen av den speciella informationen för att generera en hash; och
generering av den digitala signaturen från hashen.

105. Metoden enligt patentkrav 91, varvid varje uppsättning av exekverbar objektkod innefattar en op-kod och en eller flera operander, varvid samma bestämda byte för varje uppsättning innefattar den första byten i uppsättningen.

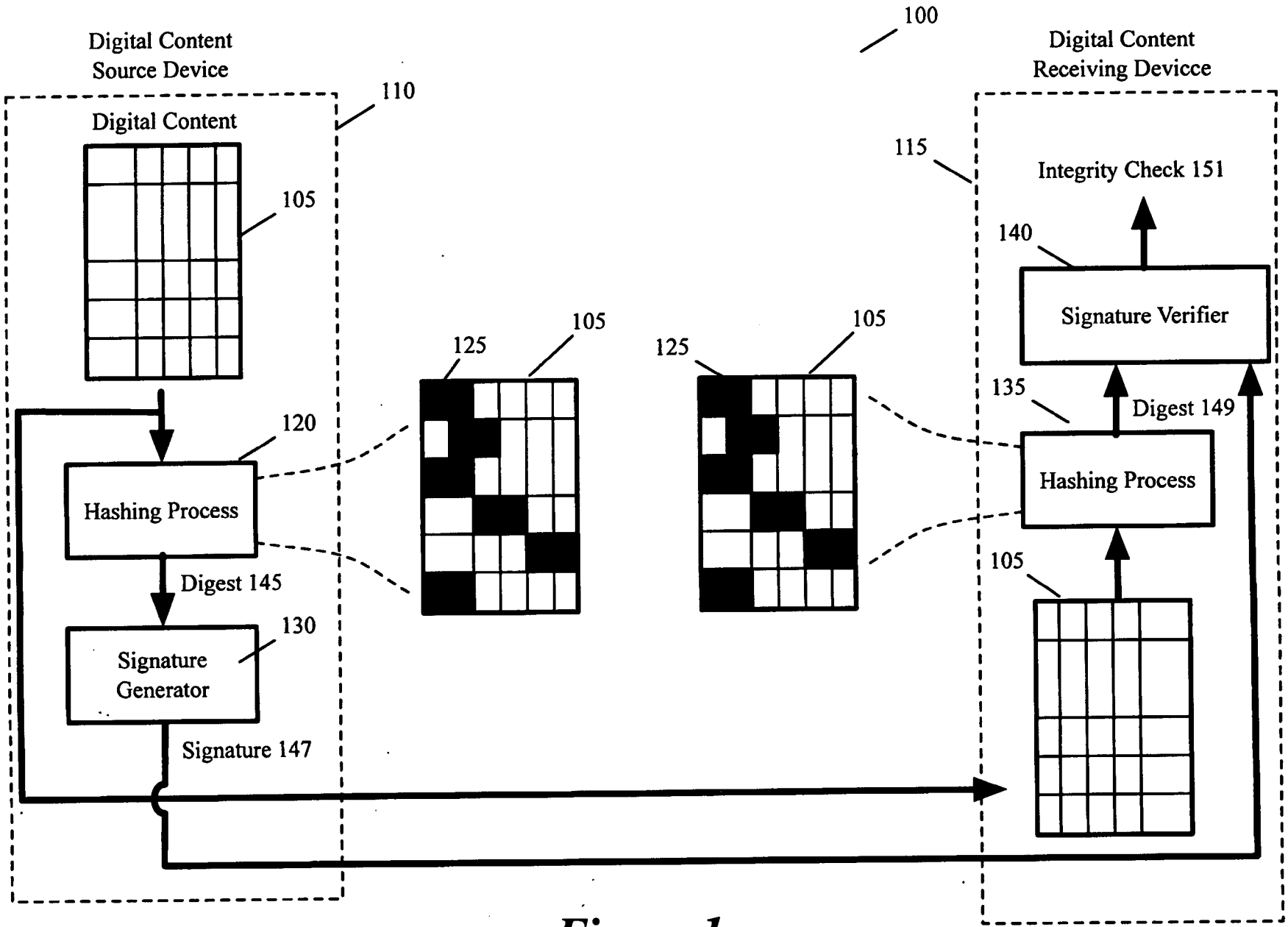

100
Digital Content
Source Device
110
Digital Content
105
120
Hashing Process
Digest 145
130
Signature
Generator
Signature 147
125
105
125
105
Digital Content
Receiving Devicce
115
Integrity Check 151
140
Signature Verifier
135
Digest 149
Hashing Process
105

Figure 1

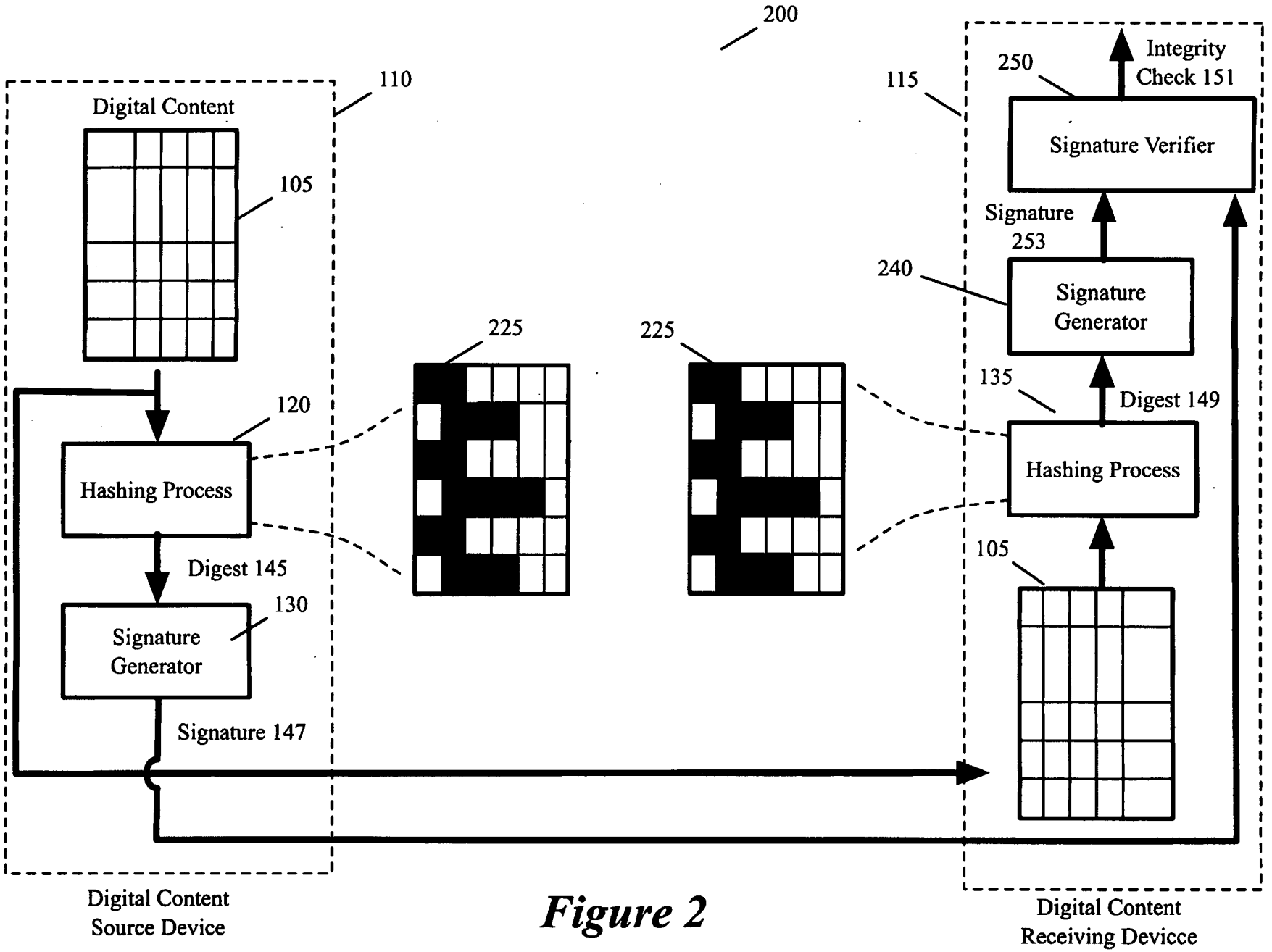

200
110
Digital Content
105
120
Hashing Process
Digest 145
130
Signature Generator
Signature 147
225
225
115
250
Integrity Check 151
Signature Verifier
Signature 253
240
Signature Generator
135
Digest 149
Hashing Process
105
Digital Content Source Device
Digital Content Receiving Devicce

Figure 2

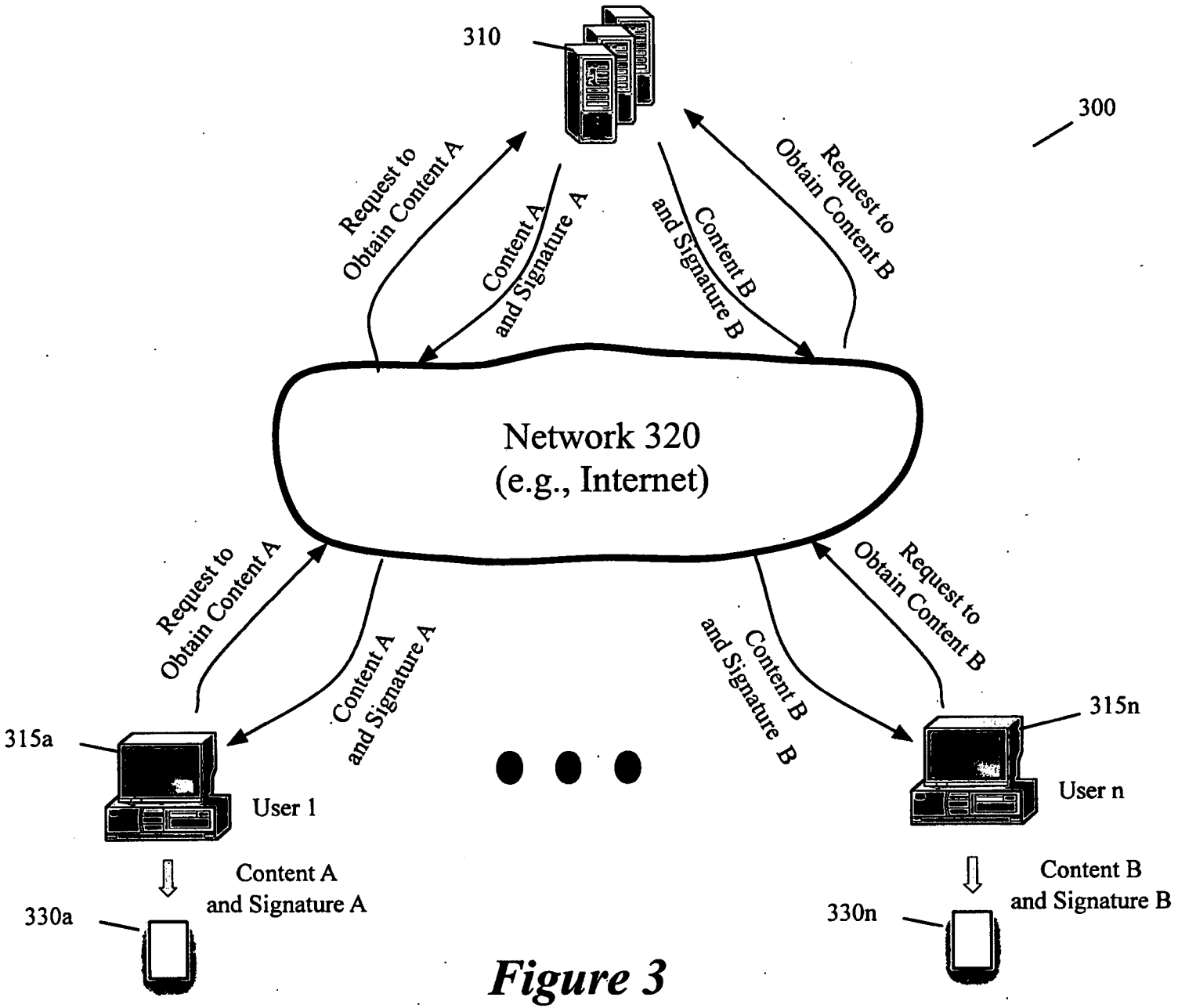

310
300
Request to Obtain Content A
Content A and Signature A
Content B and Signature B
Request to Obtain Content B
Network 320
(e.g., Internet)
Request to Obtain Content A
Content A and Signature A
Content B and Signature B
Request to Obtain Content B
315a
User 1
315n
User n
Content A and Signature A
Content B and Signature B
330a
330n

Figure 3

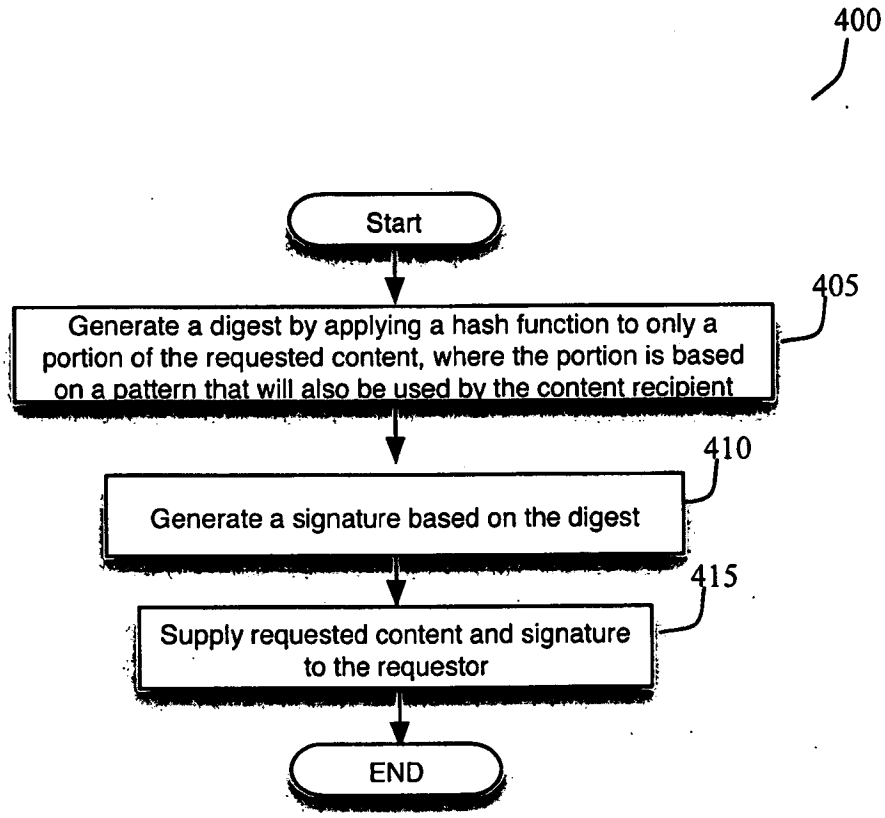

400
Start
405
Generate a digest by applying a hash function to only a portion of the requested content, where the portion is based on a pattern that will also be used by the content recipient
410
Generate a signature based on the digest
415
Supply requested content and signature to the requestor
END

Figure 4

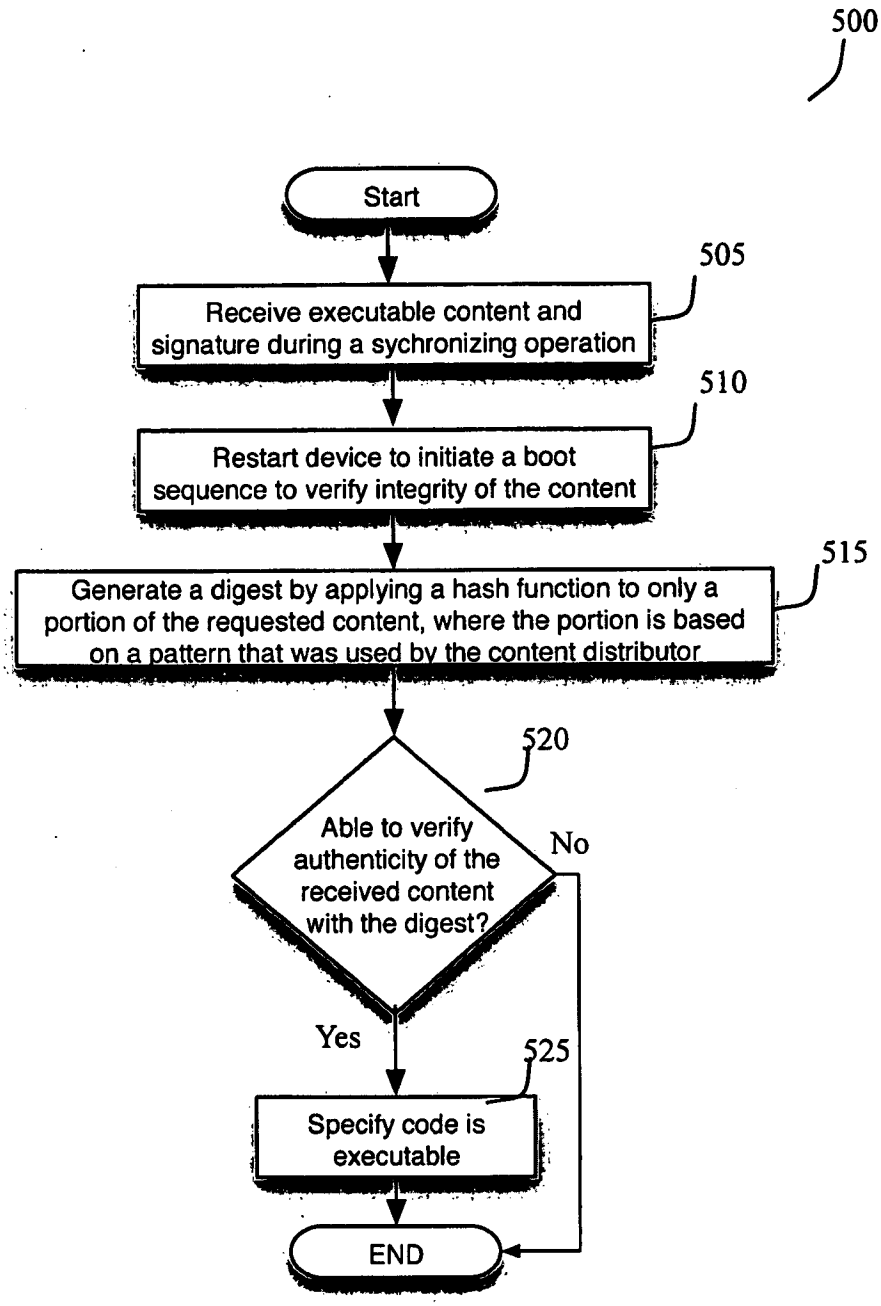

500
Start
505
Receive executable content and signature during a sychronizing operation
510
Restart device to initiate a boot sequence to verify integrity of the content
515
Generate a digest by applying a hash function to only a portion of the requested content, where the portion is based on a pattern that was used by the content distributor
520
Able to verify authenticity of the received content with the digest?
No
Yes
525
Specify code is executable
END

Figure 5

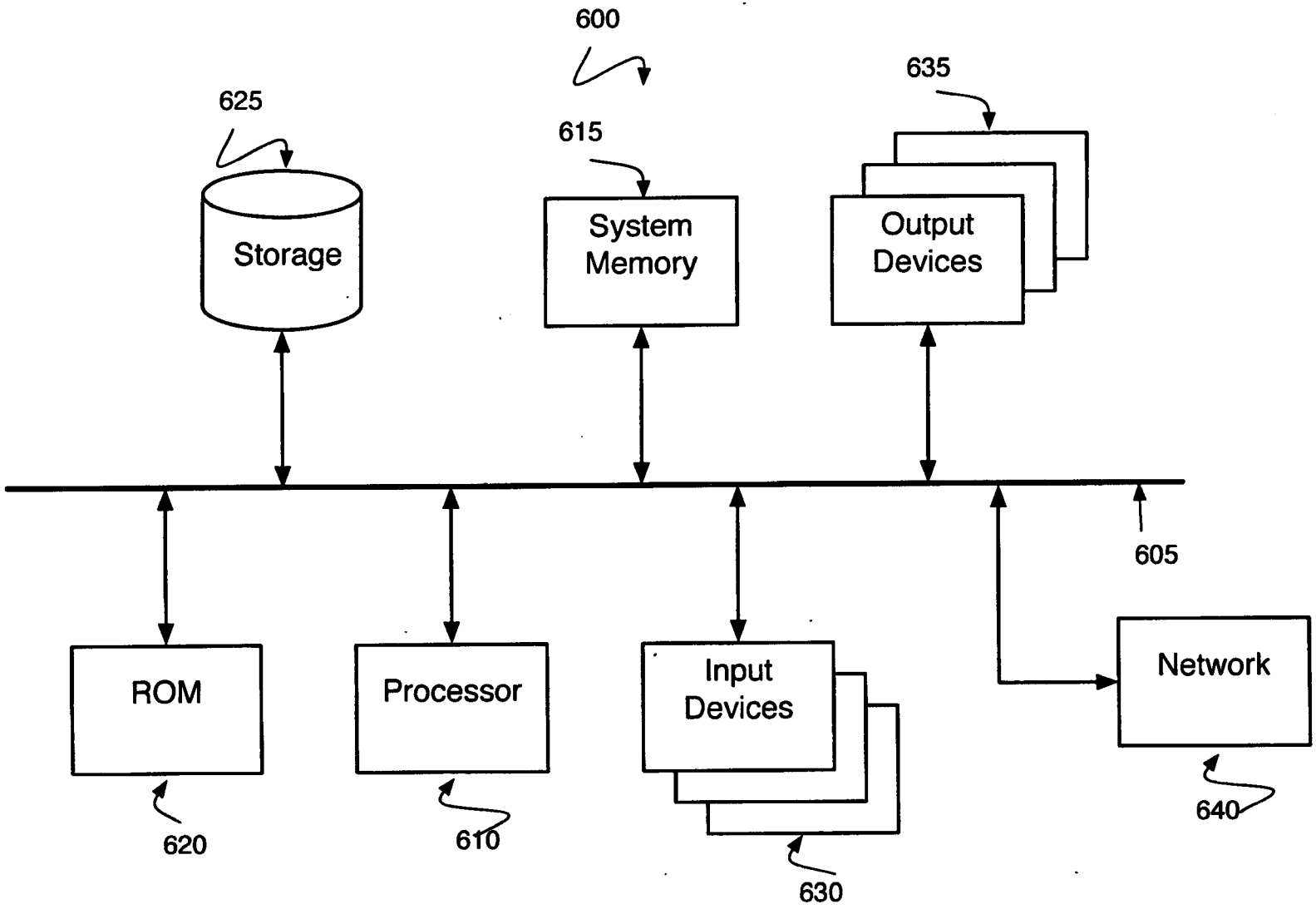

600
625
615
635
Storage
System Memory
Output Devices
605
ROM
Processor
Input Devices
Network
620
610
630
640

Figure 6