Förfarande för att skapa signaler för tidsstämpling av dokument och förfarande för tidsstämpling av dokument

För tillämpningar i den fysiska domänen finns det många kända förfaranden för tidsstämpling och integritetsskydd av dokument, såsom brev. Sådana förfaranden innefattar till exempel signaturer, förseglingar, offentliga notariseringsarrangemang och så vidare. Kontrollen av sådana tidsstämplar och integritetsskyddande åtgärder är ofta beroende av den kontinuerliga, spårbara och icke-reversibla naturen hos materia i den fysiska domänen.

I den digitala domänen, där materians natur är diskret, inte alltid spårbar och ofta reversibel, finns det andra typer av problem som måste hanteras för att kunna tidsstämpla och integritetsskydda information.

Olika typer av kryptografiska metoder, där endast personer som kontrollerar vissa kryptografiska nycklar har tillgång till viss information, har utvecklats under de senaste decennierna, för användning i den datoriserade digitala domänen.

Vissa kryptografiska metoder använder envägsfunktioner, såsom vissa hashfunktioner, i syfte att skapa sådana kryptografiska nycklar. En fördel med envägsfunktioner av tillräcklig kvalitet är att det är praktiskt taget omöjligt att beräkna ingångsdata till en envägsfunktion givet utgångsvärdet från envägsfunktionen, varför förekomsten av en viss kryptografisk nyckel kan användas som bevis på existensen av sagda ingångsdata före det att beräkningen utfördes.

En känd teknik är kopplad tidsstämpling, där flera digitalt lagrade dokument hashas vid olika på varandra följande tidpunkter, och där varje hash innehåller hashen av ett tidigare

dokument genom konkatenering. Sådana hashar publiceras periodiskt i allmänt tillgängliga publikationer, såsom tidningar. Eftersom förekomsten av varje länkad hash implicerar den tidigare existensen av de uppgifter på vilka hashen baseras, medför en sådan metod är det i praktiken är omöjligt att bakdatera ett visst dokument, inom gränserna för publiceringsfrekvensen. Vidare kan ordningen i vilken dokument skapas skyddas. Se till exempel WO2007/072468 A1.

Vidare är det känt att använda så kallade merkleträd i denna typ av tillämpningar. Ett merkleträd är en trädstruktur där datainnehållet i varje nod är utgångsvärdet från en envägsfunktion vars indata är en konkatenering av vardera av nodens barnnoders datainnehåll. Detta åstadkommer ett snabbt sätt att verifiera integriteten för stora datamängder ifall rotnodens datainnehåll tas emot från en betrodd källa. Se exempelvis US4309569 och EP0932109 A2.

Annan tidigare känd teknik med en relation med föreliggande uppfinning innefattar följande:

US5136646 och 5136647 beskriver båda sätt att tidsstämpla dokument, där en tillhandahållande part använder en envägsfunktion för att skapa en verifierbar kod innefattande en aktuell tidsstämpel. Förfarandet är rekursivt och använder tidigare tidsstämplade dokument.

US6381696 B1 beskriver ett förfarande för autentisering av dokument, där transienta kryptografiska nycklar används, vilka nycklar endast är giltiga under ett visst respektive tidsintervall och därefter förstörs.

US6742119 B1 och US7490241 B1 beskriver båda förfaranden för tidsstämpling av ett dokument, varigenom en central part som har en pålitlig klocka validerar en tidsstämpel som utförts av en dokumentskapande part.

US8312284 beskriver ett förfarande för tidsstämpling av ett dokument, såsom ett digitalt fotografi, varvid dokumentet kringgärdas av en tidigare och en senare tidsstämpel.

US2007/0179748 A1 beskriver en mätanordning med inbyggda funktioner för att tidsstämpla mätvärden kontinuerligt med hjälp av en privat nyckel.

US2009/0067667 A1 beskriver ett förfarande för att skydda integriteten för bildmetadata genom att införliva en kodad version av sådant metadata i en vattenstämpel i bilden.

WO1999/035785 A1 beskriver olika sätt att skydda integriteten för, och tidsstämpling av, dokument över flera versioner och med hjälp av envägshashfunktioner.

WO2006/075566 A1 beskriver förfaranden för att garantera äktheten i bilder, som exempelvis dokumenterar försäkrad egendom, inklusive digital bearbetning och specifikt anpassat inspelningsutrustning.

JP2008/216342 A beskriver ett förfarande för att verifiera äktheten hos en kriminalteknisk analys av en dators hårddisk, varvid analysen fångas på film. Kedjade hashfunktioner används för att säkerställa synkronisering.

JP2001022848 beskriver ett digitalt notariseringsförfarande för att bevisa äkthet och tidpunkt för elektroniska dokument.

CA 2317139 beskriver ett förfarande för tidsstämpling av ett elektroniskt dokument, varvid en kombinerad bearbetning beräknas för ett flertal dokument.

Ett problem med den tidigare kända tekniken är att i efterhand kunna fastställa, på ett trovärdigt sätt, att ett dokument faktiskt tidsstämplats efter en viss historisk tidpunkt. För sådan fastställelse är det i vissa fall inte tillräckligt att en trovärdig tredje part helt enkelt säger att så var fallet.

Föreliggande uppfinning löser de ovan beskrivna problemen.

Således hänför sig föreliggande uppfinning till ett förfarande för att skapa en signal för tidsstämpling av dokument, och kännetecknas av att förfarandet innefattar följande steg: a) välja ett digitalt lagrat referensdokument, vilket referensdokument är en digital beskrivning eller sampling av det aktuella tillståndet för en viss fysisk referenskälla och/eller informationsreferenskälla vid en viss första tidpunkt, varvid äktheten hos varje referensdokument kan verifieras genom att konsultera en eller flera offentligt tillgängliga informationskällor beträffande det historiska tillståndet för nämnda referenskälla; b) använda referensdokumentet som ett av åtminstone ett ingångsvärde till en envägsfunktion, och beräkna motsvarande utgångsvärde från envägsfunktionen; c) uppdatera signalen baserat på nämnda utgångsvärde, så att nämnda utgångsvärde utgörs av eller kan bestämmas baserat på värdet av signalen; och d) upprepa från a) med ett annat digitalt lagrat referensdokument som är en digital beskrivning eller sampling av det aktuella fysiska tillståndet och/eller informationstillståndet för samma eller en annan referenskälla vid en senare tidpunkt.

I det följande kommer föreliggande uppfinning att beskrivas i detalj, med hänvisning till följande ritningar:

Figur 1 är en översiktsvy av ett system för utförande av ett förfarande i enlighet med föreliggande uppfinning;

Figur 2 är en översiktsvy över ett förfarande för att skapa en signal för tidsstämpling av dokument i enlighet med föreliggande uppfinning;

Figur 3 visar förfarandestegen enligt ett förfarande enligt föreliggande uppfinning för att framställa en tidsstämplingssignal;

Figurerna 4a-4c är schematiska representationer av olika respektive sätt att tidsstämpla ett dokument;

Figurerna 5a-5d är schematiska representationer av olika respektive sätt att automatiskt inkorporera ett aktuellt värde på en tidsstämpel i ett dokument;

Figur 6 är en schematisk representation av en dynamiskt uppdaterad webbsida i enlighet med föreliggande uppfinning;

Figurerna 7A och 7B illustrerar schematiskt ett förfarande för att tillhandahålla ett sätt för att verifiera integriteten hos ett dokument i enlighet med uppfinningen;

Figurerna 8a och 8b visar schematiskt ett förfarande för att tillhandahålla ett sätt att verifiera integriteten hos ett dokument i enlighet med uppfinningen, vilket dokument publicerats på internet;

Figur 8c illustrerar schematiskt ett förfarande för filtrering av en webbsida i enlighet med föreliggande uppfinning;

Figurerna 9a och 9b visar respektive förfarandesteg för att verifiera integriteten hos ett dokument respektive tillhörande data;

Figur 10 illustrerar schematiskt ett förfarande enligt föreliggande uppfinning för att bevisa att en informationsström tillhandahålls i realtid; och

Figur 11 illustrerar schematiskt ett förfarande för att verifiera integriteten av data i en databas.

Alla figurer delar samma hänvisningssiffror och beteckningar för liknande eller likadana delar.

Häri används följande beteckningar med följande respektive betydelser:

Ett "dokument" är en information, såsom en text, en bild, ett ljudklipp, ett rörligt bildklipp, såsom en film eller liknande, eller en kombination av flera sådana informationer, som antingen är digitalt lagrade eller som kan samplas och sedan lagras i digital form.

Att "sampla" ett dokument innebär att omvandla ett dokument från analog form till digital form. Att "sampla" ett verkligt fysiskt fenomen innebär att omvandla analog information som samlats in i samband med nämnda fenomen och att konvertera sådan insamlad information till digital form. Alternativt kan att "sampla" innebära att ta emot eller hämta digital information som representerar eller utgör ett dokument som redan har omvandlats till digital form, eller som finns i den digitala domänen.

Att "tidsstämpla" ett dokument betyder att införa eller skapa en information, vilken information lagras tillsammans med dokumentet som en del av dokumentet eller på ett sätt som garanterat kan återassocieras med dokumentet, och som medför att, vid ett senare tillfälle, en tidpunkt kan fastställas vid vilken tidsstämplingen inträffade. Ett exempel på en sådan tidsstämpling är att skapa en signatur (se definition nedan) för dokumentet och att lagra signaturen och associera den med det aktuella dokumentet.

En "referenskälla" är en viss väldefinierad informationskälla som kan samplas, beskrivas eller användas som den är för att få fram ett referensdokument som beskriver ett aktuellt tillstånd för referenskällan. Exempel på referenskällor innefattar aktuella priser för vissa fördefinierade börshandlade aktier; den nuvarande ställningen i ett sportevenemang; den aktuella bildramen i ett offentligt sänt live-tv-program eller en för tillfället sänd ljudsignal i ett sådant program eller ett offentligt sänt liveradioprogram; och den nuvarande förstasidan för en tidning på internet.

Ett "referensdokument" är en digital sampling, beskrivning eller ögonblicksbild av det aktuella tillståndet, vid en viss tidpunkt, för en viss referenskälla med vilken referensdokumentet är associerat. Ett referensdokument är "externt tillhandahållet" i den meningen att referenskällan är en källa som är extern i förhållande till systemet 100.

En "envägsfunktion" är en funktion vars ingångsvärde är i praktiken omöjligt att fastställa baserat endast på det motsvarande utgångsvärdet från funktionen, och som är i huvudsak ett till ett i den meningen att, i de praktiska tillämpningarna som beskrivs häri, två olika ingångsvärden i praktiken alltid kommer att resultera i två olika utgångsvärden. Exempel innefattar många hashfunktioner som är konventionella i sig, såsom SHA-hashfunktioner, såsom SHA-1, SHA-2 och SHA-3, såväl som MD5.

En "offentligt publicerad" information eller ett sådant dokument är publicerat på ett sådant sätt så att den eller det är lätt tillgänglig för en tillräckligt bred publik, och över tillräckligt lång tid, för att en tredje part sannolikt kommer att kunna verifiera tiden för publikation och innehållet i informationen eller dokumentet exakt som de var vid datumet och tiden för publicering, även om en viss tid, såsom flera år, har förlöpt efter offentliggörandet.

En "signatur" av ett dokument är ett värde som skapas så att det består av, innehåller eller har beräknats baserat på utgångsvärdet för en viss signaturenvägsfunktion, till vilken åtminstone en del av dokumentet är ett av ett eller flera ingångsvärden, på ett sådant sätt att signaturen är väsentligen omöjlig att beräkna utan att ha tillgång till relevant information om dokumentet ifråga.

En "bevissignatur" är en signatur som beräknas för ett dokument för att, vid en senare tidpunkt, kunna bevisa tillgången till relevant information om dokumentet vid tidpunkten för skapandet av bevissignaturen.

En "verifieringssignatur" är en signatur som skapas i relation till ett visst dokument för jämförelse med en bevissignatur som har beräknats tidigare.

En "digitalt kodad vattenstämpel" är en information som är inkodad i ett digitalt lagrat dokument på ett sådant sätt att det bara syns eller märks när dokumentet observeras under

vissa förutbestämda villkor, till exempel när dokumentet underkastas vissa algoritmer, och som annars bara har en försumbar eller osynlig effekt på dokumentet.

Figur 1 visar ett system 100 i enlighet med föreliggande uppfinning, innefattande en central styranordning 101 och följande digitala gränssnitt:

- ett dokumentinläsningsgränssnitt 102, anordnat att läsa olika referensdokument D1, D2, D3, företrädesvis referensdokument av flera olika typer och associerade med olika referenskällor;
- ett tidsstämplingssignalpubliceringsgränssnitt 103, anordnat att publicera värdet för en tidsstämplingssignal i form av en tidssekvens av värden vilka kommer till uttryck i olika dokument P1, P2, P3, helst dokument av flera olika typer, som publicerats vid på varandra följande tidpunkter, vilket gränssnitt 103 också kan vara anordnat att på begäran kunna kommunicera ett tidsstämplingssignalvärde (se nedan) till tredjepartssystem;
- ett dokumentmottagnings- och tidsstämpelleveransgränssnitt 104, anordnat att tillåta en användare 131 att, via en datoranordning 130, leverera ett dokument A till systemet 100 för tidsstämpling, och att leverera en motsvarande tidsstämpel eller ett tidsstämplat dokument till datoranordningen 130; och
- ett dokumentverifieringsgränssnitt 105, anordnat att erhålla verifieringsbegäran från en datorenhet 140 och att leverera verifieringsstatusrapporter till datoranordningen 140.

Eftersom varje dokument D1, D2, D3 utgör ett respektive samplat tillstånd för en respektive referenskälla, är gränssnittet 102 anordnat att utföra sådan sampling för en eller flera

referenskällor, och därmed skapa referensdokument D1, D2, D3, och/eller att helt enkelt ta emot sådana referensdokument D1, D2, D3. På samma sätt kan gränssnittet 103 anordnas att helt enkelt skicka dokument P1, P2, P3 till en eller flera publicerande parter, och/eller att beställa publicering med hjälp av en eller flera publiceringstjänster av självbetjäningstyp.

Varje publicering P1-P3 bör publiceras offentligt över åtminstone en kanal som kontrolleras av en tredje part annan än operatören av systemet 100, företrädesvis över flera parallella kanaler, där varje sådan kanal bör tillhandahålla väsentligen permanent fortbestånd i den meningen att dokumenten P1-P3 och tiden och datumet för deras publicering bör vara offentligt tillgängliga även efter det att flera år har förlupit efter publiceringen; vara lätt tillgängliga för ett stort antal tredje parter; lätt kunna hänvisas till; och helst inte kunna modifieras av den part som beställer publiceringen. Exempel på detta är olika publiceringskanaler på internet, såsom populära bloggplattformar, Twitter (registrerat varumärke), videopubliceringssajter som YouTube (registrerat varumärke), nyhetssidor, e-post till förutbestämda mottagare; papperspublikationer såsom tidningar och bulletiner; etermedia som radio, TV, text-TV, etc.; och telekomplattformar såsom SMS (eng. Short Message Service) till förutbestämda mottagare.

Varje sådan kanal bör ge möjlighet till ett brett spektrum av tredje parter att, vid en senare tidpunkt, helst minst flera år efter publiceringstidpunkten, kunna verifiera publiceringstidpunkten för den publicerade informationen.

Helst ska minst tio olika plattformar användas parallellt, helst minst tio olika plattformar som är oberoende av

varandra i termer av gemensamt ägande och kontroll, helst också lydande under olika lagstiftningar.

Systemet 100 innefattar vidare en databas 106 och en klocka 107, som båda tillsammans med gränssnitten 102, 103, 104, 105, kommunicerar med den centrala styranordningen 101. Klockan 107 kan vara intern i systemet 100, och i detta fall periodiskt synkroniserad med en extern, betrodd klocka, men företrädesvis är klockan 107 i form av en klocksignal som tas emot från en betrodd extern part.

Systemet 100 är implementerat som en datoriserad anordning, och som sådan kan systemet 100 innefatta en eller flera sammankopplade datorer, och funktionalitet som är implementerad som logik i form av lämplig hårdvara och/eller mjukvara. Datoranordningarna 130, 140 i figur 1, samt andra datoranordningar som avbildas i andra figurer häri, är endast ämnade att vara illustrativa och kan utgöras av en eller flera datorer, mobiltelefoner, datornätverk eller någon annan typ av anordning som är kapabel till automatiserad kommunikation över de digitala gränssnitten 104, 105.

Figur 2 är en förenklad illustration av ett förfarande enligt föreliggande uppfinning. Pilen T står för tiden, och de olika händelserna som illustreras i figur 2 är ordnade i tidsled på det sätt som visas, förutom det envägsfunktionsträd som visas längst ned till höger, i en ruta med kanter i form av brutna linjer. Det senare envägsfunktionträdet utgör snarare ett ögonblickstillstånd för en viss envägsfunktionsstruktur vid tiden strax före publiceringen av P6. Ett exempel på ett sådant envägsfunktionsträd är ett konventionellt hashträd.

I figur 2 representerar A, B och D1-D9 olika digitalt lagrade referensdokument; D1#-D9# representerar respektive utgångs-

värden för en viss envägsfunktion vars respektive ingångsvärde är det respektive referensdokumentet D1-D9; T#1-T#8 representerar respektive värden för en signal enligt föreliggande uppfinning för tidsstämpling av dokument, eller mellanliggande värden för beräkning av sådana signalvärden; och P1-P8 representerar publicerade respektive värden för en sådan signal för tidsstämpling av dokument. Således kan antingen T#1-T#8 eller P1-P8 användas som tidsstämplingssignalen (som beskrivs nedan). Om T#1-T#8 används som tidsstämpelsignalen publiceras de företrädesvis på ett sätt som motsvarar det som beskrivs häri i förhållande till P1-P8. Oavsett vilken ström av värden som används som tidsstämpelsignalen, bör denna signal uppdateras ofta, vara väldefinierad och lagras i databasen 106, så att det är möjligt att senare verifiera de historiska värdena för tidsstämplingssignalen.

A och B är digitalt lagrade dokument, såsom texter, ordbehandlingsdokument, bilder, videofilmer och så vidare, som tillhandahålls av användaren 131 till systemet 100; och D1-D9 är dokument som automatiskt valts av systemet 100 baserat på förutbestämda associeringar mellan systemet 100 och motsvarande referenskällor.

$\#_1$, $\#_2$ och $\#_3$ representerar respektive envägsfunktioner. Envägsfunktionen $\#_1$, som används för att framställa D1#-D9#, är inte nödvändigtvis densamma som envägsfunktionen $\#_2$, som används för att framställa T#1-T#8, eller $\#_3$, som används för att framställa P1-P8. Även om det är föredraget att samma envägsfunktion till exempel används för att framställa alla utgångsvärden D1#-D9#, skulle det vara möjligt att ändra vilken envägsfunktion som används, ifall information, beträffande vilken envägsfunktion som användes för vilken funktion och vid vilken tidpunkt, lagras i databasen 106 för senare användning. Varje respektive envägsfunktion kan utgöras av en

enda funktion eller ett aggregat av funktioner, och kan även acceptera andra ingångsdata än de ingångsdata som visas i figur 2, så länge som ett sådant aggregat i sig utgör en envägsfunktion med ett utgångsvärde som återigen kan beräknas på deterministiskt sätt vid en senare tidpunkt, givet alla de använda ingångsvärdena.

Figur 3 illustrerar förfarandestegen i ett förfarande för att åstadkomma en signal för tidsstämpling av dokument i enlighet med föreliggande uppfinning. En sådan signal kan exempelvis vara i form av ett alfanumeriskt värde eller en grafisk kod, såsom en QR-eller streckkod, som representerar ett sådant värde, eller har någon annan typ av informationsformat, och som publiceras, överförs, är publicerbar eller är överförbar.

I ett första steg väljs ett digitalt lagrat referensdokument A, B, D1, D2, D3, D4, D5, D6, D7, D8 eller D9. Referensdokumentet är en digital beskrivning eller en sampling av det aktuella tillståndet, vid en viss första tidpunkt, för en viss referenskälla. Äktheten hos varje referensdokument kan i efterhand verifieras genom konsultation av en eller flera publikt tillgängliga informationskällor beträffande det historiska tillståndet för nämnda referenskälla.

Det aktuella tillståndet för en och samma referenskälla kan samplas vid flera på varandra följande tidpunkter, för att på så sätt skapa flera olika referensdokument. Att referensdokumentet "väljs" innebär att en referenskälla väljs och att det digitalt lagrade referensdokument åstadkoms, exempelvis genom direkt sampling av tillståndet för referenskällan, genom att avläsa det aktuella tillståndet för referenskällan eller genom att ta emot en digital representation av det aktuella tillståndet för referenskällan.

I ett nästa steg, såsom illustreras i figurerna 2 och 3, används en envägsfunktion, såsom till exempel ett aggregat av flera envägsfunktioner, och ett utgångsvärde för envägsfunktionen beräknas för vissa indata. Enligt uppfinningen används det valda referensdokumentet som ett av åtminstone ett ingångsvärde till envägsfunktionen.

I figur 2 illustreras flera olika möjliga alternativ för envägsfunktionen. För dokumentet A är exempelvis envägsfunktionen $\#_2$, och motsvarande utgångsvärde T#1 beräknas med hjälp av A och D123#, vilket senare värde i sig är utgångsvärdet för en tidigare använd envägsfunktion $\#_1$ och beroende av dokumenten D1-D3. A och D123# kan, exempelvis, konkateneras innan de används som ett enda ingångsvärde till $\#_2$, alternativt kan $\#_2$ utformas att acceptera åtminstone två ingångsparametrar. För dokumentet D4 utgörs envägsfunktionen av de respektive envägsfunktionerna $\#_1$ och $\#_2$, som används efter varandra. För dokumenten D1, D2 och D3 används $\#_1$, $\#_1$ och $\#_2$ i serie efter varandra, med mellanliggande inmatning av andra parametrar D1#, D2# respektive D3#.

Således kan envägsfunktionen vara en enstaka envägsfunktion eller ett aggregat av flera envägsfunktioner, och samma envägsfunktion eller aggregat av envägsfunktioner kan men behöver inte användas för alla referensdokument A, B, D1-D9. Det viktiga är att referensdokumentet i fråga är ingångsparameter till en envägsfunktion i den meningen att det i praktiken är omöjligt att beräkna utgångsvärdet utan att känna till värdet för det motsvarande och ifrågavarande referensdokumentet. Således kan även annan information, såsom andra utgångsvärden från envägsfunktioner, användas som ingångsparametrar till envägsfunktionen vid beräkning av motsvarande utgångsvärde. Företrädesvis lagras samtliga ingångsvärden, och deras an-

vändning, helst i databasen 106, för enkel återberäkning av utgångsvärdet vid en senare tidpunkt.

I ett nästa steg bringas tidsstämplingssignalen att uppdateras baserat på nämnda beräknade utgångsvärde, så att nämnda utgångsvärde utgörs av eller kan bestämmas baserat på värdet av signalen.

I den exemplifierande utföringsform som illustreras i figur 2 publiceras signalvärdet som dokumenten P1-P8, efter ytterligare beräkningar baserade på värden för T#1-T#8, såsom beskrivs nedan. I alternativa utföringsformer kan emellertid värdena för T#1-T#8 utgöra signalvärdet själva. Det viktiga är att det vid en senare tidpunkt är möjligt att härleda varje motsvarande publicerat signalvärde T#1-T#8 eller P1-P8 baserat på tillräcklig kunskap om referensdokumenten A, B, D1-D9 och all annan information som användes vid beräkning av följden av tidsstämplingssignalvärden, och om hur dessa beräkningar utfördes.

Figur 2 visar, i rektangeln med streckade linjer, den specifika beräkningen av P6. I den exemplifierande utföringsform som illustreras i figur 2 utförs en motsvarande beräkning, vid varje respektive tidpunkt och för varje publicerat signalvärde P1-P8. En trädstruktur, exempelvis ett konventionellt hashträd, växes steg för steg, allteftersom nya envägsfunktionsutgångsvärden T#1-T#8 beräknas.

Nämnda värden T#1-T#8 lagras logiskt som bladen i trädstrukturen. Sedan används en viss trädenvägsfunktion $\#_3$ för att digerera bladvärdena T#1-T#8 lager för lager i trädet, tills en trädrot nås, vilken trädrot beror, via trädenvägsfunktionen $\#_3$, på varje blad som är en förfader till nämnda trädrot. Mer specifikt beräknas, för varje föräldranod, ett respektive

utgångsvärde för trädenvägsfunktionen $\#_3$, där det respektive signalutgångsvärdet från envägsfunktionen $\#_2$ och/eller det respektive beräknade utgångsvärdet från trädenvägsfunktionen $\#_3$, för var och en de respektive barnnoderna för föräldranoden ifråga, används som ingångsvärden för trädenvägsfunktionen $\#_3$ för föräldranoden. Således används T#1 och T#2 som ingångsvärden i trädenvägsfunktionen $\#_3$, vilken åstadkommer utgångsvärdet I#12. I#12 används, i sin tur tillsammans med utgångsvärdet I#34, vilket beräknats med T#1 och T#2 som ingångsvärden, för att, återigen via envägsfunktionen $\#_3$, beräkna utgångsvärdet I#1234. Slutligen används I#1234 tillsammans med I#56, för att, via envägsfunktionen $\#_3$, beräkna I#123456, vilket utgör trädrotutgångsvärdet.

Det är sedan detta rotvärde I#123456 som, vid en tidpunkt efter tillsatsen av T#6 och omberäkning av trädet, publiceras som P6. Motsvarande kan vara sant vad avser värdena T#1-T#5, T#7-T#8 respektive de publicerade dokumenten P1-P5, P7-P8.

Med andra ord är det trädrotens utgångsvärde från trädenvägsfunktionen, eller ett värde som har beräknats baserat på detta utgångsvärde, som publiceras offentligt som P6.

Således innefattar endast lövnoderna envägsfunktionsutgångsvärden som matas in till trädet, och varje föräldranod är en envägsfunktionsdigerering av sina barn. Trädet växes genom att lägga till fler barn och att sedan beräkna om motsvarande del av trädet, vilket åstadkommer en ny rotnod.

I ett nästa steg upprepas därefter proceduren, och ett annat digitalt lagrat referensdokumentet väljs, vilket referensdokument är en digital beskrivning eller sampling av det aktuella fysiska- och/eller informationstillståndet för samma eller en annan referenskälla vid en senare tidpunkt. Efter

bearbetning av exempelvis referensdokument D4, vilket resulterar i beräkningen av T#4 och publiceringen av P4, bearbetas referensdokumentet D5, vilket resulterar i beräkningen av T#5 och publiceringen av P5. Som ett resultat av detta växer trädet med ytterligare en lövnod, nämligen T#5. På så sätt kan trädet så småningom växa till att bli mycket stort, potentiellt innefattande alla tidigare T#-värden sedan förfarandets start. Ändå är det beräkningsmässigt billigt att bearbeta trädet, eftersom endast en begränsad delmängd av trädet måste ändras för att till exempel lägga till en nod, och eftersom en verifiering involverar endast den respektive grenen ifråga.

När trädet växer sätts fler lövnoder till, och som en följd därav kommer antalet föräldranodskikt att växa. Eftersom kapaciteten hos trädet växer exponentiellt med antalet skikt, kommer endast ett begränsat antal skikt att krävas även för ett mycket stort antal lagrade löv, såsom flera miljarder löv eller till och med väsentligen större antal.

Det är föredraget att alla, eller åtminstone de flesta, beräknade tidsstämplingssignalvärden sedan förfarandets start lagras i trädet, och att varje trädrot som publiceras offentligt är beroende av alla tidigare beräknade signalvärden.

Det är vidare föredraget att åtminstone åtta underordnade noder är associerad med varje föräldranod innan föräldranoden ifråga anses vara fullbelagd.

När trädet växer så att ett nytt lager skapas, blir den tidigare rotnoden en barnnod i det nya, växta trädet, och en ny rotnod införs.

De referenskällor som används kan vara av olika typer. Enligt en föredragen utföringsform är åtminstone en referenskälla en uppsättning specificerade offentligt publicerade immateriella informationer, vilkas tillstånd inte är kända på förhand. Exempel på sådana referenskällor innefattar en uppsättning börskurser från en eller flera officiellt erkända börser; en uppsättning vinnande lottnummer från stora lotterier; eller slumpmässigt utvalda uppgifter från tredje part på en allmänt använd, offentligt tillgänglig publiceringsplattform, såsom YouTube (registrerat varumärke) eller Twitter (registrerat varumärke). Att tillståndet för referenskällan "inte är känd i förväg" ska tolkas så att det skulle ha varit väsentligt omöjligt att förutse tillståndet innan själva tidpunkten för samplingen eller valet av referensdokument, i den meningen att utgångsvärdet från en envägsfunktion som accepterar det valda referensdokumentet som ingångsvärde skulle ha varit praktiskt taget omöjligt att förutse före tiden för valet av referensdokumentet.

Enligt en föredragen utföringsform är åtminstone en referenskälla, på motsvarande sätt, en offentligt publicerad, konkret fysisk händelse, vars tillstånd inte är känt på förhand. Exempel utgörs av ett förutbestämt specifikt idrottsevenemang, där ett motsvarande referensdokument utgörs av tagna bilder eller upptagna ljud från idrottsevenemang, till exempel från ett förutbestämt programföretag eller resultatdata; specificerade nyhetsbevakningar, där referensdokumentet är bilder eller ljud från en förutbestämd nyhetssändning som täcker sådana nyheter, textmaterial från en förutbestämd utgivare som täcker nyhetshändelsen ifråga, eller statistiska data beträffande nyhetshändelsen ifråga; meteorologiska data; data beträffande offentligt publicerade vetenskapliga framsteg inom ett specificerat område, såsom till exempel utforskning av rymden; och så vidare.

Kombinationer av sådana källor kan också naturligtvis användas parallellt. Det viktiga är att varje referenskälla och metoden för att välja motsvarande referensdokument är tillräckligt väl definierade så att det är möjligt att fastställa det faktiska och specifika historiska värdet för referensdokument vid en senare tidpunkt, till exempel fler än ett, eller helst flera, år efter tidpunkten för valet av referensdokument ifråga. Det inses dock att även om vissa, eller till och med de flesta, av referenskällorna blir otillgängliga för retroaktiv verifiering efter en viss tid, kommer ett förfarande enligt uppfinningen att kunna utföra trovärdiga verifieringar av dokumenttidsstämplar och de relaterade verifieringsuppgifter som beskrivs häri, på grund av den redundans som åstadkoms genom att använda tillräckligt många disparata referenskällor.

För att underlätta sådana senare återupprättanden av referensdokument, associeras minst ett, helst samtliga, av referensdokumenten A, B, D1-D9, helst tillsammans med andra data som används som ingångsvärden till en eller flera använda respektive envägsfunktioner, med det respektive beräknade envägsfunktionsutgångsvärdet D1#-D9#, D123#, D56#, D78#, T#1-T#8 och/eller det uppdaterade och publicerade signalvärdet P1-P8, och referensdokumentet, eventuellt tillsammans med ytterligare information, lagras företrädesvis också i databasen 106 för framtida hänvisning. Dessutom är det föredraget att tidpunkten för skapandet och/eller valet av varje referensdokument D1-D9 lagras i databasen 106, och associeras med respektive referensdokument.

Med hjälp av ett förfarande enligt föreliggande uppfinning åstadkoms en tidsstämplingssignal som kan användas för tidsstämpling, så att det för tidsstämplar är möjligt att retro-

aktivt bevisa att de inte fanns före en viss tidpunkt. Det finns nämligen i praktiken inget sätt att förutse det exakta innehållet i ett visst referensdokument, som till exempel D7, före samplingen av den motsvarande referenskällan och därmed skapandet av D7. Eftersom publiceringen P6 beror på D7 i en relation av envägstyp, kunde P6 inte i praktiken har beräknats före det att D7 var känd. Därför kan det garanteras att tidsstämplingssignalvärdet P6 inte existerade före tidpunkten för skapandet av D7. Genom att verifiera att D7 faktiskt är en korrekt representation av tillståndet i motsvarande referenskälla vid den påstådda tidpunkten för skapandet eller valet av D7, kan det verifieras att P6 inte existerade före denna tidpunkt.

Om tredje part exempelvis begär bevis på att P6 inte existerade innan en påstådd tidpunkt för skapandet av D7, räcker det med att tidsstämplingssignalens leverantör förser den tredje parten med värdena D8#, T#5, I#1234 samt vilken envägsfunktion eller -funktioner $\#_1$, $\#_2$, $\#_3$ som användes. Sedan kan den tredje parten utföra beräkningarna, och därmed verifiera att, med tillfredsställande statistisk säkerhet, inga andra referensdokument än D7 kunde ha givit upphov till det publicerade värdet P6. Det noteras att den tredje parten inte behöver förses med de verkliga värdena för alla andra dokument, till exempel A eller D1-D6 eller D8. Det är tillräckligt att tillhandahålla motsvarande utgångsvärden för respektive envägsfunktioner. Detta är fördelaktigt, eftersom en del referensdokumentinformationen kan vara hemlig eller känslig.

Således innefattar ett förfarande enligt föreliggande uppfinning för att verifiera ett tidsstämplingssignalvärde, som beräknats i enlighet med föreliggande uppfinning, att tillhandahålla information till en begärande part beträffande ett offentligt publicerat digitalt lagrat referensdokument av den

ovan beskrivna typen, som inte kunde ha skapats före en viss tidpunkt, såväl som en specificering av någon envägsfunktion eller -funktioner som använts för att beräkna tidsstämplingssignalvärdet, och eventuella ingående variabler som användes för sådana beräkningar bortsett från det nämnda referensdokumentet.

En tidsstämplingssignal i enlighet med föreliggande uppfinning kan exempelvis användas för att garantera färskheten för ett dokument som är tidsstämplat med hjälp av signalen. Denna och andra tillämpningar beskrivs i närmare detalj nedan.

Enligt en särskilt föredragen utföringsform är åtminstone en, företrädesvis flera, av referenskällorna av typer vars respektive tillstånd typiskt förändras mycket ofta, företrädesvis flera gånger varje sekund. Ett exempel på detta är att referenskällan är förutbestämt och entydigt definierat videomaterial, såsom videomaterial från en förutbestämd videokamera; som utsänds av en förutbestämd sändningsstation; eller liknande. Företrädesvis är videomaterialet allmänt tillgängligt, till exempel via ett sändningsnät eller via internet. I detta fall används de enskilda bilderna i videoströmmen, eller kluster av sådana bilder, och/eller en tillhörande ljudström, som referensdokument. Att använda en sådan frekvent uppdaterad och frekvent samplad referenskälla gör det möjligt att åstadkomma en tidsstämplingssignal som uppdateras ofta och som därmed ger fin tidsgranularitet.

Vidare är det föredraget att det aktuella värdet för signalen kontinuerligt eller periodiskt publiceras, vilket visas i figurerna 1 och 2, i form av dokument P1-P8. Signalen kan också kontinuerligt eller periodiskt sändas till en förutbestämd mottagare. "Kontinuerligt" ska häri tolkas så att sig-

nalen publiceras eller sänds så snart signalvärdet ändras, och/eller med en viss minsta periodicitet.

Företrädesvis ändras signalens värde, och den uppdaterade signalen publiceras eller sänds, åtminstone en gång per minut, mer företrädesvis åtminstone en gång var tionde sekund, mest företrädesvis åtminstone en gång varje sekund.

Enligt en föredragen utföringsform leder ett tillägg av ett nytt trädlöv T#1-T#6 inte alltid automatiskt till publiceringen av ett nytt motsvarande dokument P1-P6. Nya dokument kan istället publiceras regelbundet, oavsett nytillskott av löv, och/eller på begäran om ett nytt tidsstämplingssignalvärde internt från systemet 100, till exempel i syfte att tidsstämpla ett inkommande dokument, eller härrörande från någon tredje part.

För att få bättre tidsgranularitet, bättre robusthet, bättre motståndskraft mot organiserade attacker från tredje part eller parter som kontrollerar referenskällor, och högre trovärdighet, är det dessutom föredraget att en uppsättning av flera olika referenskällor används parallellt, och att referensdokument som representerar olika referenskällor används som det respektive ingångsvärdet till en envägsfunktion $\#_1$ i olika respektive iterationer av förfarandet.

Det är också föredraget att åtminstone vissa, företrädesvis de flesta, helst åtminstone 90%, av de använda referensdokumenten, vilka i sig publiceras offentligt, regelbundet används utan att ursprunget till referensdokumentdata publiceras till tredje part, utan istället bara avslöjas i samband med en begäran om verifiering från en tredje part. Detta tillför ytterligare säkerhet till användningen av tidsstämplingssignalen.

Såsom visas i figur 2 föreligger ett återkopplingsförhållande mellan på varandra följande tidsstämplingssignalvärden, i form av ett beroende hos senare tidsstämplingssignalvärden av tidigare tidsstämplingssignalvärden för åtminstone ett, företrädesvis de flesta och mest företrädesvis väsentligen alla, tidsstämplingssignalvärden. Således innefattar ett sådant beroende tidstämplingssignalvärde T#1-T#8 eller P1-P8 ett föregående tidstämplingssignalvärde T#1-T#7 eller P1-P7, i den meningen att ett föregående eller aktuellt värde för tidstämplingssignalen, ett värde på vilket ett föregående eller aktuellt värde hos signalen är baserat, eller ett värde som beräknats baserat på ett sådant föregående eller aktuellt signalvärde, används som ett ingångsvärde till en envägsfunktion eller ett aggregat av envägsfunktioner som används för att beräkna värdet för tidsstämplingssignalvärdet ifråga.

Sådan återkoppling tillför redundans till tidsstämplingssignalen, eftersom viss förlust av information kan tolereras samtidigt som det är möjligt att retroaktivt beräkna de flesta tidsstämplingssignalvärdena. Olika typer av sådan återkoppling är exemplifierade i figur 2 enligt följande:

- Utgångsvärdet T#1 från envägsfunktionen #2, vilket i sig kan utgöra värdet för tidsstämplingssignalen vid tidpunkten ifråga, eller enbart användas för att beräkna tidsstämplingssignalvärdet P1, används som ingångsvärde till en envägsfunktion #2 för att få fram utgångsvärdet T#4, som i sig kan utgöra värdet för tidsstämplingssignalen vid denna senare tidpunkt, eller enbart användas för att beräkna värdet för tidsstämplingssignalen P4.
- På ett liknande sätt används D56#, vilket är utgångsvärdet från envägsfunktionen #1, som ingångsvärde till envägsfunktionen #2 både för beräkning av T#3 och, vid en

senare tidpunkt, T#5. På så sätt kommer både T#3, P3, T#5 och P5 att bero av D56#.

- Varje tidsstämplingssignalvärde eller mellanliggande värde T#2-T#8 beror av åtminstone ett tidigare sådant värde T#1-T#7, genom att detta värde används som ingångsvärde till envägsfunktionen #2. Detta är föredraget, eftersom det skapar en kedja av beroenden vilket gör det mycket svårt för en tredje part att reproducera tidstämplingssignalvärdet. I synnerhet är det föredraget att åtminstone regelbundet, snarare väsentligen varje gång ett tidsstämplingssignalvärde eller ett mellanliggande värde T#2-T#8 beräknas, detta bringas att vara beroende av åtminstone ett tidigare värde för T#1-T#7, helst det omedelbart föregående sådana värdet T#1-T#7. Det inses att motsvarande kan tillämpas vid beräkning av P2-P8.

Det inses att vissa, eller de flesta, av tidsstämplingssignalvärdena T#1-T#3, T#6-T#8 är beroende av åtminstone ett externt tillhandahållet referensdokument A, B, D1-D9, och beräknas som en direkt följd av valet av ett nytt motsvarande referensdokument. Vissa signalvärden T#4-T#5 skapas emellertid inte som en direkt följd av valet av ett nytt motsvarande referensdokument, utan av valet av vissa internt genererade informationer. I detta fall kan sådan information som sådan vara beroende av externt tillhandahållna referensdokument, och innefattar företrädesvis åtminstone ett tidigare beräknat signalvärde. Den senare typen av signalvärden används företrädesvis för att öka uppdateringsfrekvensen för tidstämplingssignalen. Enligt en föredragen utföringsform är, över tid, antalet signalvärden som är baserade på valet av ett nytt respektive externt tillhandahållet referensdokument i minoritet, helst finns det över tid åtminstone 10, hellre

åtminstone 100, signalvärden som är baserade på en internt genererad information för varje signalvärde som är baserat på ett externt tillhandahållet referensdokument.

Ett sätt att uppnå sådana tidsstämplingssignalvärden som inte är beroende av något externt tillhandahållet referensdokument är att återiterera trädnoder, såsom den aktuella trädroten, i den trädstruktur som visas i figur 2, tillbaka till bladnivå, genom att göra den återitererade trädnoden till en ytterligare bladnod. Detta kan göras med valfria tidsmellanrum, och kan användas för att öka publiceringsfrekvensen för dokumenten P1-P6 utöver frekvensen för faktiska tillskott av nya referensdokument. I kombination med vad som beskrivits ovan beträffande tillägg av nya trädblad T#1-T#6 som inte resulterar i en ny publicering av ett dokument P1-P6, kan således publiceringen av nya tidsstämplingssignaler P1-P6 göras oberoende av tillskott av referensdokument. Även om inflödet av nya referensdokument varierar, kan exempelvis en tidsstämplingssignal som uppdateras med jämna mellanrum, till och med mycket ofta, uppnås med hög tillförlitlighet och säkerhet. Det är föredraget att de data som är interna för systemet 100 och som används för att beräkna sådana tidsstämplingssignalvärden inte har specificerats för tredje part i förväg, eftersom detta skulle göra det möjligt att förutse framtida värden för tidsstämplingssignalen.

Enligt en föredragen utföringsform, som också visas i figur 2, tidsstämplas ett visst referensdokument B med det aktuella respektive värdet P6 för tidsstämplingssignalen, och åtminstone en del av en digitalt lagrad version av det vissa tidsstämplade dokumentet B, eller utgångsvärdet från en envägsfunktion till vilken ett ingångsvärde är det vissa dokument B, används som ingångsvärde för beräkning av ett efterföljande tidsstämplingssignalvärde T#8.

Sådan tidsstämpling av ett dokument B beskrivs i närmare detalj nedan, men kan till exempel innefatta inkorporerandet av tidsstämplingssignalvärdet P6 i dokumentet B i form av en bild eller en text. Sådan inkorporering av det aktuella värdet för tidsstämplingssignalen i ett referensdokument som används för att producera signalen kommer att påverka värdet för den efterföljande tidsstämplingssignalen T#8 eller P8. Genom att retroaktivt konsultera referensdokumentet B, kan det dåvarande tidsstämplingssignalvärdet således avläsas, och samtidigt är existensen av referensdokument B en nödvändig förutsättning för existensen av T#8. Därför lägger en sådan iteration av tidsstämplingssignalprocessen, involverande ett referensdokument B, ett extra lager av säkerhet till förfarandet.

Det är föredraget att varje publicerat tidstämplingssignalvärde P1-P8 innefattar ett utgångsvärde från en envägsfunktion enligt ovan, såsom ett hashvärde, innefattande åtminstone 256 bitar. Vidare är det föredrafet att det innefattar en datum- och tidsinformation som anger en tidpunkt efter vilken signalvärdet i fråga var publikt känt och/eller en datum- och tidsinformation som anger en tidpunkt före vilken signalvärdet i fråga inte var publikt känt. Det sistnämnda kan exempelvis vara tidpunkten för skapandet av ett motsvarande referensdokument. För sådana tidsmätningsaktiviteter används klockan 107 som referens.

Figur 2 visar även en annan aspekt av föreliggande uppfinning, nämligen att använda den vid upprepade tillfällen, eller kontinuerligt, uppdaterade tidsstämplingssignalen för att skapa en i tiden begränsad digital signatur av ett dokument A, B, D1-D9. I det exemplifierande fallet med dokument B tillhandahålls detta dokument av användaren 131 och inte

automatiskt av systemet 100, i syfte att skapa en digital signatur för dokumentet B. Det som beskrivs häri med hänvisning till att skapa en signatur för dokumentet B är emellertid också tillämpligt på dokument A såväl som på referensdokumenten D1-D9.

Enligt denna aspekt skapas sagde signatur så att den består av, innefattar eller beräknas baserat på utgångsvärdet för en viss signaturenvägsfunktion, som i figur 2 exemplifieras av envägsfunktionen $\#_2$ men som kan vara vilken envägsfunktion som helst enligt de häri beskriva definitionerna. Ett ingångsvärde till signaturenvägsfunktionen är åtminstone en del av en digitalt lagrad version av dokumentet B. I denna exemplifierande utföringsform är ingångsvärdet dokument B i sin helhet, även om någon väl definierad, förutbestämd del kan användas så länge som det i praktiken är omöjligt att beräkna motsvarande envägsfunktions utgångsvärde utan kännedom om innehållet i dokumentet B. Utgångsvärdet är t#8. Emellertid kan det nedströms värdet P8 också väljas att utgöra en signatur för dokument B.

Det är föredraget att varje signatur som skapas av eller tas emot av systemet 100 för ett dokument lagras i databasen 106 och associeras med det aktuella dokumentet, för framtida användning till exempel som en bevissignatur.

Vidare enligt denna utföringsform skapas ett tidsstämplingssignalvärde på det ovan beskrivna sättet, varvid det aktuella värdet för sagda signal, eller ett värde som har beräknats baserat på det aktuella värdet av sagda signal, också används, tillsammans med dokumentet B, som ett ingångsvärde till nämnda signaturenvägsfunktion. I detta exempel är tidsstämplingssignalvärdet T#7.

I det motsvarande exemplet i vilket dokument A används, är ingångsvärdet hela eller en del av ett dokument A i kombination med D123#, som i detta fall utgör tidsstämplingssignalvärdet, och utgångsvärdet kan vara T#1 eller P1.

Den skapade signaturen, eller ett värde som har beräknats baserat på signaturen, publiceras sedan offentligt, som P8 i det exemplifierande fallet med dokument B, över minst en, helst flera parallella, publiceringskanaler enligt ovan, vilket gör det möjligt för tredje part att senare verifiera publiceringen av signaturen. Detta åstadkommer ett sätt att kunna bevisa att dokumentet B, i den form det hade när det valdes av systemet 100, åtminstone existerade vid tidpunkten för publiceringen av P6, och att signaturen inte skapades före tidpunkten för valet av dokumenten D7 eller D8 av systemet 100. Ifall P6 inkorporeras i dokumentet B enligt ovan innan T#8 beräknas kan det dessutom senare bevisas att dokumentet B, i den form det hade när det valdes av systemet 100, med det inkorporerade P6, inte existerade före skapandet av P6. Användningen av detta utvecklas nedan.

Enligt en föredragen utföringsform beräknas respektive signaturer för ett flertal dokument A, B, D1-D9 vid olika tidpunkter, och lagras logiskt i en trädstruktur såsom beskrivits ovan, varvid ett distinkt utgångsvärde från trädenvägsfunktionen $\#_3$ för trädroten, eller ett distinkt värde som har beräknats baserat på detta utgångsvärde, publiceras offentligt för varje dokument i nämnda flertal dokument.

Analogt med vad som beskrivits ovan för framställningen av T#4 och T#5, som inte utgör en direkt följd av valet av ett visst externt referensdokument, publiceras enligt en föredragen utföringsform utgångsvärdet från trädenvägsfunktionen $\#_3$ för trädroten, eller ett värde som har beräknats baserat på detta utgångssvärde, offentligt också utan att vara en följd av att en signatur har skapats för ett dokument, och sådan publicering föregås av tillägg till trädstrukturen av ett värde som inte är den nyligen beräknade signaturen för ett dokument. Ett exempel på ett sådant värde är en internt genererad information såsom beskrivits ovan.

Det är speciellt föredraget att en sådant internt genererad information är ett av de tidigare beräknade utgångsvärdena från trädenvägsfunktion $\#_3$.

Det inses att en sådan återanvändning av trädenvägsfunktionens $\#_3$ utgångsvärden för att skapa intermediära publika publiceringar av värden mellan skapandet av signaturer för dokument liknar återanvändningen av tidigare använda tidsstämplingssignalvärden, enligt vad som beskrivits ovan och som används för att tillhandahålla uppdaterade tidsstämplingssignalvärden baserade endast på internt genererad information, och att dessa två metoder kan användas både för generering av tidsstämplingssignalen som sådan och för den nu beskrivna aspekten att skapa digitala signaturer för dokument.

Det är vidare föredraget att den digitala versionen av dokumentet A, B som används för beräkningen av sagda utgångsvärde för signaturenvägsfunktionen associeras med den skapade och/eller publicerade signaturen och lagras, företrädesvis i databasen 106, för framtida referens och användning när en tredje part begär en verifiering av den skapade signaturen.

Vissa digitalt lagrade dokument kan innehålla för lite information för att ge tillräcklig säkerhet för föreliggande syften, eftersom en brute force-attack kan vara framgångsrik när det gäller att gissa innehållet i ett sådant dokument och på det sättet beräkna den motsvarande envägsfunktionens utgångsvärde. Exempel är dokument som innehåller 10 byte eller mindre av signifikant information. Därför, och i synnerhet för sådana små dokument, är det föredraget att ett slumptal används även som ett ingångsvärde till signaturenvägsfunktionen, utöver själva dokumentet i sig. I detta fall är det också föredraget att nämnda slumptal är associerat med litet dokument och/eller signaturenvägsfunktionens utgångsvärde, och lagras i databasen 106 för framtida referens vid återberäkningen av utgångsvärdet från envägsfunktion ifråga. Företrädesvis är ett sådant slumptal en slumpmässig alfanumerisk sträng som innehåller åtminstone 16, företrädesvis åtminstone 256, slumpmässiga bytes.

Det är föredraget att systemet 100 är anordnat att kontinuerligt ge upphov till den ovan beskrivna tidsstämplingssignalen, och att åstadkomma den till tredje man väsentligen i realtid via de beskrivna publiceringarna av signalvärdet via gränssnittet 103. Det är också föredraget att systemet 100, via gränssnittet 104, digitalt accepterar lagrade dokument från tredje part, till exempel användaren 131, för vilka dokument en signatur skapas och publiceras såsom beskrivits ovan. Det är också föredraget att varje dokument som accepteras för att skapa signaturen även används som ingångsvärde till åtminstone en envägsfunktion vars utgångsvärde används för att beräkna nämnda tidsstämplingssignalvärdet. På så sätt blir alla dokument som tillhandahålls av en tredje part automatiskt en del av tidsstämplingssignalprocessen, så att dokumentet och utvecklingen av tidsstämplingssignalen över tiden griper in i varandra på ett ömsesidigt beroende sätt, vilket

gör det väsentligen omöjligt för utomstående att förfalska signaturer som framställts enligt föreliggande uppfinning, eftersom detta skulle kräva att hela den historiska tidsstämplingssignalprocessen rekonstrueras eller förfalskas.

Enligt ett förfarande för tidsstämpling av ett dokument i enlighet med föreliggande uppfinning, inbäddas eller inkorporeras en tidsstämplingssignal i enlighet med föreliggande uppfinning i ett dokument, till exempel dokumentets B i figur 2, som tidigare har tillhandahållits till systemet 100 av en tredje part eller som efter inbäddning eller inkorporering tillhandahålls till systemet 100, såsom av användaren 131. Inbäddning eller inkorporering sker på ett sådant sätt att det är möjligt att läsa av värdet för den inbäddade eller inkorporerade tidsstämplingssignalen från, eller på basis av, dokumentet. Sedan skapas en signatur för dokumentet B, med det inbäddade eller inkorporerade signalvärdet, så att denna signatur kan beräknas endast med kännedom om innehållet i dokument B med den inbäddade eller inkorporerade signalen. På detta sätt är det möjligt att, vid ett senare tillfälle, bevisa att dokument B med den inbäddade eller inkorporerade signalen inte existerade före tidpunkten för tidsstämplingen av den inbäddade eller inkorporerade tidsstämplingssignalen, och att dokument B åtminstone existerade när signaturen skapades.

Därför kan ett tidsintervall under vilket dokument B med den inbäddade eller inkorporerade signalen måste ha skapats fastställas, och bevisas på ett publikt sätt med hög säkerhet. Det är särskilt föredraget att tidsstämplingssignalen faktiskt bäddas in eller inkorporeras i dokumentet i omedelbar anslutning till skapandet eller en uppdatering av dokumentet ifråga. Det är speciellt föredraget att en sådan inbäddning sker med hjälp av en fristående teknisk dokumentskapande

utrustning som är anordnad att läsa en tidsstämplingssignal från systemet 100 direkt via gränssnittet 103 eller via publiceringar P1-P8, att bädda in eller inkorporera tidstämplingssignalvärdet som en integrerad del av den dokumentskapande processen, och att väsentligen omedelbart därefter tillhandahålla det skapade dokumentet till systemet 100, via gränssnittet 104, för att skapa en signatur och för att publicera den motsvarande tidsstämplingssignalen. Exempel på sådana förfaranden ges i det följande.

Som ett alternativ till att bädda in eller inkorporera det aktuella värdet för tidsstämplingssignalen vid tidpunkten för tidsstämplingen av dokumentet, kan det aktuella värdet associeras och lagras tillsammans med dokumentet på en central server, såsom i databasen 106, för framtida referens. Alternativt kan dokumentet vara tillgängligt från en extern källa, i vilket fall endast ett envägsfunktionsutgångsvärde från en envägsfunktion till vilken dokumentet utgjorde ingångsvärdet kan lagras i databasen 106.

Figurerna 4a, 4b och 4c visar tre olika sätt att bädda in tidsstämplingssignalen 402 i ett digitalt lagrat dokument 400, där den inbäddade tidstämplingssignalen är i form av en information från vilken signalens värde kan härledas. De tre exemplen tillämpas samtliga på ett dokument 400 som innefattar bilddata 401, men det inses att motsvarande tidsstämplingstekniker kan tillämpas på andra typer av dokument, såsom till exempel dokument som innefattar videomaterial, ren text, ljud, en webbsida och så vidare, eller kombinationer därav.

I figur 4a införs tidsstämplingssignalen 402 i form av ett grafiskt element, såsom en sträng av alfanumeriska tecken, en QR-kod eller en streckkod, in i en visuell representation av dokumentet, vilket grafiska element bär nämnda information.

Genom att visa dokumentbilden 400 och tolka det grafiska elementet, är därför värdet för tidsstämplingssignalen lätt tillgängligt.

I figur 4b innefattar dokumentet 400, förutom bilddata 401, även konceptuellt illustrerad metadatainformation 403, 404. Sagda information 402 läggs då till en digitalt lagrad version av dokumentet som ett metadatafält. Ett sådant metadatafält är naturligtvis endast synligt när det läses med hjälp av en algoritm för att läsa sådana metadata, vilken algoritm kan vara konventionell i sig.

I figur 4c är informationen 402 i form av en digitalt kodad vattenstämpel 402 som är inkorporerad i en digitalt lagrad version av dokumentet 400. I det exemplifierande fall som visas i figur 4c är bilddata 401 och tidsstämplingssignalvärdet 402 sammanfogade med hjälp av en i och för sig konventionell algoritm för digital vattenstämpling, så att det resulterande dokumentet 400 innefattar en bild som är väsentligen opåverkad när den betraktas på ett normalt sätt, men som visar det kodade tidstämplingssignalvärdet 402 när det underkastas en förutbestämd, i sig konventionell, avkodningsalgoritm för vattenmärken.

Det är föredraget att inkorporera ett aktuellt värde för en tidstämplingssignal, till exempel en tidsstämplingssignal enligt vad som beskrivits ovan, automatiskt vid framställningen av ett dokument. Företrädesvis sker detta vid samma tillfälle som, eller i omedelbar anslutning till, framställnigen av dokumentet. När det gäller ett dokument som endast finns tillgängligt i digital form när det väl har framställts, såsom exempelvis en digitalt lagrad bild som erhållits genom sampling av ljus infallande mot en digital bildsensor, är det föredraget att den nämnda inkorporeringen sker

som en del av samplingsprocessen, eller åtminstone som ett integrerat steg av bildframställningsprocessen före det att en slutgiltig, digitalt lagrad bild åstadkoms och kan användas.

Figurerna 5a, 5b och 5c visar användningen av en dokumentframställande hårdvarusamplingsutrustning 500, anordnad att sampla ett verkligt fysiskt fenomen, såsom att ta ett digitalt fotografi, och anordnad att åstadkomma ett digitalt lagrat samplat dokument 501 som återspeglar ett motsvarande tillstånd för den verkliga världen. Utrustningen 500 är speciellt anpassad för att utföra ett tidsstämplingsförfarande i enlighet med föreliggande uppfinning.

I figurerna 5a-5c exemplifieras det framställda dokumentet 501 med en bild, och utrustningen 500 är en optisk kamera. Det inses emellertid att även andra typer av dokument kan behandlas på motsvarande sätt, som beskrivits i närmare detalj ovan i anslutning till figurerna 4a-4c. Således kan kameran 500 i stället vara till exempel en digital ljudinspelningsutrustning eller en digital videokamera.

Ett verkligt objekt 510 avbildas med hjälp av kameran 500 i form av ett digitalt lagrat, konceptuellt illustrerat, dokument 501, och det är föredraget att dokumentet 501 väsentligen omedelbart överförs av kameran 500, till ett system 100 i enlighet med föreliggande uppfinning, via gränssnittet 104 till vilket kameran 500 är ansluten via en kommunikationskanal till vilken kameran 500 har givits tillgång, exempelvis via fast eller trådlöst internet.

Sedan använder systemet 100 företrädesvis dokumentet 501 som ingångsvariabel till en envägsfunktion så att senare framställda tidstämplingssignalvärden är beroende av existensen

av dokumentet 501. Närmare bestämt är det föredraget att en digital signatur av det tidsstämplade dokumentet 501 skapas såsom beskrivits ovan, och att den framställda signaturen associeras med dokumentet 501 och lagras i databasen 106.

Enligt en föredragen utföringsform bringas utrustningen 500 att beräkna ett envägsfunktionsutgångsvärde för dokumentet 501, i samband med att samplingen utförs, vilket samplade fysiska fenomen utgör dokumentet 501, och nämnda utgångsvärde kommuniceras sedan från utrustningen 500 till det centrala systemet 100 över nämnda kommunikationskanal.

Det är också möjligt, i andra utföringsformer, för utrustningen 500 att själv beräkna signaturen för dokumentet 501. I detta fall erhåller först utrustningen 500 det aktuella värdet för tidsstämplingssignalen, från gränssnittet 103, via en kommunikationskanal som tillhandahålls mellan systemet 100 och utrustningen 500, till exempel en kommunikationskanal via trådbundet eller trådlöst internet.

I synnerhet när dokumentet 501 innefattar åtminstone en stillbild eller en bildruta i en rörlig bild är det föredraget att det aktuella signalvärdet vid tidpunkten för samplingen av dokumentet 501 är inbäddad 502 i bilden eller bildrutan genom att positionera en grafikpresenterande anordning 520, anordnad att visa ett grafiskt element som bär nämnda information i form av exempelvis en alfanumerisk kod, en streckkod eller en QR-kod, i den bild eller bildruta som ses av kameran 500, så att det grafiska elementet fångas som en del av det samplade dokumentet. Detta åskådliggörs i figur 5a, i vilken den grafikpresenterande anordningen 520 har givits tillgång till nämnda kommunikationskanal till gränssnittet 103 av systemet 100, över vilken det aktuella tidstämplingssignalvärdet kommuniceras till anordningen 520

för visning. Anordningen 520 kan till exempel vara i form av en liten skärm.

Figurerna 5b och 5c, å andra sidan, illustrerar båda situationer i vilka kameran 500 i sig ges tillgång till en kommunikationskanal över vilken det aktuella värdet för tidsstämplingssignalen kommuniceras till kameran 500 från gränssnittet 103, och varvid kameran 500 i sig bäddar in det aktuella signalvärdet i dokumentet 501 i anslutning till att samplingen utförs.

I figur 5b finns det en grafikpresenterande anordning 530 som är en integrerad del av samma allmänna anordning som den bildfångande anordning 500. Exempelvis kan anordningen 530 vara i form av en liten skärm placerad på den främre sidan om kameran 500, som skärmen på en så kallad smartphone vars främre kamera används för att fånga dokumentbilden 501. Den grafikpresenterande anordningen 530 är anordnad att presentera det grafiska elementet samtidigt som kameran 500 fångar dokumentbilden 501. En spegel 531 används, så att anordningen 530 är synlig i vyn för den fångade dokumentbilden 501. Således avbildar dokumentet 501, via spegeln 531, en bild som täcker enheten 530.

Båda de förfaranden som illustreras i figurerna 5B och 5C är särskilt användbara när dokumentet 501 innefattar åtminstone en stillbild eller en bildruta i en rörlig bild. I det senare fallet är det föredraget att de efterföljande bildrutorna i den rörliga bildserien behandlas såsom beskrivs häri för en enda bildruta, på ett iterativt sätt.

I figur 5c bäddas det aktuella signalvärdet in vid tidpunkten för fångandet av bilden eller bildrutan i dokumentet 501 genom att signalen matas till kameran 500, från gränssnittet

103, och orsakar därmed att kameran 500 bäddar in nämnda information digitalt i dokumentbilden 501. Detta uppnås genom att ett digitalt bildbehandlingsorgan 540, som kan vara mjukvaruimplementerat men av säkerhetsskäl företrädesvis är i form av en dedikerad hårdvaruutrustning som är integrerad i kameran 500 och anordnad att ta emot och automatiskt visa sagda information i dokumentet 501 vid samplingen.

Det inses att de inbäddningstekniker som illustreras i figurerna 4a-4c kan användas tillsammans med de inbäddningstekniker som visas i figurerna 5a-5c i vilken kombination som helst, både för bilddokument och vilken annan typ av tillämpliga dokument som helst.

Genom att bädda in det aktuella värdet för tidsstämplingssignalen i dokumentet 501, kan dokumentet tidsstämplas på ett säkert sätt som i efterhand kan verifieras av tredje part. Om dokumentet 501 också väsentligen omedelbart sänds till systemet 100, så att det används för att beräkna framtida tidstämplingssignalvärden, kan det fångade dokumentet 501 tidsstämplas säkert inom ett mycket kort tidsintervall, inom vilket dokumentet måste har framställts.

Figur 5d visar schematiskt en tidslinje T och tillhörande händelser mellan en verklig händelse som involverar en boll 600 studsande på marken 601, vilket skildras med hjälp av en stillbildskamera eller en videokamera 500 som i sin tur är ansluten till ett system 100 enligt uppfinningen.

Kameran 500 är anordnad att sampla 610 det ljus som faller in från scenen med bollen 600 i riktning mot kameran 500, och att framställa 611 en serie av digitalt lagrade bilder 501, var och en skildrande den studsande bollen 600 vid olika tidpunkter. Denna serie av bilder 501 kan företrädesvis vara

i form av videomaterial, så att varje bild 501 utgör en respektive bildruta i en videofilm av den studsande bollen 600.

Företrädesvis tas det respektive aktuella värdet för tidstämplingssignalen emot 613 från systemet 100, via gränssnittet 103, och inkorporeras 502, såsom beskrivits ovan, i sekvensen av bilder 501 genom att enskilda bilder bringas att innefatta det respektive aktuella värdet för signalen vid tidpunkten för att bilden ifråga fångas, eller åtminstone det senast kända uppdaterade sådana värdet vid tidpunkten för att bilden 501 fångas.

Såsom illustreras i figur 5d behöver alla bilder 501 inte ha ett inbäddat signalvärde 502. I syfte att förbättra säkerheten är det emellertid föredraget att åtminstone en bildruta för varje sekund av en videoström innehåller ett sådant värde 502, och helst minst 10% av de enskilda bildrutorna 501 i en bildsekvens som fångats av kameran 500 i enlighet med vad som beskrivs häri.

Detta gör bildsekvensen svår att förfalska för en tredje part, eftersom utvecklingen för tidsstämplingssignalen kan spåras i efterhand i bildsekvensen 501.

För att ytterligare förbättra säkerheten är det föredraget att åtminstone en bild 501, företrädesvis åtminstone en bild för varje sekund av fångad videoström, och företrädesvis åtminstone 10% av de enskilda bildrutorna 501 i en bildsekvens som fångats av kameran 500 i enlighet med vad som beskrivs häri, kommuniceras till systemet 100, via gränssnittet 104, så att bilden kan användas som ett referensdokument för framställning av tidsstämplingssignalen såsom beskrivits ovan. På så sätt kommer den uppdaterade tidsstämplingssignalen att bäddas in i åtminstone en senare fångad bild som

kommer att innehålla en inbäddad tidsstämplingssignal som är beroende av en tidigare fångad bild i samma serie av bilder eller i samma videoström. Företrädesvis hade åtminstone en sådan tidigare fångad bild det vid den tiden aktuella värdet för tidsstämplingssignalen inbäddad på ett sådant sätt att det påverkar värdet hos tidsstämplingssignalen som beräknas baserat på den bilden. Detta gör att bildsekvensen eller videoströmmen utgör en integrerad del av utvecklingen av tidsstämplingssignalen, vilket i sin tur gör det möjligt att vid en senare tidpunkt, med mycket hög säkerhet, verifiera tidpunkten för fångandet av bildsekvensen eller videoströmmen genom att hänvisa till offentligt publicerad information såsom beskrivits ovan.

Istället för att använda till exempel en enda bildruta i ett videomaterial är det föredraget att som referensdokument använda en del av en ström, såsom en video-och/eller ljudström, som är tillräckligt lång för att en människa som tar del av nämnda del vid en senare tidpunkt kan få en god förståelse av innehållet i strömmen vid denna senare tidpunkt. Till exempel bör den valda delen vara minst 10 sekunder lång, företrädesvis åtminstone 1 minut lång, företrädesvis åtminstone 2 minuter lång. Den tidsstämpel som är associerad med referensdokumentet skulle i så fall vara den faktiska sluttiden för delen, och denna tidsinformation bör associeras med referensdokumentet och lagras i databasen 106. Det är föredraget att data från i stort sett hela tidsintervallet som täcks av den valda delen används som ingångsvärde till motsvarande envägsfunktion.

Vidare kommer referensdokument från samma strömreferenskälla i detta fall företrädesvis att framställas oftare än längden för varje del. Sedan är det föredraget att strömmen själv, med andra ord referenskälldata eller en konverterad eller

samplad form av densamma, lagras i sin helhet i databasen 106, tillsammans med information om hur vilka referensdokument extraheras från den lagrade strömmen. På så sätt finns det inget krav på att lagra varje vald del för varje referensdokument, inte heller i de fall då dessa delar överlappar varandra.

För att ytterligare öka säkerheten är det föredraget att ett antal på varandra följande bilder 501 innefattar bildmaterial som visar ett naturligt fenomen vars utveckling är förutsägbar för en betraktare. Detta illustreras i figur 5d, i form av den studsande bollen 600, och gör det svårare att förfalska bildserien genom exempelvis bildmanipulering. Ett sådant deterministiskt fenomen är användbart, men det är ännu mer föredraget att, i stället för den studsande bollen 600 som beskrivs häri, på motsvarande sätt använda ett fenomen vars allmänna utveckling är förutsägbar och tydligt tidsstyrd, men där detaljerna innefattar kaotiska inslag. Exempel på detta är utvecklingen av en brand och en väg med förbipasserande trafik.

Ett sådant förfarande är särskilt lämpligt för användning i ett videokonferenssystem eller ett videoövervakningssystem, som är anordnat för att fånga videosekvenser i enlighet med vad som har beskrivits ovan i anslutning till figur 5d, och eventuellt i kombination med vad som har beskrivits ovan i anslutning till figurerna 5a-5c.

Till exempel kan ett videokonferenssystem eller ett övervakningssystem innefatta en bildvisande anordning 520, placerad i den vy som ses av en videokamera och anordnad att visa ett aktuellt och företrädesvis kontinuerligt uppdaterat värde för den tidstämplingssignal som skall fångas som en del av det fångade videomaterialet, medan videofilmdata kontinuerligt

sänds till systemet 100, vilket skapar en återkopplingsslinga som i sin tur gör det enkelt att senare verifiera tidpunkten för inspelningen av videoströmmen. I ett annat exempel är ett naturfenomen, såsom en rörlig pendel, placerat i videokamerans vy.

Med andra ord bringas i dessa utföringsformer samplingsutrustningen 500 att sampla 611 det fysiska fenomenet upprepade gånger under en viss tidsperiod T, så att ett flertal referensdokument 501 framställs, åtminstone ett sådant dokument tidsstämplas såsom beskrivits ovan, åtminstone en del av en digitalt lagrad version av det nämnda tidsstämplade dokumentet används, av systemet 100, som ingångsvärde för beräkning av tidsstämplingssignalen såsom beskrivits ovan, och tidstämplingssignalvärdet, efter det att det har uppdaterats med användning av nämnda tidsstämplade referensdokument, bäddas in i ett senare framställt referensdokument som fångas av utrustningen 500.

Figur 6 illustrerar en webbserver 600, anordnad att förse en webbsida 601 till en begärande datoranordning 610, på kommando av en användare 611. Webbsidan 601 illustreras av tydlighetsskäl endast schematiskt i figur 6.

Webbsidan 601 innefattar ett inbäddat tidsstämplingssignalvärde 602, som kan vara inbäddat på något av de sätt som beskrivits ovan i anslutning till figurerna 4a-4c, men som företrädesvis är en komponent på webbsidan 601 som är synlig för en användare 611 som betraktar webbsidan på datoranordningens 610 skärm.

Således utgör webbsidan 601 det digitalt lagrade dokument som avses ovan.

Webbsidan 601 innefattar vidare programkod 603, som schematiskt illustreras i figur 6, vilken kod 603 är anordnad att initiera en tidsstämpling av dokumentet, det vill säga hemsidan 601 enligt vad som har beskrivits ovan. Således är programkoden 603 anordnad att från servern 100, via en kommunikationskanal såsom internet och via gränssnittet 103, ta emot ett uppdaterat tidsstämplingssignalvärde från servern 100, och att uppdatera det inbäddade värdet 602 i enlighet med denna uppdaterade signal som tagits emot från servern 100. Företrädesvis föregås denna mottagning av det uppdaterade tidsstämplingssignalvärdet av att programkoden 603 kommunicerar ett aktuellt tillstånd, såsom det visuella utseendet för webbsidan 601, till servern 100, via en motsvarande kommunikationskanal och via gränssnittet 104, så att det uppdaterade signalvärdet är baserat på nämnda kommunicerade tillstånd.

Det är föredraget att en sådan uppdateringsprocedur beträffande den inbäddade koden 602 initieras av programkoden 603 som en följd av att webbsidan 601 begärs av datorenheten 610, och därmed visas. På detta sätt garanteras att användaren alltid ser en inbäddad kod 602 som var den senaste som fanns tillgänglig vid tidpunkten för begäran av webbsidan 601. Det kan därmed även senare bevisas hur ofta och när en webbsida har begärts, genom att konsultera systemet 100 via gränssnittet 105.

Programkoden kan vara av konventionell typ, såsom till exempel Javascript (registrerat varumärke).

Figur 7a illustrerar strukturen, och figur 7b förfarandestegen, för ett förfarande i enlighet med föreliggande uppfinning för att tillhandahålla ett sätt att verifiera integriteten för ett dokument 701, vilket dokument kan men inte behöver vara digitalt lagrat, och kan exempelvis vara ett

dokument som är tryckt i en tidning eller ett tryckt dokument som finns på en reklamplats utomhus, eller som visas på en elektronisk skärm. Det är föredraget att dokumentet 701 är tryckt på ett permanent sätt, integrerat i dokumentet.

I detta förfarande är dokumentet för det första tidsstämplat enligt vad som har beskrivits ovan, i den meningen att systemet 100 beräknar ett uppdaterat tidsstämplingssignalvärde och associerar en digitalt lagrad version av dokumentet 701, såsom en digital sampling av dokumentet eller ett digitalt lagrat original i form av en huvudkopia av dokumentet 701, i databasen 106 med nämnda uppdaterade signalvärde.

I ett nästa steg publiceras dokumentet med en visuellt synlig inbäddad information 702, såsom beskrivits ovan i anslutning till figur 4a. Denna publicering utförs med hjälp av en publiceringsanordning 700, som exempelvis kan vara ett större eller mindre tryckeri, vilken anordning 700 är anordnad att ta emot den ovan nämnda uppdaterade tidsstämplingssignalen och att bädda in den i bilden 701 i form av informationen 702. Det är föredraget att informationen 702 publiceras som en integrerad och oskiljbar del av dokumentet 701. Det är vidare föredraget att informationen 702 är inbäddad i form av en QR-kod eller streckkod, eftersom sådana är lätta att känna igen med bildtolkningsmjukvara i systemet 100.

Sedan tillhandahålls en kommunikationskanal, över vilken en användare i form av en tredje part 710 kan sända, via gränssnittet 105 till systemet 100, en avbildning av det publicerade dokumentet 701. Användaren 710 kan typiskt sett använda sin vanliga internetanslutna kamera 711 eller smartphone för att ta ett fotografi av bilden 701, inklusive informationen 702, och skicka den digitalt lagrade bilden, via gränssnittet 105, till systemet 100 för analys.

Systemet 100 tar i sin tur emot återgivningen av det publicerade dokumentet och härleder värdet för tidsstämpelsignalen från den i återgivningen synliga informationen 702. Detta görs på ett sätt som är konventionellt i sig, och kan innefatta bildtolkningslogik, och specifikt innefatta tolkningen av en QR-kod som en alfanumerisk kod som utgör eller är associerad med signalvärdet i fråga.

Baserat på det nämnda tidsstämplingssignalvärdet som representeras av informationen 702, och baserat på dess associering med den digitalt lagrade versionen av dokumentet 701 i databasen 106, hittar systemet 100 sedan sagda digitalt lagrad version, om det finns en sådan digitalt lagrad version som är associerad med nämnda tidsstämplingssignalvärde i databasen 106.

Om ett sådant dokument hittas, kommuniceras den digitalt lagrade versionen av själva dokumentet, eller information hänförlig till dokumentet, till den tredje parten 710, via gränssnittet 105 från systemet 100, och till exempel till en internetansluten datorutrustning 712 tillhörig användaren 710. Sådan information som är relaterad till dokumentet kan exempelvis vara förutbestämd ytterligare information, till exempel metadata som i förväg har associerats med dokumentet i databasen 106.

Det är föredraget att sådan metadata är en information med hjälp av vilken användaren 710 kan identifiera bilden, och på så sätt verifiera äktheten hos bilden 701. Till exempel kan själva dokumentet sändas, i vilket fall det är lätt för användaren 710 att verifiera bilden genom att helt enkelt jämföra bilden 701 med det av datorutrustningen 712 mottagna dokumentet.

Ett sådant förfarande åstadkommer ett sätt för användaren 710 att, med enbart standardutrustning såsom exempelvis en vanlig smartphone, snabbt och säkert kunna verifiera äktheten hos en bild, oavsett var eller i vilket format den presenteras.

I en föredragen utföringsform analyserar den bildfångande utrustningen 711 kontinuerligt bildmaterial som fångas av utrustningen 711, och bevakar bildmaterialet beträffande visuella informationer 702 som är synliga för utrustningen 711. När sådan information 702 har upptäckts av utrustningen 711 sänds informationen till systemet 100 för verifiering, såsom beskrivits ovan, och om det tidsstämplingssignalvärde som representeras av den detekterade informationen 702 befinns motsvara ett dokument som tidigare tidsstämplats av systemet 100, tas uppgifter beträffande det tidsstämplade dokumentet emot av utrustningen 711 från systemet 100, varefter utrustningen 711 visar en bild med en grafisk överlagring i anslutning till den detekterade informationen 702, syftande till att ge information till användaren 710 beträffande att den detekterade informationen 702 är associerad med ett tidsstämplat dokument. Till exempel kan en mindre version av själva bilden visas ovanpå eller i anslutning till informationen 702 när denna är synlig för utrustningen 711.

Figur 8a visar strukturen, och figur 8b förfarandestegen, för ett förfarande enligt föreliggande uppfinning för att tillhandahålla ett sätt att verifiera integriteten för ett digitalt lagrat dokument 801 som publicerats på internet och som betraktas med hjälp av en webbläsare 802, exempelvis som en del av en webbsida 803.

Ett sådan förfarande innefattar steget att, för det första, tidsstämpla dokumentet 801 i enlighet med vad som har beskri-

vits ovan och i analogi med den initiala tidsstämplingen av dokumentet 801 som beskrivits ovan i anslutning till figur 7A. Dokumentet 801 kan exempelvis vara en bild, en videosekvens eller andra typer av grafiskt material vars äkthet kan vara önskvärt för en tredjepartsanvändare 810 som betraktar webbsidan 803 att verifiera.

I ett nästa steg publiceras dokumentet 801 på internet, med en associerad programkod anordnad att reagera på något slags aktivering av användaren 810. Programkoden är företrädesvis en del av webbsidan 802, och kan vara integrerad i dokumentet 801 självt. Sådan aktivering kan exempelvis vara i form av aktivering av ett aktiveringsorgan, såsom att dokumentet 810 väljs eller klickas på i webbläsaren 803, eller en aktivering av en användarkontroll 804, såsom ett grafiskt representerat, klickbart fält, såsom exempelvis i samma webbsida 802 som dokumentet 801.

Vid en detektering av en sådan aktivering sänds dokumentet 801 till systemet 100, via gränssnittet 105. Vid mottagandet av dokumentet 801 av systemet 100, bringas systemet 100 att slå upp, i databasen 106, ifall dokumentet 100 har tidsstämplats, genom att beräkna den motsvarande digitala signaturen och kontrollera ifall ett dokument med samma digitala signatur tidigare har tidsstämplats. Denna kontroll baseras lämpligen på tidigare beräknade hashvärden snarare än på de tidigare lagrade underliggande dokumenten själva. Alternativt beräknas ett utgångsvärde från en envägsfunktion, med dokumentet 801 som ingångsvärde, och sagda utgångsvärde kommuniceras till systemet 100, via gränssnittet 105. Sedan kontrollerar systemet 100 ifall ett dokument med samma signatur som det tillhandahållna värdet har tidsstämplats. I detta senare fall behöver systemet 100 inte lagra dokumentet 801 i sig,

utan endast den digitalt lagrade signaturen av dokumentet 801.

Om ett sådant dokument hittas, är systemet 100 anordnat att kommunicera, till tredjepartsanvändaren 810, någon form av information 805 som är hänförlig till dokumentet 801 och som gör att användaren 810 kan verifiera att dokumentet 801 är äkta i den meningen att det går att verifiera att dokumentet 801 tidigare har tidsstämplats av systemet 100.

Det är föredraget att nämnda relevanta information presenteras i webbläsaren 803, eventuellt i samma webbsida 802, i så fall företrädesvis i form av en inbäddad del i dokumentet 801. I vissa utföringsformer är den relevanta informationen 805 en symbol, exempelvis ett kontrollmärke eller motsvarande, vilken helt enkelt signalerar att en matchning har funnits i databasen 106. I andra utföringsformer är den relevanta informationen 805 i form av ett grafiskt element som liknar elementet 402 beskrivet ovan i anslutning till figur 4a, så att användaren kan identifiera, direkt eller indirekt, ett tidsstämplingssignalvärde som är associerat med dokumentet 801, som sedan kan användas för att direkt verifiera det tidsstämplade dokumentets äkthet 801 via gränssnittet 105. Det är också föredraget att den relevanta informationen innefattar en tidpunkt och ett datum för tidsstämplingen av dokumentet 801 av systemet 100.

Det är föredraget att gränssnittet 103 är anordnat att tillhandahålla nämnda relevanta information i form av dokumentet 801 självt, med den nämnda relevanta information visuellt inbäddad i dokumentet 801, och att webbläsaren 803 är anordnad att ersätta dokumentet 801 med det som tillhandahålls via gränssnittet 103 vid sagda aktivering av användaren 810 och uppslagningen i databasen 106.

I det speciella fall i vilket dokumentet 801 är en stillbild eller rörliga bilder, är det dessutom föredraget att, vid en första aktivering av användaren 810, sagda relevanta information publiceras i anslutning till bilden, såsom exempelvis att ett uppdaterat dokument 801 med inbäddad relevant information 805 kommuniceras, såsom beskrivits ovan, men utan att webbläsaren 803 lämnar den för tillfället visade webbsidan 802.

Vid en andra aktivering av användaren 810 är det i detta exempel dock föredraget att webbläsaren 803 omdirigeras, helst på initiativ av nämnda programkod på webbsidan 802, till en annan sida, där dokumentet 801 tillsammans med den relevanta informationen 805 presenteras för användaren 810 i webbläsaren 803. I detta fall är det föredraget att webbsidan omdirigeras till en betrodd webbsida, som drivs av operatören av systemet 100, där mer detaljerad information om dokumentet 801 och dess tidsstämpling kan presenteras för användaren 810.

I alla de ovan beskrivna exemplen i anslutning till figurerna 8a och 8b är det föredraget att den nämnda relevanta informationen 805 innefattar tidpunkten för tidsstämplingen av dokumentet 801, enligt vad som lagrats i databasen 106.

Enligt en annan, relaterad, utföringsform förses ett dokument som ännu inte tidsstämplats av systemet 100 med en programkod som tillhandahåller ett aktiveringsorgan som i sin tur tillåter en betraktande användare att aktivera en funktion som resulterar i att dokumentet ifråga sänds, via gränssnittet 104, till systemet 100 för tidsstämpling. Företrädesvis sänds också metadata som är specifika för den webbsida i vilken dokumentet ifråga visas, företrädesvis även tillsammans med

metadata som är specifika för den aktiverande användaren, till systemet 100 för tidsstämpling associerad med dokumentet. Enligt en föredragen utföringsform ändrar programkoden därefter aktiveringsorganet till att vara av den typ som diskuterats ovan, som tillåter en användare som betraktar webbsidan att verifiera tidsstämplingen av dokumentet.

Enligt en föredragen utföringsform tillhandahålls en webbsida i vilken alla dokument på webbsidan som redan har tidsstämplats är försedda med respektive aktiveringsorgan, så att användaren kan verifiera en tidigare utförd tidsstämpling, medan de återstående dokument som finns i webbsidan ifråga som kan tidsstämplas av systemet 100 är försedda med respektive aktiveringsorgan så att användaren kan utföra en tidsstämpling av det respektive dokumentet i fråga.

Figur 8c visar en utföringsform av föreliggande uppfinning, i vilken användaren 810 använder en datoranordning 811 för att visa en viss webbsida som tillhandahålls av en server 820. 821 är en förenklad illustration av hur webbsidan ser ut när den visas i en webläsare på datorn 811, och efter att ha direkt kommunicerats från servern 820 till datorn 811, till exempel via internet.

Användaren 810 kan emellertid välja att visa webbsidan som tillhandahålls av servern 820 genom en filterserver 830, varvid den visade webbsidan ser ut som den förenklade illustrationen 831. I 831 visas webbsidan på ett sätt som motsvarar sättet i 821, men med tillagt eller modifierat innehåll. I 831 exemplifieras detta innehåll av bockar på dokument som har bekräftats ha blivit tidsstämplade tidigare av systemet 100.

För att producera webbsidevyn 831 hämtar filterservern 830, på begäran av användaren 810, webbsidan ifråga från servern 820, och undersöker dess innehåll. Företrädesvis undersöks både webbsidan som helhet och dess olika beståndsdelar individuellt, och vardera sänds till systemet 100 för verifiering av eventuella tidsstämplar som gjorts för respektive sända delar. Förfarandet för att utföra sådan verifiering har förklarats ovan. Därefter lagras varje positiv verifiering av servern 830, som sedan lägger till element eller modifierar dokument som har verifierats att tidigare ha tidsstämplats av systemet 100, och sänder den modifierade webbsidan till användarens 810 dator 811 för visning som 831. I figur 8c har alla tre dokumenten på webbsidan, samt webbsidan själv, verifierats ha blivit tidsstämplade.

Det är föredraget att det sagda tillförda eller modifierade innehållet utgör respektive aktiveringsorgan enligt ovan, genom aktivering av vilka användaren 810 kan verifiera att tidsstämpeln verkligen är äkta enligt det ovan beskrivna.

Således är filterservern 830 anordnad att läsa websidedata från webbservern 820, att undersöka ifall de mottagna webbsidedata innehåller några dokument av en typ som kan tidsstämplas av systemet 100, att sända en förfrågan till systemet 100 med en begäran om verifiering, för vart och ett av de eventuellt funna dokumenten, beträffande huruvida de olika dokumenten tidigare har tidsstämplats av systemet 100, och att sedan åstadkomma uppdaterade websidedata med inbyggda verifieringssignaleringselement för dokument som har verifierats att ha blivit tidsstämplade, till datorn 811 som kontrolleras av användaren 810. Det är föredraget att signaleringsorganen är i form av visuella element som visas i anslutning till varje verifierat dokument i den modifierade webbsidan.

Det är vidare föredraget att filterservern 830 är anordnad att, som en följd av att användaren 810 begär webbsidedata via filterservern 830, sända till systemet 100, via gränssnittet 104, varje dokument som återfinns på webbsidan, och företrädesvis även webbsidan själv i förekommande fall, som kan tidsstämplas av systemet 100 och som ännu inte blivit tidsstämplade av systemet 100, för tidsstämpling i enlighet med det ovan beskrivna. Alternativt kan envägsfunktionsutgångsvärden för sådana dokument sändas till systemet 100, med användning av en förutbestämd envägsfunktion som är känd av systemet 100.

Genom att tillämpa de ovan beskrivna teknikerna, särskilt skapandet av en digital signatur av en digitalt lagrad version av ett dokument, är det möjligt att uppnå ett sätt att kunna verifiera integriteten för ett digitalt lagrat dokument i den meningen att det är möjligt att fastställa att det aktuella dokumentet är identiskt med ett dokument för vilket en digital signatur skapades vid en historisk tidpunkt, vilken tidpunkt kan anges med hög säkerhet såsom beskrivits ovan.

I ett sådant förfarande i enlighet med föreliggande uppfinning, som illustreras i figur 9a, skapas en digital bevissignatur först för det digitalt lagrade originaldokumentet, där integriteten för en digital kopia av sagda dokument senare kommer att ifrågasättas. Skapandet av den digitala signaturen utförs såsom beskrivits ovan, och signaturen associeras med dokumentet och lagras i databasen 106. Sedan, vid en senare andra tidpunkt, ifrågasätts integriteten hos ett digitalt lagrat dokument som påstås vara en identisk, icke-manipulerad version av samma dokument som det för vilket bevissignaturen beräknades. Systemet 100 tar då emot, från en ifrågasättande

tredje part eller ett tredjepartssystem och via gränssnittet 105, en digitalt lagrad kopia av det ifrågasatta dokumentet, för vilket en motsvarande digital verifieringssignatur skapas för det mottagna dokumentet. Denna verifieringssignatur beräknas på samma sätt som bevissignaturen, och med användning av samma historiska värde för tidsstämplingssignalen som användes för att skapa den digitala bevissignaturen. Således söks lagrade historiska uppgifter om tidsstämplingssignal ut i databasen 106, och används vid skapandet av verifieringssignaturen. Slutligen verifieras integriteten hos det mottagna dokumentet positivt endast om den digitala bevissignaturen är identisk med den digitala verifieringssignaturen. Om sådan verifiering är möjlig kommer det också att vara möjligt att, på ett bevisbart sätt såsom beskrivs ovan, ange en tidpunkt då det ursprungliga dokumentet existerade i samma form som det ifrågasatta dokumentet.

Med hjälp av föreliggande förfarande är det också möjligt att verifiera integriteten för, och tidpunkten för tidsstämpling av, en eller flera delar av digitalt lagrade metadata som är relevanta för ett visst digitalt lagrat dokument. Till exempel kan en bild av en olycksplats som ska användas för försäkringsändamål innefatta metadata om fotograferingstid och -datum; geografisk plats; en textbeskrivning; information om de parter som var inblandade i olyckan; och referensnummer för relaterade försäkringar. Var och en av dessa metadata kan ifrågasättas vid en senare tidpunkt, och behöver verifieras.

I allmänhet liknar ett förfarande i enlighet med föreliggande uppfinning för att verifiera integriteten hos en viss metadatainformation som är hänförlig till ett digitalt lagrat dokument det förfarande som beskrivits ovan i anslutning till figur 9a, och innefattar stegen att, vid en första tidpunkt, skapa en digital bevissignatur av dokumentet, såsom beskrivs

ovan i samband med figur 9a, men där signaturenvägsfunktionen beräknas utifrån både åtminstone en del av en digitalt lagrad version av dokumentet i sig samt utifrån nämnda metadatainformation. Den skapade digitala bevissignaturen lagras i databasen 106. Sedan, vid en senare andra tidpunkt, verifieras integritet för metadata ifråga genom att ta emot metadatainformationen från en begärande användare eller ett begärande system, att skapa en motsvarande digital verifieringssignatur av dokumentet, såsom beskrivits ovan i anslutning till figur 9a och med användning av samma värde för signalen som användes för att skapa den digitala bevissignaturen. Slutligen verifieras integriteten för metadatainformationen endast ifall den digitala bevissignaturen är identisk med den digitala verifieringssignaturen som är associerad med dokumentet.

Figur 9b illustrerar ett specialfall av detta allmänna förfarande för att verifiera integriteten hos en viss del metadata, som ger den ytterligare fördelen att integriteten för en eller flera delar av metadatainformation kan verifieras utan att information måste tillhandahållas från eller till en ifrågasättande part eller tredje man beträffande andra metadata, vilket kan vara känsligt. Till exempel i försäkringsexemplet ovan, kanske fotograferingstidpunkten måste verifieras utan att behöva utbyta information om den geografiska platsen för olyckan.

I detta fall finns således flera delar av metadata #1, #2 och #3, vilka är associerade med det digitalt lagrade dokumentet, och för var och en av vilka, vid en första tidpunkt, en separat digitalt lagrad metadatasignatur skapas såsom beskrivits ovan, till exempel i anslutning till figur 2. För detta ändamål behandlas metadatadelen som ett dokument, och metadatasignaturen beräknas sedan på samma sätt som en signatur

skulle ha beräknats för ett dokument, och lagras i databasen 106. För delar av metadata som endast innefattar begränsade mängder information är det föredraget att ett slumptal också används som ingångsvärde till signaturfunktionen, för att beräkna respektive metadatasignatur, enligt det som beskrivs ovan.

Därefter skapas den digitalt lagrade bevissignaturen för det ursprungliga dokumentet, så att den använda signaturenvägsfunktionen även beräknas utifrån varje digital metadatasignatur. Det är föredraget att de respektive metadatasignaturerna och bevissignaturerna arrangeras i form av en trädstruktur, såsom ett hashträd liknande det som beskrivits ovan i anslutning till figur 2, i vilken bevissignaturen ligger i trädets rot och så att varje blad utgör en respektive metadatasignatur. Bevissignaturen för det ursprungliga dokumentet lagras i databasen 106.

Vid en senare, andra tidpunkt, tillhandahåller en ifrågasättande tredjepartsanvändare eller ett tredjepartssystem en delmängd av de flera delarna metadata, till exempel metadata #1 och #2, men inte #3, vilka tas emot av systemet 100 via gränssnittet 105. Den ifrågasättande parten kan också tillhandahålla en digitalt lagrad kopia av originaldokumentet, om själva dokumentet också ifrågasätts. Därefter skapas först motsvarande digitala verifieringssignaturer för de mottagna delarna metadata, och sedan för det ursprungliga dokumentet, eller för den medföljande digitala kopian, på samma sätt på vilket bevissignaturen för det ursprungliga dokumentet skapades och med användning av samma värde för signalen som användes för att skapa de digitala metadatasignaturerna och den digitala bevissignaturen. De lagrade digitala metadatasignaturerna används emellertid endast för delar av metadata som inte mottagits vid den andra tidpunkten. Tillhandahållna

delar metadata ersätter motsvarande lagrad metadatainformation.

Slutligen verifieras integriteten för den tillhandahållna delmängden av metadatadelar, via gränssnittet 105, endast ifall den digitala bevissignaturen är identisk med den digitala verifieringssignaturen som är associerad med dokumentet.

Figur 10 illustrerar ett förfarande för att tillhandahålla ett sätt att verifiera att ett visst dokument 1001 publiceras på distans i realtid eller nära realtid så att en användare 1010 kan se dokumentet ifråga. I figuren publiceras dokumentet 1001 som en del av en webbsida 1002 i en webbläsare 1003, men det inses att dokumentet 1001 kan publiceras på andra sätt, såsom exempelvis på en TV-skärm eller liknande. Ett sådant dokument 1001 innefattar uppgifter vars natur uppdateras till att återspegla utvecklingen för ett verkligt skeende som samplas och kontinuerligt publiceras i form av dokumentet 1001.

I ett sådant förfarande tidsstämplas dokumentet 1001 kontinuerligt enligt ovan, genom att sändas till systemet 100, via gränssnittet 104, och genom att systemet 100 kontinuerligt skapar och publicerar, via gränssnitt 103, en uppdaterad signatur för det för tillfället mottagna dokumentet 1001. Företrädesvis används signaturen som en ingångsvariabel till en envägsfunktion som används för beräkning av ett uppdaterat värde för tidsstämplingssignalen i enlighet med uppfinningen.

Med "kontinuerligt" avses i detta sammanhang att en ny signatur beräknas antingen regelbundet med en kort period, såsom åtminstone en gång per minut eller åtminstone en gång var tionde sekund och/eller så snart innehållet i dokumentet 1001

ändrats och/eller så snart som tidsstämplingssignalen uppdaterats av systemet 100.

Sedan ges tredjepartsanvändaren 1010 tillgång till ett organ anordnat att jämföra en kontinuerligt uppdaterad information 1005 som är inbäddad i dokumentet 1001 med ett motsvarande nuvarande tidsstämplingssignalvärde som är lagrat i den centrala servern 100.

En sådan jämförelse kan göras direkt eller indirekt. Till exempel kan en förnärvarande uppdaterad tidstämplingssignal, beräknad baserat på åtminstone den uppdaterade signaturen för dokumentet 1001, eller på signaturen själv, vara inbäddad som ett grafiskt objekt 1005 i dokumentet 1001 självt, såsom beskrivits ovan i anslutning till figur 4a, och ett motsvarande värde kan sändas via en oberoende kommunikationskanal, till samma eller en annan skärm som kan visas för användaren, så att de två objekten kan jämföras direkt och visuellt av användaren 1010. Alternativt kan webbsidan 1002 innefatta en programkod som är associerad med dokumentet och anordnad att ta emot båda de nämnda signalerna och att automatiskt utföra en jämförelse mellan dem och signalera resultatet av jämförelsen till användaren 1010.

I det fall signalerna matchar, till exempel, kan programkoden vara anordnad att publicera en markör, såsom en bock 1006, för visuell verifiering från användarens 1010 sida. Vidare kan den nämnda programkoden vara anordnad att extrahera värdet för delen 1005 och att begära, via gränssnittet 105, att systemet ska verifiera att det extraherade värdet verkligen är ett korrekt och nyligen uppdaterat värde, och om svaret via gränssnittet 105 från systemet 100 är jakande, att visa bocken 1006. Det är föredraget att "nyligen uppdaterat" bety-

der att systemet 100 kan garantera en tidsavvikelse av högst 10 sekunder.

Ett specifikt sätt för användaren 1010 att uttryckligen verifiera att dokumentet 1001 verkligen är en realtids- eller nära realtidsrepresentation av nämnda händelseförlopp kan också tillhandahållas, tillgängligt genom att till exempel initiera någon av de beskrivna verifieringsprocesserna genom att aktivera en kontroll, till exempel genom att trycka på en knapp 1004 på webbsidan 1002.

Specifikt kan programkoden vara anordnad att, vid en första aktivering av en kontroll 1004 eller en klickning på dokumentet 1001, utföra en verifiering enligt ovan, samt att visa en visuell resultatsignal 1006, och, vid en andra sådan aktivering eller klickning, omdirigera webbläsaren 1003 till en annan webbsida, vilken helst drivs av systemets 100 operatör och helst presenterar mer detaljerad information för användaren 1010 om till exempel det aktuella tillståndet för dokumentet 1001 och/eller ett bevis beträffande tidpunkten för tidsstämpling av ett nyligen existerande tillstånd för dokumentet 1001.

Figur 11 visar ett system som konfigurerats för att utföra ett förfarande för att verifiera integriteten för data i en databas 1100. Databasen 1100 kan vara vilken typ av databas som helst som innefattar någon typ av digitalt lagrade data; som innefattar en kontinuerligt uppdaterad dataström; eller liknande. I ett sådant förfarande skapas åtminstone en digital bevissignatur av samtliga, eller en delmängd, av nämnda data, på ett sätt som liknar det som beskrivits ovan, genom att kommunicera nämnda data till systemet 100, via gränssnittet 104, och med hjälp av systemet i 100, vid mottagning av sådana uppgifter, beräkna en signatur baserad på ett uppdate-

rat värde för tidsstämplingssignalen, och företrädesvis låta den skapade signaturen vara indata till en envägsfunktion vars resultat är eller används för att beräkna ett senare tidstämplingssignalvärde. Den skapade signaturen lagras i databasen 106.

Därefter utvärderas integriteten för dessa data i databasen 1100 upprepade gånger, till exempel regelbundet, varje dag eller oftare, eller så snart tillträde tillhandahålls till uppgifterna i databasen 1100, genom att jämföra nämnda lagrade digitala bevissignatur med en motsvarande men senare skapad digital verifieringssignatur som baseras på det aktuella värdet för de data som ska verifieras och på samma tidsstämplingssignalvärde som användes för att skapa den digitala bevissignaturen. Ifall en eventuell avvikelse mellan den digitala verifieringssignaturen och den digitala bevissignaturen hittas, sänds en rapport.

Det är föredraget att en fristående modul 1110, såsom en mjukvaruprodukt som exekveras på samma dator som databasen 1100 eller en annan dator, sätts i kommunikation med databasen 1100 och systemet 100 via gränssnitten 104 och 105. Därefter läser modulen 1110 data från databasen 1100, sänder de data som ska signeras till gränssnittet 104, och begär en verifiering av den tidigare skapade signaturen via gränssnittet 105. Alla dessa åtgärder beskrivs närmare i detalj ovan. Dessutom sänder modulen rapporten till en dator 1120 som kontrolleras av en användare 1121, beträffande ifall en avvikelse påträffas, vilket då tyder på att data har förändrats.

I en föredragen utföringsform uppdateras värdet för den lagrade digitala bevissignaturen upprepade gånger, genom att en ny digital bevissignatur skapas enligt ovan. Företrädesvis utlöses uppdateringen av värdet för den lagrade digitala

bevissignaturen av tillträdeshändelser till databasen 1100, så att en ny digital signatur skapas som en följd av varje databasmodifiering, såsom infogningar, uppdateringar eller borttagningar, utförda av vilken part som helst. Detta kan i praktiken implementeras med hjälp av så kallade SQL (eng. Structured Query Language) query triggers eller liknande. Företrädesvis utförs en ny jämförelse före varje uppdatering av signalen.

Ett sådant förfarande åstadkommer ett snabbt förfarande med liten prestandapåverkan för kontinuerlig övervakning av en databas och för avgivandet av varningar ifall vissa data, till exempel data som är tänkt att vara oföränderliga, ändras till följd av olyckshändelser eller missbruk, och där förekomsten av och tidpunkten för sådana ändringar kan bevisas och spåras exakt och med hög tillförlitlighet och pålitlighet.

Ovan har ett antal utföringsformer beskrivits. Det inses dock att många förändringar kan göras av de beskrivna utföringsformerna, utan att avvika från uppfinningens grundläggande idé.

Till exempel kan tidsstämplingssignalen användas i andra tillämpningar, till exempel endast publiceras på ett ständigt uppdaterat sätt på en webbsida för allmän referens.

Ett gemensamt syfte med samtliga former av tidsstämpling som beskrivs häri är att i efterhand kunna avgöra vilket dokument eller vilka data som var eller inte var tillgängliga vid en viss historisk tidpunkt. Därför hänför sig den tidsstämpling som nämns häri primärt till tidpunkten för skapandet av dokument, till skillnad från när de förstördes.

För att mer fullständigt förstå de möjliga kombinationerna av de olika aspekterna av föreliggande uppfinning enligt beskrivningen ovan, kan följande ytterligare definitioner införas:

- En **positiv tidsstämpel** är en tidsstämpel som kan användas för att bevisa att ett dokument fanns vid en viss angiven tidpunkt, det vill säga att dokumentet redan hade skapats vid den angivna tidpunkten. Ifall en dokumentsignatur skapas i enlighet med föreliggande uppfinning, och ifall signaturen associeras med dokumentet och publiceras offentligt i enlighet med föreliggande uppfinning, utgör tidsstämplingen ifråga en positiv tidsstämpel.
- En **negativ tidsstämpel** är en tidsstämpel som kan användas för att bevisa att ett dokument inte kunde ha funnits, alltså inte kunde ha skapats, före en viss angiven tidpunkt. Ifall utgångsvärdet för en envägsfunktion, till vilken ett referensdokument matats in som ingångsvärde, införs i ett dokument, och en signatur för det resulterande dokumentet med nämnda envägsfunktionsutgångsvärde skapas och associeras med dokumentet, utgör detta en negativ tidsstämpel för dokumentet. Då kan dokumentet med tidsstämplingssignalen inte ha existerat före beräkningen av tidsstämplingssignalvärdet ifråga. Detta har beskrivits ovan i samband med figur 2.
- En **inramad tidsstämpel** är en kombination av en positiv och en negativ tidsstämpel för samma dokument, som innebär att en tidsram definieras, vilken tidsram anger en första möjliga tidpunkt då ett dokument skulle kunna ha skapats, med hjälp av en negativ tidsstämpel, och en senaste möjliga tidpunkt när dokumentet säkerligen hade skapats, med hjälp av en positiv tidsstämpel. Ett exempel är om den nämnda skapade signaturen för ett negativt tidsstämplad dokument publiceras offentligt i enlighet med föreliggande uppfinning.

- En **absolut tidsstämpel** är en inramad tidsstämpel där både en positiv och en efterföljande negativ tidsstämpel avser samma referenskälla. Med andra ord återmatas signaturen så att den blir en del av samma referenskälla som användes för att skapa signaturen. När tidsfönstret för manipulering minskar mot sekunder eller mindre, blir det mycket svårt att förfalska tidsstämplarna.
- En **integrerad tidsstämpel** kan tillämpas på dokument som har en inneboende tidsdimension, det vill säga sträcker sig över en viss tidsperiod, till exempel video eller audio som fångas mellan en starttid och en sluttid. En integrerad tidsstämpel tillämpas vid själva tidpunkten för skapandet av dokumentet, och innefattar en upprepade gånger tillämpad inramad eller absolut tidsstämpel. Således tidsstämplas dokumentet först negativt. Därefter tidsstämplas dokument positivt, och den resulterande signaturen matas tillbaka till en referenskälla så att det påverkar en senare negativ tidsstämpel som tillämpas på dokumentet vid en senare tidpunkt under tillkomsten av dokumentet. Detta kan pågå över flera eller ett stort antal iterationer. Allt eftersom slingan itereras blir det allt svårare att skapa en falsk tidsstämpel för dokumentet.

Tidsstämplingssignalen enligt uppfinningen utgör grunden för bekväm, precis och storskalig digital negativ tidsstämpling av dokument, där dokumenten tidsstämplas med tidsstämplingssignalvärden som ingångsvärden.

För att på ett effektivt sätt få kunskap beträffande tidpunkten för skapandet av ett digitalt dokument, är det en fördel om tidsstämplingsprocessen spelar en roll vid själva skapandet av dokumentet. Om dokumentet skapas på ett sådant sätt så att det framtida värdet av tidsstämplingssignalen beror på processen för att skapa dokumentet, kommer säker tidsstämpel-

verifiering att vara möjlig trots de inneboende egenskaperna hos den digitala domänen, såsom absolut stabilitet och omfattande reversibilitet.

En särskild klass av dokument som kan tidsstämplas med hjälp av föreliggande uppfinning innefattar digitala bilder, speciellt digitala fotografier. Dessa har några signifikanta egenskaper, enligt följande. Kodning och komprimering gör det icke-trivialt att förändra enskilda databitar, eller att lägga till information, utan att förstöra dokumentets giltighet. Visuell analys kommer att avslöja icke-realistiska bildmanipulationer. Ju högre bildupplösning, desto svårare blir det att manipulera dokumentet på ett trovärdigt sätt. Visuella element i bilden som bär informationen kan åtföljas av digitalt lagrad metainformation i samma dokument, eller i samband med dokumentet i någon form av digitalt konvolut. Verifiering av överensstämmelsen av sådana metadata ökar trovärdigheten för tidsstämplingen.

Bildsekvenser, såsom video, medför den ytterligare möjligheten att använda integrerade tidsstämplar.

Följaktligen är uppfinningen inte begränsad till de beskrivna utföringsformerna, utan kan varieras inom det fulla omfånget för de bifogade patentkraven.