2. SISTEME DE PROTECŢIE ŞI SECURIZARE A CONŢINUTULUI MULTIMEDIA

2.1. Criptografie

Criptografia este prima tehnologie la care proprietarii drepturilor intelectuale ar trebui să apeleze. Este probabil cea mai obişnuită metodă de protecţie a documentelor digitale şi sigur una dintre cele mai bine dezvoltate ca ştiinţă.

Criptografia este ştiinţa creării şi menţinerii mesajelor secrete, în sensul imposibilităţii citirii lor de către neautorizaţi. Înainte de livrare documentul este criptat şi cheia de decriptare este distribuită doar celor ce au permisiunea de a accesa copii legale ale conţinutului. Apoi fişierul criptat se publică pe Internet, dar ar fi inutil pentru un pirat fără cheia corespunzătoare. După criptare structura mesajului este schimbată; mesajul este fără înţeles şi neinteligibil până la decriptare [1-3].

În Figura 2.1 este dată schema de principiu a unui sistem de cripatre.

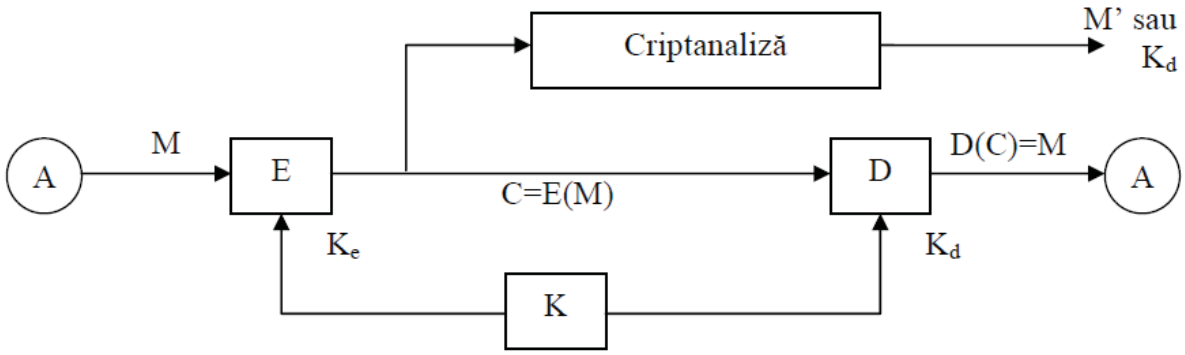

Figura 2.1. Schema bloc a unui sistem de criptare

Cu *M* se notează de regulă mesajul (textul) în clar (plain/clear text) ce urmează a fi secretizat, cu *C* se notează mesajul cifrat, secretizat, inaccesibil neavizaţilor (criptograma, cipher text), iar E este procedeul de ascundere (criptare/cifrare) a unui mesaj în clar în mesajul secretizat, conform relației (2.1).

$$C = \mathrm{E}(M) \tag{2.1}$$

D este procedeul de regăsire a mesajului în clar *M* din mesajul cifrat *C* (decriptare/descifrare) conform relației (2.2).

$$D(C) = D(E(M)) = M \tag{2.2}$$

Cheia criptografica (*K*) este mărimea necesară realizării criptării şi decriptării. Astfel, un criptosistem este sistemul format din:

- Algoritm de criptare
- Toate mesajele în clar (*M*)
- Toate mesajele criptate (*C*)
- Toate cheile (*K*)

Criptanaliza (cryptanalysis) este ştiinţa spargerii cifrurilor, deci a obţinerii mesajului *M* sau a cheii secrete *K* din mesajul criptat *C* [3].

2.1.1. Criptare cu chei simetrice (secrete)

Criptosistemele cu chei simetrice sunt sisteme de criptare pentru care cheile folosite la criptare şi decriptare sunt identice ($K_E = K_D = K$). În Figura 2.2 este dată schema de principiu a unui astfel de sistem de criptare.

Sistemele de criptare simetrice au o problemă: „cum se transportă cheia secretă de la expeditor la destinatar într-o manieră secretă şi fără posibilitate de modificare?” [2]. Dacă s-ar putea trimite cheia în siguranţă, atunci, teoretic, s-ar putea utiliza canalul securizat pentru a transmite mesajul iniţial fără a mai cripta mesajul folosind sistemul de criptare simetric. De obicei, pentru a rezolva această problemă, se folosesc curieri de încredere.

Un exemplu de folosire a unui sistem de criptare simetric este prezentat în Figura 2.3. Cristina şi Mihai doresc să comunice în secret, în timp ce George vrea să tragă cu urechea. Cristina şi Mihai pot fi avioane militare, afaceri online sau doar prieteni, ce doresc sa aibă o conversaţie privată. Nu îl pot opri pe George să asculte semnalele lor radio, dar comunică folosind criptografia.

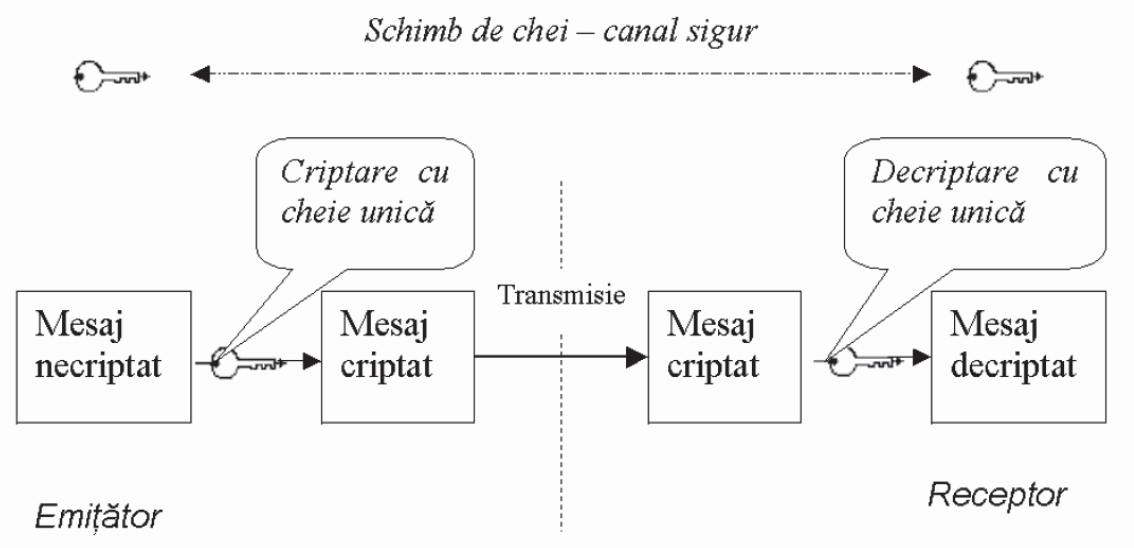

Figura 2.2. Schema de principiu a unui sistem de criptare cu chei simetrice

Cristina şi Mihai schimbă între ei o cheie digitală, astfel încât ambii să o cunoască, dar în rest să fie secretă [2]. Cristina foloseşte această cheie ca să cripteze mesajele pe care le trimite şi Mihai reconstruieşte mesajul original prin decriptare cu aceeaşi cheie. Mesajele criptate sunt inutile pentru George care nu cunoaşte cheia şi, deci, nu poate reconstrui mesajul iniţial. Cu un algoritm bun de criptare această schemă poate funcţiona bine, dar transferul cheii şi, în acelaşi timp, păstrarea ei secretă pentru George este o problemă.

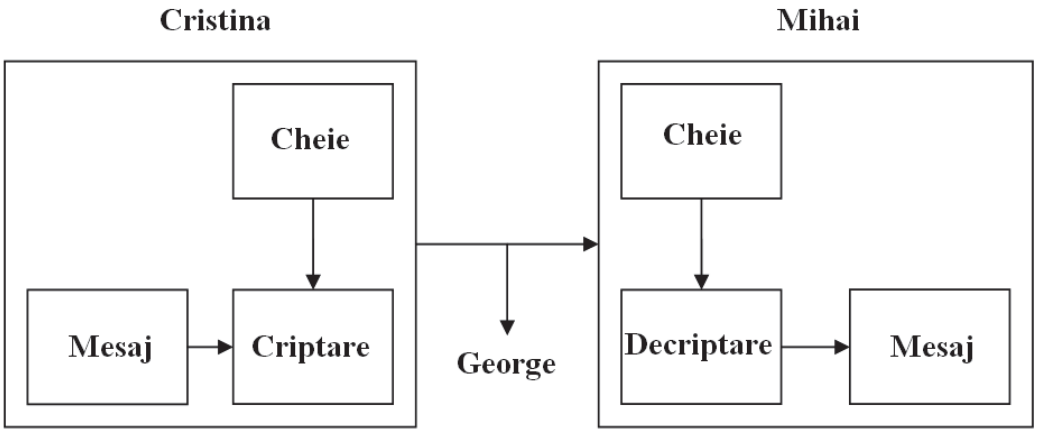

Figura 2.3. Sistem de criptare simetric

2.1.2. Criptare cu chei asimetrice (publice)

Criptosistemele cu chei asimetrice sunt sisteme de criptare pentru care cheile folosite la criptare şi decriptare sunt diferite ($K_E \neq K_D$). În Figura 2.4 este dată schema de principiu a unui astfel de sistem de criptare. La criptare se utilizează o cheie publică, iar la decriptare o cheie privată (secretă). Deoarece este imposibilă deducerea unei chei din cealaltă, una dintre chei este făcută publică, fiind pusă la dispoziţia oricui doreşte să transmită un mesaj cifrat. Doar destinatarul, care deţine cea de-a doua cheie, poate descifra şi utiliza mesajul.

Criptografia asimetrică se bazează pe ideea unei funcţii cu trapă. O funcţie cu trapă are următoarele caracteristici:

- Este o funcție biunivocă, ușor de calculat, publică *f*;
- Are o funcţie inversă f^{-1} greu de calculat;
- f^{-1} este ușor de calculat dacă este cunoscută trapa.

Astfel, deşi în criptografia convențională este necesar un schimb prealabil de chei, în criptografia cu cheie publică nu este necesar un asemenea schimb.

Sistemul de criptare asimetric este o altă soluţie mai eficientă şi mai sigură. Un exemplu de sistem de criptare asimetric este RSA care este o cunoscută unealtă de securitate [2].

Un scenariu de utilizare a unui sistem de criptare cu chei asimetrice este dat în Figura 2.5. Mihai generează o pereche de chei, spune tuturor, inclusiv lui George, cheia lui publică, dar păstrează doar pentru el cheia secretă. Oricine poate folosi cheia publică a lui Mihai ca sa îi trimită mesaje criptate, dar doar Mihai cunoaşte cheia secretă ca să le decripteze. Această schemă permite ca Mihai şi Cristina să comunice în secret fără să fie nevoie să se întâlnească.

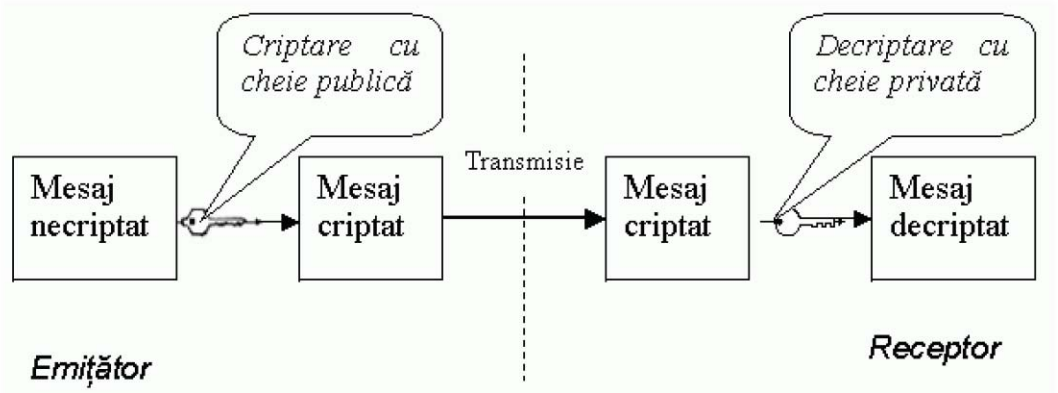

Figura 2.4. Schema de principiu a unui sistem de criptare cu chei asimetrice

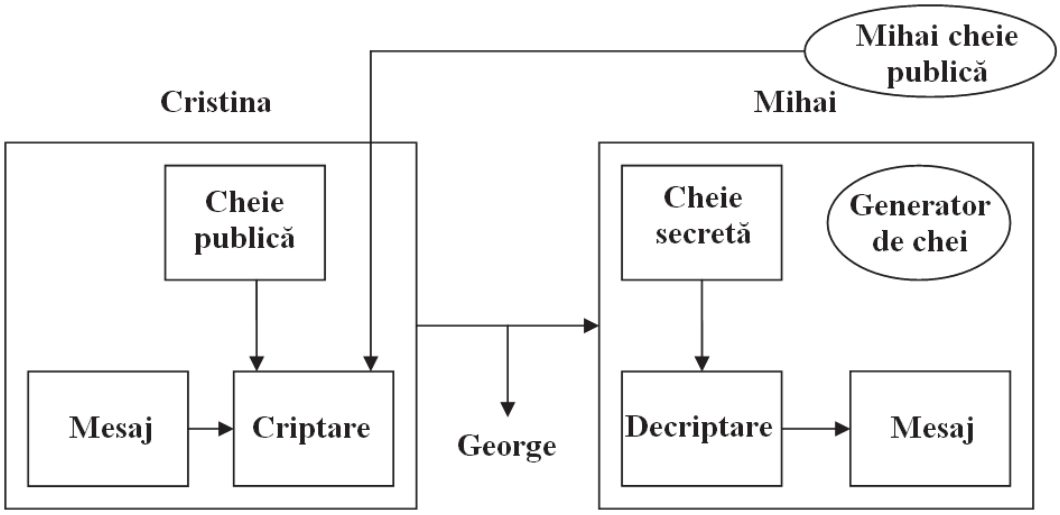

Figura 2.5. Sistem de criptare asimetric

2.2. Watermarking

Watermarking-ul digital este o tehnologie relativ nouă care inserează informaţie ascunsă în imagini, muzică, date audio sau video prin modificarea imperceptibila a acestora. Este o tehnica diferită de cea de criptare în sensul că watermarking-ul constă în ascunderea existenţei informaţiei secrete, în timp ce criptarea încearcă doar să protejeze această informaţie. Deşi procedurile de inserare sunt proiectate astfel încât oamenii să nu observe marcajele inserate, pot fi create programe care să poată extrage marcajele originale cu destul de multă uşurinţă. Apoi ele pot fi folosite pentru protecţia drepturilor de autor, supravegherea transmisiei sau pentru autentificarea conţinutului.

Datorită gamei largi de aplicaţii şi potenţialului mare al watermarking-ului, această sub-disciplină a securităţii comunicaţiilor a atras mult interes în ultimii ani. La momentul actual a evoluat până la stadiul de candidat recunoscut pentru protecţia dreptului de autor, dreptului de proprietate şi a sistemelor de securitate bazate pe amprentă. Mai mult, o serie de aplicaţii comerciale ale watermarking-ului pentru dispozitive de control al copierii sunt planificate sau chiar deja implementate. Pe viitor se doreşte dezvoltarea unor scheme *mai robuste* de watermarking care să îmbunătăţească permanent utilitatea acestei tehnici.

2.2.1. Necesitatea sistemelor de watermarking

Acum 20 de ani documentele multimedia erau aproape inexistente pe piaţa de consum. Dar, odată cu dezvoltarea rapidă a tehnologiei informaţiei digitale, orice calculator are la dispoziţie compresia de imagini şi video de înaltă calitate, acces şi bandă largă în reţea, medii portabile de stocare cu densitate mare şi puterea de procesare necesară. Dar aceste avansuri tehnologice au condus la o altă criză. Utilizatorii multimedia au posibilitatea să modifice, să producă copii ale conţinutului digital distribuit ilegal. Fără rezolvarea acestei probleme de securitate, produsele şi serviciile multimedia digitale nu pot fi lansate corespunzător în comerţul electronic [4].

Semnătura digitală şi criptografia sunt două domenii standardizate pentru protecţia conţinutului digital. Semnătura digitală este folosită pentru autentificarea transmisiunilor digitale. Este bazată pe criptografia cu cheie publică şi funcţii hash unidirecţionale. Prin trecerea documentului printr-o funcţie hash unidirecţională publică este generat un identificator unic care este codat cu cheia privată a utilizatorului. Astfel este produs un şir de caractere numit semnătură digitală. Pe lângă documentul semnat, destinatarii primesc chei publice din partea autorităţilor de certificare [4]. Documentul este autentic doar dacă se potriveşte cu semnătura decriptată prin aplicarea funcţiei hash. Oricum, documentul şi semnătura nu sunt legate în nici un fel. La transmiterea documentelor multimedia ele pot fi separate accidental sau intenţionat de către o persoană răuvoitoare. Astfel, destinatarul nu o să poată verifica autenticitatea documentului. În plus, această metodă de detecţie a modificărilor este prea restrictivă pentru obiecte multimedia. Nu permite documentului să fie supus compresiei şi schimbărilor de format şi să îşi menţină, în acelaşi timp, autenticitatea. Dacă doar un singur bit diferă de original, de exemplu datorită compresiei fără pierderi pentru transfer eficient în reţea, testul de identificare cu funcţia hash o să eşueze.

Folosirea cheilor de licenţă sigure din punct de vedere al criptografiei este altă metodă de protecţie a proprietăţii intelectuale digitale. Conţinutul documentelor este protejat împotriva manipulării şi furtului în timpul livrării prin faptul că deschiderea documentului este permisă doar persoanelor care posedă cheia corespunzătoare. Oricum, dezavantajul critic al acestei soluţii este că, după transmisia şi livrarea documentului [4], destinatarul permis are acces la datele proprietare, ce apoi pot fi reproduse perfect şi distribuite fără cheltuieli. Deci, această tehnică nu este efectivă datorită faptului că nu oferă protecţie permanentă conţinutului multimedia după livrare. Mai mult chiar, prin această metodă proprietarul intelectual nu poate depista responsabilii pentru piratare.

O soluţie ideală ar trebui să integreze, într-un fel, informaţia de securitate direct în conţinutul documentului multimedia şi informaţia de securitate să fie inseparabilă de document de-a lungul timpului lui de viaţă util. Mai mult, informaţia adiţională ar trebui să fie perceptual invizibilă deoarece, în cele din urmă, documentele multimedia sunt procesate de către observatori sau ascultători umani iar conţinutul nu trebuie să fie afectat. În sfârşit, mai intervine şi flexibilitatea sistemului folosit. Ar trebui să poată identifica copii diferite ale documentului.

Watermarking-ul digital este una dintre soluţiile potrivite. Cu mult timp în urmă era o tehnică analogică folosită pentru protecţia de documente valoroase, ca de exemplu bani, cecuri şi corespondenţa oficială. Watermark-ul pe hârtie reprezintă un model fin ce este adăugat de către producător hârtiei. Aceste urme sunt greu de reprodus convingător şi, în acelaşi timp, nu obstrucţionează procesarea normală, cum ar fi citirea, şi sunt imposibil de eliminat fără a cauza distrugerea puternică a conţinutului documentului. Tehnologiile de watermarking digital tind spre a atinge aceste scopuri în mediul digital prin inserarea unui watermark recuperabil direct în copia soft a datelor.

2.2.2. Scurt istoric

Tehnicile de watermarking nu sunt noi. Ele sunt doar un subdomeniu al steganografiei. Cuvântul steganografie provine din cuvintele greceşti: *steganos* care înseamnă acoperit, ascuns şi *graphia* care înseamnă scris, deci steganografia ar fi *scrierea ascunsă*. În comparaţie cu criptografia care codează mesajul pentru a fi neinteligibil pentru persoane neautorizate, steganografia ascunde existenţa mesajului. Kahn a găsit rădăcinile steganografiei in Egipt acum 4000 de ani, unde, pentru a înscrie informaţii în mormântul unui nobil, Khnumhoteb II, au fost folosite substituiri de simboluri hieroglifice [5], [6].

Herod a scris cum grecii au fost înştiinţaţi de intenţiile ostile ale lui Xerxes printr-un mesaj scris sub vopseaua unei mese. O altă metodă de scriere ascunsă pe care a descris-o, era tunderea mesagerului şi tatuarea mesajului sau a unei imagini pe capul acestuia. După creşterea părului mesajul era indetectabil pană la tundere [7], [8].

O altă metodă sugerată de Aenas Tacticianul era marcarea diferitelor litere dintr-un text cu cerneală invizibilă iar literele marcate formau mesajul secret.

Tehnica “watermarking” a fost folosită prima dată în secolul al XIII-lea în Fabriano, Italia, pentru etichetarea bucăţilor de hârtie făcute de mână [9]. Inventatorii au introdus desene în foile de hârtie prin subţierea anumitor regiuni sau prin plasarea unor fire în material.

Se putea avea acces la desenul inserat prin punerea bucăţii uscate a hârtiei marcate într-o lumină puternică. Tehnica Watermarking a fost folosită pentru a distinge materialul folosit la fabricare, pentru a identifica marcajul hârtiei [10] sau, mai simplu, pentru decoraţiuni [11]. Tehnica a fost numita "watermarking" deoarece urmele formate de fire erau percepute ca suprafeţe de apă pe articolele marcate [9].

Aceasta tehnică a fost acceptată ca o unealtă de etichetare pentru foi de hârtie. În secolul al XVIII-lea, marcatorii de hârtie foloseau watermark-uri pentru înregistrarea informaţiilor despre hârtia produsă. În acest fel, watermark-urile au servit şi încă servesc ca un mijloc de identificare a hârtiei cu membrii organizaţiei care au produs-o. În aproximativ acelaşi timp, numărul în creştere al schimburilor comerciale şi circulaţia bancnotelor au mărit problemele legate de falsificarea banilor. Din acest motiv, watermarking-ul a devenit rapid o metodă eficientă de a împiedica duplicarea bancnotelor. Deoarece s-a dovedit că este eficientă, tehnica watermarking este încă folosită pentru protejarea bancnotelor.

Johannes Trithemius (1462-1526), un călugăr german, a fost primul care a folosit termenul steganografie. El a codat litere folosind cuvinte religioase, astfel încât mesajele să fie practic transformate în rugăciuni cu sens. Drept recompensă pentru artificiul său, prima copie tipărită a manuscrisului său Steganographia, realizată în anul 1606, a fost plasată în Index-ul interzis al Vaticanului şi caracterizată ca „plină de superstiţii" [5], [12].

În anul 1593, Giovanni Baptista Porta a publicat o carte despre criptografie sub titlul: „De occultis literarum notis seu artis animemi occulte alijs significadi, aut ab alijs significata expiscandi enodandique. Libri III" (vezi Figura 2.6).

El a descris, printre altele, în cartea sa o metodă de ascundere a unui mesaj text secret într-un document gazdă prin intermediul unei măşti. In următorul exemplu mesajul secret poate fi extras prin ignorarea textului mascat (gri) [13]:

Honor Militiae tuus suit Carolus pater, nam cum infini to victus est, cum minima exercitu inuitus parte hostis fugit, ac prope ultimum diem iniurius peribit, necabunt Bere illum; atque extemplo puer Arato peribit, res omnes deprehensae bonae si sunt, ante Sillam, & optimo capite non poenitentias amplius decidere sperabit. Vale.

În secolul al 17-lea nu era neobişnuit să publici manuscrise anonime, mai ales când era vorba despre scrieri istorice. Riscul de a stârni mânia diferitelor grupări politice puternice, ce ar fi avut urmări severe pentru autor, era prea mare. Din acest motiv, episcopul Francis Godwin şi-a codat numele în prima literă a fiecărui capitol din manuscrisul său [12]. Acesta este un exemplu timpuriu de protecţie a drepturilor de autor.

DE
OCCVLTIS
LITERARVM NO-
TIS
SEV
ARTIS ANIMI SENSA
IO. BAPTISTA PORTA
NEAPOLITANO AVCTORE.
EXPLICANTVR AVTEM INTER
SCIENTIA
IMMVTABILIS.
MONTISBELIGARDI
M. D. XCIII.

Figura 2.6. Prima pagină a cărţii lui Porta: „De occultis notis”

Un exemplu de codare a informaţiei de drepturi de autor in piese muzicale a fost practicat de Bach care şi-a ascuns numele în multe din piesele sale. De exemplu, în piesa sa pentru cor, „Vor deinem Tor”, a folosit codarea cu cheie nulă scriind B-A-C-H în note muzicale prin numărul de apariţii a unor note: o apariţie pentru A, două apariţii pentru B, trei pentru C şi opt pentru H [6]. La mijlocul anilor 1950, Emil Hembrooke, un inginer de la Muzak Corporation, a introdus o autorizaţie prin watermarking pentru lucrările muzicale. Introducerea unei chei de identificare a autorului a fost destinată să identifice respectiva piesă. Tehnica foloseşte aplicarea intermitentă a unui filtru îngust în semnalul audio folosind un cod bazat pe codul Morse. In [14], sistemul este descris după cum urmează:

Prezenta invenţie face posibilă identificarea provenienţei unei prezentări muzicale şi, în consecinţă, constituie o metodă eficientă de prevenire a pirateriei; poate fi comparată cu watermark-ul la hârtie.

În cel de-al doilea război mondial, tehnicile de steganografie erau deja larg răspândite [5], [7]. În SUA, serviciul poştal a interzis mai multe obiecte ce ar fi putut ascunde mesaje, ca de exemplu jocuri de şah, reviste de cuvinte încrucişate şi fragmente de ziare. Alte obiecte au fost modificate înainte de livrare, ora ceasurilor de mână a fost schimbată, timbre au fost dezlipite şi coli de hârtie goale au fost schimbate. Cenzura a refrazat telegrame pentru a preveni eventualele mesaje text ce ar fi putut fi ascunse în mesaje text normale. Mii de oameni

au fost implicaţi în citirea de scrisori, în căutarea exprimării ambigue. De exemplu, următorul exemplu a fost trimis de un spion german [5]:

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

Extrăgând a doua literă a fiecărui cuvânt se obţine:

Pershing sails from NY June 1.

În anii 1980, tehnicile steganografice au fost folosite ca amprentă. Premierul Margaret Thatcher a devenit atât de iritată de scurgerea de informaţii din documente ale cabinetului spre presă încât a ordonat ca editoarele de text să fie astfel reprogramate, încât identitatea utilizatorului să fie codată în spaţierea dintre cuvinte, reuşind astfel să identifice miniştrii neloiali [15].

Watermarking-ul a trebuit să aştepte mult până să atragă destulă atenţie şi să devină un câmp activ de cercetare. În 1988, Komatsu şi Tominaga au fost primii care au folosit termenul „digital watermarking" pentru sistemul lor de autentificare a imaginii [16]. Deşi au mai existat câteva publicaţii între timp, o lucrare scrisă de Cox şi al. [17] a fost începutul unei cercetări intense. Numărul de publicaţii despre watermarking a crescut aproape exponenţial între 1995 şi 2010. Desigur, meritul nu a fost al lucrării scrise de Cox şi al., ci al organizaţiilor de cercetători în domeniul watermarking-ului. Prima conferinţă „Information Hiding Workshop" a avut loc în anul 1996 şi în 1999 „Societatea inginerilor în instrumentaţie foto-optică", SPIE, a început să organizeze conferinţe în special cu tema „Securitate si tehnici de Watermarking pentru conţinut multimedia". În afară de eforturile oficiale, diferite persoane au contribuit la formarea unei noi comunităţi de cercetare. Munca lui Martin Kutter pe tema „Digital Watermarking" este primul şi probabil cel mai bun exemplu de efort individual pentru avansarea tehnologiei. Între timp, folosirea comercială a watermarking-ului digital (WD) a început să intereseze companii şi organizaţii. Industria muzicală a apărut cu „Iniţiativa Securizării Digitale a Muzicii", SDMI, în 1999, pentru a crea un mediu legitim pentru distribuţia muzicii digitale. În plus, au fost create câteva companii (ex. Digimarc Corporation, Alpvision si Alpha-Tec), specializate în DW. Acest lucru a avut ca rezultat o creştere considerabilă a efortului destinat cercetării în diferite domenii ale WD. Este de aşteptat ca un număr mare de afaceri să fie create în viitorul apropiat pentru a crea noi baze pentru această tehnologie [4].

2.2.3. Watermarking digital

Watermark-ul digital se defineşte ca un semnal digital inserat în datele digitale şi poate fi numit şi informaţie de drepturi de autor. Watermarking-ul este un proces cheie în protejarea drepturilor de proprietate a datelor electronice, inclusiv imagini, video, sunet, etc. Cerinţa adiţională pentru watermarking este robusteţea. Chiar dacă existenţa watermark-ului este cunoscută, cum este cazul în schemele publice de watermarking, în mod ideal ar trebui să fie imposibil pentru un atacator să îndepărteze sau să distrugă informaţia watermark fără a distruge inclusiv documentul sursă. În general, watermark-ul are trei proprietăţi: este imperceptibil, inseparabil de documentul sursă şi parcurge aceleaşi transformări ca şi documentul sursă [18]. O schemă simplă de watermarking este prezentată în Figura 2.7. Procesul de watermarking reprezintă, de fapt, adăugarea semnalului watermark *W* la semnalul sursă. Semnalul watermark poate depinde, în afară de informaţia de watermark *W'* şi de o cheie *K* şi de semnalul sursă în care este ascuns (vezi relaţia (2.3)).

$$W = f_0(I, K, W') \tag{2.3}$$

Algoritmul de inserare a watermark-ului are la intrare datele sursă *I*, ca de exemplu o imagine, watermark-ul *W* şi eventual o cheie *K* şi oferă la ieşire imaginea cu watermark *I'* (vezi relaţia (2.4)).

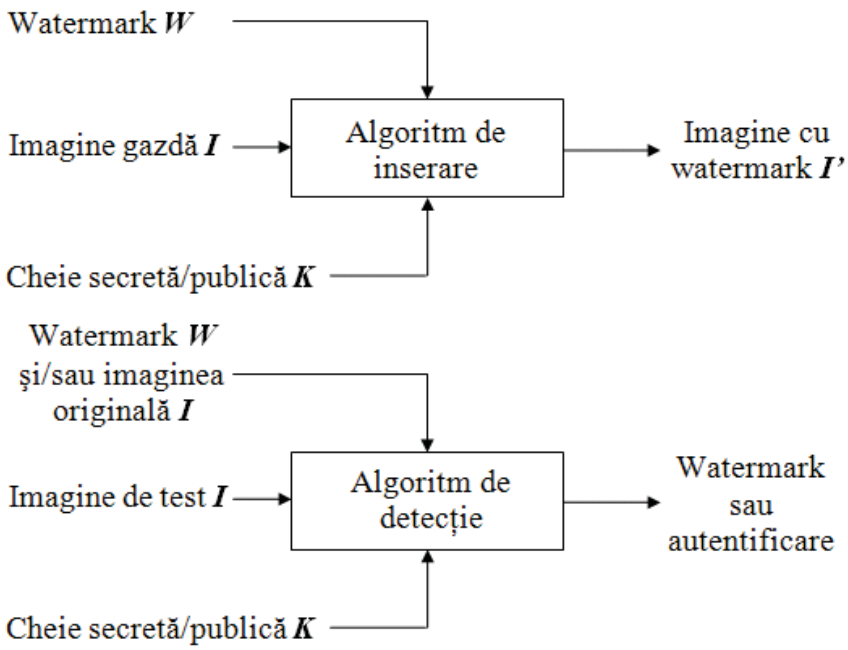

Figura 2.7. Inserarea şi detecţia watermark-ului

$$I \oplus W \longrightarrow I' \tag{2.4}$$

Algoritmul de verificare este o metoda corespunzătoare de recuperare a informaţiei watermark din semnalul mixat, eventual cu ajutorul unei chei şi a imaginii/watermark-ului original (vezi relaţia (2.5)).

$$W' = g(I, I', K) \tag{2.5}$$

2.2.4. Cerinţele unui sistem de watermarking

Fiecare sistem de watermarking are propriile cerinţe specifice. De aceea nu există un set de cerinţe ce trebuiesc îndeplinite de toate tehnicile de watermarking. Oricum, câteva direcţii generale pot fi date pentru majoritatea aplicaţiilor:

a) **Transparenţă perceptuală:** În majoritatea aplicaţiilor, algoritmul de watermarking trebuie să ascundă watermark-ul astfel încât acest lucru să nu afecteze calitatea datelor gazdă. O procedură de ascundere a watermark-ului este cu adevărat imperceptibilă dacă oamenii nu pot deosebi datele originale de cele cu watermark-ul inserat. Deoarece utilizatorii datelor cu watermark nu au acces la datele originale, nu pot face această comparaţie. De aceea, ar fi suficient ca modificările datelor supuse procesului de watermarking să treacă neobservate, atâta timp cât datele nu sunt comparate cu cele originale.

b) **Capacitate (adaos de informaţie):** Cantitatea de informaţie ce poate fi stocată în watermark depinde de aplicaţie. Pentru protecţia la copiere, un singur bit de informaţie ar fi suficient. Conform unei propuneri pentru tehnologiile de watermarking audio din partea International Federation for Phonographic Industry (IFPI), adaosul minim de informaţie pentru un watermark audio ar trebui să fie 20 biţi/s, independent de nivelul semnalului şi de tipul muzicii [19]. Oricum, conform [20], acest minim este foarte ambiţios şi ar trebui scăzut la câţiva biţi pe secundă. Pentru protecţia proprietăţii intelectuale pare rezonabil de presupus că cineva doreşte să ascundă o cantitate de informaţie similară cu cea folosită de ISBN, International Standard Book Numbering, (10 digiţi) sau ISRC, International Standard Recording Code (12 caractere alfa-numerice). În afară de acest lucru, ar mai trebui inclus anul şi drepturile acordate asupra datelor. Deci am ajunge la 60 biţi [21] sau 70 biţi [22] de

informaţie ce ar trebui introdusă în datele gazdă (imagine, cadru video, fragment audio).

c) **Robusteţe:** Un watermark fragil ce îşi propune să dovedească autenticitatea datelor gazdă, nu trebuie să fie robust la tehnicile de procesare sau alterări intenţionate ale datelor gazdă, deoarece eşuarea tentativei de a detecta watermark-ul dovedeşte că datele gazdă au fost modificate şi nu mai sunt autentice. Dar dacă watermark-ul este folosit pentru alt tip de aplicaţie, este preferabil să rămână permanent în datele gazdă, chiar dacă calitatea lor se degradează intenţionat sau neintenţionat. Exemple de modificări neintenţionate sunt aplicaţiile de stocare sau transmisiune a datelor, deoarece sunt aplicate tehnici de compresie cu pierderi pentru a reduce rata de bit şi a creşte eficienţa. Alte tehnici de procesare ce includ degradarea neintenţionată a calităţii includ filtrarea, reeşantionarea, conversiile digital-analog şi analog-digital. Pe de altă parte, datele cu watermark pot fi supuse procesării cu singurul scop de a elimina watermark-ul. În plus, atunci când există mai multe copii ale aceluiaşi conţinut cu watermark-uri diferite, ca în cazul amprentei digitale, eliminarea watermark-ului este posibilă prin conlucrarea dintre mai mulţi proprietari de copii. În general, nu ar trebui să existe nici o cale de a elimina sau altera watermark-ul fără o degradare a calităţii perceptuale a datelor gazdă suficientă pentru a le face inutilizabile.

d) **Securitate:** Securitatea tehnicilor de watermarking poate fi interpretată în acelaşi fel ca şi securitatea tehnicilor de criptare. Conform [15], ar trebui presupus că metoda folosită pentru a cripta datele este cunoscută unei părţi neautorizate şi că securitatea trebuie să fie asigurată prin alegerea unei chei. Astfel, o tehnică de watermarking este cu adevărat sigură, dacă cunoaşterea exactă a algoritmului de ascundere şi de extragere a watermark-ului nu ajută o parte neautorizată să detecteze prezenţa watermark-ului.

e) **Watermarking public şi privat:** În unele aplicaţii, ca de exemplu protecţia drepturilor de autor şi monitorizarea datelor, algoritmii de extragere a watermark-ului pot folosi datele originale, fără watermark, pentru a găsi watermark-ul. Aceste tehnici se numesc tehnici de watermarking *private*. Pentru majoritatea celorlaltor aplicaţii, ca de exemplu protecţia la copiere şi indexarea, algoritmii de extragere nu au acces la datele fără watermark. În aceste cazuri extragerea watermark-ului este

mai dificilă. Algoritmii de watermarking de acest tip se numesc *publici, orbi* sau *evidenţi*.

Toate cerinţele de mai sus sunt legate între ele. De exemplu, un watermark foarte robust poate fi obţinut prin realizarea de modificări foarte puternice ale datelor gazdă pentru fiecare bit al watermark-ului. Oricum, modificările mari ale datelor sursă vor fi observabile, iar multe modificări per bit de watermark vor limita cantitatea maximă de biţi de watermark ce pot fi stocaţi într-un obiect de date. Pe de altă parte, securitatea algoritmului de watermarking influenţează enorm robusteţea lui. Dacă nu este sigur, nu poate fi nici prea robust.

Astfel, ar trebui găsit un compromis între diferitele cerinţe, încât să poată fi dezvoltat un watermark optim pentru fiecare aplicaţie în parte. Dependenţele mutuale dintre cerinţele de bază sunt descrise în Figura 2.8.

2.2.5. Domenii de aplicabilitate

Tehnicile watermarking pot fi folosite pentru următoarele scopuri:

- **Protecţia drepturilor de autor:** Pentru protejarea drepturilor intelectuale, proprietarii datelor pot ascunde în datele lor un watermark reprezentând informaţie de drepturi de autor. Acest watermark poate dovedi proprietatea în instanţă atunci când cineva a încălcat drepturile de autor.

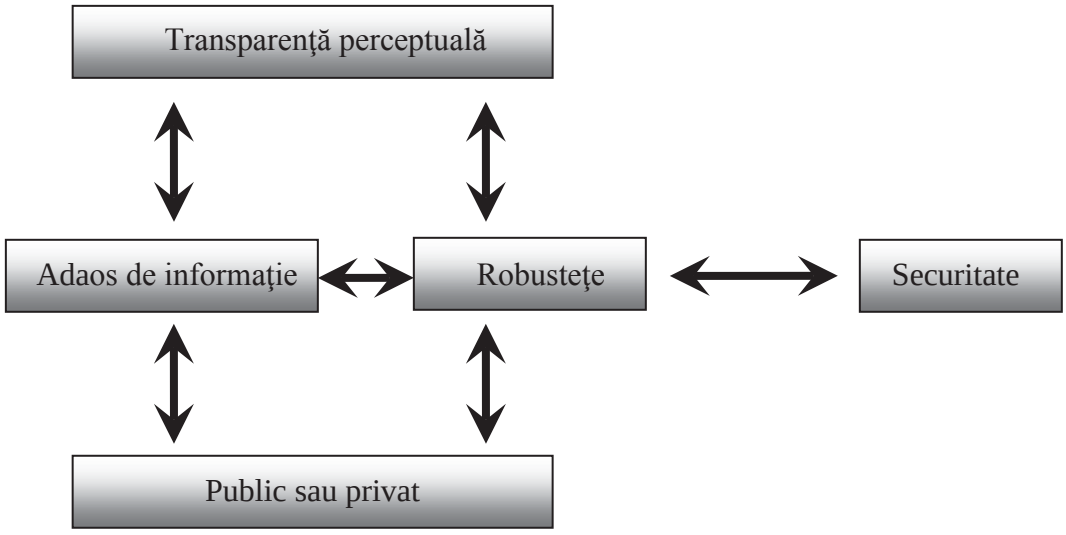

Figura 2.8. Dependenţele mutuale dintre cerinţele de bază ale unui sistem de watermarking

- **Amprentarea:** Pentru a descoperi sursa copiilor ilegale, proprietarul poate folosi o tehnică de amprentare. În acest caz, proprietarul ascunde watermark-uri diferite în copiile documentului, ce sunt distribuite diferiţilor clienţi. Amprentarea poate fi comparată cu ascunderea în datele originale a unui număr serial ce este legat de identitatea clientului. Acest lucru permite proprietarului drepturilor intelectuale să identifice clienţii care au încălcat condiţiile de licenţă prin punerea datelor la dispoziţia unei părţi terţe.
- **Protecţia la copiere:** Informaţia stocată în watermark poate controla direct aparate digitale de înregistrare cu scopul protecţiei la copiere [23]. În acest caz, watermark-ul este un bit ce interzice copierea şi detectoarele din recorder determină dacă datele oferite pot fi stocate sau nu.
- **Monitorizarea emisiei:** Prin ascunderea de watermark-uri în reclame comerciale, un sistem de monitorizare automatizat poate verifica dacă reclamele sunt emise conform contractului [15]. Nu doar reclame, ci şi producţii TV valoroase pot fi protejate prin monitorizarea traficului [24]. Buletinele de ştiri pot avea o valoare de sute de mii de USD pe oră, fapt ce le face foarte vulnerabile la violări ale drepturilor de proprietate intelectuală. Un sistem de monitorizare a traficului poate verifica toate canalele de transmisie şi poate factura posturile TV în funcţie de rezultate.
- **Autentificarea datelor:** Pot fi folosite watermark-uri fragile [25] pentru verificarea autenticităţii datelor. Un watermark fragil indică faptul că datele au fost alterate şi oferă informaţii în legătură cu poziţia părţii alterate.

Tehnicile de watermarking nu sunt folosite doar în scopuri de protecţie. Alte aplicaţii ar fi:

- **Indexarea:** Indexarea de muzică, imagini sau secvenţe video unde pot fi incluse comentarii direct în conţinut, indexarea de filme şi buletine de ştiri în care pot fi inserate marcaje şi comentarii ce pot fi apoi folosite de motoare de căutare.
- **Siguranţa medicală:** Inserarea datei şi numelui pacientului în imagini medicale poate fi o măsură de securitate folositoare [15].
- **Ascunderea datelor:** Tehnicile de watermarking pot fi folosite pentru transmiterea de mesaje private secrete. Deoarece diferite guverne restricţionează folosirea serviciilor de criptare, anumite persoane ar putea ascunde mesaje în altfel de date.

În ultimii ani au fost propuse mai multe tehnici de watermarking pentru diferite domenii de aplicabilitate folosind diferite metode de inserare şi extragere. Tehnicile de watermarking pot fi clasificate din mai multe puncte de vedere conform Tabelului Tabelul 2.1.

Tabelul 2.1. Clasificarea tehnicilor de watermarking

Clasificare		**Conţinut**
Tipul datelor gazdă		Text Imagine Audio Video
Transparenţă perceptuală		Vizibil Invizibil
Robusteţea watermark-ului		Robust Semi-fragil Fragil
Tipul watermark-ului inserat		Zgomot Text Siglă Imagine
Domeniul de procesare	Domeniul spaţial	LSB Corelaţie Metode statistice Cuantizare
	Domeniul frecvenţă	Cosinus (DCT) Wavelet (DWT) Fourier (DFT)
	Domeniul comprimat	JPEG JPEG2000 MPEG1 MPEG2 MPEG4
	Hibrid	Audio-vizual Watermark-uri diferite Scheme watermarking diferite
Date necesare pentru extragere		Privat Semi-privat Public

Watermarking-ul digital poate fi aplicat pentru mai multe tipuri de documente, ca de exemplu text, audio, imagini şi video. Tehnicile de watermarking pot fi clasificate în tehnici cu watermark vizibil sau invizibil. De obicei sunt folosite cele cu watermark invizibil, dar există aplicaţii şi pentru watermark-uri vizibile, ca de exemplu pagina de internet a unei agenţii de fotografii. Clienţii agenţiei ar trebui să poate vedea fotografiile, dar să nu le poată folosi decât după ce au efectuat plata pentru fotografiile respective. Astfel, agenţia poate insera un watermark vizibil, ca de exemplu sigla firmei, peste materialul foto şi să permită eliminarea ei doar după ce clientul a efectuat plata.

Watermark-ul trebuie să fie robust pentru a proteja proprietatea împotriva diferitelor atacuri. Astfel, se poate face o clasificare în trei categorii: watermark-uri robuste, semi-fragile şi fragile. Pot fi alese, în funcţie de necesităţi, diferite aplicaţii pentru diferite nivele de robusteţe. Aplicaţiile pentru protecţia drepturilor de autor au nevoie de un watermark robust, aplicaţii pentru autentificare sau demonstrarea integrităţii necesită un watermark fragil sau semi-fragil.

Din punctul de vedere al tipului informaţiei watermark, ele pot fi: zgomot, text, sigle, imagini binare. Primul tip include secvenţe de zgomot pseudo-aleator, aleator gaussian sau haotic. Watermark-ul poate fi o secvenţa aleatoare cu un singur bit de informaţie sau informaţie cu sens formată din mai mulţi biţi. O secvenţă aleatoare este de obicei mai robustă, dar inserarea de informaţie cu sens este pentru unele aplicaţii mai importantă.

O altă clasificare se poate face în funcţie de domeniul în care se realizează inserarea watermark-ului: domeniul spaţial, frecvenţă, comprimat sau hibrid.

În sfârşit, metodele de extragere a watermark-ului pot fi clasificate ca private, semi-private şi publice, în funcţie de necesitatea datelor originale pentru extragere.

2.3. Criptare vs. watermarking

În Figura 2.9 se face o comparație între tehnicile criptografice și cele de watermarking în ceea ce privește perioada de timp în care documentul digital este protejat. În cazul criptografiei odată ce documentul digital este decriptat, el nu mai este protejat și poate fi copiat și retransmis fără restricții. În schimb, în cazul tehnicilor de watermarking, informația de copyright este ascunsă în documentul digital şi nu se pierde la copiere/retransmitere, obiectivul fiind să rămână permanent în documentul gazdă și să nu poată fi eliminat.

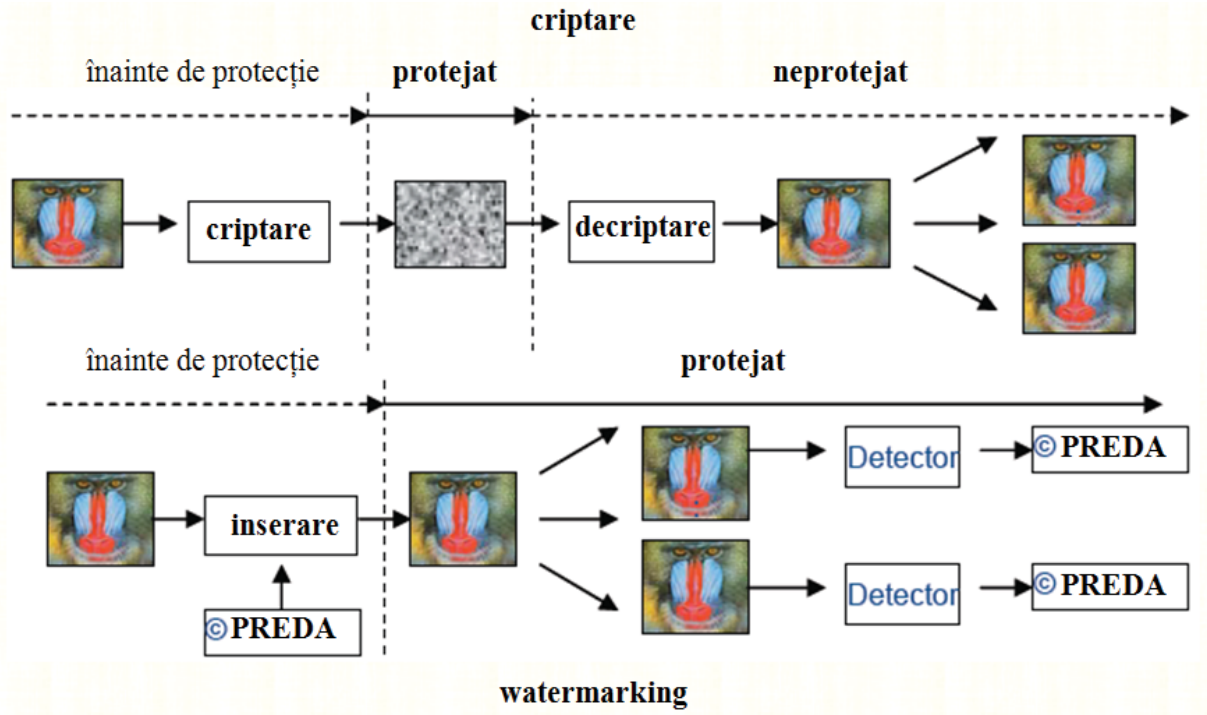

Figura 2.9. Comparație între tehnicile criptografice și cele de watermarking