Proiect IC

Securizarea imaginilor medicale delicate prin watermarking si criptografie

Autor: **Danoiu Sabrina-Elena, Facultatea de Automatica si Calculatoare, an IV, grupă 343A3**

Cuprins:

1. Introducere in watermarking

Watermark-ul reprezinta o modalitate de protectie a documentelor oficiale (inscrisuri, bancnite, etc.), ce face imposibila (sau cel putin dificila) duplicarea lor neautorizata sau falsificarea. Initial, procesul tehnologic se limita la aplicarea unei stampile pe hartia uda sau umeda, alterandu-i acesteia densitatea si textura, de aici si denumirea de watermark (water = apa / mark = semn), pentru ca mai apoi, dezvoltarea conditiilor de tiparire sa duca la aparitia unor semne complexe ce implica elemente 3D sau care pot fi citite doar de catre dispozitive speciale.

Watermark-ul digital se refera la procesul de adaugare a unui semn distinctiv pe sursa originala de semnal (fie el video, audio sau imagini) astfel incat orice copiere sau retransmitere a materialului electronic sa contina elementele de identificare si/sau marca producatorului. Cel mai cunoscut exemplu de watermark digital este sigla televiziunilor, prezenta intr-un colt al ecranului in aproape orice moment al transmisiei. In functie de interesele detinatorului de drepturi, numarul elementelor distinctive incluse in materialul digital, precum si vizibilitatea acestora, variaza de la "banalul" text de copyright (prezentat uneori ostentativ), pana la situatii in care watermark-ul digital nu poate fi identificat cu ochiul liber (hidden watermark).

Pentru o mai buna siguranță a informației, tehnica de watermarking este combinarea transformarii armonice discreta (DWT) cu transformarea cosinus discreta (DCT). Aceasta combinatie duce la aplicarea unui watermark ascuns, detectabil doar prin analiza PSNR.

1. *Exemplu de watermarking vizibil*

2. Criptarea cu AES

AES (Advanced Encryption Standard - în limba engleză, Standard Avansat de Criptare), cunoscut și sub numele de Rijndael, este un algoritm standardizat pentru criptarea simetrică, pe blocuri, folosit astăzi pe scară largă în aplicații și adoptat ca standard de organizația guvernamentală americană NIST.

Rijndael, ca și toți ceilalți algoritmi ajunși în etapa finală de selecție pentru standardul AES, a fost revizuit de NSA și, ca și ceilalți finaliști, este considerat suficient de sigur pentru a fi folosit la criptarea informațiilor guvernamentale americane neclasificate. În iunie 2003, guvernul SUA a decis ca AES să poată fi folosit pentru informații clasificate. Până la nivelul SECRET, se pot folosi toate cele trei lungimi de cheie standardizate, 128, 192 și 256 biți. Informațiile TOP SECRET (cel mai înalt nivel de clasificare) pot fi criptate doar cu chei pe 256 biți.

Atacul cel mai realizabil împotriva AES este îndreptat împotriva variantelor Rijndael cu număr redus de iterații. AES are 10 iterații la o cheie de 128 de biți, 12 la cheie de 192 de biți și 14 la cheie de 256 de biți. La nivelul anului 2008, cele mai cunoscute atacuri erau accesibile la 7, 8, respectiv 9 iterații pentru cele trei lungimi ale cheii.

Algoritmul AES foloseste o cheie comuna atat pentru encriptie, cat si pentru decriptie. Datorita complexitatii algoritmului si a avantajului foarte mic al unui potential adversar, am folosit aceasta metoda de criptare pentru a securiza imaginea asupra careia i s-a aplicat anterior watermarkingul.

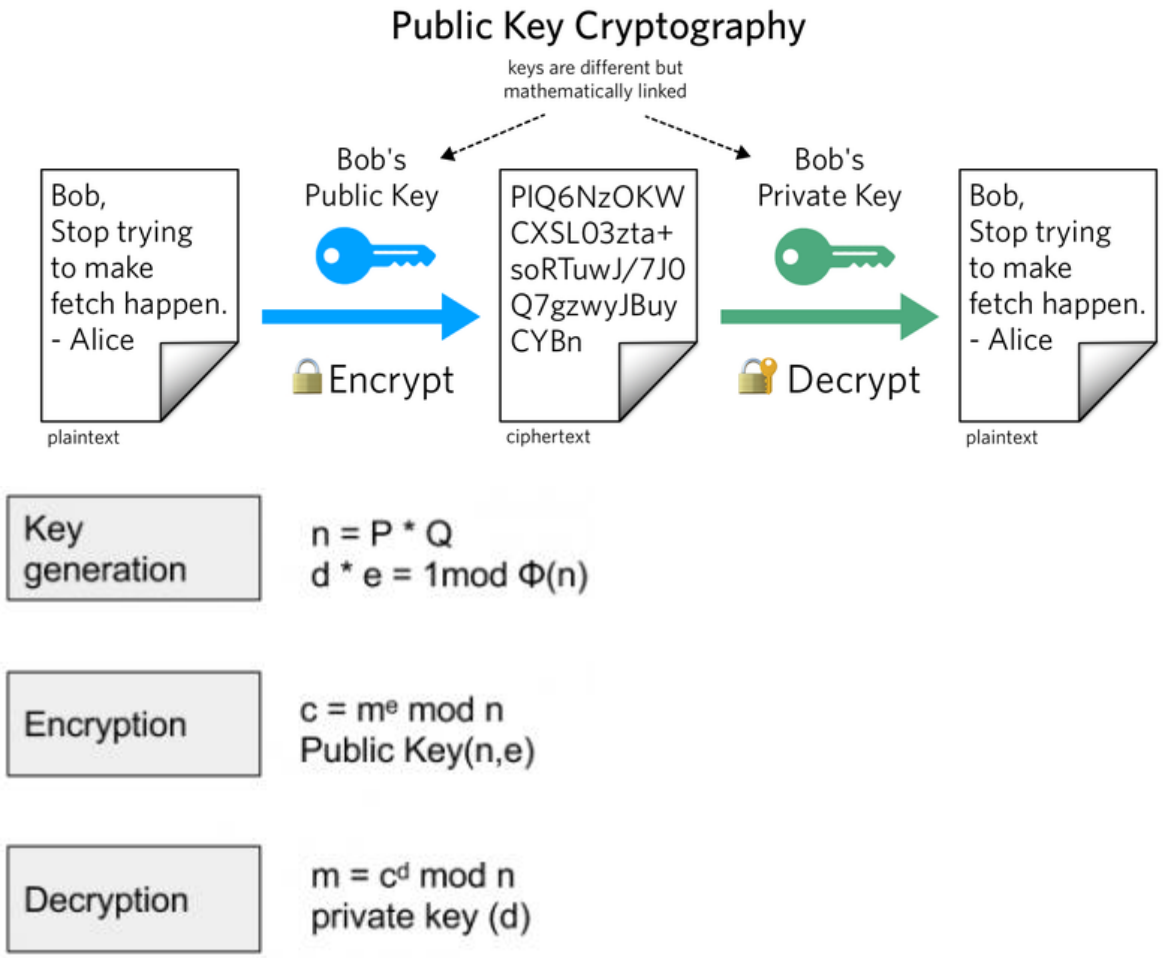
3. Criptare cu RSA

În criptografie, RSA este un algoritm criptografic cu chei publice, primul algoritm utilizat atât pentru criptare, cât și pentru semnătura electronică. Puterea sa criptografică se bazează pe dificultatea problemei factorizării numerelor întregi, problemă la care se reduce criptanaliza RSA și pentru care toți algoritmii de rezolvare cunoscuți au complexitate exponențială. Există însă câteva metode de criptanaliză care ocolesc factorizarea efectivă, exploatând maniere eronate de implementare efectivă a schemei de criptare.

RSA este un algoritm de criptare pe blocuri. Aceasta înseamnă că atât textul clar cât și cel cifrat sunt numere între 0 și n-1, cu un n ales. Un mesaj de dimensiune mai mare decât $\log n$ este împărțit în segmente de lungime corespunzătoare, numite blocuri, care sunt cifrate rând pe rând. De asemenea, ca algoritm criptografic cu chei publice, funcționează pe baza unei perechi de chei legate matematic între ele: o cheie publică, cunoscută de toată lumea, și una secretă, cunoscută doar de deținătorul acesteia.

Oricine poate cripta mesaje cu cheia publică a destinatarului, dar numai acesta din urmă poate decripta, deoarece trebuie să folosească cheia sa secretă.

Algoritmul poate fi folosit și pentru semnătura electronică, folosind cheile invers. Dacă o entitate criptează un mesaj (sau mai degrabă un hash al acestuia) cu cheia sa secretă și atașează rezultatul mesajului său, atunci oricine poate verifica, decriptând cu cheia publică a semnatarului și comparând rezultatul cu mesajul clar (sau cu hash-ul acestuia), că într-adevăr acea entitate este autorul mesajului.



Datorita complexitatii algoritmului RSA si a necesitatii computationala ridicata pentru a efectua atacuri eficiente asupra acestuia, am adaugat un pas suplimentar in securitate imaginilor encriptate, si anume encriptia cu RSA a parolei pe baza careia se afla cheia (cu SHA256) .

4. Implementare

Pasi ai implemenatrii:

I. Incepere proces de watermarking
- Pregatire date
- Aplicare DWT
- Aplicare DCT
- Reconstructie imagine
- Salvare imagine
- Recuperare watermark

II. Initializare proces de comunicatie

- Generare chei RSA
- Scriere cheie privata in fisier PEM
- Scriere cheie publica in fisier PEM

III. Trimitere cheia publica pentru encriptarea imaginii

IV. Incepere proces de encriptare
- Encriptie imagine cu AES
- Encriptie parola cu RSA

V. Primire imaginea encriptata

VI. Primire parola encriptata

VII. Incepere proces de decriptare
- Citire cheie privata
- Citire parola encriptata
- Decriptare parola

- Decriptare imagine

VIII. Comparare PSNR pentru a determina criterii de performanta

- Determinare PSNR dupa aplicarea watermarkului
- Determinare PSNR dupa decriptare (comparat cu originalul)
- Determinare grad de alterare al imaginii

IX. Concluzie

- A fost sau nu a fost imaginea alterata ?

5. Rezultate

- **Set de date:**

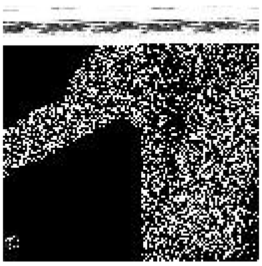
Imagine medicala de securizat:

Watermark de integrat:

- **Rezultate:**

Imagine cu watermark:

Watermark recuperat din imagine:



Parola criptata cu RSA:

ԾԹ蛺뙖□온吀쏒ꞴꝖ□ᵢ 쾩뤦嗡峋숍輖馌軨뾇□□봉□锂齇載ᑕ□□巐 ꙽8 厌□漸韊團 □□

뗀□枅□ꞓꞌ□횻ᒣ꙰□봄濊팍□□艕蟦□枫죓昐剄匯닉억켑꾌쬠ᴨᴇ□暅姐⪢駷月樂릇겭門樆

虧猇罭韠鵟畣Ÿ絡□□ꞁ 罹□□ꝑ□칍擗苎앰█□搟□◕巩瘋纣篚놐骰□✝㑲泝□熵닶↗⑹扭□

凶退ꞃꞃ□□⇩懲

Imagine decriptata ce contine watermark:

Concluzii:

- PSNR dupa aplicarea watermarkului: 35.86794767570916
- PSNR dupa decriptare (comparat cu originalul): 35.86794767570916
- Gradul de alterare al imaginii: 0 %
- Imaginea NU a fost alterata!

6. Bibliografie

1. Pooja Prakash.M, Sreeraj.R, Fepslin AthishMon, K. Suthendran (2018). Combined Cryptography And Digital watermarking For Secure Transmission of Medical Images in EHR Systems

2. Bruce Schneier (1996). Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C

3. William Stallings (2005). Cryptography and Network Security, 4th edition

4. John Kelsey, Stefan Lucks, Bruce Schneier, Mike Stay, David Wagner, Doug Whiting (2000). „Improved Cryptanalysis of Rijndael, Fast Software Encryption Workshop”

5. Ingemar J. Cox (2008). Digital watermarking and steganography.

6. Ali Al-Haj (2007). Combined DWT-DCT Digital Image Watermarking