(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) **RO 134859 A0**
(51) Int.Cl.
G06F 21/60 (2013.01),
G09C 5/00 (2006.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2020 00555**

(22) Data de depozit: **03/09/2020**

(41) Data publicării cererii:
30/03/2021 BOPI nr. **3/2021**

(71) Solicitant:
• **UNIVERSITATEA POLITEHNICA DIN BUCUREŞTI**, *SPLAIUL INDEPENDENŢEI NR.313, SECTOR 6, BUCUREŞTI, B, RO*

(72) Inventatori:
• **PREDA RADU-OVIDIU**, *CALEA DUMBRĂVII, BL.16, SC.D, AP.50, SIBIU, SB, RO;*
• **DOBRE ROBERT-ALEXANDRU**, *STR.VALEA OLTULUI, NR.2, BL.M9, SC.B, ET.7, AP.107, SECTOR 6, BUCUREŞTI, B, RO*

Această publicaţie include şi modificările descrierii, revendicărilor şi desenelor depuse conform art. 35 alin. (20) din HG nr. 547/2008

(54) # PROCEDEU DE SECURIZARE ŞI AUTENTIFICARE A IMAGINILOR DIGITALE CAPTURATE CU DISPOZITIVE MOBILE DOTATE CU CAMERĂ FOTO

(57) **Rezumat:**

Invenţia se referă la un procedeu de securizare şi autentificare a imaginilor digitale capturate cu dispozitive mobile dotate cu cameră foto. Procedeul, conform invenţiei, cuprinde inserarea unui marcaj de securitate în conţinutul imaginii, folosind tehnici de multithreading, marcajul fiind generat automat, cu parametri impliciţi, sau pe baza unei parole introduse de utilizator, marcajul fiind inserat prin cuantizare în coeficienţi de frecvenţe medii ai Transformatei Cosinus Discrete Bidimensionale, calculată pe blocuri de 8x8 pixeli de luminanţă, autentificarea imaginii fiind realizată pe acelaşi dispozitiv mobil sau pe un calculator prin extragerea marcajului de securitate din imaginea de test şi compararea cu marcajul original regenerat la decodor. Zonele falsificate sunt localizate şi marcate în imaginea de test printr-o culoare solidă, iar imaginea autentificată rezultată este salvată în spaţiul de stocare al dispozitivului mobil sau al calculatorului.

Revendicări iniţiale: 8
Revendicări amendate: 6
Figuri: 2

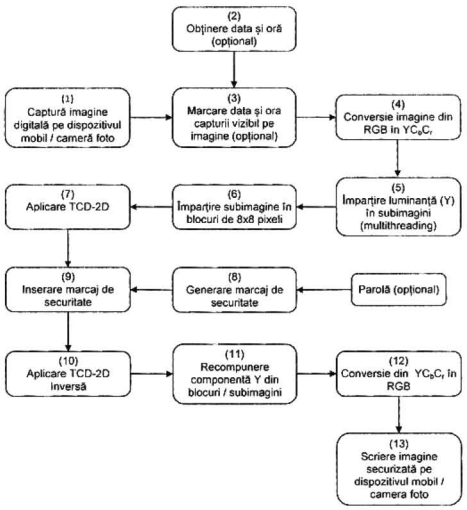

Fig. 1

RO 134859 A0

33

Descrierea invenției

Invenția se referă la un **procedeu de securizare și autentificare a imaginilor digitale capturate cu dispozitive mobile dotate cu cameră foto** fără a implica transmiterea imaginilor la distanță pentru a fi stocate ca originale sau prelucrate, cu capabilitatea de a identifica cu precizie zonele falsificate din imaginile neautentice, asigurând un necesar redus de trafic de date și respectând intimitatea utilizatorilor. Imaginile capturate cu camera foto a dispozitivului mobil sunt prelucrate imediat după captură, în totalitate offline, numai în cadrul dispozitivului mobil, fiind inserat în ele un marcaj invizibil cu rolul de le securiza conținutul imaginii. Imaginile securizate astfel obținute pot fi transmise prin medii de comunicație multimedia cum ar fi WhatsApp, Google Hangouts, Facebook Messenger sau prin e-mail fără ca marcajul de securitate să fie afectat. Un utilizator destinatar poate folosi procedeul pentru a extrage marcajul, a-l investiga din punctul de vedere al integrității și a concluziona dacă imaginea este autentică sau nu. În cazul în care imaginea nu este autentică, procedeul permite indicarea zonelor din imagine care au fost modificate după ce aceasta a fost capturată și securizată. Un exemplu reprezentativ de scenariu este în cadrul pieței de asigurări, în care agenții de asigurări fotografiază obiectul de asigurat pentru a constata starea acestuia înaintea încheierii unei polițe. În situația globală actuală, o soluție sigură de autentificare a imaginilor digitale ar conduce la evitarea acestor acțiuni, contribuind la menținerea distanțării sociale, sporind siguranța în fața COVID-19 atât a angajaților cât și a clienților. În plus, firmele din domeniu pot face tranziția către un flux de lucru mai eficient.

În prezent, din soluțiile existente se remarcă cele oferite de compania americană Truepic Inc. În cererea de brevet **US 2019356644 A1**, compania prezintă metode de autentificare a imaginilor digitale care necesită conexiune la Internet pentru a transmite imaginea către un server deținut tot de aceeași companie. Totodată, metoda propusă capturează mai multe proprietăți împreună cu fotografia, cum ar fi coordonatele GPS sau data și ora capturii, care sunt folosite în cadrul procesului de autentificare. În brevetul **US 10361866 B1** compania prezintă o metodă similară care include și o rețea blockchain. Principalele dezavantaje ale acestor soluții sunt reprezentate de necesitatea de a avea acces la Internet în cadrul procesului de autentificare, de traficul de date necesar a fi efectuat în vederea autentificării (i.e., transmiterea întregului fișier imagine către server) și de faptul că toate imaginile utilizatorilor se află în posesia companiei, prin stocarea lor pe serverul folosit în cadrul autentificării. Încă un dezavantaj care se răsfrânge asupra clienților este dat de imposibilitatea de a mai demonstra că imaginile

securizate conform metodei sunt autentice, în cazul în care compania dispare de pe piață, din cauza dispariției serverului de autentificare.

Problema pe care o rezolvă invenția se referă la securizarea și autentificarea imaginilor capturate cu camera foto a unui dispozitiv mobil fără a necesita acces la Internet, fără a stoca imaginile utilizatorilor în infrastructura companiei, garantând astfel neinvadarea intimității, permițând ca procesele de securizare și autentificare să poată fi accesate de utilizatori și după eventuala ieșire de pe piață a companiei care oferă serviciul, cele două procese nefiind dependente de infrastructura IT a acesteia.

Concret, procedeul constă în două operații:

a) operația de securizare a imaginilor, care presupune inserarea în imaginile capturate cu camera foto a unui dispozitiv mobil a unui marcaj invizibil, generat automat sau pe baza unei parole date de utilizator, printr-un algoritm de prelucrare de imagini descris în această cerere de brevet.
b) operația de autentificare a imaginilor, care presupune extragerea marcajului invizibil dintr-o imagine și compararea acestuia cu marcajul de referință, generat automat sau pe baza unei parole. În cazul în care cele două marcaje coincid, se constată că imaginea este autentică. Dacă diferă, imaginea nu este autentică, iar pe baza diferențelor se poate indica zona din imagine care a fost modificată după ce aceasta a fost securizată.

Avantajele invenției față de stadiul tehnicii sunt următoarele:

1. procedeul nu necesită acces la Internet pentru securizarea sau autentificarea imaginilor. Accesul la Internet este opțional, numai pentru obținerea datei și a orei. Chiar și în cazul optării pentru obținerea datei și a orei, traficul de date este neglijabil, mult mai redus decât în cazul metodelor de comparație;
2. imaginile capturate de utilizatori folosind procedeul propus nu părăsesc dispozitivul mobil decât daca aceștia le trimit în mod voluntar. Nu este necesar un server de autentificare pentru funcționarea procedeului. În acest fel, intimitatea utilizatorilor nu este invadată;
3. procesele de securizare și autentificare nu sunt dependente de infrastructura IT a unei companii, ci toată prelucrarea imaginii are loc pe dispozitivul mobil.

Prezentăm în continuare un exemplu de realizare a invenției, cu cele două procese ale sale (securizare și autentificare) cu referire la Figurile 1 și 2. În Figura 1 este ilustrată schema de principiu a procesului de securizare. Se pot identifica următoarele operații:

(1) – captura imaginii digitale direct de la senzor, nu printr-o aplicație terță și nu prin încărcarea unei imagini din memoria dispozitivului mobil sau din alt mediu de stocare;

(2) – etapă opțională, reprezintă contactarea unui server de timp din Internet și obținerea datei și orei actuale. Este utilă când se dorește marcarea imaginilor cu data și ora capturii. Nu se pot folosi datele stocate pe dispozitivul mobil deoarece acestea pot fi modificate de utilizator după bunul plac, lăsându-i posibilitatea de a introduce date care nu sunt conforme cu momentul capturii;

(3) – etapă opțională, se scrie peste imaginea primită de la senzor un text care indică data și ora la care a fost capturată imaginea. Se poate oferi utilizatorului opțiunea de a selecta poziționarea textului în imagine;

(8) – generarea unor date binare care reprezintă marcajul de securitate ce urmează a fi introdus în imagine. Acesta se poate genera automat, cu parametri impliciți, sau pe baza unei parole setate de utilizator;

(4-7),(9) – inserarea în imagine a marcajului generat conform punctului (4) din această listă. Inserarea se face conform unui algoritm special dezvoltat pentru a asigura că modificările aduse imaginii în urma procesului de inserare sunt invizibile pentru sistemul vizual uman. Algoritmul este prezentat în acest document;

(10-12) – recompunerea imaginii RGB din blocurile marcate conform algoritmului prezentat în acest document;

(13) – imaginea astfel obținută este scrisă în spațiul de stocare al dispozitivului mobil sau al camerei foto, putând fi de acum trimisă către alți utilizatori și devenind accesibilă și pentru alte aplicații.

În Figura 2 este ilustrată schema de principiu a procesului de autentificare. Se pot identifica următoarele operații:

(1) – încărcarea imaginii digitale care se dorește a fi investigată, disponibilă ca fișier imagine în spațiul de stocare al dispozitivului mobil;

(2-6) – extragerea marcajului din imaginea încărcată, conform algoritmului prezentat în acest document;

(7) – regenerarea datelor binare care reprezintă marcajul de securitate ce a fost introdus în imagine. Acesta se poate genera automat, cu parametri impliciți, sau pe baza parolei date de utilizator. Pentru o funcționare corectă, cele două parole (cea folosită în procesul de securizare și cea folosită în procesul de autentificare) trebuie să fie identice;

(8) – cele două marcaje (i.e., cel extras din imagine și cel regenerat) sunt comparate. Dacă cele două marcaje sunt identice înseamnă că imaginea este autentică (i.e., nu a suferit modificări după ce a fost securizată). Daca marcajele nu sunt identice înseamnă că imaginea a suferit modificări după securizare;

(9) – generarea matricei de autentificare, în care blocurile autentice sunt marcate cu 0 logic, iar blocurile potențial falsificate cu 1 logic;

(10) – rezultatele anterioare sunt rafinate, asupra matricei de autentificare fiind aplicate operații de morfologie matematică pentru a elimina falsurile pozitive. În urma rezultatelor de la finalul acestei etape se poate lua decizia dacă imaginea este autentică sau nu;

(11) – folosind matricea de autentificare se localizează zonele falsificate din imagine. Acestea sunt marcate cu o culoare solidă astfel încât utilizatorul să le poată identifica ușor.

(12) – utilizatorul poate salva rezultatul procesului de autentificare, adică imaginea cu zonele marcate ca fiind neautentice.

Conform invenției, procesul de securizare a imaginilor împotriva falsificării are loc exclusiv pe dispozitivul mobil sau pe camera foto digitală, iar procesul de autentificare a imaginilor potențial falsificate poate avea loc pe dispozitivul mobil sau pe calculator.

Procesul de securizare a imaginii se realizează folosind algoritmul următor, ce este parte componentă a acestei invenții:

1. Imaginea digitală originală este captată direct de la senzorul dispozitivului mobil sau al camerei foto digitale.

2. Peste imaginea captată sunt suprapuse într-unul dintre colțuri data și ora curentă, interogate de la un server de timp securizat de pe Internet (pas opțional). Notăm această imagine RGB cu I_0.

3. Imaginea $\mathbf{I}_0$ este convertită din spațiul de culoare RGB în spațiul de culoare YC_bC_r și din cele trei componente se păstrează mai departe doar componenta de luminanță (Y), notată cu $\mathbf{Y}_0$.

4. Imaginea de luminanță $\mathbf{Y}_0$ este împărțită în 8 subimagini, fiecare subimagine conținând un număr de întreg de blocuri nesuprapuse de 8x8 pixeli din imaginea $\mathbf{Y}_0$. Cele 8 subimagini pot fi prelucrate în paralel folosind tehnici de multithreading, dacă terminalul mobil conține un procesor cu 8 sau mai multe nuclee, sau într-o combinație serie-paralel, dacă se lucrează cu un procesor cu mai puține nuclee.

5. Marcajul de securitate ce va fi inserat în imagine este generat ca o secvență pseudo-aleatoare binară **M** în mod automat, cu parametri impliciți, sau pe baza unei parole P date de utilizator folosind un generator de numere pseudo-aleatoare. Un exemplu este utilizarea algoritmului Mersenne-Twister pentru a genera secvența pseudo-aleatoare **M** pe baza parolei P. Presupunând că imaginea de luminanță are o rezoluție de a x b pixeli, dimensiunea vectorului binar **M** este:

$$d_M = n[a/8][b/8],$$

unde n este numărul de biți ce vor fi inserați în fiecare bloc de 8x8 pixeli al imaginii $\mathbf{Y}_0$, iar [.] este operatorul de parte întreagă. Inserarea marcajului **M** în subimagini se va face conform pașilor ce vor fi prezentați în continuare.

6. Confrom modului prezentat anterior de impărțire a imaginii $\mathbf{Y}_0$ în subimagini și a modului de generare a marcajului M, fiecărui bloc de dimensiune 8x8 pixeli al imaginii $\mathbf{Y}_0$ îi va corespunde un șir de *n* biți ai marcajului **M**. Deoarece inserarea se realizează identic pentru fiecare bloc, în continuare se va prezenta modul în care se inserează un șir $\mathbf{M}_i$ de *n* biți ai marcajului **M** într-un bloc $\mathbf{Y}_{0,i}$ de 8x8 pixeli de luminanță ai unei subimagini, unde *i* este indicele blocului.

7. Asupra blocului $\mathbf{Y}_{0,i}$ se aplică Transformata Cosinus Discretă Bidimensională (TCD-2D) obținându-se un bloc $\mathbf{C}_{0,i}$ de 8x8 coeficienți TCD-2D.

8. Fie $\mathbf{Q}_1$ matricea standard JPEG de cuantizare a luminanței corespunzătoare factorului de calitate JPEG de 50. Pe baza matricei $\mathbf{Q}_{50}$ se calculează matricea de cuantizare $\mathbf{Q}_1$ corespunzătoare factorului de calitate f_1 conform relației:

$$\mathbf{Q}_1 = \begin{cases} \text{rot}\left(50 \cdot \mathbf{Q}_{50} / f_1\right), \textit{dacă } 1 \le f_1 \le 50 \\ \text{rot}\left[\mathbf{Q}_{50}\left(2 - 0.02 \cdot f_1\right)\right], \textit{dacă } 50 < f_1 \le 100 \end{cases}$$

unde rot(.) este operatorul de rotunjire la cel mai apropiat număr întreg.

9. Matricele $\mathbf{C}_{0,i}$ și $\mathbf{Q}_1$ sunt scanate în zigzag, obținându-se vectorii $\mathbf{C}_{0,i,z}$ și $\mathbf{Q}_{1,z}$. În mod automat sau pe baza parolei P din fiecare vector de coeficienți $\mathbf{C}_{0,i,z}$ sunt selectați un număr de *n* coeficienți de frecvențe medii în care vor fi inserați cei *n* biți corespunzători ai marcajului de securitate **M**, câte un bit de securitate în fiecare coeficient. Fie *b* bitul de securitate din **M** ce urmează a fi inserat într-un coeficient $\mathbf{C}_{0,i,z}(j)$ selectat, unde *j* este indicele corespunzător poziției coeficientului în vectorul $\mathbf{C}_{0,i,z}$. Inserarea bitului b în $\mathbf{C}_{0,i,z}(j)$ se face printr-un procedeu de cuantizare conform relației:

$$\mathbf{C}_{1,i,z}(j) = \text{rot}\left[\frac{\mathbf{C}_{0,i,z}(j)}{2 \cdot Q_{1,z}(j)} - b\right] \cdot 2 \cdot \mathbf{Q}_{1,z}(j) + b \cdot \mathbf{Q}_{1,z}(j),$$

unde $\mathbf{C}_{1,i,z}(j)$ este coeficientul ce va conține bitul de securitate *b*.

10. După inserare, coeficienții originali $\mathbf{C}_{o,i,z}(j)$ sunt înlocuiți în vectorul $\mathbf{C}_{0,i,z}$ cu cei marcați $\mathbf{C}_{1,i,z}(j)$, obținându-se vectorul $\mathbf{C}_{1,i,z}$ de 64 coeficienți, ce conține marcajul de securitate. Prin scanare zigzag inversă, din vectorul $\mathbf{C}_{1,i,z}$ se obține matricea $\mathbf{C}_{1,i}$ de 8x8 coeficienți marcați, asupra căreia se aplică transformata TCD-2D Inversă pentru a obține blocul marcat $\mathbf{Y}_{1,i}$ de 8x8 pixeli de luminanță.

11. Pașii 7-10 ai algoritmului se repetă pentru fiecare bloc $\mathbf{Y}_{1,i}$ de 8x8 pixeli de luminanță, obținându-se matricea de luminanță $\mathbf{Y}_1$ ce conține întreg marcajul de securitate **M**. Ulterior se face trecerea înapoi de la spațiul de culori YC_bC_r la spațiul de culori RGB, rezultând imaginea marcată $\mathbf{I}_1$.

12. Imaginea $\mathbf{I}_1$ este salvată în spațiul de stocare al dispozitivului mobil sau al camerei foto.

Imaginea $\mathbf{I}_1$ este securizată împotriva modificărilor de conținut și, în plus, orice compresie JPEG ulterioară a acestei imagini cu factori de calitate $f_2 \geq f_1$ nu va fi detectată ca o falsificare, algoritmul diferențiind între o falsificare intenționată și compresia JPEG utilizată de majoritatea aplicațiilor pentru stocarea imaginilor.

Procesul de autentificare a unei imagini de test se realizează pe dispozitivul mobil sau pe calculator folosind algoritmul următor, ce este, de asemenea, parte componentă a acestei invenții:

1. Marcajul de securitate original de referință **M** este regenerat la decodor în mod automat sau pe baza parolei P date de utilizator la fel ca la procesul de securizare.

2. Imaginea de test $\mathbf{I}'_1$, posibil falsificată, este încărcată în memoria telefonului în format RGB.

3. Asupra imaginii $\mathbf{I}'_1$ se aplică pașii 3-5 ai procesului de inserare, obținând imaginea de luminanță $\mathbf{Y}'_1$ ce este împărțită în 8 subimagini, fiecare putând fi prelucrată în paralel pe terminalul mobil pentru creșterea vitezei de procesare.

4. Din fiecare bloc $\mathbf{Y}'_{1,i}$ de 8x8 pixeli al $\mathbf{Y}'_1$ se extrage o secvență de câte *n* biți conform algoritmului descris în pașii următori.

5. Asupra blocului $\mathbf{Y}'_{1,i}$ se aplică TCD-2D obținându-se un bloc $\mathbf{C}'_{1,i}$ de 8x8 coeficienți TCD-2D.

6. Matricea $\mathbf{C}'_{1,i}$ este scanată în zigzag, obținându-se vectorul $\mathbf{C}'_{1,i,z}$. În mod automat sau pe baza parolei P, din fiecare vector de coeficienți $\mathbf{C}'_{1,i,z}$ sunt selectați aceiași *n* coeficienți folosiți și în procesul de securizare. Din fiecare din cei *n* coeficienți este extras câte un bit de securitate. Extragerea bitului $b'(k)$ din $\mathbf{C}'_{1,i,z}(j)$ se face conform relației:

$$b'(k) = \mathrm{mod}2\left\{\mathrm{rot}\left[\frac{\mathbf{C}'_{1,i,z}(j)}{\mathbf{Q}_{1,z}(j)}\right]\right\},\ k = \overline{0,n-1},$$

unde $b'(k)$ sunt biții de securitate extrași din blocul curent, mod2(.) este restul împărțirii la 2, iar $\mathbf{Q}_{1,z}$ se obține la fel ca în procesul de inserare (pașii 8 și 9).

7. Fie $b(k)$ biții de securitate originali ai blocului curent, obținuți din marcajul de securitate **M** regenerat la punctul 1. Pentru a clasifica blocul current ca fiind autentic sau potențial falsificat, marcajul $b'(k)$ extras este comparat cu cel original $b(k)$. Dacă cele două sunt identice, blocul de test este considerat ca fiind autentic, altfel este clasificat ca fiind potențial falsificat.

8. Repetând procedeul anterior pentru fiecare bloc, se obține o matrice sau mască de autentificare binară **A** de dimensiune egală cu numărul de blocuri de 8x8 pixeli din imagine $d_A = [a/8][b/8]$, unde a x b este rezoluția imaginii originale și [.] este operatorul de parte întreagă. Dacă pe poziția (x,y) a matricii **A** se află un bloc potențial falsificat, $\mathbf{A}(x,y)=1$, altfel $\mathbf{A}(x,y)=0$.

9. Pentru a elimina alarme false (valori de "1" izolate din matricea de autentificare) ce pot apărea datorită unor prelucrări neagresive de imagini, asupra matricei A se aplică operații succesive de morfologie matematică de eroziune și dilatare, obținând matricea de autentificare corectată $\mathbf{A}'$.

10. Zonele falsificate sunt localizate și marcate în imaginea de test $\mathbf{I}'_1$ prin colorarea cu o culoare solidă a blocurilor pentru care matricea $\mathbf{A}'$ are valori "1".

11. Imaginea cu zonele falsificate marcate, numită imagine autentificată, este salvată în spațiul de stocare al dispozitivului mobil sau pe calculator.

Algoritmul de securizare a imaginilor descris în prima parte poate fi utilizat pe terminale mobile sau în camere foto digitale. Algoritmul de autentificare a imaginilor prezentat în a doua parte poate fi utilizat atât pe terminale mobile, dar și ca aplicație pentru calculatoare pentru a autentifica un număr mare de imagini de test într-un timp scurt.

Procesele descrise mai sus au potențial de a fi valorificate atât în mediul industrial, în companii, cât și la nivel de consumator și pot reduce fraudele bazate pe falsificarea de imagini.

Revendicări

1. Procedeu de securizare și autentificare a imaginilor digitale capturate cu dispozitive mobile dotate cu cameră foto sau cu o cameră foto digitală caracterizat prin aceea că securizarea imaginilor se face exclusiv pe dispozitivul de captură, fără necesitatea conexiunii la Internet.

2. Procedeu conform revendicării 1 caracterizat prin aceea că se securizează imaginea digitală pe dispozitivul de captură prin inserarea unui marcaj de securitate în conținutul imaginii folosind tehnici de multithreading, astfel încât modificările aduse imaginii în urma procesului de inserare sunt invizibile pentru sistemul vizual uman.

3. Procedeu conform revendicării 2 caracterizat prin aceea că marcajul de securitate ce este inserat în imagine este generat în mod automat sau pe baza unei parole introduse de utilizator.

4. Procedeu conform revendicării 2 caracterizat prin aceea că marcajului de securitate se inserează prin cuantizare în coeficienți de frecvențe medii ai Transformatei Cosinus Discrete Bidimensionale, calculată pe blocuri de 8x8 pixeli de luminanță, utilizând metoda prezentată în descrierea brevetului, marcajul inserat fiind robust la compresia JPEG cu pierderi și fragil la modificări intenționate de conținut.

5. Procedeu conform revendicării 1 caracterizat prin aceea că se determină autenticitatea unei imagini potențial falsificate și se localizează zonele falsificate pe dispozitivul mobil sau pe calculator folosind tehnici de multithreading.

6. Procedeu pentru a determina autenticitatea imaginii de test conform revendicării 5 caracterizat prin aceea că se extrage marcajul de securitate din imaginea de test prin tehnica prezentată în descrierea brevetului și se compară cu marcajul regenerat pe dispozitiv în mod automat sau pe baza parolei introduse de utilizator.

7. Procedeu conform revendicării 5 caracterizat prin aceea că se elimină alarmele false la autentificare, ce pot apărea datorită unor prelucrări neagresive de imagini, prin aplicarea de operații succesive de morfologie matematică.

8. Procedeu conform revendicării 5 caracterizat prin aceea că, în cazul detectării falsificării imaginii, zonele falsificate sunt localizate și marcate în imaginea de test printr-o culoare solidă și imaginea autentificată rezultată este salvată în spațiul de stocare al dispozitivului mobil sau calculatorului.

Figuri

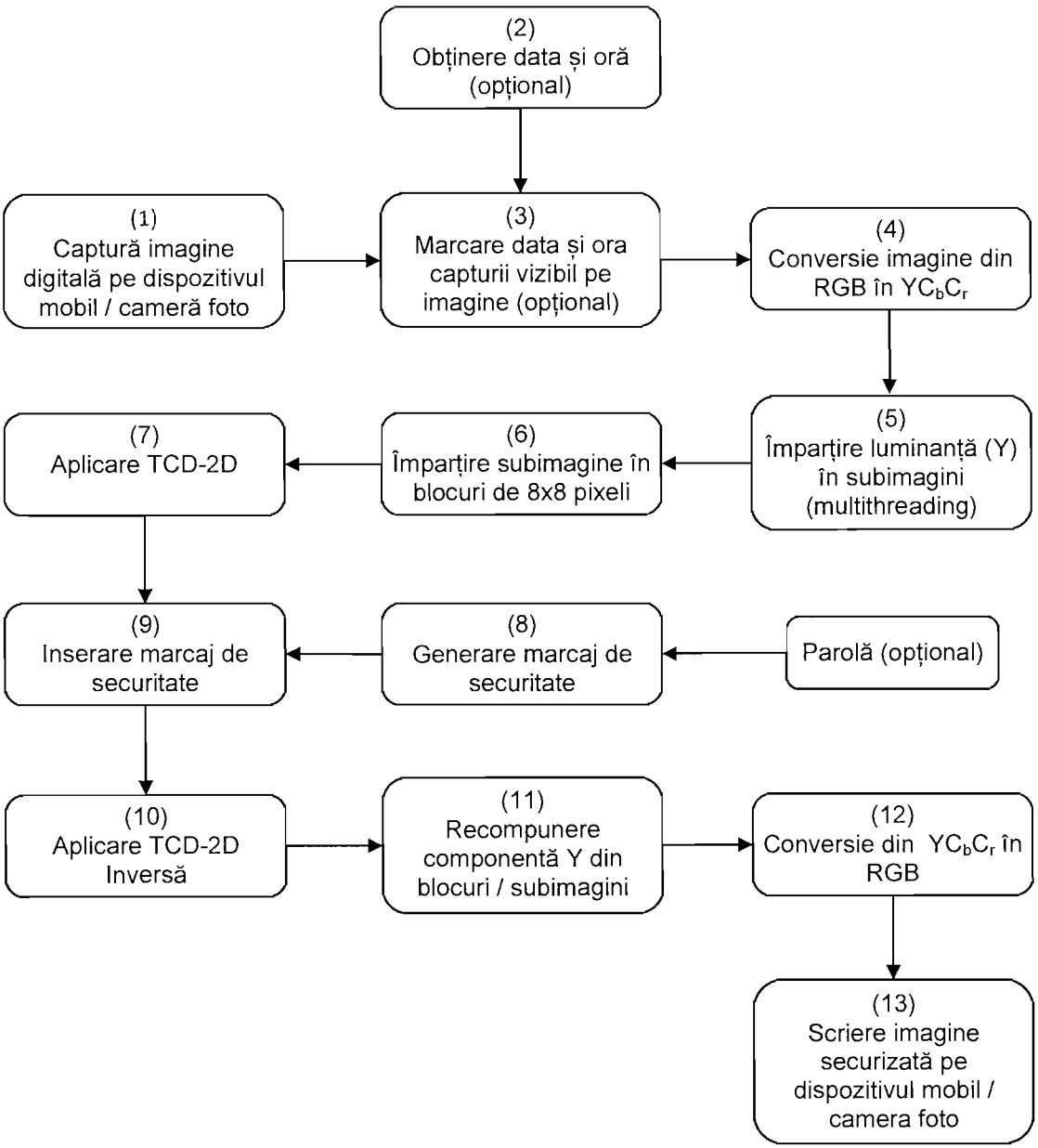

Figura 1. Schema de principiu a procesului de securizare.

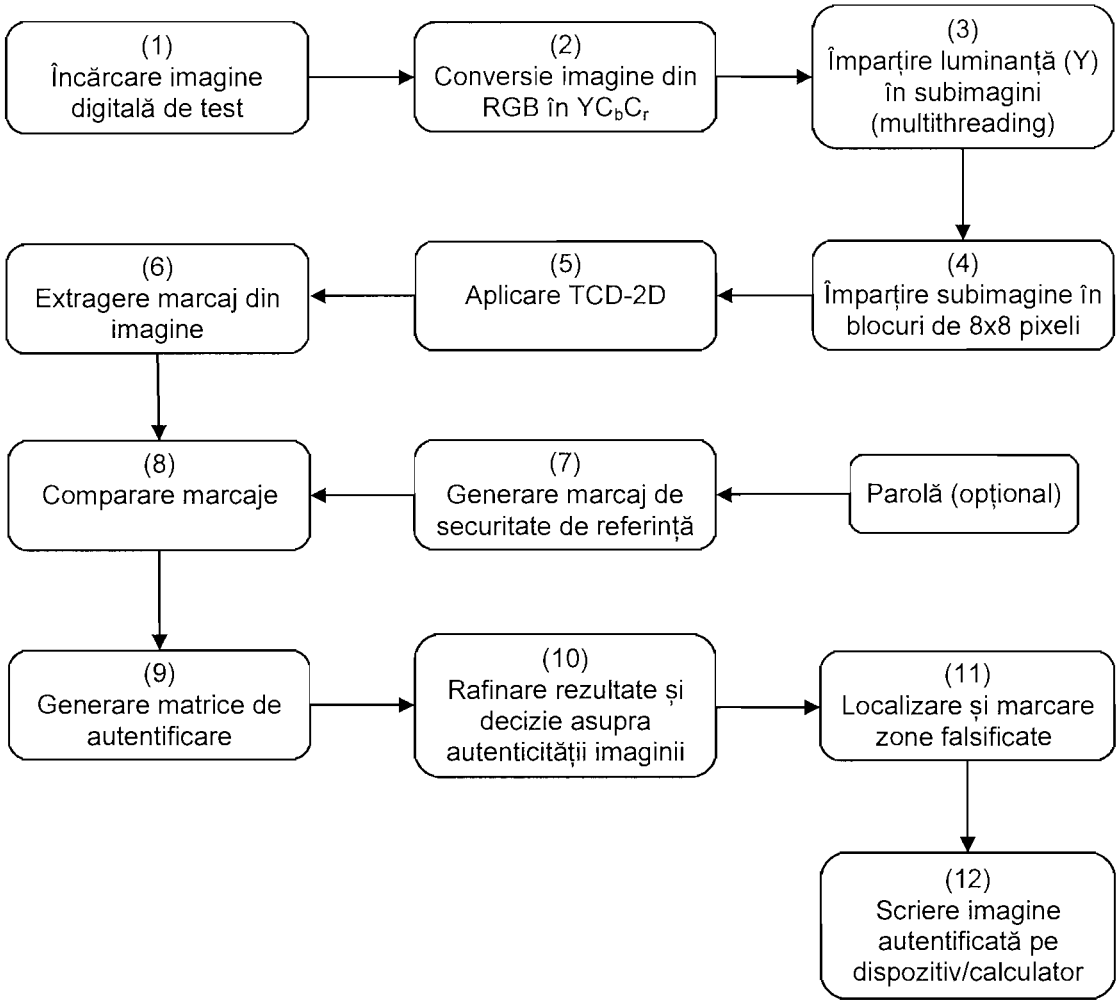

Figura 2. Schema de principiu a procesului de autentificare.

Procedeu de securizare și autentificare a imaginilor digitale capturate cu dispozitive mobile dotate cu cameră foto

Revendicări

1. Procedeu de securizare și autentificare a imaginilor digitale capturate cu dispozitive mobile dotate cu cameră foto sau cu o cameră foto digitală caracterizat prin aceea că permite securizarea și autentificarea imaginilor exclusiv pe dispozitivul de captură, imaginea rămânând pe dispozitivul mobil în timpul securizării și autentificării, fără a folosi o conexiune la Internet sau la orice alte dispozitive pentru efectuarea celor două operații, funcționând prin inserarea, respectiv verificarea integrității unui marcaj generat automat sau pe baza unei parole introduse de utilizator, marcajul fiind inserat, respectiv extras, în/din coeficienții Transformatei Cosinus Discretă de frecvențe spațiale medii, fiind capabil, în etapa de autentificare, de a detecta și indica zonele falsificate din imaginile care au fost securizate cu acest procedeu.

2. Procedeu conform revendicării 1 caracterizat prin aceea că se securizează imaginea digitală pe dispozitivul de captură prin inserarea unui marcaj de securitate în conținutul imaginii folosind tehnici de multithreading, astfel încât modificările aduse imaginii în urma procesului de inserare sunt invizibile pentru sistemul vizual uman.

3. Procedeu conform revendicării 1 caracterizat prin aceea că marcajului de securitate se inserează prin cuantizare în coeficienți de frecvențe medii ai Transformatei Cosinus Discrete Bidimensionale, calculată pe blocuri de 8x8 pixeli de luminanță, marcajul inserat fiind robust la compresia JPEG cu pierderi și fragil la modificări intenționate de conținut.

4. Procedeu pentru a determina autenticitatea imaginii de test conform revendicării 1 caracterizat prin aceea că se marcajul de securitate extras din imaginea de test se compară cu marcajul regenerat pe dispozitivul mobil sau, opțional, pe calculator, în mod automat sau pe baza parolei introduse de utilizator.

5. Procedeu conform revendicării 1 caracterizat prin aceea că se elimină alarmele false la autentificare, ce pot apărea datorită unor prelucrări uzuale, neagresive de imagini, prin aplicarea de operații succesive de morfologie matematică.

6. Procedeu conform revendicării 1 caracterizat prin aceea că, în cazul detectării falsificării imaginii, zonele falsificate sunt localizate și marcate în imaginea de test printr-o culoare solidă și imaginea autentificată rezultată este salvată în spațiul de stocare al dispozitivului mobil sau, opțional, pe calculator.