(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) RO 129752 A0
(51) Int.Cl.
H04N 7/18 (2006.01),
G06T 5/10 (2006.01),
G06T 5/40 (2006.01),
G06T 7/60 (2006.01),
G06K 9/36 (2006.01),
G08B 25/08 (2006.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2014 00203**

(22) Data de depozit: **14.03.2014**

(41) Data publicării cererii:
29.08.2014 BOPI nr. **8/2014**

(71) Solicitant:
• **BUDIŞTEANU IONUŢ ALEXANDRU**,
STR. FERDINAND NR. 28,
RÂMNICU VÂLCEA, VL, RO

(72) Inventatori:
• **BUDIŞTEANU IONUŢ ALEXANDRU**,
STR. FERDINAND NR. 28,
RÂMNICU VÂLCEA, VL, RO

(54) # DISPOZITIV ŞI METODĂ PENTRU SUPRAVEGHEREA AUTOMATĂ A UNEI LOCAŢII

(57) **Rezumat:**

Invenţia se referă la un dispozitiv şi la o metodă destinate să asigure detecţia automată a unor cadre care conţin informaţii a căror prelucrare trebuie făcută într-un timp relativ scurt, cu utilizare într-o incintă dintr-o bancă comercială, spaţiu comercial sau altele asemenea. Dispozitivul conform invenţiei are în componenţă o cameră (**1**) de supraveghere cu calitate destul de bună, căreia i s-a înlăturat filtrul optic de bandă infraroşu, şi cu o rezoluţie relativ mare, care este conectată prin portul de comunicaţie I^2C sau USB la un microprocesor (**2**), un sistem GPS (**3**) cu protocol de conectare SiRF 3 sau NMEA, o memorie (**4**) Flash/NVRAM de minimum 1 GB şi o conexiune (**5**) la internet/o reţea privată securizată/GPRS, pentru a transmite alarma la un centru specializat. Metoda conform invenţiei cuprinde parcurgerea paşilor I...XVI, în care imaginile de interes sunt selecţionate şi prelucrate, astfel încât, dacă sunt îndeplinite condiţiile impuse, să fie generată o alarmă, care conţine gradul de confidenţă şi secvenţa cadrelor suspecte, după care se dă curs la analize de către o persoană umană a imaginii, în vederea confirmării şi luării măsurilor care se impun.

Revendicări: 2
Figuri: 2

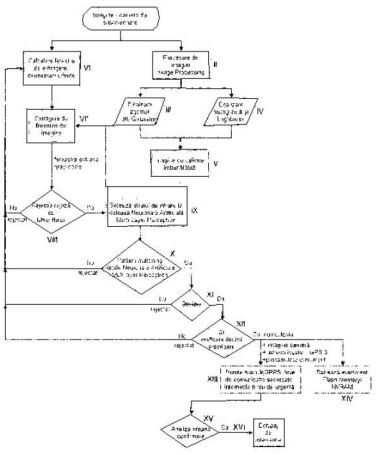


Fig. 2

Cu începere de la data publicării cererii de brevet, cererea asigură, în mod provizoriu, solicitantului, protecţia conferită potrivit dispoziţiilor art.32 din Legea nr.64/1991, cu excepţia cazurilor în care cererea de brevet de invenţie a fost respinsă, retrasă sau considerată ca fiind retrasă. Întinderea protecţiei conferite de cererea de brevet de invenţie este determinată de revendicările conţinute în cererea publicată în conformitate cu art.23 alin.(1) - (3).

RO 129752 A0

a 2014 00203
14-03-2014

DISPOZITIV ŞI METODĂ PENTRU SUPRAVEGHEREA AUTOMATĂ A UNEI LOCAŢII

Invenţia se referă la un dispozitiv şi o metodă destinate să asigure detecţia automată a unor cadre care conţin informaţii a căror prelucrare trebuie făcută într-un timp relativ scurt cu utilizare într-o incintă dintr-o bancă comercială, spaţiu comercial sau altele asemenea.

Sunt cunoscute dispozitive de supraveghere împotriva jafului într-o bancă sau în alte instituţii care au în construcţie, una sau mai multe camere de luat vederi de la care informaţiile sunt transmise, la un monitor de supraveghere.

Dezavantajele acestor dispozitive constau în aceea că imaginile înregistrate în timp real nu pot fi analizate într-un timp relativ scurt pentru a depista eventuale persoane care au participat la o infracţiune sau pentru a acţiona vre-un buton de panică.

Sunt cunoscute metode de supraveghere împotriva jafului în locaţii care constau în înregistrarea continuă a imaginilor din locaţie şi transmiterea informaţiilor la un birou de monitorizare în care o persoană analizează vizual calitatea înregistrării şi verifică persoanele existente în succesiunea de imagini pentru a constanta jaful. Dezavantajele acestor metode constau în aceea că nu este posibilă analiza automată a camerelor de supraveghere direct în locaţie fiind necesară analiza imaginilor de către persoanele angajate care să constate jaful, iar alertarea unei infracţiuni nedetectate de sistemul de supraveghere este făcută după producerea evenimentului de către partea vătămată.

Problema tehnică pe care o rezolvă dispozitivul şi metoda revendicate constă în depistarea, în timp real, a secvenţelor în care apar persoane fizice, ale căror chipuri sunt acoperite în cazul unor evenimente de forţare a incintelor unor bănci, spaţii comerciale sau altele asemenea.

Dispozitivul conform invenţiei elimină dezavantajele arătate mai inainte, are în componenţă o cameră de supraveghere cu calitate destul de bună, căreia i s-a înlăturat filtrul optic de bandă infraroşu şi o rezoluţie mare, care este conectată prin port de comunicaţie I^2C sau USB la un microprocesor, un sistem GPS cu protocol de conectare SiRF 3 sau NMEA, o memorie Flash/NVRAM de minimum 1 GB şi o conexiune la internet/o reţea privată securizată/GPRS, pentru a transmite alarma la un centru specializat.

Metoda conform invenţiei înlătură dezavantajele arătate mai înainte prin aceea că într-un pas I are loc o preluare de imagine de la camera 1 de supravegheat, printr-un

protocol de comunicaţie I²C de către microprocesorul 2 care în pasul al II-lea fiind procesată cu tehnici de îmbunătăţire a calităţii imaginii, după care în pasul al III-lea fiind eliminat mai întâi zgomotul alb şi cel Gaussian printr-o mediere a pixelilor vecini în prezenţa unor filtre gaussiene, în continuare în pasul al IV-lea fiind egalizate histograma şi luminozitatea permiţând ajustarea contrastului, astfel că în pasul al V-lea fiind regăsită imaginea cu calitatea îmbunătăţită de prelucrare ulterioară, această imagine fiind supusă în cadrul pasului al VI-lea unor descompuneri în subimagini de mărimi diferite luate succesiv şi unei convertiri în gray-scale, iar în pasul al VII-lea are loc extragerea ferestelor cu dimensiuni diferite din imaginea îmbunătăţită, în pasul al VIII-lea după extragerea ferestrelor fiind realizată o rejecţie rapidă cu 3 Haar-like features, care asigură cu o probabilitate relativ mare că în fereastra respectivă nu există o persoană, care are faţa acoperită, featuresurile Haar primind ca parametru sub-imaginea obţinută în pasul al VII-lea convertită în gray-scale şi în caz, în care filtrele Haar nu pot decide rejecţia fereastrei atunci, în pasul al IX-lea subimaginea fiind setată la stratul de intrare a unei Reţele Neuronale Artificiale de tip Multilayer Perceptron, care a fost antrenată să clasifice şi să recunoască persoana care are chipul acoperit mult mai bine, în pasul al X-lea fiind calculate ieşirile reţelei neuronale feedforward la datele de intrare, care constituie ferestra iar în pasul al XI-lea fiind fuzzificate ieşirile, în caz în care metoda conexionistă, adică Reţeaua Neuronală Artificială de tip Multilayer Perceptron de la pasul al X-lea, scoate un răspuns afirmativ indentificând că a recunoscut un posibil infractor, care are chipul acoperit de o mască, moment în care se revine la pasul al XII-lea unde fiind reactualizat Δt - timpul minim, care reprezintă secundele în care acest pattern anormal a fost detectat în secvenţa de imagini de interes, dacă la pasul al XII-lea Δt se constantă ca fiind suficient de mare atunci se consideră că nu a fost o întâmplare, ci că e posibil să fie un infractor, iar în cadrul pasului al XIII-lea fiind calculat un grad de confidenţă, pe care îl trimite printr-o conexiune 5 la internet/reţea privată securizată/ GPRS împreună cu un mesaj de alarmă, care conţine cadrele suspecte de la camera de supraveghere la un birou de monitorizare al XV-lea care să analizeze şi să confirme auto-sesizarea, în acelaşi timp în cadrul pasului ak XII-lea microprocesorul 2 va face o copie de siguranţă salvând în pasul al XIV-lea datele suspecte trimise într-o memorie Flash sau NVRAM, în funcţie de gradul de importanţă în pasul al XV-lea o persoană va confirma detecţia şi va trimite un echipaj de intervenţie în cadrul pasului al XVI-lea la coordonatele GPS 3 ale locaţiei curente.

Prin aplicarea invenţiilor revendicate sunt obţinute următoarele avantaje:

- detecţia rapidă şi automată în timp real a jafurilor produse de spărgători mascaţi care îşi acoperă chipul;

- o singură persoană poate monitoriza una, doua sau mai multe(zeci-sute) de locaţii deoarece dispozitivul revendicat în această invenţie trimite la analiza manuală numai imaginile suspecte care au fost procesate cu Inteligenţă Artificială şi s-a recunoscut ceva anormal în imaginile de la camerele de supravegheat considerând că este posibil să fie un infractor cu mască ce produce o infracţiune;

- dispozitivul odată implement, poate fi montat şi folosit de către oricine;

- se poate integra foarte uşor în reţelele actuale de supraveghere, instalarea dispozitivului nu necesită modificări esenţiale, dar maximizează rezultatele;

- maximizează rezultatele în special cu reţelele cu foarte multe puncte de supraveghere;

- reduce personalul de securitate.

Se dă în continuare câte un exemplu de realizare a dispozitivului şi respectiva metodei, conform invenţiei, în legătură cu figura 1 şi 2 care reprezenintă.

- fig. 1, schema bloc a dispozitivul invenţiei conform invenţiei;

- fig. 2, schema bloc a metodei conform invenţiei.

Dispozitivul, conform invenţiei are în componenţă o cameră 1 de supraveghere care faţă de una uzuală nu conţine un filtru de bandă infraroşu pentru o înregistrare fidelă a imaginii în vederea recunoaşterii componetelor spectrale a imaginii, camera 1, de preferinţă trebuie să aibe caracteristici anume: o rezoluţie de minimum 1280x720 şi să se conecteze prin I^2C sau USB la un microprocesor 2 cu o frecvenţă de minimum 1 GHz, un sistem GPS 3 cu protocol de conectare NMEA/SiRF 3, o memorie 4 Flash/ NVRAM de minimum 1 GB şi o conexiune 5 la internet/o reţea privată securizată/GPRS, pentru a transmite o alarmă la un centru de confirmare. Metoda, conform invenţiei constă în aceea că la pasul I are loc o preluare de imagine de la camera 1 de supravegheat, printr-un protocol de comunicaţie I^2C de către microprocesorul 2 care în pasul al II-lea este procesată cu tehnici de îmbunătăţire a calităţii imaginii. După care în pasul al III-lea este eliminat mai întâi zgomotul alb şi cel Gaussian printr-o mediere a pixelilor vecini în prezenţa unor filtre gaussiene. În continuare în pasul al IV-lea este egalizată histograma şi luminozitatea permiţând ajustarea contrastului, astfel că în pasul al V-lea este regăsită imaginea cu calitatea îmbunătăţită de prelucrare ulterioară. Această imagine este supusă în cadrul pasului al VI-lea unor descompuneri în subimagini de mărimi diferite luate succesiv şi unei convertiri în gray-scale, iar în pasul al VII-lea are loc extragerea ferestelor cu dimensiuni diferite din imaginea îmbunătăţită.

În pasul al VIII-lea după extragerea ferestrelor este realizată o rejecţie rapidă cu 3 Haar-like features care asigură cu o probabilitate relativ mare că în fereastra respectivă nu există o persoană, care are faţa acoperită, featuresurile Haar primind ca parametru sub-imaginea obţinută în pasul al VII-lea convertită în gray-scale şi în caz, în care filtrele Haar nu pot decide rejecţia fereastrei atunci, în pasul al IX-lea subimaginea este setată la stratul de intrare a unei Reţele Neuronale Artificiale de tip Multilayer Perceptron, care a fost antrenată să clasifice şi să recunoască persoana care are chipul acoperit mult mai bine. În pasul al X-lea se vor calcula ieşirile reţelei neuronale feedforward la datele de intrare, care constituie ferestra iar în pasul al XI-lea sunt fuzzificate ieşirile. În caz în care metoda conexionistă, adică Reţeaua Neuronală Artificială de tip Multilayer Perceptron de la pasul al X-lea, scoate un răspuns afirmativ indentificând că a recunoscut un posibil infractor, care are chipul acoperit de o mască, moment în care se revine la pasul al XII-lea unde este reactualizat Δt - timpul minim, care reprezintă secundele în care acest pattern anormal a fost detectat în secvenţa de imagini de interes. Dacă la pasul al XII-lea Δt este suficient de mare, atunci se consideră că nu a fost o întâmplare, ci că e posibil să fie un infractor, atunci este calculat în cadrul pasului al XIII-lea un grad de confidenţă, pe care îl trimite printr-o conexiune la internet/o reţea privată securizată/GPRS împreună cu un mesaj de alarmă, care conţine cadrele suspecte de la camera de supraveghere la un birou de monitorizare care să analizeze şi să confirme auto-sesizarea. În acelaşi timp în cadrul pasului al XII-lea microprocesorul 2 va face o copie de siguranţă salvând în pasul al XIV-lea datele suspecte trimise într-o memorie Flash sau NVRAM. În funcţie de gradul de importanţă în pasul al XV-lea o persoană va confirma detecţia şi va trimite un echipaj de intervenţie în cadrul pasului al XVI-lea la coordonatele GPS 3 ale locaţiei curente. Gradele de confidenţă calculate în pasul al XII-lea sunt sortate electronic şi este determinat gradul de importanţă în funcţie de care o persoană umană decide intervenţie în pasul al XVI-lea.

În cadrul pasului al XII-lea are loc şi o monitorizare privind o viitoare probabilă poziţie a persoanei(lor) care are(au) chipul acoperit urmărite astfel încât decizile luate pe baza informaţiilor date de către imaginile luate de la camera 1 să aibe în cadru aceasta(e) persoană(e) pentru a creşte gradul de confidenţialitate în vederea recunoaşterii persoanei(lor) şi a traseul(elor) acesteia/acestora.

Prin aplicarea dispozitivului şi metodei conform invenţiilor s-au făcut teste într-o incintă în care au apărut instantaneu 1 sau 2 persoane purtând cagulă de diferite modele, mărimi şi culori - negru şi albastru deschis. În urma testelor făcute cu ajutorul

camerei 1 de supraveghere utilizată de microprocesorul 2 şi aplicând succesiunea de paşi ai metodei, într-un timp relativ scurt de 4 secunde au fost puse în evidenţă secvenţele de imagini începând cu primele cadre care ar genera un eveniment permanent sigur. Aceste informaţii au fost transmise în vederea confirmării la un calculator unde o persoană umană pe baza lor poate lua o decizie.

În cazul unei bănci aceste informaţii preluate de dispozitiv reprezintă alarma semnalată de apariţia unui eveniment legat de existenţa în imagini a unei persoane cu cagulă fiind trimisă la un centru, unde o persoană va analiza alarma şi va decide dacă va trimite un echipaj de intervenţie pentru soluţionarea incidentului. Timpul minim de detecţie a unei persoane ce are chipul acoperit este de aproximativ 0.13 secunde. Detecţia de minim 40 de cadre într-un interval Δt de 4 secunde va consta în generarea unui eveniment. Selecţia unui interval Δt mai mare va spori gradul de confidenţă al evenimentului.

a-2014-00203--
14-03-2014

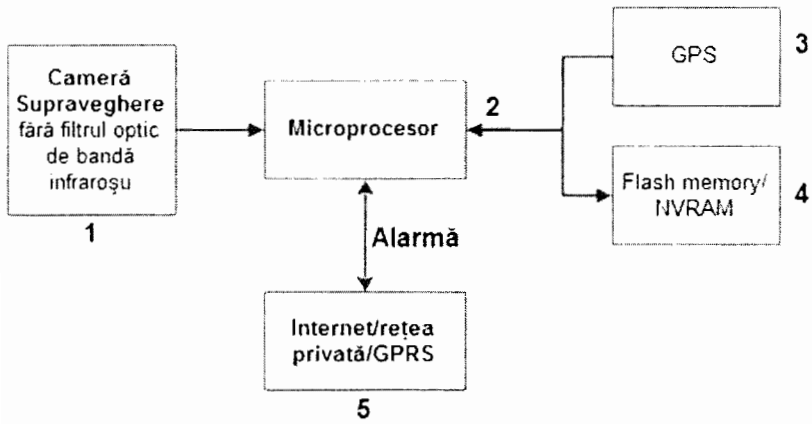
REVENDICĂRI

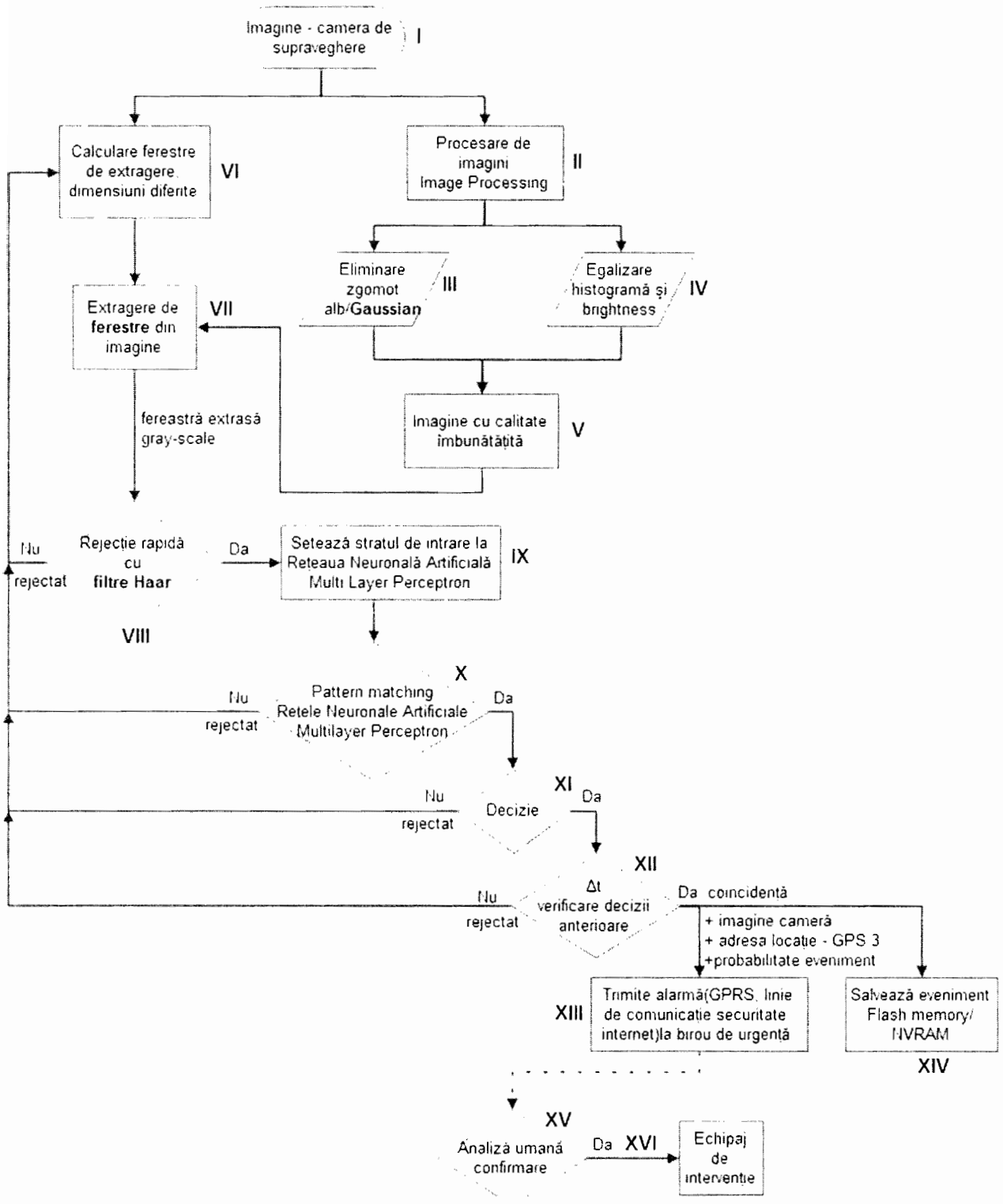
1. Dispozitiv pentru supravegherea automată a unei locaţii, conform invenţiei, **caracterizată prin aceea că** are în componenţă o cameră (1) de supraveghere cu calitate destul de bună, căreia i s-a înlăturat filtrul optic de bandă infraroşu şi o rezoluţie mare, care este conectată prin portul de comunicaţie I²C sau USB la un microprocesor (2), un sistem GPS (3) cu protocol de conectare SiRF 3 sau NMEA, o memorie (4) Flash/NVRAM de minimum 1 GB şi o conexiune (5) la internet/o reţea privată securizată/GPRS, pentru a transmite alarma la un centru specializat.

2. Metodă pentru supravegherea automată a unei locaţii conform invenţiei care este aplicată în cadrul dispozitivului conform revendicării 1 **caracterizată prin aceea că** într-un pas I are loc o preluare de imagine de la camera (1) de supravegheat, printr-un protocol de comunicaţie I²C de către microprocesorul (2) care în pasul al II-lea fiind procesată cu tehnici de îmbunătăţire a calităţii imaginii, după care în pasul al III-leafiind eliminat mai întâi zgomotul alb şi cel Gaussian printr-o mediere a pixelilor vecini în prezenţa unor filtre gaussiene, în continuare în pasul al IV-lea fiind egalizate histograma şi luminozitatea permiţând ajustarea contrastului, astfel că în pasul al V-lea fiind regăsită imaginea cu calitatea îmbunătăţită de prelucrare ulterioară, această imagine fiind supusă în cadrul pasului al VI-lea unor descompuneri în subimagini de mărimi diferite luate succesiv şi unei convertiri în gray-scale, iar în pasul al VII-lea are loc extragerea ferestelor cu dimensiuni diferite din imaginea îmbunătăţită, în pasul al VIII-lea după extragerea ferestrelor fiind realizată o rejecţie rapidă cu 3 Haar-like features care asigură cu o probabilitate relativ mare că în fereastra respectivă nu există o persoană, care are faţa acoperită, featuresurile Haar primind ca parametru sub-imaginea obţinută în pasul al VII-lea convertită în gray-scale şi în caz, în care filtrele Haar nu pot decide rejecţia fereastrei atunci, în pasul al IX-lea subimaginea fiind setată la stratul de intrare a unei Reţele Neuronale Artificiale de tip Multilayer Perceptron, care a fost antrenată să clasifice şi să recunoască persoana care are chipul acoperit mult mai bine, în pasul al X-lea fiind calculate ieşirile reţelei neuronale feedforward la datele de intrare, care constituie ferestra iar în pasul al XI-lea fiind fuzzificate ieşirile, în caz în care metoda conexionistă, adică Reţeaua Neuronală Artificială de tip Multilayer Perceptron de la pasul al X-lea, scoate un răspuns afirmativ indentificând că a recunoscut un posibil infractor, care are chipul acoperit de o mască, moment în care se revine la pasul al XII-lea unde fiind reactualizat Δt - timpul minim, care reprezintă secundele în care acest pattern anormal a fost detectat în secvenţa de imagini de

interes, dacă la pasul al XII-lea Δt se constantă ca fiind suficient de mare atunci se consideră că nu a fost o întâmplare, ci că e posibil să fie un infractor, iar în cadrul pasului al XIII-lea fiind calculat un grad de confidenţă, pe care îl trimite printr-o conexiune (5) la internet/reţea privată securizată/ GPRS împreună cu un mesaj de alarmă, care conţine cadrele suspecte de la camera de supraveghere la un birou de monitorizare care să analizeze şi să confirme auto-sesizarea, în acelaşi timp în cadrul pasului al XII-lea microprocesorul (2) va face o copie de siguranţă salvând în pasul al XIV-lea datele suspecte trimise într-o memorie Flash sau NVRAM, în funcţie de gradul de importanţă în pasul al XV-lea o persoană va confirma detecţia şi va trimite un echipaj de intervenţie în cadrul pasului al XVI-lea la coordonatele GPS (3) ale locaţiei curente.

a-2014-00203--
14 -03- 2014




Imagine - camera de supraveghere
I
Calculare ferestre de extragere dimensiuni diferite
VI
Procesare de imagini Image Processing
II
Eliminare zgomot alb/Gaussian
III
Egalizare histogramă și brightness
IV
Extragere de ferestre din imagine
VII
fereastră extrasă gray-scale
Imagine cu calitate îmbunătățită
V
Nu
rejectat
Rejecție rapidă cu filtre Haar
Da
Setează stratul de intrare la Rețeaua Neuronală Artificială Multi Layer Perceptron
IX
VIII
X
Nu
rejectat
Pattern matching Retele Neuronale Artificiale Multilayer Perceptron
Da
Nu
rejectat
Decizie
XI
Da
XII
Nu
rejectat
Δt verificare decizii anterioare
Da coincidență
+ imagine cameră
+ adresa locație - GPS 3
+probabilitate eveniment
XIII
Trimite alarmă(GPRS, linie de comunicatie securitate internet)la birou de urgență
Salvează eveniment Flash memory/ NVRAM
XIV
XV
Analiză umană confirmare
Da
XVI
Echipaj de intervenție