



(12) **BREVET DE INVENȚIE**

(21) Nr. cerere: **a 2008 00559**

(22) Data de depozit: **21.07.2008**

(45) Data publicării mențiunii acordării brevetului: **28.10.2011** BOPI nr. **10/2011**

(41) Data publicării cererii:
30.06.2009 BOPI nr. **6/2009**

(73) Titular:
• **SEEKTRON S.R.L., ȘOSEAUA VESTULUI
NR.33, CAM.2, PLOIEȘTI, PH, RO**

(72) Inventatori:
• **MELINTE TOADER,
STR.ENĂCHIȚĂ VĂCĂRESCU NR.15A,
BL.121B, AP.25, PLOIEȘTI, PH, RO;**

• **PRICOP EMIL, STR.GĂRII NR.88,
SAT HOMORĂCIU, COMUNA IZVOARELE,
PH, RO;**
• **LORENTZ ADRIAN, STR.COSMINELE
NR.4, BL.120, SC.C, AP.44, PLOIEȘTI, PH,
RO;**
• **ANDRON LIVIU, STR.AUREL SUCIU
NR.32, AP.223, CLUJ-NAPOCA, CJ, RO**

(56) Documente din stadiul tehnicii:
US 2003172279 A1

(54) **CARD RFID BIOMETRIC ȘI METODĂ DE STOCARE A
INFORMAȚIILOR PE CARDUL RFID BIOMETRIC**

(57) Rezumat:

Invenția se referă la o metodă și la un sistem pentru tranzații bancare, destinat identificării unei persoane ce realizează tranzații bancare prin intermediul unui automat bancar. Metoda de identificare, conform invenției, constă din stocarea, pe un card destinat efectuării de tranzații bancare prin intermediul unui automat bancar, a unor amprente digitale și a altor date ale persoanelor autorizate să efectueze operațiuni bancare, precum și a unor informații bancare, identificarea persoanei prin citirea datelor de pe card și compararea amprente digitale de pe acesta cu amprenta digitală preluată de automatul bancar, urmată de validarea amprente și de inițierea operațiunii bancare solicitate, sau de invalidarea amprente și de semnalarea încercării de inițiere frauduloasă a unei operațiuni bancare. Sistemul pentru tranzații bancare, conform invenției, constă dintr-un echipament (EI) de înregistrare a identității, ce are în componență un cititor de amprente (CA) și un inscripător de carduri (IR), și dintr-un echipament (EV) de verificare a identității, destinat montării în componența unui automat bancar, alcătuit dintr-un cititor de amprente (CA), un cititor de carduri (CR) și un dispozitiv (DC) de comparare a datelor.

Revendicări: 2
Figuri: 6

Adresa Obiect 5	Obiect 1	Obiect 2	Obiect 3	Obiect 4	Obiect 5	Obiect 6	Obiect 7
0000				00C			000K
0010				PH			0017
0018							
0110				SA1			0117
0120							
0210				SA2			0217
0218							
0310				SA3			0317
0318				SC SA1			0317
0320				SC SA2			0327
0322				SC SA3			0327
0328				EO			0327
0330							
0338				DU			0337
0340							
0348				DB			0347
0350							
0358							0357

Fig. 1

Examinator: ing. DUMITRU DANIELA



Orice persoană are dreptul să formuleze în scris și motivat, la OSIM, o cerere de revocare a brevetului de invenție, în termen de 6 luni de la publicarea mențiunii hotărârii de acordare a acesteia

RO 123364 B1

1 Invenția denumită Card RFID biometric și metodă de stocare a informațiilor pe cardul
RFID biometric se referă la un tip inovativ de card RFID și la o metodă de stocare a informa-
3 țiilor pe acesta, cu ajutorul cărora se realizează o identificare mai sigură a persoanelor care
realizează tranzacții bancare prin intermediul ATM (Automatic Teller Machine). Metoda
5 prezentată în această propunere de invenție se poate aplica în ATM-urile care utilizează
principiile de autentificare aflate în uz, bazate pe bandă magnetică și/sau smartcard. Utili-
7 zarea cardului RFID biometric nu este însă limitată la domeniul bancar.

 Majoritatea automatelor bancare din lume utilizează la ora actuală autentificarea
9 bazată pe PIN (Personal Identification Number) în corespondență cu informațiile de auten-
tificare stocate de cele mai multe ori pe bandă magnetică sau smartcard, deci se bazează
11 pe cunoștințe ale utilizatorului. Acestea pot fi divulgate sau aflate prin diverse metode, repre-
zentând astfel o mare vulnerabilitate în securitatea sistemului. Pentru a crește siguranța
13 sistemelor actuale, în prezenta invenție propunem utilizarea amprentelor digitale pentru iden-
tificarea utilizatorilor, măbind astfel gradul de securitate al tranzacției.

15 Dintre metodele biometrice de identificare a persoanei, metoda bazată pe analiza am-
prentelor digitale are cea mai bogată istorie. Amprenta digitală poate fi reprezentată printr-o
17 largă varietate de particularități utilizate în detecția punctelor caracteristice: geografia striațiu-
nilor și muchiilor, frecvența acestora, locația și poziția punctelor singulare, mijlocul amprenteii,
19 zone triunghiulare (delta), tipul, direcția și locația punctelor specifice (minutiae), numărul de
striații dintre două puncte caracteristice, locația porilor. Toate caracteristicile anterioare
21 contribuie la ceea ce numim unicitatea amprenteii; s-a constatat că nu există două persoane
care să aibă aceeași amprentă digitală. Pe lângă unicitate, amprenta digitală prezintă și alte
23 caracteristici care o impun ca factor de identificare biometrică: universalitate - orice persoană
normală posedă această caracteristică; permanență - amprentele nu se modifică într-o
25 perioadă mare de timp; colectabilitate - amprentele pot fi cuantificate cu ajutorul unui senzor.

 Algoritmii de analiză a amprenteii se bazează pe procesarea imaginii achiziționate de
27 senzor și au ca rezultat un fișier cu dimensiunea de 256 octeți, care conține codificat puncte-
le caracteristice. Fișierul obținut este stocat într-o bază de date și apoi utilizat într-un algoritm
29 de comparare pentru identificarea utilizatorului. Structura șablonului obținut este, de cele mai
multe ori, proprietară, fiind patentată de autorii algoritmului de analiză.

31 În ultimii ani, în lume sunt semnalate încercări de realizare a unor automate bancare
biometrice, care realizează identificarea utilizatorului pe baza amprenteii digitale. Aceasta
33 este stocată pe serverul băncii. Deși metoda pare sigură și modernă, ea suferă de o mare
vulnerabilitate, și anume aceea că este necesară existența bazelor de date cu amprentele
35 utilizatorilor în diverse locații, lucru care este inacceptabil din punct de vedere al securității
și intimității persoanelor. Modelul existent funcționează pe principiul vehiculării șablonului
37 ampreentei de la ATM la bancă, ceea ce face ca metoda să fie vulnerabilă, existând
posibilitatea interceptării comunicației.

39 De exemplu, cererea de brevet **US 2003172279** (Yudasaka Ichio, 2003) se referă la
un card RFID, a cărui memorie este inscripționată cu diverse informații referitoare la posesor,
41 compania la care posesorul lucrează și alte organisme, care pot fi alertate în legătură cu
posesorul cardului. Tipurile de informații incluse în memoria cardului sunt: o zonă cuprinde
43 informații personale ale posesorului de card, care include parola, amprenta digitală, numele,
data nașterii, adresa, numărul de telefon, contul din bancă, ș.a.; o altă zonă este rezervată
45 companiei și cuprinde codul acesteia, numele, departamentul, codul corporației, numărul de
identificare, numărul de cont, ș.a.; o altă zonă în care se înscriu date bancare referitoare la
47 posesor, date ale oficiilor municipale, ale permisului de conducere, ale unor unități sanitare.

RO 123364 B1

Se precizează că se pot înregistra și amprentele altor utilizatori. Se arată, de asemenea, că
întâi se înregistrează datele purtătorului de card, după care, cardul este dus la bancă și se
fac celelalte înregistrări. 1 3

Un automat bancar care implementează metoda propusă în prezenta invenție
realizează securizarea operațiunilor bancare, fără să vehiculeze amprenta digitală în
sistemul de comunicație între automat și bancă, autentificarea realizându-se după modelul
descries în continuare. Într-un card RFID sunt introduse amprente digitale ale persoanelor
care sunt autorizate să efectueze operațiuni cu acest card. Numărul amprentelor digitale
depinde de capacitatea cardului RFID. În prezenta invenție se propune realizarea unui card
RFID MIFARE cu memorie de 1 KB, care va stoca trei amprente. 5 7 9

Metoda propusă în această invenție are la bază realizarea unui card RFID biometric,
având un mod unic și inovativ de memorare a informațiilor. Modul de stocare al datelor este
prezentat în fig. 1. Cardul biometric este emis de bancă sau altă instituție financiară. Atunci
când utilizatorul solicită emiterea cardului, la unitatea emitentă cu un echipament special se
citesc amprentele acestuia. După procesarea automată a imaginii și obținerea șablonului,
acesta se înscrie în cardul biometric, ce va fi înmănat utilizatorului. Pe card alături de
amprente se stochează și alte date așa cum este descris în continuare. Posesorul cardului,
în momentul în care dorește să execute o operațiune bancară, apropie cardul de automatul
bancar cu card RFID. Prin citirea prin radiofrecvență (fără contact) a informațiilor de pe card,
se solicită introducerea amprente digitale fizice a persoanei, operațiune urmată de
compararea celor două informații biometrice, cea stocată pe card și cea obținută în timp real.
Dacă această comparare este validă, atunci se inițiază procesul de operațiune bancară dorit
de utilizator. Datele necesare identificării nu sunt stocate în memoria unui dispozitiv situat
în automat sau la sediul unității emitente, ci doar pe cardul aflat la utilizator. Chiar dacă acest
card este însușit de terțe persoane, el nu poate fi utilizat întrucât nu va putea compara
amprenta reală cu cea de pe card, acestea aparținând la două persoane diferite. Mai mult
decât atât, procesul de încercare a inițierii unei operațiuni bancare în mod fraudulos este
depistat și semnalat în consecință. 11 13 15 17 19 21 23 25 27

Cardul prezentat în această invenție conține și elementele de securitate existente în
prezent: bandă magnetică sau circuit integrat de tip smartcard, putând fi utilizat în sistemele
existente. Aparatul și metoda propuse în această invenție nu au ca scop înlocuirea
ATM-urilor existente, ci sporirea securității tranzacțiilor bancare prin adăugarea de elemente
suplimentare de verificare a identității sistemelor aflate în exploatare. 29 31 33

Cardurile RFID utilizate la realizarea invenției sunt pasive, adică se alimentează din
câmpul magnetic generat de cititor, și au o memorie de tip write-once read-many, care se
înscrie o singură dată la emiterea cardului și se poate citi ori de câte ori este nevoie. În
invenția prezentată se utilizează comunicația full duplex la care alimentarea cardului RFID
se realizează pe toată durata comunicației, iar datele sunt transmise simultan de ambele
entități implicate, card și cititor. 35 37 39

Descrierea exemplului de realizare a invenției se face prin referire la fig. 1...6, care
reprezintă: 41

- fig. 1, structura memoriei cardului; 43
- fig. 2, structura din memoria cardului care conține datele utilizatorului; 43
- fig. 3, structura din memoria cardului care conține datele de identificare ale băncii; 45
- fig. 4, schema bloc a automatului biometric; 45
- fig. 5, schema bloc a echipamentului de înregistrare a identității; 47
- fig. 6, schema bloc a echipamentului de verificare a identității. 47

RO 123364 B1

1 În cadrul acestei invenții, propunem următoarea structură pentru memoria cardului
RFID care se utilizează în automatul biometric, așa cum s-a arătat din fig. 1. Din punct de
3 vedere constructiv, memoria conține 128 blocuri a câte 8 octeți fiecare, obținându-se astfel
o capacitate de 1 KB. Fiecare octet este adresabil, plaja de adrese începând cu 0000H până
5 la 03FFH. Pentru această invenție, se definesc următoarele câmpuri:

7 - IDC - identificator card - dimensiunea de 16 octeți, adresa de început 0000H, adresa
ultimului octet 000FH;

9 - PIN - stochează un PIN criptat - dimensiunea maximă 8 octeți, adresa de început
0010H, adresa ultimului octet 0017H;

11 - SA1, SA2, SA3 - șabloanele amprentelor digitale, având fiecare dimensiunea de
256 octeți. SA1 începe de la adresa 0018H, ultimul octet are adresa 0117H. SA2 se înscrie
de la adresa 0118H la adresa 0217H, iar SA3 de la 0218H la 0317H;

13 - SC_SA1, SC_SA2, SC_SA3 - sume de control pentru șabloanele amprentelor.
Fiecare sumă de control ocupă 8 octeți, de la 0318H la 031FH pentru SC_SA1, suma de
15 control corespunzătoare SA1, de la 0320H la 0327H pentru SC_SA2, respectiv de la 0328H
la 032FH pentru SC_SA3;

17 - CO - codurile operațiilor permise, începând cu adresa 0330H până la 0337H. Fiecare
operație este codificată pe 1 octet;

19 - DU - datele de identificare ale utilizatorului, adresa de început 0338H, adresa de
final 03B7, având rezervat un spațiu de memorie de 128 octeți;

21 - DB - datele de identificare specifice băncii, adresa de început 03B8H, adresa de
final 03FFH, având rezervat spațiu de memorie de 72 octeți.

23 Codurile operațiilor permise sunt stocate în zona CO. Aceste operații sunt codificate
pe 8 biți (1 octet), deci este posibilă declararea a maximum 8 operații. Completarea zonei
25 CO începe cu octetul aflat la adresa 0330H. Biții aflați în componența octeților neutilizați au
valoarea 0.

27 Structura zonei DU care conține datele utilizatorului este redată în fig. 2. Zona de
memorie conține datele personale ale utilizatorului, astfel:

29 - NC - memorează în clar numele utilizatorului, adresa de început pentru câmp este
0338H, iar adresa de final 034BH, dimensiunea câmpului fiind de 20 de octeți;

31 - NP - memorează în clar prenumele utilizatorului, de la adresa 034CH la 035FH;
- CNP - codul numeric personal ocupă 16 octeți, deoarece se memorează criptat șirul
33 unic de 13 caractere de tip numeric. Intervalul de adrese alocat pentru CNP este
0360H-036FH;

35 - IAC - informații auxiliare despre utilizator (tipul de client, informații de fidelitate) se
stochează în spațiul de memorie de la 0370H la 0380H.

37 Structura zonei DB este prezentată în fig. 3. Zona de memorie cuprinde date de
identificare specifice unităților bancare. Se definesc următoarele câmpuri:

39 - NB - nume bancă, cu dimensiunea de 16 octeți, de la adresa 0388H la 03C7H;

- NC - număr card, dimensiunea de 16 octeți, memorat de la 03C8H la 03D7H;

41 - DE - data emiterii cardului, stocată în format ZZ-LL-AAAA, pe 8 biți, de la 03D8H
la 03DFH;

43 - DV - data expirării cardului, stocată în format ZZ-LL-AAAA, pe 8 biți, de la 03E0H
la 03E7H;

45 - UE - denumirea unității emitente a cardului (de obicei agenția la care clientul are
domicilierea contului). Dimensiunea maximă este de 16 octeți, de la 03E8H la 03F8H;

47 - TC - tipul de card (credit, debit, co-branded, fidelizare) codificat pe 8 octeți de la
03F7H la 03FFH.

RO 123364 B1

Cardul RFID biometric, ce poate fi utilizat pentru autentificarea utilizatorului la un automat biometric destinat tranzacțiilor bancare, este caracterizat prin aceea că are capacitatea de memorie de 1 kB, organizată în 128 de blocuri a câte 8 octeți fiecare, având o zonă de 16 octeți pentru identificarea cardului, o zonă de 8 octeți pentru stocarea unui PIN criptat, trei zone a câte 256 octeți destinate stocării șabloanelor amprentelor digitale, urmate de trei zone a câte 8 octeți fiecare, ce memorează sumele de control corespunzătoare, o zonă de memorie ce conține codurile operațiilor permise, o zonă de 128 de octeți, ce stochează datele utilizatorului, constând din nume, prenume, cod numeric personal, tip de client și o zonă de 72 octeți, ce memorează date specifice băncii, constând din numele acesteia, numărul cardului, data emiterii și expirării acestuia, unitatea emitentă și tipul cardului.

Metoda de înregistrare a informațiilor pe card RFID biometric, care face obiectul acestei invenții, este implementată în cardul echipamentului de înregistrare a identității (EI). Această metodă este caracterizată de următoarele etape:

- înregistrarea datelor utilizatorului în zonele de memorie ale cardului specificate anterior;
- solicitarea și citirea a trei amprente digitale, procesarea acestora și generarea șabloanelor numerice;
- calculul sumelor de control corespunzătoare fiecărei amprente digitale citite la pasul anterior;
- înscrierea datelor biometrice și a sumelor de control în zonele corespunzătoare din memoria cardului RFID;
- solicitarea și înscrierea informațiilor despre bancă (unitate emitentă a cardului), în zonele predefinite ale memoriei acestuia.

În continuare, se prezintă un model de realizare a automatului biometric cu card RFID pentru tranzacții bancare, în conformitate cu metoda prezentată anterior. Automatul biometric, care are schema bloc din fig. 4, este compus din două echipamente: echipament de înregistrare EI și echipament de verificare EV a identității.

Echipamentul de înregistrare a identității EI, cu schema bloc redată în fig. 5, are în componență următoarele elemente:

- cititor de amprente (CA);
- inscriptor de carduri RFID (IR).

Echipamentul de înregistrare a identității se montează la sediul băncii emitente a cardului. Cu ajutorul EI se înscriu pe card șabloanele amprentelor digitale și celelalte informații necesare, așa cum s-a specificat anterior în prezentarea structurii memoriei. Metoda prezentată în această invenție înregistrează pentru fiecare utilizator trei amprente digitale. Două dintre acestea vor fi utilizate pentru desfășurarea de operațiuni bancare prin intermediul automatului bancar, iar cea de-a treia va fi utilizată ca element de siguranță, atunci când utilizatorul este forțat să se autentifice și să permită accesul la contul său. Folosind această amprentă vor fi permise tranzacții și se va genera un eveniment de securitate.

Echipamentul de verificare a identității EV are schema bloc din fig. 6. Acesta este compus din următoarele elemente:

- cititor de amprente (CA);
- cititor de carduri RFID (CR);
- dispozitiv de comparare statistică a datelor (DC).

Echipamentul de verificare a identității se adaugă ATM-urilor existente în rețeaua băncii, fără a modifica funcționarea sau modul de utilizare al acestora. Posesorul cardului, în momentul în care dorește să execute o operațiune bancară, apropie cardul de ATM și implicit de cititorul

RO 123364 B1

1 de carduri RFID **CR**. Prin citirea prin radiofrecvență (fără contact) a informațiilor de pe card,
se solicită introducerea amprentei digitale fizice a persoanei, operațiune urmată de
3 compararea celor două informații biometrice: cea stocată pe card și cea obținută în timp real.
Dacă această comparare este validă, atunci se inițiază procesul de operațiune bancară dorit
5 de utilizator. Echipamentul și metoda propuse sunt redundante din punct de vedere al
securității, deoarece este posibilă solicitarea a două sau mai multe amprente pentru
7 validarea identității utilizatorului.

Integrarea echipamentelor necesare utilizării cardului RFID biometric în ATM-urile
9 existente se realizează prin introducerea în ATM a unui echipament de verificare a identității
EV și actualizarea componentelor software și structurilor de date specifice ATM-ului.
11 Programele utilizate în cadrul automatului bancar sunt particularizate în funcție de tipul
elementelor componente **CA, DC, CR, IR**.

RO 123364 B1

Revendicări

- | | |
|---|----------------------------|
| | 1 |
| 1. Card RFID biometric, ce poate fi utilizat pentru autentificarea utilizatorului la un automat biometric destinat tranzacțiilor bancare, caracterizat prin aceea că are capacitatea de memorie de 1 kB, organizată în 128 de blocuri a câte 8 octeți fiecare, având o zonă de 16 octeți pentru identificarea cardului, o zonă de 8 octeți pentru stocarea unui PIN criptat, trei zone a câte 256 octeți destinate stocării șabloanelor amprentelor digitale, urmate de trei zone a câte 8 octeți fiecare, ce memorează sumele de control corespunzătoare, o zonă de memorie ce conține codurile operațiunilor permise, o zonă de 128 de octeți, ce stochează datele utilizatorului, constând din nume, prenume, cod numeric personal, tip de client și o zonă de 72 octeți, ce memorează date specifice băncii, constând din numele acesteia, numărul cardului, data emiterii și expirării acestuia, unitatea emitentă și tipul cardului. | 3
5
7
9
11 |
| 2. Metodă de stocare a informațiilor pe cardul RFID biometric, conform revendicării 1, pentru autentificarea utilizatorului la un automat biometric destinat tranzacțiilor bancare, caracterizată prin aceea că , într-o primă etapă se execută înregistrarea datelor utilizatorului în zonele specifice de memorie ale cardului, urmată de o etapă de citire a trei amprente digitale și de generare a șabloanelor acestora, după care, într-o a treia etapă se face calculul sumelor de control ale șabloanelor generate, într-o a patra etapă are loc înscrierea tuturor datelor biometrice și a sumelor de control în zonele corespunzătoare de memorie, urmată de o ultimă etapă de înscriere a informațiilor despre bancă, în zonele predefinite din memoria cardului. | 13
15
17
19
21 |

RO 123364 B1

(51) Int.Cl.
G06K 19/14 (2006.01);
G07F 7/08 (2006.01);
G07F 19/00 (2006.01)

Adresa Octet 0	Octet 0	Octet 1	Octet 2	Octet 3	Octet 4	Octet 5	Octet 6	Octet 7
0000				IDC				
0008								000F
0010				PIN				0017
0018								
				SA1				
0110								0117
0118								
				SA2				
0210								0217
0218								
				SA3				
0310								0317
0318				SC_SA1				031F
0320				SC_SA2				0327
0328				SC_SA3				032F
0330				CO				0337
0338								
				DU				
03B0								03B7
03B8								
				DB				
03F8								03FF

Fig. 1

RO 123364 B1

(51) Int.Cl.

G06K 19/14 (2006.01);

G07F 7/08 (2006.01);

G07F 19/00 (2006.01)

Adresa Octet 0	Octet 0	Octet 1	Octet 2	Octet 3	Octet 4	Octet 5	Octet 6	Octet 7
0338								
0340			NC					
0348				034B	034C			
0350						PC		
0358								
0360				CNP				
0368								
0370								
0378								
0380								
0388								
0390				IAC				
0398								
03A0								
03A8								
03B0								

Fig. 2

Adresa Octet 0	Octet 0	Octet 1	Octet 2	Octet 3	Octet 4	Octet 5	Octet 6	Octet 7
03B8				NB				
03C0								
03C8				NC				
03D0								
03D8				DE				
03E0				DV				
03E8				UE				
03F0								
03F8				TC				

Fig. 3

(51) Int.Cl.
G06K 19/14 (2006.01);
G07F 7/08 (2006.01);
G07F 19/00 (2006.01)

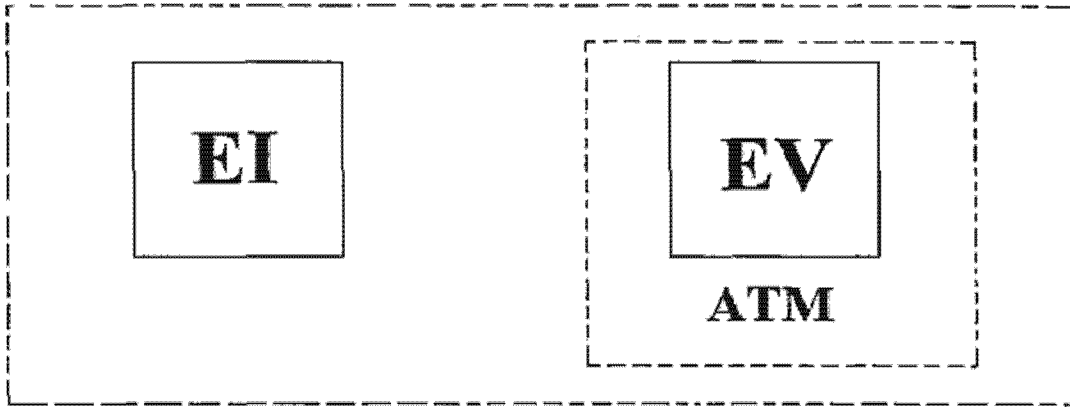


Fig. 4

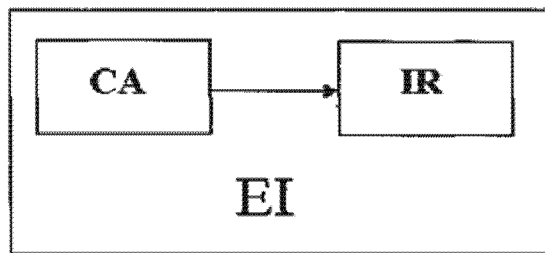


Fig. 5

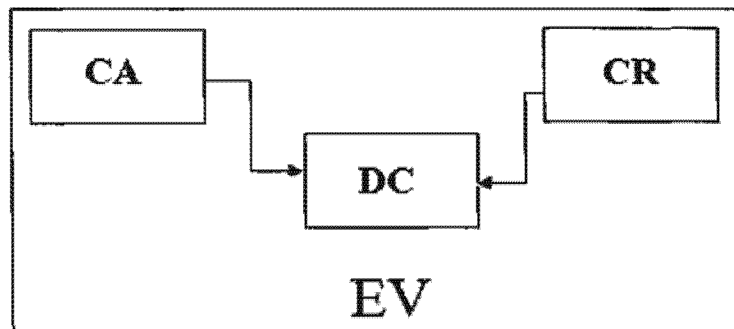


Fig. 6

