MD 4260 B1 2013.11.30

REPUBLICA MOLDOVA

(19) Agenţia de Stat pentru Proprietatea Intelectuală

(11) 4260 (13) **B1**

(51) Int.Cl: ***G06K 1/00*** (2006.01)
G06K 9/18 (2006.01)
G06K 9/20 (2006.01)
G06K 9/36 (2006.01)
G06K 9/62 (2006.01)
G06K 9/78 (2006.01)
G06K 9/80 (2006.01)
G06K 9/82 (2006.01)
G06K 19/08 (2006.01)
G06K 19/10 (2006.01)

(12) BREVET DE INVENŢIE

In termen de 6 luni de la data publicării menţiunii privind hotărârea de acordare a brevetului de invenţie, orice persoană poate face opoziţie la acordarea brevetului

(21) Nr. depozit: a 2011 0042
(22) Data depozit: 2011.05.11

(41) Data publicării cererii: 2012.11.30

(45) Data publicării hotărârii de acordare a brevetului:
2013.11.30, BOPI nr. 11/2013

(71) Solicitanţi: PUŞNEAC Iurie, MD; ŞCHILIOV Vladimir, MD; ADAMCIUC Arcadi, MD
(72) Inventatori: PUŞNEAC Iurie, MD; ŞCHILIOV Vladimir, MD; ADAMCIUC Arcadi, MD
(73) Titulari: PUŞNEAC Iurie, MD; ŞCHILIOV Vladimir, MD; ADAMCIUC Arcadi, MD

(54) Document de hartie protejat criptografic, procedeu de marcare şi procedeu de identificare a acestuia

(57) Rezumat:

Invenţia se referă la tehnologiile informaţionale şi poate fi utilizată pentru protecţia contra falsificării documentelor de hartie.

Documentul de hartie protejat criptografic conţine un marcaj de identificare, executat în formă de o imagine individuală, formată dintr-o totalitate de perforaţii, obţinute printr-un proces aleatoriu de descărcări electrice, şi un cod numeric. Documentul mai conţine un cod de bare bidimensional, care include informaţie despre imaginea individuală, codul numeric, conţinutul documentului, precum şi o semnătură digitală.

Procedeul de marcare a documentului de hârtie constă în aplicarea pe acesta a marcajului de identificare sus-menţionat, scanarea acestuia cu un dispozitiv de scanare şi procesare cu memorie, comprimarea imaginii scanate, introducerea in memoria dispozitivului de scanare şi procesare a informaţiei despre marcajul de identificare şi conţinutul documentului, semnarea informaţiei menţionate cu semnătură digitală, transformarea informaţiei semnate într-un cod de bare bidimensional, imprimarea codului de bare bidimensional obţinut pe documentul de hârtie alături de marcajul de identificare.

Procedeul de identificare a documentului de hârtie constă în citirea codului de bare bidimensional imprimat pe acesta cu ajutorul unui dispozitiv de scanare şi procesare cu memorie, deschiderea semnăturii digitale cu ajutorul cheii publice, obţinerea informaţiei comprimate despre marcajul de identificare, identificarea documentului de hartie prin confruntarea informaţiei obţinute în urma citirii codului de bare bidimensional şi imaginii scanate şi comprimate a marcajului de identificare de pe documentul de hartie.

Revendicări: 3
Figuri: 3

MD 4260 B1 2013.11.30

(54) Cryptographically secure paper document, method for marking and method for identifying it

(57) Abstract:

The invention relates to information technologies and can be used to protect paper documents from forgery.

The cryptographically secure paper document contains an identification tag, made in the form of an individual image, consisting of a plurality of perforations, randomly obtained by an electric discharge process, and a digital code. The document further contains a two-dimensional barcode, which includes information about the individual image, the digital code, the content of the document, and a digital signature.

The method for marking a paper document consists in applying on it the above identification tag, its scanning with a scanning and processing storage device, compressing the scanned image, introducing into the memory of the scanning and processing device the information about the identification tag and the content of the document, signing the said information with the digital signature, conversing the signed information into a two-dimensional barcode, imprinting the obtained two-dimensional barcode on the paper document next to the identification tag.

The method for identifying a paper document consists in reading the two-dimensional barcode imprinted on it with the help of a scanning and processing storage device, disclosing the digital signature using the public key, obtaining the compressed information about the identification tag, identifying the paper document by comparing the information obtained as a result of reading the two-dimensional barcode and the compressed scanned image on the paper document.

Claims: 3

Fig.: 3

(54) Криптографически защищенный бумажный документ, способ его маркировки и способ его идентификации

(57) Реферат:

Изобретение относится к информационным технологиям и может быть использовано для защиты бумажных документов от фальсификации.

Криптографически защищенный бумажный документ содержит идентификационную метку, выполненную в виде индивидуальной картинки, состоящей из совокупности перфораций, полученных случайным электроразрядным процессом, и цифрового кода. Документ еще содержит двухмерный штриховой код, который включает информацию об индивидуальной картинке, цифровом коде, содержании документа, а также включает цифровую подпись.

Способ маркировки бумажного документа состоит в нанесении на него вышеуказанной идентификационной метки, ее сканировании устройством сканирования и обработки с памятью, сжатии отсканированного изображения, внесении в память устройства сканирования и обработки информации об идентификационной метке и содержания документа, подписании упомянутой информации цифровой подписью, преобразовании подписанной информации в двухмерный штриховой код, печати полученного двухмерного штрихового кода на бумажном документе рядом с идентификационной меткой.

Способ идентификации бумажного документа состоит в считывании напечатанного на нем двухмерного штрихового кода с помощью устройства сканирования и обработки с памятью, открытии цифровой подписи с помощью открытого ключа, получении сжатой информации об идентификационной метке, идентификации бумажного документа путем сличения информации, полученной в результате считывания двухмерного штрихового кода и сжатого отсканированного изображения идентификационной метки с бумажного документа.

П. формулы: 3

Фиг.: 3

Descriere:

Invenţia se referă la tehnologiile informaţionale şi poate fi utilizată pentru protecţia contra falsificării documentelor de hârtie.

Este cunoscut un document protejat printr-un cod numeric [1].

Dezavantajele acestui document constau în lipsa protecţiei informaţionale a codului numeric şi uşurinţa falsificării documentului.

Mai este cunoscut un document, care conţine o imagine individuală de protecţie în formă de set de perforaţii, obţinute printr-un proces aleatoriu de descărcare electrică, şi un cod numeric. Imaginea individuală şi codul numeric sunt stocate într-o bază de date centrală [2].

Dezavantajul acestui document constă în necesitatea adresării permanente la baza de date centrală.

Este cunoscută utilizarea semnăturii digitale la protejarea documentelor electronice virtuale [3].

Dezavantajul acestui procedeu constă în imposibilitatea protecţiei documentelor de hârtie din cauza imposibilităţii aplicării semnăturii electronice pe un obiect material, şi anume pe un document de hartie.

Este cunoscut un procedeu de protecţie a documentelor fără adresare la baza de date centrală. Procedeul dat se bazează pe compararea vizuală a documentului cu imaginea holografică a acestuia [4].

Dezavantajul acestui procedeu constă în insuficienţa protecţiei.

Mai este cunoscut un procedeu de creare a documentului de hartie protejat prin aplicarea pe acesta a unei imagini individuale, obţinute printr-un proces aleatoriu de descărcări electrice, şi a unui cod numeric, scanarea şi, în caz de necesitate, introducerea acestei informaţii în baza de date [5].

De asemenea, se cunoaşte un procedeu de confirmare a autenticităţii documentului de hârtie, care include scanarea imaginii individuale de pe document şi compararea acesteia cu imaginea individuală, stocată anterior într-o bază de date [5].

Dezavantajul acestor procedee constă în insuficienţa protecţiei şi necesitatea adresării la baza de date.

Problema pe care o rezolvă invenţia constă în majorarea nivelului de protecţie a documentului de hârtie şi posibilitatea identificării documentului de hârtie fără adresarea la o bază de date.

Documentul de hartie protejat criptografic, conform invenţiei, înlătură dezavantajele menţionate mai sus prin aceea că conţine un marcaj de identificare, executat în formă de o imagine individuală, formată dintr-o totalitate de perforaţii, obţinute printr-un proces aleatoriu de descărcări electrice, şi un cod numeric. Documentul mai conţine un cod de bare bidimensional, care include informaţie despre imaginea individuală, codul numeric, conţinutul documentului, precum şi o semnătură digitală.

Procedeul de marcare a documentului de hartie, conform invenţiei, înlătură dezavantajele menţionate mai sus prin aceea că include aplicarea pe acesta a marcajului de identificare susmenţionat, scanarea acestuia cu un dispozitiv de scanare şi procesare cu memorie, comprimarea imaginii scanate, introducerea în memoria dispozitivului de scanare şi procesare a informaţiei despre marcajul de identificare şi conţinutul documentului, semnarea informaţiei menţionate cu semnătură digitală, transformarea informaţiei semnate într-un cod de bare bidimensional, imprimarea codului de bare bidimensional obţinut pe documentul de hârtie alături de marcajul de identificare.

Procedeul de identificare a documentului de hârtie, conform invenţiei, înlătură dezavantajele menţionate mai sus prin aceea că include citirea codului de bare bidimensional imprimat pe acesta cu ajutorul unui dispozitiv de scanare şi procesare cu memorie, deschiderea semnăturii digitale cu ajutorul cheii publice, obţinerea informaţiei comprimate despre marcajul de identificare, identificarea documentului de hârtie prin confruntarea informaţiei obţinute în urma citirii codului de bare bidimensional şi imaginii scanate şi comprimate a marcajului de identificare de pe documentul de hartie.

Invenţia se explică prin desenele din fig. 1-3, care reprezintă:

- fig. 1, document de hartie;
- fig. 2, schema-bloc a procedeului de marcare a documentului de hartie;
- fig. 3, schema-bloc a procedeului de identificare a documentului de hartie.

In fig. 1 este prezentat un exemplu al documentului de hartie 1, care in afară de conţinutul principal (text, imagine, semnătură, ştampilă), conţine următoarele elemente de protecţie suplimentare: 2 – o zonă pe documentul de hârtie 1, desemnată pentru marcajul de identificare; 3 – o imagine individuală, care reprezintă un set de perforaţii de dimensiuni şi configuraţii arbitrare, obţinute printr-un proces aleatoriu de descărcări electrice multiple, efectuate în zona 2 a documentului 1; 4 – un număr de identificare, care simplifică procesul de identificare a documentului 1; 5 – un cod de bare bidimensional, care include informaţie despre imaginea individuală 3, codul numeric 4, conţinutul documentului, precum şi o semnătură digitală a emitentului *(P)*, părţii, care emite (editează, publică) un document legal.

In fig. 2 sunt reprezentate următoarele elemente: 1 – documentul de hârtie, care urmează să fie protejat. Acesta poate fi orice document cu conţinut arbitrar (text, desen, foto, etc.), de exemplu, un document financiar, certificat, buletin de identitate, paşaport, etc.; 6 – un dispozitiv cu descărcări electrice de înaltă tensiune pentru aplicarea unei imagini individuale 3 pe documentul 1; 7 – documentul, care conţine imaginea individuală 3, obţinută printr-un proces aleatoriu de descărcări electrice multiple în zona 2. Imaginea individuală 3 reprezintă o totalitate de perforaţii de mărimi şi configuraţii diferite. Fiecare imagine 3, obţinută în aşa mod, este unică şi ireproductibilă, procesul de creare a acesteia fiind aleatoriu, deoarece nu poate fi controlat; 8 – un dispozitiv de scanare şi procesare cu memorie. În calitate de astfel de dispozitiv poate fi utilizat orice smartphone, calculator tabletă, asistent personal digital (PDA), produs în serie şi echipat cu o cameră digitală cu rezoluţia necesară şi un set de programe de aplicaţie pentru citirea şi prelucrarea imaginilor. De asemenea, este posibilă utilizarea unui calculator personal cu un scaner staţionar, conectat la acesta. La rândul său, dispozitivul de scanare şi procesare 8 conţine următoarele elemente: 8.1 – procedura de scanare a imaginii individuale 3, care asigură obţinerea imaginii digitalizate 8.2 a imaginii 3 şi stocarea acesteia în memoria dispozitivului 8; 8.3 – procedura de comprimare a imaginii digitalizate 8.2 iniţiale, ca rezultat al căreia ultima, posedând o anumită redundanţă informaţională, se transformă într-un cod numeric compact X 8.4. Procedura de comprimare 8.3 este realizată pentru a economisi memoria necesară pentru stocarea imaginii digitalizate în dispozitivul 8 şi accelerarea procedurilor ulterioare de prelucrare. Procedura de comprimare 8.3 se efectuează fără pierderea informaţiei despre parametrii unei imagini 3 concrete; 8.5 – procedura de semnare a codului numeric compact X 8.4 cu semnătura digitală a emitentului P. Semnătura digitală certifică autenticitatea codului numeric compact X 8.4 şi, prin urmare, autenticitatea imaginii digitalizate 8.2 iniţiale a imaginii individuale 3. Procedura de semnare cu semnătură digitală este descrisă prin următoarea expresie matematică:

$$S=DP(X),$$

unde X este codul numeric compact, a cărui autenticitate este certificată;

DP – criptarea asimetrică, efectuată cu ajutorul cheii private a emitentului P;

S – secvenţa binară 8.6, care reprezintă rezultatul criptării codului numeric compact X cu cheia privată;

8.7 – procedura de transformare a secvenţei binare 8.6, codului numeric 4 şi conţinutului documentului 1 intr-un cod de bare 9, de exemplu, intr-un QR-cod bidimensional utilizat pe scară largă. Transformarea 8.7 este utilizată pentru a asigura posibilitatea reproducerii şi citirii ulterioare a informaţiei prin mijloace convenţionale. În fig. 2 mai sunt reprezentate următoarele elemente: 9 – codul de bare, care include informaţie despre secvenţa binară 8.6, codul numeric 4 şi conţinutul documentului 1, a cărei autenticitate este certificată prin semnătura digitală a emitentului P. Codul de bare 9 este creat în dispozitivul de scanare şi procesare 8 şi este transmis la dispozitivul de imprimare 10; 10 – orice dispozitiv de imprimare produs in serie, care poate reproduce pe suportul de hartie un cod de bare 9, de exemplu, imprimanta; 11 – documentul de hârtie final, care conţine un marcaj de identificare şi un cod de bare bidimensional 5 imprimat, care confirmă autenticitatea marcajului de identificare şi a conţinutului, şi respectiv a documentului.

În fig. 3 sunt reprezentate următoarele elemente: 11 – documentul de hartie protejat, 12 – un dispozitiv de scanare şi procesare cu memorie. În calitate de astfel de dispozitiv poate fi utilizat orice smartphone, calculator tabletă, asistent personal digital (PDA), produs în serie şi echipat cu o cameră digitală cu rezoluţia necesară şi un set de programe de aplicaţie pentru citirea şi prelucrarea imaginilor. De asemenea, este posibilă utilizarea unui calculator personal cu un scaner staţionar, conectat la acesta. La rândul său, dispozitivul de scanare şi procesare 12 conţine următoarele elemente: 12.1 – procedura de scanare a imaginii individuale 3, care asigură obţinerea imaginii digitalizate 12.2 a imaginii 3 şi stocarea acesteia în memoria

dispozitivului 12; 12.3 – procedura de comprimare a imaginii digitalizate 12.2 iniţiale, ca rezultat al căreia ultima se transformă într-un cod numeric compact X^* 12.4; 12.5 – scanarea codului de bare 5 imprimat pe documentul 11; 12.6 – codul de bare 9, care include informaţie despre secvenţa binară 8.6, codul numeric 4 şi conţinutul documentului 1; 12.7 – procedura de decodificare a codului de bare 9, care asigură obţinerea secvenţei binare S 12.8, care reprezintă rezultatul criptării codului numeric compact X cu cheia privată a emitentului P; 12.9 – procedura de verificare a semnăturii digitale, descrisă prin următoarea expresie matematică:

$X= EP (S)$,

unde X este codul numeric compact 12.10;

EP – decriptarea asimetrică, realizată cu ajutorul cheii publice, transmise părţii verificatoare V de către emitent P;

S – secvenţa binară 12.8, care reprezintă rezultatul criptării codului numeric compact X cu cheia privată;

12.11 – confruntarea bit cu bit a codului numeric compact X^*, obţinut în urma scanării şi procesării imaginii individuale 3 de pe documentul 11, şi codului numeric compact X, semnat cu semnătura digitală de către emitentul P şi obţinut în urma citirii codului de bare 5, imprimat pe documentul 11; 13 – decizia cu privire la autenticitatea documentului, care reprezintă un mesaj, format de dispozitivul 12. Dacă codurile X^* şi X coincid până la bit, atunci documentul este considerat autentic.

Procedeul de marcare a documentului de hârtie se efectuează de către emitentul P, care doreşte să protejeze documentul de ieşire contra redactării sau modificării ulterioare neautorizate posibile.

La etapa iniţială, în zona 2 a documentului de hârtie 1, care este supus protecţiei, se aplică marcajul de identificare prin imprimarea codului numeric 4 şi executarea imaginii individuale 3 în formă de perforaţii, obţinute prin intermediul dispozitivului cu descărcări electrice 6 de înaltă tensiune. Marcajul de identificare este scanat 8.1, imaginea scanată 8.2 fiind comprimată 8.3, semnată 8.5 cu semnătură digitală împreună cu conţinutul documentului 1 de către dispozitivul de scanare şi procesare 8. Secvenţa binară S 8.6, care reprezintă rezultatul criptării codului numeric compact X cu cheia privată, se transformă 8.7 într-un cod de bare bidimensional 9, care include informaţie despre secvenţa binară 8.6, codul numeric 4 şi conţinutul documentului 1, a cărei autenticitate este certificată prin semnătura digitală a emitentului P. Codul de bare 9 se transmite la dispozitivul de imprimare 10 şi se imprimă pe documentul de hartie.

Ca rezultat, se creează documentul 11, care în afară de conţinutul principal (text, desen, foto), conţine elemente de protecţie suplimentare: marcaj de identificare, executat în formă de imagine individuală 3, formată dintr-o totalitate de perforaţii, şi codul numeric 4, şi codul de bare 5 imprimat, care atestă autenticitatea imaginii individuale 3 şi marcajului de identificare al acestui document 11.

Procedeul de identificare a documentului protejat criptografic se efectuează de către verificatorul V.

La etapa iniţială verificatorul V primeşte un document de hârtie 11 având în afară de conţinutul principal un marcaj de identificare, care constă din imaginea individuală 3 şi codul numeric 4, şi un cod de bare bidimensional 5.

Verificatorul V scanează 12.1 marcajul de identificare cu dispozitivul de scanare şi procesare 12. Imaginea digitalizată 12.2 obţinută este comprimată 12.3, ca rezultat ultima se transformă într-un cod numeric compact X^* 12.4, care este stocat in memoria dispozitivului de scanare şi procesare 12.

Ulterior, cu ajutorul dispozitivului 12, verificatorul V scanează 12.5 şi decodifică 12.7 codul de bare 5 de pe documentul 11, ca rezultat se obţine secvenţa binară S 12.8, care reprezintă rezultatul criptării codului numeric compact X cu cheia privată a emitentului P. Secvenţa binară S 12.8 se decriptează 12.9 cu cheia publică. Drept rezultat, cu ajutorul dispozitivului 12 se decriptează şi se stochează în memorie codul numeric compact X, autenticitatea căruia a fost anterior certificată de către emitentul P.

Codurile X^* şi X se compară bit cu bit. Dacă acestea coincid, atunci documentul se consideră autentic şi se adoptă decizia cu privire la autenticitatea documentului 13.

(56) Referinţe bibliografice citate in descriere:

1. RU 2286886 C2 2006.11.10
2. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. Москва, Триумф, 2002, 816 p.
3. MD 4051 C1 2010.06.30
4. RU 2399496 C2 2010.09.20
5. MD 4060 C1 2010.07.31

(57) Revendicări:

1. Document de hârtie protejat criptografic, care conţine un marcaj de identificare, executat în formă de o imagine individuală, formată dintr-o totalitate de perforaţii, obţinute printr-un proces aleatoriu de descărcări electrice, şi un cod numeric; un cod de bare bidimensional, care include informaţie despre imaginea individuală, codul numeric, conţinutul documentului, precum şi o semnătură digitală.

2. Procedeu de marcare a documentului de hârtie, definit în revendicarea 1, care constă în aplicarea pe documentul de hartie a unui marcaj de identificare prin imprimarea codului numeric şi prin executarea imaginii individuale în formă de perforaţii, obţinute prin descărcări electrice aleatorii; scanarea marcajului de identificare cu un dispozitiv de scanare şi procesare cu memorie; comprimarea imaginii scanate; introducerea in memoria dispozitivului de scanare şi procesare a informaţiei despre marcajul de identificare şi conţinutul documentului; semnarea informaţiei menţionate cu semnătură digitală; transformarea informaţiei semnate într-un cod de bare bidimensional; imprimarea codului de bare bidimensional obţinut pe documentul de hârtie alături de marcajul de identificare.

3. Procedeu de identificare a documentului de hartie, definit in revendicarea 1, care constă in citirea codului de bare bidimensional imprimat pe documentul de hartie, conform revendicării 2, cu ajutorul unui dispozitiv de scanare şi procesare cu memorie; deschiderea semnăturii digitale cu ajutorul cheii publice; obţinerea informaţiei comprimate despre marcajul de identificare; identificarea documentului de hârtie prin confruntarea informaţiei obţinute în urma citirii codului de bare bidimensional şi imaginii scanate şi comprimate a marcajului de identificare de pe documentul de hartie.

Şef secţie: SĂU Tatiana

Examinator: CERNEI Tatiana

Redactor: CANŢER Svetlana


ПРОТОКОЛ СОГЛАШЕНИЯ
246584265
4
3
2
5
1

Fig. 1

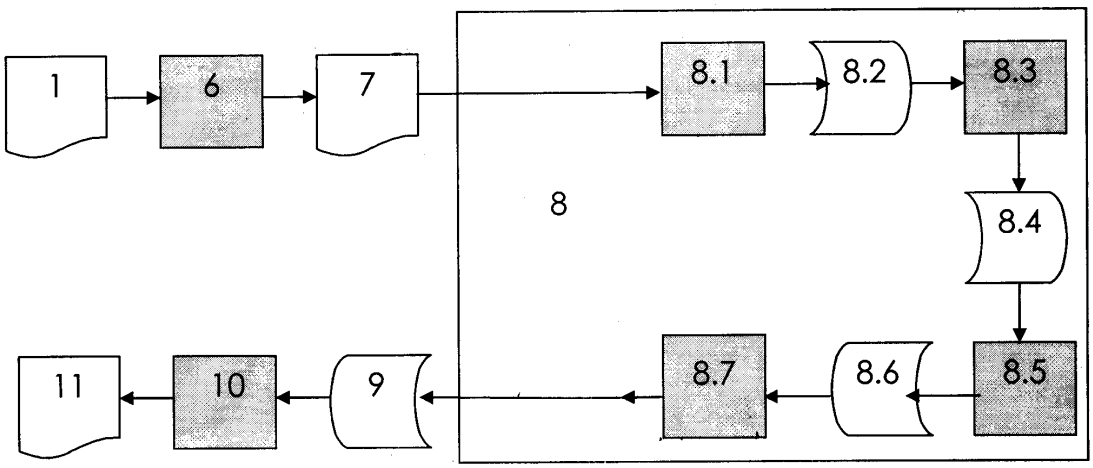
1
6
7
8
8.1
8.2
8.3
8.4
8.5
8.6
8.7
9
10
11

Fig. 2

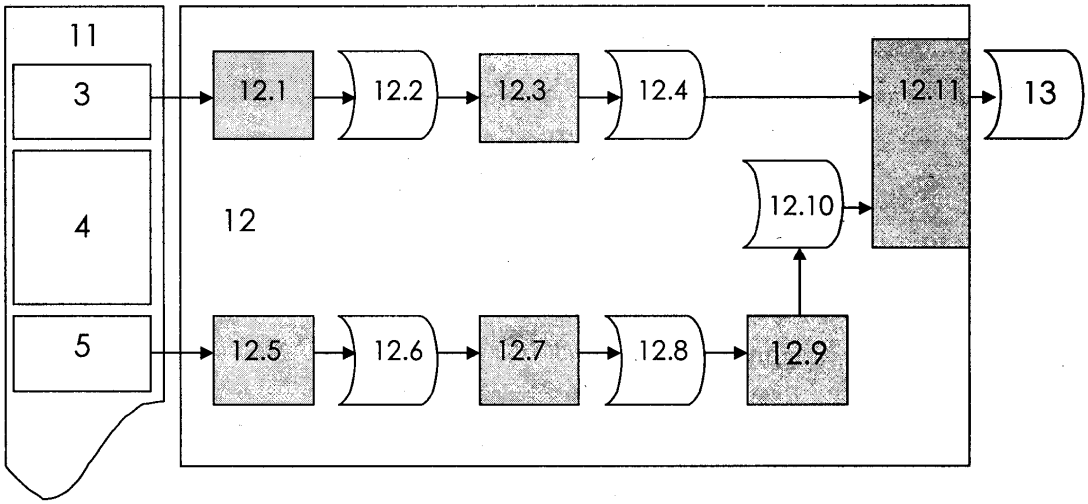

Fig. 3