(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 February 2010 (18.02.2010)

PCT

(10) International Publication Number
WO 2010/018587 Al

(51) **International Patent Classification:**
H04L 9/32 (2006.01)

(21) **International Application Number:**
PCT/IN2008/000500

(22) **International Filing Date:**
11 August 2008 (11.08.2008)

(25) **Filing Language:** English

(26) **Publication Language:** English

(71) **Applicant and**
(72) **Inventor: ALLE, Mohandas, Damodar** [IN/IN]; Worli B.D.D. Chawls, Chawl NO-60, Room NO-75, G.M. Bhosale Marg, Worli, Mumbai 400 018 (IN).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available):* AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, **BH,** BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, **EC,** EE, **EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL,** IN, **IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,** NA, **NG,** NI, NO, **NZ, OM, PG, PH, PL, PT,** RO, **RS, RU, SC, SD, SE, SG,** SK, SL, SM, ST, SV, SY, **TJ,** TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available):* ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasim (AM> AZ, BY, KG> KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, **IT,** LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (**BF' BJ' CF' CG' CI' CM' GA' GN' ° Q, GW' ML' MR'** NE' SN' TD' TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.1 7(U))*

— *of inventorship (Rule 4.1 7(W))*

Published:

— *with international search report (Art. 21(3))*

(54) Title: VERIFICATION OF DOCUMENT AND IT'S CONVEYING INFORMATION FOR THE RELIABLE AUTHENTIFICATION

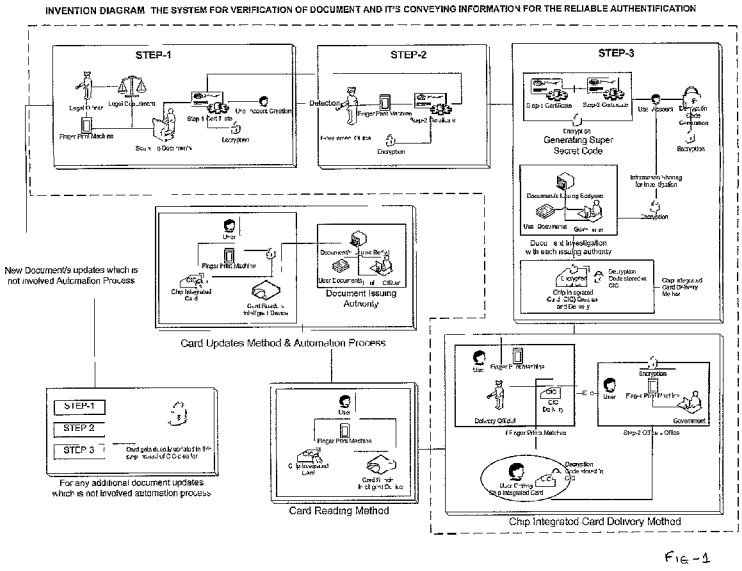

Fig-1

(57) Abstract: This Invention provides to get verified and very reliable authentication certified by private and government officials by taking finger prints and approves the document/s for further steps to get move ahead to final step for chip integrated card delivery, this is a unique and non-match able method to prevent from copying existing IP. All the steps involve in private and government officials verification and certification involved secure and safer ways of encryption and decryption with super secret code to match prevent from fraudulent in the process, finally all stored IP will get secret codes of each IP, which is stored in user database, user data will be stored on one chip integrated card for user use, this card will help in simple term, for entire world to make faster and safer document verification whenever required.

WO 2010/018587 A1

VERIFICATION OF DOCUMENT AND IT'S CONVEYING INFORMATION FOR THE RELIABLE AUTHENTICATION

FIELD OF INVENTION:

The present invention generally relates to a reliable document verification system and, in particular, relates to a reliable document verification system using a public key cryptosystem. this service provides the users to store their certificates and upload their documents with the help of attorneys to get the copy is certified before *uploading* on their *account to* make *sure to prevent fraudulent.*

OBJECT OF THE INVENTION:

The present invention provides a particularly verified document system. Wherein The users store their certificates and upload their documents with the help of attorneys to get the copy is certified before uploading on their account to make sure to prevent fraudulent. This process works as, all stored Intellectual Properties (certificates / documents / plans / agreements/deeds) are TRUE and ORIGINAL based on terms and conditions of individual government body of each country. This process involves tie-up with governments to get certified these TRUECOPIES with Originality of its concept. This will help Governments to reduce fraudulent, in any sector/process of government/semi-government/public/private/corporate/indivfdual in all manners and easier way to get process done and verified smoother and faster with secure way.

This process will be considered with individual country law to maintain their privacy and confidentiality.

BACKGROUND OF THE INVENTION:

This Invention particularly relates to document verification system. When specific types of documents are issued on behalf of one or more specific person(s) or object(s) it may be necessary to verify the association of such document with the person(s) or object(s) to deter the unauthorized use of such document on behalf of a person(s) or object(s) not associated with the document. The fastest and easiest way to verify an association is by visual verification of validated information concerning the authorized person(s) and/or object(s) and the actual person(s) and/or object(s) for which use of the document is sought. An individual whose responsibility it may be to verify the authorized use of a document on behalf of specific person(s) or object(s) can easily confirm such authorized use if he or she has immediate availability to such verified information concerning the person(s) or object(s) associated with the document.

BRIEF DESCRIPTION OF THE INVENTION:

he present Invention provides the users to store their certificates and upload their documents with the help of attorneys to get the copy is certified before uploading on their account to make sure to prevent fraudulent. This process works as, all stored Intellectual Properties (certificates / documents / plans / agreements/deeds) are TRUE and ORIGINAL based on terms and conditions of individual government body of each country. This process involves tie-up with governments to get certified these TRUECOPIES with Originality of its concept. This will help Governments to reduce fraudulent, in any sector/process of government/semi-government/public/private/corporate/individual in all manners and easier way to get process done and verified smoother and faster with secure way.

This process will be considered with individual country law to maintain their privacy and confidentiality.

TURE COPIES PROCESS:-

STEP-1:

User certificates/documents/agreements/deeds, all of user Intellectual Property (IP) will be verified in front of Lawyer/Attomey/who is having authority to certify while scanning the documents. Legal Official gives one certificate saying all the documents are certified in his presence, and takes user Finger Prints.

This Certificate will be having one unique certificate number which is for security reason.

And scanned IP & Finger Print will be stored on one server, which is fully protected and under 24/7 monitoring machine to provide security. Each user unique certificate number will be stored referring their documents to cross verify and match with other process's codes in this process cycle.

STEP-2:

From the Government one of official will verify all the documents which are certified in Step-1 .

Here in this step also, government official gives one certificate saying he personally verified all the documents and legal officials' certificate. Government official issued certificate having one unique number with prefix of the legal official's issued certificate, and also check Finger Prints again.

Unique certificate number of this step will be affix to the step-1 unique number.

STEP-3:

Once Step-1 &2 are cleared, then both the unique certificate numbers clubbed and based on some algorithm adding to it one secret code will be generated and shared with govemment/s for record.

Here government will verify each document, with respective issuing body. After successful verification each document get one value and these values are stored in Chip Integrated Card and will be delivered to the user.

These will be stored in encrypted format, so this card can't be editable by anyone without decryption code. This decryption code will be with user only. And these details with one Chip Integrated Card will be delivered to user with very important registered mailing method. While delivering here again user's Finger Prints will be verified, after successful verification documents will be given to user, if user fails in any reason. Decryption code gets deactivated immediately. If there is a problem with Finger Prints Reader, then it will be delivered in presence of government verification office, which is verified in the Step-2. While giving these documents in official's office, Finger Prints will be taken at this point of time and once the user gets positive reply the decryption code gets active, and Chip Integrated Card will be delivered to the user.

HOW UPDATES DONE:

For any document/s updates again step 1 to 3 will be involved and in step 3 document/s values will be updated in user database and those document/s values will be updated in Chip Integrated Card.

AUTOMATION PROCESS:

In each department one Intelligent Device which reads user's Chip Integrated Card while issuing any new document/s, and these values will be updated and store in user database and user will get updated their cards immediately. By the document/s issuing body they will be having that authority, and this authority will be given by Patent Holder.

OR user can visit authorized official body office/government, if they miss updates on document/s issuing time.

HOW GOVERNMENT WILL BE GETTING THE INTELLIGENT DEVICES TO READ AND UPDATE THE USER DATA:

Patent Holder will be proving to the authorizing body under his agreement, with terms & conditions.

HOW GOVERNMENT WILL GET BENEFITED:

For Government Verification Patent Holder will give some funds to government, this can be monthly/quarterly/yearly basis to clear a settled amount at a given and agreed terms & conditions. Payment based on user/s, and onetime payment only for each user/s. When Government Official verify the certified documents, for each user/s some funds which is decided by Patent Holder will be given as goodwill, Patent Holder is having full rights to change this at anytime, this payment is one time only.

Patent Holder holds the rights to change this Terms & Conditions at any point of time.

WHAT ABOUT UPDATES FEES:

This will be decided by Patent Holder and each time documents get updated which is not involved automation process then additional fees will be collected.

ANNUAL CHARGES:

This will be decided by Patent Holder.

WHAT NATION GETS BENEFITED BY DOING THIS?

1. Protecting fraudulent in document forgery.
2. Faster verification of documents.
3. Faster Process in all governments/semi-government / public / corporate / forms / individuals.
4. Security for original documents.
5. Connecting all at one hub.

HOW USER CAN GET ACCESS OF DOCUMENTS:

TRUECOPIES will have one web portal for online access.

WHO'S FINGER PRINTS WILL BE MAINTAIN FOR RECORDS:

Finger Prints validation, for users / authorized / legal / government /document (s) issuing officials finger prints are stored for process record to maintain a track of the process involvement, to prevent internal fraudulent and protection.

WHAT TYPE OF FEATURES WEB PORTAL HAS:-

1. User admin section where user can share documents online / apply for jobs in government / public / private / corporate / forms / individual sectors.
2. User can track applications.
3. Maintaining accounts for his users to give access to his documents online.
4. All documents opened are tracked by IP, TIME, DATE, number of times document viewed his users which they share to view documents.
5. All documents will be shared in encrypted manner and accessed by secure mode.
6. Applying and sharing will be done only via online or via Chip Integrated Card. This will again protect super fraudulent.
7. Users can take a back up of their documents for personal use.
8. Making all the process easy and faster with secure and safer mode for entire nation. And entire world with having different country with different government policies.

I CLAIM:

Claim-1 . A method of producing and authenticating a secure document Comprising the steps of:

a) scanning said (certified by private and government officials by taking finger prints and approves) document to produce a first signal representative of an image of said at least a portion of said document;
b) encrypting a second signal, comprising a representation of said image, said second signal being derived at least in part from said first signal;
c) incorporating a coded representation of said encrypted second signal with said document;
d) reading said coded representation of said second signal from said document;
e) decoding said second signal;
f) decrypting said decoded second signal;
g) inputting said decrypted second signal to a display to display said representation of said image;
h) comparing said document to said displayed image to authenticate said document.

Claim-2. A system for authenticating a plurality of documents, said system comprises:

a) An authenticating source, said authenticating source including means for providing a first public key encryption key to a third party;

b) Means, associated with said source, for providing an authentication message to said third party in the form of coefficient of a polynomial, said authentication message being encrypted by a second public key encryption key and including the decryption key for said first public key encryption key; means, associated with said third party, for generating variables and values to said polynomial and applying different ones of said variables and value to each of said plurality of documents; means, associated with an authenticating service, for recovering said

c) Authentication message from a plurality of different ones of said variables and values; and means, associated with said source, for providing the decryption key corresponding to said second public key encryption key to said authenticating service such that said authentication message can be decrypted.

Claim-3. The process of authenticating a secure document. where in shown on Fig: 1, the comprising steps of:

1. Finger Prints Capturing by Legal/Government Officials.
2. Documents Scanning of Authorized Official updates on to the server, here official finger prints will be stored for verification and cross checking purpose. To protect fraud.
3. Legal Official Certification.
4. Government Official Verification certificate, including finger print checking.
5. Secret Code Development with includes Finger Prints value in it.
6. Chip Integrated Card (CIC) Development with encrypted values in it and decryption value in encrypted way.
7. Intellectual Devices to read CIC.
8. Secure Mailing System for CIC delivery.
9. Finger Prints validation, for users / authorized / legal / government /document (s) issuing officials finger prints are stored for process record to maintain a track of the process involvement, to prevent internal fraudulent and protection.

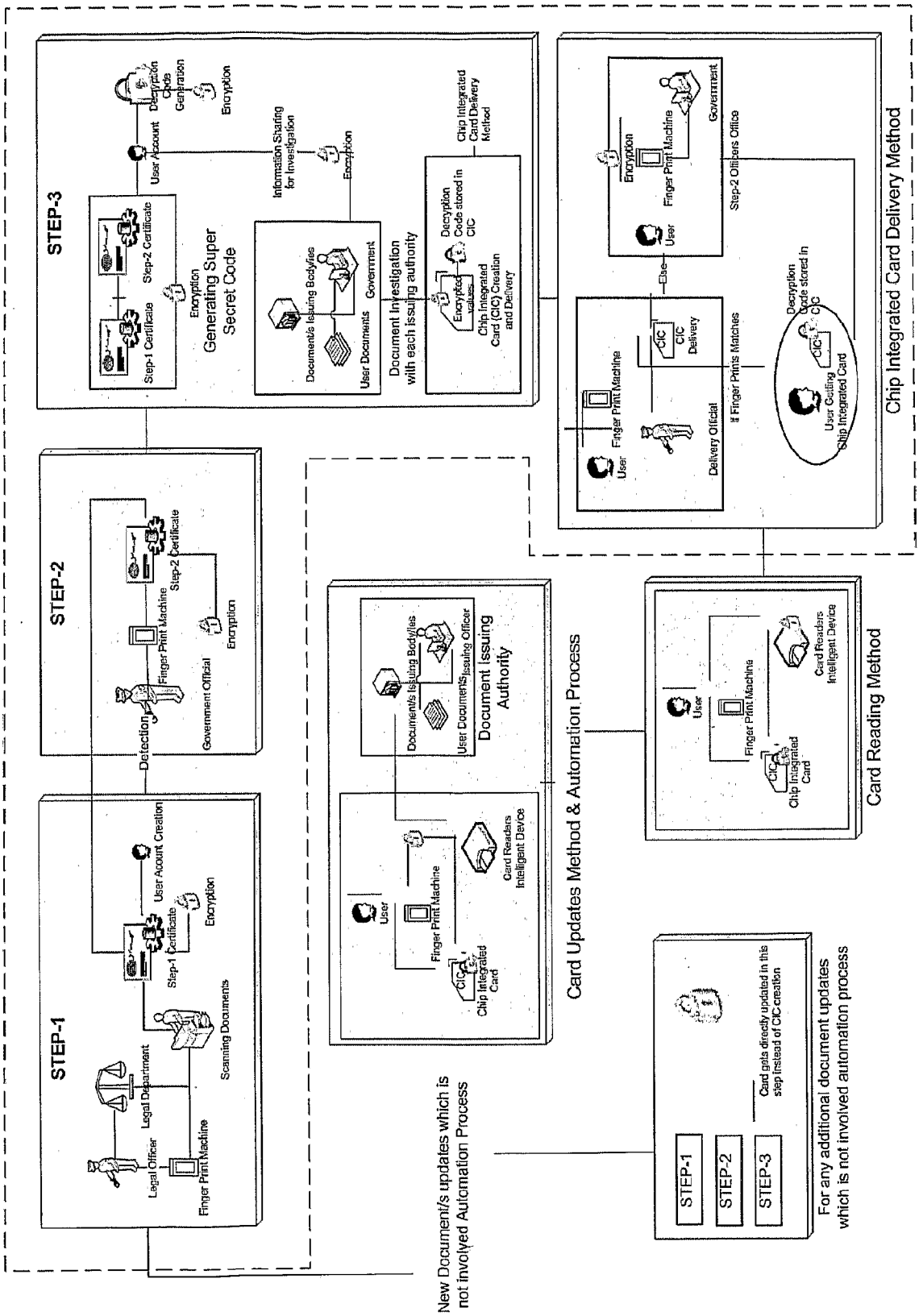
INVENTION DIAGRAM: THE SYSTEM FOR VERIFICATION OF DOCUMENT AND IT'S CONVEYING INFORMATION FOR THE RELIABLE AUTHENTIFICATION.
STEP-1
Legal Officer
Legal Department
Finger Print Machine
Scanning Documents
User Acount Creation
Step-1 Certificate
Encryption
STEP-2
Detection
Government Official
Finger Print Machine
Step-2 Certificate
Encryption
STEP-3
Step-1 Certificate
Step-2 Certificate
Encryption
Generating Super Secret Code
User Account
Decryption Code Generation
Encryption
Information Sharing for Investigation
Encryption
Documents Issuing Bodyties
Government
User Documents
Document Investigation with each issuing authority
Encrypted values
Chip Integrated Card (CIC) Creation and Delivery
Decryption Code stored in CIC
Chip Integrated Card Delivery Method
Chip Integrated Card Delivery Method
User
Finger Print Machine
Delivery Official
CIC
CIC Delivery
If Finger Prints Matches
Else
Encryption
User
Finger Print Machine
Government
Step-2 Officers Office
Decryption Code stored in CIC
CIC
User Ocding Chip Integrated Card
Card Updates Method & Automation Process
User
Finger Print Machine
CIC
Chip Integrated Card
Card Readers Intelligent Device
Card Reading Method
Document Issuing Authority
Documents Issuing Bodyties
User Documents
Issuing Officer
User
Finger Print Machine
CIC
Chip Integrated Card
Card Readers Intelligent Device
New Document/s updates which is not involved Automation Process
STEP-1
STEP-2
STEP-3
Card gets directly updated in this step instead of CIC creation
For any additional document updates which is not involved automation process

Fig-1

INTERNATIONAL SEARCH REPORT

International application No
PCT/IN 08/Q0500

A CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 9/32 (2009.01)
USPC - 713/168
According to International Patent Classification (IPC) or to both national classification and IPC

B FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
USPC 713/168

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC 713/150, 164, 168, 170, 176, 715/200, 221, 243, 726/2, 5, 26, 27,

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
USPTO WEST (PGPB, USPT, EPAB, JPAB), GoogleScholar
Search Terms Used fingerprint, encrypt, encode, decrypt, public, private, key, authenticate, venfy, fraud, document, government, polynomial, coefficient, third, party, scan, certificate etc

C DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No
X	US 2004/0003295 A1 (ELDERFIELD et al) 01 January 2004 (01 01 2004), entire document, especially para [0005], [0010], [0025], [0031], [0033], [0049] and abstract	1 and 3
X	US 2008/0037776 A1 (AKIYAMA et al) 14 February 2008 (14 02 2008), entire document, especially [0007]-[0009], [0068] , [0092]-[0099], [0134]-[0143]	2
A	US 2008/0141033 A1 (GINTER et al) 12 June 2008 (12 06 2008)	1-3
A	US 7,330,974 B1 (SILVERBROOK et al) 12 February 2008 (12 02 2008)	1-3

I I Further documents are listed in the continuation of Box C | |

* Special categories of cited documents
'A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority cla tm(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 July 2009 (20 07 2009)	1 % JUL 2009
Name and mailing address of the ISA/US Mail Stop PCT, Attn ISA/US, Commissioner for Patents P O Box 1450, Alexand πa, Virginia 22313-1450 Facsimile No 571-273-3201	Authorized officer Lee W Young PCT Helpdesk 571-272-4300 PCT OSP 571-272 7774

Form PCT/ISA/2 10 (second sheet) (April 2007)