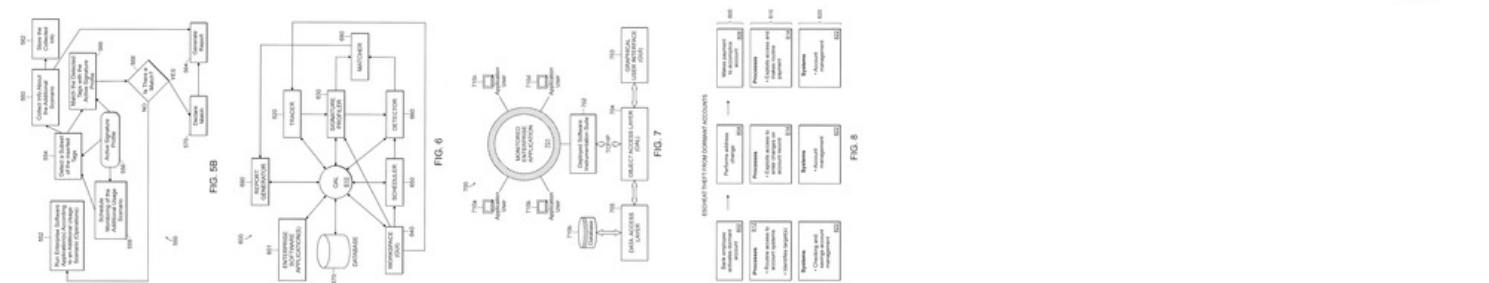
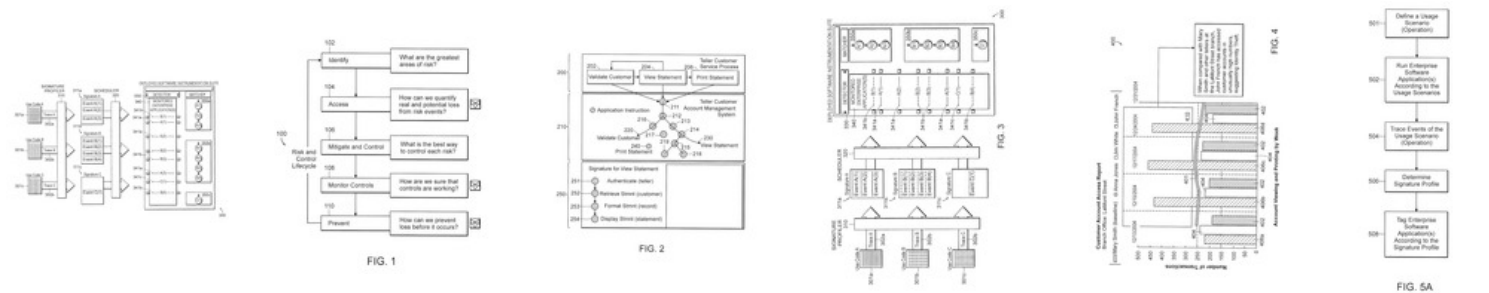
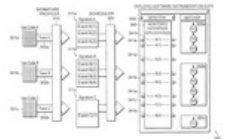


202 results for ((fraud+)/TI/AB/IW/CLMS/TX/DESC/ODES/OBJ/ICLM/ADB/KEYW AND (call)/TI/AB/IW/CLMS/DESC/ODES/OBJ/ADB/ICLM/KEYW/TX AND (monitor+)/TI/AB/IW/CLMS/DESC/ODES/OBJ/ADB/ICLM/KEYW/TX AND (center)/TI/AB/IW/CLMS/DESC/ODES/OBJ/ADB/ICLM/KEYW/TX AND (evidence)/TI/AB/IW/OBJ/ADB/ICLM) - Collection: FAMPAT

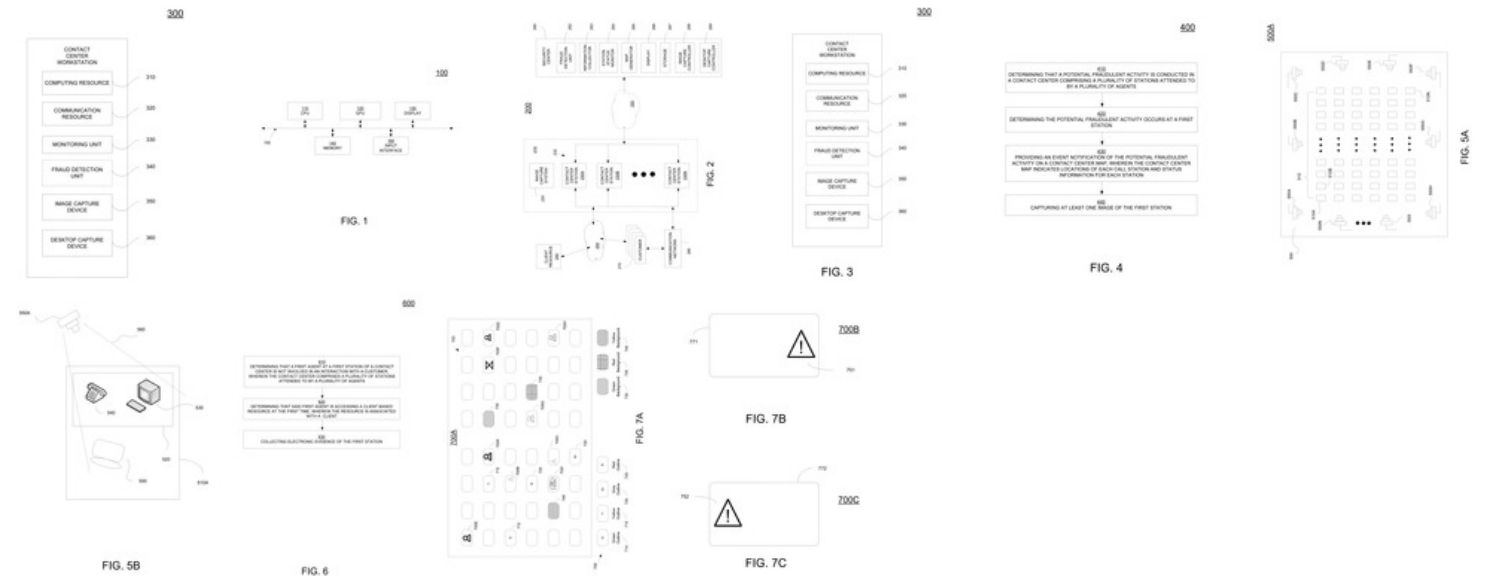
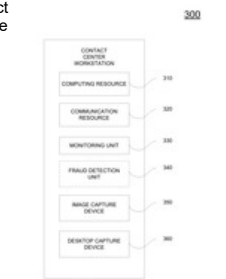
#	 Title	Publication number	1st App. date	Applicant/Assignee	1st Publ. date	Publ. date
1.	 System and method for monitoring and detecting fraudulent use of software applications	US2005182750	2005-02-11	FIS FINANCIAL COMPLIANCE SOLUTIONS* MEMENTO	2005-08-18	2005-08-18

A systems and methods are described detect **fraud** in existing logs of raw data. There can be several disparate logs, each including data of disparate data types and generated by different and possibly unrelated software enterprise applications. The **fraud** management system aggregates and organizes the raw log data, extends the raw data with reference data, archives the data in a manner that facilitates efficient access and processing of the data, allows for investigation of potentially **fraudulent** usage scenarios, and uses the results of the investigation to identify patterns of data that correspond to high risk usage scenarios and/or process steps. In subsequent processing, archived data can be compared against the identified patterns corresponding to high risk usage scenarios to detect matches, and the invention thereby automatically detects high risk usage scenarios and issues appropriate alerts and reports.



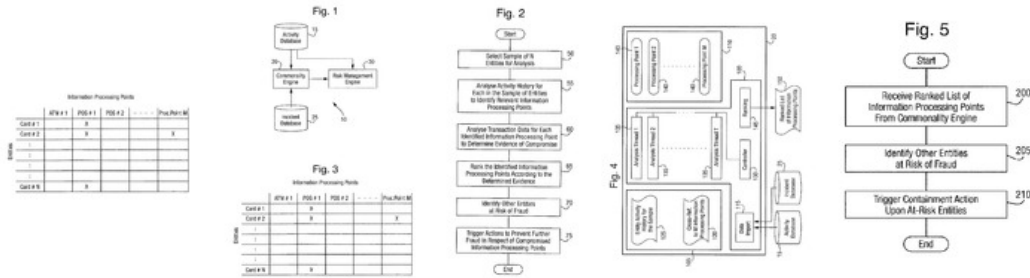
2.	 Contact center anti-fraud monitoring, detection and prevention solution	US2016065732	2015-06-25	TELEPERFORMANCE*	2016-03-03	2016-03-03
----	---	--------------	------------	------------------	------------	------------

A method of **fraud** detection is disclosed. The method includes determining that a first agent at a first workstation of a contact **center** is not on a **call** at a first time. The contact **center** includes a plurality of workstations attended to by a plurality of agents. The method includes determining that the first agent is accessing a client based resource at the first time, wherein the resource is associated with a client. The method includes collecting electronic **evidence** of the first workstation.

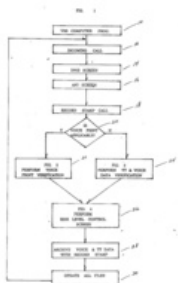
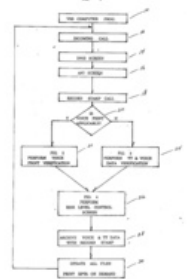


A fraud detection method and apparatus are provided, arranged to: (i) select a sample of entities, including at least one entity known to have been exposed to fraudulent activity or suspected of having been so exposed; (ii) inputting, from an activity database, transaction data defining activity in respect of the sample of entities, the transaction data identifying associated information processing points; (iii) processing the input transaction data to determine, using a predetermined set of metrics, evidence of compromise in any one or more of the identified information processing points; and (iv) ranking the identified information processing points according to likelihood of compromise. In this way, one or more information processing points may be identified as a potential source of fraud and steps triggered to identify, from the activity database, any other entities associated with those potential sources of fraud to prevent further fraud.

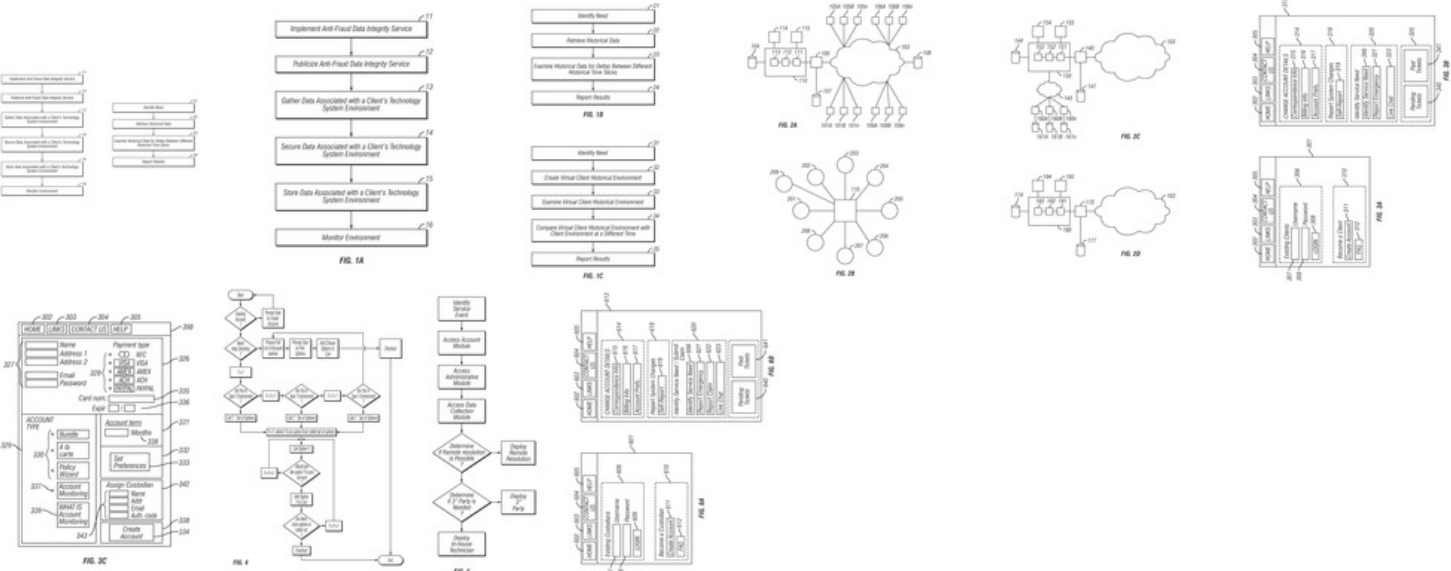
Information Processing Points				
	Info P1	Info P2	Info P3	Info P4
Card 1	X			
Card 2		X		
Card 3			X	
Card 4				X



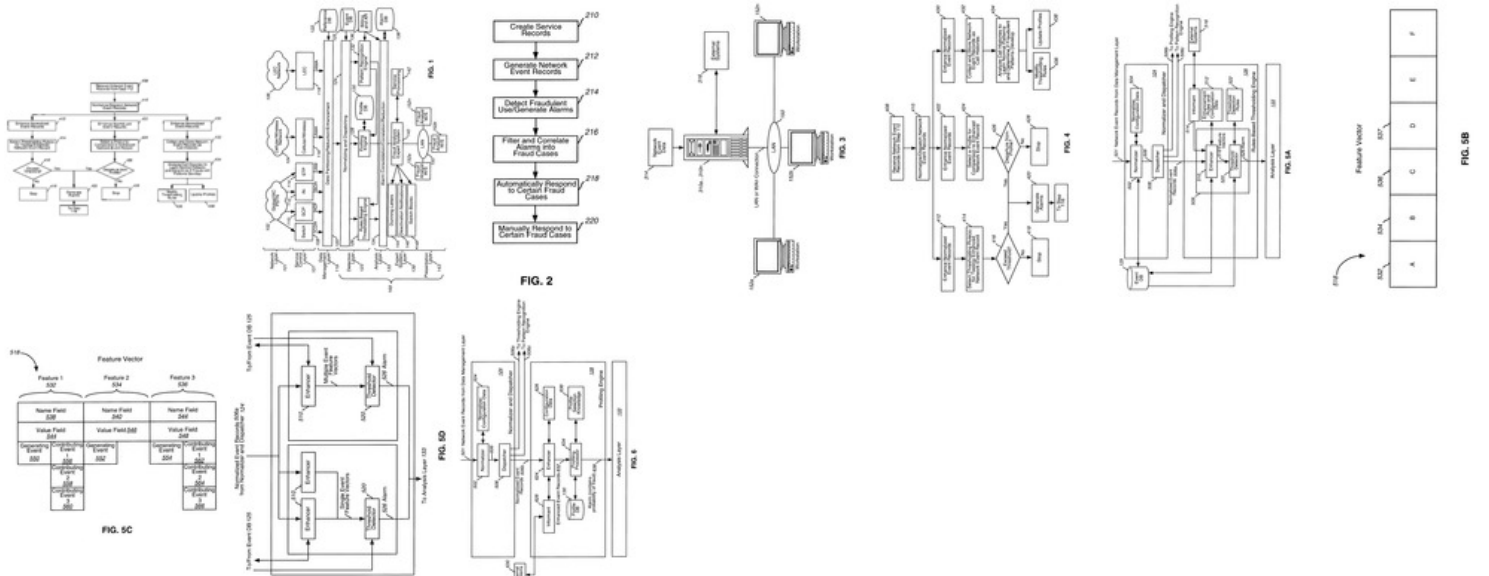
The INTERACTIVE CREDIT CARD FRAUD CONTROL PROCESS system utilizes a computer with telephone interface, memory, voice recognition software and hardware, and an information archive and retrieval process. A computer program (10) is used to automatically and electronically control the determination of the caller as the authorized credit card holder, or conversely an unauthorized perpetrator attempting to make a credit card transaction. The telephone interface is connected to a telephone line and the caller dials a number that connects the caller with the present invention (12), which then captures certain information about the incoming call (14 & 16) and creates a permanent Record Stamp (18) of the call to which transactional information is added as the call progresses. The caller is asked question prompts, and the system receives voice and touch tone responses from the caller from which the system determines if a VoicePrint is applicable (20). The caller responses are managed by the present invention in a method that determines if the caller is the authorized credit card holder, and if the caller is not the authorized credit card holder the present invention captures information that can lead to the capture and conviction of the caller as a credit card fraud felon. The present invention uses the caller's spoken voice print of the card holder's name as one of the determining factors to determine if the caller is the authorized credit card holder (22). The VoicePrint, included in a claim in the present invention, uniquely and positively identifies a single person, and therefore becomes a valuable tool and evidence in the apprehension and conviction of perpetrators of credit card fraud. With a VoicePrint of the authorized credit card holder on file, the present invention prevents any other person except approved persons from making credit card transactions with that card number. Even without the VoicePrint, the control process is highly effective in limiting fraud risk and the present invention creates a VoicePrint of the caller, ties that identifier to the Record Stamp, and can thereafter identify that person as the person who was the caller. Additional claims relate to using the present invention for security and access control, including the gathering of positive identifying evidence of perpetrators. <IMAGE>



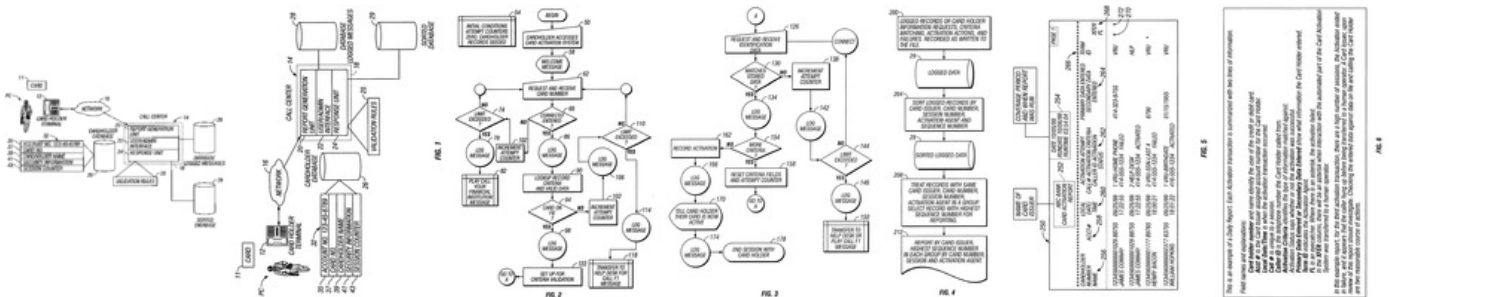
Any of various comparisons of computer folders from different points in time is performed. Such comparisons provide the ability to discover missing documents or documents with modification dates that have changed when there would otherwise have been no need to change them and thus allows discovery of missing documents to discover fraud or to search for evidence after a fraud is suspected. In another embodiment, deltas in accounting system vendor invoice accounts are compared at different points in time, potentially exposing the practice of moving fraudulent vendor transactions into a large group of legitimate transactions for a legitimate vendor. Per period transaction totals for specific periods for legitimate vendors are compared over historical time for suspicious activity. A comparison of reports from the two different periods, using exact data and software from those separate periods (instead of reporting from "current" data), may raise a red flag otherwise missed.



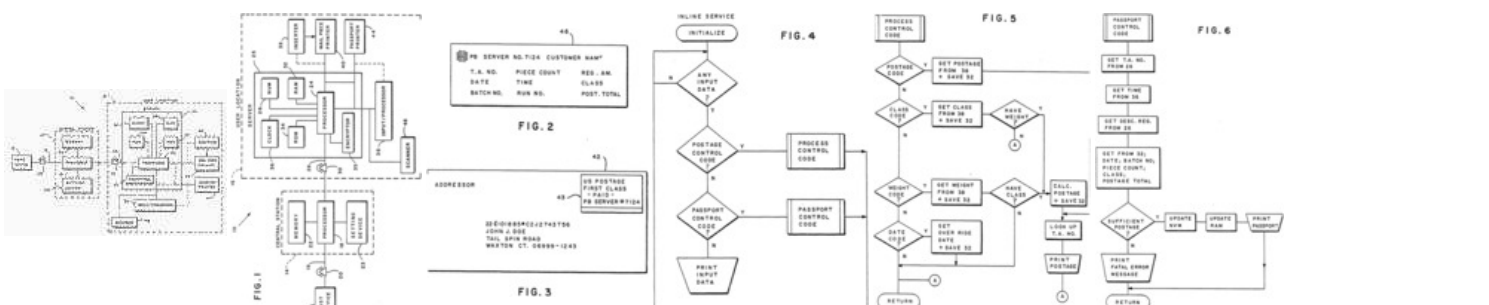
A system, method and computer program product for processing event records. The present invention includes a detection layer (123), an analysis layer (133), an expert systems layer (139), and a presentation layer (143). The layered system includes a core infrastructure (1310) and a configurable, domain-specific implementation (1312). The detection layer (123) employs one or more detection engines, such as, for example, a rules-based thresholding engine (126) and a profiling engine (128). The detection layer can include an AI-based pattern recognition engine (132) for detecting new and interesting patterns and for updating the detection engines to ensure that the detection engines can detect the new patterns.



A method and apparatus (10) for the detection and investigation of **fraudulent** debit and charge card (11) activation transactions. Cardholder information on file is matched with information provided at activation time. Where matching does not occur, **fraud** is a possibility. All activity is captured and summarized (20, 22). Absolute failures are highlighted. Subsequent use of **fraudulently** activated cards can be investigated resulting in possible identification of the alleged **fraudulent** card user.

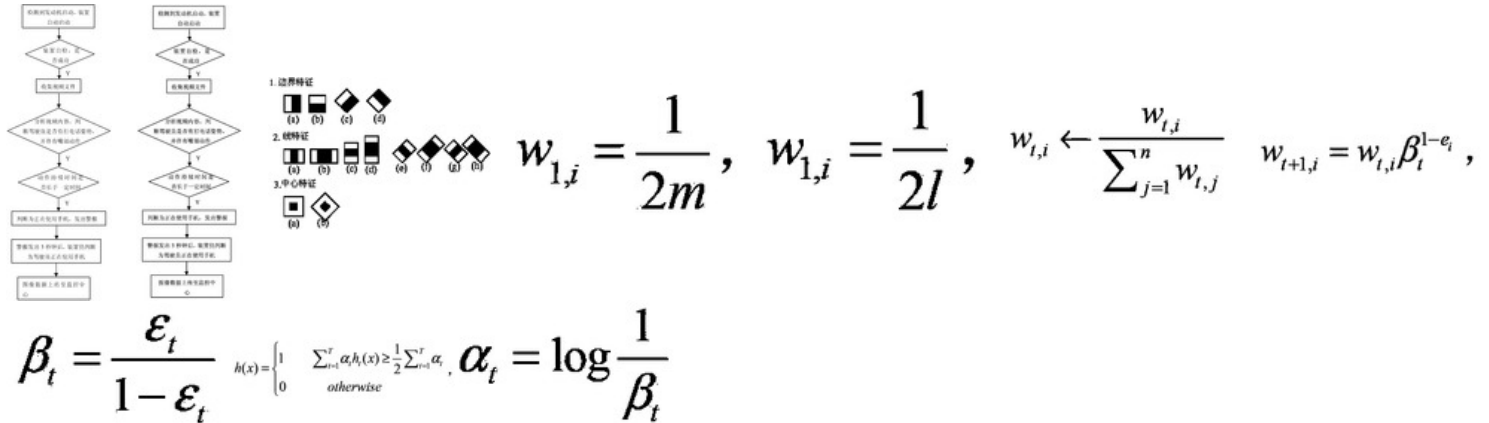


A system for processing batch mail in which a mail sender processes batches of mail each of which includes a statement containing data that allows mail payment verification. Included in this data is the balance of postage value after processing the mail.



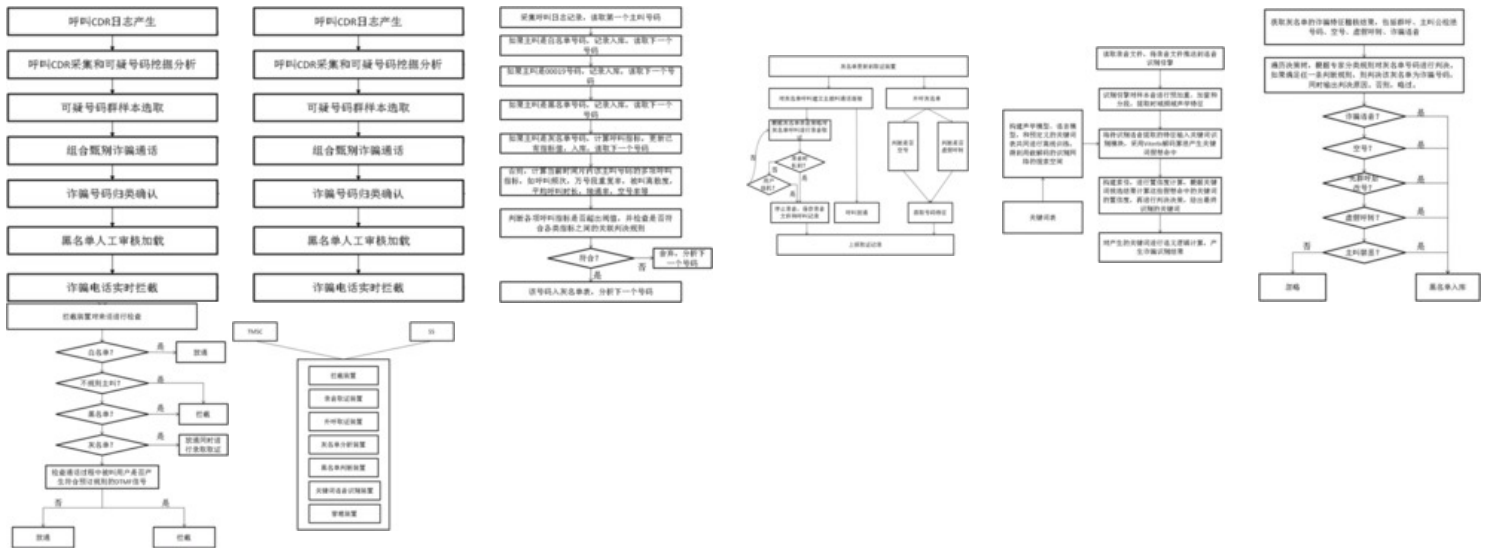
9.	Device and method for automatically monitoring telephone call behavior of driver when driving	CN103366506	2013-06-27	BEIJING UNIVERSITY OF TECHNOLOGY*	2013-10-23 2013-10-23
----	---	-------------	------------	-----------------------------------	-----------------------

The invention relates to a device and a method for automatically **monitoring** a telephone **call** behavior of a driver when driving and belongs to the fields of intelligent traffic and aided driving. The device comprises an image acquisition device, a calculating device, a warning device and a wireless transmission device. The method comprises the following steps of firstly acquiring a head and nearby area image of the driver, secondly, obtaining the positions of the face and both hands of the driver in the image by skin color detection, and classifying by a support vector machine to determine whether the driver makes a telephone **call** or not; warning the driver if the driver makes the telephone **call**; uploading the image that the driver makes the telephone **call** to the **monitoring center** of the road transport bureau through a wireless network if the warning is useless to be used as an **evidence** that the driver breaks the law. According to the device and the method for automatically **monitoring** the telephone **call** behavior of the driver when driving disclosed by the invention, the unlawful act of the driver can be effectively **monitored**, the working strength of law enforcement personnel is relieved, the working efficiency is improved, and the occurrence rate of traffic accidents is reduced.

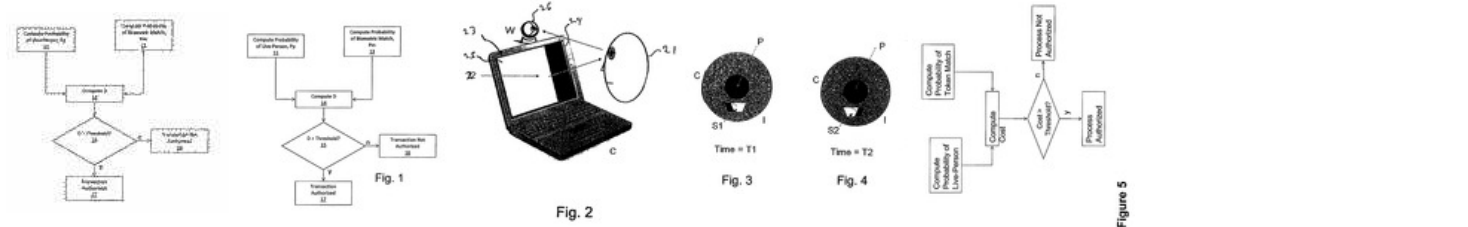


10.	Method and system for discriminating, classifying and intercepting fraud samples of suspicious numbers	CN106550155	2016-11-25	SHANGHAI CİNTEL INTELLİGENT SYSTEM* SHANGHAI XINFANG SOFTWARE*	2017-03-29 2017-03-29
-----	--	-------------	------------	---	-----------------------

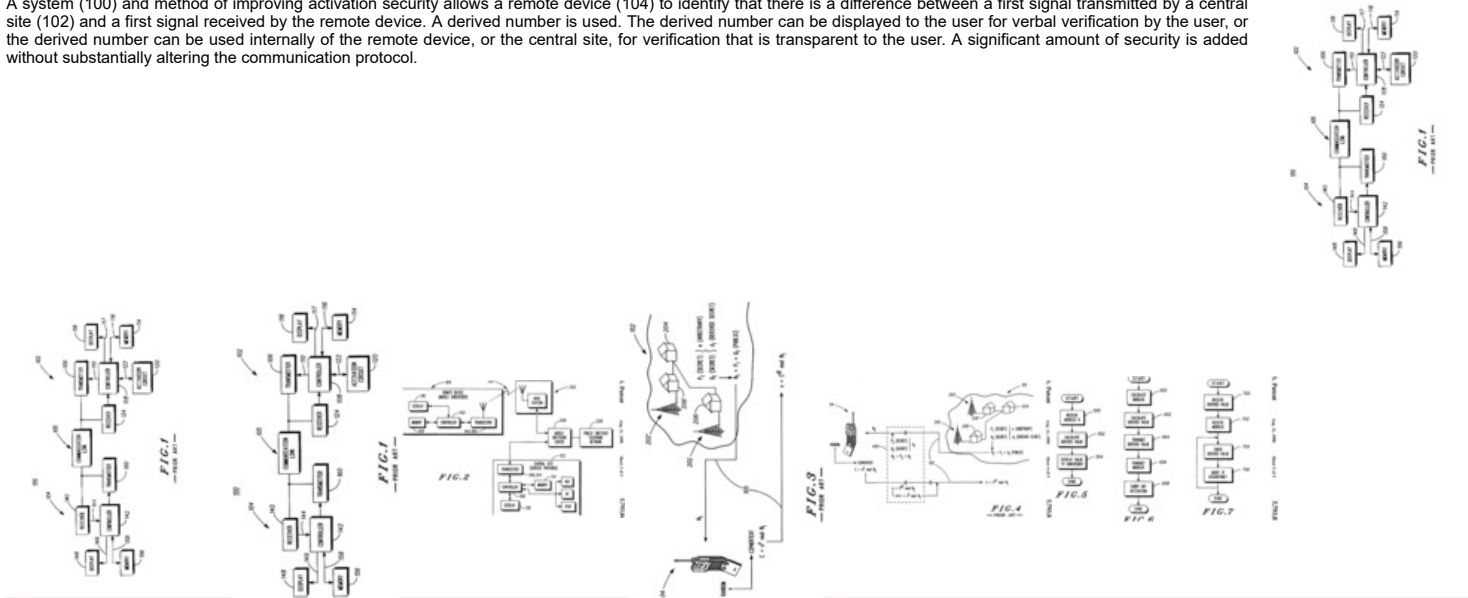
The invention discloses a method for discriminating, classifying and intercepting **fraud** samples of suspicious numbers. The method comprises the following steps: 1) accessing to a core network, and collecting **call** logs; 2) extracting and analyzing the suspicious numbers; 3) obtaining **fraud** numbers; and 4) manually reviewing a blacklist, and real-time intercepting **fraud** calls. According to the method disclosed by the invention, whether record samples of the suspicious numbers include the predefined combination of **fraud** keywords can be identified by using a mature keyword recognition technology, the function of intercepting and recognizing the **fraud** calls can be achieved, illegal calls that include, but are not limited to, **fraud** voices can be accurately recognized, and the **fraud** numbers can be further intercepted by using an anti-**fraud** interception platform which is accessed to the core network. The system disclosed by the invention can be applicable to various network standards, can be used for covering the fixed communication networks and mobile communication networks of China Telecom, China Mobile and China Unicom, and can be used for identifying and intercepting overseas **fraud** calls and domestic **fraud** calls.



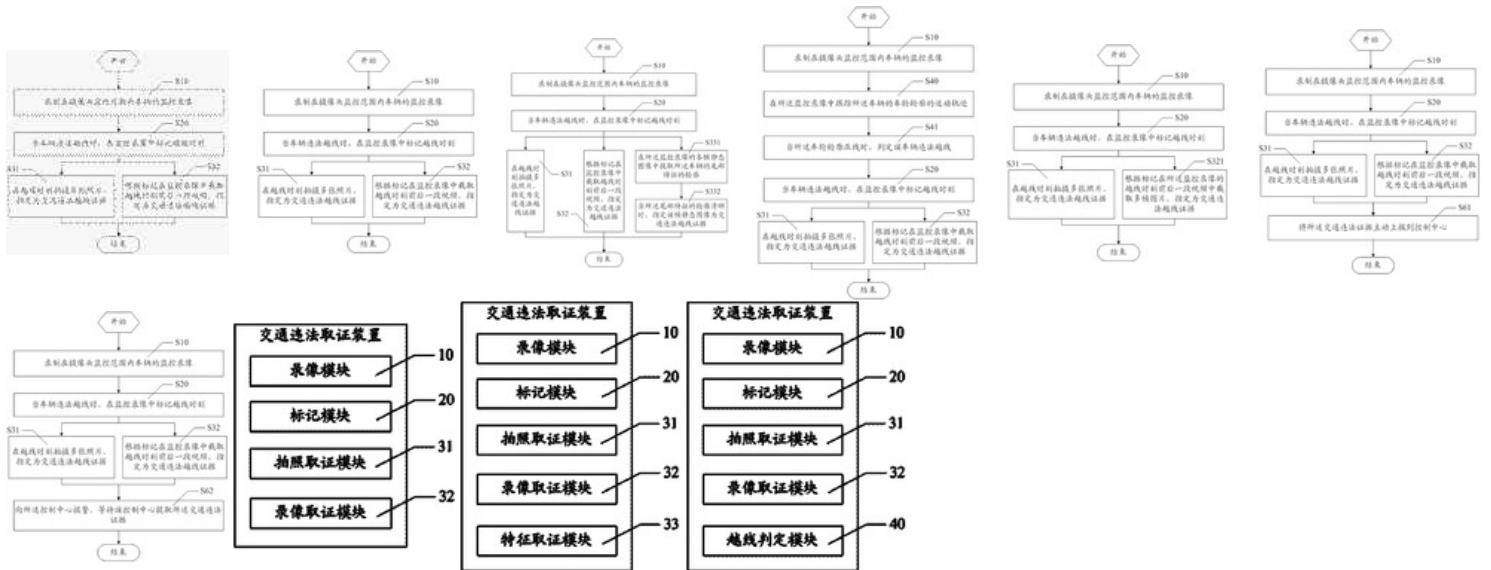
A method and system for authenticating financial transactions is disclosed wherein biometric data is acquired from a person and the probability of liveness of the person and probability of a match between the person and known biometric information are calculated, preferably according to a formula $D = P(p) * (K + P(m))$, wherein K is a number between 0.1 and 100, and authenticating if the value of D exceeds a predetermined value.



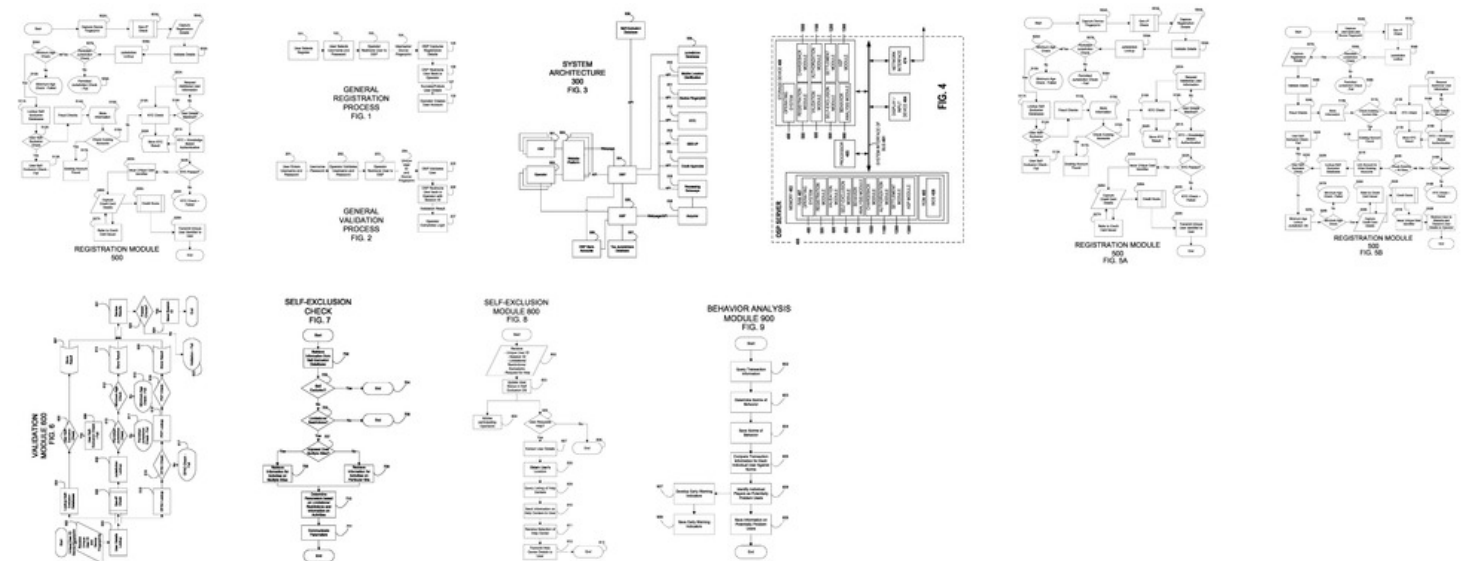
A system (100) and method of improving activation security allows a remote device (104) to identify that there is a difference between a first signal transmitted by a central site (102) and a first signal received by the remote device. A derived number is used. The derived number can be displayed to the user for verbal verification by the user, or the derived number can be used internally of the remote device, or the central site, for verification that is transparent to the user. A significant amount of security is added without substantially altering the communication protocol.



The invention discloses a traffic illegal line-cross evidence obtaining method and device. The traffic illegal line-cross evidence obtaining method comprises the following steps of: recording monitor video of vehicles in a camera monitoring range; when a vehicle crosses a line illegally, marking a line-cross time in the monitor video; taking a plurality of photos at the time when the vehicle crosses the line, and appointing the photos as a line-crossing and line-passing evidence; and intercepting videos before and after the line-cross time in the monitor video according to the mark, and appointing the videos as the traffic illegal line-cross evidences. According to the method disclosed by the invention, a vehicle illegal line-cross process can be positioned at an instant of illegal line-cross according to the high-definition photos; and the overall vehicle illegal line-cross process can be reflected clearly through dynamic videos, so that more intuitive observation is achieved.



Various embodiments of the present invention involve systems and methods providing services and mechanisms to online operators for gathering information about individuals the operators may engage in transaction activities with as well as ensuring certain protections are maintained with regard to these transaction activities. In particular embodiments, the systems and methods provide services and mechanisms such as the non-limiting examples of user registration, user verification, user validation, user self-exclusion, unique identifiers across multiple websites, session identifiers and/or certificate control features, underage controls, jurisdiction controls, compulsive behavior controls, chargeback controls, clearance and settlement functions, and tax identification and collection mechanisms.



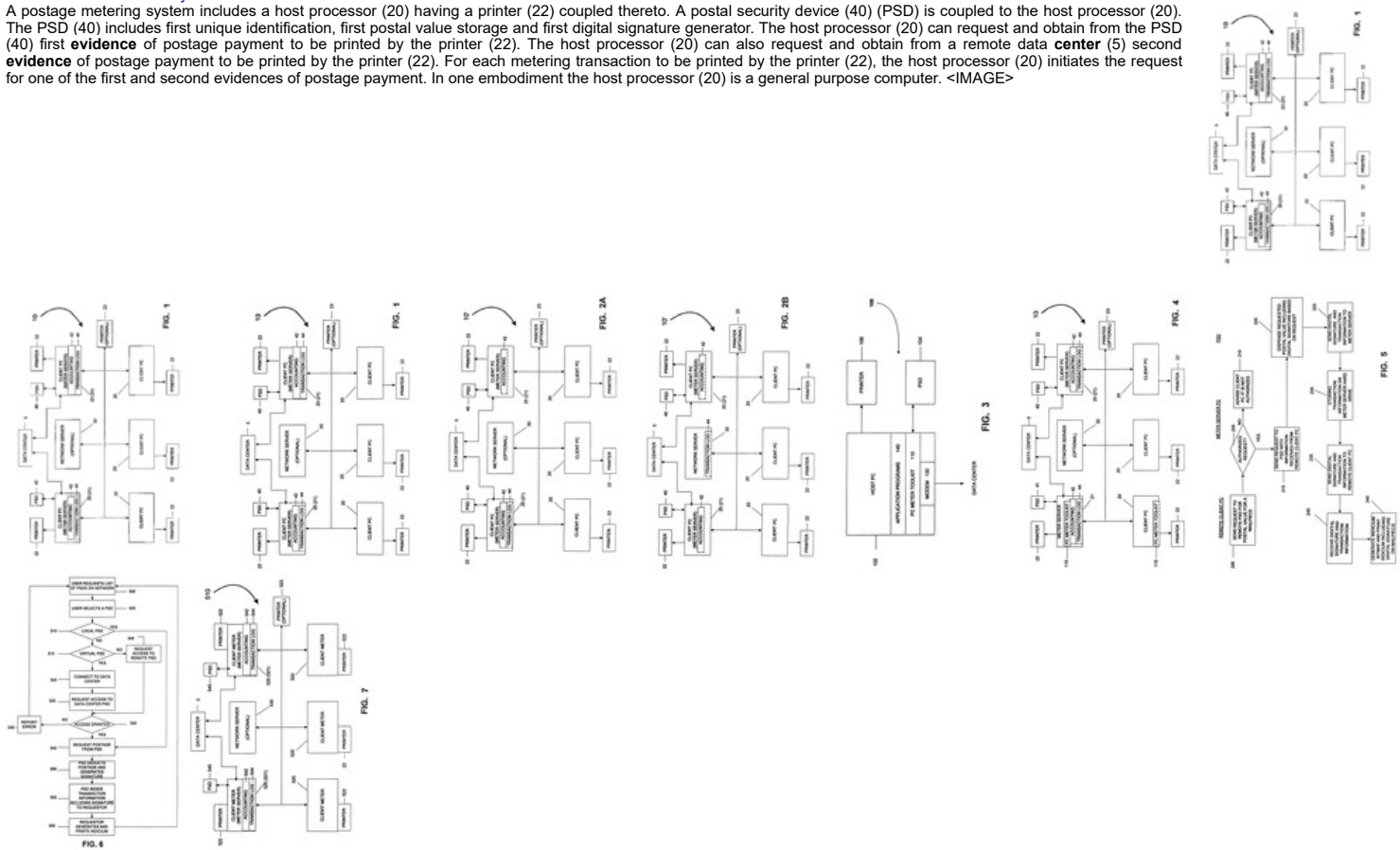
15. [Postage metering system and method for a stand-alone meter having virtual meter functionality](#)

1997-12-18

PITNEY BOWES*

1999-06-18 1999-06-18

A postage metering system includes a host processor (20) having a printer (22) coupled thereto. A postal security device (40) (PSD) is coupled to the host processor (20). The PSD (40) includes first unique identification, first postal value storage and first digital signature generator. The host processor (20) can request and obtain from the PSD (40) first **evidence** of postage payment to be printed by the printer (22). The host processor (20) can also request and obtain from a remote data center (5) second **evidence** of postage payment to be printed by the printer (22). For each metering transaction to be printed by the printer (22), the host processor (20) initiates the request for one of the first and second evidences of postage payment. In one embodiment the host processor (20) is a general purpose computer. <IMAGE>



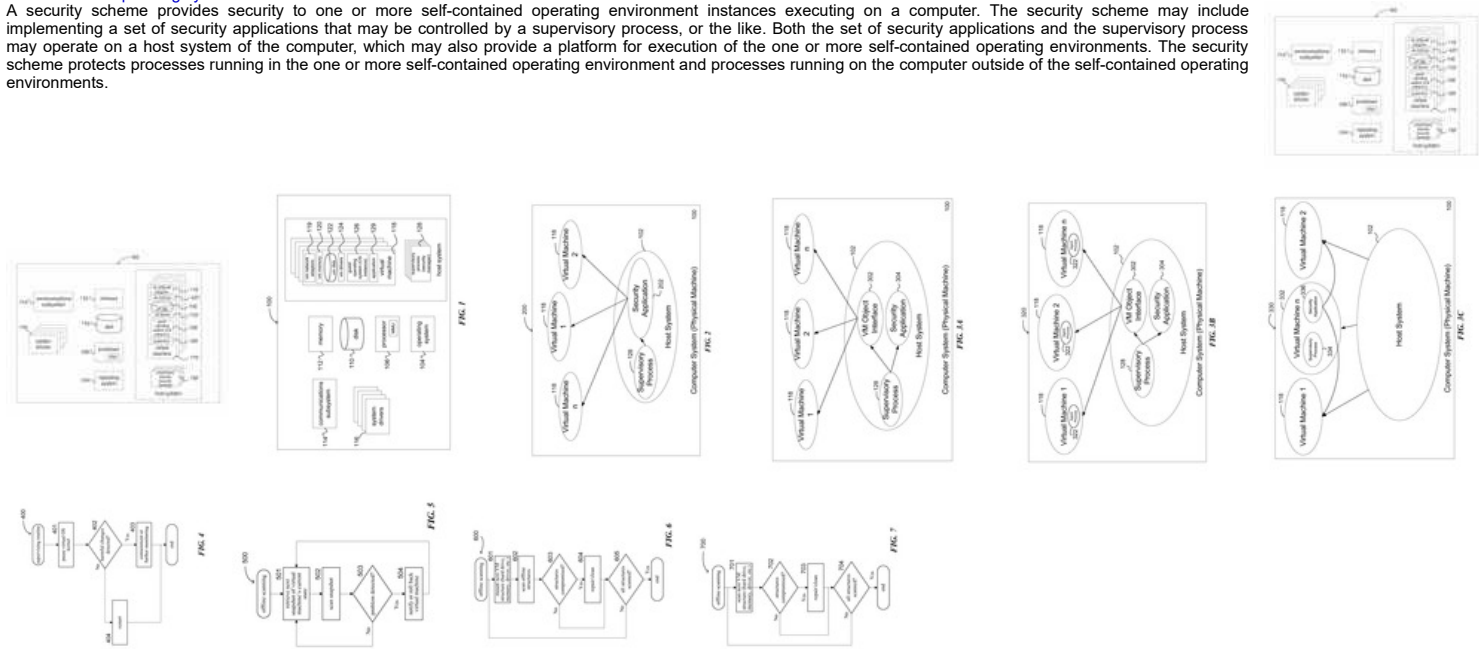
16. [Computer security management, such as in a virtual machine or hardened operating system](#)

2004-12-21

MICROSOFT
MICROSOFT TECHNOLOGY
LICENSING*

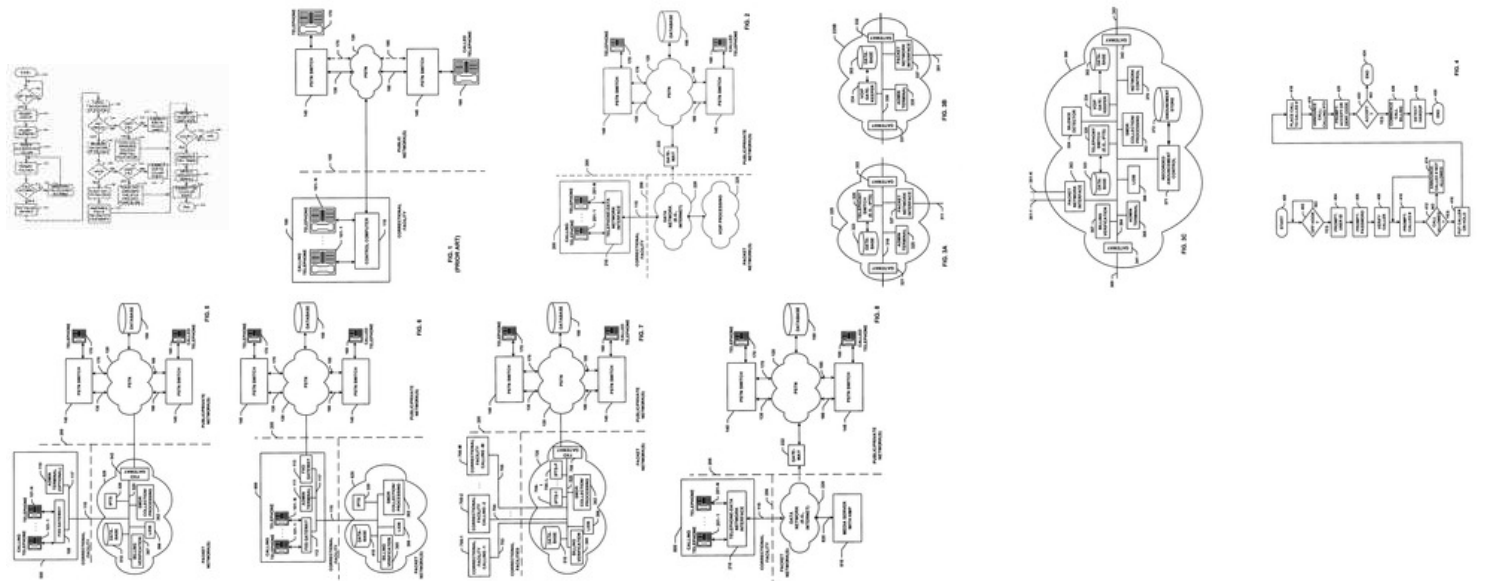
2006-03-01 2006-03-01

A security scheme provides security to one or more self-contained operating environment instances executing on a computer. The security scheme may include implementing a set of security applications that may be controlled by a supervisory process, or the like. Both the set of security applications and the supervisory process may operate on a host system of the computer, which may also provide a platform for execution of the one or more self-contained operating environments. The security scheme protects processes running in the one or more self-contained operating environment and processes running on the computer outside of the self-contained operating environments.



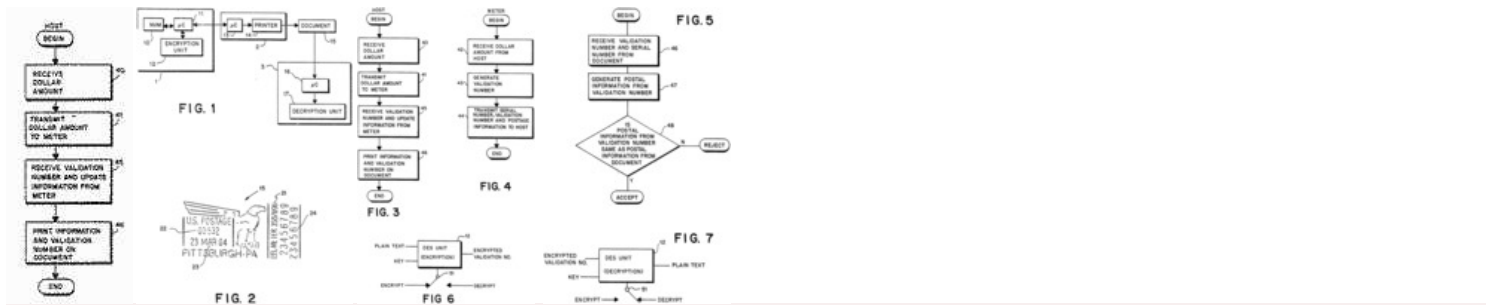
17.	Telephony system and method with enhanced call monitoring , recording and retrieval	US7881446	2005-09-02	CONFINEMENT TELEPHONY TECHNOLOGY* GUMBINER ESQ KENNETH J GUMBINER KENNETH J GUMBINER KENNETH J ESQ KENNETH J GUMBINER ESQ	2011-02-01 2011-02-01
-----	--	-----------	------------	---	-----------------------

Inmate communications systems provide a feature-rich platform with a high degree of flexibility and security employing **call** control facilities located of institutional premises. Authentication processes for calling and called party verification include biometric techniques in some embodiments. Distributed processing of **call** control and billing provide flexible interactive **call** payment processes. Preferred embodiments feature voice over IP transmission and control featuring controlled access to avoid addition of unauthorized third-party **call** participants. **Monitoring**, recording and selective forwarding of calls is provided under control of system administrators.

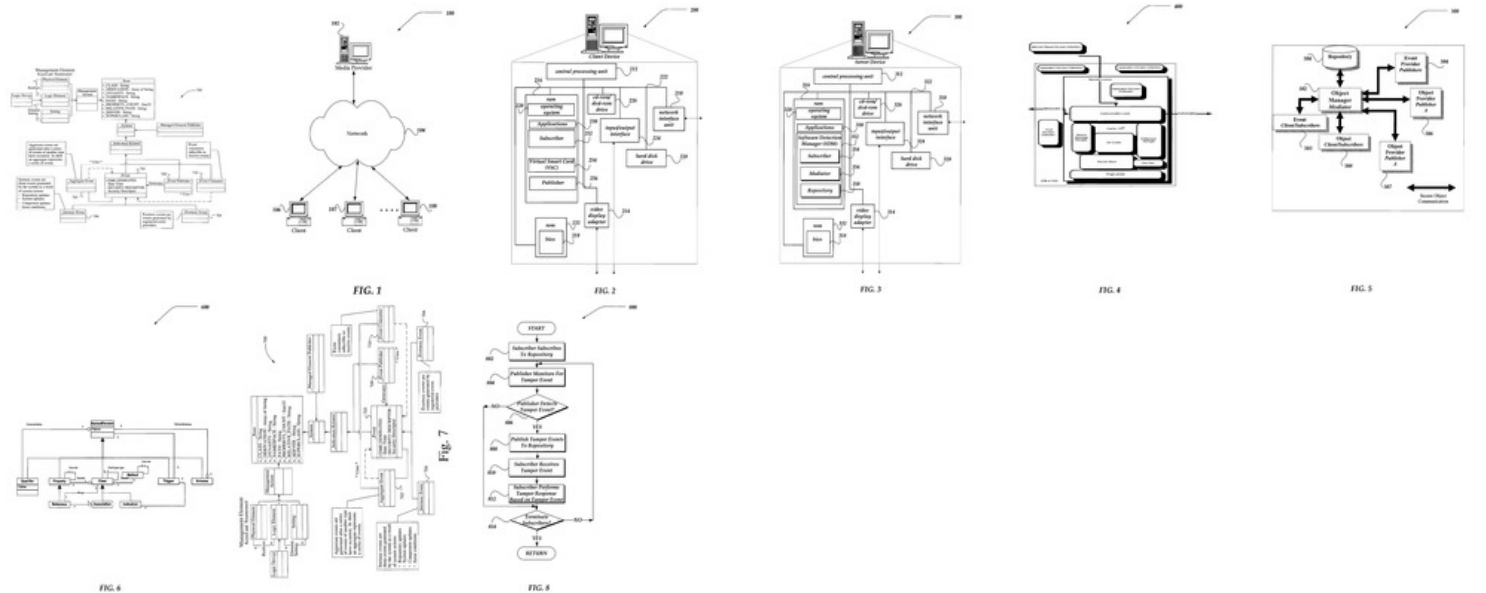


18.	System for detecting unaccounted for printing in a value printing system	IT8647901	1985-04-17	PITNEY BOWES*	1986-04-17 1986-04-17
-----	--	-----------	------------	---------------	-----------------------

A system for detecting **fraudulent** imprints on documents is disclosed. The system comprises a metering device, a host and a verifying facility. The metering device provides a validation signal to the host and its associated printer. Thereafter, the printer prints information which includes information from the validation signal. Thereafter the information printed on a mailpiece can be validated at the verifying facility by detecting the validation information provided by the metering device. The system provides a method to make a secure metering device without an integral printer. This value printing system provides for a secure system that will allow for the detection of **fraudulent** imprints at a verifying facility.



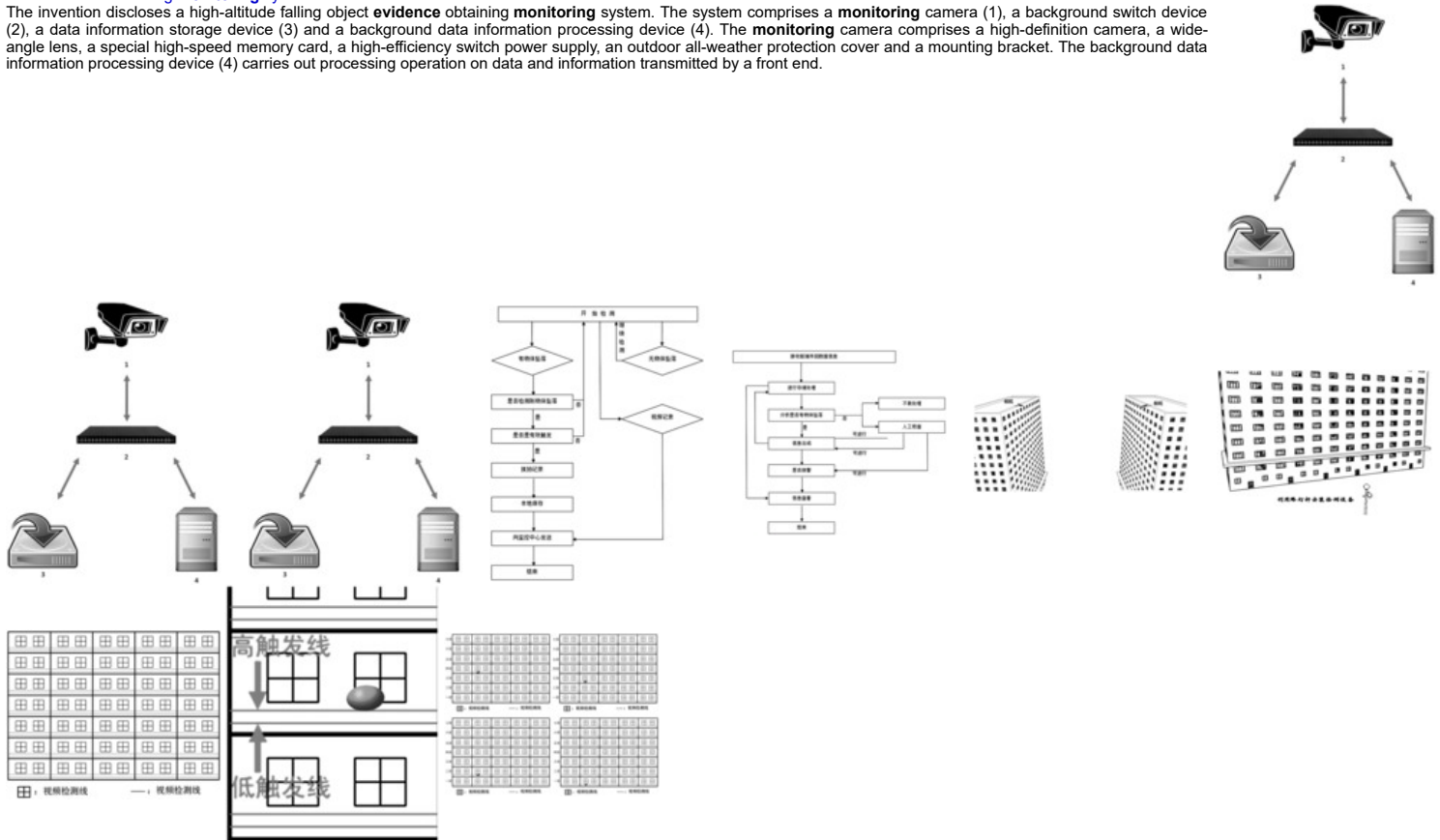
A system, apparatus, and method are directed to providing digital copyprotection of media using a subscriber/publisher architecture. In one embodiment, a publisher employs various dynamic and/or static tamper detection, including, filter graph change detectors, ICE detectors, screen scraping detectors, debugger detectors, pattern recognizers, or the like. When a tampering event is detected by one or more of the publishers, the tamper event may be published for access by a subscriber. Published tamper events may be pushed to or pulled by the subscribers. When one or more subscribers receive the tamper event, the subscribers may perform one or more tamper response actions according to various business rules, and/or other core rules.



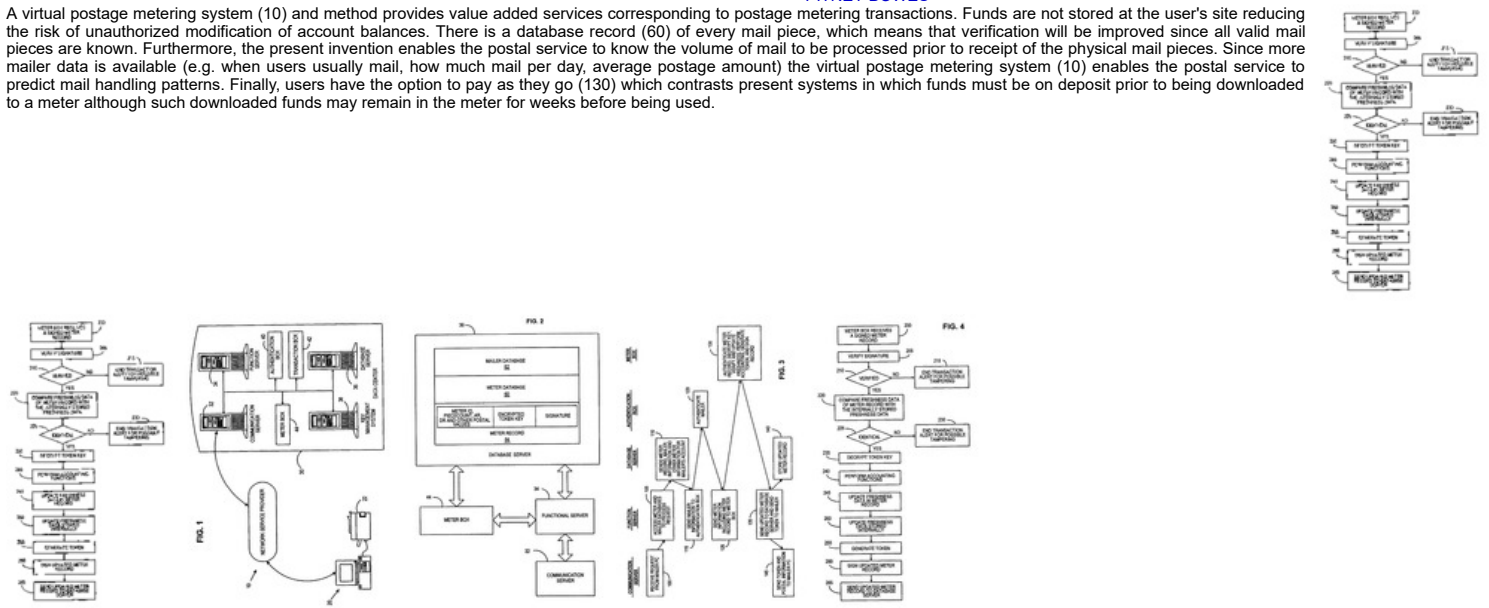
The present invention provides an electronic information system and a method thereof, and constructs two sets of subsystems of field data collecting and indoor data processing. The field data collecting system is based on a Mobile GIS platform and is combined with GPS positioning, GPRS network, bluetooth communication, etc. The field data collecting system realizes high-precision positioning of earth **monitoring**, uses different methods for executing difference positioning, digital information collecting, eraser list constructing, photograph taking/camera shooting **evidence** obtaining and terrainhyperlinking for realizing electronic information of field land surveying at the state with/without VRS network. The indoor data processing system is based on SuperMap GIS developing platform and Browser/Server structure, and is combined with XML data interchange, spatial geographical coordinate projection switching, overlapping analyzing, etc. The indoor data processing system realizes multiple functions of indoor multi-source map data expression and operation, combined inquiry, report generation, land **monitoring** database updating, property formwork customizing, etc., and realizes electronicinformation of indoor land **monitoring** operation.



The invention discloses a high-altitude falling object **evidence obtaining monitoring system**. The system comprises a **monitoring camera** (1), a background switch device (2), a data information storage device (3) and a background data information processing device (4). The **monitoring camera** comprises a high-definition camera, a wide-angle lens, a special high-speed memory card, a high-efficiency switch power supply, an outdoor all-weather protection cover and a mounting bracket. The background data information processing device (4) carries out processing operation on data and information transmitted by a front end.



A virtual postage metering system (10) and method provides value added services corresponding to postage metering transactions. Funds are not stored at the user's site reducing the risk of unauthorized modification of account balances. There is a database record (60) of every mail piece, which means that verification will be improved since all valid mail pieces are known. Furthermore, the present invention enables the postal service to know the volume of mail to be processed prior to receipt of the physical mail pieces. Since more mailer data is available (e.g. when users usually mail, how much mail per day, average postage amount) the virtual postage metering system (10) enables the postal service to predict mail handling patterns. Finally, users have the option to pay as they go (130) which contrasts present systems in which funds must be on deposit prior to being downloaded to a meter although such downloaded funds may remain in the meter for weeks before being used.



The invention discloses an off-site vessel violation **evidence** collection system which comprises a radar antenna and receiver unit, a radar video processing unit, a VTS (vessel traffic service) display unit, an AIS (automatic identification system) base station, an AIS base station data processing unit, an AIS display unit, a data acquisition unit, and a VTS and AIS data integrated display unit. The radar antenna and receiver unit, the VTS display unit and the data acquisition unit are all connected with the radar video processing unit. The AIS base station, the AIS display unit and the data acquisition unit are all connected with the AIS base station data processing unit. The data acquisition unit is connected with the VTS and AIS data integrated display unit. The off-site vessel violation **evidence** collection system enables punishment for violating vessels to be electronic, deterrence of maritime control is further increased, and vessels are safer.

