Subject Matter Eligibility Examples: Business Methods

The following examples should be used in conjunction with the *2014 Interim Guidance on Subject Matter Eligibility* (2014 IEG) and the follow-on guidance. As the examples are intended to be illustrative only, they should be interpreted based on the fact patterns set forth below. Other fact patterns may have different eligibility outcomes. While some of the fact patterns draw from U.S. Supreme Court or U.S. Court of Appeals for the Federal Circuit decisions, each of the examples shows how claims should be analyzed under the 2014 IEG. All of the claims are analyzed for eligibility in accordance with their broadest reasonable interpretation. Citations for the cases discussed in these examples are provided in the chart of court decisions available on the Office's website.

Note that the examples herein are numbered consecutively beginning with number 34, because 33 examples were previously issued.

34. System for Filtering Internet Content

The following was a claim found eligible by the Federal Circuit in BASCOM Global Internet v. AT&T Mobility LLC, 119 USPQ2d 1236 (Fed. Cir. 2016) (BASCOM). The patent at issue is U.S. Patent No. 5,987,606. As the claim in this example is eligible, no written analysis would be provided in an Office action. Claim 1 is directed to an abstract idea and has additional elements that amount to significantly more than the abstract idea because they add specific limitations other than what are well-understood, routine, conventional activities in the field and result in an improvement to the technology of filtering content on the Internet. The court's rationale for eligibility is explained below in the context of the 2014 IEG.

Background

Applicant has invented a system for filtering content from an Internet computer network by an Internet Service Provider (ISP) server using individual controlled access network accounts. At the time of applicant's invention in 1997, there was a need to block access to certain web sites for certain end users. For example, a corporation may want to allow access to certain technical or business sites, while blocking access to certain entertainment sites, and a parent may seek to block access by their children to certain objectionable sites.

Previous systems controlled access to content received by client machines over the Internet by filtering the information available using "black-listing" (*i.e.*, preventing access to all web sites on a predetermined list of web sites), "white-listing" (*i.e.*, allowing access to all web sites that are on a predetermined list of web sites), or word-screening or phrase-screening (*i.e.*, preventing access to a web page that contains any word or phrase on a predetermined list). Initially, the filtering software was placed on a client computer. However, this configuration suffered from several disadvantages because the end user could modify or work around the filtering software, the difficulty and time to install on each client computer was great, each client computer required configuration of the software based on its hardware and operating system, and a database storing the allowed or disallowed websites needed to be frequently updated. To overcome the disadvantages of installing the filtering software on a client computer, the filtering software was placed on a local server. In this configuration, client computers on a local area network connected to the Internet through a local server. If an end user on a client computer requested a website on the Internet, the local server would filter all requests for Internet content. This approach suffered from similar disadvantages including being limited to one set of filtering criteria, time-consuming installation and maintenance, and the filtering software being tied to one local area network or local server platform. Finally, ISPs used a server-based configuration in which a filter was installed on their remote servers to prevent

subscribers from accessing certain websites. However, this configuration only allowed for a single set of filtering criteria for all of the subscriber's end users.

In the instant application, applicant's system improves upon the prior art filtering systems by providing a system for filtering Internet content by subscribers on an individually customizable basis. An ISP server stores a filtering scheme in memory and a database of a plurality of sets of filtering elements associated with individual end users. The filtering scheme is executable code, including object code, interpreted code (*e.g.*, Java™ or Javascript™), other high-level code, or a combination thereof. The ISP server associates an end user account with a set of filtering elements from a plurality of filtering elements (*e.g.*, a master list of words or phrases that are not allowed) and one or more filtering schemes (*e.g.*, a word-screening type or phrase-screening type filtering scheme).

In applicant's system, the ISP server receives a log-in request from an end user. After verifying the identity of the end user, the ISP server determines the filtering scheme and filtering elements associated with the end user based on the end user account. The ISP server then receives a request to access a website from the end user and identifies the particular website requested. The ISP server implements the filtering scheme associated with the end user account utilizing the customized filtering elements that are associated with the end user account. The ISP server then determines whether the filtering scheme authorizes the request. If the request is authorized, it is processed and forwarded to the Internet. If it is not authorized, the ISP server provides a rejection notice to the end user.

In one embodiment, a request to access the Internet from an end user is partially processed while the ISP server monitors the content for certain words or phrases using the filtering scheme (*e.g.*, a word-screening or phrase-screening scheme). In this embodiment, the ISP server stores a table of logged-in end users associated with the filtering scheme. The request for Internet access is forwarded directly to the Internet. The ISP server then monitors all data packets transmitted to the ISP server to determine which packets will be forwarded to the end users stored in the table. If a data packet is being sent to a user stored in the table, the ISP server screens the packet based on the filtering scheme and filtering elements associated with that end user's account. If the data packet(s) match the filtering elements of the filtering scheme, such as by containing specific words or phrases, the transmission of the data packet(s) to the user is terminated.

Representative Claim

1. A content filtering system for filtering content retrieved from an Internet computer network by individual controlled access network accounts, said filtering system comprising:

a local client computer generating network access requests for said individual controlled access network accounts;

at least one filtering scheme;

a plurality of sets of logical filtering elements; and

a remote ISP server coupled to said client computer and said Internet computer network, said ISP server associating each said network account to at least one filtering scheme and at least one set of filtering elements, said ISP server further receiving said network access requests from said client computer and executing said associated filtering scheme utilizing said associated set of logical filtering elements.

Analysis

Claim 1: Eligible

The claim recites a local client computer and a remote ISP server that implements at least one filtering scheme and a plurality of sets of logical filtering elements. The system comprises a device or set of devices and, therefore, is a machine, which is a statutory category of invention (*Step 1: YES*).

The claim is then analyzed to determine if the claim is directed to a judicial exception. The claim recites a system for filtering content retrieved from an Internet computer network, which generates access requests for individual accounts, associates each account with at least one filtering scheme and at least one set of filtering elements from a plurality of sets of filtering elements, receives the access requests, and executes the associated filtering scheme utilizing the associated set of filtering elements. Thus, the focus of the claim and its character as a whole is on the idea of filtering content, which is implemented by a system that uses computer and networking components.

Filtering content is according to the court a "method of organizing human behavior" that is similar to other concepts that have been identified as abstract by the courts, such as tracking financial transactions to determine whether they exceed a pre-set spending limit in *Intellectual Ventures I v. Capital One Bank;* 1) collecting data, 2) recognizing certain data within the collected data set, and 3) storing that recognized data in a memory in *Content Extraction;* and organizing information through mathematical correlations in *Digitech*. Therefore, it is reasonable to conclude based on the similarity of the idea described in this claim to several abstract ideas found by the courts that claim 1 is directed to an abstract idea (*Step 2A: Yes*).

This conclusion is not altered by *Enfish*, where the Federal Circuit stated that certain claims directed to improvements in computer-related technology, including claims directed to software, are not necessarily abstract (*Step 2A*). Unlike the claims in *Enfish*, claim 1 is not clearly directed to an improvement in computer-related technology (*e.g.*, computer functionality). Thus, because it is not readily apparent that claim 1 is directed to a non-abstract idea under *Step 2A*, it is necessary to analyze the additional elements in claim 1 under *Step 2B*.

It is noted, however, that the Federal Circuit in BASCOM described claim 1 as presenting a "close call" as to what it is directed to. Thus, if an examiner skilled in this art recognizes that the claim is directed to an Internet-centric problem, for example, or clearly to an improvement in the computer technology of filtering, it would be appropriate to find that the claim, while "involving" an abstract idea is not "directed" to that idea standing alone, thus ending the analysis with a finding of eligibility at Step 2A.

Under *Step 2B*, the claim as a whole is analyzed to determine whether any element, or combination of elements, is sufficient to ensure the claim amounts to significantly more than the abstract idea. The claim recites the additional limitations of 1) controlled access network accounts, 2) a local client computer to generate network access requests for the controlled access network accounts, 3) an Internet computer network, and 4) a remote ISP server coupled to the client computer and the Internet computer network. The remote ISP server associates each account with at least one filtering scheme and at least one set of filtering elements from a plurality of sets of filtering elements, receives the access requests, and executes the associated filtering scheme utilizing the associated set of filtering elements. The local computer, ISP server, Internet computer network, and controlled access network account are generic computer and networking components performing generic computer and networking functions at a high level of generality. As the Federal Circuit determined, these limitations do not amount to significantly more when "taken individually, [because they] recite generic computer, network and Internet components, none of which is inventive by itself."

However, the analysis under *Step 2B* (also called the "inventive concept inquiry") requires more than determining that each additional claim element – the controlled access network accounts, a local

client computer, an Internet computer network, and a remote ISP server – is well known by itself. Here, an inventive concept can be found in the unconventional and non-generic ***combination*** of known elements, and more specifically "the installation of a filtering tool at a specific location, remote from the end-users, with customizable filtering features specific to each end user" where the filtering tool at the ISP is able to "identify individual accounts that communicate with the ISP server, and to associate a request for Internet content with a specific individual account." The Federal Circuit also determined that the claimed arrangement of elements in the system results in an improvement in the technology of filtering content on the Internet, because it offers "both the benefits of a filter on the local computer, and the benefits of a filter on the ISP server."

Further, these limitations confine the abstract idea to a particular, practical application of the abstract idea and, as explained in the specification, this combination of limitations is not well-understood, routine or conventional activity. Unlike the claimed system, previous content filtering systems were able to be modified by end users when the systems were located on local client computers rather than on the ISP server and were dependent on hardware and software on the local computer, or limited to a configuration based on the particular local client computer, local server, or ISP server. In addition, these limitations do not simply recite an instruction to apply the abstract idea of filtering content on the Internet or to perform the abstract idea on a generic set of computers. Instead, the claim recites a "technology-based solution" of filtering content on the Internet that overcomes the disadvantages of prior art filtering systems. Thus, when viewed as an ordered combination, the claim limitations amount to significantly more than the abstract idea of content filtering (*Step 2B: Yes*). The claim is patent eligible.

In practice, if an examiner believes the record would benefit from clarification, remarks could be added to the Office action or reasons for allowance indicating that the claim recites the abstract idea of filtering content. However, the claim is eligible because analyzing the claim limitations as an ordered combination demonstrates that the claim is a particular application of and an improvement to the technology of filtering content on the Internet, rather than well-understood, routine, conventional activity or a simple instruction to apply the abstract idea of filtering content on the Internet or to perform the abstract idea on a generic set of computers.

Additional explanation of prior decisions from *BASCOM*

The following discussion of case law is informative regarding the reasoning that led the court in *BASCOM* to hold claim 1 patent-eligible. It may be useful to examiners to recognize the similarities and differences as identified by the Federal Circuit between claim 1 and the claims at issue in *DDR*, *OIP, Intellectual Ventures I*, *Content Extraction*, *Ultramercial*, and *Accenture*. A discussion of the case law to this extent is not required during examination.

In *DDR*, the claimed invention solved the problem of retaining potential customers on a website by "sending the viewer to a hybrid webpage that combined visual elements of the first website with the desired content from the second website that the viewer wished to access." The claimed invention in *DDR* was not a "business method *per se*." Similarly, even though claim 1 in *BASCOM* was "engineered in the context of filtering content," claim 1 is not simply directed to the abstract idea of filtering content applied to the Internet, *i.e.*, abstract idea + "apply it". Instead, claim 1 recites a "technology-based solution" of filtering content on the Internet that overcomes the problems in the prior art with other Internet content filtering systems rather than "an abstract-idea-based solution" (*i.e.*, a solution "implemented with generic technical components in a conventional way").

In contrast, in *OIP*, the claims were directed to the performance of the abstract idea of price optimization on generic computer components using conventional computer functions. In other words, the claimed invention was "simply the generic automation of traditional price-optimization

techniques" and was not a "technology-based solution" of the abstract idea. Claim 1 of *BASCOM* presents a "technology-based solution" of filtering content on the Internet that overcomes the problems in the prior art with other Internet content filtering systems as discussed above.

Finally, the claims in *Intellectual Ventures I*, *Content Extraction*, *Ultramercial*, and *Accenture* are directed to an abstract idea performed on generic computer components, "without providing a specific technical solution beyond simply using generic computer concepts in a conventional way." In *Intellectual Ventures I*, the claims were directed to the abstract idea of tracking financial transactions to determine whether they exceed a pre-set spending limit simply implemented on a generic computer and the Internet. In *Content Extraction*, the claims were directed to the abstract idea of collecting data, recognizing certain data within the collected data set, and storing that recognized data in a memory performed on generic scanning devices and computers. In *Ultramercial*, the claims were directed to the abstract idea of using advertising as an exchange or currency on the Internet. And finally, the claims in *Accenture* were directed to the abstract idea of generating rule-based tasks for processing an insurance claim using generic computer components performing conventional activities. Unlike the claims in *Intellectual Ventures I*, *Content Extraction*, *Ultramercial*, and *Accenture*, claim 1 of *BASCOM* is not simply directed to the abstract idea of filtering content on the Internet or on generic computer components performing conventional activities. Instead, claim 1 "carve[s] out a specific location for the filtering system (a remote ISP server) and require the filtering system to give users the ability to customize filtering for their individual network accounts."

35. Verifying A Bank Customer's Identity To Permit An ATM Transaction

The following fact pattern and claims are hypothetical. Assume that the claims are presented in a recently filed application that is under examination and thus each claim is given its broadest reasonable interpretation in view of the specification as it would be understood by one of ordinary skill in the art. In this example, the terms in the claim are given their plain meaning in the art because no special definitions have been set forth in the specification. An abbreviated version of the hypothetical specification is provided below. Claim 1 is ineligible, because it is directed to an abstract idea and does not recite additional elements that amount to significantly more. Claims 2 and 3 are directed to the same abstract idea, but are eligible because they have additional elements that amount to significantly more than the abstract idea (i.e., provide an inventive concept) because they implement the abstract idea with specific meaningful limitations.

Background

Financial institutions routinely provide automated teller machines (ATMs) for customers to conduct banking transactions at convenient locations other than brick-and-mortar banks, and without the need to interact with a bank teller. Typical ATMs include a customer interface with a keypad, function key, display, outlet slot for statements or other information, cash dispenser slot, deposit inlet, and often a speaker to provide customer voice guidance and a camera to monitor transactions. A reader is provided for customers to present data bearing records, which can include data corresponding to the customer, financial accounts, or other data, and are commonly embodied as a bank card with a magnetic strip or a contactless card with a radio frequency identification (RFID) tag. Other input devices, such as a biometric reader to receive customer identifying inputs such as fingerprints, iris scans, and face topography data, a camera, or speech recognition device, used to identify a user can be provided as well. The customer interface is coupled to a controller with a processor and memory and a network communicator to enable communication between the controller and a financial institution to exchange information about the transactions. To conduct a transaction, a customer typically inserts a bank card into the appropriate slot in the ATM and inputs a personal identification

number (PIN) that verifies that the user is an authorized user for the bank account associated with the bank card. The account data is read from the card using the reader in the ATM and the PIN associated with the card. The network communicator transmits the read data and PIN to a remote computer at the financial institution, which then transmits instructions back to the ATM regarding authorization to carry out the requested transaction.

Due to its speed and convenience, the use of ATMs to conduct banking business has become ubiquitous, but so have problems with theft and fraud. For example, if another person illegally or fraudulently obtains a user's PIN, that person can gain access to funds in the account. Another problem associated with ATMs is "skimming" where a false card reader that appears to be a legitimate reader is affixed to an ATM to obtain an authorized user's account information and PIN. In skimming operations, an authorized user unwittingly presents their bank card to the skimming device on the ATM and enters their PIN, which is then captured and stored for subsequent fraudulent activity.

There have been various solutions attempting to reduce the instance of fraud associated with ATMs and to improve security when verifying an authorized user. For example, some bank cards are provided with chips that interact with a special reader to generate a unique transaction number each time a transaction is conducted to reduce the chance that a user's account information and PIN can be stolen for later use (so-called "chip and pin" cards). Bank cards have also been outfitted with RFID tags or "smart labels" (non-contact transponders) that allow account information to be transmitted to an ATM without inserting the card into the machine, and thus exposing it to theft or skimming. The smart label can contain various types of customer information, including profile data, preferences, and unique customer identification data. To conduct a transaction using such a contactless card, the customer brings the card into range of an ATM reader, which uses radio frequencies to interrogate the smart label to receive information about the customer. The interrogation can be encrypted to provide additional security. The customer can then start a transaction, *e.g.*, by pressing an enter key on the ATM. While such cards can prevent fraud based on skimming, these non-contact cards have given rise to other security issues, such as allowing a malicious person to obtain card information by use of an unauthorized RFID reader.

Applicant has invented a method of ensuring secure transmission of data from a card using a smart label and encryption techniques. The invention leverages the wide-spread use of mobile personal communication devices (smart phones) to facilitate the secure transmission. When a customer is issued a bank card with a smart label, the financial institution also provides a downloadable software application to the customer to install on their mobile communication device. The software application is designed to assist communication with a specially outfitted ATM.

The ATM in accordance with this invention includes a controller that is programmed with a time-variant random code generator. The code generator generates a random code when activated in response to the reader receiving data from the customer's bank card. In other words, when the customer is within a certain range of the ATM with their bank card, the smart label is read from the RFID reader in the ATM, which signals the code generator to generate a time-variant random code, which can be a plurality of digits, numbers and/or letters. The ATM then provides the random code to the customer. In one embodiment, the ATM provides the random code by displaying it. The customer is prompted to enter the displayed code into their mobile device, which already has the institutional software installed. In another embodiment, the random code is transmitted by the ATM to the customer's mobile device, *e.g.*, by a near-field communication or Bluetooth link, if the customer has installed the institutional software on their mobile device and registered their mobile device with the institution.

The software provided by the institution generates data in response to the random code, which may be, *e.g*., a customer confirmation code or an encryption that includes the code data and the card's data. The software then causes the mobile device to communicate the responsive data to the ATM. In one embodiment, the mobile device displays the encrypted data as an image on its display screen. The image can be machine readable data in the form of a bar code or an image such as a colored pattern. The customer is prompted to allow the ATM to scan the image displayed by the mobile device. The reader of the ATM reads the encrypted image and verifies that it is authentic by, for example, determining if it is readable, recognizable, or properly formatted. Once verified, the processor in the ATM decrypts the data and confirms that the decrypted code matches the random code that was generated for the current transaction session. In another embodiment, the customer confirmation code is obtained by the ATM (*e.g*., by transmission over near-field communication or Bluetooth link), and the ATM then confirms that the customer confirmation code matches the random code. The outcome of the comparison between the responsive code data (*e.g*., the decrypted code or the customer confirmation code) and the random code is used to control access to the keypad. In particular, if the responsive code data and the generated code match and the elapsed time is within a certain time frame, the transaction is continued in conventional fashion with the customer entering a PIN using the keypad. If the responsive code data and generated code do not match or the elapsed time exceeds the time frame, a signal is sent to lock the keypad so that any attempts at entering a PIN will be futile.

Applicant's method allows the ATM to receive user card data in a more secure and efficient manner. Customer card data entry begins before PIN entry and verification, so if the ATM user is not the authorized customer and does not have the appropriate verification software on their mobile device, the transaction is concluded before entry of the PIN. This method prevents skimming and other techniques to fraudulently obtain a customer's PIN and even theft of the card since the downloaded software can authenticate the user and likewise authenticate the ATM before the PIN is produced.

Claims

1. A method of conducting a secure automated teller transaction with a financial institution by authenticating a customer's identity, comprising the steps of:

obtaining customer-specific information from a bank card,

comparing, by a processor, the obtained customer-specific information with customer information from the financial institution to verify the customer's identity, and

determining whether the transaction should proceed when a match from the comparison verifies the authenticity of the customer's identity.

2. A method of conducting a secure automated teller transaction with a financial institution by authenticating a customer's identity, comprising the steps of:

obtaining customer-specific information from a bank card,

comparing, by a processor, the obtained customer-specific information with customer information from the financial institution to verify the customer's identity, by

generating a random code and transmitting it to a mobile communication device that is registered to the customer associated with the bank card,

reading, by the automated teller machine, an image from the customer's mobile communication device that is generated in response to receipt of the random code, wherein the image includes encrypted code data,

decrypting the code data from the read image, and

analyzing the decrypted code data from the read image and the generated code to determine if the decrypted code data from the read image matches the generated code data, and

determining whether the transaction should proceed when a match from the analysis verifies the authenticity of the customer's identity.

3. A method of conducting a secure automated teller transaction with a financial institution by authenticating a customer's identity, comprising the steps of:

obtaining customer-specific information from a bank card,

comparing, by a processor, the obtained customer-specific information with customer information from the financial institution to verify the customer's identity, by

generating a random code and visibly displaying it on a customer interface of the automated teller machine,

obtaining, by the automated teller machine, a customer confirmation code from the customer's mobile communication device that is generated in response to the random code, and

determining whether the customer confirmation code matches the random code, and

automatically sending a control signal to an input for the automated teller machine to provide access to a keypad when a match from the analysis verifies the authenticity of the customer's identity, and to deny access to a keypad so that the transaction is terminated when the comparison results in no match.

Analysis

Claim 1: Ineligible

The claim recites a method of conducting a secure automated teller transaction comprising a series of steps. Thus, the claim is directed to a process, which is a statutory category of invention (*Step 1: Yes*).

The claim is then analyzed to determine if the claim is directed to a judicial exception. The claim recites the steps of obtaining customer-specific information, comparing the obtained customer-specific information with customer information from the financial institution to authenticate the customer's identity, and determining whether the transaction should proceed when a match from the comparison verifies the authenticity of the customer's identity. These steps describe a method of fraud prevention by verifying the authenticity of the customer's identity prior to proceeding with a banking transaction, which is a "long prevalent" business practice that bank tellers have used for many years. Fraud prevention by verifying the identity of the customer is as fundamental to business as the economic concepts that were identified as abstract ideas by the Supreme Court, such as intermediated settlement (*Alice Corp.*) and risk hedging (*Bilski*). The claim as a whole is also similar to the claimed invention in *CyberSource*, which the Federal Circuit described as directed to an abstract mental process for detecting fraud by obtaining and comparing intangible data pertinent to business risks. The method of claim 1 similarly recites steps of obtaining and comparing data pertinent to business risks. More particularly, it describes a method of fraud prevention by authenticating a customer's identity. Therefore, claim 1 is directed to an abstract idea (*Step 2A: Yes*).

Next, the claim as a whole is analyzed to determine whether any element, or combination of elements, is sufficient to ensure the claim amounts to significantly more than the abstract idea. In addition to the steps that describe the abstract idea of preventing fraud through verifying a customer's identity, the claim recites the additional limitation of obtaining customer-specific information from a bank card. This additional element taken individually represents a conventional action of an ATM, as evidenced by the discussion of the prior art in the background specification. Further, the step is recited at a high level of generality such that it amounts to insignificant pre-solution activity, *e.g.*, a mere data gathering step necessary to use the abstract idea. The claim also recites the additional element of a processor comparing data. This processor is no more than a generic computer component, and the comparison performed by the processor does not represent any computer function beyond what processors typically perform. Taken individually therefore, the additional elements of claim 1 do not provide significantly more, *i.e.*, an inventive concept, to the claim.

Looking at the combination of elements in claim 1 also fails to show an inventive concept. Unlike the eligible claims in *Diehr* and *Bascom*, in which the elements limiting the exception were individually conventional but taken together provided an inventive concept because they improved a technical field, the claim here does not invoke any of the considerations that courts have identified as providing significantly more than an exception. The combination of elements is no more than the sum of their parts, and provides nothing more than mere automation of verification steps that were in years past performed mentally by tellers when engaging with a bank customer. Mere automation of an economic business practice does not provide significantly more (*i.e.*, provide an inventive concept). For these reasons, claim 1 is ineligible (*Step 2B: No*).

A rejection of claim 1 should identify the abstract idea by pointing to the language of the claim that describes fraud prevention by identity verification (*i.e.*, obtaining customer information, comparing the obtained customer information to customer information from a financial institution, and determining whether the transaction should proceed when a match from the comparison verifies the authenticity of the customer's identity) and explaining that fraud prevention by identity verification is similar to concepts that courts have previously found abstract. The rejection should identify the additional limitations regarding obtaining customer-specific information from a bank card and a processor that compares data, and explain why those limitations are conventional or are only generic computer components performing generic functions and are mere automation of economic business practices.

Claim 2: Eligible

The claim recites a method of conducting a secure automated teller transaction comprising a series of steps. Thus, the claim is directed to a process, which is a statutory category of invention (*Step 1: Yes*).

The claim is then analyzed to determine if the claim is directed to a judicial exception. Claim 2 recites steps of obtaining customer-specific information, comparing the obtained customer-specific information with customer information from the financial institution to authenticate the customer's identity, and determining whether the transaction should proceed when a match from the analysis verifies the authenticity of the customer's identity. Like the steps of obtaining and comparing customer information in claim 1, these steps in claim 2 describe a method of fraud prevention by identity verification before proceeding with a banking transaction, which as explained above is a fundamental business practice and is similar to ideas found abstract by the courts. Therefore, claim 2 is directed to an abstract idea (*Step 2A: Yes*).

Next, the claim as a whole is analyzed to determine whether any element, or combination of elements, is sufficient to ensure the claim amounts to significantly more than the abstract idea. In addition to

the steps that describe the abstract idea of preventing fraud through identity verification, the claim recites the additional limitations of obtaining customer-specific information from a bank card, a processor comparing data, generating a random code and transmitting it to the customer's mobile communication device, and the processor reading an image that was generated by the customer's mobile communication device in response to receipt of the random code, where the image includes encrypted code data. The encrypted code data from the image is then used by the processor to verify the customer's identity by decrypting the code data and analyzing the decrypted code data. Considered individually, the steps of obtaining information from a bank card and the comparing data do not provide significantly more for the same reasons as in claim 1. Similarly, the processor and the mobile communication device are recited at a high level of generality and perform programmed functions that represent conventional and generic operations for these devices, including reading data, generating random codes, and analyzing data.

However, the ***combination*** of the steps (*e.g.*, the ATM providing a random code, the mobile communication device's generation of the image having encrypted code data in response to the random code, the ATM's decryption and analysis of the code data, and the subsequent determination of whether the transaction should proceed based on the analysis of the code data) operates in a non-conventional and non-generic way to ensure that the customer's identity is verified in a secure manner that is more than the conventional verification process employed by an ATM alone. In combination, these steps do not represent merely gathering data for comparison or security purposes, but instead set up a sequence of events that address unique problems associated with bank cards and ATMs (*e.g.*, the use of stolen or "skimmed" bank cards and/or customer information to perform unauthorized transactions). Thus, like in *BASCOM*, the claimed combination of additional elements presents a specific, discrete implementation of the abstract idea. Further, the combination of obtaining information from the mobile communication device (instead of the ATM keypad) and using the image (instead of a PIN) to verify the customer's identity by matching identification information does not merely select information by content or source, in contrast to *Electric Power,* but instead describes a process that differs from the routine and conventional sequence of events normally conducted by ATM verification, such as entering a PIN, similar to the unconventional sequence of events in *DDR*. The additional elements in claim 2 thus represent significantly more (*i.e.,* provide an inventive concept) because they are a practical implementation of the abstract idea of fraud prevention that performs identity verification in a non-conventional and non-generic way, even though the steps use well-known components (a processor and mobile communication device). Claim 2 is eligible (*Step 2B: Yes*).

While an examiner would not be required to provide an explanation of eligibility, the record would be enhanced if clarifying remarks were provided to point to the reason for eligibility. In this instance, clarification could easily be made by simply pointing to the combination of elements used in the non-conventional implementation of identity verification in the method of fraud prevention.

Claim 3: Eligible

The claim recites a method of conducting a secure automated teller transaction comprising a series of steps. Thus, the claim is directed to a process, which is a statutory category of invention (*Step 1: Yes*).

The claim is then analyzed to determine if the claim is directed to a judicial exception. Claim 3 recites steps of obtaining customer-specific information, comparing the obtained customer-specific information with customer information from the financial institution to authenticate the customer's identity, and permitting the transaction to proceed when a match from the analysis verifies the authenticity of the customer's identity, and terminating the transaction when there is no match. Like the steps of obtaining and comparing customer information in claim 1, these steps in claim 3 describe

a method of fraud prevention by identity verification before proceeding with a banking transaction, which as explained above is a fundamental business practice and is similar to ideas found abstract by the courts. Therefore, claim 3 is directed to an abstract idea (*Step 2A: Yes*).

Next, the claim as a whole is analyzed to determine whether any element, or combination of elements, is sufficient to ensure the claim amounts to significantly more than the abstract idea. In addition to the steps that describe the abstract idea of preventing fraud through identity verification, the claim recites the additional limitations of obtaining customer-specific information from a bank card, a processor comparing data, the ATM generating a random code and visibly displaying it on a customer interface, and the ATM obtaining a customer confirmation code that was generated by the customer's mobile communication device in response to the random code. The customer confirmation code is then used by the ATM to verify the customer's identity by analyzing the customer confirmation code with respect to the random code, and controlling the transaction by providing or preventing access to a keypad of the ATM based on the analysis of the code data. Considered individually, the ATM obtaining information from a bank card and the processor comparing data do not provide significantly more for the same reasons as in claim 1. Similarly, the ATM and the mobile communication device are recited at a high level of generality and perform programmed functions that represent conventional and generic operations for these devices, including reading data, generating random codes, and analyzing data.

However, the ***combination*** of the steps (*e.g*., the ATM's provision of the random code, the mobile communication device's generation of the customer confirmation code in response to the random code, the ATM's analysis of the customer confirmation code, and the ATM's subsequent sending of a control signal to provide or prevent access to the keypad of the ATM and thus allow or prevent a transaction based on the analysis of the code data sets) operates in a non-conventional and non-generic way to ensure that the customer's identity is verified in a secure manner that is more than the conventional verification process employed by an ATM alone. In combination, these steps do not represent merely gathering data for comparison or security purposes, but instead set up a sequence of events that address unique problems associated with bank cards and ATMs (*e.g*., the use of stolen or "skimmed" bank cards and/or customer information to perform unauthorized transactions). Thus, like in *BASCOM*, the claimed combination of additional elements presents a specific, discrete implementation of the abstract idea. Further, the combination of obtaining information from the mobile communication device (instead of the ATM keypad) and using the customer confirmation code (instead of a PIN) to verify the customer's identity does not merely select information by content or source, in contrast to *Electric Power,* but instead describes a process that differs from the routine and conventional sequence of events normally conducted by ATM verification, such as entering a PIN, similar to the unconventional sequence of events in *DDR*. The additional elements in claim 3 thus represent significantly more (*i.e.,* provide an inventive concept) because they are a practical implementation of the abstract idea of fraud prevention that performs identity verification in a non-conventional and non-generic way, even though the steps use a combination of well-known components (an ATM and mobile communication device). Claim 3 is eligible (*Step 2B: Yes*).

While an examiner would not be required to provide an explanation of eligibility, the record would be enhanced if clarifying remarks were provided to point to the reason for eligibility. In this instance, clarification could easily be made by simply pointing to the combination of elements used in the non-conventional implementation of identity verification in the method of fraud prevention.

36. Tracking Inventory

The following fact pattern and claims are hypothetical. Assume that the claims are presented in a recently filed application that is under examination and thus each claim is given its broadest reasonable interpretation in view of the specification as it would be understood by one of ordinary skill in the art. In this example, the terms in the claim are given their plain meaning in the art because no special definitions have been set forth in the specification. An abbreviated version of the hypothetical specification is provided below. Claim 1 is ineligible, because it is directed to an abstract idea and does not recite additional elements that amount to significantly more. Claims 2 and 3 are directed to the same abstract idea, but are eligible because they recite specific limitations other than what would be well-understood, routine, conventional activities in the field, which amount to significantly more (i.e., provide an inventive concept).

Background

Inventory management is a commercial practice involving the acquisition and monitoring of stocked goods to maintain stock levels in a business. Particularly when goods are stored in large warehouses, managing inventory requires monitoring what goods are currently in stock and where those goods are located in the warehouse in order to fulfill orders in an efficient manner. Some prior methods of tracking inventory required items of inventory to have an attached tracking device such as a RFID or GPS transmitter, but these methods were cumbersome to implement since each item needed a transmitter to be affixed and detached as the item entered and exited the warehouse. In addition, these methods could not accurately track an item if the transmitter was obscured, improperly affixed, or detached from the item. Other prior methods used imaging technology to acquire and process images to track the items of inventory, but these methods did not have much success because they used the view of a single camera to track an object and attempted to identify items solely based upon character data (such as identification codes or product names) printed on the item. Due to using the view of a single camera to track an object, it was difficult to determine an object's physical three-dimensional (3-D) location. Therefore, these methods required items that were moved to be reimaged or otherwise tracked through manual scanning or logging. Mistakes in data entry or failure to scan a moved item resulted in lost or misplaced items. Accordingly, previous attempts to implement image recognition to track items of inventory have not achieved a high rate of accuracy.

Applicant has invented a system for tracking the presence and location of items of inventory in a warehouse using an integrated camera system with computer vision technology that overcomes many of the problems in the existing technologies typically used in the industry. Applicant's system overcomes the issues relating to accurately identifying items and tracking missing items by using a high resolution video camera array with overlapping views in combination with a recognition model that uses not only the character data of the item but also contour information (*i.e.* shape) from the collected images and predictive location data. By using a combination of character and contour recognition, applicant's system greatly reduces the possibility of item misidentification and significantly improves accuracy of inventory over prior techniques that used only character information. Because the cameras in the array have overlapping views, objects can be tracked across multiple cameras and the 3-D location of the objects can be automatically reconstructed. Applicant's improvement to computer vision technology to manage inventory within existing warehouse operations thus results in more accurate inventory tracking while eliminating the need for procedures such as scanning and logging items.

In practice, the invention uses high resolution video cameras positioned to have overlapping fields of view in pre-determined locations throughout the inventory storage space. Such cameras enable the system to automatically track an item across the entire storage space and estimate its physical location. An inventory recognition model is also stored in the memory and comprises a mathematical

representation of each item of inventory handled by the particular warehouse. This model may be a Gaussian mixture model, neural network, Bayes classifier or other known pattern classifier. The model is developed using a supervised training algorithm using numerous images of each item at multiple distances and positions with respect to the camera. During training, characteristics of each item are extracted from the images including character information such as the item's name and identification code and contour information such as the shape of the item and/or the shape of the packaging for the item. The recognition model may be updated as needed when items are added or discontinued.

During operation, the video cameras capture an image sequence (*e.g.*, multiple images from one or more of the cameras) comprising overlapping images of an item, which is stored in the memory in an inventory record. The system then uses a programmed computer to extract characteristics of an item including character and contour information from the high resolution images in the image sequence using a combination of existing text and edge detection algorithms. The programmed computer uses the characteristics to form feature vectors, and then classify the item by processing the feature vectors with the inventory recognition model to determine the most likely item in the image. A positive recognition result indicates the presence of the item in the warehouse. After an item is recognized, it is tracked in real-time throughout the warehouse using a tracking algorithm that takes advantage of the overlapping camera views to confirm the location of the item (thus improving retrieval time and accuracy). Specifically, the item is tracked in the image sequence of one camera using a known method, such as Kalman filtering, and once that item enters the field of vision of a second camera, its position in the first camera's view is used to quickly locate the item in the second camera's view. The item can then be tracked similarly in the image sequence of the second and subsequent cameras. The computer then reconstructs the 3-D coordinates of the item based upon the item's location in multiple overlapping images and prior knowledge of the location and field of view of the camera(s) that are tracking the item. Finally, the computer updates the item's inventory record with the 3-D location information.

In this hypothetical scenario, computer vision technology has not been used in the manner disclosed by this inventor prior to the filing of the application.

Claims

1. A system for managing an inventory record comprising a memory and processor configured to perform the steps of:

   (a) creating an inventory record for an item of inventory comprising acquired images of the item;

   (b) adding classification data relating to the acquired images to the inventory record;

   (c) adding location data relating to each acquired image to the inventory record; and

   (d) updating the inventory record with a physical location of each item of inventory in the warehouse to thereby manage the items of inventory.

2. A system for managing an inventory record by tracking the location of items of inventory in a warehouse:

   a high-resolution video camera array, each video camera positioned at pre-determined locations with overlapping views, for acquiring at least one high-resolution image sequence of each item of inventory;

a memory and processor configured to perform the steps of:

(a) creating an inventory record for an item of inventory comprising the acquired image sequence of the item from the video camera array;

(b) adding classification data relating to the acquired image sequence to the inventory record;

(c) adding location data relating to each acquired image to the inventory record, the location data providing a position of the item of inventory in the image sequence;

(d) reconstructing the 3-D coordinates of an item of inventory using the location data from multiple overlapping images and prior knowledge of the location and field of view of the camera(s); and

(e) automatically updating the inventory record with the 3-D coordinates of each item of inventory in the warehouse to thereby manage the items of inventory.

3. A system for managing inventory by tracking the location of items of inventory in a warehouse using image recognition, comprising:

a high-resolution video camera array for acquiring at least one high resolution image sequence of each item;

a memory for storing the acquired image sequences, classification and location data relating to the acquired image sequences, and a recognition model representing contour information and character information of each item; and

a processor that is configured to manage inventory by performing, for each item, the steps of:

(a) creating an inventory record for the item comprising the acquired image sequence(s) of the item;

(b) extracting characteristics from the acquired image sequence(s) of an item to form feature vectors, the characteristics comprising contour information and character information that is stored in the inventory record as classification data relating to the acquired image sequence(s);

(c) recognizing and tracking the position of item in the image sequence as classification and location data by processing the feature vectors using the stored recognition model and adding the classification and location data to the inventory record;

(d) determining a physical location of the item in the warehouse using the location data relating to the item in the image sequence(s); and

(e) automatically updating the inventory record with the physical location of the item.

Analysis

Claim 1: Ineligible

The claim recites a system for managing an inventory record comprising a memory and a processor configured to perform a series of steps. The claimed system is a device or set of devices, which is a machine and thus a statutory category of invention (*Step 1: Yes*).

The claim is then analyzed to determine if the claim is directed to a judicial exception. The claim recites a system that performs the steps of (a)-(c) storing acquired images and related classification

and location data, and (d) updating the inventory record with the physical location of each item of inventory in the warehouse. That is, the claim describes the steps of managing inventory by creating an inventory record for each item of inventory comprising images of the item, adding classification data relating to the images to the inventory record, adding location data for each image to the inventory record, and updating the inventory record with the physical location of each item of inventory in the warehouse. The data collection, recognition, and storage concept described in the claim is similar to the data collection and management concepts that were held to be abstract ideas in *Content Extraction, TLI Communications*, and *Electric Power Group.* Although the claim enumerates the type of information (*i.e.*, the images, classification data, and location data) that is acquired, stored and analyzed, the Federal Circuit has explained in *Electric Power Group* and *Digitech* that the mere selection and manipulation of particular information by itself does not make an abstract concept any less abstract. Further, the claim is not made any less abstract by the invocation of a programmed computer. Unlike *Enfish*, where the claims were focused on a specific improvement in ***how*** the computer functioned, the claim here merely uses the computer as a tool to perform the abstract concepts. Therefore, based on the similarity of the concept described in this claim to abstract ideas identified by the courts, claim 1 is directed to an abstract idea (*Step 2A: Yes*).

Next, the claim as a whole is analyzed to determine whether any element, or combination of elements, is sufficient to ensure the claim amounts to significantly more than the abstract idea. The claim recites the additional limitations of a memory and processor to perform the steps of inventory tracking. A memory for storing data and a processor for processing data are well-understood, routine, conventional computer components, which in this claim are recited at a high level of generality and perform generic computer functions (*e.g.*, storing and processing information). Generic computer components performing generic computer functions, alone, do not amount to significantly more than the abstract idea.

Viewing the limitations in combination also fails to amount to significantly more than the abstract idea. The claimed invention seeks to record, process, and archive digital images simply, fast, and in such a way that the information may be easily tracked, but these functions reflect ordinary usage typically performed by a generic computer, as would be recognized by those of ordinary skill in the field of data processing. For example, as noted in *TLI Communications*, using a computer to attach classification data, such as dates and times, to images for purposes of storing those images in an organized manner does not add significantly more to a judicial exception. The recitation of conventional processing technology performing well-understood, routine, conventional functions such as recognizing and storing data from specific data fields does not reflect an "inventive concept." Thus, whether viewed individually or in combination, the additional limitations do not amount to a claim as a whole that is significantly more than the abstract idea (*Step 2B: No*). The claim is not patent eligible.

A rejection of claim 1 should identify the abstract idea by pointing to the language of the claim that describes inventory management and explaining that inventory management is similar to concepts that courts have previously found abstract. The rejection should identify the additional limitations regarding the memory and processor and explain why those limitations comprise only a generic computer performing well-understood, routine, conventional generic functions in the particular technological environment of image processing, for the reasons noted above.

Claim 2: Eligible

The claim recites a system comprising a video camera array, a memory and a processor. The system is a device or set of devices and therefore is a machine, which is a statutory category of invention (*Step 1: Yes*).

The claim is then analyzed to determine if the claim is directed to a judicial exception. Like claim 1, claim 2 recites a system that performs the steps of (a)-(c) acquiring and storing images and related data about items of inventory, and (e) updating the inventory record with the physical location of each item of inventory in the warehouse. Claim 2 thus describes using data collection and management techniques to practice the concept of inventory management, which as explained above is an abstract idea. Therefore, the claim is directed to an abstract idea (*Step 2A: Yes*).

Next, the claim as a whole is analyzed to determine whether any element, or combination of elements, is sufficient to ensure the claim amounts to significantly more than the abstract idea. The claim recites the additional limitations of a high-resolution video camera array at predetermined positions with overlapping views, memory and processor to (d) reconstruct the 3-D coordinates of the item of inventory from multiple overlapping images obtained from the camera array and prior knowledge of the location and field of view of the camera(s). Individually, the memory and processor limitations do not amount to significantly more for the reasons discussed above for claim 1. For example, they are still well-understood, routine, conventional devices that are used in this invention for their conventional functions of processing and storing information. Similarly, high-resolution video cameras are widely used and, in this invention, perform their typical function of acquiring image sequences.

However, the memory and processor in combination with a high-resolution video camera array with predetermined overlapping views that reconstructs the 3-D coordinates of the item of inventory using overlapping images of the item and prior knowledge of the location and field of view of the camera(s) provides significantly more than the abstract idea of using data collection techniques to manage inventory. As explained in the specification, at the time of this invention, using a high-resolution video camera array with overlapping views to track items of inventory was not well-understood, routine, conventional activity to those in the field of inventory control. In fact, the use of this camera array provides the ability to track objects throughout the entire storage space rather than simply the view of a single camera and determine their 3-D location without any of the manual steps that were required of previous methods. That is, the video camera array with reconstruction software provides the technological solution to the technological problem of automatically tracking objects and determining their physical position using a computer vision system. Like in *DDR*, the claimed solution here is necessarily rooted in computer technology to address a problem specifically arising in the realm of computer vision systems. The claimed limitations are not simply an attempt to generally link the abstract idea to the technological environment of computer vision systems. Rather, these are meaningful limitations that confine the claim to a particular useful application. Accordingly, when viewed as a combination, the additional elements thus yield a claim as a whole that amounts to significantly more than the abstract idea of inventory management (*Step 2B: Yes*). The claim is patent eligible.

If the examiner believes the record would benefit from clarification, remarks could be added to the Office action or reasons for allowance indicating that the claim recites the abstract idea of inventory management. Nevertheless, the claim is eligible because analyzing the claim elements in combination demonstrates the claim is a technology-based solution to address a problem arising in the realm of computer vision systems and is not simply limiting the abstract idea to a particular technological environment.

Claim 3: Eligible

The claim recites a system comprising one or more video cameras, memory and a processor. The system is a device or set of devices and therefore is a machine, which is a statutory category of invention (*Step 1: Yes*).

The claim is then analyzed to determine if the claim is directed to a judicial exception. Like claim 1, claim 3 recites a system that performs the steps of (a) & (c) storing acquired images and related classification and location data, and (e) updating the inventory record with the physical location of each item of inventory in the warehouse. Claim 3 thus describes using data collection and management techniques to practice the concept of inventory management, which as explained above is an abstract idea. Therefore, the claim is directed to an abstract idea (*Step 2A: Yes*).

Next, the claim as a whole is analyzed to determine whether any element, or combination of elements, is sufficient to ensure the claim amounts to significantly more than the abstract idea. The claim recites the additional limitations of a high-resolution video camera array for acquiring high resolution image sequences of items of inventory, a memory to store the acquired images, related data, and the recognition model, and a processor to perform step (b)'s extracting characteristics from the acquired images, step (c)'s recognizing and tracking the position of the item using the recognition model and step (d)'s determining a physical location of the item using the position of the item in the images. Individually, the camera array, memory and processor limitations do not amount to significantly more for the reasons discussed above for claims 1 and 2. For example, these components are used in this invention for their well-understood, routine, conventional functions of acquiring, processing and storing information.

In combination, however, the limitations do amount to significantly more than the abstract idea of inventory management. As explained in the specification, the combination of the camera array's acquisition of high resolution image sequences, and the processor's performance of step (b)'s extracting contour and character information from the images to create feature vectors, step (c)'s recognizing and tracking items of inventory using the feature vectors and a recognition model, and step (d)'s determining the physical location of the recognized items using the position of the item in the image sequence(s) is not well-understood, routine, conventional activity in this field. This combination of limitations provides a hardware and software solution that improves upon previous inventory management techniques by avoiding the cumbersome use of RFID and GPS transmitters and the inaccuracy issues that plagued previous computer vision solutions. This combination of features provide meaningful limitations to the practical application of inventory tracking with computer vision, by improving the system's ability to identify and track objects across multiple cameras in a three-dimensional space. These limitations do not simply limit the abstract idea to the technological environment of image processing, but are instead meaningful limitations that integrate the abstract idea into a particular application that uses character and contour information from high resolution images to recognize items of inventory. When viewed as a combination, the additional elements thus yield a claim as a whole that amounts to significantly more than the abstract idea of inventory management (*Step 2B: Yes*). The claim is patent eligible.

If the examiner believes the record would benefit from clarification, remarks could be added to the Office action or reasons for allowance indicating that the claim recites the abstract idea of inventory management. Nevertheless, the claim is eligible because analyzing the claim elements in combination demonstrates the claim is a particular application rather than well-understood, routine, conventional activity or simply limiting the abstract idea to a particular technological environment.