Title: DETECTION AND PREVENTION OF INMATE TO INMATE MESSAGE RELAY

Abstract: Secure system and method of detecting and preventing inmate to inmate message relays. A system and method which monitors inmate communications for similar phrases that occur as part of two or more separate inmate messages. These similar phrases may be overlapping in real time as in a conference call or can occur at separate times in separate messages. The communications that appear similar are assigned a score and the score is compared to a threshold. If the score is above a certain threshold, the communication is flagged and remedial actions are taken. If the flagged communication contains illegal matter then the communication can be disconnected or restricted in the future.
DETECTION AND PREVENTION OF INMATE TO INMATE MESSAGE RELAY

BACKGROUND

Field

[0001] The disclosure relates to a system and method of detecting and preventing illegal inmate-to-inmate communications in a controlled environment facility.

Related Art

[0002] In current prison facilities, inmates are generally permitted to communicate, using the prison's communication system, with a wide variety of individuals both inside and outside of the prison facility. As such, inmates of a particular facility may be capable of communicating with other inmates, either in their own facility, or in other facilities. Even if direct contact is prohibited, such communication can still occur via an intermediary.

[0003] There are monitoring systems and methods currently implemented in controlled environment facilities. However, the ability of inmates to communicate with other inmates presents a number of challenges that are unique to a controlled environment facility and that are not sufficiently hampered by current monitoring and control systems.

BRIEF DESCRIPTION OF THE DRAWINGS/FIGURES

[0004] Embodiments are described with reference to the accompanying drawings. In the drawings, like reference numbers indicate identical or functionally similar elements. Additionally, the left most digit(s) of a reference number identifies the drawing in which the reference number first appears.

[0005] Fig. 1A illustrates a centralized detection and prevention system connected to several controlled environment facilities, according to an embodiment of the invention;

[0006] Fig. 1B illustrates localized detection and prevention systems supporting several controlled environment facilities, according to an embodiment of the invention;

[0007] Fig. 2 illustrates a block diagram of a detection and prevention system, according to an embodiment of the invention;
Fig. 3 illustrates a block diagram of a detection and prevention analysis engine, according to an embodiment of the invention;

Fig. 4 illustrates a block diagram of a scoring module, according to an embodiment of the invention;

Fig. 5 illustrates a flowchart diagram of a method for detecting and preventing illegal communication, according to an embodiment of the invention;

Fig. 6 illustrates a flowchart diagram of a method for scoring a monitored communication, according to an embodiment of the invention; and

Fig. 7 illustrates a block diagram of a general purpose computer that may be used to perform various aspects of the present disclosure.

DETAILED DESCRIPTION

The following Detailed Description refers to accompanying drawings to illustrate exemplary embodiments consistent with the disclosure. References in the Detailed Description to "one exemplary embodiment," "an exemplary embodiment," "an example exemplary embodiment," etc., indicate that the exemplary embodiment described may include a particular feature, structure, or characteristic, but every exemplary embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same exemplary embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an exemplary embodiment, it is within the knowledge of those skilled in the relevant art(s) to affect such feature, structure, or characteristic in connection with other exemplary embodiments whether or not explicitly described.

Embodiments may be implemented in hardware (e.g., circuits), firmware, computer instructions, or any combination thereof. Embodiments may be implemented as instructions stored on a machine-readable medium, which may be read and executed by one or more processors. A machine-readable medium may include any mechanism for storing or transmitting information in a form readable by a machine (e.g., a computing device). For example, a machine-readable medium may include read only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices, or other hardware devices. Further, firmware, routines, computer instructions may be described herein as performing certain actions. However, it
should be appreciated that such descriptions are merely for convenience and that such actions in fact result from computing devices, processors, controllers, or other devices executing the firmware, routines, instructions, etc. Further, any of the implementation variations may be carried out by a general purpose computer, as described below.

For purposes of this discussion, the term "module" shall be understood to include at least one of hardware (such as one or more circuit, microchip, processor, or device, or any combination thereof), firmware, computer instructions, and any combination thereof. In addition, it will be understood that each module may include one, or more than one, component within an actual device, and each component that forms a part of the described module may function either cooperatively or independently of any other component forming a part of the module. Conversely, multiple modules described herein may represent a single component within an actual device. Further, components within a module may be in a single device or distributed among multiple devices in a wired or wireless manner.

The following Detailed Description of the exemplary embodiments will so fully reveal the general nature of the disclosure that others can, by applying knowledge of those skilled in relevant art(s), readily modify and/or adapt for various applications such exemplary embodiments, without undue experimentation, without departing from the spirit and scope of the disclosure. Therefore, such adaptations and modifications are intended to be within the meaning and plurality of equivalents of the exemplary embodiments based upon the teaching and guidance presented herein. It is to be understood that the phraseology or terminology herein is for the purpose of description and not of limitation, such that the terminology or phraseology of the present specification is to be interpreted by those skilled in relevant art(s) in light of the teachings herein.

Those skilled in the relevant art(s) will recognize that this description may be applicable to many different communications protocols.

American correctional facilities house millions of individuals in controlled environments all over the country. An ongoing problem for such correctional facilities is the ability for inmates to communicate with other inmates in order to arrange illegal activities. Such illegal activities might include a hit (e.g., orchestrated killing) on a person that is incarcerated or perhaps is part of the general public. Another example of such
illegal activities might be to arrange and organize a riot. The ability of inmates to plan and coordinate these events with other inmates over the prison communication system is a serious security concern with potentially fatal consequences.

[0019] Generally, correctional facilities restrict phone access by designating the time and place of calls permitted to the inmates. Correctional facilities also restrict phone access for inmates by permitting communication with only preapproved individuals or prohibiting inmates from dialing specific numbers. In extreme situations, correctional facilities may terminate all prison communication services for a certain period of time, particularly during a riot or other emergency situation.

[0020] Most communications made by inmates are closely monitored by correctional facilities. However, regardless of the measures taken by correctional facilities, inmates repeatedly attempt to avoid detection of suspicious communication regarding illegal activities by relaying messages to other inmates or third parties outside of the correctional facilities. For example, in some instances, an inmate may be permitted to directly contact an inmate within their own facility, or within a separate facility. This provides a direct line of communication to facilitate the coordination of criminal acts. In other instances, an inmate may call an outside third party and instruct the third party to contact another inmate in order to relay certain information. In this manner, the inmate is able to skirt the restrictions in order to effectively "communicate" with the other inmate. Thus, even without the direct line of communication, coordination can still occur via the use of the intermediary.

[0021] As illustrated by these examples, there are many unique concerns associated with monitoring the communications by inmates of a controlled facility. To further complicate matters, certain facilities may be outfitted to allow inmates to carry personal inmate devices (PIDs) and use their own personal devices, in the form of tablet computers, smartphones, etc. for personal calls, digital content streaming, among other uses.

[0022] With these concerns in mind, it is preferable to implement a system and/or method of detecting and preventing inmate-to-inmate message relays. With this objective in mind, the following description is provided for a system and method which monitors separate inmate communications for similar phrases. These similar phrases may be overlapping in real time, for example as part of a conference call, or can occur at separate times in separate communications. Communications are scored based on their similarity, and the
resulting score is compared to a threshold. If the score is above the threshold, any number of preventative measures are taken, such as flagging the communications and alerting authorities. Additional measures may include identifying whether the communications contain illegal matter and then disconnecting the communications, restricting future communications, and/or preparing countermeasures to thwart the illegal activity.

Exemplary Centralized Detection and Prevention System

[0023] Fig. 1A illustrates an exemplary centralized detection and prevention system environment 100. In the environment 100, a detection and prevention system 110 is a centralized system that is connected to one or more controlled environments 105A-C through each respective controlled environment communication system 120A-C. In an embodiment, the controlled environment communication systems 120A-C control the majority of communications coming into or leaving the respective facilities, particularly those by or for inmates within the facility. The detection and prevention system 110 may be connected through wired and/or wireless connections to the controlled environment communications systems 120A-C. In an embodiment, so as to facilitate communication with outsider third parties, the detection and prevention system 110 is connected to one or both of the PSTN 150 and the Internet 160. Each of the PSTN 150 and the Internet 160 may be connected to various communications devices, such as devices 155 and 165.

[0024] In an embodiment, the detection and prevention system 110 performs a variety of functions with respect to the communications, such as monitoring for key words and/or phrases indicative of a rules violation, recording conversations for future review by an investigator or other authorized person, as well as call control, such as disconnecting the call in response to the detection of a rules violation, alerting an official of a rules violation, etc. The function of the detection and prevention system 110 may vary depending on the time sensitivity of communications between outsider parties and inmates in the controlled environments 120A-C. For time sensitive communications, such as live telephone calls, the detection and prevention system 110 is transparent to the communication and monitors the ongoing communication until the detection and prevention system 110 detects a rule violation or until the communication ends. For non-time sensitive communications, such as emails and texts, the detection and prevention system 110 may act as a communication interceptor, withholding the communication
while it is being analyzed for a rules violation before releasing the communication (e.g., forwarding it) to the intended recipient.

In an embodiment, the controlled environment communication system 120A provides a local wireless network 130 for providing wireless communication connectivity to wireless communication devices 135A. Wireless communication devices 135A may include electronic wireless communication devices such as smart phones, tablet computers, PIDs, game consoles, and laptops, among others. In an embodiment, wired communication devices 135B are also connected to the controlled environment communication system 120A. Wired communication devices 135B may include telephones, workstations, computers, in-pod kiosks, game consoles, and fax machines, among others.

In an embodiment, communication devices outside of the controlled environment 145A-B communicate with devices within the controlled environment 105A. Wireless communication devices 145A may be connected to the controlled environment communication system 120A through a wireless network 140. In an embodiment, wired communication devices 145B are connected directly to the controlled environment communication system 120A without an intervening network.

Exemplary Localized Detection and Prevention System

Fig. 1B illustrates an exemplary localized detection and prevention system environment 100. In the environment 100, detection and prevention systems 110A-C are localized systems that are located in one or more controlled environments 105A-C. Most communications flowing in and out of controlled environments 105A-C are controlled by the controlled environment communication systems 120A-C. Most communications flowing through the controlled environment communication systems 120A-C are monitored by the localized detection and prevention systems 110A-C. The detection and prevention systems 110A-C may be connected through wired and/or wireless connection to the controlled environment communications systems 120A-C. In an embodiment, so as to facilitate communication with other controlled environments 105A-C and outsider third parties, the detection and prevention systems 110A-C are connected to one or both of the LAN and WAN 170 networks, such as the PSTN and the Internet, among others. Each of the WAN and LAN 170 networks may provide connection for various communications devices 175A-B.
Exemplary Detection and Prevention System

[0028] Fig. 2 illustrates a block diagram of a detection and prevention system 200, according to an embodiment of the invention. The detection and prevention system 200 includes at least a processing subsystem 205, a communication transceiver 210, and a database 280, and may represent an exemplary embodiment of any of the detection and prevention systems 110 illustrated in Figs. IA and IB. The processing subsystem 205 includes a communication storage 220, an image detector 225, a transcriber 230, a language converter 240, a metadata extractor 250, a detection and prevention analysis engine 260, and an alerting module 270. The database 280 includes a metadata database 282, a transcript database 284, a language dictionary 286, and a keyword database 288.

[0029] The communication transceiver 210 detects communications sent to/from the controlled environment. The communications may be time sensitive, such as phone calls or video conferences, in which case the communication transceiver 210 detects real time communications between inmates and outsider third parties. Examples of real time communications include voice calls, video conference calls, video visitation sessions, video hand messaging sessions, multi-player game sessions, among others. In another embodiment, the communication transceiver 210 detects non time sensitive communications such as, voice messages, email messages, text messages, among others. The communication transceiver 210 is connected to the processing subsystem 205 in order to further analyze the communication.

[0030] The communication storage 220 receives and stores communications detected by the communication transceiver 210, according to an embodiment of the invention. The communications are stored in the appropriate file format in which the communications have been detected by the communication transceiver 210. The communication storage 220 stores the detected communications in the appropriate file format according to the type of communication. Audio communications are stored in various uncompressed and compressed audio file formats. Exemplary audio file formats include, WAV, AIFF, FLAC, WavPack, MP3, among others. In an embodiment, communications detected by the communication transceiver 210 may be in the form of audio, video, text or other suitable formats depending on the type of communication received. Video communications are stored in various video file formats such as WMV, AVI, Quicktime,
among others. Text communications are stored in various text file formats such as TXT, CSV, DOC, among others.

The image detector 225 receives and analyzes video files stored in the communication storage 220, according to an embodiment of the invention. In order to determine whether two or more inmates are present on the same video communication, the image detector 225 captures images from the video communication and utilizes well-known 2D and 3D image recognition algorithms to determine the images of the participants. The image detector 225 compares the determined images of the video communication participants with images of inmates at the controlled environment. Upon a determination by the image detector 225 that there are two or more inmates present on the same video communication, the image detector 225 transmits a notification signal regarding the violating communication to the alerting module 270. In an embodiment, the image detector 225 can determine the presence of the same inmate on two or more simultaneous video communications made to the same phone number, IP address, or MAC address. In other words, the image detector 225 is capable of detecting a violating video communication between two or more inmates connected by each inmate separately calling the same phone number, IP address, or MAC address at the same time.

The transcriber 230 receives and transcribes audio files stored in the communication storage 220, according to an embodiment of the invention. In order to monitor the communications for rule violations, the transcriber 230 directly transcribes the audio file into a text file. The resulting text file contains the transcript of the detected communication. In an embodiment, the transcriber 230 receives and transcribes audio associated with video files stored in the communication storage 220.

The transcriber 230 performs analysis of the audio file for the transcription and annotation of speech signals by comparing the speech signals with known sound waveforms and speech signature frequencies stored in the language dictionary 286. The language dictionary 286 contains sound waveforms and speech signature frequencies for different languages. In an embodiment, the transcriber 286 can analyze an audio file containing different languages by comparing it with the sound waveforms and speech signature frequencies for the corresponding language contained in the language dictionary 286. In another embodiment, the transcriber 230 conducts voice analysis of the audio file and recognizes phonemes and/or intonations and identifies the speech as associated with
the different speakers using voice analysis techniques. In other words, the transcriber can
assign speech segments to different speakers in order to generate a dialog transcript of the
actual conversation. The transcriber 230 lists and names the different participants in the
audio file and labels the sentences in the transcript in order to indicate which speaker is
communicating in that particular portion of the transcript. The transcriber 230 transcribes
events that occur during the conversation such as long pauses, extra dialed digits,
progress tones, among others into the transcript. The transcriber 230 can conduct phonetic
transcription of the audio based on a phoneme chart stored in the language dictionary 286.

[0034] The language converter 240 receives the communications from the transcriber 230
and the communication storage 220 and converts the communications into a standard
language, according to an embodiment of the invention. As mentioned above, the
communications may be conducted in different languages. The conversion into a standard
language facilitates a more efficient and universal method of monitoring the
communications to detect rule violations. In an embodiment, the language converter 240
converts the communications into English. The language dictionary contains dictionaries
for many different languages. When the language converter 240 receives a
communication containing languages other than English, the language converter 240
searches the language dictionary 286 for the corresponding words and phrases in English
and converts the communication accordingly. Using well-known grammatical algorithms,
the language converter 240 is able to perform the language conversion without significant
grammatical errors in the converted text. The conversion results in a text file containing a
transcript of the detected communication in a standard language. In an embodiment, the
language converter 240 and the transcriber work as part of a combined system to
simultaneously perform language conversion and transcription.

[0035] The metadata extractor 250 receives the transcribed and/or converted
communication from the language converter 240 and extracts metadata from the
communication, according to an embodiment of the invention. The metadata summarizes
basic information about the communication. For example, the basic information about the
communication may include the names of the people communicating, the phone numbers
or email accounts, and the date and time of the communication, among others. The
metadata extractor 250 transmits and saves the metadata in the metadata database 282 and
the text file containing the corresponding communication in the transcript database 284.
The detection and prevention analysis engine 260 receives the communication from the metadata extractor 250 and analyzes the communication for illegal or suspicious contents, according to an embodiment of the invention. The detection and prevention analysis engine 260 analyzes the communication and compares it to past communications to detect rule violations. The detection and prevention analysis engine 260 will be described in detail in the following Figure 3.

Upon the determination of a rule violation, the detection and prevention analysis engine 260 transmits a notification signal regarding the violating communication to the alerting module 270. Subsequently, the alerting module 270 alerts responsible supervising personnel at the controlled environments 105A-C. In an embodiment, the alerting module 270 may disconnect a real time communication upon receipt of a notification signal from the detection and prevention analysis engine 260. The alerting module may withhold the transmission of the non time sensitive communication until the supervising personnel reviews and "OKs" the communication. In some embodiments, the alerting module transmits the converted transcript of the violating communication along with the notification signal.

The metadata database 282 stores the metadata extracted from most communications detected by the detection and prevention system 200, according to an embodiment of the invention. The metadata in the metadata database 282 contains basic information about the corresponding communication stored in the transcript database. Basic information about a communication may include the names of the people communicating, the numbers and accounts used, the time and date of the communication, among others. The metadata database 282 helps the detection and prevention system 200 organize the large volume of communications and provides digital identification for each communication detected by the detection and prevention system 200. The metadata database 282 supports archiving and preserving the communications detected by the system. The metadata database 282 assists with searching for previous communications in the transcript database 284 by accommodating an initial search within the metadata database 282 for past communications based on basic information such as the name of the inmates or the phone numbers used in the communication. The initial search through the metadata database 282 allows the system to narrow the search to identified past communications in the transcript database284.
The transcript database 284 contains the communications detected by the
detection and prevention system 200 in a text file format, according to an embodiment of
the invention. The communications in the transcript database 284 have mostly been
converted to a standard language and have corresponding metadata in the metadata
database 282.

The language dictionary 286 includes the language dictionaries of different types
of languages. The language dictionary 286 also includes sound waveforms and speech
signature frequencies for each respective language. For example, the language dictionary
286 may include vocabulary and phrases in Spanish, Arabic, Chinese, Japanese, Korean,
among others. The keyword database 288 includes keywords that are typically used by
controlled environments to monitor inmate communications. In an embodiment, the use
of a keyword in an inmate communication would be detected by the detection and
prevention system 200 and consequently trigger the monitoring of the communication for
an extended period of time. For example, keywords may include "kill," "drugs," and
"riot" and the detection of a key word in an inmate communication would trigger the
extended monitoring of the communication.

Exemplary Detection and Prevention Analysis Engine

Fig. 3 illustrates a block diagram of a detection and prevention analysis engine
300, according to an embodiment of the invention. The detection and prevention system
includes a signal input/output 305A-B, a keyword searching and monitoring module 310,
metadata search engine, and scoring module 330. The detection and prevention analysis
engine 300 may represent an exemplary embodiment of the detection and prevention
analysis engine 260.

The signal I/O 305A receives and transmits the communications to be analyzed by
the detection and prevention analysis engine 300. The keyword searching and monitoring
module 310 receives and searches the communication for keywords and/or phrases stored
in the keyword database 288, according to an embodiment of the invention. When a
keyword is detected, the monitoring function is triggered and the message is monitored
for an extended period of time. The monitored communication is received by the scoring
module to be compared with relevant past communications stored in the transcript
database 284. The keyword searching and monitoring module 310 reads the metadata
associated with the communication, which will be used by the metadata to the metadata
search engine 320 to conduct a search for past communications containing similar metadata. In another embodiment, the keyword searching and monitoring module 310 searches the received communication for terms and phrases that indicate contact information. Such terms and phrases may include addresses, phone numbers, email addresses, among others. For example, the keyword searching and monitoring module 310 is capable of recognizing a string of spoken numbers that resemble a phone number. Any received communication that contains an address, phone number, email address, or any other means of contacting a different party is assigned a predetermined high score.

The metadata search engine 320 receives the metadata associated with a monitored communication and conducts a search in the metadata database 282 for any overlap in the metadata for past communications, according to an embodiment of the invention. The search of the metadata database 282 identifies the relevant metadata with corresponding communication transcripts stored in the transcript database 284. The metadata search engine 320 receives the corresponding communication transcripts from the transcript database 284. The corresponding communication transcripts are provided to the scoring module 330 to be compared with the monitored communication transmitted by the keyword searching and monitoring module 310.

The scoring module 330 scores the monitored communication transmitted by the keyword searching and monitoring module 310, according to an embodiment of the invention. The scoring module compares the monitored communication with the relevant communication transcripts transmitted by the metadata search engine 320. The scoring module 330 searches and compares similar phrases contained in the monitored communication with the relevant communication transcripts. The scoring module 330 assigns a score to the monitored communication and compares the score with a predetermined threshold. If the score is higher than the threshold, the communication is flagged and a notification signal is sent to the alerting module 260. The scoring module 330 will be described in detail in the following Figure 4.

Exemplary Scoring Module

Fig. 4 illustrates a block diagram of a scoring module 400, according to an embodiment of the invention. The scoring module includes a real time communication scoring module 410, a separate communication scoring module 420, and a score
comparison module 430. The scoring module 400 may represent an exemplary embodiment of the scoring module 330.

The real time communication scoring module 410 scores real time communications by comparing similar phrases and keywords within the real time communications with relevant past communications, according to an embodiment of the invention. The real time communications scoring module 410 receives monitored communications from the keyword searching and monitoring module 310 and determines whether there are any rule violations within the real time communication. An example of a rule violation within a real time communication would be an ongoing conversation containing message relays from one inmate to another. Accordingly, the focus of the real time communication scoring module 410 is to determine the similarities of words being spoken between the participants in a real time communication in relation to a past communication. The real time communication scoring module 410 compares the monitored communication with relevant past communications stored in the transcript database 284 in order to determine the similarities of words between the relevant past communications and the real time communication. The real time communication scoring module 410 calculates and assigns a score to the monitored communication.

In an embodiment, the monitored communication received by the real time communication scoring module 410 is in the form of a language converted transcript. The transcript indicates who is communicating in each specific section of the transcript. The real time communication scoring module 410 distinguishes the different participants in the monitored communication and searches for similarities between the communications of each participant. The real time communication scoring module 410 identifies the same or similar textual content within the transcript and compares the textual content with relevant past communications. The real time communication scoring module 410 calculates a score for the monitored communication by calculating a correlation of between the contents of the monitored communication and relevant past communications. The score for the monitored communication can vary depending on the number of times a similar phrase is used and the significance of the phrase. The score is higher for monitored communications containing a higher correlation and/or a higher frequency of similar phrases used, and the use of a suspicious or illegal keyword. The score is lower for communications containing a lower correlation and/or a lower frequency of similar
phrases used, and the use of benign phrases. In another embodiment, the real time communication scoring module 410 accesses the key word database 288 and the score may additionally or alternatively depend on the frequency of key words detected in the real time communication. The score is higher for monitored communications containing a higher frequency of key words.

The separate communication scoring module 420 scores communications that are not in real time, according to an embodiment of the invention. An example of a separate communication includes emails and texts sent between inmates at separate times, among others. The separate communication scoring module 420 focuses on comparing the monitored communication with relevant past communications stored in the transcript database 284 in order to determine the similarities of words between the separate communications. The separate communication scoring module 420 calculates and assigns a score to the monitored communication.

In an embodiment, the separate time communication scoring module 420 receives a monitored communication from the keyword searching and monitoring module 310. The separate time communication scoring module 420 receives past communications related to the monitored communication from the metadata search engine 320. The communications are in the form of a language converted transcript. The separate time communication scoring module 420 identifies the same or similar textual content between the monitored communication and the relevant past communications and calculates a score for the monitored communication based on the comparison. The separate time communication scoring module 420 calculates a correlation between the contents of the relevant past communications with the current monitored communication. The score for the monitored communication can vary depending on the number of times a similar phrase is used and the significance of the phrase. The score is higher for monitored communications containing a higher correlation, a higher frequency of similar phrases used in the separate communications, and the use of a suspicious or illegal keyword. The score is lower for communications containing a lower correlation, a lower frequency of similar phrases used, and the use of benign phrases. In another embodiment, the separate time communication scoring module 420 accesses the key word database 288 and the score may additionally or alternatively depend on the frequency of key words detected in
the monitored communication. The score is higher for monitored communications containing a higher frequency of key words.

[0050] The score comparison module 430 receives the communication scores from the real time communication scoring module 410 and the separate communication scoring module 420, according to an embodiment of the invention. The score comparison module 430 may have a memory that contains a threshold score. The threshold score is predetermined and can be adjusted by an administrator. The score comparison module 430 compares the received communication scores with the threshold score. If the communication score is higher than the threshold score, then the communication is sent to the alerting module 270 along with a notification signal for the supervising personnel at the controlled environment. If the communication is a real time communication, then the communication can be disconnected if the score is higher than the threshold score. If the communication is a separate time communication, the communication can be withheld until reviewed by the supervising personnel and future communication can be restricted if the score is higher than the threshold score.

System Operation

[0051] Fig. 5 illustrates a flowchart diagram of an exemplary method 500 for detecting and preventing illegal communications. The method of Fig. 5 is described below with reference to Figs. 2 and 3.

[0052] At the outset, a communication is detected (502). The detected communication is stored in a communication storage 220 (504) for later analysis. The communication is stored in the appropriate file format in which the communication has been detected and arranged in a queue. The system makes a determination of whether the communication is in an audio format (506). If the communication is stored as in audio format (506 - Y), transcriber 230 receives and transcribes the audio file into a text file (508). The resulting text file contains the transcript of the detected communication. If the communication is not in an audio format (506 - N), no transcription is needed.

[0053] The system subsequently determines whether the communication is in a standard language (510). This refers to whether the communication is in a common language employed by the analysis engine, e.g. North American English. If the communication is not in the standard language (510 - N), then the language converter 240 receives the communication and converts the communication into a standard language (512). The
conversion into a standard language facilitates a more efficient and universal method of monitoring the communications to detect rule violation. If the communication is in a standard language (510 - Y), language conversion does not occur.

Once the communication is determined to be in the standard language, the system searches the communication for keywords that are typically used by controlled environments to monitor inmate communications (514). The system continues to search for keywords in the communication if it does not find a match (516 - N). If the system finds a keyword match in the communication (516 - Y), then the system monitors the communication for an extended period of time (518). The scoring module 330 receives the monitored communication and assigns a score (520) to the communication. This step is described in detail in Fig. 6.

The monitored communication is received by the scoring module 330 (602) in order to be analyzed and compared with relevant past communications. Next, the scoring module 330 determines whether the monitored communication is a real-time communication (604), such as a voice or video call.

If the monitored communication is determined to be a real-time communication (604 - Y), the real time communication scoring module 410 compares similar phrases and keywords within the monitored communication and assigns a score (606). The focus of the real time communication scoring module 410 is to determine the similarities of words being spoken between the participants in a real time communication in relation to a past communication. The real time communication scoring module 410 compares the monitored communication with relevant past communications stored in the transcript database 284 in order to determine the similarities of words between the relevant past communications and the ongoing real time communication. The real time communication scoring module 410 calculates a score for the monitored communication by calculating a correlation of between the contents of the monitored communication and relevant past communications. The score for the monitored communication can vary depending on the number of times a similar phrase is used and the significance of the phrase.

If the monitored communication is not a real-time communication (604 - N), the separate time communication scoring module (420) compares similar phrases and
keyword between the monitored communication and past communications stored in the
database 280 (608). The separate time communication scoring module 420 identifies the
same or similar textual content between the separate communications and calculates a
score for the monitored communication. The separate time communication scoring
module 420 calculates a correlation between the contents of the relevant past
communications with the current monitored communication. The score for the monitored
communication can vary depending on the number of times a similar phrase is used and
the significance of the phrase

Once the communication has been scored, the assigned score is compared to a
predetermined threshold score (610/552). Referring back to Fig. 5, if the score is lower
than the threshold (522 - N), then the system determines whether the communication is
still ongoing (524). If the communication is still ongoing (524- Y), then the system
continues to search for keywords in the communication (514). If the communication has
ended (524 -N), the method 500 ends (528).

On the other hand, if the assigned score is higher than the threshold (522 - Y),
then the system takes any number of remedial measures (526), such as alerting a
supervisor that a rule violation has occurred in the communication, terminating the
communication (in the case of a real-time communication), withholding the
communication for closure inspection (in the case of a non-real-time communication),
among others. Following the remedial measures (526), the method ends (528).

Exemplary Computer System Implementation

It will be apparent to persons skilled in the relevant art(s) that various elements
and features of the present disclosure, as described herein, can be implemented in
hardware using analog and/or digital circuits, in software, through the execution of
computer instructions by one or more general purpose or special-purpose processors, or
as a combination of hardware and software.

The following description of a general purpose computer system is provided for
the sake of completeness. Embodiments of the present disclosure can be implemented in
hardware, or as a combination of software and hardware. Consequently, embodiments of
the disclosure may be implemented in the environment of a computer system or other
processing system. For example, the method of flowcharts 500 and 600 can be
implemented in the environment of one or more computer systems or other processing
systems. An example of such a computer system 700 is shown in Fig. 7. One or more of
the modules depicted in the previous figures can be at least partially implemented on one
or more distinct computer systems 700.

[0063] Computer system 700 includes one or more processors, such as processor 704.
Processor 704 can be a special purpose or a general purpose digital signal processor.
Processor 704 is connected to a communication infrastructure 702 (for example, a bus or
network). Various software implementations are described in terms of this exemplary
computer system. After reading this description, it will become apparent to a person
skilled in the relevant art(s) how to implement the disclosure using other computer
systems and/or computer architectures.

[0064] Computer system 700 also includes a main memory 706, preferably random
access memory (RAM), and may also include a secondary memory 708. Secondary
memory 708 may include, for example, a hard disk drive 710 and/or a removable storage
drive 712, representing a floppy disk drive, a magnetic tape drive, an optical disk drive, or
the like. Removable storage drive 712 reads from and/or writes to a removable storage
unit 716 in a well-known manner. Removable storage unit 716 represents a floppy disk,
magnetic tape, optical disk, or the like, which is read by and written to by removable
storage drive 712. As will be appreciated by persons skilled in the relevant art(s),
removable storage unit 716 includes a computer usable storage medium having stored
therein computer software and/or data.

[0065] In alternative implementations, secondary memory 708 may include other similar
means for allowing computer programs or other instructions to be loaded into computer
system 700. Such means may include, for example, a removable storage unit 718 and an
interface 714. Examples of such means may include a program cartridge and cartridge
interface (such as that found in video game devices), a removable memory chip (such as
an EPROM, or PROM) and associated socket, a thumb drive and USB port, and other
removable storage units 718 and interfaces 714 which allow software and data to be
transferred from removable storage unit 718 to computer system 700.

[0066] Computer system 700 may also include a communications interface 720.
Communications interface 720 allows software and data to be transferred between
computer system 700 and external devices. Examples of communications interface 720
may include a modem, a network interface (such as an Ethernet card), a communications
port, a PCMCIA slot and card, etc. Software and data transferred via communications interface 720 are in the form of signals which may be electronic, electromagnetic, optical, or other signals capable of being received by communications interface 720. These signals are provided to communications interface 720 via a communications path 722. Communications path 722 carries signals and may be implemented using wire or cable, fiber optics, a phone line, a cellular phone link, an RF link and other communications channels.

As used herein, the terms "computer program medium" and "computer readable medium" are used to generally refer to tangible storage media such as removable storage units 716 and 718 or a hard disk installed in hard disk drive 710. These computer program products are means for providing software to computer system 700.

Computer programs (also called computer control logic) are stored in main memory 706 and/or secondary memory 708. Computer programs may also be received via communications interface 720. Such computer programs, when executed, enable the computer system 700 to implement the present disclosure as discussed herein. In particular, the computer programs, when executed, enable processor 704 to implement the processes of the present disclosure, such as any of the methods described herein. Accordingly, such computer programs represent controllers of the computer system 700. Where the disclosure is implemented using software, the software may be stored in a computer program product and loaded into computer system 700 using removable storage drive 712, interface 714, or communications interface 720.

In another embodiment, features of the disclosure are implemented primarily in hardware using, for example, hardware components such as application-specific integrated circuits (ASICs) and gate arrays. Implementation of a hardware state machine so as to perform the functions described herein will also be apparent to persons skilled in the relevant art(s).

CONCLUSION

The disclosure has been described above with the aid of functional building blocks illustrating the implementation of specified functions and relationships thereof. The boundaries of these functional building blocks have been arbitrarily defined herein for the
convenience of the description. Alternate boundaries may be defined so long as the
specified functions and relationships thereof are appropriately performed.

[0071] It will be apparent to those skilled in the relevant art(s) that various changes in
form and detail can be made therein without departing from the spirit and scope of the
disclosure.
WHAT I S CLAIMED IS:

1. A communication monitoring method, the method comprising:
   receiving a communication involving an inmate of a controlled-environment facility;
   extracting metadata from the received communication, the metadata containing information about the communication;
   retrieving at least one previously-stored second communication that has overlapping metadata with the received communication;
   correlating contents of the received communication with contents of the other communications;
   assigning a score to the received communication based on the correlation;
   comparing the score with a predetermined threshold; and
   taking remedial action based on the score comparison.

2. The communication monitoring method of claim 1, wherein the received communication is in an audio format, the method further comprising:
   storing the received communication in the audio format; and
   transcribing the received communication into a text format, wherein the text format reflects the contents of the communication.

3. The communication monitoring method of claim 1, wherein the received communication is in a text format, the method further comprising:
   storing the received communication in the text format.

4. The communication monitoring method of claim 1, further comprising:
   determining that the communication contains non-standard language; and
   converting non-standard language portions of the communication into a standard language, the converting including:
   accessing a language dictionary to identify the non-standard language; and
   translating the non-standard language into the standard language using the language dictionary and a plurality of conversion protocols.
5. The communication monitoring method of claim 1, further comprising:
   determining that the communication is a real-time communication;
   detecting keywords and/or key phrases within the communication in real-time;
   and
   storing a recording of the communication for performing the correlating at a later time.

6. The communication monitoring method of claim 1, further comprising:
   determining that the communication is not a real-time communication;
   identifying one or more stored second communications having overlapping metadata with the communication in response to the determining; and
   correlating contents of the communication with contents of the identified second communications.

7. The communication monitoring method of claim 5, wherein the remedial action includes alerting a supervising personnel and disconnecting the communication.

8. The communication monitoring method of claim 6, wherein the remedial action includes withholding the communication from being forwarded to an intended recipient until after the correlating.

9. A communication monitoring method, the method comprising:
   receiving a first communication that involves an inmate of a controlled-environment facility;
   extracting metadata from the first communication;
   identifying at least one previously-stored second communication based on the metadata;
   comparing the first communication to the at least one second communication to identify overlapping keywords and/or key phrases;
   scoring the first communication based on the comparison; and
   comparing the score with a predetermined threshold.
10. The communication monitoring method of claim 9, further comprising:
   determining that the first communication is a real-time communication;
   forwarding the first communication to an intended recipient prior to completing the comparing; and
   storing a copy of the first communication,
   wherein the comparing is performed using the stored copy of the first communication.

11. The communication monitoring method of claim 10, further comprising correlating contents of the first communication with contents of the at least one second communication,
   wherein the scoring of the first communication is performed based on the correlation.

12. The communication monitoring method of claim 9, further comprising:
   determining that the first communication is not in real time;
   correlating contents of the first communication with contents of the at least one second communication in response to the determination before forwarding the first communication to an intended recipient; and
   scoring the first communication based on the correlation.

13. A communication monitoring system, the system comprising:
   a database;
   a transceiver, configured to receive a communication involving an inmate of a controlled-environment facility;
   a processing subsystem configured to extract metadata from the communication, the metadata containing information about the communication; and
   a detection and prevention analysis engine configured to:
      correlate contents of the communication with contents of other communications having overlapping metadata;
      assign a score to the communication based on the correlation;
      compare the score with a predetermined threshold; and
take remedial action based on the score comparison.

14. The communication monitoring system of claim 13, further comprising a communication storage configured to store the received communication in an appropriate format depending on a type of the received communication.

15. The communication monitoring system of claim 13, further comprising a transcriber configured to transcribe the received communication into a text format, wherein the text format reflects the contents of the communication.

16. The communication monitoring method of claim 13, further comprising a language converter configured to:
   - determine that the communication contains non-standard language; and
   - convert the communication into a standard language, the converting including:
     - access a language dictionary to identify the non-standard language; and
     - translate nonstandard language portions of the communication into the standard language using the language dictionary and a plurality of conversion protocols.

17. The communication monitoring system of claim 13, wherein the detection and prevention analysis engine is further configured to:
   - determine that the communication is in real time; and
   - forward the communication to an intended recipient prior to performing the correlating.

18. The communication monitoring system of claim 13, wherein the detection and prevention analysis engine is further configured to:
   - determine whether the communication is not in real time; and
   - perform the correlating prior to forwarding the communication to an intended recipient.

19. The communication monitoring system of claim 17, wherein the remedial action includes alerting a supervising personnel and disconnecting the communication.
20. The communication monitoring method of claim 18, wherein the remedial action includes withholding the communication and preventing future communication containing the same metadata.
Detection and Prevention Analysis Engine 300

Signal I/O 305A

Metadata Search Engine 320

Keyword Searching and Monitoring Module 310

Scoring Module 330

Signal I/O 305B
600

Receive monitored communication

602

Real time communication scoring

606

Is communication in real time?

604

Yes

No

Separate communication scoring

608

Compare score to threshold value

610

FIG. 6
Communication Infrastructure 702

- Processor 704
- Main Memory 706

Secondary Memory 708

- Hard Disk Drive 710
- Removable Storage Drive 712
- Interface 714

Removable Storage Unit 716
Removable Storage Unit 718

Interface 720

Communications Path 722

FIG. 7
### INTERNATIONAL SEARCH REPORT

**PCT/US2017/022169**

**A. CLASSIFICATION OF SUBJECT MATTER**

**INV.** H04M3/22  G10L15/26  H04M3/38  H04M3/42

**ADD.**

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

H04M  G10L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

**EPO-Internal**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 2015/281433  AI (GAINSBORO JAY [US] ET AL) 1 October 2015 (2015-10-01)</td>
<td>1, 6, 13</td>
</tr>
<tr>
<td></td>
<td>paragraphs [0002], [0009], [0042]-[0045], [0049]; claim 1</td>
<td>2-5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7-12, 14-20</td>
</tr>
<tr>
<td></td>
<td>paragraphs [0051], [0054], [0071], [0090]-[0091]; figure 4</td>
<td>7-12, 14-20</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C.  

See patent family annex.

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

**T** later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

**X** document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

**Y** document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

**Z** document member of the same patent family

Date of the actual completion of the international search: 18 May 2017

Date of mailing of the international search report: 29/05/2017

Name and mailing address of the ISA:

European Patent Office, P.B. 5818 Patentlaan 2

NL-2280 HV Rijswijk

Tel. (+31-70) 340-2040

Fax: (+31-70) 340-3016

Authorized officer: Mukasa, Oliver
<table>
<thead>
<tr>
<th>Patent document</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>US 2015281433 Al</td>
<td>01-10-2015</td>
</tr>
<tr>
<td>US 2008201143 Al</td>
<td>21-08-2008</td>
<td>US 2008201143 Al</td>
<td>21-08-2008</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2008201158 Al</td>
<td>21-08-2008</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2014254777 Al</td>
<td>11-09-2014</td>
</tr>
</tbody>
</table>