US 20130283401A1

(19) **United States**

(12) **Patent Application Publication**

Pabla et al.

(10) **Pub. No.: US 2013/0283401 A1**

(43) **Pub. Date: Oct. 24, 2013**

(54) **INFORMATION CONTENT VALIDATION FOR ELECTRONIC DEVICES**

(71) Applicant: **SAMSUNG ELECTRONICS CO., LTD.**, Suwon (KR)

(72) Inventors: **Kuldip S. Pabla**, San Jose, CA (US); **Asokan Ashok**, San Diego, CA (US)

(73) Assignee: **Samsung Electronics Co., Ltd.**, Suwon (KR)

(21) Appl. No.: **13/865,945**

(22) Filed: **Apr. 18, 2013**

Related U.S. Application Data

(60) Provisional application No. 61/637,785, filed on Apr. 24, 2012.

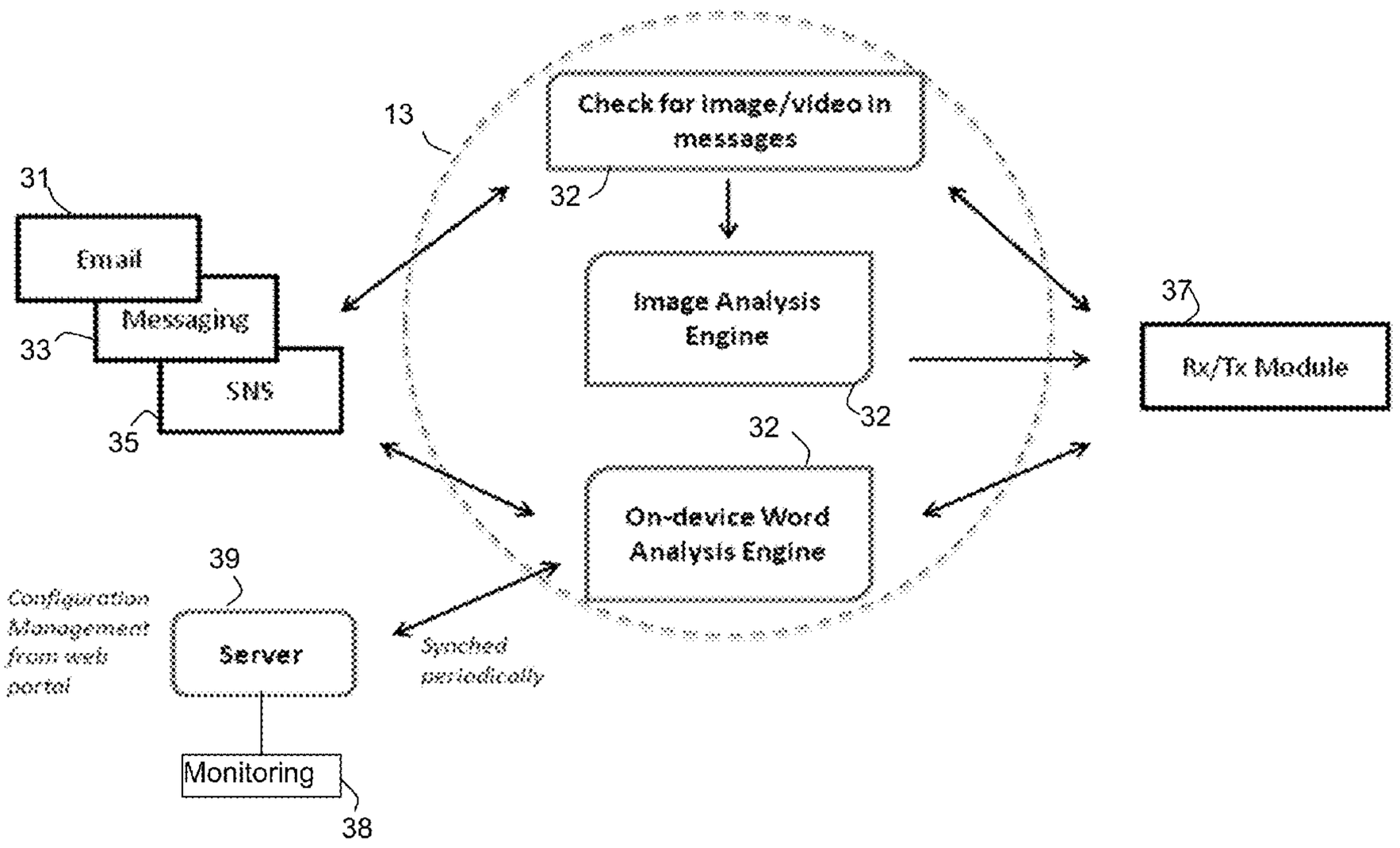
Publication Classification

(51) **Int. Cl.**
G06F 21/60 (2006.01)

(52) **U.S. Cl.**
CPC ***G06F 21/60*** (2013.01)
USPC **726/30**

(57) **ABSTRACT**

A circuit device comprises a processing device connected to a memory. The processing device comprises a detection module that detects information content received in the memory from an electronic device. A validation module validates the information content in real time. Validating the information content includes analyzing the information content to detect selected content and preventing dissemination of the selected content from the electronic device.



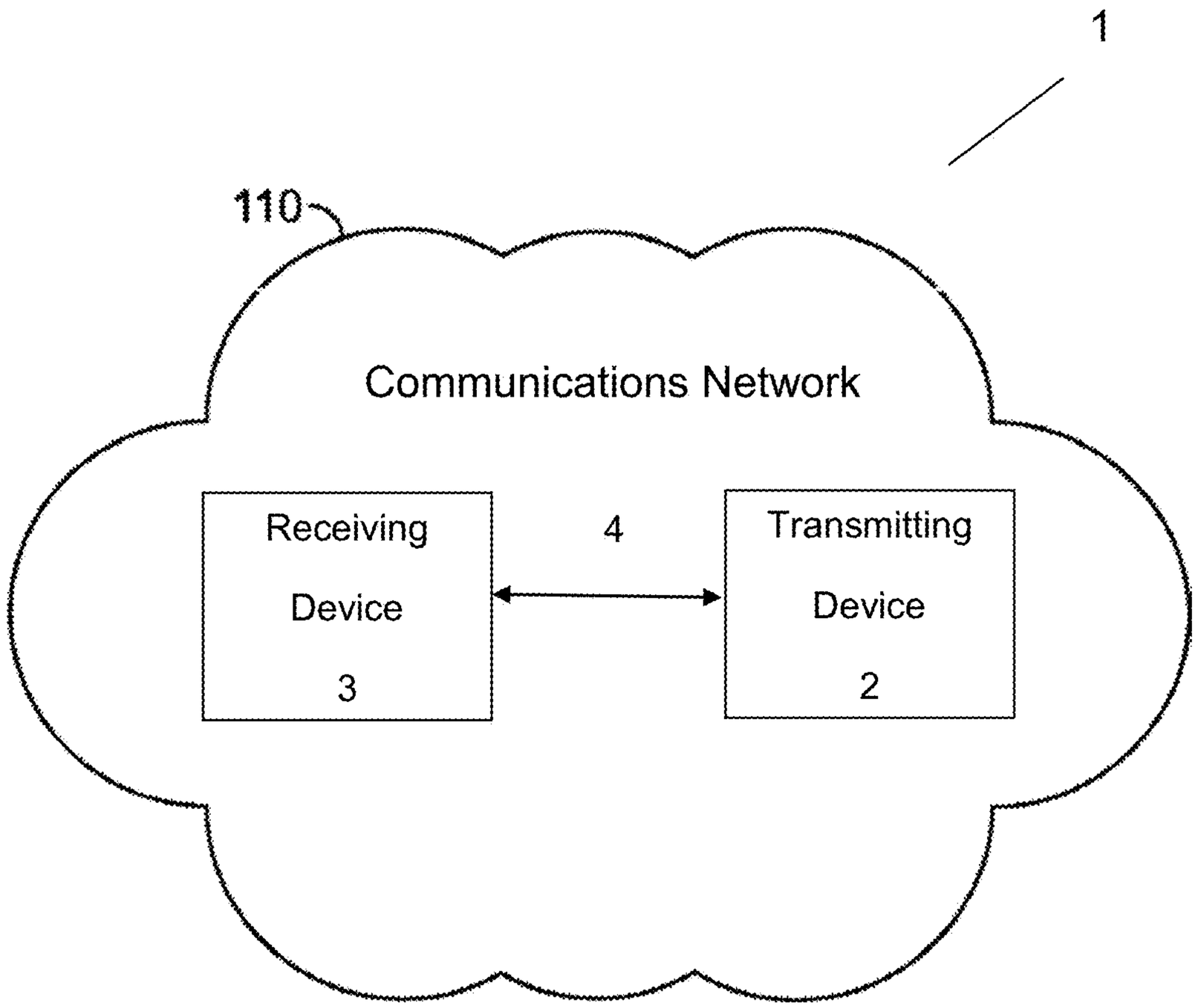

1
110
Communications Network
Receiving
Device
3
4
Transmitting
Device
2

FIG. 1

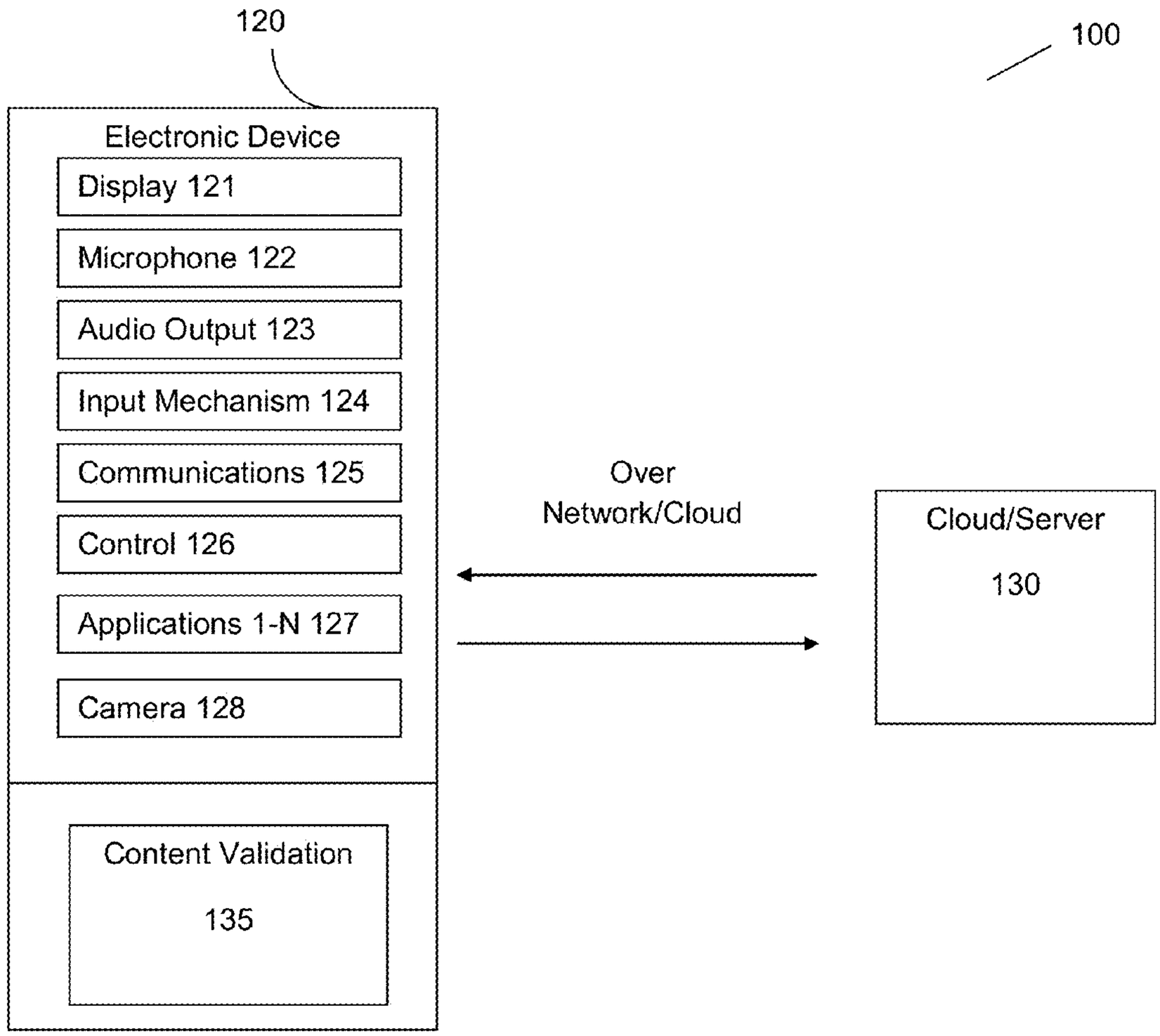

120
100
Electronic Device
Display 121
Microphone 122
Audio Output 123
Input Mechanism 124
Communications 125
Control 126
Applications 1-N 127
Camera 128
Content Validation
135
Over
Network/Cloud
Cloud/Server
130

FIG. 2

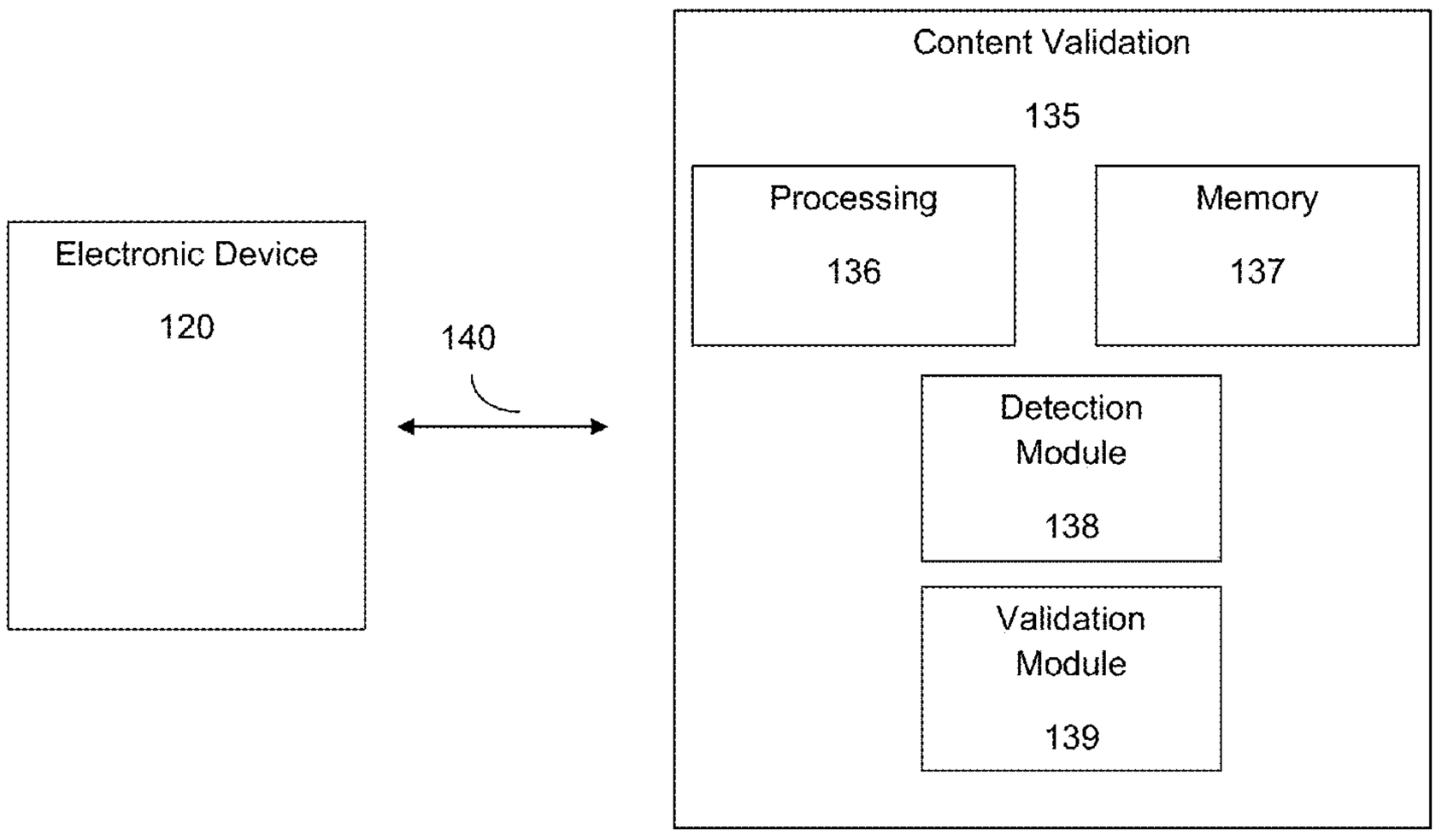

Content Validation
135
Processing
136
Memory
137
Detection Module
138
Validation Module
139
Electronic Device
120
140

FIG. 3

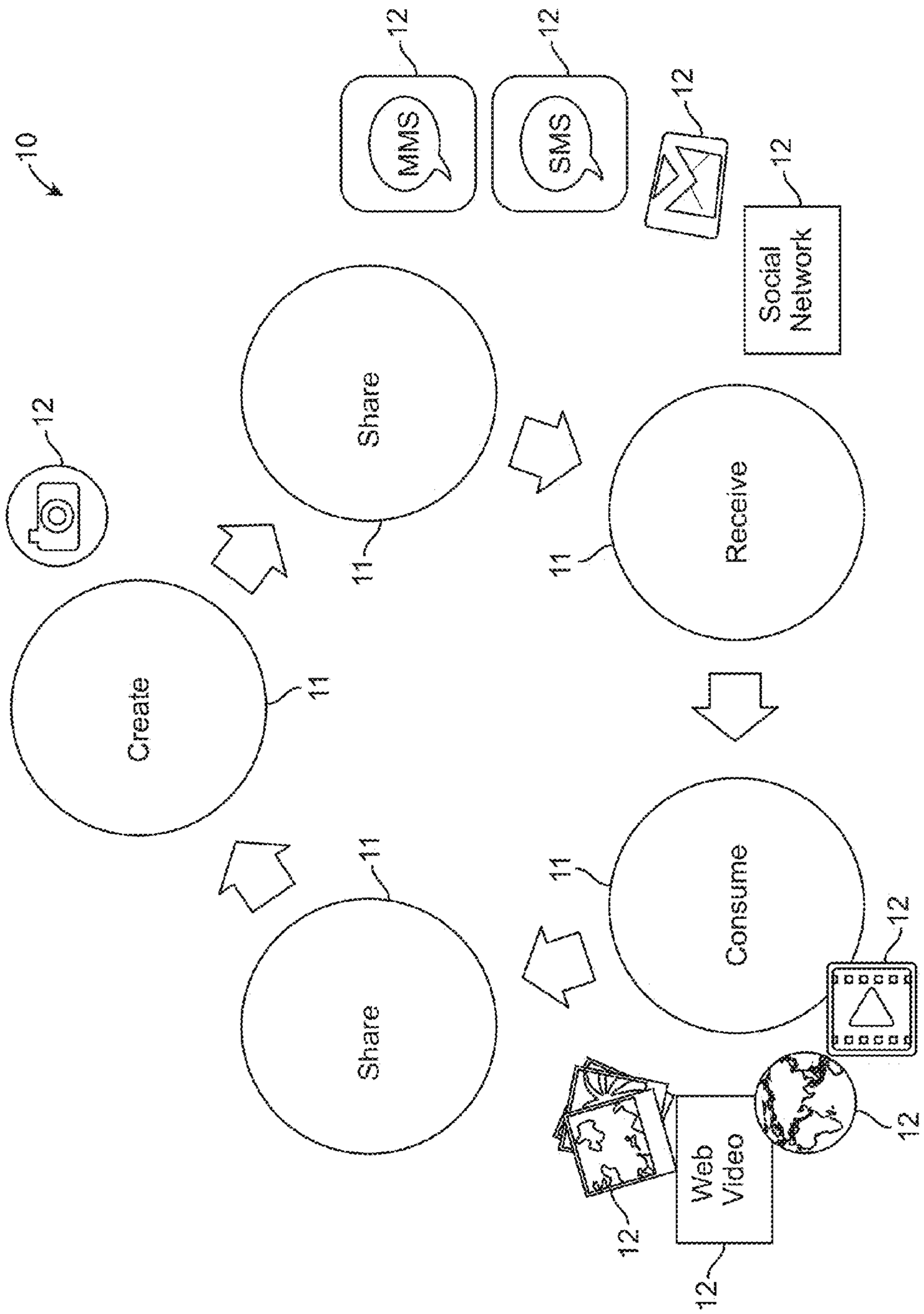
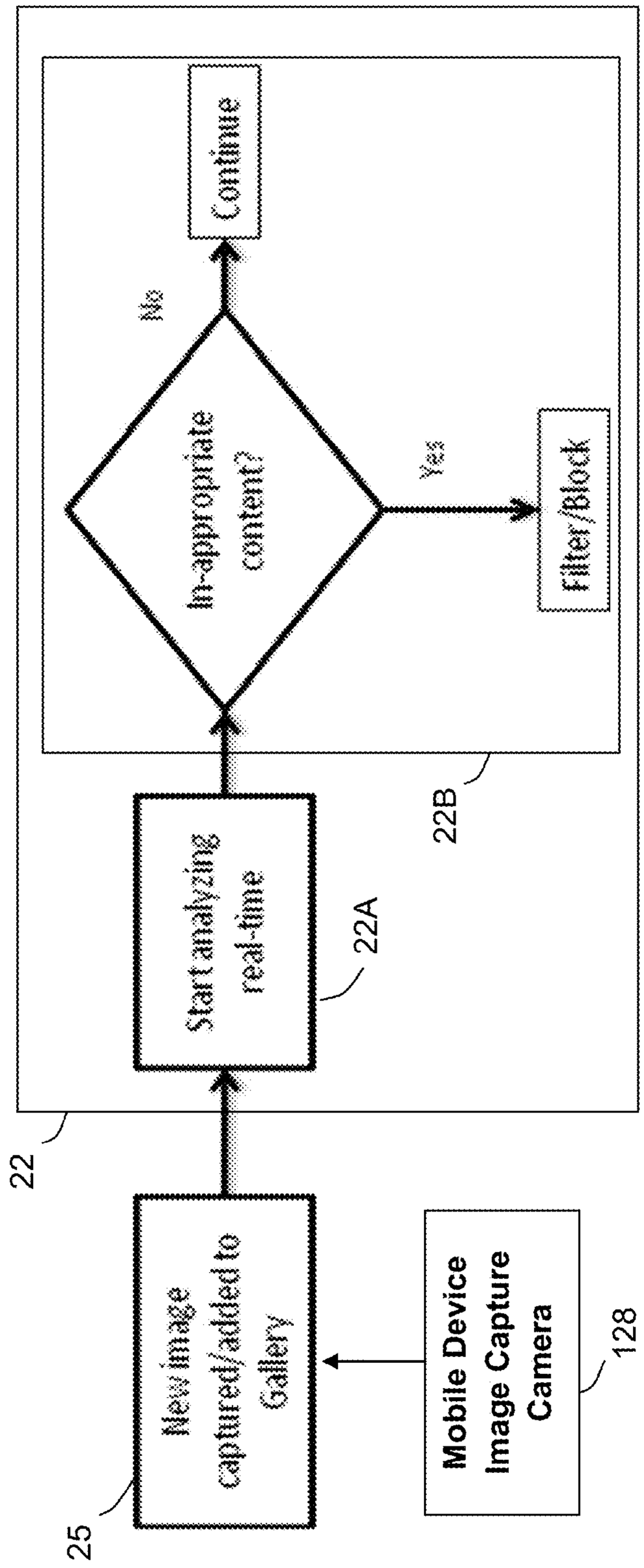
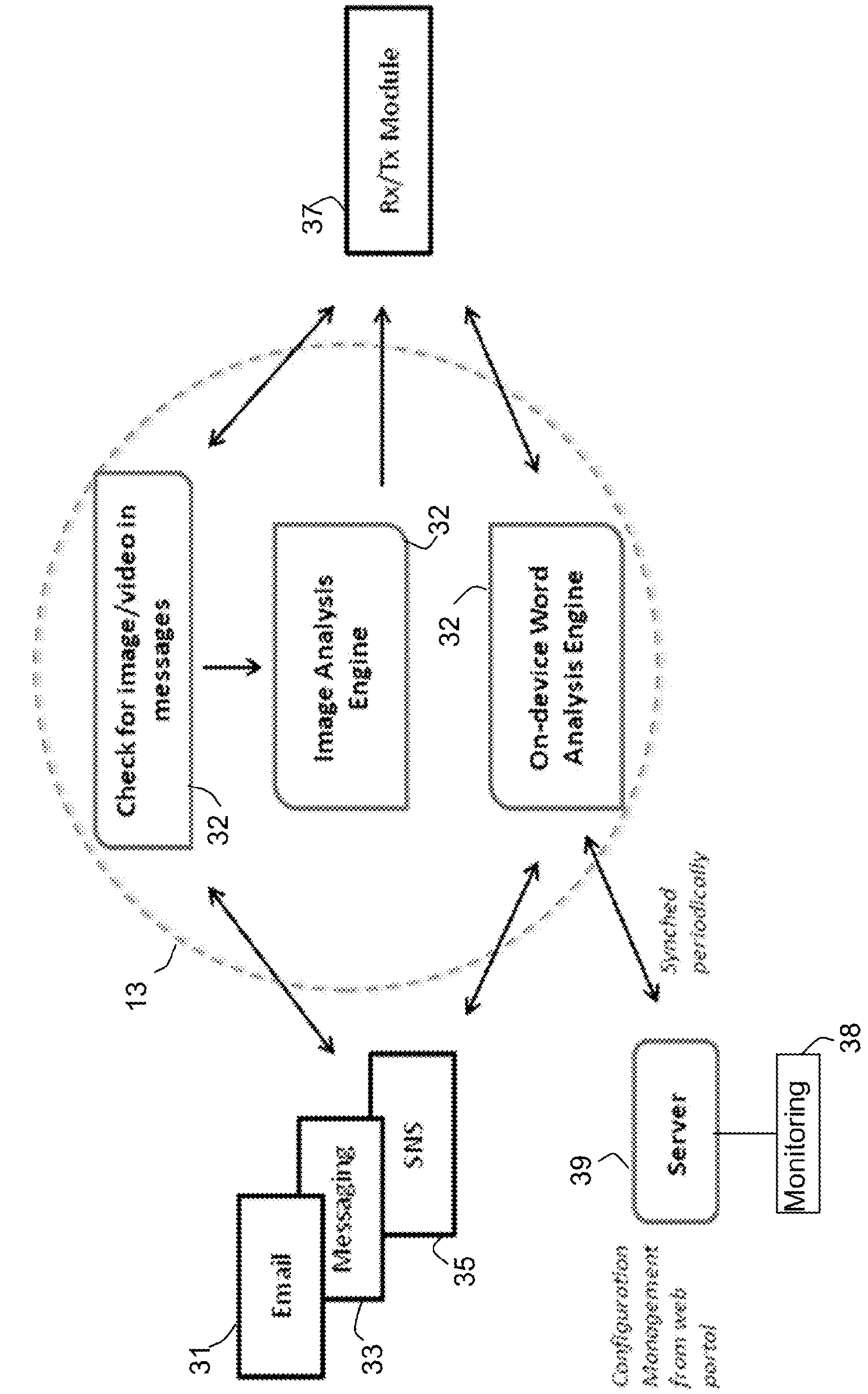

10
12
MMS
12
SMS
12
12
Social Network
Create
11
Share
11
Receive
11
Consume
11
Share
11
12
Web
Video
12
12
12

FIG. 4


New image captured/added to Gallery
25
Mobile Device Image Capture Camera
128
22
Start analyzing real-time
22A
In-appropriate content?
No
Continue
Yes
Filter/Block
22B

20

FIG. 5


Rx/Tx Module
37
Check for image/video in messages
32
Image Analysis Engine
32
32
On-device Word Analysis Engine
13
Synched periodically
Email
31
Messaging
33
SMS
35
Server
39
Monitoring
38
Configuration Management from web portal

30

FIG. 6

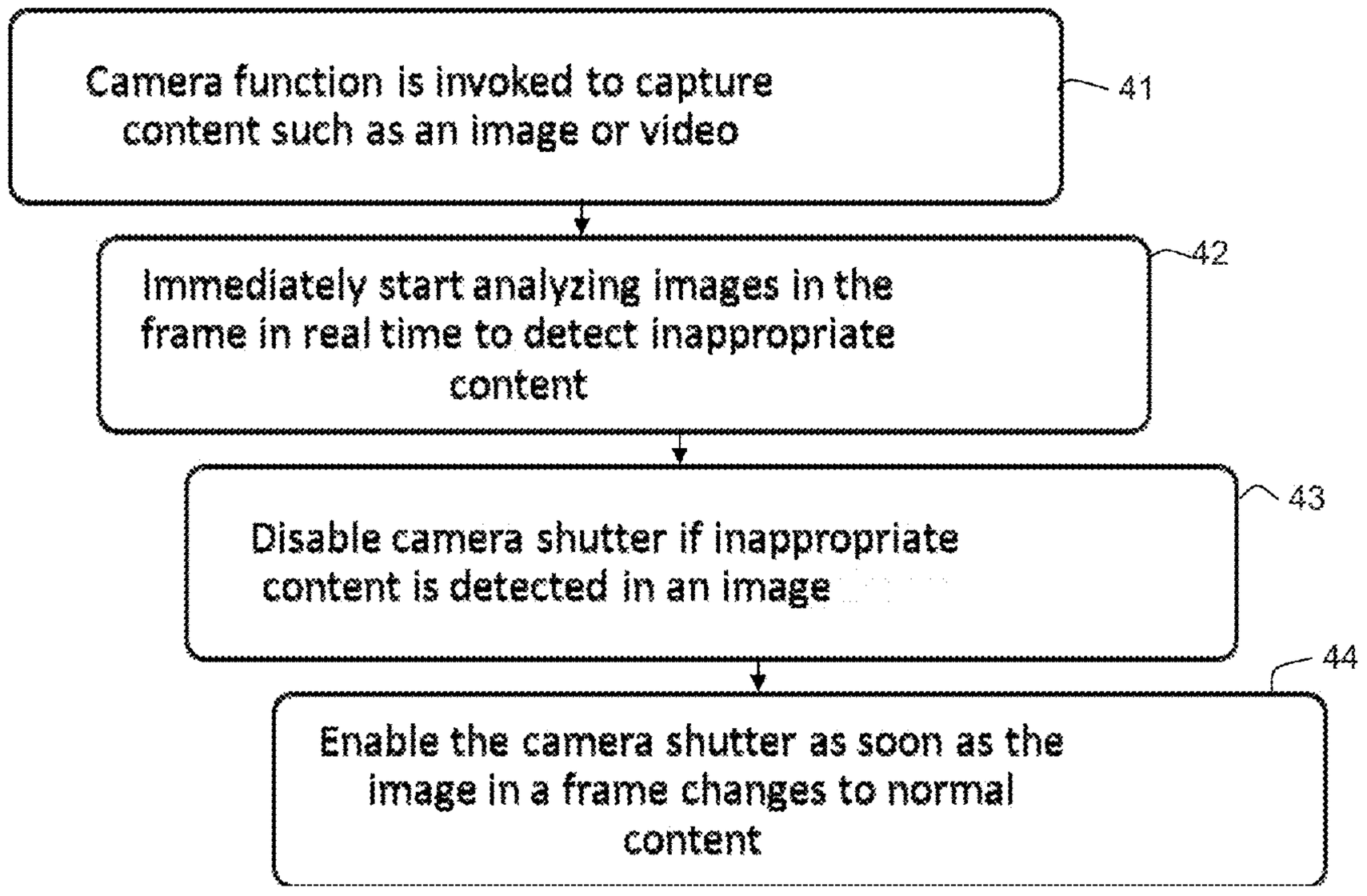
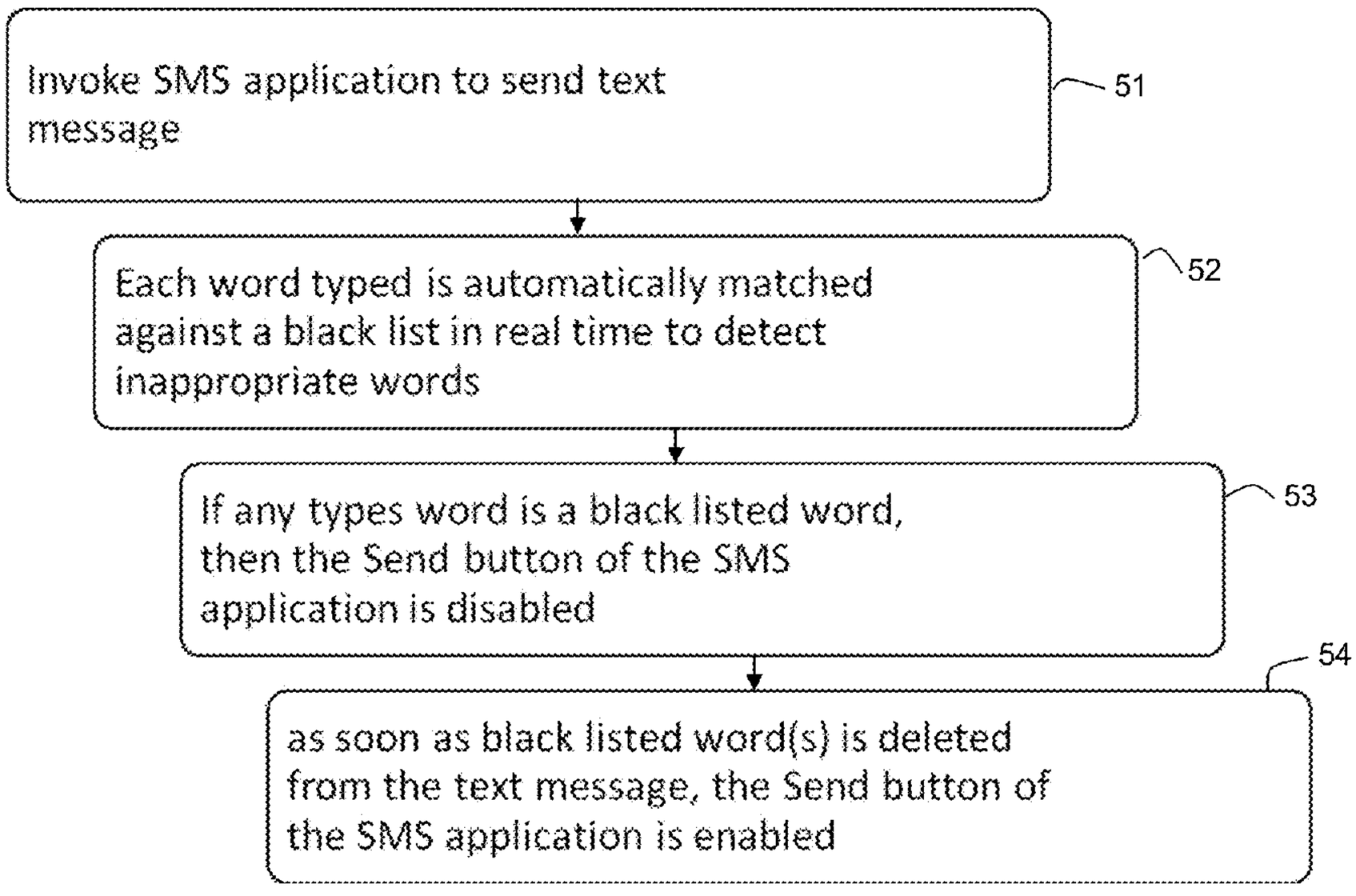

Camera function is invoked to capture content such as an image or video
41
Immediately start analyzing images in the frame in real time to detect inappropriate content
42
Disable camera shutter if inappropriate content is detected in an image
43
Enable the camera shutter as soon as the image in a frame changes to normal content
44
40

FIG. 7


Invoke SMS application to send text message
51
Each word typed is automatically matched against a black list in real time to detect inappropriate words
52
If any types word is a black listed word, then the Send button of the SMS application is disabled
53
as soon as black listed word(s) is deleted from the text message, the Send button of the SMS application is enabled
54

50

FIG. 8

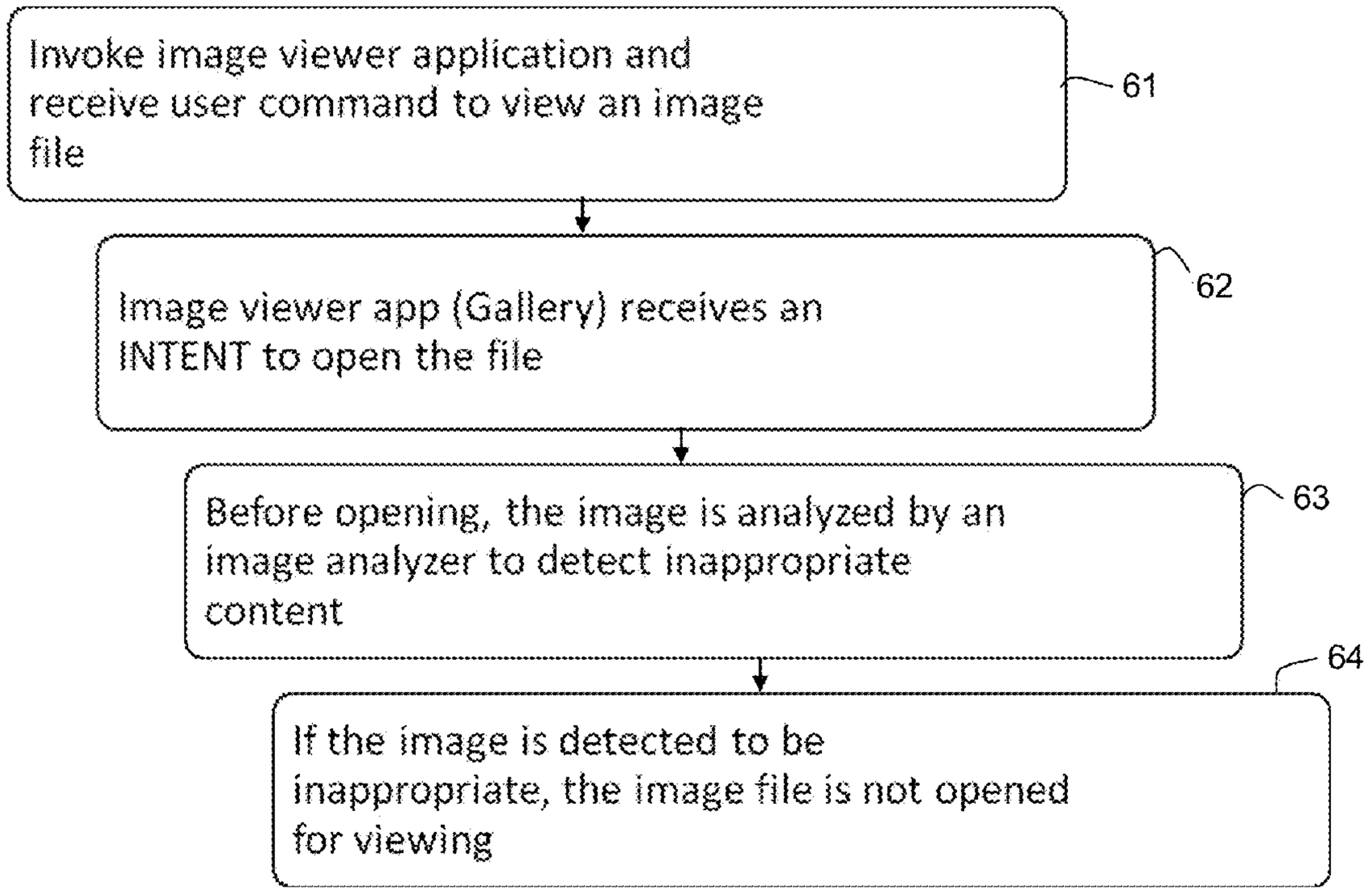

Invoke image viewer application and receive user command to view an image file
61
Image viewer app (Gallery) receives an INTENT to open the file
62
Before opening, the image is analyzed by an image analyzer to detect inappropriate content
63
If the image is detected to be inappropriate, the image file is not opened for viewing
64
60

FIG. 9

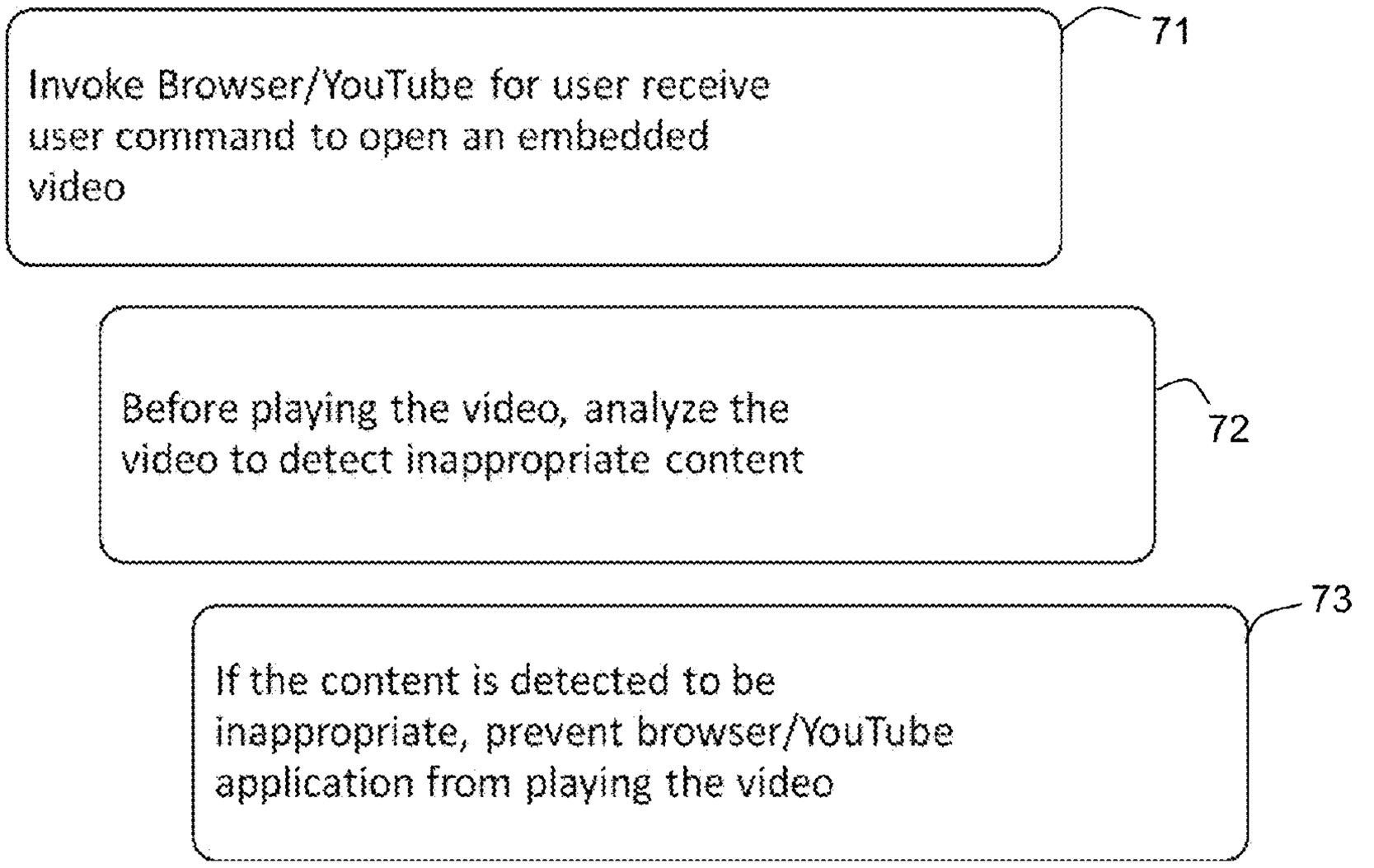
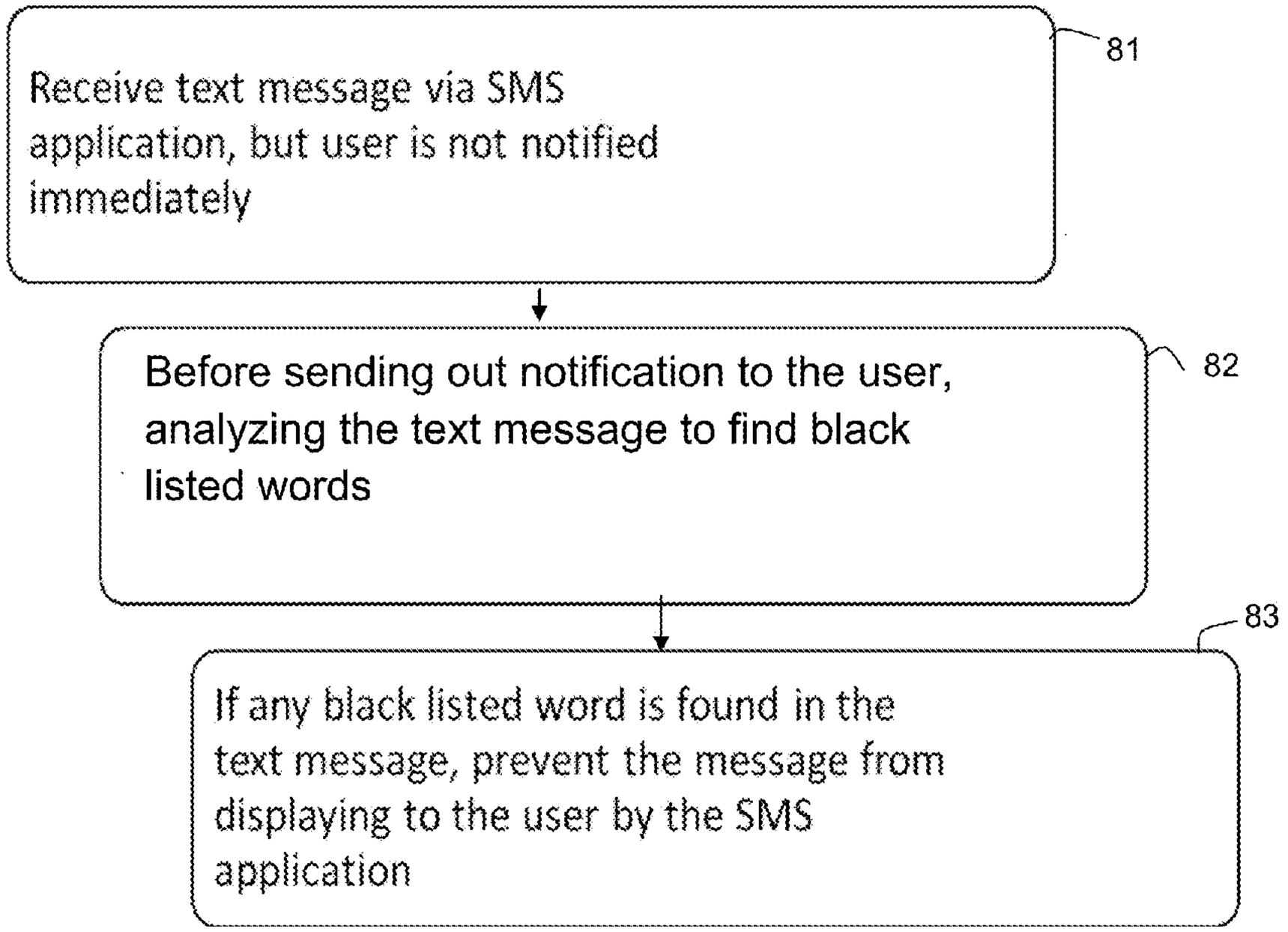

Invoke Browser/YouTube for user receive user command to open an embedded video
71
Before playing the video, analyze the video to detect inappropriate content
72
If the content is detected to be inappropriate, prevent browser/YouTube application from playing the video
73
70

FIG. 10


Receive text message via SMS application, but user is not notified immediately
81
Before sending out notification to the user, analyzing the text message to find black listed words
82
If any black listed word is found in the text message, prevent the message from displaying to the user by the SMS application
83

80

FIG. 11

INFORMATION CONTENT VALIDATION FOR ELECTRONIC DEVICES

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims the priority benefit of U.S. Provisional Patent Application Ser. No. 61/637,785, filed on Apr. 24, 2012, incorporated herein by reference.

TECHNICAL FIELD

[0002] One or more embodiments generally relate to content validation and, in particular, to content filtering for mobile communication devices.

BACKGROUND

[0003] With the rapid proliferation of mobile communication devices such as smartphones among users such as teenagers and children, there is an increase in abusive and/or inappropriate behavior through content communicated via such devices. These devices provide access to a number of multimedia and messaging applications along with internet connectivity, thus making a user of such devices vulnerable to "cyber bullying," "sexting," nudity, etc.

SUMMARY

[0004] One or more embodiments generally relate to a circuit device for content validation. In one embodiment, a circuit device comprises a processing device connected to a memory. Information content is detected on an electronic device. In one embodiment, the information content is validated in real time. In one embodiment, the information content is validated by analyzing the information content to detect selected content, and to prevent dissemination of the selected content from the electronic device.

[0005] In one embodiment, a method for content validation comprises detecting information content using a processing device. In one embodiment, the information content is validated using the processing device. In one embodiment, validating the information content includes analyzing the information content to detect selected content, and preventing dissemination of the selected content via an electronic device.

[0006] In one embodiment an apparatus comprises an integrated circuit (IC) coupled with a memory. In one embodiment, a content interface is coupled between the IC and an electronic device. In one embodiment, the IC comprises a detection module that detects information content received in the memory over the content interface from an electronic device. In one embodiment, a validation module validates the information content in real time. In one embodiment, validating the information content includes analyzing the information content to detect selected content, and preventing dissemination of the selected content from the electronic device.

[0007] These and other aspects and advantages of one or more embodiments will become apparent from the following detailed description, which, when taken in conjunction with the drawings, illustrate by way of example the principles of the one or more embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] For a fuller understanding of the nature and advantages of the embodiments, as well as a preferred mode of use, reference should be made to the following detailed description read in conjunction with the accompanying drawings, in which:

[0009] FIG. **1** shows a schematic view of a communications system, according to an embodiment.

[0010] FIG. **2** shows a block diagram of an architecture system including content validation, according to an embodiment.

[0011] FIG. **3** shows a block diagram of a circuit device for content validation, according to an embodiment.

[0012] FIG. **4** shows a block diagram of content validation architecture on a mobile device, according to an embodiment.

[0013] FIG. **5** shows a block diagram of an architecture for image content validation for an image capture camera on a mobile device, according to an embodiment.

[0014] FIG. **6** shows a block diagram of an architecture for image content and word content validation on a mobile device, according to an embodiment.

[0015] FIG. **7** shows a flowchart of a content validation process with camera application integration for filtering selected content, according to an embodiment.

[0016] FIG. **8** shows a flowchart of another content validation process with short message service (SMS) application integration for filtering selected content, according to an embodiment.

[0017] FIG. **9** shows a flowchart of another content validation process with image viewer application integration for filtering selected content, according to an embodiment.

[0018] FIG. **10** shows a flowchart of another content validation process with browser application integration for filtering selected content, according to an embodiment.

[0019] FIG. **11** shows a flowchart of another content validation process with SMS application integration for filtering selected content, according to an embodiment.

DETAILED DESCRIPTION

[0020] The following description is made for the purpose of illustrating the general principles of one or more embodiments and is not meant to limit the inventive concepts claimed herein. Further, particular features described herein can be used in combination with other described features in each of the various possible combinations and permutations. Unless otherwise specifically defined herein, all terms are to be given their broadest possible interpretation including meanings implied from the specification as well as meanings understood by those skilled in the art and/or as defined in dictionaries, treatises, etc.

[0021] One or more embodiments generally relate to content validation and, in particular, to content filtering on electronic devices such as mobile communication devices. In one embodiment, content validation comprises using an embedded device or system, such as a system on chip (SOC), application specific integrated circuit (ASIC), firmware device, etc. for detecting information content on an electronic device and validating the information content in real time on the electronic device. In one embodiment, the information content comprises information content originating and/or terminating at the electronic device. In one embodiment, validating the information content includes analyzing the information content to detect selected content and preventing dissemination of the selected content via the electronic device. In one embodiment, preventing dissemination includes filtering out the selected content using the embedded device on the electronic device. In one embodiment, dissemination of content

via the electronic device includes communication, transmission, reception, origination, and termination of content via the electronic device, as described in more detail herein below.

[0022] One or more embodiments provide a real-time device or system to validate selected content by screening and filtering out selected content before such content reaches the user device for display (e.g., on screen viewing) or speech (e.g., audio). One embodiment provides a real-time device or system to validate by screening and filtering out selected content before the content is sent out by an electronic user device (e.g., mobile phone device, tablet computing device, camera device, camcorder device, media device, laptop computing device, personal computing (PC) device, personal digital assistant (PDA) device, television device, etc.). One embodiment provides a real-time device or system for such content validation and control (such as parental control, rating control, etc.) to prevent communication of selected content such (as abusive and/or inappropriate content) to and from user devices, whether created, originating, received, transferred to/from, etc.

[0023] In one embodiment, the device or system is not Internet-based and does not require server validation (such as SMSC/MMSC or sending out the content to a server located in the network). In one embodiment, the device or system is suitable for embedding in a mobile device environment wherein most, if not all content validation is performed on the mobile device itself in real time.

[0024] In one embodiment, an embedded device or system provides a real-time, end-to-end, device-embedded protocol and system for mobile communication devices, such as wireless mobile communication devices (e.g., smartphones, tablets, cameras, camcorders, etc.) to proactively prevent users such as teenagers and children from indulging in inappropriate behavior including, but not limited to: (1) sending/receiving (to individuals or broadcasting) text messages and e-mails with selected content such as sexually explicit words, swear words, short forms with sexual meanings, etc., (2) sending/receiving (to individuals or broadcasting) selected content such as nude images/videos, images/videos showing private body parts through e-mail, MMS, social networking sites, etc., (3) viewing selected content such as pornography, explicit user-generated videos on browsers, media players or custom applications, etc., and (4) capturing selected content such as sexually explicit images/videos through a mobile device camera, camera, camcorder, etc.

[0025] One or more embodiments provide a real-time, end-to-end, device-integrated protocol implementing a holistic approach of placing checkpoints at processing and functional points in an electronic device through which the user can create, capture, share, receive, and consume content such as texts, e-mails, images, videos, etc. Said protocol is incorporated with hardware and software components of the electronic device for content validation including filtering out content originating from the electronic device as well as terminating on the electronic device, according to an embodiment.

[0026] In one embodiment, incorporating content validation at an origination point in an electronic device includes embedding a device or system in an electronic device for interfacing with a camera module in the electronic device to prevent capturing of selected content such as an inappropriate image/video, wherein content validation includes real-time analysis of live video frames from the mobile device camera. In another embodiment, incorporating content validation at an origination point in an electronic device includes embedding a device or system in an electronic device for interfacing with email/SMS applications, wherein content validation includes monitoring and preventing creation of selected content by real-time word matching against a list such as a blacklist of words and/or phrases.

[0027] In one embodiment, incorporating content validation at a termination point in an electronic device includes embedding a device or system in an electronic device for interfacing with image gallery storage (e.g., in the electronic device), wherein content validation includes analyzing each image/video file before opening it (e.g., from an email attachment) and preventing viewing if found to be inappropriate. In another embodiment, incorporating content validation at a termination point in an electronic device includes embedding a device or system in an electronic device for interfacing with a browser on the electronic device, wherein content validation includes analyzing and preventing access to selected content from each link.

[0028] In one embodiment, incorporating content validation at a termination point in an electronic device includes embedding a device or system in an electronic device for interfacing with an SMS/Email application in the electronic device, wherein content validation includes analyzing messages for selected content such as blacklisted words and filtering out such selected content before showing messages to a user.

[0029] In one embodiment, content validation includes only filtering selected words (e.g., "bad" or inappropriate words). In another embodiment, content validation filtering may include preventing a user from viewing an entire sentence itself. In one embodiment, the filtering may be based on application and business partner requests (e.g., the carriers). In one embodiment, words are analyzed before they may be viewed by a user on a display (or heard via an audio device) and taking one of multiple possible steps to handle the outcome once the trigger (i.e., selected words) is received.

[0030] In embodiment, incorporating content validation includes embedding a device or system in an electronic device for interfacing with a multimedia messaging service (MMS) application, wherein content validation includes analyzing each image/video received, and filtering out selected content before showing it to a user.

[0031] In one embodiment, content validation includes filtering out selected content from media before the media originates or terminates on an electronic device. In another embodiment, content validation includes preventing access to media that includes such selected content via the electronic device. In one embodiment, content validation includes analyzing media and filtering out selected content during creation of the media, using real-time analysis of media (such as images, videos, text, words, web site links, etc.) using the device or system on an electronic device. The analysis is performed in real time using the device or system on the mobile device itself, and therefore it is network and server-independent.

[0032] FIG. **1** is a schematic view of a communications system, in accordance with one embodiment. Communications system **1** may include a communications device that initiates an outgoing communications operation (transmitting device **2**) and a communications network **110**, which transmitting device **2** may use to initiate and conduct communications operations with other communications devices within communications network **110**. For example, communications

system **1** may include a communication device that receives the communications operation from the transmitting device **2** (receiving device **3**). Although communications system **1** may include multiple transmitting devices **2** and receiving devices **3**, only one of each is shown in FIG. **1** to simplify the drawing.

[0033] Any suitable circuitry, device, system or combination of these (e.g., a wireless communications infrastructure including communications towers and telecommunications servers) operative to create a communications network may be used to create communications network **110**. Communications network **110** may be capable of providing communications using any suitable communications protocol. In some embodiments, communications network **110** may support, for example, traditional telephone lines, cable television, Wi-Fi (e.g., an IEEE 802.11 protocol), Bluetooth®, high frequency systems (e.g., 900 MHz, 2.4 GHz, and 5.6 GHz communication systems), infrared, other relatively localized wireless communication protocol, or any combination thereof. In some embodiments, the communications network **110** may support protocols used by wireless and cellular phones and personal email devices (e.g., a Blackberry®). Such protocols can include, for example, GSM, GSM plus EDGE, CDMA, quadband, and other cellular protocols. In another example, a long range communications protocol can include Wi-Fi and protocols for placing or receiving calls using VoIP or LAN. The transmitting device **2** and receiving device **3**, when located within communications network **110**, may communicate over a bidirectional communication path such as path **4**. Both the transmitting device **2** and receiving device **3** may be capable of initiating a communications operation and receiving an initiated communications operation.

[0034] The transmitting device **2** and receiving device **3** may include any suitable device for sending and receiving communications operations. For example, the transmitting device **2** and receiving device **3** may include a mobile telephone devices, television systems, cameras, camcorders, a device with audio video capabilities, tablets, and any other device capable of communicating wirelessly (with or without the aid of a wireless-enabling accessory system) or via wired pathways (e.g., using traditional telephone wires). The communications operations may include any suitable form of communications, including for example, voice communications (e.g., telephone calls), data communications (e.g., e-mails, text messages, media messages), or combinations of these (e.g., video conferences).

[0035] FIG. **2** shows a functional block diagram of an architecture system **100** that may be used for content validation on an electronic device **120**, according to an embodiment. Both the transmitting device **2** and receiving device **3** may include some or all of the features of the electronics device **120**. In one embodiment, the electronic device **120** may comprise a display **121**, a microphone **122**, an audio output **123**, an input mechanism **124**, communications circuitry **125**, control circuitry **126**, a camera module **128**, an embedded content validation device **135**, and any other suitable components. In one embodiment, applications **1**-N **127** are provided and may be obtained from a cloud or server **130**, a communications network **110**, etc., where N is a positive integer equal to or greater than 1.

[0036] In one embodiment, all of the applications employed by the audio output **123**, the display **121**, input mechanism **124**, communications circuitry **125**, and the microphone **122** may be interconnected and managed by control circuitry **126**. In one example, a handheld music player capable of transmitting music to other tuning devices may be incorporated into the electronics device **120**.

[0037] In one embodiment, the audio output **123** may include any suitable audio component for providing audio to the user of electronics device **120**. For example, audio output **123** may include one or more speakers (e.g., mono or stereo speakers) built into the electronics device **120**. In some embodiments, the audio output **123** may include an audio component that is remotely coupled to the electronics device **120**. For example, the audio output **123** may include a headset, headphones, or earbuds that may be coupled to communications device with a wire (e.g., coupled to electronics device **120** with a jack) or wirelessly (e.g., Bluetooth® headphones or a Bluetooth® headset).

[0038] In one embodiment, the display **121** may include any suitable screen or projection system for providing a display visible to the user. For example, display **121** may include a screen (e.g., an LCD screen) that is incorporated in the electronics device **120**. As another example, display **121** may include a movable display or a projecting system for providing a display of content on a surface remote from electronics device **120** (e.g., a video projector). Display **121** may be operative to display content (e.g., information regarding communications operations or information regarding available media selections) under the direction of control circuitry **126**.

[0039] In one embodiment, input mechanism **124** may be any suitable mechanism or user interface for providing user inputs or instructions to electronics device **120**. Input mechanism **124** may take a variety of forms, such as a button, keypad, dial, a click wheel, or a touch screen. The input mechanism **124** may include a multi-touch screen.

[0040] In one embodiment, communications circuitry **125** may be any suitable communications circuitry operative to connect to a communications network (e.g., communications network **110**, FIG. **1**) and to transmit communications operations and media from the electronics device **120** to other devices within the communications network. Communications circuitry **125** may be operative to interface with the communications network using any suitable communications protocol such as, for example, Wi-Fi (e.g., an IEEE 802.11 protocol), Bluetooth®, high frequency systems (e.g., 900 MHz, 2.4 GHz, and 5.6 GHz communication systems), infrared, GSM, GSM plus EDGE, CDMA, quadband, and other cellular protocols, VoIP, or any other suitable protocol.

[0041] In some embodiments, communications circuitry **125** may be operative to create a communications network using any suitable communications protocol. For example, communications circuitry **125** may create a short-range communications network using a short-range communications protocol to connect to other communications devices. For example, communications circuitry **125** may be operative to create a local communications network using the Bluetooth® protocol to couple the electronics device **120** with a Bluetooth® headset.

[0042] In one embodiment, control circuitry **126** may be operative to control the operations and performance of the electronics device **120**. Control circuitry **126** may include, for example, a processor, a bus (e.g., for sending instructions to the other components of the electronics device **120**), memory, storage, or any other suitable component for controlling the operations of the electronics device **120**. In some embodiments, a processor may drive the display and process inputs

received from the user interface. The memory and storage may include, for example, cache, Flash memory, ROM, and/or RAM. In some embodiments, memory may be specifically dedicated to storing firmware (e.g., for device applications such as an operating system, user interface functions, and processor functions). In some embodiments, memory may be operative to store information related to other devices with which the electronics device **120** performs communications operations (e.g., saving contact information related to communications operations or storing information related to different media types and media items selected by the user).

[0043] In one embodiment, the control circuitry **126** may be operative to perform the operations of one or more applications implemented on the electronics device **120**. Any suitable number or type of applications may be implemented. Although the following discussion will enumerate different applications, it will be understood that some or all of the applications may be combined into one or more applications. For example, the electronics device **120** may include an automatic speech recognition (ASR) application, a dialog application, a map application, a media application (e.g., QuickTime, MobileMusic.app, or MobileVideo.app), social networking applications (e.g., Facebook®, Twitter®, Etc.), an Internet browsing application, etc. In some embodiments, the electronics device **120** may include one or multiple applications operative to perform communications operations. For example, the electronics device **120** may include a messaging application, a mail application, a voicemail application, an instant messaging application (e.g., for chatting), a videoconferencing application, a fax application, or any other suitable application for performing any suitable communications operation.

[0044] In some embodiments, the electronics device **120** may include a microphone **122**. For example, electronics device **120** may include microphone **122** to allow the user to transmit audio (e.g., voice audio) for speech control and navigation of applications **1**-N **127**, during a communications operation or as a means of establishing a communications operation or as an alternative to using a physical user interface. The microphone **122** may be incorporated in the electronics device **120**, or may be remotely coupled to the electronics device **120**. For example, the microphone **122** may be incorporated in wired headphones, the microphone **122** may be incorporated in a wireless headset, the microphone **122** may be incorporated in a remote control device, etc.

[0045] In one embodiment, the camera module **128** comprises a camera device that includes functionality for capturing still and video images, editing functionality, communication interoperability for sending, sharing, etc. photos/videos, etc.

[0046] In one embodiment, the electronics device **120** may include any other component suitable for performing a communications operation. For example, the electronics device **120** may include a power supply, ports, or interfaces for coupling to a host device, a secondary input mechanism (e.g., an ON/OFF switch), or any other suitable component.

[0047] In one embodiment, the content validation device **135** provides incorporation of content validation at an origination point in the electronic device **120** for interfacing with the camera module **128** on the electronic device **120** to prevent capturing of selected content, such as an inappropriate image/video, wherein content validation includes real-time analysis of live video frames from the camera module **128**. In another embodiment, incorporating content validation at an origination point in the electronic device **120** includes embedding the content validation device **135** in the electronic device **120** for interfacing with email/SMS applications (e.g., applications **1**-N **127**), wherein content validation includes monitoring and preventing creation of selected content by real-time word matching against a list such as a blacklist of words and/or phrases.

[0048] FIG. **3** shows a block diagram of the content validation device **135** for content validation of an electronic device **120**, according to an embodiment. In one embodiment, the content validation device **135** includes a processing block **136**, a memory block **137**, a detection module **138**, and a validation module **139**.

[0049] In one embodiment, a content interface **140** interfaces with the electronic device **120** for communications between the content validation device **135** and the electronic device **120**. In one embodiment, the processing block **136** comprises one or more processors, microprocessors, etc. In one embodiment, the memory block **137** comprises one or more memory devices. In one embodiment, the detection module **138** detects inappropriate text, voice, and images received from the electronic device **120**. In one embodiment, the content interface comprises a bus, or other type of appropriate interface.

[0050] FIG. **4** shows a block diagram of an architecture **10** for content validation checkpoints **11** on a mobile device for stages in the life of content, such as when content originates, terminates and is processed in a mobile device. In one embodiment, the content validation checkpoints include content communication modules **12** that forward content to the content validation device **135** for analyzing, detecting, and filtering selected content such as inappropriate content (e.g., images, videos, texts, emails) that originates or terminates at the electronic device **120**. The content communication modules **12** forward content to the content validation device **135** over the content interface **140** for proactively preventing selected content from being recorded, sent/received, and consumed via the mobile device.

[0051] In one embodiment, the content validation device **135** provides image, video, URL, and text analysis engines for content from checkpoints situated both on the mobile device as well as in the network. For applications which inherently rely on network connectivity, such as online video streaming, the content validation device **135** may be implemented to receive content from the network. One or more embodiments proactively screen out content before it reaches the user's eyes rather than reactively raising alerts. Example scenarios for performing content validation for content from a network server include viewing videos on a website through the electronic device **120** and attempting to view nude/inappropriate images on a browser.

[0052] In one embodiment, the content validation device **135** is integrated seamlessly with the functions of the electronic device **120** using the content communication modules **12** for content origination, termination, and processing, as described herein. In one embodiment, instead of using content communication modules **12**, all content is first passed from the electronic device **120** to the content validation device **135** prior to being output by the electronic device **120** for a user's consumption.

[0053] FIG. **5** shows a block diagram of an architecture **20** for an implementation of the content validation process **22** of the validation module **139** for image content validation for the camera module **128** on the electronic device **120**, according to

an embodiment. In one embodiment, the image content validation process **22** uses the detection module **138** for providing real-time image detection to prevent capturing selected content, such as nude images/videos, via the camera module **128**. The image content validation process **22** combines with an image analysis process **22**A (of the detection module **138**), which analyzes an image **25** to detect selected content therein, and a controller process **22**B of the validation module **139** that filters the detected selected content (e.g., inappropriate nudity image).

[0054] In one embodiment, the content validation process **22** is not network dependent and performs its function on the electronic device **120**. In another embodiment, the content validation process **22** performs post and processing/integration with the gallery. In one example implementation, analysis of image/video content for content validation begins after the content is captured but before it is saved in the gallery/file structure. In one embodiment, saving only occurs once the content validation module clears the content (e.g., indicates the content does not include inappropriate information). Otherwise, the content is not saved and any (if at all) temporary files or caches are deleted.

[0055] In another embodiment, in an example implementation analysis of image/video content for content validation includes analysis of raw content frames as soon as the camera module **128** is invoked either for video or still image capture. Real-time frame analysis is performed on the raw frames received from the camera buffer at a particular sampling rate appropriate to meet performance requirements while allowing desired content filtering. In one example, whenever frames including inappropriate content are detected, corresponding functions are invoked such as disabling camera shutter, turning off camera, etc. The analysis and invoked functions may be based on several factors including performance (e.g., processing power, battery, latency, etc.), partner requests (e.g., carrier requests), business case variations, cultural nuances, target demographics (e.g., age, geographical region, etc.). In one embodiment, content validation analysis for appropriate and inappropriate content occurs in real-time such that a frame-by-frame analysis detects and validates captured frames in order to avoid situations where a user attempts to capture appropriate content in a first frame and inappropriate content in a next frame, or vice-versa.

[0056] FIG. **6** shows a block diagram of an architecture **30** for an implementation of a content communication module **12** for forwarding content to the validation device **135** on the electronic device **120**, according to an embodiment. In one embodiment, the content validation device **135** receives intercepted message flow to check outgoing and incoming content for selected content. In one embodiment, the content validation device **135** interfaces with an e-mail module **31**, a messaging module **33**, an social networking site (SNS)module **35**, and a transceiver module **37**. The content validation device **135** receives intercepted message flow from the content interface **140** through modules **31**, **33**, **35**, and **37** and checks outgoing and incoming content for selected content.

[0057] In one embodiment, the content validation device **135** includes a detector **32**A (of the detection module **138**) that checks for an image/video in a message. The content validation device **135** further includes an image analysis module **32**B that checks a detected image/video for selected image content (e.g., nudity) and filters out the image/video if it contains said selected image content. The content validation device **135** further includes a word analysis module **32**C that checks a message for selected word content (e.g., selected words, phrases) and filters out the message if it contains said selected word content.

[0058] In one embodiment, the content validation device **135** prevents consumption of selected content by integrating with mobile device applications (e.g., web browser, image gallery application, YouTube, media player) to disallow viewing/playing inappropriate content. Such integration, at lower application layers on the electronic device **120**, allows validation of content such as streaming content (e.g., video/photos) before such content is shown on a display **121** of the electronic device **120**.

[0059] One or more embodiments provide a web portal monitoring module **38** for a secure web-based frontend, which users (e.g., parents) may access to monitor traffic on selected user (e.g., teenager) electronic devices **120**. In one example, the monitoring module **38** allows viewing images and videos taken and received on a selected electronic device **120**. The monitoring module **38** further allows separate viewing for deleted/blacklisted content originated/terminated on a selected user electronic device **120**. The monitoring module **38** further allows viewing filtered out texts, emails, containing black listed words originated/terminated on a selected user electronic device **120**. In one embodiment, the monitoring module **38** further allows set up of alerts for certain events (e.g., incoming nude picture, etc.) on a selected user electronic device **120**. The server **39** hosts blacklisted words, acronyms, and phrases dictionaries which may be periodically synchronized to the one residing on the electronic device **120**. The period may be customizable (e.g., once per week). This will ensure that the on-device blacklist is always up-to-date.

[0060] FIG. **7** shows a flowchart of a content validation process **40** for filtering selected content originating at an electronic device (such as electronic device **120**), according to an embodiment. In one embodiment, the electronic device has an image capture camera. In one embodiment, the content validation process **40** is embedded in a mobile device and integrated with the electronic device functions (i.e., camera integration) for analyzing content and filtering out inappropriate content originating at the mobile device.

[0061] In one embodiment, in process block **41**, the device camera function is invoked for a user to capture content such as an image or video. In one embodiment, in process block **42**, each image frame (or video frame) is immediately analyzed in real time to detect selected content (e.g., nudity, over exposed body) in the image frame. In one embodiment, process block **43** comprises disabling the camera shutter if such selected content is detected in the image frame. In one example, such image frame is discarded so that is it not available for further processing such as storage, viewing, transmission, etc. In one embodiment, process block **44** comprises repeating process blocks **42-43** for each image frame and enabling the camera shutter to capture a next image frame as soon as an analyzed image frame does not contain the selected content.

[0062] FIG. **8** shows a flowchart of a content validation process **50** for filtering selected content originating at an electronic device (such as electronic device **120**), according to an embodiment. In one embodiment, the electronic device may wirelessly communicate information. In one embodiment, the content validation process **50** is embedded in a device (e.g., content validation device **135**) and integrated with the electronic device functions (e.g., SMS Integration)

for analyzing content and filtering out inappropriate content originating at the mobile device.

[0063] In one embodiment, process block **51** comprises invoking an SMS application of the electronic device for a user to send a text message. In one embodiment, in process block **52**, each word typed is automatically analyzed by matching against selected content in real time (e.g., a blacklist of inappropriate words) to detect if the word is inappropriate. In one embodiment, in process block **53**, if any typed word is a blacklisted word, then the Send button of the SMS application is disabled. The user is allowed to edit the words typed in, and the words are analyzed as in process blocks **52-53**. In one embodiment, in process block **54**, as soon as all blacklisted words are deleted from the text message, the Send button of the SMS application is enabled again.

[0064] In one example embodiment, a user keeps typing a message normally without any interruptions even for blacklisted words. When the user attempts to send the message, a content validation device intercepts the send command and performs analysis on the message text to detect blacklisted words before the message is actually sent. If none is detected, then the message is transmitted from the electronic device. If a blacklisted word is detected, then the user is notified told that the message cannot be sent because of the content or the control is returned to the SMS application to transmit the message with the blacklisted words deleted. In another example, for every word that is typed, it is immediately matched against a blacklist and the Send button is disabled if a current sentence includes any blacklisted words. In one embodiment, only when the complete sentence is devoid of any blacklisted words is the send button enabled for the user to send the message.

[0065] FIG. **9** shows a flowchart of a content validation process **60** for filtering out selected content terminating at an electronic device (such as electronic device **120**), according to an embodiment. In one embodiment, the electronic device may wirelessly communicate information. The content validation process **60** is embedded in a device (e.g., content validation device **135**) and integrated with the electronic device functions (e.g., image gallery integration) for analyzing content and filtering out incoming inappropriate content terminating at the electronic device.

[0066] In one embodiment, process block **61** comprises invoking an image viewer application (e.g., image gallery) of the electronic device for a user to view an incoming image on the electronic device display (e.g., display **121**) and receiving user command (e.g., user click) to view an image file (e.g., from email/SMS). In one embodiment, in process block **62**, the image viewer application receives an intent to open image file message. In one embodiment, in process block **63**, before opening, the image is analyzed by an image analyzer to detect selected content, such as inappropriate nudity. In one embodiment, in process block **64**, if the image is detected to be inappropriate, the image file is not opened for viewing. In one example embodiment, the user receives a message (e.g., "Content inappropriate to view" message).

[0067] FIG. **10** shows a flowchart of a content validation process **70** for filtering selected content terminating at an electronic device (such as electronic device **120**), according to an embodiment. In one embodiment, the electronic device may wirelessly communicate information. In one embodiment, the content validation process **70** is embedded in a device (e.g., content validation device **135**) and integrated with the electronic device functions (e.g., Browser/YouTube® Integration) for analyzing content and filtering out incoming inappropriate content terminating at the electronic device.

[0068] In one embodiment, process block **71** comprises invoking a web application, such as a browser or YouTube® based on user request, and receiving user command to open an embedded video from the Internet. In one embodiment, process block **72** comprises, before playing the video, analyzing the video to detect selected content such as inappropriate content. In one embodiment, process block **73** comprises, upon detecting inappropriate content, preventing the web application from playing the video. In one example embodiment, the video is completely stopped from playing on the mobile device. In another example embodiment, image frames within appropriate content are deleted from the video and the remainder of the images frames are displayed to the user on the mobile device.

[0069] FIG. **11** shows a flowchart of a content validation process **80** for filtering selected content terminating at an electronic device (such as electronic device **120**). In one embodiment, the electronic device may wirelessly communicate information. In one embodiment, the content validation process **80** is embedded in a device (e.g., content validation device **135**) and integrated with the electronic device functions (e.g., SMS Integration) for analyzing content and filtering out incoming inappropriate content terminating at the electronic device.

[0070] In one embodiment, process block **81** comprises receiving an SMS text message via an SMS application on the electronic device, without notifying the user of the received text message. In one embodiment, process block **82** comprises, before sending out a notification to the user on the electronic device, analyzing the text message to find blacklisted words (e.g., inappropriate words, profanity). In one embodiment, process block **83** comprises, if any blacklisted words are found, preventing the message from being displayed to the user on the electronic device by the SMS application. In one example embodiment, a received SMS message with inappropriate words is deleted (filtered out) without user knowledge. In another example embodiment, a received SMS message with inappropriate words is not displayed, but the user is notified that a SMS text message has arrived, which was not shown due to inappropriate content.

[0071] In one or more of the above content validation processes, if content validation indicates that inappropriate content is not detected, then the content is processed by the electronic device as normal operation (i.e., without filtering out by the content validation process).

[0072] In one embodiment, filtering out selected content (e.g., inappropriate content) from terminated/originated content comprises blocking the entire terminated/originated content that includes the selected content. In another embodiment, filtering out selected content comprises blocking only the detected selected content and processing the remainder of the terminated/originated content as usual. There may also be relevant messages or pop-ups to let the user know that content was blocked. There may also be a notification or alert sent out to other users (e.g., parent) when such inappropriate content is detected.

[0073] According to one or more embodiments, after content is analyzed (and found to include selected content such as inappropriate content), such content may be handled in different ways, including but not limited to: deleted without user knowledge, deleted with user knowledge (e.g., pop-up noti-

fication), sending notification (e.g., SMS, email) to a controlling individual such as a parent, replacing content with appropriate content, and generating a warning pop-up (e.g., "This content is inappropriate for your viewing.") but without deleting the content or notifying the parent.

[0074] According to one or more embodiments, web portal monitoring by a controlling individual such as a parent includes automatically uploading detected inappropriate content from the mobile device to a server that is accessible by such individual. The individual is allowed to view the inappropriate content and take actions including: set thresholds for flagging selected content (e.g., according to age, personal preferences, etc.) to prevent dissemination thereof, set up alerts for certain events, and enable/disable features on the mobile device. In one embodiment, the content validation analysis may be enabled/disabled by a user (e.g., a parent) remotely from another device, a website, cloud computing environment, etc.

[0075] As is known to those skilled in the art, the aforementioned example architectures described above, according to said architectures, can be implemented in many ways, such as program instructions for execution by a processor, as software modules, microcode, as computer program product on computer readable media, as analog/logic circuits, as application specific integrated circuits, as firmware, as consumer electronic devices, AV devices, wireless/wired transmitters, wireless/wired receivers, networks, multi-media devices, etc. Further, embodiments of said Architecture can take the form of an entirely hardware embodiment, an entirely software embodiment or an embodiment containing both hardware and software elements.

[0076] One or more embodiments have been described with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to one or more embodiments. Each block of such illustrations/diagrams, or combinations thereof, can be implemented by computer program instructions. The computer program instructions when provided to a processor produce a machine, such that the instructions, which execute via the processor create means for implementing the functions/operations specified in the flowchart and/or block diagram. Each block in the flowchart/block diagrams may represent a hardware and/or software module or logic, implementing one or more embodiments. In alternative implementations, the functions noted in the blocks may occur out of the order noted in the figures, concurrently, etc.

[0077] The terms "computer program medium," "computer usable medium," "computer readable medium", and "computer program product," are used to generally refer to media such as main memory, secondary memory, removable storage drive, a hard disk installed in hard disk drive. These computer program products are means for providing software to the computer system. The computer readable medium allows the computer system to read data, instructions, messages or message packets, and other computer readable information from the computer readable medium. The computer readable medium, for example, may include non-volatile memory, such as a floppy disk, ROM, flash memory, disk drive memory, a CD-ROM, and other permanent storage. It is useful, for example, for transporting information, such as data and computer instructions, between computer systems. Computer program instructions may be stored in a computer readable medium that can direct a computer, other programmable data processing apparatus, or other devices to function in a particular manner, such that the instructions stored in the computer readable medium produce an article of manufacture including instructions which implement the function/act specified in the flowchart and/or block diagram block or blocks.

[0078] Computer program instructions representing the block diagram and/or flowcharts herein may be loaded onto a computer, programmable data processing apparatus, or processing devices to cause a series of operations performed thereon to produce a computer implemented process. Computer programs (i.e., computer control logic) are stored in main memory and/or secondary memory. Computer programs may also be received via a communications interface. Such computer programs, when executed, enable the computer system to perform the features of the embodiments as discussed herein. In particular, the computer programs, when executed, enable the processor and/or multi-core processor to perform the features of the computer system. Such computer programs represent controllers of the computer system. A computer program product comprises a tangible storage medium readable by a computer system and storing instructions for execution by the computer system for performing a method of one or more embodiments.

[0079] Though the embodiments have been described with reference to certain versions thereof; however, other versions are possible. Therefore, the spirit and scope of the appended claims should not be limited to the description of the preferred versions contained herein.

What is claimed is:

1. A circuit device, comprising:

a processing device coupled to a memory;

the processing device comprising:

a detection module that detects information content received in the memory from an electronic device; and

a validation module that validates the information content in real time,

wherein validating the information content includes analyzing the information content to detect selected content, and preventing dissemination of the selected content from the electronic device.

2. The circuit device of claim **1**, wherein:

the validation module prevents dissemination of the selected content via the electronic device by filtering the selected content using the processing device on the electronic device.

3. The circuit device of claim **2**, wherein:

the detection module detects information content on the electronic device by detecting origination of information content on the electronic device.

4. The circuit device of claim **3**, wherein:

the validation module filters the selected content to prevent communication of the selected content from the electronic device.

5. The circuit device of claim **4**, wherein:

the detection module detects origination of information content on the electronic device by detecting creation of the information content on the electronic device.

6. The circuit device of claim **5**, wherein the creation of the information content that is detected by the detection module is received in the memory from one or more of an image capture module, a short message service (SMS) module, a multimedia messaging service (MMS) module, an email module, a browser module, and a social network module.

7. The circuit device of claim **2**, wherein:

the detection module detects information content on the electronic device by detecting termination of information content on the electronic device.

8. The circuit device of claim **7**, wherein:

the validation module filters the selected content to prevent access to the selected content via the electronic device.

9. The circuit device of claim **8**, wherein:

the detection module detects termination of information content on the electronic device by detecting reception of the information content on the electronic device.

10. The circuit device of claim **9**, wherein the termination of information content is detected by the detection module from one or more of an image capture module, a short message service (SMS) module, a multimedia messaging service (MMS) module, an email module, a browser module, and a social network module.

11. The circuit device of claim **2**, wherein:

the information content comprises content selected from: text, image, video, and audio information content.

12. The circuit device of claim **2**, wherein the circuit device comprises one of a system on chip (SOC) device, an application specific integrated circuit (ASIC) device, and a firmware device.

13. The circuit device of claim **12**, wherein the electronic device comprises one of a mobile phone device, a camera device, a tablet computing device, a laptop computing device, and a personal computer (PC) device.

14. The circuit device of claim **1**, wherein the validation module prevents dissemination of the selected content via the electronic device by filtering out the selected content on the electronic device and preventing consumption of the selected content on the electronic device by a user.

15. The circuit device of claim **1**, wherein the validation module prevents dissemination of the selected content via the electronic device by filtering out the selected content on the electronic device and preventing communication of the selected content from the electronic device by a user.

16. A method for content validation, comprising:

detecting information content using a processing device;

validating the information content using the processing device, wherein validating the information content includes:

analyzing the information content to detect selected content; and

preventing dissemination of the selected content via an electronic device.

17. The method of claim **16**, wherein:

validating the information content includes validating the information content in real time using the processing device on the electronic device by analyzing the information content to detect selected content, and preventing dissemination of the selected content via the electronic device comprises filtering the selected content using the processing device on the electronic device.

18. The method of claim **17**, wherein:

detecting information content using the processing device comprises detecting origination of information content using the processing device on the electronic device; and

filtering the selected content comprises filtering the selected content to prevent communication of the selected content from the electronic device.

19. The method of claim **18**, wherein:

detecting origination of information content using the processing device comprises detecting creation of the information content on the electronic device; and

the creation of the information content that is received by the processing device from one or more of an image capture module, a short message service (SMS) module, a multimedia messaging service (MMS) module, an email module, a browser module, and a social network module.

20. The method of claim **17**, wherein:

detecting information content on the electronic device comprises detecting termination of information content on the electronic device; and

filtering the selected content comprises filtering the selected content to prevent access to the selected content via the electronic device.

21. The method of claim **20**, wherein:

detecting termination of information content on the electronic device comprises detecting reception of the information content on the electronic device; and

the termination of information content is detected by the processing device from one or more of an image capture module, a short message service (SMS) module, a multimedia messaging service (MMS) module, an email module, a browser module, and a social network module.

22. The method of claim **17**, wherein:

the information content comprises content selected from: text, image, video and audio information content.

23. The method of claim **17**, wherein the processing device comprises one of a system on chip (SOC) device, an application specific integrated circuit (ASIC) device, and a firmware device.

24. The method of claim **23**, wherein the electronic device comprises one of a mobile phone device, a camera device, a tablet computing device, a laptop computing device, and a personal computer (PC) device.

25. The method of claim **16**, wherein:

preventing dissemination of the selected content via the electronic device comprises filtering out the selected content using the processing device on the electronic device and preventing consumption of the selected content on the electronic device by a user; and

preventing dissemination of the selected content via the electronic device comprises filtering out the selected content using the processing device on the electronic device and preventing communication of the selected content from the electronic device by a user.

26. An apparatus, comprising:

an integrated circuit (IC) coupled with a memory; and

a content interface coupled between the IC and an electronic device;

the IC comprising:

a detection module that detects information content received in the memory over the content interface from an electronic device; and

a validation module that validates the information content in real time,

wherein validating the information content includes analyzing the information content to detect selected content, and preventing dissemination of the selected content from the electronic device.

27. The apparatus of claim **26**, wherein:

the validation module prevents dissemination and communication of the selected content via the electronic device by filtering the selected content using the processing device on the electronic device; and.

the detection module detects information content on the electronic device by detecting origination and creation of information content on the electronic device.

28. The apparatus of claim **27**, wherein:

the detection module detects information content on the electronic device by detecting termination of information content on the electronic device; and

the validation module filters the selected content to prevent access to the selected content via the electronic device.

29. The apparatus of claim **28**, wherein:

the information content comprises content selected from: text, image, video, and audio information content;

the validation module prevents dissemination of the selected content via the electronic device by filtering out the selected content on the electronic device and preventing consumption and communication of the selected content on the electronic device by a user.

30. The apparatus of claim **29**, wherein the IC is embedded in the electronic device, and the electronic device comprises one of a mobile phone device, a camera device, a tablet computing device, a laptop computing device and a personal computer (PC) device.

* * * * *